Susanna S. Epp

Discrete Mathematics with Applications Third Edition

for

Discrete Mathematics with Applications
Third Edition

Susanna S. Epp

Instructor's Manual

for

Discrete Mathematics
with Applications

Third Edition

Susanna S. Epp
DePaul University

with the assistance of
Tom Jenkyns
Brock University

THOMSON

BROOKS/COLE

Australia • Canada • Mexico • Singapore • Spain • United Kingdom • United States

For more information about our products,
contact us at:
Thomson Learning Academic Resource Center
1-800-423-0563

For permission to use material from this text or
product, submit a request online at
http://www.thomsonrights.com.
Any additional questions about permissions can be
submitted by email to **thomsonrights@thomson.com.**

http://pakimonda.blog.com
paki.monda@gmail.com
paki.monda@yahoo.com

INSTRUCTOR'S MANUAL

FOR

DISCRETE MATHEMATICS WITH APPLICATIONS

THIRD EDITION

Susanna S. Epp
DePaul University

with the assistance of
Tom Jenkyns
Brock University

Table of Contents

Preface

This manual contains complete solutions to all exercises not fully solved in Appendix B of the third edition of *Discrete Mathematics with Applications*, and suggestions for how to teach the material in the book. The suggestions are directed primarily toward those who have not previously taught discrete mathematics at the freshman-sophomore level. Most are based on my own experience and are offered modestly and with apologies to those whose pedagogical insights are deeper than my own. Comments and suggestions from users of this manual are always welcome. The manual also contains review material for each chapter, additional problems to use for extra practice or exams, and ideas for projects. The review material is also included in the *Student Solutions Manual and Review Guide for Discrete Mathematics with Applications, 3rd edition*.

The primary aim of *Discrete Mathematics with Applications* is to help students attain the knowledge and reasoning skills they need to be successful in upper-level computer science and mathematics courses. Three parallel threads run through the book: exposition of standard facts of discrete mathematics, incremental development of mathematical reasoning skills, and discussion of applications. Almost every section contains exercises designed to help students explore facts, theory, and applications. You can assign whatever mix you wish of exercises of the three types.

The book contains unusually complete explanations and a very large number of illustrative examples on the theory that it is easier for a student who has caught on to an idea to skim over a passage than for a student who is still mystified to fill in the reason for something that is not understood. The extensiveness of the exposition should also make it possible to use the book in courses that use class time primarily for collaborative learning and problem solving rather than lecturing. Each section contains exercises of several different levels of difficulty so that you can choose those most appropriate for your students.

Like many other skills, the skill of mathematical reasoning, once acquired, becomes such a fundamental part of a person's being that it passes from consciousness to instinct. It is natural for mathematicians to think that things that seem totally obvious and trivial to them are equally obvious and trivial to their students. However, the habit of reasoning according to standard logical principles is thought to be innate in only about 4% of the population. Large numbers of students confuse a statement with its converse, do not intuitively understand the equivalence between a statement and its contrapositive (which means that the idea of proof by contradiction is foreign to them), think that the negation of "All mathematicians wear glasses" is "No mathematicians wear glasses," and have the dim impression that an irrational number is any decimal that goes on forever (such as 0.333333. . .). Of course, the extent to which students have such misconceptions varies from school to school, but no institution is immune and at many the problem is epidemic.

Because of the wide variety of backgrounds and abilities of students typically enrolled in a discrete mathematics course, it is important to stay in close touch with how your students are doing. The following are various techniques that have been found helpful:

- Increasing the discussion part of a lecture-discussion class by encouraging students to interrupt lectures with questions and by asking frequent, non-rhetorical questions of students. To counteract the problem of having only a small group of students respond to questions, you might call on students by name, using a class list if necessary. If you find that students are unable to answer simple questions on the material being presented, you can backtrack immediately to find common ground. A side benefit of increased class participation is that it improves students' ability to use mathematical language correctly.

- Having students present their solutions to selected homework exercises at the board, following each presentation with class discussion and (tactful) critique. This technique is especially useful when covering topics that involve proof and disproof and is an effective means both of giving feedback on how students are doing and of conveying to students the standards of exposition required in the course.

- Giving frequent quizzes and grading them promptly. This technique gives both you and your students feedback on the kinds of problems students are having at a point in the course when both you and they can take measures to correct them.

- Assigning a few problems to be done on an "until correct" basis, or allowing students to hand in "draft solutions" that are read by you and are handed back for redoing if they are not entirely correct.

It is likely that some, perhaps even many, of your students will do excellent work. But it is also likely that some will have considerable difficulty, especially if asked to write proofs or justify answers to questions. If you are teaching discrete mathematics for the first time, you may be appalled by the awkwardness and illogic of some of your students' efforts. But the very fact that students have difficulty expressing mathematics logically and coherently attests to the value and importance of trying to teach them how to do it. It takes months for a child to learn to walk, days or weeks to learn to ride a bicycle, swim, or play tennis, and years to learn to read at an advanced level. We should not be discouraged if students catch on slowly to new modes of thinking. Prospective employers of students of mathematics and computer science are looking for brain power in those whom they hire, and students enjoy the feeling that they are increasing their mental capacity. It is in everyone's interest to help students develop as much reasoning capability as possible.

Students often come to a discrete mathematics skeptical of its practical usefulness, especially of those parts that seem abstract. One reason for including the large number of applications in the book is to overcome such skepticism. You can also encourage students to broaden their perspective by referring, whenever possible, to relationships between the topics and modes of thought under discussion and actual uses in computer science. You do not need to be an expert to convey these ideas effectively. Much can be learned by spending some time looking through computer science texts in such areas as data structures, design and analysis of algorithms, relational database theory, theory of computation, and artificial intelligence. It is also desirable, if possible, to coordinate the topics of the course with those of a computer science course that students take concurrently. Hardly anything more effectively convinces students of the utility of discrete mathematics than to hear references to it in their computer science courses.

The part of the Brooks/Cole website (www.brookscole.com) devoted to *Discrete Mathematics with Applications, 3rd edition* contains a variety of material that may be useful for students and for instructors. Because additional material is being added on an ongoing basis, you may want to check the website from time to time. The material available both to students and instructors includes links to websites with discrete mathematics applets and information about discrete mathematical topics, review material, a list of errata, and a set of exercises using Derive that are coordinated with the book. The instructor's portion of the website gives access to PowerPoint slides, to additional review material, and to all the supplementary exercises and exam questions that are contained in this manual.

Acknowledgements

I am enormously indebted to the work of Tom Jenkyns, whose eagle eye, mathematical knowledge, and understanding of language made an invaluable contribution to this volume. I am also most grateful to my husband, Helmut Epp, who constructed all the diagrams and provided much support and wise counsel over many years.

Susanna S. Epp
DePaul University

Chapter 1: The Logic of Compound Statements

The ability to reason using the principles of logic is essential for solving problems in abstract mathematics and computer science and for understanding the reasoning used in mathematical proof and disproof. Because a significant number of students who come to college have had limited opportunity to develop this ability, a primary aim of both Chapters 1 and 2 is to help students develop an inner voice that speaks with logical precision. Consequently, the various rules used in logical reasoning are developed both symbolically and in the context of their somewhat limited but very important use in everyday language. Exercise sets for Sections 1.1–1.3 and 2.1–2.4 contain sentences for students to negate, write the contrapositive for, and so forth. Virtually all students benefit from doing these exercises. Another aim of Chapters 1 and 2 is to teach students the rudiments of symbolic logic as a foundation for a variety of upper-division courses. Symbolic logic is used in, among others, the study of digital logic circuits, relational databases, artificial intelligence, and program verification.

Suggestions

1. In Section 1.1 many students apply De Morgan's law to write the negation of, for example, "$1 < x \leq 3$" as "$1 \geq x > 3$." You may find that it takes some effort to teach them to avoid making this mistake.

2. In Sections 1.1 and 1.4, students have more difficulty than you might expect simplifying statement forms and circuits. Only through trial and error can you learn the extent to which this is the case at your institution. If it is, you might either assign only the easier exercises or build in extra time to teach students how to do the more complicated ones. Discussion of simplification techniques occurs again in Chapter 5 in the context of set theory. At this later point in the course most students are able to deal with it successfully.

3. In ordinary English, the phrase "only if" is often used as a synonym for "if and only if." But it is possible to find informal sentences in which the intuitive interpretation is the same as the logical definition, and it is helpful to give examples of such statements when you introduce the logical definition. For instance, it is not hard to get students to agree that "The team will win the championship only if it wins the semifinal game" means the same as "If the team does not win the semifinal game then it will not win the championship." Once students see this, you can suggest that they remember this translation when they encounter more abstract statements of the form "A only if B."

Through guided discussion, students will also come to agree that the statement "Winning the semifinal game is a necessary condition for winning the championship" translates to "If the team does not win the semifinal game then it will not win the championship." They can be encouraged to use this (or a similar statement) as a reference to help develop intuition for general statements of the form "A is a necessary condition for B."

With students of lower ability, you may find yourself tying up excessive amounts of class time discussing "only if" and "necessary and sufficient conditions" with little success. You might just assign the easier exercises or you might assign exercises on these topics to be done for extra credit (putting corresponding extra credit problems on exams) and use the results to help distinguish A from B students. It is probably best not to omit these topics altogether, though, because the language of "only if" and "necessary and sufficient conditions" is a standard part of the technical vocabulary of textbooks used in upper-division courses.

4. In Section 1.3, many students mistakenly conclude that an argument is valid if, when they compute the truth table, they find a single row in which both the premises and the conclusion are true. To help counteract this misconception, you could give examples of invalid arguments whose truth tables have eight rows, several of which have true premises and a true conclusion. The source of students' difficulty understanding the concept of validity appears to be their tendency to ignore

quantification and to misinterpret if-then statements as "and" statements. Since the definition of validity includes both a universal quantifier and if-then, it is helpful to go back over the definition and the procedures for testing for validity and invalidity after discussing the general topic of universal conditional statements in Section 2.1.

5. Also in Section 1.3, you might suggest that students just familiarize themselves with, but not memorize, the various forms of valid arguments covered in Section 1.3. It is wise, however, to have them learn modus ponens and modus tollens (because these terms are used in some upper-division computer science courses) and converse and inverse errors (because these errors are so common).

Section 1.1

2. common form: If p then q.
$\sim q$
Therefore, $\sim p$.

   b. all prime numbers are odd; 2 is odd

4. common form: If p then q.
If q then r.
Therefore, if p then r.

   b. x equals 0; the guard condition for the **while** loop is false; program execution moves to the next instruction following the loop

5. b. The truth or falsity of this sentence depends on the reference for the pronoun "she." Considered on its own, the sentence cannot be said to be either true or false, and so it is not a statement.

   c. This sentence is true; hence it is a statement.

   d. This is not a statement because its truth or falsity depends on the value of x.

7. $m \wedge \sim c$

8. b. $\sim w \wedge (h \wedge s)$

   c. $\sim w \wedge \sim h \wedge \sim s$

   e. $w \wedge \sim (h \wedge s)$ $(w \wedge (\sim h \vee \sim s)$ is also acceptable)

9. $(n \vee k) \wedge \sim (n \wedge k)$

10. b. $p \wedge \sim q$ d. $(\sim p \wedge q) \wedge \sim r$ e. $\sim p \vee (q \wedge r)$

13. (jaguar AND cheetah)AND (speed OR fastest) AND NOT (car OR automobile OR auto)

15.

p	q	$p \wedge q$	$p \vee q$	$\sim (p \wedge q)$	$(p \wedge q) \vee \sim (p \vee q)$
T	T	T	T	F	T
T	F	F	T	T	T
F	T	F	T	T	T
F	F	F	F	T	T

17.

p	q	r	$\sim q$	$\sim q \vee r$	$p \wedge (\sim q \vee r)$
T	T	T	F	T	T
T	T	F	F	F	F
T	F	T	T	T	T
T	F	F	T	T	T
F	T	T	F	T	F
F	T	F	F	F	F
F	F	T	T	T	F
F	F	F	T	T	F

18.

p	q	r	$\sim p$	$\sim r$	$\sim p \vee q$	$q \wedge \sim r$	$\sim (q \wedge \sim r)$	$p \vee (\sim p \vee q)$	$(p \vee (\sim p \vee q)) \wedge \sim (q \wedge \sim r)$
T	T	T	F	F	T	F	T	T	T
T	T	F	F	T	T	T	F	T	F
T	F	T	F	F	F	F	T	T	T
T	F	F	F	T	F	F	T	T	T
F	T	T	T	F	T	F	T	T	T
F	T	F	T	T	T	T	F	T	F
F	F	T	T	F	T	F	T	T	T
F	F	F	T	T	T	F	T	T	T

20.

p	q	$p \wedge q$	$\sim p$	$\sim q$	$\sim (p \wedge q)$	$\sim p \wedge \sim q$
T	T	T	F	F	F	F
T	F	F	F	T	T	F
F	T	F	T	F	T	F
F	F	F	T	T	T	T

different truth values in rows 2 and 3

The truth table shows that $\sim (p \wedge q)$ and $\sim p \wedge \sim q$ do not always have the same truth values. Therefore they are not logically equivalent.

22.

p	$\mathbf{t}$	$p \wedge \mathbf{t}$	p
T	T	T	T
F	T	F	F

same truth values

The truth table shows that $p \wedge \mathbf{t}$ and p always have the same truth values. Thus they are logically equivalent. This proves the identity law for $\wedge$.

24.

p	q	r	$q \vee r$	$p \wedge q$	$p \wedge r$	$p \wedge (q \vee r)$	$(p \wedge q) \vee (p \wedge r)$
T	T	T	T	T	T	T	T
T	T	F	T	T	F	T	T
T	F	T	T	F	T	T	T
T	F	F	F	F	F	F	F
F	T	T	T	F	F	F	F
F	T	F	T	F	F	F	F
F	F	T	T	F	F	F	F
F	F	F	F	F	F	F	T

same truth values

The truth table shows that $p \wedge (q \vee r)$ and $(p \wedge q) \vee (p \wedge r)$ always have the same truth values. Therefore they are logically equivalent. This proves the distributive law for $\wedge$ over $\vee$.

26.

p	q	r	$p \vee q$	$p \wedge r$	$(p \vee q) \vee (p \wedge r)$	$(p \vee q) \wedge r$	
T	T	T	T	T	T	T	
T	T	F	T	F	T	F	←
T	F	T	T	T	T	T	←
T	F	F	T	F	T	F	
F	T	T	T	F	T	T	
F	T	F	T	F	T	F	←
F	F	T	F	F	F	F	
F	F	F	F	F	F	F	

different truth values

The truth table shows that $p \vee q$ $p \wedge r$ $(p \vee q) \vee (p \wedge r)$ and $(p \vee q) \wedge r$ have different truth values in rows 2, 3, and 6. Hence they are not logically equivalent.

28.

p	q	r	$r \vee p$	$\sim r$	$p \wedge q$	$\sim r \vee (p \wedge q)$	$r \vee q$	$(\sim r \vee (p \wedge q)) \wedge (r \vee q)$	$(r \vee p) \wedge ((\sim r \vee (p \wedge q)) \wedge (r \vee q))$	$p \wedge q$
T	T	T	T	F	T	T	T	T	T	T
T	T	F	T	T	T	T	T	T	T	T
T	F	T	T	F	F	F	T	F	F	F
T	F	F	T	T	F	T	F	F	F	F
F	T	T	T	F	F	F	T	F	F	F
F	T	F	F	T	F	T	T	T	F	F
F	F	T	T	F	F	F	T	F	F	F
F	F	F	F	T	F	T	F	F	F	F

same truth values

The truth table shows that $(r \vee p) \wedge ((\sim r \vee (p \wedge q)) \wedge (r \vee q))$ and $p \wedge q$ always have the same truth values. Hence they are logically equivalent.

30. Sam is not an orange belt or Kate is not a red belt.

32. This computer program does not have a logical error in the first ten lines and it is not being run with an incomplete data set.

33. The dollar is not at an all-time high or the stock market is not at a record low.

34. The train is not late and my watch is not fast.

36. $-10 \geq x$ or $x \geq 2$

38. $0 \leq x$ or $x < -7$

40. The statement's logical form is $(p \wedge q) \vee ((r \wedge x) \wedge t)$, so its negation has the form

$$\begin{aligned}
\sim ((p \wedge q) \vee ((r \wedge s) \wedge t)) &\equiv \sim (p \wedge q) \wedge \sim ((r \wedge s) \wedge t)) \\
&\equiv (\sim p \vee \sim q) \wedge (\sim (r \wedge s) \vee \sim t)) \\
&\equiv (\sim p \vee \sim q) \wedge ((\sim r \vee \sim s) \vee \sim t)).
\end{aligned}$$

Thus a negation is ($num\_orders \geq 50$ or $num\_instock \leq 300$) and (($50 > num\_orders$ or $num\_orders \geq 75$) or $num\_instock \leq 500$).

43.

p	q	r	$\sim p$	$\sim q$	$\sim p \wedge q$	$q \wedge r$	$((\sim p \wedge q) \wedge (q \wedge r))$	$((\sim p \wedge q) \wedge (q \wedge r))$ $\wedge$ $\sim q$
T	T	T	F	F	F	T	F	F
T	T	F	F	F	F	F	F	F
T	F	T	F	T	F	F	F	F
T	F	F	F	T	F	F	F	F
F	T	T	T	F	T	T	T	F
F	T	F	T	F	T	F	F	F
F	F	T	T	T	F	F	F	F
F	F	F	T	T	F	F	F	F

all $F's$

Since all the truth values of $((\sim p \wedge q) \wedge (q \wedge r)) \wedge \sim q$ are F, $((\sim p \wedge q) \wedge (q \wedge r)) \wedge \sim q$ is a contradiction.

44.

p	q	$\sim p$	$\sim q$	$\sim p \vee q$	$p \wedge \sim q$	$(\sim p \vee q) \vee (p \wedge \sim q)$
T	T	F	F	T	F	T
T	F	F	T	F	T	T
F	T	T	F	T	F	T
F	F	T	T	T	F	T

all $T's$

Since all the truth values of $(\sim p \vee q) \vee (p \wedge \sim q)$ are T, $(\sim p \vee q) \vee (p \wedge \sim q)$ is a tautology.

46. *a.* the commutative law for $\vee$ *b.* the distributive law

c. the negation law for $\wedge$ *d.* the identity law for $\vee$

48. *Solution 1:* $\quad p \wedge (\sim q \vee p) \quad \equiv \quad p \wedge (p \vee \sim q) \quad$ commutative law for $\vee$
$$\equiv \quad p \qquad\qquad\quad \text{absorption law}$$

Solution 2: $\quad p \wedge (\sim q \vee p) \quad \equiv \quad (p \wedge \sim q) \vee (p \wedge p) \quad$ distributive law
$$\equiv \quad (p \wedge \sim q) \vee p \qquad \text{identity law for } \wedge$$
$$\equiv \quad p \qquad\qquad\qquad\quad \text{by the steps of exercise 47.}$$

49. $\quad \sim (p \vee \sim q) \vee (\sim p \wedge \sim q) \quad \equiv \quad (\sim p \wedge \sim (\sim q)) \vee (\sim p \wedge \sim q) \quad$ De Morgan's law
$$\equiv \quad (\sim p \wedge q) \vee (\sim p \wedge \sim q) \qquad \text{double negative law}$$
$$\equiv \quad \sim p \wedge (q \vee \sim q) \qquad\qquad\quad \text{distributive law}$$
$$\equiv \quad \sim p \wedge \mathbf{t} \qquad\qquad\qquad\qquad \text{negation law for } \vee$$
$$\equiv \quad \sim p \qquad\qquad\qquad\qquad\quad \text{identity law for } \wedge$$

51. $(p \wedge (\sim (\sim p \vee q))) \vee (p \wedge q)$

$\equiv$	$(p \wedge (\sim (\sim p) \wedge \sim q)) \vee (p \wedge q)$	De Morgan's law
$\equiv$	$(p \wedge (p \wedge \sim q)) \vee (p \wedge q)$	double negative law
$\equiv$	$((p \wedge p) \wedge \sim q)) \vee (p \wedge q)$	associative law for $\wedge$
$\equiv$	$(p \wedge \sim q)) \vee (p \wedge q)$	idempotent law for $\wedge$
$\equiv$	$p \wedge (\sim q \vee q)$	distributive law
$\equiv$	$p \wedge (q \vee \sim q)$	commutative law for $\vee$
$\equiv$	$p \wedge \mathbf{t}$	negation law for $\vee$
$\equiv$	p	identity law for $\wedge$

52. *b.* Yes.

p	q	r	$p \oplus q$	$q \oplus r$	$(p \oplus q) \oplus r$	$p \oplus (q \oplus r)$
T	T	T	F	F	T	T
T	T	F	F	T	F	F
T	F	T	T	T	F	F
T	F	F	T	F	T	T
F	T	T	T	F	F	F
F	T	F	T	T	T	T
F	F	T	F	T	T	T
F	F	F	F	F	F	F

same truth values

The truth table shows that $(p \oplus q) \oplus r$ and $p \oplus (q \oplus r)$ always have the same truth values. So they are logically equivalent.

c. Yes.

p	q	r	$p \oplus q$	$p \wedge r$	$q \wedge r$	$(p \oplus q) \wedge r$	$(p \wedge r) \oplus (q \wedge r)$
T	T	T	F	T	T	F	F
T	T	F	F	F	F	F	F
T	F	T	T	T	F	T	T
T	F	F	T	F	F	F	F
F	T	T	T	F	T	T	T
F	T	F	T	F	F	F	F
F	F	T	F	F	F	F	F
F	F	F	F	F	F	F	F

same truth values

The truth table shows that $(p \oplus q) \wedge r$ and $(p \wedge r) \oplus (q \wedge r)$ always have the same truth values. So they are logically equivalent.

54. The conditions are most easily symbolized as $p \vee (q \wedge \sim (r \wedge (s \wedge t)))$, but may also be written in a logically equivalent form.

Section 1.2

2. If I catch the 8:05 bus, then I am on time for work.

4. If you don't fix my ceiling, then I won't pay my rent.

6.

p	q	$\sim p$	$\sim p \wedge q$	$p \vee q$	$(p \vee q) \vee (\sim p \wedge q)$	$(p \vee q) \vee (\sim p \wedge q) \to q$
T	T	F	F	T	T	T
T	F	F	F	T	T	F
F	T	T	T	T	T	T
F	F	T	F	F	F	T

8.

p	q	r	$\sim p$	$\sim p \vee q$	$\sim p \vee q \to r$
T	T	T	F	T	T
T	T	F	F	T	F
T	F	T	F	F	T
T	F	F	F	F	T
F	T	T	T	T	T
F	T	F	T	T	F
F	F	T	T	T	T
F	F	F	T	T	F

10.

p	q	r	$p \to r$	$q \to r$	$(p \to r) \leftrightarrow (q \to r)$
T	T	T	T	T	T
T	T	F	F	F	T
T	F	T	T	T	T
T	F	F	F	T	F
F	T	T	T	T	T
F	T	F	T	F	F
F	F	T	T	T	T
F	F	F	T	T	T

11.

p	q	r	$q \to r$	$p \to (q \to r)$	$p \wedge q$	$p \wedge q \to r$	$(p \to (q \to r)) \leftrightarrow (p \wedge q \to r)$
T	T	T	T	T	T	T	T
T	T	F	F	F	T	F	T
T	F	T	T	T	F	T	T
T	F	F	T	T	F	T	T
F	T	T	T	T	F	T	T
F	T	F	F	T	F	T	T
F	F	T	T	T	F	T	T
F	F	F	T	T	F	T	T

13. *b.*

p	q	$\sim q$	$p \to q$	$\sim (p \to q)$	$p \wedge \sim q$
T	T	F	T	F	F
T	F	T	F	T	T
F	T	F	T	F	F
F	F	T	T	F	F

same truth values

The truth table shows that $\sim (p \to q)$ and $p \wedge \sim q$ always have the same truth values. Hence they are logically equivalent.

14. *a.*

p	q	r	$\sim q$	$\sim r$	$q \vee r$	$p \wedge \sim q$	$p \wedge \sim r$	$p \to q \vee r$	$p \wedge \sim q \to r$	$p \wedge \sim r \to q$
T	T	T	F	F	T	F	F	T	T	T
T	T	F	F	T	T	F	T	T	T	T
T	F	T	T	F	T	T	F	T	T	T
T	F	F	T	T	F	T	T	F	F	F
F	T	T	F	F	T	F	F	T	T	T
F	T	F	F	T	T	F	F	T	T	T
F	F	T	T	F	T	F	F	T	T	T
F	F	F	T	T	F	F	F	T	T	T

same truth values

The truth table shows that the three statement forms $p \to q \vee r$, $p \wedge \sim q \to r$, and $p \wedge \sim r \to q$ always have the same truth values. Thus they are all logically equivalent.

b. If n is prime and n is not odd, then n is 2.

And: If n is prime and n is not 2, then n is odd.

15.

p	q	r	$q \to r$	$p \to q$	$p \to (q \to r)$	$(p \to q) \to r$	
T	T	T	T	T	T	T	
T	T	F	F	T	F	F	
T	F	T	T	F	T	T	
T	F	F	T	F	T	T	
F	T	T	T	T	T	T	
F	T	F	F	T	T	F	$\leftarrow$
F	F	T	T	T	T	F	$\leftarrow$
F	F	F	T	T	T	F	$\leftarrow$

different truth values

The truth table shows that $p \to (q \to r)$ and $(p \to q) \to r$ do not always have the same truth values. (They differ for the combinations of truth values for p, q, and r shown in rows 6, 7, and 8.) Therefore they are not logically equivalent.

17. Let p represent "Rob is goalkeeper," q represent "Aaron plays forward," and r represent "Sam plays defense." The statement "If Rob is goalkeeper and Aaron plays forward, then Sam plays defense" has the form $p \wedge q \to r$. And the statement "Rob is not goalkeeper or Aaron does not play forward or Sam plays defense" has the form $\sim p \vee \sim q \vee r$.

p	q	r	$\sim p$	$\sim q$	$p \wedge q$	$p \wedge q \to r$	$\sim p \vee \sim q \vee r$
T	T	T	F	T	T	T	T
T	T	F	F	T	T	F	F
T	F	T	F	F	F	T	T
T	F	F	F	F	F	T	T
F	T	T	T	T	F	T	T
F	T	F	T	T	F	T	T
F	F	T	T	F	F	T	T
F	F	F	T	F	F	T	T

same truth values

The truth table shows that $p \wedge q \to r$ and $\sim p \vee \sim q \vee r$ always have the same truth values. Therefore they are logically equivalent.

18. *Part 1*: Let p represent "It walks like a duck," q represent "It talks like a duck," and r represent "It is a duck." The statement "If it walks like a duck and it talks like a duck, then it is a duck" has the form $p \wedge q \rightarrow r$. And the statement "Either it does not walk like a duck or it does not talk like a duck or it is a duck" has the form $\sim p \vee \sim q \vee r$.

p	q	r	$\sim p$	$\sim q$	$p \wedge q$	$\sim p \vee \sim q$	$p \wedge q \rightarrow r$	$(\sim p \vee \sim q) \vee r$
T	T	T	F	F	T	F	T	T
T	T	F	F	F	T	F	F	F
T	F	T	F	T	F	T	T	T
T	F	F	F	T	F	T	T	T
F	T	T	T	F	F	T	T	T
F	T	F	T	F	F	T	T	T
F	F	T	T	T	F	T	T	T
F	F	F	T	T	F	T	T	T

same truth values

The truth table shows that $p \wedge q \rightarrow r$ and $(\sim p \vee \sim q) \vee r$ always have the same truth values. Thus the following statements are logically equivalent: "If it walks like a duck and it talks like a duck, then it is a duck" and "Either it does not walk like a duck or it does not talk like a duck or it is a duck."

Part 2: The statement "If it does not walk like a duck and it does not talk like a duck then it is not a duck" has the form $\sim p \wedge \sim q \rightarrow \sim r$.

p	q	r	$\sim p$	$\sim q$	$\sim r$	$p \wedge q$	$\sim p \wedge \sim q$	$p \wedge q \rightarrow r$	$(\sim p \wedge \sim q) \rightarrow \sim r$	
T	T	T	F	F	F	T	F	T	T	
T	T	F	F	F	T	T	F	F	T	←
T	F	T	F	T	F	F	F	T	T	
T	F	F	F	T	T	F	F	T	T	
F	T	T	T	F	F	F	F	T	T	
F	T	F	T	F	T	F	F	T	T	
F	F	T	T	T	F	F	T	T	F	←
F	F	F	T	T	T	F	T	T	T	

different truth values

The truth table shows that $p \wedge q \rightarrow r$ and $(\sim p \wedge \sim q) \rightarrow \sim r$ do not always have the same truth values. (They differ for the combinations of truth values of p, q, and r shown in rows 2 and 7.) Thus they are not logically equivalent, and so the statement "If it walks like a duck and it talks like a duck, then it is a duck" is not logically equivalent to the statement "If it does not walk like a duck and it does not talk like a duck then it is not a duck." In addition, because of the logical equivalence shown in Part 1, we can also conclude that the following two statements are not logically equivalent: "Either it does not walk like a duck or it does not talk like a duck or it is a duck" and "If it does not walk like a duck and it does not talk like a duck then it is not a duck."

20. *b.* Today is New Year's Eve and tomorrow is not January.

c. The decimal expansion of r is terminating and r is not rational.

e. x is nonnegative and x is not positive and x is not 0.

Or: x is nonnegative but x is not positive and x is not 0.

Or: x is nonnegative and x is neither positive nor 0.

g. n is divisible by 6 and either n is not divisible by 2 or n is not divisible by 3.

21. By the truth table for $\rightarrow$, $p \rightarrow q$ is false if, and only if, p is true and q is false. Under these circumstances, (b) $p \vee q$ is true and (c) $q \rightarrow p$ is also true.

22. b. If tomorrow is not January, then today is not New Year's Eve.

    c. If r is not rational, then the decimal expansion of r is not terminating.

    e. If x is not positive and x is not 0, then x is not nonnegative.

    Or: If x is neither positive nor 0, then x is negative.

    g. If n is not divisible by 2 or n is not divisible by 3, then n is not divisible by 6.

23. b. *Converse*: If tomorrow is January, then today is New Year's Eve.

    Inverse: If today is not New Year's Eve, then tomorrow is not January.

    c. *Converse*: If r is rational then the decimal expansion of r is terminating.

    Inverse: If the decimal expansion of r is not terminating, then r is not rational.

    e. *Converse*: If x is positive or x is 0, then x is nonnegative.

    Inverse: If x is not nonnegative, then both x is not positive and x is not 0.

      Or: If x is negative, then x is neither positive nor 0.

25.

p	q	$\sim p$	$\sim q$	$p \rightarrow q$	$\sim p \rightarrow \sim q$
T	T	F	F	T	T
T	F	F	T	F	T
F	T	T	F	T	F
F	F	T	T	T	T

different truth values

The truth table shows that $p \rightarrow q$ *and* $\sim p \rightarrow \sim q$ have different truth values in rows 2 and 3, so they are not logically equivalent. Thus a conditional statement is not logically equivalent to its inverse.

27.

p	q	$\sim p$	$\sim q$	$q \rightarrow p$	$\sim p \rightarrow \sim q$
T	T	F	F	T	T
T	F	F	T	T	T
F	T	T	F	F	F
F	F	T	T	T	T

same truth values

The truth table shows that $q \rightarrow p$ *and* $\sim p \rightarrow \sim q$ always have the same truth values, so they are logically equivalent. Thus the converse and inverse of a conditional statement are logically equivalent to each other.

28. The if-then form of "I say what I mean" is "If I mean something, then I say it."

    The if-then form of "I mean what I say" is "If I say something, then I mean it."

    Thus "I mean what I say" is the converse of "I say what I mean." The two statements are not logically equivalent.

30. The corresponding tautology is $p \wedge (q \vee r) \leftrightarrow (p \wedge q) \vee (p \wedge r)$

p	q	r	$q \lor r$	$p \land q$	$p \land r$	$p \land (q \lor r)$	$(p \land q) \lor (p \land r)$	$p \land (q \lor r) \leftrightarrow$ $(p \land q) \lor (p \land r)$
T	T	T	T	T	T	T	T	T
T	T	F	T	T	F	T	T	T
T	F	T	T	F	T	T	T	T
T	F	F	F	F	T	F	F	T
F	T	T	T	F	F	F	F	T
F	T	F	T	F	F	F	F	T
F	F	T	T	F	F	F	F	T
F	F	F	F	F	F	F	F	T

$\underbrace{\qquad\qquad}_{\text{all } T\text{'s}}$

The truth table shows that $p \land (q \lor r) \leftrightarrow (p \land q) \lor (p \land r)$ is always true. Hence it is a tautology.

31. The corresponding tautology is $(p \to (q \to r)) \leftrightarrow ((p \land q) \to r)$.

p	q	r	$p \to q$	$p \land q$	$p \to (q \to r)$	$(p \land q) \to r)$	$p \to (q \to r) \leftrightarrow (p \land q) \to r$
T	T	T	T	T	T	T	T
T	T	F	F	T	F	F	T
T	F	T	T	F	T	T	T
T	F	F	T	F	T	T	T
F	T	T	T	F	T	T	T
F	T	F	F	F	T	T	T
F	F	T	T	F	T	T	T
F	F	F	T	F	T	T	T

$\underbrace{\qquad\qquad}_{\text{all } T\text{'s}}$

The truth table shows that $(p \to (q \to r)) \leftrightarrow ((p \land q) \to r)$ is always true. Hence it is a tautology.

33. If Sam is not an expert sailor, then he will not be allowed on Signe's racing boat.

If Sam is allowed on Signe's racing boat, then he is an expert sailor.

34. The Personnel Director did not lie. By using the phrase "only if," the Personnel Director set forth conditions that were necessary but not sufficient for being hired: if you did not satisfy those conditions then you would not be hired. The Personnel Director's statement said nothing about what would happen if you did satisfy those conditions.

36. If it doesn't rain, then Ann will go.

37. *b.* If a security code is not entered, then the door will not open.

39. *a.* $\begin{aligned} p \lor \sim q \to r \lor q \quad &\equiv \quad \sim (p \lor \sim q) \lor (r \lor q) \qquad \textit{[an acceptable answer]} \\ &\equiv \quad (\sim p \land \sim (\sim q)) \lor (r \lor q) \qquad \text{by De Morgan's law} \\ & \qquad\qquad\qquad\qquad\qquad\qquad\qquad \textit{[another acceptable answer]} \\ &\equiv \quad (\sim p \land q) \lor (r \lor q) \qquad \text{by the double negative law} \\ & \qquad\qquad\qquad\qquad\qquad\qquad\qquad \textit{[another acceptable answer]} \end{aligned}$

   b. $\begin{aligned} p \lor \sim q \to r \lor q \quad &\equiv \quad (\sim p \land q) \lor (r \lor q) \qquad \text{by part (a)} \\ &\equiv \quad \sim (\sim (\sim p \land q) \land \sim (r \lor q)) \qquad \text{by De Morgan's law} \\ &\equiv \quad \sim (\sim (\sim p \land q) \land (\sim r \land \sim q)) \qquad \text{by De Morgan's law} \end{aligned}$

The steps in the answer to part (b) would also be acceptable answers for part (a).

41. $a.$ $\quad (p \to (q \to r)) \leftrightarrow ((p \wedge q) \to r)$

$\equiv \quad [\sim p \vee (q \to r)] \leftrightarrow [\sim (p \wedge q) \vee r]$

$\equiv \quad [\sim p \vee (\sim q \vee r)] \leftrightarrow [\sim (p \wedge q) \vee r]$

$\equiv \quad \sim [\sim p \vee (\sim q \vee r)] \vee [\sim (p \wedge q) \vee r]$

$\qquad \wedge \sim [\sim (p \wedge q) \vee r] \vee [\sim p \vee (\sim q \vee r)]$

$b.$ By part (a), De Morgan's law, and the double negative law,

$(p \to (q \to r)) \leftrightarrow ((p \wedge q) \to r)$

$\equiv \quad \sim [\sim p \vee (\sim q \vee r)] \vee [\sim (p \wedge q) \vee r]$

$\qquad \wedge \sim [\sim (p \wedge q) \vee r] \vee [\sim p \vee (\sim q \vee r)]$

$\equiv \quad \sim [\sim p \vee (\sim q \vee r)] \wedge \sim [\sim (p \wedge q) \vee r]$

$\qquad \wedge \sim \sim [(p \wedge q) \wedge \sim r] \wedge \sim [\sim p \vee (\sim q \vee r)]$

$\equiv \quad \sim \sim [p \wedge \sim (\sim q \vee r)] \wedge [(p \wedge q) \wedge \sim r]$

$\qquad \wedge \sim \sim [(p \wedge q) \wedge \sim r] \wedge [p \wedge \sim (\sim q \vee r)]$

$\equiv \quad \sim \sim [p \wedge (q \wedge \sim r)] \wedge [(p \wedge q) \wedge \sim r]$

$\qquad \wedge \sim \sim [(p \wedge q) \wedge \sim r] \wedge [p \wedge (q \wedge \sim r)].$

The steps in the answer to part (b) would also be acceptable answers for part (a).

42. Yes. As in exercises 29–32, the following logical equivalences can be used to rewrite any statement form in a logically equivalent way using only $\sim$ and $\wedge$:

$$p \to q \equiv \sim p \vee q \qquad\qquad p \leftrightarrow q \equiv (\sim p \vee q) \wedge (\sim q \vee p)$$
$$p \vee q \equiv \sim (\sim p \wedge \sim q) \qquad \sim (\sim p) \equiv p$$

The logical equivalence $p \wedge q \equiv \sim (\sim p \vee \sim q)$ can then be used to rewrite any statement form in a logically equivalent way using only $\sim$ and $\vee$.

44. If this triangle has two 45° angles, then it is a right triangle.

46. If Jim does not do his homework regularly, then Jim will not pass the course.

If Jim passes the course, then he will have done his homework regularly.

48. If this computer program produces error messages during translation, then it is not correct.

If this computer program is correct, then it does not produce error messages during translation.

49. $c.$ must be true $d.$ not necessarily true $e.$ must be true $f.$ not necessarily true

Note: To solve this problem, it may be helpful to imagine a compound whose boiling point is greater than 150° C. For concreteness, suppose it is 200° C. Then the given statement would be true for this compound, but statements a, d, and f would be false.

Section 1.3

2. This is a **while** loop.

4. This figure is not a quadrilateral.

5. They did not telephone.

9.

						premises			conclusion	
p	q	r	$\sim q$	$\sim r$	$p \wedge q$	$p \wedge q \to \sim r$	$p \vee \sim q$	$\sim q \to p$	$\sim r$	
T	T	T	F	F	T	T	T	T	F	critical row
T	T	F	F	T	T	F	T	T	T	
T	F	T	T	F	F	T	T	T	F	critical row
T	F	F	T	T	F	T	T	T	T	
F	T	T	F	F	F	T	F	T	F	
F	T	F	F	T	F	T	F	T	T	
F	F	T	T	F	F	T	T	F	F	
F	F	F	T	T	F	T	T	F	T	

Rows 1 and 3 of the truth table show that it is possible for an argument of this form to have true premises and a false conclusion. Hence the argument form is invalid.

10.

				premises			conclusion	
p	q	r	$p \vee \sim q$	$p \to r$	$q \to r$	$p \vee q \to r$	
T	T	T	T	T	T	T	← critical row
T	T	F	T	F	F	F	
T	F	T	T	T	T	T	← critical row
T	F	F	T	F	T	F	
F	T	T	T	T	T	T	← critical row
F	T	F	T	T	F	F	
F	F	T	F	T	T	T	← critical row
F	F	F	F	T	T	T	← critical row

The truth table shows that in every situation (represented by rows 1, 3, 5, 7, and 8) in which all the premises are true, the conclusion is also true. Therefore, the argument is valid.

11.

							premises		conclusion	
p	q	r	$\sim p$	$\sim q$	$\sim r$	$q \vee r$	$p \to q \vee r$	$\sim q \vee \sim r$	$\sim p \vee \sim r$	
T	T	T	F	F	F	T	T	F	F	
T	T	F	F	F	T	T	T	T	T	← critical row
T	F	T	F	T	F	T	T	T	F	← critical row
T	F	F	F	T	T	F	F	T	T	
F	T	T	T	F	F	T	T	F	T	
F	T	F	T	F	T	T	T	T	T	← critical row
F	F	T	T	T	F	T	T	T	T	← critical row
F	F	F	T	T	T	F	T	T	T	

Row 3 of the truth table shows that it is possible for an argument of this form to have true premises and a false conclusion. Hence the argument form is invalid.

12.

		premises		conclusion	
p	q	$p \to q$	$\sim q$	$\sim p$	
T	T	T	F	F	
T	F	F	T	F	
F	T	T	F	T	
F	F	T	T	T	← critical row

The truth table shows that in the only situation (represented by row 4) in which both premises are true, the conclusion is also true. Therefore, modus tollens is valid.

13. *b.*

		premises		conclusion	
p	q	$p \to q$	$\sim p$	$\sim q$	
T	T	T	F	F	
T	F	F	F	T	
F	T	T	T	F	← critical row
F	F	T	T	T	← critical row

Row 3 of the truth table shows that it is possible for an argument of this form to have true premises and a false conclusion. Hence the argument form (inverse error) is invalid.

15.

		premise	conclusion	
p	q	q	$p \vee q$	
T	T	T	T ←	critical row
T	F	F	T	
F	T	T	T ←	critical row
F	F	F	F	

The truth table shows that in the two situations (represented by rows 1 and 3) in which the premise is true, the conclusion is also true. Therefore, the the second version of generalization is valid.

16.

		premise	conclusion	
p	q	$p \wedge q$	p	
T	T	T	T ←	critical row
T	F	F	T	
F	T	F	F	
F	F	F	F	

The truth table shows that in the only situation (represented by row 1) in which both premises are true, the conclusion is also true. Therefore, the the first version of specialization is valid.

17.

		premise	conclusion	
p	q	$p \wedge q$	q	
T	T	T	T ←	critical row
T	F	F	F	
F	T	F	T	
F	F	F	F	

The truth table shows that in the only situation (represented by row 1) in which both premises are true, the conclusion is also true. Therefore, the second version of specialization is valid.

19.

		premises		conclusion	
p	q	$p \vee q$	$\sim p$	q	
T	T	T	F	T	
T	F	T	F	F	
F	T	T	T	T ←	critical row
F	F	F	T	F	

The truth table shows that in the only situation (represented by row 3) in which both premises are true, the conclusion is also true. Therefore, the the second version of elimination is valid.

20.

			premises		conclusion	
p	q	r	$p \to q$	$q \to r$	$p \to r$	
T	T	T	T	T	T ←	critical row
T	T	F	T	F	F	
T	F	T	F	T	T	
T	F	F	F	T	F	
F	T	T	T	T	T ←	critical row
F	T	F	T	F	T	
F	F	T	T	T	T ←	critical row
F	F	F	T	T	T ←	critical row

The truth table shows that in the two situations (represented by rows 1, 5, 7, and 8) in which both premises are true, the conclusion is also true. Therefore, the argument form (transitivity) is valid.

21.

			premises			*conclusion*
p	q	r	$p \vee q$	$p \to r$	$q \to r$	r
T	T	T	T	T	T	T ← — *critical row*
T	T	F	T	F	F	F
T	F	T	T	T	T	T ← — *critical row*
T	F	F	T	F	T	F
F	T	T	T	T	T	T ← — *critical row*
F	T	F	T	T	F	F
F	F	T	F	T	T	T
F	F	F	F	T	T	F

The truth table shows that in the three situations (represented by rows 1, 3, 5) in which all three premises are true, the conclusion is also true. Therefore, proof by division into cases is valid.

23. form: $p \vee q$
           $p \to r$
    $\therefore$ $q \vee \sim r$

				premises		*conclusion*
p	q	r	$\sim r$	$p \vee q$	$p \to r$	$q \vee \sim r$
T	T	T	F	T	T	T ← — *critical row*
T	T	F	T	T	F	T
T	F	T	F	T	T	F ← — *critical row*
T	F	F	T	T	F	T
F	T	T	F	T	T	T ← — *critical row*
F	T	F	T	T	T	T ← — *critical row*
F	F	T	F	F	T	F
F	F	F	T	F	T	T

Row 3 of the truth table shows that it is possible for an argument of this form to have true premises and a false conclusion. Hence the argument form is invalid.

28. form: $p \to q$ invalid, converse error
             q
    $\therefore$ p

29. form: $p \to q$ invalid, inverse error
             $\sim p$
    $\therefore$ $\sim q$

30. form: $p \to q$ invalid, converse error
             q
    $\therefore$ p

31. form: $p \land q$ valid, generalization
    $\therefore\ q$

32. form: $p \to r$ valid, proof by division into cases
    $q \to r$
    $\therefore\ p \lor q \to r$

33. An invalid argument with a true conclusion can have premises that are either true or false. In the following example the first premise is true for either one of two reasons: its hypothesis is false and its conclusion is true.

    If the square of every real number is positive, then some real numbers are positive.

    Some real numbers are positive.

    Therefore, the square of every real number is positive.

34. A valid argument with a false conclusion must have at least one false premise. In the following example, the second premise is false. (The first premise is true because its hypothesis is false.)

    If the square of every real number is positive, then no real number is negative.

    The square of every real number is positive.

    Therefore, no real number is negative.

35. A correct answer should indicate that for a valid argument, any argument of the same form that has true premises has a true conclusion, whereas for an invalid argument, it is possible to find an argument of the same form that has true premises and a false conclusion. The validity of an argument does not depend on whether the conclusion is true or not. The validity of an argument only depends on the formal relationship between its premises and its conclusion.

38. *b.* 1. Suppose C is a knight.
    2. $\therefore$ C is a knave (because what C said was true).
    3. $\therefore$ C is both a knight and a knave (by (1) and (2)), which is a contradiction.
    4. $\therefore$ C is not a knight (because by the contradiction rule the supposition is false).
    5. $\therefore$ What C says is false (because since C is not a knight he is a knave and knaves always speak falsely).
    6. $\therefore$ At least one of C or D is a knight (by De Morgan's law).
    7. $\therefore$ D is a knight (by (4) and (6) and elimination).
    8. $\therefore$ C is a knave and D is a knight (by (4) and (7)).
    To check that the problem situation is not inherently contradictory, note that if C is a knave and D is a knight, then each could have spoken as reported.
    c. There is one knave. E and F cannot both be knights because then both would also be knaves (since each would have spoken the truth), which is a contradiction. Nor can E and F both be knaves because then both would be telling the truth which is impossible for knaves. Hence, the only possible answer is that one is a knight and the other is a knave. But in this case both E and F could have spoken as reported, without contradiction.
    d. The following is one of many solutions.
    1. The statement made by U must be false because if it were true then U would not be a knight (since none would be a knight), but since he spoke the truth he would be a knight and this would be a contradiction.
    2. $\therefore$ there is at least one knight, and U is a knave (since his statement that there are no knights is false).
    3. Suppose Z spoke the truth. Then so did W (since if there is exactly one knight then it is also true that there are at most three knights). But this implies that there are at least two knights, which contradicts $Z's$ statement. Hence Z cannot have spoken the truth.

4. ∴ there are at least two knights, and Z is a knave (since his statement that there is exactly one knight is false). Also $X's$ statement is false because since both U and Z are knaves it is impossible for there to be exactly five knights. Hence X also is a knave.

5. ∴ there are at least three knaves (U, Z, and X), and so there are at most three knights.

6. ∴ $W's$ statement is true, and so W is a knight.

7. Suppose V spoke the truth. Then V, W, and Y are all knights (otherwise there would not be at least three knights because U, Z, and X are known to be knaves). It follows that Y spoke the truth. But Y said that exactly two were knights. This contradicts the result that V, W, and Y are all knights.

8. ∴ V cannot have spoken the truth, and so V is a knave.

9. ∴ U, Z, X, and V are all knaves, and so there are at most two knights.

10. Suppose that Y is a knave. Then the only knight is W, which means that Z spoke the truth. But we have already seen that this is impossible. Hence Y is a knight.

11. By 6, 9, and 10, the only possible solution is that U, Z, X, and V are knaves and W and Y are knights. Examination of the statements shows that this solution is consistent: in this case, the statements of U, Z, X, and V are false and those of W and Y are true.

40. Suppose Socko is telling the truth. Then Fats is also telling the truth because if Lefty killed Sharky then Muscles didn't kill Sharky. Consequently, two of the men were telling the truth, which contradicts the fact that all were lying except one. Therefore, Socko is not telling the truth: Lefty did not kill Sharky. Hence Muscles is telling the truth and all the others are lying. It follows that Fats is lying, and so Muscles killed Sharky.

42.   (1) $q \rightarrow r$ premise b
             $\sim r$ premise d
      ∴ $\sim q$ by modus tollens

  (2) $p \vee q$ premise a
             $\sim q$ by (1)
      ∴ p by elimination

  (3) $\sim q \rightarrow u \wedge s$ premise e
             $\sim q$ by (1)
      ∴ $u \wedge s$ by modus ponens

  (4) $u \wedge s$ by (3)
      ∴ s by specialization

  (5) p by (2)
             s by (4)
      ∴ $p \wedge s$ by conjunction

  (6) $p \wedge s \rightarrow t$ premise c
             $p \wedge s$ by (5)
      ∴ t by modus ponens

44.   (1) $\sim q \vee s$ premise d
             $\sim s$ premise e
      ∴ $\sim q$ by elimination

(2) $p \to q$ premise a
       $\sim q$ by (1)
∴ $\sim p$ by modus tollens

(3) $r \vee s$ premise b
       $\sim s$ premise e
∴ r by elimination

(4) $\sim p$ by (2)
       r by (3)
∴ $\sim p \wedge r$ by conjunction

(5) $\sim p \wedge r \to u$ premise f
       $\sim p \wedge r$ by (4)
∴ u by modus ponens

(6) $\sim s \to \sim t$ premise c
       $\sim s$ premise e
∴ $\sim t$ by modus ponens

(7) $w \vee t$ premise g
       $\sim t$ by (6)
∴ w by elimination

(8) u by (5)
       w by (7)
∴ $u \wedge w$ by conjunction

Section 1.4

2. $R = 1$

4. $S = 1$

6. The input/output table is as follows:

Input		Output
P	Q	R
1	1	0
1	0	1
0	1	0
0	0	0

8. The input/output table is as follows:

Input			Output
P	Q	R	S
1	1	1	1
1	1	0	1
1	0	1	1
1	0	0	1
0	1	1	1
0	1	0	1
0	0	1	1
0	0	0	1

10. $(P \vee Q) \wedge \sim Q$

12. $(P \vee Q) \vee \sim (Q \wedge R)$

14.
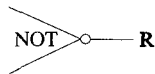
15.
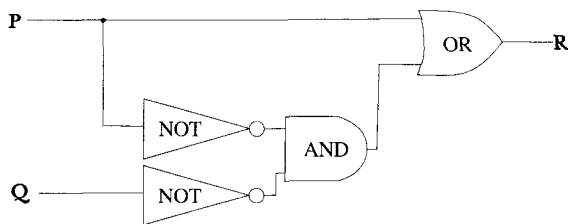
17.
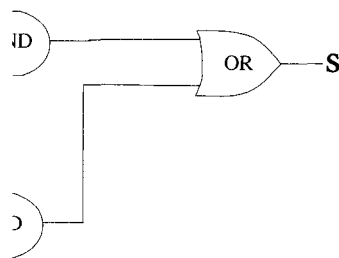
19. *a.* $(P \wedge Q \wedge \sim R) \vee (P \wedge \sim Q \wedge \sim R) \vee (\sim P \wedge Q \wedge \sim R)$

b. One circuit having the given input/output table is the following:
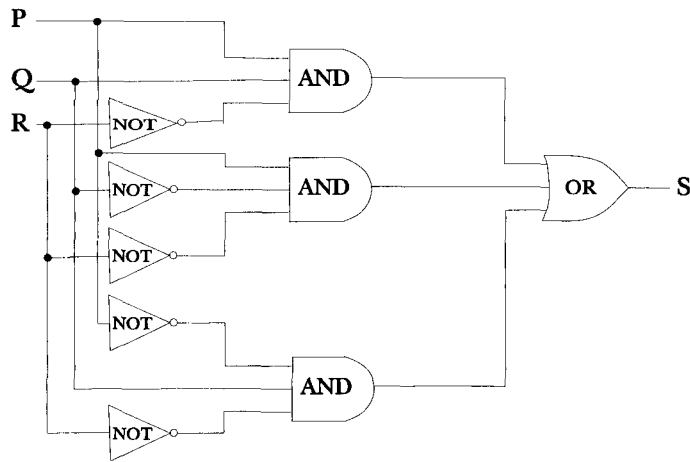
21. *a.* $(P \wedge Q \wedge \sim R) \vee (\sim P \wedge Q \wedge R) \vee (\sim P \wedge Q \wedge \sim R)$

b. One circuit having the given input/output table is the following:
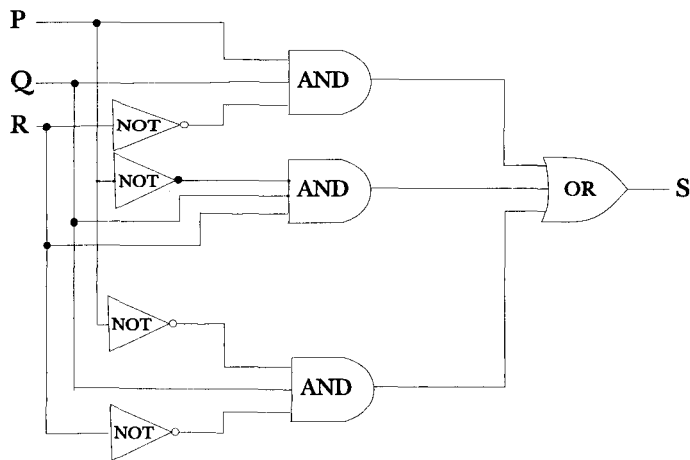
23. The input/output table is as follows:

Input			Output
P	Q	R	S
1	1	1	1
1	1	0	0
1	0	1	0
1	0	0	0
0	1	1	0
0	1	0	0
0	0	1	0
0	0	0	1

One circuit (among many) having this input/output table is the following:
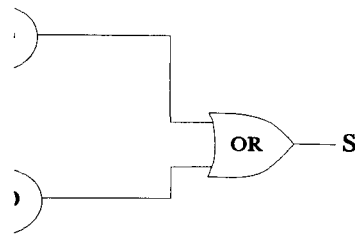
25. Let P, Q, and R indicate the positions of the switches, with 1 indicating that the switch is in the on position. Let an output of 1 indicate that the security system is enabled. The complete input/output table is as follows:

Input			Output
P	Q	R	S
1	1	1	1
1	1	0	1
1	0	1	1
1	0	0	0
0	1	1	1
0	1	0	0
0	0	1	0
0	0	0	0

One circuit (among many) having this input/output table is the following:
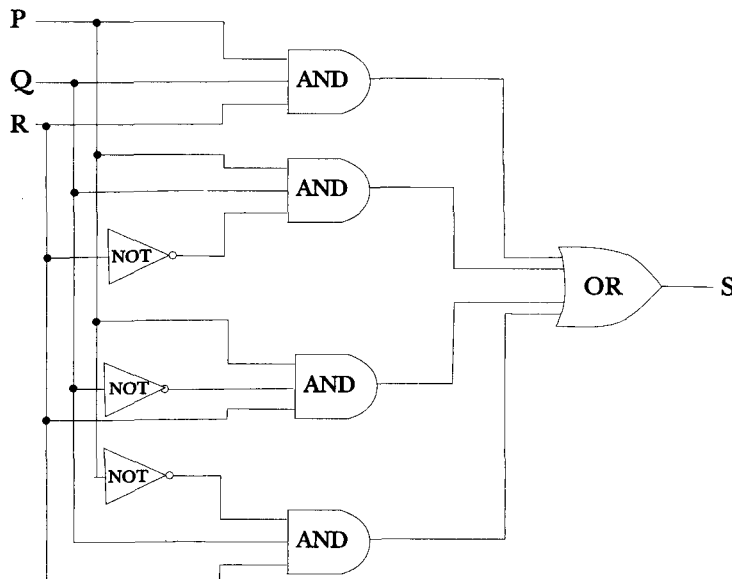
Note: One alternative answer interchanges the 1's and 0's.

27. The Boolean expression for circuit (a) is $\sim P \wedge (\sim (\sim P \wedge Q))$ and for circuit (b) it is $\sim (P \vee Q)$. We must show that if these expressions are regarded as statement forms, then they are logically

equivalent. But

$$
\begin{aligned}
\sim P \wedge (\sim (\sim P \wedge Q)) &\equiv \sim P \wedge (\sim (\sim P) \vee \sim Q) && \text{by De Morgan's law} \\
&\equiv \sim P \wedge (P \vee \sim Q) && \text{by the double negative law} \\
&\equiv (\sim P \wedge P) \vee (\sim P \wedge \sim Q) && \text{by the distributive law} \\
&\equiv \mathbf{c} \vee (\sim P \wedge \sim Q) && \text{by the negation law for } \wedge \\
&\equiv \sim P \wedge \sim Q && \text{by the identity law for } \vee \\
&\equiv \sim (P \vee Q) && \text{by De Morgan's law.}
\end{aligned}
$$

29. The Boolean expression for circuit (a) is $(P \wedge Q) \vee (\sim P \wedge Q) \vee (P \wedge \sim Q)$ and for circuit (b) it is $P \vee Q$. We must show that if these expressions are regarded as statement forms, then they are logically equivalent. But

$$
\begin{aligned}
(P \wedge Q) \vee (\sim P \wedge Q) \vee (P \wedge \sim Q) & \\
\equiv\ &((P \wedge Q) \vee (\sim P \wedge Q)) \vee (P \wedge \sim Q) && \text{by inserting parentheses (which is} \\
& && \text{legal by the associative law for } \vee) \\
\equiv\ &((Q \wedge P) \vee (Q \wedge \sim P)) \vee (P \wedge \sim Q) && \text{by the commutative law for } \wedge \\
\equiv\ &(Q \wedge (P \vee \sim P)) \vee (P \wedge \sim Q) && \text{by the distributive law} \\
\equiv\ &(Q \wedge \mathbf{t}) \vee (P \wedge \sim Q) && \text{by the negation law for } \vee \\
\equiv\ &Q \vee (P \wedge \sim Q) && \text{by the identity law for } \wedge \\
\equiv\ &(Q \vee P) \wedge (Q \vee \sim Q) && \text{by the distributive law} \\
\equiv\ &(Q \vee P) \wedge \mathbf{t} && \text{by the negation law for } \vee \\
\equiv\ &Q \vee P && \text{by the identity law for } \wedge \\
\equiv\ &P \vee Q && \text{by the commutative law for } \vee.
\end{aligned}
$$

31. $(\sim P \wedge \sim Q) \vee (\sim P \wedge Q) \vee (P \wedge \sim Q) \equiv ((\sim P \wedge \sim Q) \vee (\sim P \wedge Q)) \vee (P \wedge \sim Q)$

$$
\begin{aligned}
& && \text{by inserting parentheses (which is} \\
& && \text{legal by the associative law)} \\
\equiv\ &(\sim P \wedge (\sim Q \vee Q)) \vee (P \wedge \sim Q) && \text{by the distributive law} \\
\equiv\ &(\sim P \wedge (Q \vee \sim Q)) \vee (p \wedge \sim Q) && \text{by the commutative law} \\
\equiv\ &(\sim P \wedge \mathbf{t}) \vee (P \wedge \sim Q) && \text{by the negation law} \\
\equiv\ &\sim P \vee (P \wedge \sim Q) && \text{by the identity law} \\
\equiv\ &(\sim P \vee P) \wedge (\sim P \vee \sim Q) && \text{by the distributive law} \\
\equiv\ &(P \vee \sim P) \wedge (\sim P \vee \sim Q) && \text{by the commutative law} \\
\equiv\ &\mathbf{t} \wedge (\sim P \vee \sim Q) && \text{by the negation law} \\
\equiv\ &(\sim P \vee \sim Q) \wedge \mathbf{t} && \text{by the commutative law} \\
\equiv\ &\sim P \vee \sim Q && \text{by the identity law} \\
\equiv\ &\sim (P \wedge Q) && \text{by De Morgan's law.}
\end{aligned}
$$

32. $(P \wedge Q \wedge R) \vee ((P \wedge \sim Q \wedge R) \vee (P \wedge \sim Q \wedge \sim R)$

$$
\begin{aligned}
\equiv\ &((P \wedge (Q \wedge R)) \vee (P \wedge (\sim Q \wedge R))) \vee (P \wedge (\sim Q \wedge \sim R)) \vee (P \wedge \sim Q) \\
& \quad\quad\quad\quad \text{by inserting parentheses (which is legal by the associative law)} \\
\equiv\ &(P \wedge [(Q \wedge R) \vee (\sim Q \wedge R)] \vee (P \wedge [\sim Q \wedge \sim R]) && \text{by the distributive law} \\
\equiv\ &P \wedge ([(Q \wedge R) \vee (\sim Q \wedge R)] \vee [\sim Q \wedge \sim R]) && \text{by the distributive law} \\
\equiv\ &P \wedge ([(R \wedge Q) \vee (R \wedge \sim Q)] \vee [\sim Q \wedge \sim R]) && \text{by the commutative law for } \wedge \\
\equiv\ &P \wedge ([(R \wedge (Q \vee \sim Q)] \vee [\sim Q \wedge \sim R]) && \text{by the distributive law} \\
\equiv\ &P \wedge ([(R \wedge \mathbf{t}] \vee [\sim Q \wedge \sim R]) && \text{by the negation law for } \vee \\
\equiv\ &P \wedge (R \vee [\sim Q \wedge \sim R]) && \text{by the identity law for } \wedge \\
\equiv\ &P \wedge ((R \vee \sim Q) \wedge (R \vee \sim R)) && \text{by the distributive law} \\
\equiv\ &P \wedge ((R \vee \sim Q) \wedge \mathbf{t}]) && \text{by the negation law for } \vee \\
\equiv\ &P \wedge (R \vee \sim Q) && \text{by the identity law for } \wedge.
\end{aligned}
$$

33. *a.*

$$
\begin{aligned}
(P \mid Q) \mid (P \mid Q) &\equiv \sim [(P \mid Q) \wedge (P \mid Q)] && \text{by definition of } \mid \\
&\equiv \sim (P \mid Q) && \text{by the idempotent law for } \wedge \\
&\equiv \sim [\sim (P \wedge Q)] && \text{by definition of } \mid \\
&\equiv P \wedge Q && \text{by the double negative law.}
\end{aligned}
$$

b.

$$
\begin{aligned}
P \wedge (\sim Q \vee R) &\equiv (P|(\sim Q \vee R))|(P|(\sim Q \vee R)) \\
&\qquad \text{by part (a)} \\
&\equiv (P|[(\sim Q|\sim Q)|(R|R)])|(P|[(\sim Q|\sim Q)|(R|R)]) \\
&\qquad \text{by Example 1.4.7(b)} \\
&\equiv (P|[((Q|Q)|(Q|Q))|(R|R)])|(P|[((Q|Q)|(Q|Q))|(R|R)]) \\
&\qquad \text{by Example 1.4.7(a)}
\end{aligned}
$$

34. *b.*

$$
\begin{aligned}
P \vee Q &\equiv \sim (\sim (P \vee Q)) && \text{by the double negative law} \\
&\equiv \sim (P \downarrow Q) && \text{by definition of } \downarrow \\
&\equiv (P \downarrow Q) \downarrow (P \downarrow Q) && \text{by part (a).}
\end{aligned}
$$

c.

$$
\begin{aligned}
P \wedge Q &\equiv \sim (\sim P \vee \sim Q) && \text{by De Morgan's law and the double negative law} \\
&\equiv \sim P \downarrow \sim Q && \text{by definition of } \downarrow \\
&\equiv (P \downarrow P) \downarrow (Q \downarrow Q) && \text{by part (a).}
\end{aligned}
$$

d.

$$
\begin{aligned}
P \rightarrow Q &\equiv \sim P \vee Q && \text{by Exercise 13(a) of Section 1.2} \\
&\equiv (\sim P \downarrow Q) \downarrow (\sim P \downarrow Q) && \text{by part (b)} \\
&\equiv ((P \downarrow P) \downarrow Q) \downarrow ((P \downarrow P) \downarrow Q) && \text{by part (a).}
\end{aligned}
$$

e.

$$
\begin{aligned}
P \leftrightarrow Q &\equiv (P \rightarrow Q) \wedge (Q \rightarrow P) \\
&\qquad \text{by the truth table on page 24 of the text} \\
&\equiv ([[(P \downarrow P) \downarrow Q] \downarrow [(P \downarrow P) \downarrow Q)]]) \wedge ([[(Q \downarrow Q) \downarrow P] \downarrow [(Q \downarrow Q) \downarrow P)]]) \\
&\qquad \text{by part (d)} \\
&\equiv (([[(P \downarrow P) \downarrow Q] \downarrow [(P \downarrow P) \downarrow Q)]]) \downarrow [[(P \downarrow P) \downarrow Q] \downarrow [(P \downarrow P) \downarrow Q)]])) \\
&\qquad \downarrow ((([(Q \downarrow Q) \downarrow P] \downarrow [(Q \downarrow Q) \downarrow P)]]) \downarrow ([[(Q \downarrow Q) \downarrow P] \downarrow [(Q \downarrow Q) \downarrow P)]])) \\
&\qquad \text{by part (c)}
\end{aligned}
$$

Section 1.5

2. $55 = 32 + 16 + 4 + 2 + 1 = 110111_2$

3. $287 = 256 + 16 + 8 + 4 + 2 + 1 = 100011111_2$

5. $1609 = 1024 + 512 + + 64 + 8 + 1 = 11001001001_2$

6. $1424 = 1024 + 256 + 128 + 16 = 10110010000_2$

8. $10111_2 = 16 + 4 + 2 + 1 = 23_{10}$

9. $110110_2 = 32 + 16 + 4 + 2 = 54_{10}$

11. $1000111_2 = 64 + 4 + 2 + 1 = 71_{10}$

14.
$$
\begin{array}{r}
1001_2 \\
+\ 1011_2 \\
\hline
10100_2
\end{array}
$$

16.
$$
\begin{array}{r}
110111011_2 \\
+\ 1001011010_2 \\
\hline
10000010101_2
\end{array}
$$

18.
$$
\begin{array}{r}
11010_2 \\
-\ 1101_2 \\
\hline
1101_2
\end{array}
$$

20.
$$\begin{array}{r} 1010100_2 \\ -\ \ \ \ \ 10111_2 \\ \hline 111101_2 \end{array}$$

21. *b.* $S = 0, T = 1$ *c.* $S = 0, T = 0$

22. Note that

$$\begin{array}{r} 11111111_2 \\ +\ \ \ \ \ \ \ \ 1_2 \\ \hline 100000000_2 \end{array}$$

and $100000000_2 = 2^8_{10}$. Because $1_2 = 1_{10}$, we have that

$$\begin{array}{rclcl} 11111111_2 + 1_2 & = & & & 2^8_{10} \\ -\ \ \ \ \ \ \ \ \ \ 1_2 & & -& & 1_{10} \\ \hline 11111111_2 & = & & & (2^8 - 1)_{10} \end{array}$$

24. $67_{10} = (64 + 2 + 1)_{10} = 01000011_2 \longrightarrow 10111100 \longrightarrow 10111101.$
    So the two's complement is 10111101.

26. $115_{10} = (64 + 32 + 16 + 2 + 1)_{10} = 1110011_2 \longrightarrow 01110011 \longrightarrow 10001100 + 1 \longrightarrow 10001101$
    So the two's complement is 10001101.

28. $10011001 \longrightarrow -(01100110 + 1)_2 \longrightarrow -01100111_2 = -(64 + 32 + 4 + 2 + 1)_{10} = -103_{10}$

30. $10111010 \longrightarrow -(01000101 + 1)_2 \longrightarrow -01000110_2 = -(64 + 4 + 2)_{10} = -70_{10}$

34. $89_{10} = (64 + 16 + 8 + 1)_{10} = 01011001_2$
    $-55_{10} = -(32 + 16 + 4 + 2 + 1)_{10} = -00110111_2 \longrightarrow (11001000 + 1)_2 \longrightarrow 11001001$
    So the 8-bit representations of 79 and −43 are 01001111 and 11010101. Adding the 8-bit representations in binary notation gives

$$\begin{array}{r} 01011001 \\ +\ \ \ 11001001 \\ \hline 100100010 \end{array}$$

Truncating the 1 in the 2^8th position gives 00100010. Since the leading bit of this number is a 0, the answer is positive. Converting back to decimal form gives

$$00100010 \longrightarrow 100010_2 = (32 + 2)_{10} = 34_{10}.$$

So the answer is 34.

35. $-15_{10} = -(8 + 4 + 2 + 1)_{10} = -1111_2 \longrightarrow 00001111 \longrightarrow 11110000 \longrightarrow 11110001$
    $-46_{10} = -(32 + 8 + 4 + 2)_{10} = -101110_2 \longrightarrow 00101110 \longrightarrow 11010001 \longrightarrow 11010010$
    So the 8-bit representations of −15 and −46 are 11110001 and 10100010. Adding the 8-bit representations gives

$$\begin{array}{r} 11110001 \\ +\ \ \ 11010010 \\ \hline 111000011 \end{array}$$

Truncating the 1 in the 2^8th position gives 11000011. Since the leading bit of this number is a 1, the answer is negative. Converting back to decimal form gives

$$11000011 \longrightarrow -(00111100 + 1)_2 = -00111101_2 = -(32 + 16 + 8 + 4 + 1)_{10} = -61_{10}.$$

So the answer is −61.

36. $123_{10} = (64 + 32 + 16 + 8 + 2 + 1)_{10} = 01111011_2$

$-94_{10} = -(64 + 16 + 8 + 4 + 2)_{10} = -01011110_2 \longrightarrow (10100001 + 1)_2 \longrightarrow 10100010$

So the 8-bit representations of 123 and -94 are 01111011 and 10100010. Adding the 8-bit representations gives

$$\begin{array}{r} 01111011 \\ + \quad 10100010 \\ \hline 100011101 \end{array}$$

Truncating the 1 in the 2^8th position gives 00011101. Since the leading bit of this number is a 0, the answer is positive. Converting back to decimal form gives

$$00011101 \longrightarrow 11101_2 = (16 + 8 + 4 + 1)_{10} = 29_{10}.$$

So the answer is 29.

37. Suppose a and b are two integers in the range from 1 through 128 whose sum $a + b$ is also in this range. Since

$$1 \le a + b \le 128$$

then

$$-1 \ge -(a + b) \ge -128 \qquad \text{by multiplying through by } -1.$$

Adding 2^9 to all parts of the inequality gives

$$2^9 - 1 \ \ge \ 2^9 - (a + b) \ \ge \ 2^9 - 128 \ > \ 2^8,$$

and so

$$2^8 \ < \ 2^9 - (a + b) \ < \ 2^9. \quad (*)$$

Now observe that

$$(2^8 - a) + (2^8 - b) = 2 \cdot 2^8 - (a + b) = 2^9 - (a + b).$$

Hence by substitution into $(*)$,

$$2^8 \ < \ (2^8 - a) + (2^8 - b) \ < \ 2^9.$$

Consequently,

$$(2^8 - a) + (2^8 - b) = 2^8 \ + \ \text{smaller powers of 2,}$$

and so the binary representation of $(2^8 - a) + (2^8 - b)$ has a leading 1 in the 2^8th position.

39. $E0D_{16} = 14 \cdot 16^2 + 0 + 13 = 3597_{10}$

40. $39EB_{16} = 3 \cdot 16^3 + 9 \cdot 16^2 + 14 \cdot 16 + 11 = 14827_{10}$

42. $B53DF8_{16} = 1011\ 0101\ 0011\ 1101\ 1111\ 1000_2$

43. $4ADF83_{16} = 0100\ 1010\ 1101\ 1111\ 1000\ 0011_2$

45. $1011\ 0111\ 1100\ 0101_2 = B7C5_{16}$

47. b. $20763_8 = 2 \cdot 8^4 + 0 \cdot 8^3 + 7 \cdot 8^2 + 6 \cdot 8 + 3 = 8691_{10}$

   c. To convert an integer from octal to binary notation:

      i. Write each octal digit of the integer in fixed 3-bit binary notation (and include leading zeros as needed). Note that

octal digit	0	1	2	3	4	5	6	7
3-bit binary equivalent	000	001	010	011	100	101	110	111

ii. Juxtapose the results.

As an example, consider converting 61502_8 to binary notation:

$$6_8 = 110_2 \quad 1_8 = 001_2 \quad 5_8 = 101_2 \quad 0_8 = 000_2 \quad 2_8 = 010_2.$$

So in binary notation the integer should be $110\,001\,101\,000\,010_2$. To check this result, write the integer in decimal notation and compare it to the result of part (a):

$$110\,001\,101\,000\,010_2 = (1 \cdot 2^{14} + 1 \cdot 2^{13} + 1 \cdot 2^9 + 1 \cdot 2^8 + 1 \cdot 2^6 + 1 \cdot 2)_{10} = 25410_{10}.$$

It agrees.

(a) To convert an integer from binary to octal notation:

    i. Group the digits of the binary number into sets of three, starting from the right and adding leading zeros as needed;

    ii. Convert the binary numbers in each set of three into octal digits;

    iii. Juxtapose those octal digits.

As an example consider converting 1101011101_2 to octal notation. Grouping the binary digits in sets of three and adding two leading zeros gives

$$001\,101\,011\,101.$$

To convert each group into an octal digit, note that

$$001_2 = 1_8 \quad 101_2 = 5_8 \quad 011_2 = 3_8 \quad 101_2 = 5_8.$$

So the octal version of the integer should be 1535_8. To check this result, observe that

$$1\,101\,011\,101_2 = (1 \cdot 2^9 + 1 \cdot 2^8 + 1 \cdot 2^6 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1)_{10} = 861_{10}$$

and

$$1535_8 = (1 \cdot 8^3 + 5 \cdot 8^2 + 3 \cdot 8 + 5)_{10} = 861_{10}$$

also.

Chapter 2: The Logic of Quantified Statements

Ability to use the logic of quantified statements correctly is necessary for doing mathematics because mathematics is, in a very broad sense, about quantity. The main purpose of this chapter is to familiarize students with the language of universal and existential statements. The various facts about quantified statements developed in this chapter are used extensively in Chapter 3 and are referred to throughout the rest of the book. Experience with the formalism of quantification is especially useful to students planning to study LISP or Prolog, program verification, or relational databases.

Many students come to college with inconsistent interpretations of quantified statements. In tests made at DePaul University, over 60% of students chose the statement "No fire trucks are red" as the negation of "All fire trucks are red." Yet, through guided discussion, these same students came fairly quickly to accept that "Some fire trucks are not red" conveys the negation more accurately, and most learned to take negations of general statements of the form "$\forall x$, if $P(x)$ then $Q(x)$," "$\forall x$, $\exists y$ such that $P(x, y)$," and so forth with reliable accuracy.

One thing to keep in mind is the tolerance for potential ambiguity in ordinary language, which is typically resolved through context or inflection. For instance, as the "Caution" on page 90 of the text indicates, the sentence "All mathematicians do not wear glasses" is one way to phrase a negation to "All mathematicians wear glasses." (To see this, say it out loud, stressing the word "not.") Some grammarians ask us to avoid such phrasing because of its potentially ambiguity, but the usage is widespread even in formal writing in high-level publications ("All juvenile offenders are not alike," Anthony Lewis, The New York Times, 19 May 1997, Op-Ed page), or in literary works ("All that glisters is not gold," William Shakespeare, The Merchant of Venice, Act 2, Scene 7, 1596-1597).

Even rather complex sentences can be negated in this way. For instance, when asked to write a negation for "The sum of any two irrational numbers is irrational," a student wrote "The sum of any two irrational numbers is not irrational," which is an acceptable informal negation (again, say it out loud, stressing the word "not"). To avoid such responses, it may be necessary to specify to students that simply inserting the word "not" is not an acceptable answer to a problem that asks for a negation.

The modified formal language of the text includes the words "such that" in statements containing an existential quantifier because when students write multiply-quantified statements "formally," they often insert the words "such that" in the wrong place. That is, they insert it in a place that changes the meaning of the statement they were given. If they were not required to include the words "such that," an opportunity to correct their misunderstanding would be missed. It can also be helpful to alternate between writing out the words "if-then" (to encourage students to take the word "if" more seriously than they may be inclined to do[1]) and using an arrow to denote the conditional (to communicate the dynamic nature of deductive reasoning).

Another aspect of students' backgrounds that may surprise college and university mathematics instructors concerns their understanding of the meaning of "real number." For instance, when asked about of the following statement, many students only consider integer values for a and b: $\exists$ a positive real number a such that $\forall$ positive real numbers b, $a \leq b$. An informal description of the relationship between real numbers and points on a number line is given in Section 2.1 on page 77. The main purpose is to illustrate the existence of many real numbers between any pair of consecutive integers. Examples 2.3.5 and 2.3.6 on page 101 are intended to deepen students' understanding of this fact, and the discussion on page 449 that precedes the proof of the uncountability of the real numbers between 0 and 1 describes a procedure for approximating the (possibly infinite) decimal expansion for a point on a number line.

---

[1] Many students (and other people) mistakenly interpret *if-then* statements as *and* statements. For instance, when students are asked to state what it means for a binary relation R to be symmetric, a significant fraction write "aRb and bRa."

Note

Instructors who wish to incorporate more about sets to accompany the material of Chapter 2 can do so by covering some of the topics from Sections 5.1 and 5.2 at the beginning of Chapter 2. However, because almost all students have difficulty with element proofs and with some of the subtler issues concerning sets, the bulk of the material on set theory is best left until students have had experience working with simpler proofs.

Suggestions

1. The exercises in Sections 2.1–2.3 are designed to try to imprint new language patterns on students' minds. Because it takes time to develop new habits, it is helpful to continue assigning exercises from these sections for several days after covering them in class. To prepare for Chapter 3, universal conditional statements should especially be emphasized. As in Section 1.2, care may need to be taken not to spend excessive class time going over the more difficult exercises, such as those on "necessary" and "sufficient" conditions.

2. The most important idea of Section 2.4 is also the simplest: the rule of universal instantiation. Yet this inference rule drives an enormous amount of mathematical reasoning. If you wish to move rapidly through Chapter 2, you could focus on this rule and its immediate consequences in Section 2.4 and omit the discussion of how to use diagrams to check validity of arguments.

Section 2.1

1. *c.* False   *d.* True   *e.* False   *f.* True

4. *a.* $Q(2)$: $2^2 \leq 30$ - true because $2^2 = 4$ and $4 \leq 30$, $Q(-2)$: $(-2)^2 \leq 30$ - true because $(-2)^2 = 4$ and $4 \leq 30$

   $Q(7)$: $7^2 \leq 30$ - false because $7^2 = 49$ and $49 \not\leq 30$, $Q(-7)$: $(-7)^2 \leq 30$ - false because $(-7)^2 = 49$ and $49 \not\leq 30$

   c. truth set $= \{n \in \mathbf{Z}^+ | n^2 \leq 30\} = \{1, 2, 3, 4, 5\}$

5. *b.* Let $x = -1$ and $y = 0$. Then $x < y$ because $-1 < 0$ but $x^2 \not< y^2$ because $(-1)^2 = 1 \not< 0^2 = 0$. Thus the hypothesis $x < y$ is true and the conclusion $x^2 < y^2$ is false, so the statement as a whole is false.

   d. Here are examples of three kinds of correct answers:

   (1) Let $x = 2$ and $y = 3$. Then $x < y$ because $2 < 3$ and $x^2 < y^2$ because $2^2 = 4 < 3^2 = 9$. Thus both the hypothesis and the conclusion are true, so the statement as a whole is true.

   (2) Let $x = 3$ and $y = 2$. Then $x \not< y$ because $3 \not< 2$ and $x^2 \not< y^2$ because $3^2 = 9 \not< 2^2 = 4$. Thus both the hypothesis and the conclusion are false, so the statement as a whole is true.

   (3) Let $x = 2$ and $y = -3$. Then $x \not< y$ because $2 \not< -3$ and $x^2 < y^2$ because $2^2 = 4 < (-3)^2 = 9$. Thus the hypothesis is false and the conclusion is true, so the statement as a whole is true.

6. *a.* When $m = 25$ and $n = 10$,the statement "m is a factor of n^2" is true because $n^2 = 100$ and $100 = 4 \cdot 25$. But the statement "m is a factor of n" is false because 10 is not a product of 25 times any integer. Thus the hypothesis is true and the conclusion is false, so the statement as a whole is false.

   b. $R(m, n)$ is also false when $m = 8$ and $n = 4$ because 8 is a factor of $4^2 = 16$, but 8 is not a factor of 4.

   c. When $m = 5$ and $n = 10$, both statements "m is a factor of n^2" and "m is a factor of n" are true because $n = 10 = 5 \cdot 2 = m \cdot 2$ and $n^2 = 100 = 5 \cdot 20 = m \cdot 20$. Thus both the hypothesis and conclusion of $R(m, n)$ are true, and so the statement as a whole is true.

d. Here are examples of two kinds of correct answers:

(1) Let $m = 2$ and $n = 6$. Then both statements "m is a factor of n^2" and "m is a factor of n" are true because $n = 6 = 2 \cdot 3 = m \cdot 3$ and $n^2 = 36 = 2 \cdot 18 = m \cdot 18$. Thus both the hypothesis and conclusion of $R(m, n)$ are true, and so the statement as a whole is true.

(2) Let $m = 6$ and $n = 2$. Then both statements "m is a factor of n^2" and "m is a factor of n" are false because $n = 2 \neq 6 \cdot k$, for any integer k, and $n^2 = 4 \neq 6 \cdot j$, for any integer j. Thus both the hypothesis and conclusion of $R(m, n)$ are false, and so the statement as a whole is true.

7. *b.* Truth set $= \{1, 2, 3, 6\}$

   d. Truth set $= \{-2, -1, 1, 2\}$

8. *b.* Truth set $= \{1, 2, 3, 4, 5, 6, 7, 8.9\}$

   d. Truth set $= \{-8, -6, -4, -2, 0, 2, 4, 6, 8\}$

10. *Counterexample 1*: Let $a = 1$, and note that $(1 - 1)/1 = 0$ is an integer.

    Counterexample 2: Let $a = -1$, and note that $(-1 - 1)/(-1) = 2$ is an integer.

12. *Counterexample*: Let $x = 1$ and $y = 1$, and note that $\sqrt{1 + 1} = \sqrt{2}$, $\sqrt{1} + \sqrt{1} = 1 + 1 = 2$, and $2 \neq \sqrt{2}$. (This is one counterexample among many. Any real numbers x and y with $xy \neq 0$ will produce a counterexample.)

15. *a. Some acceptable answers:* All squares are rectangles. If a figure is a square then that figure is a rectangle. Every square is a rectangle. All figures that are squares are rectangles. Any figure that is a square is a rectangle.

    b. Some acceptable answers: There is a set with sixteen subsets. Some set has sixteen subsets. Some sets have sixteen subsets. There is at least one set that has sixteen subsets.

16. *b.* ∀ real numbers x, x is positive, negative, or zero.

    d. ∀ logicians x, x is not lazy.

    f. ∀ real numbers x, $x^2 \neq -1$.

17. *b.* ∃ a real number x such that x is rational.

18. *c.* ∀s, if $C(s)$ then $\sim E(s)$.

    d. ∃x such that $C(s) \wedge M(s)$.

20. *Some acceptable answers*: If a student is in CSC 321, then that student has taken MAT 140. All students in CSC 321 have taken MAT 140. Every student in CSC 321 has taken MAT 140. Each student who is in CSC 321 has taken MAT 140. Given any student in CSC 321, that student has taken MAT 140.

21. *b.* ∀x, if x is a valid argument with true premises, then x has a true conclusion.

    Or: ∀ arguments x, if x is valid and x has true premises then x has a true conclusion.

    Or: ∀ valid arguments x, if x has true premises then x has a true conclusion.

    d. ∀ integers m and n, if m and n are odd then mn is odd.

22. *b.* ∀x, if x is a computer science student then x needs to take data structures.

    ∀ computer science students x, x needs to take data structures.

23. *b.* ∃ a question x such that x is easy.

    ∃x such that x is a question and x is easy.

24. *a.* $\forall x$, if x is an integer then x is rational, but $\exists x$ such that x is rational and x is not an integer.

25. *c.* This statement translates as "There is a square that is above *d*." This is false because the only objects above *d* are *a* (a triangle) and *b* (a circle).

    d. This statement translates as "There is a triangle that has *f* above it," or, "*f* is above some triangle." This is true because *g* is a triangle and *f* is above *g*.

26. *a* This statement translates as "0 is a positive real number." This is false: 0 is neither positive nor negative. (See also the order axiom Ord3 on page A-2 of Appendix A: Properties of the Real Numbers.)

    c. This statement translates as "All integers are real numbers." This is true; each integer corresponds to a position along the number line.

27. *a.* This statement translates as "There is a geometric figure that is both a rectangle and a square." This is true. As an example take any square; it is a rectangle whose sides all have the same length.

    b. This statement translates as "There is a geometric figure that is a rectangle but is not a square." This is true. Any rectangle whose sides are not all of the same length is a rectangle that is not a square. For example, one pair of parallel sides could be twice as long as the other pair of parallel sides.

    c. This statement translates as "Every square is a rectangle." This is true. A square is a rectangle satisfying the additional condition that all its sides have the same length.

28. *a.* This statement translates as "There is a prime number that is not odd." This is true. The number 2 is prime and it is not odd.

    c. This statement translates as "There is a number that is both an odd number and a perfect square." This is true. For example, the number 9 is odd and it is also a perfect square (because $9 = 3^2$).

30. *b.* This statement translates as "For all real numbers x, if $x > 2$ then $x^2 > 4$," which is true.

    d. This statement translates as "For all real numbers x, $x^2 > 4$ if, and only if, $|x| > 2$." This is true because $x^2 > 4$ if, and only if, $x > 2$ or $x < -2$, and $|x| > 2$ means that either $x > 2$ or $x < -2$.

31. *c.* This statement translates as "For all real numbers a and b, if $ab = 0$ then $a = 0$ or $b = 0$," which is true.

    d. This statement translates as "For all real numbers a, b, c, and d, if $a < b$ and $c < d$ then $ac < bd$," which is false. *Counterexample*: Let $a = -2$, $b = 1$, $c = -3$, and $d = 0$. Then $a < b$ because $-2 < 1$ and $c < d$ because $-3 < 0$, but $ac \not< bd$ because $ac = (-2)(-3) = 6$ and $bd = 1 \cdot 0 = 0$ and $6 \not< 0$.

Section 2.2

2. Statements *c* and *f* are negations for the given statement.

3. *b.* $\exists$ a computer C such that C does not have a CPU.

   d. $\forall$ bands *b*, *b* has won fewer than 10 Grammy awards.

4. *b.* Some birds cannot fly.

   d. No dogs have spots.

5. *b. Formal negation*: ∃ a real number x such that x is not positive and x is not negative and x is not zero.

   Some acceptable informal negations: There is a real number that is not positive, negative, or zero. There is a real number that is neither positive, negative, nor zero.

   d. Formal negation: ∃ a logician x such that x is lazy.

   Some acceptable informal negations: Some logicians are lazy. There is a logician who is lazy. There is a lazy logician.

   f. Formal negation: ∃ a real number x such that $x^2 = -1$.

   Some acceptable informal negations: There is a real number whose square is -1. The square of some real number is -1.

6. *b. Formal negation*: ∀ real numbers x, x is not rational.

   Some acceptable informal negations: No real numbers are rational. All real numbers are irrational.

8. *Informal negation of the statement*: "There are some simple solutions to life's problems," or "Some solutions to life's problems are simple."

   Formal version of the statement: "∀ solutions to life's problems x, x is not simple," or "∀x, if x is a solution to life's problems then x is not simple."

   Informal version of the statement: "None of the solutions to life's problems is simple," or "No solution to life's problems is simple."

10. ∃ a computer program P such that P compiles without error messages but P is not correct.

12. The proposed negation is not correct. *Correct negation:* There are an irrational number x and a rational number y such that xy is rational. Or: There are an irrational number and a rational number whose product is rational.

14. The proposed negation is not correct. There are two mistakes: The negation of a "for all" statement is not a "for all" statement, and the negation of an "if-then" statement is not an "if-then" statement. *Correct negation:* ∃ real numbers x_1 and x_2 such that $x_1^2 = x_2^2$ and $x_1 \neq x_2$.

15. *b.* True   *d.* True

    e. False: $x = 36$ is a counterexample because the ones digit of x is 6 and the tens digit is neither 1 nor 2.

16. *b. Some acceptable answers*: There is a valid argument with true premises and a false conclusion. ∃ a valid argument x such that x has true premises and x does not have a true conclusion. Some valid arguments with true premises do not have true conclusions.

    d. Some acceptable answers: There are two odd integers whose product is even. ∃ integers m and n such that m and n are odd and mn is even. ∃ odd integers m and n such that mn is even. For some odd integers m and n, mn is even.

17. *Some acceptable answers:* Some computer science student does not need to take data structures. ∃ a computer science student x such that x does not need to take data structures. Some computer science students do not need to take data structures. There is at least one computer science student who does not need to take data structures.

19. ∃ an integer d such that $6/d$ is an integer and $d \neq 3$.

21. ∃ an integer n such that n is prime and both n is not odd and $n \neq 2$.

    Or: ∃ an integer n such that n is prime and n is neither odd nor equal to 2.

23. ∃ an animal x such that x is a dog and either x does not have paws or x does not have a tail.

25. There is an integer n such that n^2 is odd but n is not odd.

    Or: There is an integer that is not odd but whose square is odd.

26. *b. One possible answer*: Let $P(x)$ be "$x^2 \neq 2$." The statements "$\forall x \in \mathbf{Z}, x^2 \neq 2$" and "$\forall x \in \mathbf{Q}, x^2 \neq 2$" are true, but the statement "$\forall x \in \mathbf{R}, x^2 \neq 2$" is false.

28. The given statement cannot be false because its negation is "There exists an occurrence of the letter u in the title of this book that is not lower case," which is not true because there are no occurrences of the letter u in the title of this book. Hence the given statement is true because it is not false. Recall that in a situation such as this we call the statement "true by default" or "vacuously true."

30. *Contrapositive*: ∀ integers d, if $d \neq 3$ then $6/d$ is not an integer.

    Converse: ∀ integers d, if $d = 3$ then $6/d$ is an integer.

    Inverse: ∀ integers d, if $6/d$ is not an integer, then $d \neq 3$.

32. *Contrapositive*: ∀ integers n, if n is not odd and $n \neq 2$ then n is not prime.

    Converse: ∀ integers n, if n is odd or $n = 2$, then n is prime.

    Inverse: ∀ integers n, if n is not prime, then both n is not odd and $n \neq 2$.

    Or: ∀ integers n, if n is not prime, then neither is n odd nor is n equal to 2.

34. *Contrapositive*: ∀ animals x, if x does not have paws or x does not have a tail then x is not a dog.

    Converse: ∀ animals x, if x has paws and x has a tail then x is a dog.

    Inverse: ∀ animals x, if x is not a dog, then either x does not have paws or x does not have a tail.

36. *Contrapositive*: If an integer is not odd, then its square is not odd.

    Converse: If an integer is odd, then its square is odd.

    Inverse: If the square of an integer is not odd, then the integer is not odd.

37. *Possible example 1*: Consider the statement: ∀ real numbers x, if $x > 0$ then $x^2 > 0$. This statement is true. But its inverse is "∀ real numbers x, if $x \not> 0$ then $x^2 \not> 0$," which is false. (One counterexample is $x = -1$ because $-1 \not> 0$ but $(-1)^2 > 0$.)

    Possible example 2: Consider the statement: ∀ integers n that are greater than 2, if n is prime, then n is odd. This statement is true. But its inverse is "∀ integers n that are greater than 2, if n is not prime, then n is not odd, which is false. (One counterexample is $x = 15$ because 15 is not prime but it is odd.)

39. If an integer is divisible by 8, then it is divisible by 4.

41. If a person does not pass a comprehensive exam, then that person cannot obtain a master's degree. *Or*: If a person obtains a master's degree then that person passed a comprehensive exam.

43. There is a person who does not have a large income and is happy.

45. There is a function that is a polynomial but does not have a real root.

46. *Formal Versions*: ∀ computer programs P, if P is correct then P translates without error messages. However, ∃ a computer program P such that P translates without error messages and P is not correct.

    Informal Versions: If a computer program is correct, then it translates without error messages. But some incorrect computer programs also do not produce error messages during translation.

Section 2.3

1. *c.* True: Paris is the capital of France.

   d. False: Miami is not the capital of Brazil.

2. *c.* False: $(\frac{1}{2})^2 = \frac{1}{4} \not> \frac{1}{2}$ *d.* True: $(-2)^2 = 4 > 2$

3. *c.* Let $y = \frac{4}{3}$. Then $xy = (\frac{3}{4})(\frac{4}{3}) = 1$.

4. *b. One possible answer*: Let $n = 10^8 + 1$ *c. One possible answer*: Let $n = 10^{10^{10}} + 1$.

6. True.

Given $x =$	Choose $y =$	Is y a circle above x, with a different color from x?
e	a, b, or c	yes ✓
g	a or c	yes ✓
h	a or c	yes ✓
j	b	yes ✓

8. True. Let $x = f$ or $x = i$. The statement "$\forall$ circles y, y is above x" is true for either choice of x because all the circles are above both of these triangles.

9. *b.* True. *Solution 1*: Let $x = 0$. Then for any real number r, $x + r = r + x = r$ because 0 is an identity for addition of real numbers. Thus, because every element in E is a real number, $\forall y \in E$, $x + y = y$.

   Solution 2: Let $x = 0$. Then $x + y = y$ is true for each individual element y of E:

Choose $x = 0$	Given $y =$	Is $x + y = y$?
	-2	yes: $0 + (-2) = -2$ ✓
	-1	yes: $0 + (-1) = -1$ ✓
	0	yes: $0 + 0 = 0$ ✓
	1	yes: $0 + 1 = 1$ ✓
	2	yes: $0 + 2 = 2$ ✓

10. *b.* This statement says that every student chose a salad. This is false: Yuen did not choose a salad.

    d. This statement says that some particular beverage was chosen by every student. This is false: There is no beverage that was chosen by every student.

    e. This statement says that some particular item was not chosen by any student. This is false: every item was chosen by at least one student.

    f. This statement says that there is a station from which every student made a selection. This is true. In fact, there are three such stations: every student chose a main course, every student chose a dessert, and every student chose a beverage.

11. *b. One solution:* Present all the students in the class with a list of residence halls and ask them to check off all residence halls containing a person they have dated. If some residence hall is checked off by every student in the class, then (assuming the students are all truthful) the statement is true. Otherwise, the statement is false.

    c. One solution: Present all the students in the class with a list of residence halls and ask them to write the number of people they have dated from each hall next to the name of that hall. If no number written down is a 1, then (assuming the students are all truthful) the statement is true. Otherwise, the statement is false.

12. *b.* Every student has seen Star Wars.

   e. There are two different students who have both seen the same movie.

   f. There are two different students, one of whom has seen all the movies that the other has seen.

13. *b. first version of negation*: $\forall\ x$ in D, $\sim (\forall\ y$ in $E, x + y = -y)$.

   final version of negation: $\forall x$ in D, $\exists\ y$ in E such that $x + y \neq -y$.

   The negation is true. No matter what number you might try to use for x, someone can give you a y so that $x + y \neq -y$. Here is a table showing how all possible choices for x could be matched with a y so that $x + y \neq -y$.:

Try $x =$	A person could give $y =$	Is $x + y \neq -y$?
-2	2	$-2 + 2 = 0 \neq -2$ ✓
-1	2	$-1 + 2 = 1 \neq -2$ ✓
0	1	$0 + 1 = 1 \neq -1$ ✓
1	1	$1 + 1 = 2 \neq -1$ ✓
2	2	$2 + 2 = 4 \neq -2$ ✓

In 15, 17, and 19 there are other correct answers besides those shown.

15. *a.* There is at least one book that everyone has read.

   b. Negation: Given any book, there is a person who has not read that book.

   Or: $\forall$ books b, $\exists$ a person p such that p has not read b.

   Or: There is no book that everyone has read.

17. *a.* Every rational number is equal to a ratio of some two integers.

   b. Negation: There is at least one rational number that is not equal to a ratio of any two integers.

   Or: $\exists r \in \mathbf{Q}$ such that $\forall a \in \mathbf{Z}$ and $\forall b \in \mathbf{Z}$, $r \neq a/b$.

19. *a.* There is a real number whose sum with any real number equals zero.

   b. Negation: Given any real number x, there is a real number y such that $x + y \neq 0$.

   Or: $\forall x \in \mathbf{R}$, $\exists y \in \mathbf{R}$ such that $x + y \neq 0$.

20. *b.* Statement (1) says that no matter what circle you might choose, you can find a square of the same color. This is true. There are only three circles, and the following table shows that for each, there is a square of the same color.

Given $x =$	Choose $y =$	Is y a square and does y have the same color as x?
a or c	j	yes ✓
b	g or h	yes ✓

   Statement (2) says that there is one, single square that is the same color as all the circles. This is impossible, and hence false, because there are circles of two different colors.

22. *a.* Given any nonzero real number, a real number can be found so that the product of the two equals 1. This is true: every nonzero real number has a reciprocal. (See Example 2,3,4 or axiom F6 on page A-1 of Appendix A: Properties of the Real Numbers.)

   b. There is a real number whose product with every real number equals 1. This is false. For instance, let $r = 2$. Then because $rs = 1$, we would have $2s = 1$, and so $s = \frac{1}{2}$. But in that case, when $r = 4$ for example, we would have $rs = 4 \cdot \frac{1}{2} = 2$, and $2 \neq 1$.

23. *b.*
$$\sim (\exists x \in D \ (\exists y \in E \ (P(x,y)))) \quad = \quad \forall x \in D \ (\sim (\exists y \in E \ (P(x,y))))$$
$$= \quad \forall x \in D \ (\forall y \in E \ (\sim P(x,y)))$$

25. *a.* The statement is false. Circles *b* and *c* are not above triangle *d*.

    b. *Negation*: $\exists$ a circle *x* and a triangle *y* such that *x* is not above *y*.

27. *a.* The statement says that there are a circle and a square such that the circle is above the square and has the same color as the square. This is true. For example, circle *a* is above square *j* and *a* and *j* have the same color.

    b. *Negation*: $\forall$ circles *x* and $\forall$ squares *y*, *x* is not above *y* or *x* and *y* do not have the same color.

29. *a.* $\forall x \in \mathbf{R}$, $\exists y \in \mathbf{R}^{-}$ such that $x > y$.

    b. The original statement says that there is a real number that is greater than every negative real number. This is true. For instance, 0 is greater than every negative real number.

    The statement with interchanged quantifiers says that no matter what real number might be given, it is possible to find a negative real number that is smaller. This is also true. If the number *x* that is given is positive, *y* could be taken to be -1. Then $x > y$. On the other hand, if the number *x* that is given is 0 or negative, *y* could be taken to be $x - 1$. In this case also, $x > y$.

34. *a.* $\forall$ people *x*, $\exists$ a person *y* such that *x* trusts *y*.

    b. *Negation*: $\exists$ a person *x* such that $\forall$ people *y*, *x* does not trust *y*.

    Or: Somebody trusts nobody.

35. *a.* $\exists$ a person *x* such that $\forall$ people *y*, *x* trusts *y*.

    b. *Negation*: $\forall$ people *x*, $\exists$ a person *y* such that *x* does not trust *y*.

    Or: Nobody trusts everybody.

37. *a.* $\forall$ actions *A*, $\exists$ a reaction *R* such that *R* is equal and opposite to *A*.

    b. *Negation*: $\exists$ an action *A* such that $\forall$ reactions *R*, *R* is not equal to *A* or is not opposite to *A*.

39. *b.* $\forall$ purposes under heaven *p*, $\exists$ a time *t* such that *t* is the time for *p*.

40. *c.* The statement says that there is a real number that is one greater than every real number. This is false. For instance, if the number is one greater than 3, then it equals 4 and so it is not one greater than 4.

    d. The statement says that every positive real number has a positive reciprocal. In other words, given any positive real number, we can find a positive real number such that the product of the two equals 1. This is true.

    f. The statement says that the difference of any two positive integers is a positive integer. This is false because, for example, $2 - 3 = -1$.

    g. The statement says that the difference of any two integers is an integer. This is true.

    h. The statement says that there is a positive real number *u* whose product with any positive real number *v* is less than *v*. This is true. For example, let *u* be any positive real number between 0 and 1. Then $u < 1$, and if *v* is any positive real number we may multiply both sides of the inequality by *v* to obtain $uv < v$.

    i. The statement says that no matter what positive real number *v* might be chosen, it is possible to find a positive real number *u* so that $uv < v$. This statement is also true. For any positive real number *v*, *u* can be taken to be any real number between 0 and 1. The argument in the solution to *h* then applies.

42. $\exists$ a real number $\varepsilon > 0$ such that $\forall$ real numbers $\delta > 0$, $\exists$ a real number x such that $a - \delta < x < a + \delta$ and either $L - \varepsilon \geq f(x)$ or $f(x) \geq L + \varepsilon$.

43. *b.* This statement is false: there are two distinct integers x such that $1/x$ is an integer, namely $x = 1$ and $x = -1$.

    c. This statement is true: given any real number x, if $x + y = 0$ then $y = -x$ and so y exists and is unique.

44. $\exists! x \in D$ such that $P(x) \equiv \exists x \in D$ such that $(P(x) \wedge (\forall y \in D, \text{ if } P(y) \text{ then } y = x))$

    Or: There exists a unique x in D such that $P(x)$.

    Or: There is one and only one x in D such that $P(x)$.

46. *a.* The statement says that there is a triangle that is above all the circles. This is false. Because circle b is in the top row, no triangle is above b.

    b. $\exists x(\text{Triangle}(x) \wedge (\forall y\ (\text{Circle}(y) \rightarrow \text{Above}(x, y))))$

    c. $\forall x \sim (\text{Triangle}(x) \wedge (\forall y\ (\text{Circle}(y) \rightarrow \text{Above}(x, y))))$

    $\equiv \forall x(\sim\text{Triangle}(x) \vee \sim (\forall y(\text{Circle}(y) \rightarrow \text{Above}(x, y))))$

    $\equiv \forall x(\sim\text{Triangle}(x) \vee (\exists y\ (\text{Circle}(y) \wedge \sim \text{Above}(x, y))))$

48. *a.* The statement says that given any object, we can find another object that has a different color. This is true because there are objects of all three colors. So, for example, if we are given a blue object, we can find another that is black or gray, and we can proceed similarly if we are givenan object of either of the other two colors.

    b. $\forall x(\exists y(x \neq y \rightarrow \sim\text{SameColor}(x, y)))$

    c. $\exists x(\forall y(x \neq y \wedge \text{SameColor}(x, y)))$

50. *a.* The statement says that all the circles are to the right of all the triangles. This is false. For instance, circle b is not to the right of triangle c.

    b. $\forall x(\text{Circle}(x) \rightarrow (\forall y\ (\text{Triangle}(y) \rightarrow \text{RightOf}(x, y))))$

    c. $\exists x(\text{Circle}(x) \wedge \sim (\forall y\ (\text{Triangle}(y) \rightarrow \text{RightOf}(x, y))))$

    $\equiv \exists x(\text{Circle}(x) \wedge (\exists y\ (\text{Triangle}(y) \wedge \sim\text{RightOf}(x, y))))$

52. *a.* The statement says that there are a circle and a triangle that have the same color. This is false. All the triangles are blue, and no circles are blue.

    b. $\exists x(\text{Circle}(x) \wedge (\exists y\ (\text{Triangle}(y) \wedge \text{SameColor}(x, y))))$

    c. $\forall x(\sim\text{Circle}(x) \vee \sim (\exists y\ (\text{Triangle}(y) \wedge \text{SameColor}(x, y))))$

    $\equiv \forall x(\sim\text{Circle}(x) \vee (\forall y\ (\sim\text{Triangle}(y) \vee \sim \text{SameColor}(x, y))))$

54. These statements do not necessarily have the same truth values. For instance, let $D = \mathbf{R}$, the set of all real numbers, let $P(x)$ be "x is positive," and let $Q(x)$ be "x is negative." Then "$\exists x \in D, (P(x) \wedge Q(x)$" can be written "$\exists$ a real number x such that x is both positive and negative," which is false. On the other hand, "$(\exists x \in D,\ P(x)) \wedge (\exists x \in D, Q(x))$ can be written "$\exists$ a real number that is positive and $\exists$ a real number that is negative," which is true.

55. These statements do not necessarily have the same truth values. For example, let $D = \mathbf{Z}$, the set of all integers, let $P(x)$ be "x is even," and let $Q(x)$ be "x is odd." Then the statement "$\forall x \in D, (P(x) \vee Q(x))$" can be written "$\forall$ integers x, x is even or x is odd," which is true. On the other hand, "$(\forall x \in D, P(x)) \vee (\forall x \in D,\ Q(x))$" can be written "All integers are even or all integers are odd," which is false.

56. These statements have the same truth values for all domains D and predicates $P(x)$ and $Q(x)$.

   If the statement "$\exists x \in D, (P(x) \vee Q(x))$" is true, then by definition of the truth values for $\exists$, the predicate $P(x) \vee Q(x)$ is true for at least one element x in D. Let's call such an element x_0. Then $P(x_0) \vee Q(x_0)$ is true, and so by definition of the truth values for $\vee$, at least one of $P(x_0)$ or $Q(x_0)$ is true. In case $P(x_0)$ is true, then the statement "$\exists x \in D, \ P(x)$" is true. In case $Q(x_0)$ is true, then the statement "$\exists x \in D, \ Q(x)$" is true. Since at least one of these cases must occur, the statement "$(\exists x \in D, \ P(x)) \vee (\exists x \in D, \ Q(x))$" is true by definition of truth values for $\vee$.

   If the statement "$(\exists x \in D, \ P(x)) \vee (\exists x \in D, \ Q(x))$" is true, then by definition of truth values for $\vee$, at least one of the statements "$\exists x \in D, \ P(x)$" or "$\exists x \in D, \ Q(x)$" is true. In case "$\exists x \in D, \ P(x)$" is true, then by definition of truth values for $\exists$, there exists an element, say x_1, in D such that $P(x_1)$ is true. Then by definition of the truth values for $\vee$, $P(x_1) \vee Q(x_1)$ is true, and so by definition of the truth values for $\exists$, "$\exists x, (P(x) \vee Q(x))$" is true. Similarly, in case "$\exists x \in D, \ Q(x)$" is true, then by definition of truth values for $\exists$, there exists an element, say x_2, in D such that $Q(x_2)$ is true. It follows by definition of the truth values for $\vee$ that $P(x_2) \vee Q(x_2)$ is true, and so by definition of the truth values for $\exists$, "$\exists x, (P(x) \vee Q(x))$" is true. Since one of the two cases must occur, we can conclude that the statement "$\exists x \in D, (P(x) \vee Q(x))$" is true.

58. *a.* No   *b.* No   *c.* $X = g$

59. *a.* Yes   *b.* $X = g$ *c.* $X = b_1$, $X = w_1$

Section 2.4

1. *a.* $(x+y)^2 = x^2 + 2xy + y^2$

   e. $(\log(t_1) + \log(t_2))^2 = (\log(t_1))^2 + 2(\log(t_1))(\log(t_2)) + (\log(t_2))^2$

4. $(3^{\frac{1}{2}})^6 = 3^{(\frac{1}{2})(6)}$

6. This computer program is not correct.

11. invalid, converse error

12. invalid, inverse error

13. valid, universal modus ponens

14. invalid, inverse error

15. invalid, converse error

17. invalid, converse error

18. valid, universal modus tollens

19. *c.* valid, universal modus tollens

   d. invalid, inverse error

20. *a.* Either of the following diagrams could represent the given premises.
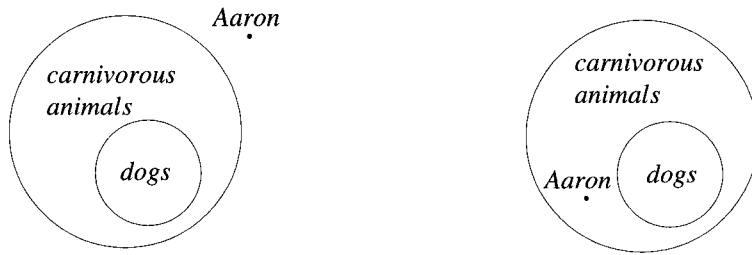
In both, the premises are true, but in (1) the conclusion is true whereas in (2) the conclusion is false.

b. The answer to (a) shows that there is an argument of the given form with true premises and a false conclusion. Hence the argument form is invalid. (This shows that the universal form of inverse error is invalid.)

22. Invalid. Let D be the set of all discrete mathematics students, T the set of all thoughtful people, and V the set of all people who can tell a valid from an invalid argument. Any one of the following diagrams could represent the given premises.
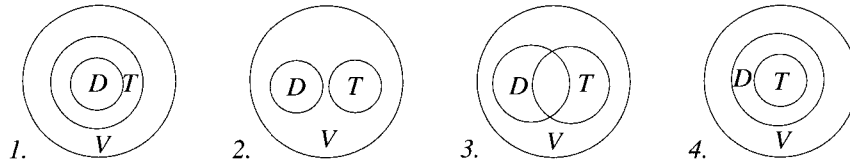
Only in drawing (1) is the conclusion true. Hence it is possible for the premises to be true while the conclusion is false, and so the argument is invalid.

24. Valid. The only drawing representing the truth of the premises also represents the truth of the conclusion.

26. Valid. The only drawing representing the truth of the premises also represents the truth of the conclusion.
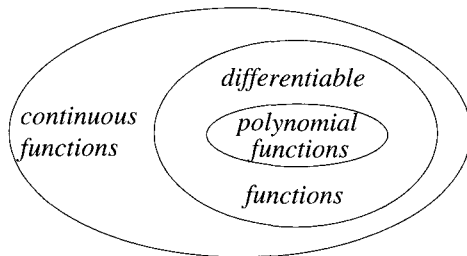
27. Valid. The only drawing representing the truth of the premises also represents the truth of the conclusion.
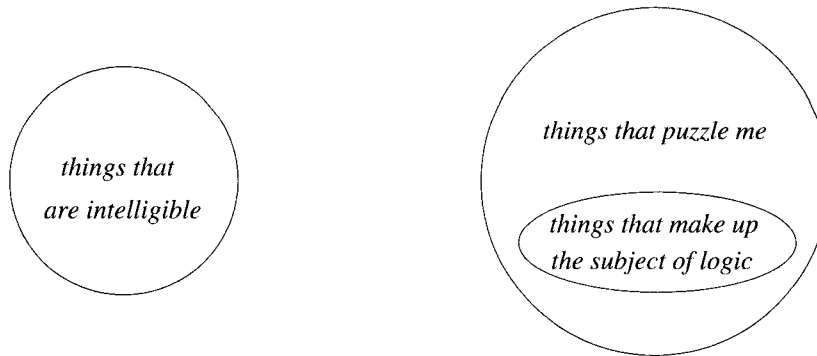
29. 2. (*contrapositive form*) If an object is a square, then it is above all the black objects.

   3. If an object is above all the black objects, then it is to the right of all the triangles.

   1. If an object is to the right of all the triangles, then it is above all the circles.

   ∴ If an object is a square, then it is above all the circles. Or, equivalently: All the squares are above all the circles.

30. 3. If an object is black, then it is a square.

   2. (*contrapositive form*) If an object is a square, then it is above all the gray objects.

   4. If an object is above all the gray objects, then it is above all the triangles.

   1. If an object is above all the triangles, then it is above all the blue objects.

   ∴ If an object is black, then it is above all the blue objects.

32. 2. The arguments in these examples are not arranged in regular order like the ones I am used to.

   4. If arguments in examples are not arranged in regular order like the ones I am used to, then I cannot understand them.

   1. (*contrapositive form*) If I can't understand a logic example, then I grumble when I work it.

   5. If I grumble at an example, then it gives me a headache.

   3. (*contrapositive form*) If an example makes my head ache, then it is not easy.

∴ These examples are not easy.

34. 3. Shakespeare wrote *Hamlet*.

   5. If a person wrote *Hamlet*, then that person was a true poet.

   2. If a person is a true poet, then he can stir the human heart.

   4. If a writer can stir the human heart, then that writer understands human nature.

   1. If a writer understands human nature, then that writer is clever.

∴ Shakespeare was clever.

35. The law of universal modus tollens says that the following form of argument is valid:

$$\forall x \text{ in } D, \text{ if } P(x) \text{ then } Q(x). \quad \leftarrow major\ premise$$
$$\sim Q(c) \text{ for a particular } c \text{ in } D. \quad \leftarrow minor\ premise$$
$$\therefore \quad \sim P(c).$$

Proof of Validity: Suppose the major and minor premises of the above argument form are both true. *[We must show that the conclusion* $\sim P(c)$ *is true.]* By the minor premise, $\sim Q(c)$ is true for a particular value of c in D. By the major premise and the rule of universal instantiation, the statement "If $P(c)$ then $Q(c)$" is true for that particular c. But by modus tollens, since the statements "If $P(c)$ then $Q(c)$" and " $\sim Q(c)$" are both true, it follows that $\sim P(c)$ is also true. *[This is what was to be shown.]*

36. The universal form of elimination (part a) says that the following form of argument is valid:

    $\forall x$ in D, $P(x) \vee Q(x)$. $\leftarrow$ *major premise*
    $\sim Q(c)$ for a particular c in D. $\leftarrow$ *minor premise*
    $\therefore$ $P(c)$

Proof of Validity: Suppose the major and minor premises of the above argument form are both true. *[We must show the truth of the conclusion* $P(c)$.*]* By definition of truth value for a universal statement, $\forall x$ in D, $P(x) \vee Q(x)$ is true if, and only if, the statement "$P(x) \vee Q(x)$" is true for each individual element of D. So, by universal instantiation, it is true for the particular element c. Hence "$P(c) \vee Q(c)$" is true. And since the minor premise says that $\sim Q(c)$, it follows by the elimination rule that $P(c)$ is true. *[This is what was to be shown.]*

Chapter 3: Elementary Number Theory and Methods of Proof

One aim of this chapter is to introduce students to methods for evaluating whether a given mathematical statement is true or false. Throughout the chapter the emphasis is on learning to prove and disprove statements of the form "$\forall x$ in D, if $P(x)$ then $Q(x)$." To prove such a statement directly, one supposes one has a particular but arbitrarily chosen element x in D for which $P(x)$ is true and one shows that $Q(x)$ must also be true. To disprove such a statement, one shows that there is an element x in D (a counterexample) for which $P(x)$ is true and $Q(x)$ is false. To prove such a statement by contradiction, one shows that no counterexample exists, that is, one supposes that there is an x in D for which $P(x)$ is true and $Q(x)$ is false and one shows that this supposition leads to a contradiction. Direct proof, disproof by counterexample, and proof by contradiction can, therefore, all be viewed as three aspects of one whole. One arrives at one or the other by a thoughtful examination of the given statement, knowing what it means for a statement of that form to be true or false.

A cautionary note: A number of students do not immediately recognize that showing that a statement is false is the same as disproving it, and that, if the statement is universal, the most common way to disprove it is by providing a counterexample. You may find it necessary to make these points more than once to convey them to all the students in your class.

Another aim of the chapter is to provide students with fundamental knowledge about numbers that is needed in mathematics and computer science. Surprisingly many college students have little intuition for numbers, even integers. Many claim not to be familiar with how to write down a prime factorization, and even very good students often do not know that a rational number is a ratio of integers (having been taught to think of rational numbers as certain kinds of decimals). To accommodate a wide range of student backgrounds and abilities, the exercise sets contain problems of varying difficulty. It is especially important in this chapter to keep in close touch with how students are doing so as to assign problems at an appropriate level.

Suggestions

1. The careful use of definitions is stressed throughout the chapter. To bring the idea alive in class, you might try the following technique. Each time you write the definition for a new term, go through a few examples, phrasing each as a question. For instance, immediately after defining rational, write "Is 0.873 rational?" and simultaneously ask the question out loud. To a student's answer of "yes," write "Yes, because" and look expectantly at the student. The student may be surprised that you seem to expect additional words but is generally able to supply the reason without difficulty (or other students may help out). You move on to slightly more complicated examples (Is $-(5/3)$ rational? Is 0 rational? Is $0.252525\ldots$ rational?), each time acting as if you take it for granted that the student answering the question will give a reason. Soon students learn to give the reference to the definition without prompting and gradually they come to understand the value of using the definition as a test to answer such questions. By the way, if your students dispute that 0 is divisible by, say, 2 (a common occurrence), you can use the occasion to emphasize that it is the definition, and only the definition, that determines the answer.

2. On due dates for assignments that ask for proofs, it is helpful to recruit members of the class to present their proofs to the class as a whole. If the students' proofs are perfect, they serves as a model for the rest of the class. If they are less than perfect, the class benefits from analyzing them together. In the early stages, it is especially helpful for students to see what kinds of things the instructor finds both to correct and to praise in a proof. Corrections must, of course, be made with regard for the feelings of the student making the presentation. But normally criticism can be balanced with praise in a way that students find encouraging.

3. A number of exercises in the book are phrased as open-ended questions, requiring students to find an answer and justify it with either a proof or a counterexample. After you have assigned one of these exercises, students will often ask that the answer be shown in class. When this happens, you might leave the question open for a while for the class to discuss as a group, perhaps suggesting that students imagine they are the mathematical problem-solving group of a large company and that the answer to the question carries consequences of considerable importance to the company. This works best if you act as a leader but stay somewhat in the background, identifying students who hold opposing points of view and inviting them to come to the board to present their answers for the rest of the class to critique, but feigning ignorance as to the answer and indicating that it is the responsibility of the group as a whole to come to a consensus. (The reason you need to lead the discussion is that if, for instance, the statement is false, you would generally want to arrange for a false "proof" to be shown before a counterexample.) Determining collectively which proofs are valid and which are not and which counterexamples work and which do not can be an informative demonstration of the nature of mathematical truth and a good advertisement for the usefulness of some of the logic studied in the course.

In cases when the given statement is false, you might ask some of the students who found a counterexample to try to explain to the other students what reasoning they used to discover it. The resulting discussion can be quite worthwhile.

4. At some point during this chapter, you might mention proof by handwaving, proof by intimidation, and so forth, contrasting the feeling of unease produced in the hearer by these methods with the feeling of "mathematical certainty" produced by careful use of the methods discussed in the chapter. The question of what is mathematical certainty has been debated in connection with mathematical results such as the proof of the four-color theorem. At the frontiers of mathematical research this question does not have a simple answer. But to understand the issues in the current debate, students need a background of experience in understanding and appreciating simpler proofs, such as those discussed in this chapter.

5. One of the trickiest issues you will face in teaching proof is what style to use for the proofs you write in class. Because students catch onto the idea of the proof at dramatically different rates, it seems best to be careful and complete in class. For instance, you might always start with the words "let" or "suppose," state the full supposition, and even include a bracketed [We must show that ...], pointing out at appropriate times how being aware of what is to be shown helps guide the steps of the argument. Part of the reason for taking care in this chapter is to encourage students to develop habits that will serve them well when they encounter mathematics that is more abstract in later chapters and subsequent courses. For instance, the habit of identifying the supposition and the conclusion to be shown in a proof of a statement is very helpful to students when they confront problems in set theory, functions, and relations (*e.g.*, the proof that a composition of one-to-one functions is one-to-one or that a given binary relation is transitive). Exercises 20–23 of Section 3.1 are designed to lay a groundwork for student appreciation of the power and generality of the method of generalizing from the generic particular. Although many students come to a full appreciation only late in the course, pointing out at an early stage that the method depends only on the form of the statement to be proved creates a point of reference for later discussion.

6. A related and equally tricky issue in teaching proof is how to specify an acceptable range of proof styles for students' work. Students need reassurance that acceptable proofs may be written in many different styles, but they also need encouragement to write coherently. To motivate students to write in sentences and in adequate detail, you might suggest that they imagine writing their proofs for an intelligent classmate who has missed the last few days of the course or in a style that they themselves would have been able to understand when they were first learning the subject matter. To emphasize the importance of precision, you might compare writing a mathematical proof with writing a computer program. You might also suggest that a proof is fundamentally a work of communication and point out that employers in business and industry are demanding ever better communication skills from those whom they hire.

Particular requirements, such as that all variables used in a proof be introduced or that all proofs be written in complete sentences, will undoubtedly vary from one instructor to another. In the answers given in Appendix B, two different versions of the first proof of Section 3.1 are written out to illustrate some of the variety that is possible. The text itself contains a note to the effect that students should expect to find out from their instructor what the requirements are to be in their class. In one of my classes I happened to write "p.b.a.c." for "particular but arbitrarily chosen" and found that a number of students enthusiastically incorporated this abbreviation in their written work. Although I tell my students that writing these words is optional, they seem to like to use the abbreviation because it reminds them of the idea of the generic particular with very little effort.

Comments on Exercises

Exercise Set 3.1: **#60** and **#61**: The solutions use the fact (proved formally in Section 3.4) that any integer is either even or odd, and they use the concept of argument by contradiction (developed formally in Section 3.6).

Exercise Set 3.3: **#24**: This exercise is often effective at stimulating lively class discussion. Occasionally, a very good student will come up with an ingenious "proof," and sometimes students will propose counterexamples that are not really counterexamples. **#31** This is another exercise whose solution requires proof by contradiction.

Exercise Set 3.7: **#5** and **#6** are designed to counter student misgeneralizations that any ratio of two numbers is rational and that any square root is irrational.

Section 3.1

3. *a.* Yes, because $4rs = 2 \cdot (2rs)$ and $2rs$ is an integer since r and s are integers and products of integers are integers.

   b. Yes, because $6r + 4s^2 + 3 = 2(3r + 2s^2 + 1) + 1$ and $3r + 2s^2 + 1$ is an integer since r and s are integers and products and sums of integers are integers.

   c. Yes, because $r^2 + 2rs + s^2 = (r + s)^2$ and $r + s$ is an integer that is greater than or equal to 2 since both r and s are positive integers and thus each is greater than or equal to 1.

5. For example, let $m = 1$ and $n = -1$. Then $\frac{1}{m} + \frac{1}{n} = \frac{1}{1} + \frac{1}{(-1)} = 1 + (-1) = 0$. (In fact, if k is any nonzero integer, then $\frac{1}{k} + \frac{1}{(-k)} = \frac{1}{k} + \left(-\frac{1}{k}\right) = 1 + (-1) = 0$.)

6. For example, let $a = 1$ and $b = 0$. Then $\sqrt{a+b} = \sqrt{1} = 1$ and $\sqrt{a} + \sqrt{b} = \sqrt{1} + \sqrt{0} = 1$ also. Hence $\sqrt{a+b} = \sqrt{a} + \sqrt{b}$ for these values of a and b. (Note that, in fact, if a is any nonzero integer and $b = 0$, then $\sqrt{a+b} = \sqrt{a+0} = \sqrt{a} = \sqrt{a} + 0 = \sqrt{a} + \sqrt{0} = \sqrt{a} + \sqrt{b}$.)

8. For example, let $x = 60$. Note that to four significant digits $2^{60} \cong 1.153 \times 10^{18}$ and $60^{10} \cong 6.047 \times 10^{17}$, and so $2^x \geq x^{10}$. Examples can also be found in the approximate range $1 < x < 1.077$. For instance, $2^{1.07} \cong 2.099$ and $1.07^{10} \cong 1.967$, and so $2^{1.07} > 1.07^{10}$.

10. Note that $2n^2 - 5n + 2 = (2n - 1)(n - 2)$. Thus, for example, we may let $n = 3$. Then $2n^2 - 5n + 2 = (2 \cdot 3 - 1)(3 - 2) = 5$, which is prime.

12. *Counterexample*: Let $n = 5$. Then $\frac{n-1}{2} = \frac{5-1}{2} = \frac{4}{2} = 2$, which is not odd.

13. *Counterexample*: Let $m = 2$ and $n = 1$. Then $2m + n = 2 \cdot 2 + 1 = 5$, which is odd. But m is not odd, and so it is false that both m and n are odd.

15. Note that $3n^2 - 4n + 1 = (3n - 1)(n - 1)$. Therefore, we can show that this property is true for some integers and false for other integers. For example, when $n = 2$, then $3n^2 - 4n + 1 = (3 \cdot 2 - 1)(2 - 1) = 5$, which is prime. However, when $n = 3$, then $3n^2 - 4n + 1 = (3 \cdot 3 - 1)(3 - 1) = 8 \cdot 2 = 16$, which is not prime.

16. This property is true for some integers and false for other integers. For example, the average of 1 and 5 is $\frac{1+5}{2} = \frac{6}{2} = 3$, which is odd. However, the average of 1 and 3 is $\frac{1+3}{2} = \frac{4}{2} = 2$, which is not odd.

18. $1^2 - 1 + 11 = 11$, which is prime. $2^2 - 2 + 11 = 13$, which is prime.
    $3^2 - 3 + 11 = 17$, which is prime. $4^2 - 4 + 11 = 23$, which is prime.
    $5^2 - 5 + 11 = 31$, which is prime. $6^2 - 6 + 11 = 41$, which is prime.
    $7^2 - 7 + 11 = 53$, which is prime. $8^2 - 8 + 11 = 67$, which is prime.
    $9^2 - 9 + 11 = 83$, which is prime. $10^2 - 10 + 11 = 101$, which is prime.

21. *Start of Proof*: Suppose x is any *[particular but arbitrarily chosen]* real number such that $x > 1$. *[We must show that $x^2 > x$.]*

23. *Start of Proof*: Suppose x is any *[particular but arbitrarily chosen]* real number such that $0 < x < 1$. *[We must show that $x^2 < x$.]*

26. *Proof 1*: Suppose m and n are any *[particular but arbitrarily chosen]* integers such that m is odd and n is even. *[We must show that $m - n$ is odd.]* By definition of odd and even, there exist integers r and s such that $m = 2r + 1$ and $n = 2s$. Then $m - n = (2r + 1) - 2s = 2r - 2s + 1 = 2(r - s) + 1$. But $r - s$ is an integer because r and s are integers and a difference of integers is an integer. Hence $m - n$ equals twice an integer plus 1, and so by definition of odd, $m - n$ is odd *[as was to be shown]*.

    Proof 2: Suppose m and n are any *[particular but arbitrarily chosen]* integers such that m is odd and n is even. *[We must show that $m - n$ is odd.]* By definition of odd and even, there exist integers r and s such that $m = 2r + 1$ and $n = 2s$. Then $m - n = (2r + 1) - 2s = 2r - 2s + 1 = 2(r - s) + 1$. Let $t = r - s$. Then t is an integer because r and s are integers and a difference of integers is an integer. Hence $m - n = 2t + 1$, where t is an integer, and so by definition of odd, $m - n$ is odd *[as was to be shown]*.

27. *Proof 1*: Suppose m and n are any *[particular but arbitrarily chosen]* odd integers. *[We must show that $m+n$ is even.]* By definition of odd, there exist integers r and s such that $m = 2r + 1$ and $n = 2s + 1$. Then $m + n = (2r + 1) + (2s + 1) = 2r + 2s + 2 = 2(r + s + 1)$. Let $u = r + s + 1$. Then u is an integer because r, s, and 1 are integers and a sum of integers is an integer. Hence $m + n = 2u$, where u is an integer, and so by definition of even, $m + n$ is even *[as was to be shown]*.

    Proof 2: Suppose m and n are any *[particular but arbitrarily chosen]* odd integers. *[We must show that $m+n$ is even.]* By definition of odd, there exist integers r and s such that $m = 2r + 1$ and $n = 2s + 1$. Then $m + n = (2r + 1) + (2s + 1) = 2r + 2s + 2 = 2(r + s + 1)$. But $r + s + 1$ is an integer because r, s, and 1 are integers and a sum of integers is an integer. Hence $m + n$ equals twice an integer, and so by definition of even, $m + n$ is even *[as was to be shown]*.

28. *Proof*: Suppose n is any *[particular but arbitrarily chosen]* odd integer. *[We must show that n^2 is odd.]* By definition of odd, $n = 2r + 1$ for some integer r. Then $n^2 = (2r + 1)^2 = (2r + 1)(2r + 1) = 4r^2 + 4r + 1 = 2(2r^2 + 2r) + 1$. Let $k = 2r^2 + 2r$. Then k is an integer because r is an integer and products and sums of integers are integers. Hence $n^2 = 2k + 1$, where k is an integer, and so by definition of odd, n^2 is odd *[as was to be shown]*.

30. *Proof:* Suppose n is any odd integer. *[We must show that $(-1)^n = -1$.]* By definition of odd, $n = 2k + 1$ for some integer k. By substitution and the laws of exponents, $(-1)^n = (-1)^{2k+1} = (-1)^{2k} \cdot (-1) = ((-1)^2)^k \cdot (-1)$. But $(-1)^2 = 1$, and since 1 raised to any power equals 1, $((-1)^2)^k = 1^k = 1$. Hence, by substitution, $(-1)^n = ((-1)^2)^k \cdot (-1) = 1 \cdot (-1) = -1$ *[as was to be shown]*.

32. To prove the given statement is false, we prove that its negation is true. The negation of the statement is "For all integers n, $6n^2 + 27$ is not prime."

Proof of the negation: Suppose n is any integer. *[We must show that $6n^2 + 27$ is not prime.]* Note that $6n^2 + 27$ is positive because $n^2 \geq 0$ for all integers n and products and sums of positive real numbers are positive. Then $6n^2 + 27 = 3(2n^2 + 9)$, and both 3 and $2n^2 + 9$ are positive integers each greater than 1 and less than $6n^2 + 27$. So $6n^2 + 27$ is not prime.

33. To prove the given statement is false, we prove that its negation is true. The negation of the statement is "For all integers k with $k \geq 4$, $2k^2 - 5k + 2$ is not prime."

    Proof of the negation: Suppose k is any integer with $k \geq 4$. *[We must show that $2k^2 - 5k + 2$ is not prime.]*. We can factor $2k^2 - 5k + 2$ to obtain $2k^2 - 5k + 2 = (2k - 1)(k - 2)$. But since $k \geq 4$, $k - 2 \geq 2$. Also $2k \geq 2 \cdot 4 = 8$, and thus $2k - 1 \geq 8 - 1 = 7$. This shows that each factor of $2k^2 - 5k + 2$ is a positive integer not equal to 1, and so $2k^2 - 5k + 2$ is not prime.

37. This incorrect "proof" begs the question. The second sentence states a conclusion that follows from the assumption that $m \cdot n$ is even. The next-to-last sentence states this conclusion as if it were known to be true. But it is not known to be true. In fact, it is the main task of a genuine proof to derive this conclusion, not from the assumption that it is true but from the hypothesis of the theorem.

38. The mistake in the "proof" is that the same symbol, k, is used to represent two different quantities. By setting both m and n equal to $2k$, the "proof" specifies that $m = n$, and, therefore, it only deduces the conclusion in case $m = n$. If $m \neq n$, the conclusion is often false. For instance, $6 + 4 = 10$ but $10 \neq 4k$ for any integer k.

42. *Proof*: Suppose m is any even integer and n is any integer. *[We must show that mn is even.]* By definition of even, there exists an integer k such that $m = 2k$. By substitution and algebra, $mn = (2k)n = 2(kn)$. But $2(kn)$ is even because kn is an integer (being a product of integers). Hence mn is even*[as was to be shown]*.

44. *Proof*: Let m and n be any even integers. By definition of even, $m = 2r$ and $n = 2s$ for some integers r and s. By substitution, $m - n = 2r - 2s = 2(r - s)$. Since $r - s$ is an integer (being a difference of integers), then $m - n$ equals twice some integer, and so $m - n$ is even by definition of even.

45. *Proof*: Let m and n be any odd integers. By definition of odd, $m = 2r + 1$ and $n = 2s + 1$ for some integers r and s. By substitution, $m - n = (2r + 1) - (2s + 1) = 2(r - s)$. Since $r - s$ is an integer (being a difference of integers), then $m - n$ equals twice some integer, and so $m - n$ is even by definition of even.

46. *Proof 1*: Suppose m and n are any *[particular but arbitrarily chosen]* integers such that $n - m$ is even. *[We must show that $n^3 - m^3$ is even.]* Note that $n^3 - m^3 = (n - m)(n^2 + nm + m^2)$, and $n - m$ is even by supposition. So, by definition of even, $n - m = 2r$ for some integer r. Thus $n^3 - m^3 = (n - m)(n^2 + nm + m^2) = 2r(n^2 + nm + m^2) = 2[r(n^2 + nm + m^2)]$. Let $s = r(n^2 + nm + m^2)$. Then s is an integer because products and sums of integers are integers. Hence, by substitution, $n^3 - m^3 = 2s$, where s is an integer, and so, by definition of even, $n^3 - m^3$ is even *[as was to be shown]*.

    Proof 2: Suppose m and n are any *[particular but arbitrarily chosen]* integers such that $n - m$ is even. *[We must show that $n^3 - m^3$ is even.]* Note that $n^3 - m^3 = (n - m)(n^2 + nm + m^2)$. Now $n - m$ is even by supposition and $n^2 + nm + m^2$ is an integer (being a sum of products of integers). Thus $(n - m)(n^2 + nm + m^2)$ is the product of an even integer and an integer, and so, by exercise 42, it is even. Hence, by substitution, $n^3 - m^3$ is even *[as was to be shown]*.

47. *Counterexample*: Let $n = 2$. Then n is prime but $(-1)^n = (-1)^2 = 1 \neq -1$.

48. *Counterexample*: Let $m = 3$. Then $m^2 - 4 = 9 - 4 = 5$, which is not composite.

49. *Counterexample*: Let $n = 11$. Then $n^2 - n + 11 = 11^2 - 11 + 11 = 11^2$, which is not a prime number.

51. *Counterexample*: The number 28 cannot be expressed as a sum of three or fewer perfect squares. The only perfect squares that could be used to add up to 28 are those that are smaller than 28: 1, 4, 9, 16, and 25. The method of exhaustion can be used to show that no combination of these numbers add up to 28. (In fact, there are just three ways to express 28 as a sum of four or fewer of these numbers: $28 = 25 + 1 + 1 + 1 = 16 + 4 + 4 + 4 = 9 + 9 + 9 + 1$, and in none of these ways are only three perfect squares used.)

52. *Proof*: Consider any product of four consecutive integers. Call the second smallest of the four n. Then the product is $(n-1)n(n+1)(n+2)$. Let $m = n^2 + n - 1$. Note that m is an integer because sums, products, and differences of integers are integers. Also
$$
\begin{aligned}
m^2 - 1 &= (n^2 + n - 1)^2 - 1 = (n^4 + 2n^3 - n^2 - 2n + 1) - 1 \\
&= n^4 + 2n^3 - n^2 - 2n = (n-1)n(n+1)(n+2).
\end{aligned}
$$
Hence the given product of four consecutive integers is one less than a perfect square.

53. *Counterexample*: Let $m = n = 3$. Then $mn = 3 \cdot 3 = 9$, which is a perfect square, but neither m nor n is a perfect square.

54. *Proof*: Suppose two consecutive integers are given. Call the smaller one n. Then the larger is $n + 1$. Let m be the difference of the squares of the numbers. Then $m = (n+1)^2 - n^2 = (n^2 + 2n + 1) - n^2 = 2n + 1$. Because n is an integer, $m = 2 \cdot (\text{an integer}) + 1$, and so m is odd by definition of odd.

55. *Proof*: Suppose a and b are any nonnegative real numbers. Then

$$\sqrt{a} = \text{ the unique nonnegative real number } u \text{ such that } u^2 \text{ equals } a$$

and
$$\sqrt{b} = \text{ the unique nonnegative real number } v \text{ such that } v^2 \text{ equals } b.$$

By substitution and the laws of exponents, $ab = u^2 v^2 = (uv)^2$. So uv is that unique nonnegative real number such that $(uv)^2 = ab$. Hence $\sqrt{ab} = uv = \sqrt{a}\sqrt{b}$.

56. *Counterexample*: Let $a = 1$ and $b = 1$. Then $\sqrt{a+b} = \sqrt{1+1} = \sqrt{2}$ and $\sqrt{a} + \sqrt{b} = \sqrt{1} + \sqrt{1} = 2$, and $\sqrt{2} \neq 2$.

57. If m and n are perfect squares, then $m = a^2$ and $n = b^2$ for some integers a and b. We may take a and b to be nonnegative because for any real number x, $x^2 = (-x)^2$ and if x is negative then $-x$ is nonnegative. By substitution,
$$
\begin{aligned}
m + n + 2\sqrt{mn} &= a^2 + b^2 + 2\sqrt{a^2 b^2} \\
&= a^2 + b^2 + 2ab \qquad \text{since } a \text{ and } b \text{ are nonnegative} \\
&= (a+b)^2.
\end{aligned}
$$
But $a + b$ is an integer (since a and b are), and so $m + n + 2\sqrt{mn}$ is a perfect square.

58. *Counterexample*: Let $p = 11$. Then $2^p - 1 = 2^{11} - 1 = 2047 = 89 \cdot 23$, and so $2^p - 1$ is not prime.

59. *Counterexample*: Let $n = 5$. Then $2^{2^n} + 1 = 2^{32} + 1 = 4,294,967,297 = (641) \cdot (6,700,417)$, and so $2^{2^n} + 1$ is not prime.

60. *a.* Note that $(x - r)(x - s) = x^2 - (r + s)x + rs$. If both r and s are odd integers, then $r + s$ is even and rs is odd (by exercises 27 and 39). If both r and s are even integers, then both $r + s$ and rs are even (by Theorem 3.1.1 and exercise 42). If one of r and s is even and the other is odd, then $r + s$ is even and rs is odd (by exercise 19 and the solution to exercise 42).

b. It follows from part(a) that $x^2 - 1253x + 255$ cannot be written as a product of the form $(x - r)(x - s)$ because for none of the possible cases (both r and s odd, both r and s even, and one of r and s odd and the other even) are both $r + s$ and rs odd integers. *[In Section 3.4, we establish formally that any integer is either even or odd.]*

61. *a.* Suppose a cubic polynomial can be written as a product of three factors of the following form:
$$(x - r)(x - s)(x - t) = x^3 - (r + s + t)x^2 + (rs + rt + st)x + rst.$$

All three of r, s, and t could be even, two could be even and one odd, two could be odd and one even, or all three could be odd.

If all three are even, then $r + s + t$, and $rs + rt + st$, and rst are all even because by Theorem 3.1.1 and exercise 42 sums and products of even integers are even.

If two are even and one is odd, then $r + s + t$ is odd because the sum of the two even integers is even (Theorem 3.1.1) and adding the odd integer makes the final sum odd (exercise 19). Also $rs + rt + st$ is even because each term of the sum has an even factor (exercise 42) and a sum of even integers is even (Theorem 3.1.1). Finally, rst is even because two of the factors are even (exercise 42).

If one is even and two are odd, then rst is even because it has an even factor (exercise 42), and $r + s + t$ is even because the sum of the two odd integers is even (exercise 27) and adding the even integer makes the final sum even (Theorem 3.1.1). Also $rs + rt + st$ is odd because (a) each of the two terms with an even factor is even (exercise 42), and so the sum of these terms is even (Theorem 3.1.1), (b) the term with two odd factors is odd (exercise 39), and thus (c) the final sum is an even integer plus an odd integer, which is odd (exercise 19).

If all three are odd, then rst is odd (exercise 39). In the sum $r + s + t$, two of the odd integers add up to an even integer (exercise 27), to which the third odd integer is added, producing an odd integer (exercise 19). Finally, rs, rt, and st are all odd (exercise 39), and so the sum of two of these is even (exercise 27) and when the third is added an odd integer is obtained (exercise 19).

Therefore: Consider a cubic polynomial of the form $x^3 + ax^2 + bx + c$, where a, b, and c are integers. If the polynomial can be factored as a product of three linear factors, then either (1) all three of a, b, and c are even, or all three of a, b, and c are odd, or two of a, b, and c are even and one is odd. In other words, it is impossible for two of a, b, and c to be odd and the third even.

b. The polynomial $15x^3 + 7x^2 - 8x - 27$ cannot be written as a product of two polynomials with integer coefficients. The reason is that if it could be so factored, then there would exist integers a, b, c, d, and e so that
$$\begin{aligned} 15x^3 + 7x^2 - 8x - 27 &= (ax^2 + bx + c)(dx + e) \\ &= adx^3 + (ae + bd)x^2 + (be + cd)x + ce. \end{aligned}$$

Equating coefficients gives
$$ad = 15, \qquad ae + bd = 7, \qquad be + cd = -8, \qquad \text{and} \qquad ce = -27.$$

Now since $ad = 15$ and $ce = -27$ and 15 and -27 are both odd integers, then a, d, c, and e are all odd *[because by exercise 42 if one of these integers were even, its product with any other integer would also be even]*. If b were also odd then because a, e, and d are odd, bd and ae would also be odd (by exercise 39) and so $ae + bd$ would be even (by exercise 27). But this is impossible because $ae + bd = 7$, which is odd. Hence b must be even. It follows that be must also be even and cd must be odd, and so $be + cd$ must be odd (by exercise 19). But this is impossible because $be + cd = -8$, which is even. Hence no such integers a, b, c, d, and e can be found. In other words, the polynomial $15x^3 + 7x^2 - 8x - 27$ cannot be factored over the integers. *[Note: The type of reasoning used in this solution is called argument by contradiction. It is introduced formally in Section 3.6.]*

Section 3.2

2. $4.6037 = 46037/10000$

5. Let $x = 0.565656\ldots$. Then $100x = 56.565656\ldots$, and so $100x - x = 99x = 56$. Hence $x = 56/99$.

7. Let $x = 52.4672167216721\ldots$. Then

$$100000x = 5246721.67216721\ldots \quad \text{and} \quad 10x = 524.672167216721\ldots,$$

and so $100000x - 10x = 99990x = 5246721 - 524 = 5246197$. Hence $x = 5246197/99990$.

8. *a.* $\forall$ real numbers x and y, if $xy = 0$ then $x = 0$ or $y = 0$.

   c. If neither of two real numbers is zero, then their product is nonzero.

10. Because m and n are integers, $5m + 12n$ and $4n$ are both integers (since products and sums of integers are integers). Also by the zero product property, $4n \neq 0$ because $4 \neq 0$ and $n \neq 0$. Hence $(5m+12n)/4n$ is a quotient of integers with a nonzero denominator, and so it is rational.

14. This statement is false.

    Counterexample: Both 1 and 0 are rational numbers (by exercise 11) but $1/0$ is not a rational number (because it is not even a number since division by 0 is not defined).

    Modified Statement: The quotient of any rational number and any nonzero rational number is rational.

    Proof of Modified Statement: Suppose r and s are *[particular but arbitrarily chosen]* rational numbers with $s \neq 0$. By definition of rational, $r = a/b$ and $s = c/d$ for some integers a, b, c, and d with $b \neq 0$ and $d \neq 0$. Furthermore, $c \neq 0$ because $c = sd$ and neither s nor d equals 0. By substitution and the laws of algebra,

$$\frac{r}{s} = \frac{\dfrac{a}{b}}{\dfrac{c}{d}} = \frac{a}{b} \cdot \frac{d}{c} = \frac{ad}{bc}.$$

    Now ad and bc are integers because a, b, c, and d are integers and products of integers are integers. Also $bc \neq 0$ by the zero product property because $b \neq 0$ and $c \neq 0$. Thus r/s can be written as a quotient of integers with a nonzero denominator, and so r/s is rational.

15. This statement is true. *Proof:* Suppose r and s are *[particular but arbitrarily chosen]* rational numbers. *[We must show that $r - s$ is rational.]* By definition of rational, $r = a/b$ and $s = c/d$ for some integers a, b, c, and d with $b \neq 0$ and $d \neq 0$. Then by substitution and the laws of algebra, $r - s = a/b - c/d = (ad - bc)/bd$. But $ad - bc$ and bd are both integers because a, b, c, and d are integers and products and differences of integers are integers and $bd \neq 0$ by the zero product property. Hence $r - s$ is a quotient of integers with a nonzero denominator, and so, by definition of rational number, $r - s$ is rational *[as was to be shown]*.

16. This statement is true. *Proof:* Suppose r is a *[particular but arbitrarily chosen]* rational number. By definition of rational, $r = a/b$ for some integers a and b with $b \neq 0$. Then $-r = -(a/b) = (-a)/b$ by substitution and the laws of algebra. But since a is an integer, so is $-a$ (being the product of -1 and a). Hence $-r$ is a quotient of integers with a nonzero denominator, and so $-r$ is rational.

17. This statement is true. *Proof:* Suppose r and s are any two distinct rational numbers. By definition of rational, $r = a/b$ and $s = c/d$ for some integers a, b, c, and d with $b \neq 0$ and $d \neq 0$. Then

$$\frac{r+s}{2} = \frac{\dfrac{a}{b} + \dfrac{c}{d}}{2} = \frac{\dfrac{ad+bc}{bd}}{2} = \frac{ad+bc}{2bd}.$$

    Now $ad + bc$ and $2bd$ are integers because a, b, c, and d are integers and products and sums of integers are integers. And $2bd \neq 0$ by the zero product property. Hence $\frac{r+s}{2}$ is a quotient of integers with a nonzero denominator, and so $\frac{r+s}{2}$ is rational.

18. This statement is true. *Proof.* Suppose a and b are any real numbers with $a < b$. By properties T18 and T19 in Appendix A, we may add b to both sides to obtain $(a + b) < 2b$, and we may divide both sides by 2 to obtain $(a + b)/2 < b$. Similarly, since $a < b$, we may add a to both sides, which gives $2a < (a + b)$, and we may divide both sides by 2, which gives $a < (a + b)/2$. By combining the inequalities, we have $a < (a + b)/2 < b$.

19. *Proof.* Suppose r and s are any two distinct rational numbers with $r < s$. Let $x = \frac{r+s}{2}$. By the result of exercise 17, x is rational, and by the result of exercise 18, $r < x < s$. So there exists another rational number between r and s.

21. True. *Proof.* Suppose a is any odd integer. Then $a^2 = a \cdot a$ is a product of odd integers and hence is odd by property 3. Therefore, $a^2 + a$ is a sum of odd integers and thus even by property 2.

22. True. *Proof.* Suppose k is any even integer and m is any odd integer. By property 1, $k + 2$ is even because it is a sum of even integers, and thus also by property 1, $(k + 2)^2$ is even because it is a product of even integers. By property 2, $m - 1$ is even because it is a difference of odd integers, and thus also by property 1, $(m - 1)^2$ is even because it is a product of even integers. Finally, by property 1, $(k + 2)^2 - (m - 1)^2$ is even because it is a difference of even integers.

24. *Proof.* Suppose r is any rational number. Then $r^2 = r \cdot r$ is a product of rational numbers and hence is rational by exercise 12 (or by the solution to exercise 13). Also 2 and 3, which are integers, are rational by exercise 11. Thus both $3r^2$ and $2r$ are rational by the solution to exercise 13 (because they are products of rational numbers), and by the solution to exercise 15, $3r^2 - 2r$ is rational (because it is a difference of two rational numbers). Finally, 4, which is an integer, is rational by exercise 11. So by Theorem 3.2.2, $3r^2 - 2r + 4 = (3r^2 - 2r) + 4$ is rational. (because it is a sum of two rational numbers).

25. *Proof.* Suppose s is any rational number. Then s^2 is the square of a rational number and hence is rational by exercise 12. Thus $s^3 = s^2 \cdot s$ is also rational because it is a product of rational numbers (solution to exercise 13). Now 5 and 8, which are integers, are rational by exercise 11. Thus both $5s^3$ and $8s^2$ are products of rational numbers and hence are rational (by the solution to exercise 13). Therefore, $5s^3 + 8s^2$ is a sum of two rational numbers and is therefore rational (by Theorem 3.2.2). Finally, 7, which is an integer, is rational by exercise 11. So $5s^3 + 8s^2 - 7 = (5s^3 + 8s^2) - 7$ is a difference of two rational numbers, and so it is rational (by the solution to exercise 15).

27. Yes. Since $\dfrac{ax + b}{cx + d} = 1$, then $ax + b = cx + d$, and so $ax - cx = d - b$, or, equivalently, $(a - c)x = d - b$. Thus $x = (d - b)/(a - c)$. Now $d - b$ and $a - c$ are integers because a, b, c, and d are integers and differences of integers are integers. Also $a - c \neq 0$ because it is given that $a \neq c$. Thus x can be written as a quotient of integers with a nonzero denominator, and so x is rational.

28. Yes.

Suppose a, b, and c are integers and x, y, and z are nonzero real numbers, where

$$a = \frac{xy}{x + y} \quad \text{and} \quad b = \frac{zx}{z + x} \quad \text{and} \quad c = \frac{yz}{y + z}.$$

Note that because a, b, and c are real numbers, none of the denominators $x + y$, or $z + x$ or $y + z$ can equal zero. *[Our strategy will be to express x in terms of the integers a, b, and c in hopes of showing that x can be written as a ratio of integers with a nonzero denominator.]* First observe that, by the zero product property,

$$
\begin{aligned}
a \neq 0 \quad &\text{because (1) } xy = a(x + y) \text{ and } xy \neq 0 \\
b \neq 0 \quad &\text{because (2) } zx = b(z + x) \text{ and } zx \neq 0 \\
c \neq 0 \quad &\text{because (3) } yz = c(y + z) \text{ and } yz \neq 0.
\end{aligned}
$$

i. Solve equation (1) for y in terms of a and x:

$$xy = a(x + y) \quad \Leftrightarrow \quad xy = ax + ay \quad \Leftrightarrow \quad xy - ay = ax \quad \Leftrightarrow \quad (x - a)y = ax.$$

Now because ax is a product of nonzero real numbers, $ax \neq 0$, and so $(x - a) \neq 0$. Thus we may divide by $x - a$ to obtain

$$y = \frac{ax}{x - a}.$$

ii. Similarly, solve equation (2) for z in terms of b and x:

$$zx = b(z + x) \quad \Leftrightarrow \quad zx = bz + bx \quad \Leftrightarrow \quad zx - bz = bx \quad \Leftrightarrow \quad (x - b)z = bx.$$

And because bx is a product of nonzero real numbers, $bx \neq 0$. Thus $(x - b) \neq 0$, and we may divide by $x - b$ to obtain

$$z = \frac{bx}{x - b}.$$

iii. Substitute the results of (i) and (ii) into equation (3)

$$\left(\frac{ax}{x - a} \right) \left(\frac{bx}{x - b} \right) = c \left(\frac{ax}{x - a} + \frac{bx}{x - b} \right),$$

and solve for x in terms of a, b, and c by first multiplying both sides by $(x - a)(y - b)$ to obtain

$$(ax)(bx) = cax(x - b) + cbx(x - a).$$

Because $x \neq 0$, both sides may be divided by x to yield

$$abx = cax - cab + cbx - cba,$$

or, equivalently (by putting all the terms involving x on the right-hand side and all the other terms on the left-hand side),

$$2abc = acx + bcx - abx = x(ac + bc - ab).$$

Because $2abc \neq 0$, by the zero product property, $ac + bc - ab$ cannot be zero either. Thus we may divide both sides by $ac + bc - ab$ to obtain

$$x = \frac{2abc}{ac + bc - ab}.$$

Finally, because products and sums of integers are integers, we see that x has been expressed as a ratio of integers with a nonzero denominator.

Note: An alternative and elegant way to solve this exercise is to start with the observation that $\dfrac{1}{a} = \dfrac{x + y}{xy} = \dfrac{1}{x} + \dfrac{1}{y}$, $\dfrac{1}{b} = \dfrac{1}{x} + \dfrac{1}{z}$, and $\dfrac{1}{c} = \dfrac{1}{y} + \dfrac{1}{z}$, and then compute $\dfrac{1}{x} - \dfrac{1}{z}$ and $\dfrac{1}{x} + \dfrac{1}{z}$ and solve for x.

29. Let the quadratic equation be $x^2 + bx + c = 0$ where b and c are rational numbers. Suppose one solution, r, is rational. Call the other solution s. Then $x^2 + bx + c = (x - r)(x - s) = x^2 - (r + s)x + rs$. By equating the coefficients of x, $b = -(r + s)$. Solving for s yields $s = -r - b = -(r + b)$. Because s is the negative of a sum of two rational numbers, s also is rational (by Theorem 3.2.2 and the solution to exercise 16).

31. *Proof:* Suppose c is a real number that is a root of a polynomial $p(x) = r_n x^n + r_{n-1} x^{n-1} + \cdots + r_1 x + r_0$ where n is a nonnegative integer, $r_n \neq 0$, and $r_0, r_1, \ldots, r_n$ are all rational numbers. By definition of rational, there exist integers $a_0, a_1, \ldots, a_n$ and $b_0, b_1, \ldots, b_n$ such

that $r_i = a_i/b_i$ and $b_i \neq 0$ for all integers i with $0 \leq i \leq n$. Since c is a root of $p(x)$, $r_n c^n + r_{n-1} c^{n-1} + \cdots + r_1 c + r_0 = 0$. By substitution,

$$(*) \qquad \frac{a_n}{b_n} \cdot c^n + \frac{a_{n-1}}{b_{n-1}} \cdot c^{n-1} + \cdots + \frac{a_1}{b_1} \cdot c + \frac{a_0}{b_0} = 0.$$

For each $i = 0, 1, 2, \ldots, n$, let m_i be the product of a_i and all the b_j except b_i. Then each m_i is an integer (being a product of integers). Multiplying both sides of (*) by $b_0 b_1 \cdots b_n$ gives $m_n c^n + m_{n-1} c^{n-1} + \cdots + m_1 c + m_0 = 0$. Hence c satisfies the equation $m_n x^n + m_{n-1} x^{n-1} + \cdots + m_1 x + m_0 = 0$ where $m_0, m_1, \ldots, m_n$ are all integers. Thus c satisfies a polynomial with integer coefficients.

32. This incorrect proof just shows the theorem to be true in the one case where one of the rational numbers is 1/4 and the other is 1/2. It is an example of the mistake of arguing from examples, which is discussed on page 135. A correct proof must show the theorem is true for *any* two rational numbers.

35. The fourth sentence claims that $r + s$ is a fraction because it is a sum of two fractions. But the statement that the sum of two fractions is a fraction is a restatement of what is to be proved. Hence this proof begs the question by assuming what is to be proved.

36. This incorrect proof begs the question. The second sentence asserts that a certain conclusion follows if $r + s$ is rational, and the rest of the proof uses that conclusion to deduce that $r + s$ is rational. Thus this incorrect proof assumes what is to be proved.

Section 3.3

2. Yes: $54 = 18 \cdot 3$.

3. Yes: $0 = 0 \cdot 5$.

5. Yes: $6m(2m + 10) = 4[3m(m + 5)]$ and $3m(m + 5)$ is an integer because m is an integer and sums and products of integers are integers.

9. Yes: $2a \cdot 34b = 4(17ab)$ and $17ab$ is an integer because a and b are integers and sums and products of integers are integers.

11. No: $73/13$ is not an integer. $(73/13 \cong 5.6)$

13. Yes: $n^2 - 1 = (4k + 3)^2 - 1 = (16k^2 + 24k + 9) - 1 = 16k^2 + 24k + 8 = 8(2k^2 + 3k + 1)$, and $2k^2 + 3k + 1$ is an integer because k is an integer and sums and products of integers are integers.

16. *Proof:* Suppose a, b, and c are integers and $a \mid b$ and $a \mid c$. *[We must show that $a \mid (b - c)$.]* By definition of divisibility, there exist integers r and s such that $b = ar$ and $c = as$. Then $b - c = ar - as = a(r - s)$ by substitution and the distributive law. But $r - s$ is an integer since it is a difference of two integers. Hence $a \mid (b - c)$ *[as was to be shown]*.

18. *Proof:* Let m and n be any two even integers. By definition of even, $m = 2r$ and $n = 2s$ for some integers r and s. Then $mn = (2r)(2s) = 4(rs)$. Since rs is an integer (being a product of integers), mn is a multiple of 4 (by definition of divisibility).

20. We must show that for all integers n, if n is divisible by 16 then n is divisible by 8.

    Proof: Let n be any integer that is divisible by 16. By definition of divisibility, $n = 16k$ for some integer k. Factoring out an 8 gives $n = 16k = 8(2k)$. Let $t = 2k$. Then t is an integer because it is a product of integers. So $n = 8t$ for some integer t, and hence, by definition of divisibility, n is divisible by 8.

22. *Proof:* Suppose a, b, and c are any integers such that $ab \mid c$. By definition of divisibility, $c = r(ab)$ for some integer r. Regrouping shows that $c = (ra)b$ and $c = (rb)a$. Now both ra and rb are integers because they are products of integers. Thus $c = $ (an integer) $\cdot b$ and $c = $ (an integer) $\cdot a$. It follows by definition of divisibility that $a \mid c$ and $b \mid c$.

24. *Counterexample:* Let $a = 2$, $b = 3$, and $c = 1$. Then $a \mid (b + c)$ because $2 \mid 4$ but $a \nmid b$ because $2 \nmid 3$ and $a \nmid c$ because $2 \nmid 1$.

25. *Counterexample:* Let $a = 6$, $b = 2$, and $c = 3$. Then $a \mid bc$ because $6 \mid 6$ but $a \nmid b$ and $a \nmid c$ because $6 \nmid 2$ and $6 \nmid 3$.

26. *Proof:* Let a and b be integers such that $a \mid b$. By definition of divisibility, $b = ak$ for some integer k. Squaring both sides of this equation gives $b^2 = (ak)^2 = a^2 k^2$. But k^2 is an integer (being a product of the integer k times itself). Hence by definition of divisibility, $a^2 \mid b^2$.

27. *Counterexample:* Let $a = 4$ and $n = 6$. Then $a \mid n^2$ and $a \leq n$ because $4 \mid 36$ and $4 \leq 6$, but $a \nmid n$ because $4 \nmid 6$.

28. *Counterexample:* Let $a = 25$ and $b = 5$. Then $a \mid 10b$ because $25 \mid 50$ but $a \nmid b$ because $25 \nmid 5$.

30. No. The values of nickels, dimes, and quarters are all multiples of 5. By exercise 15, a sum of numbers divisible by 5 is also divisible by 5. So since \$4.72 is not a multiple of 5, \$4.72 cannot be obtained using only nickels, dimes, and quarters.

31. No. If it were possible to obtain \$3 with 50 coins that are pennies, dimes, and quarters, then we could let p, d, and q be the number of pennies, dimes, and quarters, respectively, that could be used to obtain \$3. Note that p, d, and q are integers, and $q + d + p = 50$. Solving for p gives $p = 50 - q - d$. Since the coins add up to \$3, $25q + 10d + p = 300$. Substituting the value of p gives $25q + 10d + (50 - q - d) = 300$. After simplifying, we have $24q + 9d = 250$. Factoring out a 3 from the left-hand side gives $3(8q + 3d) = 250$. Now because q and d are integers, so is $8q + 3d$, and thus, by definition of divisibility, the left-hand side of the equation is divisible by 3; hence the right-hand side should also be divisible by 3. But 250 is not divisible by 3, which means that this situation described in the exercise cannot occur. In other words, it is not possible to obtain \$3 with 50 pennies, nickels, and dimes. *[Note: The form of reasoning used in this answer is called argument by contradiction. It is discussed formally in Section 3.6.]*

32. Let n be the number of minutes past 4 p.m. when the athletes first return to the start together. Then n is the smallest multiple of 8 that is also a multiple of 10. This number is 40. Hence the first time the athletes will return to the start together will be 4:40 p.m.

33. *b.* Let $N = 12,858,306,120,312$. The sum of the digits of N is 42, which is divisible by 3 but not by 9. Therefore, N is divisible by 3 but not by 9. The right-most digit of N is neither 5 nor 0, and so N is not divisible by 5. The two right-most digits of N are 12, which is divisible by 4. Therefore, N is divisible by 4.

   c. Let $N = 517,924,440,926,512$. The sum of the digits of N is 61, which is not divisible by 3 (and hence not by 9 either). Therefore, N is not divisible either by 3 or by 9. The right-most digit of N is neither 5 nor 0, and so N is not divisible by 5. The two right-most digits of N are 12, which is divisible by 4. Therefore, N is divisible by 4.

   d. Let $N = 14,328,083,360,232$. The sum of the digits of N is 45, which is divisible by 9 and hence also by 3. Therefore, N is divisible by 9 and by 3. The right-most digit of N is neither 5 nor 0, and so N is not divisible by 5. The two right-most digits of N are 32, which is divisible by 4. Therefore, N is divisible by 4.

34. *b.* $5733 = 3^2 \cdot 7^2 \cdot 13$ *c.* $3675 = 3 \cdot 5^2 \cdot 7^2$

35. *c.* $m = 3 \cdot 7 \cdot 11$

product $= 2^2 \cdot 3^5 \cdot 7 \cdot 11^2 \cdot m = 2^2 \cdot 3^6 \cdot 7^2 \cdot 11^2 = (2 \cdot 3^3 \cdot 7 \cdot 11)^2 = 4158^2$

36. *a.* $p_1^{3e_1} \cdot p_2^{3e_2} \cdots p_k^{3e_k}$

b. $k = 2^2 \cdot 3 \cdot 7^2 \cdot 11$

product $= 2^4 \cdot 3^5 \cdot 7 \cdot 11^2 \cdot k = 2^6 \cdot 3^6 \cdot 7^3 \cdot 11^3 = (2^2 \cdot 3^2 \cdot 7 \cdot 11)^3 = 2772^3$

37. *b.* Yes, $10 \mid y$. The reason is that both 2 and 5 are prime factors of $10x$, and so by the unique factorization theorem, these numbers must occur in the prime factorization for $9y$, and since neither 2 nor 5 are factors of 9, they must occur in the prime factorization of y. Similarly, $9 \mid x$ because the prime number 3 occurs at least twice in the prime factorization of $9y$, and so by the unique factorization theorem, both factors of 3 must occur in the prime factorization for $10x$, and since 3 is not a factors of 10, both 3's must occur in the prime factorization of x.

38. Note that $45^8 \cdot 88^5 = (3^2 \cdot 5)^8 \cdot (2^3 \cdot 11)^5 = (3^{16} \cdot 5^8) \cdot (2^{15} \cdot 11^5) = 2^{15} \cdot 3^{16} \cdot 5^8 \cdot 11^5$. When this number is written in ordinary decimal form, each 0 at its end comes from a factor of 10, or one factor of 2 and one factor of 5. Since there are at least eight factors of 2 but only eight factors of 5, there are exactly eight factors of 10 in the number. This implies that the number will end with 8 zeroes.

39. *b.*

$$20! = 20 \cdot 19 \cdot 18 \cdot 17 \cdot 16 \cdot 15 \cdot 14 \cdot 13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$$
$$= 2^2 \cdot 5 \cdot 19 \cdot 2 \cdot 3^2 \cdot 17 \cdot 2^4 \cdot 3 \cdot 5 \cdot 2 \cdot 7 \cdot 13 \cdot 2^2 \cdot 3 \cdot 11 \cdot 2 \cdot 5 \cdot 3^2 \cdot 2^3 \cdot 7 \cdot 2 \cdot 3 \cdot 5 \cdot 2^2 \cdot 3 \cdot 2$$
$$= 2^{18} \cdot 3^8 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19$$

c. Squaring the result of part (b) gives

$$
\begin{aligned}
(20!)^2 &= (2^{18} \cdot 3^8 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19)^2 \\
&= 2^{36} \cdot 3^{16} \cdot 5^8 \cdot 7^4 \cdot 11^2 \cdot 13^2 \cdot 17^2 \cdot 19^2
\end{aligned}
$$

When $(20!)^2$ is written in ordinary decimal form, there are as many zeros at the end of it as there are factors of the form $2 \cdot 5$ $(= 10)$ in its prime factorization. Thus, since the prime factorization of $(20!)^2$ contains eight 5's and more than eight 2's, $(20!)^2$ contains eight factors of 10 and hence eight zeros.

40. Let $m =$ the number of adult men in the town, and let $w =$ the number of adult women in the town. Then $m \geq 100$ and $\frac{2}{3}m = \frac{3}{5}w$. Cross-multiplying gives $10m = 9w$. Thus $9 \mid 10m$, and so, by the unique factorization theorem, $9 \mid m$. The least possible number of adult men in the town is, therefore, the least multiple of 9 that is greater than 100, namely $m = 108$. Given that $10m = 9w$, we have $w = \frac{10}{9}m = \frac{10}{9} \cdot 108 = 120$. So there are 108 adult men and 120 adult women in the town.

42. *Proof:* Suppose n is a nonnegative integer whose decimal representation ends in 5. By the hint for exercise 41, $n = 10m + 5$ for some integer m. By factoring out a 5, $n = 10m + 5 = 5(2m + 1)$, and $2m + 1$ is an integer since m is an integer. Hence n is divisible by 5.

43. *Proof:* Suppose the decimal representation of a nonnegative integer n ends in $d_1 d_0$. We first show that $n = 100s + 10d_1 + d_0$, for some integer s. By definition of decimal representation, $n = d_k 10^k + d_{k-1} 10^{k-1} + \cdots + d_2 10^2 + d_1 10 + d_0$ where k is a nonnegative integer and all the d_i are integers from 0 to 9 inclusive.

Case 1 (0 $\leq k < 2$): In this case, $n = d_1 10 + d_0$, and we may let $s = 0$. Then $n = 100s + 10d_1 + d_0$. *[Note that in this case we allow the possibility that either or both of d_1 and d_0 may be zero.]*

Case 2 ($k \geq 2$): In this case, $k - 2 \geq 0$. Factoring out a 100 from all but the two right-most terms of n and using the laws of exponents gives $n = 100(d_k 10^{k-2} + d_{k-1} 10^{k-1} + \cdots + d_2) + 10d_1 + d_0$. Let $s = d_k 10^{k-2} + d_{k-1} 10^{k-1} + \cdots + d_2$. Then s is an integer (being a sum of products of integers) and $n = 100s + 10d_1 + d_0$.

The above argument shows that regardless of whether case 1 or case 2 holds for n, $n = 100s + 10d_1 + d_0$ for some integer s.

Now suppose that $4 \mid (10d_1 + d_0)$. By definition of divisibility, $10d_1 + d_0 = 4r$ for some integer r. Then by substitution, $n = 100s + 4r = 4(25s + r)$. But $25s + r$ is an integer (being a sum of products of integers). Therefore, by definition of divisibility, $4 \mid n$.

44. *Proof:* Suppose n is any nonnegative integer for which the sum of the digits of n is divisible by 9. By definition of decimal representation, n can be written in the form

$n = d_k 10^k + d_{k-1} 10^{k-1} + \cdots + d_2 10^2 + d_1 10 + d_0$ where k is a nonnegative integer and all the d_i are integers from 0 to 9 inclusive. Then

$$
\begin{aligned}
n &= d_k(\underbrace{99\ldots9}_{k\ 9\text{'s}}+1) + d_{k-1}(\underbrace{99\ldots9}_{(k-1)\ 9\text{'s}}+1) + \cdots + d_2(99+1) + d_1(9+1) + d_0 \\
&= d_k \cdot \underbrace{99\ldots9}_{k\ 9\text{'s}} + d_{k-1} \cdot \underbrace{99\ldots9}_{(k-1)\ 9\text{'s}} + \cdots + d_2 \cdot 99 + d_1 \cdot 9 + (d_k + d_{k-1} + \cdots + d_2 + d_1 + d_0) \\
&= d_k \cdot \underbrace{11\ldots1}_{k\ 1\text{'s}} \cdot 9 + d_{k-1} \cdot \underbrace{11\ldots1}_{(k-1)\ 1\text{'s}} \cdot 9 + \cdots + d_2 \cdot 11 \cdot 9 + d_1 \cdot 9 + (d_k + d_{k-1} + \cdots + d_2 + d_1 + d_0) \\
&= 9(d_k \cdot \underbrace{11\ldots1}_{k\ 1\text{'s}} + d_{k-1} \cdot \underbrace{11\ldots1}_{(k-1)\ 1\text{'s}} + \cdots + d_2 \cdot 11 + d_1) + (d_k + d_{k-1} + \cdots + d_2 + d_1 + d_0) \\
&= \text{(an integer divisible by 9)} + \text{(the sum of the digits of } n\text{)}.
\end{aligned}
$$

Since the sum of the digits of n is divisible by 9, n can be written as a sum of two integers each of which is divisible by 9. It follows from exercise 15 that n is divisible by 9.

45. *Proof:* Suppose n is any nonnegative integer for which the sum of the digits of n is divisible by 3. By the same reasoning as in the answer to exercise 44,

$$
\begin{aligned}
n &= 9(d_k \cdot \underbrace{11\ldots1}_{k\ 1\text{'s}} + d_{k-1} \cdot \underbrace{11\ldots1}_{(k-1)\ 1\text{'s}} + \cdots + d_2 \cdot 11 + d_1) + (d_k + d_{k-1} + \cdots + d_2 + d_1 + d_0) \\
&= 3[3(d_k \cdot \underbrace{11\ldots1}_{k\ 1\text{'s}} + d_{k-1} \cdot \underbrace{11\ldots1}_{(k-1)\ 1\text{'s}} + \cdots + d_2 \cdot 11 + d_1)] + (d_k + d_{k-1} + \cdots + d_2 + d_1 + d_0) \\
&= \text{(an integer divisible by 3)} + \text{(the sum of the digits of } n\text{)}.
\end{aligned}
$$

Since the sum of the digits of n is divisible by 3, n can be written as a sum of two integers each of which is divisible by 3. It follows from exercise 15 that n is divisible by 3.

46. What follows is a rather formal justification for the given statement that uses only the mathematics developed in this chapter. A student might appropriately give a much less formal partial justification.

Lemma: For all nonnegative integers r, if r is even then $10^r - 1$ is divisible by 11, and if r is odd then $10^r + 1$ is divisible by 11.

Proof: Suppose r is a nonnegative even integer. If $r = 0$, then $10^r - 1 = 10^0 - 1 = 1 - 1 = 0$, which is divisible by 11 because $0 = 11 \cdot 0$. If $r \geq 2$, then

$$
\begin{aligned}
&11 \cdot [9(10^{r-2} + 10^{r-4} + 10^{r-6} + \cdots + 10^2 + 1)] \\
&= (10+1)[(10-1)(10^{r-2} + 10^{r-4} + 10^{r-6} + \cdots + 10^2 + 1)] \\
&= (10^2 - 1)(10^{r-2} + 10^{r-4} + 10^{r-6} + \cdots + 10^2 + 1) \\
&= (10^r - 10^{r-2}) + (10^{r-2} - 10^{r-4}) + (10^{r-4} - 10^{r-6}) + \cdots + ((10^4 - 10^2) + (10^2 - 1)) \\
&= 10^r - 1.
\end{aligned}
$$

Hence if r is even, then $10^r - 1$ is divisible by 11.

Suppose r is an odd integer. If $r = 1$, then $10^r + 1 = 10^1 + 1 = 10 + 1 = 11$ So $11 \mid (10^r + 1)$ because $11 = 11 \cdot 1$. If $r \geq 3$, then $r - 2 \geq 1$ and

$$11 \cdot [9 \cdot (10^{r-2} + 10^{r-4} + 10^{r-6} + \cdots + 10^3 + 10) + 1]$$

$$= (10+1)[(10-1)(10^{r-2} + 10^{r-4} + 10^{r-6} + \cdots + 10^3 + 10) + 1]$$

$$= (10^2 - 1)(10^{r-2} + 10^{r-4} + 10^{r-6} + \cdots + 10^3 + 10) + (10+1)$$

$$= (10^r - 10^{r-2}) + (10^{r-2} - 10^{r-4}) + (10^{r-4} - 10^{r-6}) + \cdots + ((10^5 - 10^3) + (10^3 - 10) + (10+1)$$

$$= 10^r + 1.$$

Hence if r is odd, then $10^r + 1$ is divisible by 11.

Proof of Exercise Statement: Suppose n is any integer for which the alternating sum of the digits is divisible by 11. By definition of decimal representation, n can be written in the form

$$n = d_k 10^k + d_{k-1} 10^{k-1} + \cdots + d_2 10^2 + d_1 10 + d_0$$

where k is a nonnegative integer and all the d_i are integers from 0 to 9 inclusive.

Case 1 (k is even): In this case,

$$n = [d_k(10^k - 1) + d_k] + [d_{k-1}(10^{k-1} + 1) - d_{k-1}] + \cdots + [d_2(10^2 - 1) + d_2] + [d_1(10+1) - d_1] + d_0$$

$$= [d_k(10^k - 1) + d_{k-1}(10^{k-1} + 1) + \cdots + d_2(10^2 - 1) + d_1(10+1)] + [d_0 - d_1 + d_2 - \cdots - d_{k-1} + d_k]$$

Case 2 (k is odd): In this case,

$$n = [d_k(10^k + 1) - d_k] + [d_{k-1}(10^{k-1} - 1) + d_{k-1}] + \cdots + [d_2(10^2 - 1) + d_2] + [d_1(10+1) - d_1] + d_0$$

$$= [d_k(10^k + 1) + d_{k-1}(10^{k-1} - 1) + \cdots + d_2(10^2 - 1) + d_1(10+1)] + [d_0 - d_1 + d_2 - \cdots + d_{k-1} - d_k]$$

Observe that in each case each term of the first bracketed sum is divisible by 11 (by the lemma), and the second bracketed sum is divisible by 11 (by hypothesis). Thus in each case n is divisible by 11.

Section 3.4

2. $q = 8$, $r = 6$

4. $q = 0$, $r = 3$

6. $q = -4$, $r = 5$

8. *a.* 7 *b.* 1

9. *a.* 5 *b.* 3

10. *a.* 15 *b.* 0

11. *b.* When today is Sunday, 7 days from today is Sunday also. Hence *DayN* should be 0. Substituting *DayT* = 0 (Sunday) and $n = 7$ into the formula gives *DayN* = (*DayT* + *N*) *mod* 7 = (0 + 7) *mod* 7 = 0, which agrees.

   c. When today is Thursday, twelve days from today is one week (which is Thursday) plus five days (which is Tuesday). Hence *DayN* should be 2. Substituting *DayT* = 4 (Thursday) and $N = 12$ into the formula gives *DayN* = (*DayT* + *N*) *mod* 7 = (4 + 12) *mod* 7 = 16 *mod* 7 = 2, which agrees.

12. Let the days of the week be numbered from 0 (Sunday) through 6 (Saturday) and let *DayT* and *DayN* be variables representing the day of the week today and the day of the week N days from today. By the quotient-remainder theorem, there exist unique integers q and r such that *DayT* + $N = 7q + r$ and $0 \leq r < 7$. Now *DayT* + N counts the number of days to the day N days from today starting last Sunday (where "last Sunday" is interpreted to mean today if today is a Sunday). Thus *DayN* is the day of the week that is *DayT* + N days from last Sunday. Because each week has seven days, *DayN* is the same as the day of the week *DayT* + $N - 7q$ days from last Sunday. But *DayT* + $N - 7q = r$ and $0 \leq r < 7$. Therefore, *DayN* = r = (*DayT* + N) *mod* 7.

14. *Solution 1*: Note that $1000 = 7 \cdot 142 + 6$. Thus if today is Tuesday, then 1,000 days from today is 142 weeks plus 6 days from today. After 142 weeks, it will again be Tuesday, and 6 days later it will be Monday.

    Solution 2: Use the formula $DayN = (DayT + N) \bmod 7$, letting $DayT = 2$ (Tuesday) and $N = 1000$. Then $DayN = (2 + 1000) \bmod 7 = 1002 \bmod 7 = 1$, which is a Monday.

15. There are 13 leap year days between January 1, 2000 and January 1, 2050 (once every four years in 2000, 2004, 2008, 2012, . . . , 2048). So 13 of the years have 366 days and the remaining 38 years have 365 days. This gives a total of $13 \cdot 366 + 37 \cdot 365 = 18,263$ days between the two dates. Using the formula $DayN = (DayT + N) \bmod 7$, and letting $DayT = 6$ (Saturday) and $N = 18,263$ gives $DayN = (6 + 18263) \bmod 7 = 18269 \bmod 7 = 6$, which is also a Saturday.

16. Suppose n is any negative integer and d is a positive integer, and let q and r be the integers whose existence is guaranteed by the quotient-remainder theorem. In other words, $n = dq + r$ where $0 \leq r < d$. By definition, $n/d = q + 1$ and $n\%d = r - d$. Then, by substitution, $d \cdot n/d + n\%d = d \cdot (q+1) + (r-d) = dq + d + r - d = dq + r = n$, *[as was to be shown]*. In addition, because $0 \leq r < d$, we can subtract d from all parts of the inequality to obtain $0 - d \leq r - d < 0$, or, equivalently, $-d \leq n\%d < 0$. Thus $n\%d$ is negative and does not satisfy the condition $0 \leq n\%d < d$, *[as was also to be shown]*.

18. When b is divided by 12, the remainder is 5. Thus there exists an integer m so that $b = 12m + 5$. Multiplying this equation by 8 gives $8b = 96m + 40 = 96m + 36 + 4 = 12(8m + 3) + 4$. Since $8m + 3$ is an integer and since $0 \leq 4 < 12$, the uniqueness part of the quotient-remainder theorem guarantees that the remainder obtained when $8b$ is divided by 12 is 4.

19. When c is divided by 15, the remainder is 3. Thus there exists an integer k so that $c = 15k + 3$. Multiplying this equation by 10 gives $10c = 10 \cdot 15k + 30 = 15(10k + 2) = 15(10k + 2) + 0$. Since $10k + 2$ is an integer and since $0 \leq 0 < 15$, the uniqueness part of the quotient-remainder theorem guarantees that the remainder obtained when $10c$ is divided by 15 is 0.

21. Recall that (1) *A is a sufficient condition for B* means *if A then B*, and (2) *A is a necessary condition for B* means *if B then A*. Thus proving the given statement requires proving both a (universal) conditional statement and its converse.

    Proof: ($\Rightarrow$) *[We first prove that given any nonnegative integer n and positive integer d, if n is divisible by d, then $n \bmod d = 0$.]* Suppose n is any nonnegative integer and d is any positive integer such that n is divisible by d. By definition of divisibility, $n = dk$ for some integer k. Thus the equation $n = dk + 0$ is true and the inequality $0 \leq 0 < d$ is also true, and so, by the uniqueness part of the quotient-remainder theorem, $n \bmod d = 0$.

    ($\Leftarrow$) *[Second, we prove the converse, namely that given any nonnegative integer n and positive integer d, if $n \bmod d = 0$ then n is divisible by d.]* Suppose n is any nonnegative integer and d is any positive integer such that $n \bmod d = 0$. Then 0 is the remainder obtained when n is divided by d, and thus by the quotient-remainder theorem there exists an integer q such that $n = dq + 0$. But this is equivalent to $n = dq$, and so, by definition of divisibility, n is divisible by d.

22. *b.* a_{ij} is stored in location $7609 + 4(i - 1) + (j - 1)$. Thus $n = 4(i - 1) + (j - 1)$.

    c. To find a formula for r, note that when $0 \leq n < 4$, $r = 1$, when $4 \leq n < 8$, $r = 2$, and when $8 \leq n < 12$, $r = 3$. Dividing these inequalities by 4 gives that when $0 \leq \frac{n}{4} < 1$, $r = 1$, when $1 \leq \frac{n}{4} < 2$, $r = 2$, and when $2 \leq \frac{n}{4} < 3$, $r = 3$. Thus, in each case, $r = \lfloor \frac{n}{4} \rfloor + 1 = n \ div \ 4 + 1$.

    To find a formula for s, note that when $n = 0$, 4, or 8, $s = 1 = 0 + 1$, when $n = 1$, 5, or 9, $s = 2 = 1 + 1$, when $n = 2$, 6, or 10, $s = 3 = 2 + 1$, and when $n = 3$, 7, or 11, $s = 4 = 3 + 1$. Thus, in each case, $s = n \bmod 4 + 1$. So

So $r = n \ div \ 4 + 1$ and $s = n \ mod \ 4 + 1$

Note that, once the floor notation has been introduced, this answer can be checked for consistency with the result of part (b) by using the formulas $a \ mod \ b = a - \lfloor a/b \rfloor b$ and $a \ div \ b = \lfloor a/b \rfloor$:

$$4(r - 1) + (s - 1) = 4[(n \ div \ 4 + 1) - 1] + [(n \ mod \ 4 + 1) - 1]$$
$$= 4 \cdot \left\lfloor \frac{n}{4} \right\rfloor + (n - \left\lfloor \frac{n}{4} \right\rfloor \cdot 4)$$
$$= n$$

23. *Solution 1*: We are given that M is a matrix with m rows and n columns, stored in row major form at locations $N + k$, where $0 \le k < mn$. Given a value for k, we want to find indices r and s so that the entry for M in row r and column s, a_{rs}, is stored in location $N + k$. By the quotient-remainder theorem, $k = nQ + R$, where $0 \le R < n$. The first Q rows of M (each of length n) are stored in the first nQ locations: $N + 0, N + 1, \ldots, N + nQ - 1$ with a_{Qn} stored in the last of these. Consider the next row. When $r = Q + 1$,

a_{r1} will be in location $N + nQ$
a_{r2} will be in location $N + nQ + 1$
a_{r3} will be in location $N + nQ + 2$

$\vdots$

a_{rs} will be in location $N + nQ + (s - 1)$

$\vdots$

and $\quad a_{rn}$ will be in location $N + nQ + (n - 1) = N + n(Q+!) - 1$.

Thus location $N + k$ contains a_{rs} where $r = Q + 1$ and $R = s - 1$. But $Q = k \ div \ n$ and $R = k \ mod \ n$, and hence $r = (k \ div \ n) + 1$ and $s = (k \ mod \ n) + 1$.

Solution 2: [After the floor notation has been introduced, the following solution can be considered as an alternative.] To find a formula for r, note that for $1 \le a \le m$, when $(a - 1)n \le k < an$, $r = a$. Dividing through by n gives that when $(a - 1) \le \frac{k}{n} < a$, or, equivalently, when $\left\lfloor \frac{k}{n} \right\rfloor = a - 1$, $r = a$. But this means that $a = \left\lfloor \frac{k}{n} \right\rfloor + 1 = r$, and since $\left\lfloor \frac{k}{n} \right\rfloor = k \ div \ n$, we have that $r = (k \ div \ n) + 1$.

To find a formula for s, note that when $k = n \cdot$ (an integer) $+ b$ and $0 \le b < n$, then $s = b + 1$. Thus by the quotient-remainder theorem, $s = (k \ mod \ n) + 1$.

24. *Proof*: Consider any two consecutive integers. Call the smaller one n. By the quotient-remainder theorem with $d = 2$, either n is even or n is odd.

Case 1 (n is even): In this case $n = 2k$ for some integer k. Then $n(n + 1) = 2k(2k + 1) = 2[k(2k + 1)]$. But $k(2k + 1)$ is an integer (because products and sums of integers are integers), and so $n(n + 1)$ is even.

Case 2 (n is odd): In this case $n = 2k + 1$ for some integer k. Then

$$n(n + 1) = (2k + 1)[(2k + 1) + 1] = (2k + 1)(2k + 2) = 2[(2k + 1)(k + 1)].$$

But $(2k + 1)(k + 1)$ is an integer (because products and sums of integers are integers), and so $n(n + 1)$ is even.

Hence in either case the product $n(n + 1)$ is even *[as was to be shown]*.

26. *Proof 1 (directly from the definitions)*: Suppose n is any integer. By the quotient-remainder theorem with $n = 2$, n is either even or odd.

Case 1 (n is even): In this case $n = 2k$ for some integer k, and so, by substitution, $n^2 - n + 3 = (2k)^2 - 2k + 3 = 4k^2 - 2k + 2 + 1 = 2(2k^2 - k + 1) + 1$. Let $t = 2k^2 - k + 1$. Then t is an integer

because products, differences, and sums of integers are integers. Hence $n^2 - n + 3 = 2t + 1$ where t is an integer, and so, by definition of odd, $n^2 - n + 3$ is odd.

Case 2 (n is odd): In this case $n = 2k + 1$ for some integer k, and so, by substitution, $n^2 - n + 3 = (2k+1)^2 - (2k+1) + 3 = 4k^2 + 4k + 1 - 2k - 1 + 3 = 4k^2 + 2k + 2 + 1 = 2(2k^2 + 2k + 1) + 1$. Let $t = 2k^2 + 2k + 1$. Then t is an integer because products and sums of integers are integers. Hence $n^2 - n + 3 = 2t + 1$ where t is an integer, and so, by definition of odd, $n^2 - n + 3$ is odd.

Thus in both cases $n^2 - n + 3$ is odd.

Proof 2 (using previously proved results): Suppose n is any integer. Note that $n^2 - n + 3 = (n-1)n + 3$, and that $n - 1$ and n are consecutive integers. By exercise 24, the product of $n - 1$ and n is even. Thus $n^2 - n + 3$ is the sum of the even integer $(n-1)n$ and the odd integer 3, and by Example 3.2.3 #5, this sum is odd.

29. *Proof:* Suppose n is any integer. By the quotient-remainder theorem with $d = 3$, we know that $n = 3q$, or $n = 3q + 1$, or $n = 3q + 2$ for some integer q.

Case 1 (n = 3q for some integer q): In this case, $n^2 = (3q)^2 = 3(3q^2)$. Let $k = 3q^2$. Then k is an integer because it is a product of integers. Hence $n^2 = 3k$ for some integer k.

Case 2 (n = 3q + 1 for some integer q): In this case, $n^2 = (3q+1)^2 = 9q^2 + 6q + 1 = 3(3q^2 + 2q) + 1$. Let $k = 3q^2 + 2q$. Then k is an integer because sums and products of integers are integers. Hence $n^2 = 3k + 1$ for some integer k.

Case 3 (n = 3q + 2 for some integer q): In this case, $n^2 = (3q+2)^2 = 9q^2 + 12q + 4 = 9q^2 + 12q + 3 + 1 = 3(3q^2 + 4q + 1) + 1$. Let $k = 3q^2 + 4q + 1$. Then k is an integer because sums and products of integers are integers. Hence $n^2 = 3k + 1$ for some integer k.

In all three cases, either $n^2 = 3k$ or $n^2 = 3k + 1$ for some integer k *[as was to be shown]*.

30. *Proof:* Suppose n and $n + 1$ are any two consecutive integers. By the quotient-remainder theorem with $d = 3$, we know that $n = 3q$, or $n = 3q + 1$, or $n = 3q + 2$ for some integer q.

Case 1 (n = 3q for some integer q): In this case, $n(n + 1) = 3q(3q + 1) = 3[q(3q + 1)]$. Let $k = q(3q + 1)$. Then k is an integer because sums and products of integers are integers. Hence $n(n + 1) = 3k$ for some integer k.

Case 2 (n = 3q + 1 for some integer q): In this case, $n(n+1) = (3q+1)(3q+2) = 9q^2 + 9q + 2 = 3(3q^2 + 3q) + 2$. Let $k = 3q^2 + 3q$. Then k is an integer because sums and products of integers are integers. Hence $n(n + 1) = 3k + 2$ for some integer k.

Case 3 (n = 3q + 2 for some integer q): In this case, $n(n + 1) = n(3q + 3) = 3[n(q + 1)]$. Let $k = n(q + 1)$. Then k is an integer because sums and products of integers are integers. Hence $n(n + 1) = 3k$ for some integer k.

Thus in all three cases, the product of the two consecutive integers either equals $3k$ or it equals $3k + 2$ for some integer k *[as was to be shown]*.

31. *a. Proof 1:* Suppose m and n are integers.

Case 1 (both m and n are even): In this case both $m + n$ and $m - n$ are even (by Example 3.2.3 #1).

Case 2 (one of m and n is even and the other is odd): In this case both $m + n$ and $m - n$ are odd (by Example 3.2.3 #5 and #7).

Case 3 (both m and n are odd): In this case both $m + n$ and $m - n$ are even (by Example 3.2.3 #2).

Thus in all three possible cases, either both $m + n$ and $m - n$ are even or both $m + n$ and $m - n$ are odd *[as was to be shown]*.

Proof 2: Suppose m and n are integers.

Case 1 (m − n is even): In this case, $m + n = (m - n) + 2n$, and so $m + n$ is a sum of two even integers and is therefore even by by Example 3.2.3 #1.

Case 2 (m − n is odd): In this case also, $m + n = (m - n) + 2n$. Hence $m + n$ is the sum of an odd integer and an even integer, and is therefore odd by by Example 3.2.3 #5.

Now either $m - n$ is even or $m - n$ is odd *[by the quotient-remainder theorem]*, and thus either case 1 or case 2 must apply. In each case, $m - n$ and $m + n$ are either both even or both odd *[as was to be shown].*

c. If $m^2 - n^2 = 88$, then $88 = (m + n)(m - n)$. Now $88 = 2^3 \cdot 11$, and by the unique factorization theorem this factorization is unique up to the order in which the factors are written down. It follows that the only representations of 40 as a product of two positive integers are $88 = 88 \cdot 1 = 8 \cdot 11 = 4 \cdot 22 = 2 \cdot 44$. By part (a), m and n must both be odd or both be even. Thus the only solutions are either $m + n = 22$ and $m - n = 4$ or $m + n = 44$ and $m - n = 2$. This gives either $m = 13$ and $n = 9$ or $m = 23$ and $n = 21$.

33. *Proof:* Suppose a, b, and c are any integers such that $a - b$ is odd and $b - c$ is even. Then $(a - b) + (b - c)$ is a sum of an odd integer and an even integer and hence is odd (by Example 3.2.3 #5). But $(a - b) + (b - c) = a - c$, and thus $a - c$ is odd.

34. *Proof:* Suppose n is any integer with $n > 3$. By the quotient-remainder theorem with $d = 3$, we know that $n = 3q$, or $n = 3q + 1$, or $n = 3q + 2$ for some integer q. Note that because n is greater than 3, q is greater than 1 or $q = 1$ and $n = 4$ or 5.

Case 1 (q = 1 and n = 4): In this case, n is not prime because $4 = 2 \cdot 2$.

Case 2 (q = 1 and n = 5): In this case, $n + 4 = 9 = 3 \cdot 3$, and so $n + 4$ is not prime.

Case 3 (q > 1 and n = 3q): In this case, n is not prime because it is a product of 3 and q and both 3 and q are greater than 1.

Case 4 (q > 1 and n = 3q + 1): In this case, $n + 2 = (3q + 1) + 2 = 3q + 3 = 3(q + 1)$. So $n + 2$ is not prime because it is a product of 3 and $q + 1$ and both 3 and $q + 1$ are greater than 1.

Case 5 (q > 1 and n = 3q + 2): In this case, $n + 4 = (3q + 2) + 4 = 3q + 6 = 3(q + 2)$. So $n + 4$ is not prime because it is a product of 3 and $q + 2$ and both 3 and $q + 2$ are greater than 1.

Hence in all five cases, at least one of n or $n + 2$ or $n + 4$ is not prime.

35. *Proof:* Suppose n is any integer. By the quotient-remainder theorem with $d = 2$, n is either even or odd.

Case 1 (n is even): In this case $n = 2q$ for some integer q, and so, by substitution, $n^4 = (2q)^4 = 16q^4 = 8(2q^4)$. Let $m = 2q^4$. Then m is an integer because it is a product of integers. Hence $n^4 = 8m$ where m is an integer.

Case 2 (n is odd): In this case $n = 2q + 1$ for some integer q, and so, by substitution, $n^4 = (2q + 1)^4 = (2q + 1)^2(2q + 1)^2 = (4q^2 + 4q + 1)(4q^2 + 4q + 1) = 16q^4 + 16q^3 + 4q^2 + 16q^3 + 16q^2 + 4q + 4q^2 + 4q + 1 = 16q^4 + 32q^3 + 24q^2 + 8q + 1 = 8(2q^4 + 4q^3 + 3q^2 + q) + 1$. Let $m = 2q^4 + 4q^3 + 3q^2 + q$. Then m is an integer because products and sums of integers are integers. Hence $n^4 = 8m + 1$ where m is an integer.

Thus in both cases $n^4 = 8m$ or $n^4 = 8m + 1$ for some integer m.

Note: If Theorem 3.4.3 is used, it can be shown that for any integer n, $n^4 = 16m$ or $n^4 = 16m + 1$ for some integer m. See the solution to exercise 43 for a partial proof of this result.

36. *Proof:* Suppose n is any integer. *[We must show that $8 \mid n(n + 1)(n + 2)(n + 3)$.]* By the quotient-remainder theorem with $d = 4$, $n = 4k$ or $n = 4k + 1$ or $n = 4k + 2$ or $n = 4k + 3$ for some integer k.

Case 1 (n = 4k for some integer k): In this case,

$$n(n + 1)(n + 2)(n + 3) = 4k(4k + 1)(4k + 2)(4k + 3) = 8[k(4k + 1)(2k + 1)(4k + 3)],$$

which is divisible by 8 (because k is an integer and sums and products of integers are integers).

Case 2 (n = 4k + 1 for some integer k): In this case,

$$n(n+1)(n+2)(n+3) = (4k+1)(4k+2)(4k+3)(4k+4) = 8[(4k+1)(2k+1)(4k+3)(k+1)],$$

which is divisible by 8 (because k is an integer and sums and products of integers are integers).

Case 3 (n = 4k + 2 for some integer k): In this case,

$$n(n+1)(n+2)(n+3) = (4k+2)(4k+3)(4k+4)(4k+5) = 8[(2k+1)(4k+3)(k+1)(4k+5)],$$

which is divisible by 8 (because k is an integer and sums and products of integers are integers).

Case 4 (n = 4k + 3 for some integer k): In this case,

$$n(n+1)(n+2)(n+3) = (4k+3)(4k+4)(4k+5)(4k+6) = 8[(4k+3)(k+1)(4k+5)(2k+3)],$$

which is divisible by 8 (because k is an integer and sums and products of integers are integers).
Hence in all four possible cases, $8 \mid n(n+1)(n+2)(n+3)$ *[as was to be shown]*.

37. *Proof:* Let n be any integer. *[We must show that $n^2 = 4k$ or $n^2 = 4k + 1$ for some integer k.]* By the quotient-remainder theorem, $n = 4q$ or $n = 4q+1$ or $n = 4q+2$ or $n = 4q+3$ for some integer q.

Case 1 (n = 4q for some integer q): In this case, $n^2 = (4q)^2 = 4(4q^2)$. Let $k = 4q^2$. Then k is an integer because it is a product of integers. Hence $n^2 = 4k$ for some integer k.

Case 2 (n = 4q + 1 for some integer q): In this case, $n^2 = (4q+1)^2 = 16q^2 + 8q + 1 = 4(4q^2 + 2q) + 1$. Let $k = 4q^2 + 2q$. Then k is an integer because it is a sum of products of integers. Hence $n^2 = 4k + 1$ for some integer k.

Case 3 (n = 4q + 2 for some integer q): In this case, $n^2 = (4q + 2)^2 = 16q^2 + 16q + 4 = 4(4q^2 + 4q + 1)$. Let $k = 4q^2 + 4q + 1$. Then k is an integer because it is a sum of products of integers. Hence $n^2 = 4k$ for some integer k.

Case 4 (n = 4q + 3 for some integer q): In this case, $n^2 = (4q + 3)^2 = 16q^2 + 24q + 9 = 16q^2 + 24q + 8 + 1 = 4(4q^2 + 6q + 2) + 1$. Let $k = 4q^2 + 6q + 2$. Then k is an integer because it is a sum of products of integers. Hence $n^2 = 4k + 1$ for some integer k.

It follows that in all four possible cases, $n^2 = 4k$ or $n^2 = 4k + 1$ for some integer k *[as was to be shown]*.

38. *Solution 1:* This result can be proved directly by dividing into four cases as is done in the proof for exercise 37. If exercise 37 was previously solved, however, the result of exercise 38 can be deduced as follows.

Proof: Let n be any integer. By the result of exercise 37, $n^2 = 4k$ or $n^2 = 4k + 1$ for some integer k. Hence $n^2 + 1 = 4k + 1$ or $n^2 + 1 = 4k + 2$ for some integer k.

Solution 2: An alternative proof uses Theorem 3.4.3.

Proof: Let n be any integer. By the parity property, n is either even or odd.

Case 1(n is even): In this case, $n = 2q$ for some integer q, and so $n^2 + 1 = (2q)^2 + 1 = 4q^2 + 1$. Let $k = q^2$. Then k is an integer because it is a product of integers, and thus $n^2 + 1$ has the form $4k + 1$ for some integer k.

Case 2(n is odd): In this case, by Theorem 3.4.3, there is an integer m such that $n^2 + 1 = (8m + 1) + 1 = 4(2m) + 2$. Let $k = 2m$. Then k is an integer because it is a product of integers, and thus $n^2 + 1$ has the form $4k + 2$ for some integer k.

39. *Proof:* Consider any four consecutive integers. Call the smallest n. Then the sum of the four integers is $n + (n + 1) + (n + 2) + (n + 3) = 4n + 6 = 4(n + 1) + 2$. Let $k = n + 1$. Then k is an integer because it is a sum of integers. Hence n can be written in the required form.

40. *Proof:* Let n be any integer and observe that $n(n^2-1)(n+2) = (n-1)n(n+1)(n+2)$, which is a product of four consecutive integers. By exercise 36, this product is divisible by 8, and hence by transitivity of divisibility (Theorem 3.3.1) the product is divisible by 4 *[as was to be shown].* *Note:* The statement can also be proved directly without using exercise 36 by dividing into four cases as is done in the proof for exercise 36. It can also be proved by using Theorem 3.4.3 and dividing into two cases as was done in the proof given in Solution 2 for exercise 38.

41. *Proof:* Let m be any integer. *[We must show that $m^2 = 5k$ or $m^2 = 5k+1$, or $m^2 = 5k+4$ for some integer k.]* By the quotient-remainder theorem, $m = 5q$ or $m = 5q + 1$ or $m = 5q + 2$, or $m = 5q + 3$, or $m = 5q + 4$ for some integer q.

Case 1 ($m = 5q$ for some integer q): In this case, $m^2 = (5q)^2 = 5(5q^2)$. Let $k = 5q^2$. Then k is an integer because it is a product of integers, and hence $m^2 = 5k$ for some integer k.

Case 2 ($m = 5q + 1$ for some integer q): In this case, $m^2 = (5q + 1)^2 = 25q^2 + 10q + 1 = 5(5q^2 + 2q) + 1$. Let $k = 5q^2 + 2q$. Then k is an integer because it is a sum of products of integers, and hence $m^2 = 5k + 1$ for some integer k.

Case 3 ($m = 5q + 2$ for some integer q): In this case, $m^2 = (5q + 2)^2 = 25q^2 + 20q + 4 = 5(5q^2 + 4q) + 4$. Let $k = 5q^2 + 4q$. Then k is an integer because it is a sum of products of integers, and hence $m^2 = 5k + 4$ for some integer k.

Case 4 ($m = 5q + 3$ for some integer q): In this case, $m^2 = (5q + 3)^2 = 25q^2 + 30q + 9 = 25q^2 + 30q + 5 + 4 = 5(5q^2 + 6q + 1) + 4$. Let $k = 5q^2 + 6q + 1$. Then k is an integer because it is a sum of products of integers, and hence $m^2 = 5k + 4$ for some integer k.

Case 5 ($m = 5q + 4$ for some integer q): In this case, $m^2 = (5q + 4)^2 = 25q^2 + 40q + 16 = 25q^2 + 40q + 15 + 1 = 5(5q^2 + 8q + 3) + 1$. Let $k = 5q^2 + 8q + 3$. Then k is an integer because it is a sum of products of integers, and hence $m^2 = 5k + 1$ for some integer k.

42. *Proof:* Let p be any prime number except 2 or 3. By the quotient-remainder theorem, p can be written as $6k$ or $6k + 1$ or $6k + 2$ or $6k + 3$ or $6k + 4$ or $6k + 5$ for some integer k. Since p is prime and $p \neq 2$, p is not divisible by 2. Consequently, $p \neq 6k$, $p \neq 6k + 2$, and $p \neq 6k + 4$ for any integer k *[because all of these numbers are divisible by 2].* Furthermore, since p is prime and $p \neq 3$, p is not divisible by 3. Thus $p \neq 6k + 3$ *[because this number is divisible by 3].* Therefore, $p = 6k + 1$ or $p = 6k + 5$ for some integer k.

43. *Proof:* Let n be any odd integer. By Theorem 3.4.4, $n^2 = 8m + 1$ for some integer m. Then $n^4 = (8m + 1)^2 = 64m^2 + 16m + 1 = 16(4m^2 + m) + 1$. But $4m^2 + m$ is an integer (because it is a sum of products of integers), and so by the quotient-remainder theorem, the remainder obtained when n^4 is divided by 16 is 1. Hence by definition of *mod*, $n^4 \bmod 16 = 1$.

45. They are equal.

Proof: Suppose m, n, and d are integers and $d \mid (m-n)$. By definition of divisibility, $m - n = dk$ for some integer k. Therefore, $m = n + dk$. Let $r = n \bmod d$. Then by definition of *mod*, $n = qd + r$ where q and r are integers and $0 \leq r < d$. By substitution, $m = n + dk = (qd + r) + dk = d(q + k) + r$. Since $q + k$ is an integer and $0 \leq r < d$, the integral quotient of the division of n by d is $q + k$ and the remainder is r. Hence $m \bmod d = r$ also, and so $n \bmod d = m \bmod d$.

46. Answer to the first question: not necessarily

Counterexample: Let $m = n = 3$, $d = 2$, $a = 1$, and $b = 1$. Then $m \bmod d = n \bmod d = 3 \bmod 2 = 1 = a = b$. But $a + b = 1 + 1 = 2$, whereas $(m + n) \bmod d = 6 \bmod 2 = 0$.

Answer to the second question: yes.

Proof: Suppose m, n, a, b, and d are integers and $m \bmod d = a$ and $n \bmod d = b$. By definition of *mod*, $m = dq_1 + a$ and $n = dq_2 + b$ for some integers q_1 and q_2. By substitution, $m + n = (dq_1 + a) + (dq_2 + b) = d(q_1 + q_2) + (a + b)$. Apply the quotient-remainder theorem to

$a + b$ to obtain unique integers q_3 and r such that $a + b = dq_3 + r$ and $0 \leq r < d$. By definition of *mod*, $r = (a + b) \bmod d$. By substitution, $m + n = d(q_1 + q_2) + (a + b) = d(q_1 + q_2) + (dq_3 + r) = d(q_1 + q_2 + q_3) + r$ where $q_1 + q_2 + q_3$ and r are integers and $0 \leq r < d$. Hence by definition of *mod*, $r = (m + n) \bmod d$, and so $(m + n) \bmod d = (a + b) \bmod d$.

47. Answer to the first question: not necessarily

    Counterexample: Let $m = n = 2$, $d = 3$, $a = 2$, and $b = 2$. Then $m \bmod d = n \bmod d = 2 \bmod 3 = 2 = a = b$. But $ab = 2 \cdot 2 = 4$, whereas $(mn) \bmod d = 4 \bmod 3 = 1$.

    Answer to the second question: yes.

    Proof: Suppose m, n, a, b, and d are integers and $m \bmod d = a$ and $n \bmod d = b$. By definition of *mod*, $m = dq_1 + a$ and $n = dq_2 + b$ for some integers q_1 and q_2. By substitution, $mn = (dq_1 + a)(dq_2 + b) = d^2 q_1 q_2 + d(aq_1 + bq_2) + ab$. Apply the quotient-remainder theorem to ab to obtain unique integers q_3 and r such that $ab = dq_3 + r$ and $0 \leq r < d$. By definition of *mod*, $r = (ab) \bmod d$. By substitution, $mn = d^2 q_1 q_2 + d(aq_1 + bq_2) + ab = d^2 q_1 q_2 + d(aq_1 + bq_2) + dq_3 + r = d(dq_1 q_2 + aq_1 + bq_2 + q_3) + r$ where $dq_1 q_2 + aq_1 + bq_2 + q_3$ and r are integers and $0 \leq r < d$. Hence by definition of *mod*, $r = (mn) \bmod d$, and so $mn \bmod d = (ab) \bmod d$.

48. *Proof*: Suppose m, d, and k are nonnegative integers and $d > 0$. Let $a = m \bmod d$. By definition of *mod*, $m = dq + a$ for some integer q and $0 \leq a < d$. By substitution, $m + dk = dq + a + dk = d(q + k) + a$. Now $q + k$ is an integer because it is a sum of integers, and $0 \leq a < d$. So by definition of *mod*, $(m + dk) \bmod d = a = m \bmod d$.

50. *Proof*: Let x and y be any real numbers.

    Case 1 (x and y are both nonnegative): In this case $|x| = x$, $|y| = y$, and xy is also nonnegative. So $|xy| = xy = |x| \cdot |y|$.

    Case 2 (x is nonnegative and y is negative): In this case $|x| = x$, $|y| = -y$ and $xy \leq 0$. So $|xy| = -(xy) = x(-y) = |x| \cdot |y|$.

    Case 3 (x is negative and y is nonnegative): In this case $|x| = -x$, $|y| = y$ and $xy \leq 0$. So $|xy| = -(xy) = (-x)y = |x| \cdot |y|$.

    Case 4 (x and y are both negative): In this case $|x| = -x$, $|y| = -y$, and $xy > 0$. So $|xy| = (-x)(-y) = |x| \cdot |y|$.

    Therefore in all four possible cases, $|xy| = |x| \cdot |y|$ *[as was to be shown]*.

52. *Proof*: Let c be any positive real number and let x be any real number.

    Part 1 (Proof that if $-c \leq x \leq c$ then $|x| \leq c$): Suppose that $-c \leq x \leq c$.(*) By the trichotomy law (see Appendix A, T16), either $x \geq 0$ or $x < 0$.

    Case 1 ($x \geq 0$): In this case $|x| = x$, and so by substitution into (*), $-c \leq |x| \leq c$. In particular, $|x| \leq c$.

    Case 2 ($x < 0$): In this case $|x| = -x$, and so $x = -|x|$. Hence by substitution into (*), $-c \leq -|x| \leq c$. In particular, $-c \leq -|x|$. Multiplying both sides by -1 gives $c \geq |x|$, or, equivalently, $|x| \leq c$.

    Therefore, regardless of whether $x \geq 0$ or $x < 0$, $|x| \leq c$ *[as was to be shown]*.

    Part 2 (Proof that if $|x| \leq c$ then $-c \leq x \leq c$): Suppose that $|x| \leq c$.(**) By the trichotomy law, either $x \geq 0$ or $x < 0$.

    Case 1($x \geq 0$): In this case $|x| = x$, and so by substitution into (**), $x \leq c$. Since $x \geq 0$ and $c \geq x$, then $c \geq 0$ by transitivity of order (Appendix A, T17). Then, by property T23 of Appendix A, $0 \geq -c$, and, again by transitivity of order, $x > -c$. Hence $-c \leq x \leq c$.

    Case 2 ($x < 0$): In this case $|x| = -x$, and so by substitution into (**) $-x \leq c$. Multiplying both sides of this inequality by -1 gives $x \geq -c$. Also since $x < 0$ and $0 < c$, then $x \leq c$. Thus $-c \leq x \leq c$.

Therefore, regardless of whether $x \geq 0$ or $x < 0$, we conclude that $-c \leq x \leq c$ *[as was to be shown]*.

53. *Proof:* Let any real numbers x and y be given. By exercise 51,

$$-|x| \leq x \leq |x|$$

and

$$-|y| \leq y \leq |y|.$$

Hence by the order properties of the real numbers (Appendix A, T25),

$$(-|x|) + (-|y|) \leq x + y \leq (|x| + |y|),$$

or, equivalently,

$$-(|x| + |y|) \leq x + y \leq (|x| + |y|)$$

It follows immediately from exercise 52 that $|x + y| \leq |x| + |y|$.

Section 3.5

2. $\lfloor 17/4 \rfloor = \lfloor 4.25 \rfloor = 4$, $\lceil 17/4 \rceil = \lceil 4.25 \rceil = 5$

4. $\lfloor -32/5 \rfloor = \lfloor -6.4 \rfloor = -7$, $\lceil -32/5 \rceil = \lceil -6.4 \rceil = -6$

5. $259 \ div \ 11 = \lfloor 259/11 \rfloor = 23$, $259 \ mod \ 11 = 259 - 11 \cdot \lfloor 259/11 \rfloor = 259 - 11 \cdot 23 = 6$

6. If k is an integer, then $\lceil k \rceil = k$ because $k - 1 < k \leq k$ and $k - 1$ and k are integers.

7. If k is an integer, then $\lceil k + 1/2 \rceil = k + 1$ because $k < k + 1/2 \leq k + 1$ and k and $k + 1$ are both integers.

8. When the ceiling notation is used, the answer is either $\lceil n/7 \rceil - 1$ if $n/7$ is not an integer or $\lceil n/7 \rceil$ if $n/7$ is an integer.

9. If the remainder obtained when n is divided by 36 is positive, an additional box beyond those containing exactly 36 units will be needed to hold the extra units. So since the ceiling notation rounds each number up to the nearest integer, the number of boxes required is $\lceil n/36 \rceil$. Also, because the ceiling of an integer is itself, if the number of units is a multiple of 36, the number of boxes required is $\lceil n/36 \rceil$ as well. Thus the ceiling notation is more appropriate for this problem because the answer is simply $\lceil n/36 \rceil$ regardless of the value of n. If the floor notation is used, the answer is more complicated: if $n/36$ is not an integer, it is $\lfloor n/36 \rfloor + 1$, but if n is an integer, it is $\lfloor n/36 \rfloor$.

10. *a.* (ii) $(2100 + \lfloor \frac{2100-1}{4} \rfloor - \lfloor \frac{2100-1}{100} \rfloor + \lfloor \frac{2100-1}{400} \rfloor) \ mod \ 7 = (2100 + 524 - 20 + 5) \ mod \ 7 = 2609 \ mod \ 7 = 5$, which corresponds to Friday.

(iii) Answers will vary.

b. When the year $n-1$ is a leap year, then, because leap years contain an extra day, January 1 of the year n is one day of the week later than it would otherwise be. If leap years occurred exactly every four years, then there would be $\lfloor (n - 1)/4 \rfloor$ extra leap year days from year 1 to year n. So the day of the week of January 1 of year n would be pushed forward $\lfloor (n - 1)/4 \rfloor \ mod \ 7$ days from its value in year 1. But leap years do not occur exactly every four years. Every century year (year that is a multiple of 100), except those that are multiples of 400, the leap year day is not added. So instead of $\lfloor (n - 1)/4 \rfloor$ leap year days from year 1 to year n, there are $\lfloor (n - 1)/4 \rfloor - \lfloor (n - 1)/100 \rfloor + \lfloor (n - 1)/400 \rfloor$ leap year days, where $\lfloor (n - 1)/100 \rfloor$ is the number of century years from year 1 to year n and $\lfloor (n - 1)/400 \rfloor$ is the number of those that are multiples of 400. Hence the day of the week of January 1 of year n is actually pushed forward $(\lfloor (n - 1)/4 \rfloor - \lfloor (n - 1)/100 \rfloor + \lfloor (n - 1)/400 \rfloor) \ mod \ 7$ days from its value in year 1.

11. A necessary and sufficient condition for the floor of a real number to equal the number is that the number be an integer.

13. *a. Proof:* Suppose n and d are integers with $d \neq 0$ and $d \mid n$. Then $n = d \cdot k$ for some integer k. By substitution and algebra, $\lfloor n/d \rfloor = \lfloor d \cdot k/d \rfloor = \lfloor k \rfloor$, and $\lfloor k \rfloor = k$ because $k \leq k < k + 1$ and both k and $k + 1$ are integers. But since $n = d \cdot k$, then $k = n/d$. Hence $\lfloor n/d \rfloor = k = n/d$. Therefore, $n = \lfloor n/d \rfloor \cdot d$ *[as was to be shown]*.

b. Proof: Suppose n and d are integers with $d \neq 0$ and $n = \lfloor n/d \rfloor \cdot d$. By definition of floor, $\lfloor n/d \rfloor$ is an integer. Hence, $n = d \cdot (some\ integer)$, and so by definition of divisibility, $d \mid n$.

c. A necessary and sufficient condition for an integer n to be divisible by an integer d is that $n = \lfloor n/d \rfloor \cdot d$.

16. *Counterexample:* Let $x = 3/2$. Then $\lfloor x^2 \rfloor = \lfloor (3/2)^2 \rfloor = \lfloor 9/4 \rfloor = 2$, whereas $\lfloor x \rfloor^2 = \lfloor 3/2 \rfloor^2 = 1^2 = 1$.

17. *Proof:* Let n be any integer. By the quotient-remainder theorem and the definition of *mod*, either $n\ mod\ 3 = 0$ or $n\ mod\ 3 = 1$ or $n\ mod\ 3 = 2$.

Case 1 ($n\ mod\ 3 = 0$): In this case, $n = 3q$ for some integer q by definition of *mod*. By substitution and algebra, $\lfloor n/3 \rfloor = \lfloor 3q/3 \rfloor = \lfloor q \rfloor$ and $\lfloor q \rfloor = q$ because q is an integer and $q \leq q < q + 1$. But solving $n = 3q$ for q gives $q = n/3$. Thus $\lfloor n/3 \rfloor = q = n/3$ *[as was to be shown]*.

Case 2 ($n\ mod\ 3 = 1$): In this case, $n = 3q + 1$ for some integer q by definition of *mod*. By substitution and algebra, $\lfloor n/3 \rfloor = \lfloor (3q + 1)/3 \rfloor = \lfloor q + 1/3 \rfloor$ and $\lfloor q + 1/3 \rfloor = q$ because q is an integer and $q \leq q + 1/3 < q + 1$. But solving $n = 3q + 1$ for q gives $q = (n - 1)/3$. Thus $\lfloor n/3 \rfloor = q = (n - 1)/3$ *[as was to be shown]*.

Case 3 ($n\ mod\ 3 = 2$): The proof for this case is included in the answers in Appendix B.

Cases 1, 2, and 3 show that no matter what integer n is given, $\lfloor n/3 \rfloor$ has one of the three forms in the statement of the exercise.

18. *Counterexample:* Let $x = y = 1.5$. Then $\lceil x + y \rceil = \lceil 1.5 + 1.5 \rceil = \lceil 3 \rceil = 3$, whereas $\lceil x \rceil + \lceil y \rceil = \lceil 1.5 \rceil + \lceil 1.5 \rceil = 2 + 2 = 4$.

19. *Proof:* Let x be any *[particular but arbitrarily chosen]* real number. Then $\lceil x + 1 \rceil$ is some integer: say $\lceil x + 1 \rceil = n$. By definition of ceiling, $n - 1 < x + 1 \leq n$. Subtracting 1 from all parts of this inequality gives $n - 2 < x \leq n - 1$, and thus by definition of ceiling $\lceil x \rceil = n - 1$. Solving this equation for n gives $n = \lceil x \rceil + 1$. But $n = \lceil x + 1 \rceil$ also. Hence $\lceil x + 1 \rceil = \lceil x \rceil + 1$ *[as was to be shown]*.

20. *Counterexample:* Let $x = y = 1.1$. Then $\lceil x \cdot y \rceil = \lceil (1.1) \cdot (1.1) \rceil = \lceil 1.21 \rceil = 2$. On the other hand, $\lceil x \rceil \cdot \lceil y \rceil = \lceil 1.1 \rceil \cdot \lceil 1.1 \rceil = 2 \cdot 2 = 4$.

21. *Proof:* Let n be any odd integer. *[We must show that $\lceil n/2 \rceil = (n + 1)/2$.]* By definition of odd, $n = 2k + 1$ for some integer k. Substituting into the left-hand side of the equation to be proved gives

$$\left\lceil \frac{n}{2} \right\rceil = \left\lceil \frac{2k + 1}{2} \right\rceil = \left\lceil k + \frac{1}{2} \right\rceil = k + 1,$$

where $\left\lceil k + \dfrac{1}{2} \right\rceil = k + 1$ by definition of ceiling because $k < k + 1/2 < k + 1$ and k is an integer. On the other hand, substituting into the right-hand side of the equation to be shown gives

$$\frac{n + 1}{2} = \frac{(2k + 1) + 1}{2} = \frac{2k + 2}{2} = \frac{2(k + 1)}{2} = k + 1$$

also. Thus both the left- and right-hand sides of the equation to be proved equal $k + 1$, and so both are equal to each other. In other words, $\lceil n/2 \rceil = (n + 1)/2$ *[as was to be shown]*.

22. *Counterexample:* Let $x = y = 1.9$. Then $\lceil xy \rceil = \lceil (1.9)(1.9) \rceil = \lceil 3.61 \rceil = 4$, whereas $\lceil 1.9 \rceil \cdot \lfloor 1.9 \rfloor = 2 \cdot 1 = 2$.

24. *Proof:* Suppose m is any integer and x is any real number that is not an integer. By definition of floor, $\lfloor x \rfloor = n$ where n is an integer and $n \le x < n + 1$. Since x is not an integer, $x \ne n$, and so $n < x < n + 1$. Multiply all parts of this inequality by -1 to obtain $-n > -x > -n - 1$. Then add m to all parts to obtain $m - n > m - x > m - n - 1$, or, equivalently, $m - n - 1 < m - x < m - n$. But $m - n - 1$ and $m - n$ are both integers, and so by definition of floor, $\lfloor m - x \rfloor = m - n - 1$. By substitution, $\lfloor x \rfloor + \lfloor m - x \rfloor = n + (m - n - 1) = m - 1$ *[as was to be shown]*.

25. *Proof:* Suppose x is any *[particular but arbitrarily chosen]* real number. *[We must show that $\lfloor \lfloor x/2 \rfloor / 2 \rfloor = \lfloor x/4 \rfloor$.]* Let $n = \lfloor x/2 \rfloor$. Then by definition of floor, $n \le x/2 < n + 1$.

    Case 1 (n is even): In this case, $n/2$ is an integer, and we divide all parts of the inequality $n \le x/2 < n + 1$ by 2 to obtain $n/2 \le x/4 < (n + 1)/2$. But $(n + 1)/2 = n/2 + 1/2 < n/2 + 1$. Hence $n/2 \le x/4 < n/2 + 1$ because $n/2$ is an integer, and so by definition of floor, $\lfloor x/4 \rfloor = n/2$. Since $n = \lfloor x/2 \rfloor$, then, $\lfloor \lfloor x/2 \rfloor / 2 \rfloor = \lfloor n/2 \rfloor = n/2 = \lfloor x/4 \rfloor$.

    Case 2 (n is odd): In this case $(n-1)/2$ is an integer, and by Theorem 3.5.2 $\lfloor n/2 \rfloor = (n-1)/2$. We divide all parts of the inequality $n \le x/2 < n + 1$ by 2 to obtain $n/2 \le x/4 < (n + 1)/2$. But $n/2 > (n - 1)/2$. Thus $(n - 1)/2 \le x/4 < (n + 1)/2$. Now $(n - 1)/2$ is an integer and $(n + 1)/2 = (n - 1)/2 + 1$. Hence by definition of floor, $\lfloor x/4 \rfloor = (n - 1)/2$. Since $(n - 1)/2 = \lfloor n/2 \rfloor$ and $n = \lfloor x/2 \rfloor$, then $\lfloor \lfloor x/2 \rfloor / 2 \rfloor = \lfloor n/2 \rfloor = \lfloor x/4 \rfloor$.

    Thus, in both cases, $\lfloor \lfloor x/2 \rfloor / 2 \rfloor = \lfloor x/4 \rfloor$ *[as was to be shown]*.

27. *Proof:* Suppose x is any real number such that $x - \lfloor x \rfloor \ge 1/2$. Multiply both sides by 2 to obtain $2x - 2\lfloor x \rfloor \ge 1$, or equivalently, $2x \ge 2\lfloor x \rfloor + 1$. Now by definition of floor, $x < \lfloor x \rfloor + 1$. Hence $2x < 2\lfloor x \rfloor + 2$. Put the two inequalities involving x together to obtain $2\lfloor x \rfloor + 1 \le 2x < 2\lfloor x \rfloor + 2$. By definition of floor, then, $\lfloor 2x \rfloor = 2\lfloor x \rfloor + 1$.

28. *Proof:* Let n be any odd integer. *[We must show that $\left\lfloor \dfrac{n^2}{4} \right\rfloor = \left(\dfrac{n-1}{2} \right)\left(\dfrac{n+1}{2} \right)$.]* By definition of odd, $n = 2k + 1$ for some integer k. Substituting into the left-hand side of the equation to be proved gives

$$\left\lfloor \frac{n^2}{4} \right\rfloor = \left\lfloor \frac{(2k+1)^2}{4} \right\rfloor = \left\lfloor \frac{4k^2 + 4k + 1}{4} \right\rfloor = \left\lfloor k^2 + k + \frac{1}{4} \right\rfloor = k^2 + k,$$

where $\left\lfloor k^2 + k + \dfrac{1}{4} \right\rfloor = k^2 + k$ by definition of floor because $k^2 + k$ is an integer and $k^2 + k < k^2 + k + \dfrac{1}{4} < k^2 + k + 1$. On the other hand, substituting into the right-hand side of the equation to be proved gives

$$\left(\frac{n-1}{2} \right)\left(\frac{n+1}{2} \right) = \left(\frac{(2k+1)-1}{2} \right)\left(\frac{(2k+1)+1}{2} \right) = \left(\frac{2k}{2} \right)\left(\frac{2k+2}{2} \right) = k(k+1) = k^2 + k$$

also. Thus the left- and right-hand sides of the equation to be proved both equal $k^2 + k$, and so the two sides are equal to each other. In other words, $\left\lfloor \dfrac{n^2}{4} \right\rfloor = \left(\dfrac{n-1}{2} \right)\left(\dfrac{n+1}{2} \right)$ *[as was to be shown]*.

29. *Proof:* Let n be any odd integer. *[We must show that $\left\lceil \dfrac{n^2}{4} \right\rceil = \dfrac{n^2 + 3}{4}$.]* By definition of odd, $n = 2k + 1$ for some integer k. Substituting into the left-hand side of the equation to be proved gives

$$\left\lceil \frac{n^2}{4} \right\rceil = \left\lceil \frac{(2k+1)^2}{4} \right\rceil = \left\lceil \frac{4k^2 + 4k + 1}{4} \right\rceil = \left\lceil k^2 + k + \frac{1}{4} \right\rceil = k^2 + k + 1$$

where $\left\lceil k^2 + k + \dfrac{1}{4} \right\rceil = k^2 + k + 1$ by definition of ceiling because $k^2 + k + 1$ is an integer and $k^2 + k < k^2 + k + \dfrac{1}{4} < k^2 + k + 1$. On the other hand, substituting into the right-hand side of the equation to be proved gives

$$\frac{n^2 + 3}{4} = \frac{(2k+1)^2 + 3}{4} = \frac{4k^2 + 4k + 1 + 3}{4} = \frac{4k^2 + 4k + 4}{4} = k^2 + k + 1$$

also. Thus the left- and right-hand sides of the equation to be proved both equal $k^2 + k + 1$, and so the two sides are equal to each other. In other words, $\left\lceil \dfrac{n^2}{4} \right\rceil = \dfrac{n^2 + 3}{4}$ *[as was to be shown].*

Section 3.6

2. By definition of irrational number, irrational numbers are real numbers that are not rational. Thus $\frac{1}{0}$ is not an irrational number because it is not a real number (since division by zero is not defined).

4. *Proof:* Suppose not. That is, suppose there is an integer n such that $7m + 4$ is divisible by 7. *[We must derive a contradiction.]* By definition of divisibility, $7m + 4 = 7k$ for some integer k. Subtracting $7m$ from both sides gives that $4 = 7k - 7m = 7(k - m)$. Since $k - m$ is an integer (being a difference of integers), 7 divides 4. But, by Example 3.3.3, this implies that $7 \leq 4$, which contradicts the fact that $7 > 4$. *[Thus for all integers m, $7m + 4$ is not divisible by 7.]*

6. *Negation of statement:* There is a greatest negative real number.

   Proof of statement: Suppose not. That is, suppose there is a greatest negative real number a. *[We must deduce a contradiction.]* Then $a < 0$ and $a \geq x$ for every negative real number x. Let $b = a/2$. Then b is a real number because b is a quotient of two real numbers (with a nonzero denominator). Also $a < a/2 < 0$. *[The reason is that $0 < 1/2 < 1$ and multiplying all parts by a, which is less than zero, gives $a < a/2 < 0$.]* By substitution, then, $a < b < 0$. Thus b is a negative real number that is greater than a. This contradicts the supposition that a is the greatest negative real number. *[Hence the supposition is false and the statement is true.]*

7. *Proof:* Suppose not. That is, suppose there is a least positive rational number. Call it r. Then r is a real number such that $r > 0$, r is rational, and for all positive rational numbers x, $r \leq x$. Let $s = r/2$. Note that if we divide both sides of the inequality $0 < r$ by 2, we obtain $0 < r/2 = s$, and if we add r to the inequality $0 < r$ and then divide by 2, we obtain $\dfrac{0 + r}{2} < \dfrac{r + r}{2}$, or, equivalently, $s = \dfrac{r}{2} < r$. Hence $0 < s < r$. Note also that since r is rational, $r = a/b$ for some integers a and b with $b \neq 0$, and so $s = \dfrac{r}{2} = \dfrac{a/b}{2} = \dfrac{a}{2b}$. Since a and $2b$ are integers and $2b \neq 0$, s is rational. Thus we have found a positive rational number s such that $s < r$. This contradicts the supposition that r is the *least* positive rational number. Therefore, there is no least positive rational number.

9. *Proof:* Suppose not. That is, suppose there are real numbers x and y such that x is irrational, y is rational and $x - y$ is rational. *[We must derive a contradiction.]* By definition of rational, $y = a/b$ and $x - y = c/d$ for some integers a, b, c, and d with $b \neq 0$ and $d \neq 0$. Then, by substitution, $x - \frac{a}{b} = \frac{c}{d}$. Solve this equation for x to obtain $x = \frac{c}{d} + \frac{a}{b} = \frac{bc}{bd} + \frac{ad}{bd} = \frac{bc + ad}{bd}$. But both $bc + ad$ and bd are integers because products and sums of integers are integers, and $bd \neq 0$ by the zero product property. Hence x is a ratio of integers with a nonzero denominator, and so x is rational by definition of rational. This contradicts the supposition that x is irrational. *[Hence the supposition is false, and the given statement is true.]*

11. *Proof:* Suppose not. That is, suppose there are rational numbers a and b such that $b \neq 0$, r is an irrational number, and $a + br$ is rational. *[We must derive a contradiction.]* By definition of rational, $a = \frac{i}{j}, b = \frac{k}{l}$, and $a + br = \frac{m}{n}$ where i, j, k, l, m, and n are integers and $j \neq 0, l \neq 0$, and $n \neq 0$. Since $b \neq 0$, we also have that $k \neq 0$. By substitution $a + br = \frac{i}{j} + \frac{k}{l} \cdot r = \frac{m}{n}$, or, equivalently, $\frac{k}{l} \cdot r = \frac{m}{n} - \frac{i}{j}$. Solving for r gives $r = \frac{mj - in}{nj} \cdot \frac{l}{k} = \frac{mjl - inl}{njk}$. Now $mjl - inl$ and njk are both integers *[because products and differences of integers are integers]* and $njk \neq 0$ because $n \neq 0, j \neq 0$, and $k \neq 0$. Hence by definition of rational, r is a rational number. But this contradicts the supposition that r is irrational.*[Hence the supposition is false and the statement is true.]*

12. *Proof 1:* Suppose not. That is, suppose $\exists$ an integer n such that $4 \mid (n^2 - 2)$. *[We must derive a contradiction.]* By definition of divisibility, $n^2 - 2 = 4m$ for some integer m. By the quotient-remainder theorem with $d = 2$, n is either even or odd.

   Case 1 (n is even): In this case, $n = 2k$ for some integer k, and so, by substitution, $n^2 - 2 = (2k)^2 - 2 = 4k^2 - 2 = 4m$, where m is an integer. Thus $4k^2 - 4m = 2$, and hence $k^2 - m = \frac{1}{2}$. But the left-hand side of this equation is an integer (because k and m are integers) and the right-hand side is not an integer. Since this is impossible, the case where n is even cannot occur.

   Case 2 (n is odd): In this case, $n = 2k + 1$ for some integer k, and so, by substitution, $n^2 - 2 = (2k + 1)^2 - 2 = 4k^2 + 4k + 1 - 2 = 4k^2 + 4k - 1 = 4m$, where m is an integer. Thus $4k^2 + 4k - 4m = 1$, and hence $k^2 + k - m = \frac{1}{4}$. But the left-hand side of this equation is an integer (because k and m are integers) and the right-hand side is not an integer. Since this is impossible, the case where n is odd cannot occur.

   It follows from cases 1 and 2 that n can be neither even nor odd, which contradicts the fact that it must be one or the other. *[Therefore the supposition is false, and the given statement is true.]*

   Proof 2: Suppose not. That is, suppose $\exists$ an integer n such that $4 \mid (n^2 - 2)$. *[We must derive a contradiction.]* By definition of divisibility, $n^2 - 2 = 4m$ for some integer m. Then $n^2 = 4m + 2 = 2(2m + 1)$, and so n^2 is even. Hence n is even (by Proposition 3.6.4). By definition of even, $n = 2k$ for some integer k. Substituting into the equation $n^2 - 2 = 4m$ gives $(2k)^2 - 2 = 4k^2 - 2 = 4m$, and so $4k^2 = 4m + 2$. Dividing by 2 gives $2k^2 = 2m + 1$. Since k^2 is an integer, this implies that $2m + 1$ is even, but, since m is an integer, $2m + 1$ is odd. This contradicts Theorem 3.6.2 that no integer is both even and odd . *[Hence the supposition is false and the statement is true.]*

13. *Proof:* Suppose not. That is, suppose there exist prime numbers a, b, and c such that $a^2 + b^2 = c^2$. Subtracting b^2 from both sides of the equation gives that $a^2 = c^2 - b^2 = (c - b)(c + b)$. Either $c - b = 1$ or $c - b > 1$ *[because since $c + b > 0$ and $a^2 > 0$, $c - b$ must be positive].*

   Case 1 (c − b = 1): In this case, because both c and b are prime numbers and the only even prime number is 2, the only possible values for b and c are $c = 3$ and $b = 2$. Then $(c - b)(c + b) = 1 \cdot 5 = 5 = a^2$, and so $\sqrt{5} = a$. But this contradicts the assumption that a is a prime number.

   Case 2 (c − b > 1): In this case, $a^2 = (c - b)(c + b)$ where both $(c - b) > 1$ and $(c + b) > 1$. Because a is prime, the only positive factors of a are 1 and a, and so, by the unique factorization theorem, the only positive factors of a^2 are 1, a, and a^2. Because both $(c - b)$ and $(c + b)$ are greater than 1, the only possibility is that both are equal to a. But this is implies that $c - b = c + b$, which implies that $-b = b$, and hence that $b = 0$. This contradicts the supposition that b is a prime number.

   Thus a contradiction is reached in both possible cases, and hence the supposition is false and the given statement is true.

14. Yes.

   Proof. Suppose not. That is, suppose $\exists$ integers a, b, and c such that a and b are both odd and $a^2 + b^2 = c^2$. By definition of odd, $a = 2k + 1$ and $b = 2m + 1$ for some integers k and m. Then, by substitution, $c^2 = a^2 + b^2 = (2k+1)^2 + (2m+1)^2 = 4k^2 + 4k + 1 + 4m^2 + 4m + 1 = 4(k^2 + k + m^2 + m) + 2$. Let $t = k^2 + k + m^2 + m$. Then t is an integer because products and sums of integers are integers. Hence $c^2 = 4t + 2$, or, equivalently, $c^2 - 2 = 4t$. So, by definition of divisibility, $c^2 - 2$ is divisible by 4. But the argument used in the answer to exercise 12 shows that this is impossible. Thus the supposition is false, and the given statement is true.

15. *Proof.* Suppose not. That is, suppose $\exists$ odd integers a, b, and c and a rational number z such that $az^2 + bz + c = 0$. By definition of rational, there exist integers m and n such that $z = m/n$ and $n \neq 0$. By cancelling common factors if necessary, we may assume that m and n have no common factors. By substitution, $a(\frac{m}{n})^2 + b(\frac{m}{n}) + c = 0$, and multiplying both sides by n^2 gives $am^2 + bmn + cn^2 = 0$.

   Case 1 (both m and n are even): In this case both m and n have a factor of 2, which contradicts the assumption that m and n have no common factors.

   Case 2 (m is odd and n is even): In this case am^2 is a product of odd integers, and hence is odd (by Example 3.2.3 #3), and both bmn and cn^2 are products that contain an even factor, and hence are even (by Example 3.2.3 #1 and #4). Thus $bmn + cn^2$ is a sum of even integers, which is even (by Example 3.2.3 #1), and so $am^2 + bmn + cn^2$ is the sum of an odd integer and an even integer, which is odd (by Example 3.2.3 #5). But $am^2 + bmn + cn^2 = 0$, which is even. Therefore, $am^2 + bmn + cn^2$ is both even and odd, which contradicts Theorem 3.6.2.

   Case 3 (m is even and n is odd): In this case cn^2 is a product of odd integers, and hence is odd (by Example 3.2.3 #3), and both am^2 and bmn are products that contain an even factor, and hence are even (by Example 3.2.3 #1 and #4). Thus $am^2 + bmn$ is a sum of even integers, which is even (by Example 3.2.3 #1), and so $am^2 + bmn + cn^2$ is the sum of an even integer and an odd integer, which is odd (by Example 3.2.3 #5). But $am^2 + bmn + cn^2 = 0$, which is even. Therefore, $am^2 + bmn + cn^2$ is both even and odd, which contradicts Theorem 3.6.2.

   Case 4 (both m and n are odd): In this case all three products am^2, bmn, and cn^2 consist only of odd factors, and hence all are odd (by Example 3.2.3 #3). Thus $am^2 + bmn$ is the sum of two odd integers, which is even (by Example 3.2.3 #2), and so $am^2 + bmn + cn^2$ is the sum of an even and an odd integer, which is odd (by Example 3.2.3 #5). But $am^2 + bmn + cn^2 = 0$, which is even. Therefore, $am^2 + bmn + cn^2$ is both even and odd, which contradicts Theorem 3.6.2.

   Hence in all four cases a contradiction is reached, and so the supposition is false and the given statement is true.

18. *Proof (by contraposition):* Suppose a and b are *[particular but arbitrarily chosen]* real numbers such that $a \geq 25$ and $b \geq 25$. Then $a + b \geq 25 + 25 = 50$. Hence if $a + b < 50$, then $a < 25$ or $b < 25$.

20. a. *Proof by contradiction:* Suppose not. That is, suppose $\exists$ a real number r such that r^2 is irrational and r is rational. Show that this supposition leads logically to a contradiction.

   b. *Proof by contraposition:* Suppose that r is any real number such that r is rational. Show that r^2 is also rational.

22. a. *Proof by contraposition:* Suppose x is a nonzero real number and $1/x$ is rational. *[We must show that x is itself rational.]* Because $1/x$ is rational, there are integers a and b with $b \neq 0$ such that $1/x = a/b$ (*). Now since $1 \cdot (1/x) = 1$, $1/x$ cannot equal zero, and so $a \neq 0$. Thus we may solve equation (*) for x to obtain $x = b/a$ where b and a are integers and $a \neq 0$. Hence, by definition of rational, $1/x$ is rational *[as was to be shown]*.

   b. *Proof by contradiction:* Suppose not. That is, suppose $\exists$ a nonzero irrational number x such that $1/x$ is rational. *[We must show that this supposition leads logically to a*

contradiction.] By definition of rational, $1/x = a/b$ (*), where a and b are integers with $b \neq 0$. Since $1 \cdot (1/x) = 1$, $1/x$ cannot equal zero, and so $a \neq 0$. Thus we may solve equation (*) for x to obtain $x = b/a$ where b and a are integers and $a \neq 0$. Hence, by definition of rational, $1/x$ is rational, which contradicts the supposition that x is irrational. *[Hence the supposition is false and the statement is true.]*

23. *a. Proof by contraposition:* Suppose n is a *[particular but arbitrarily chosen]* integer that is not odd. *[We must show that n^2 is not odd.]* *[We must show that n^2 is not even.]* By the parity property, because n is not odd, n is even. So $n^2 = n \cdot n$ is also even (by exercise 17 of Section 3.1). Hence by Theorem 3.6.2, n^2 is not odd *[as was to be shown.]*

b. Proof by contradiction: Suppose not. That is, suppose $\exists$ an integer n such that n^2 is odd and n is not odd. *[We must derive a contradiction.]* By the parity property, n is even, and by definition of even, $n = 2k$ for some integer k. Then $n^2 = (2k)^2 = 2(2k^2)$ by the laws of algebra. Let $m = 2k^2$. Then m is an integer because it is a product of integers. Thus $n^2 = 2m$ for some integer m, and so by definition of even, n^2 is even. Hence, by Theorem 3.6.2, n^2 is not odd, which contradicts the supposition that n^2 is odd. *[Hence the supposition is false and the statement is true.]*

25. *a. Proof (by contraposition):* Suppose m and n are integers such that one of m and n is even and the other is odd. By exercise 19 of Section 3.1, the sum of any even integer and any odd integer is odd. Hence $m + n$ is odd. *[This is what was to be shown].*

b. Proof by contradiction: Suppose not. That is, suppose $\exists$ integers m and n such that $m+n$ is even and either m is even and n is odd or m is odd and n is even. By exercise 19 in Section 3.1, the sum of any even integer and any odd integer is odd. Thus both when m is even and n is odd and when m is odd and n is even, the sum $m + n$ is odd. This contradicts the supposition that $m + n$ is even. *[Hence the supposition is false and the statement is true.]*

26. *a. Proof (by contraposition):* By De Morgan's law, we must show that for all integers a, b, and c, if $a \mid (b+c)$ then $a \nmid b$ or $a \mid c$. But by the logical equivalence of $p \to q \vee r$ and $p \wedge \sim q \to r$, it suffices to show that for all integers a, b, and c, if $a \mid (b+c)$ and $a \mid b$, then $a \mid c$. So suppose a, b, and c are any integers with $a \mid (b+c)$ and $a \mid b$. *[We must show that $a \mid c$.]* By definition of divisibility, $b + c = as$ and $b = ar$ for some integers s and r. By substitution, $c = (b+c) - b = as - ar = a(s - r)$. But $s - r$ is an integer (because it is a difference of integers). Thus by definition of divisibility, $a \mid c$ *[as was to be shown]*.

b. Proof by contradiction: Suppose not. That is, suppose $\exists$ integers a, b, and c such that $a \mid b$ and $a \nmid c$ and $a \mid (b+c)$. *[We must derive a contradiction.]* By definition of divisibility, $\exists$ integers r and s such that $b = ar$ and $b + c = as$. By substitution, $ar + c = as$. Subtracting ar from both sides gives $c = as - ar = a(s - r)$. But $s - r$ is an integer because r and s are integers. Hence by definition of divisibility, $a \mid c$. This contradicts the supposition that $a \nmid c$. *[Hence the supposition is false and the statement is true.]*

28. *b. Proof by contraposition:* Suppose n is an integer with $n > 1$ and n is not prime. *[We must show that n is divisible by some integer that is greater than 1 and less than or equal to $\sqrt{n}$.]* Because n is not prime, $n = rs$ where r and s are integers and $1 < r$ and $1 < s$. By part (a), if both $r > \sqrt{n}$ and $s > \sqrt{n}$, then $rs > n$, which would contradict the fact that $rs = n$. Hence at least one of r or s is less than or equal to $\sqrt{n}$, and so n is divisible by an integer that is greater than 1 and less than or equal to $\sqrt{n}$ *[as was to be shown]*.

c. Proof by contraposition: Suppose n is an integer with $n > 1$ and n is not prime. *[We must show that n is divisible by some prime number that is less than or equal to $\sqrt{n}$.]* By part (b), n is divisible by an integer, say r, such that $1 < r \leq \sqrt{n}$. By Theorem 3.3.2, there is a prime number p such that p divides r. Then the transitive property of divisibility (Theorem 3.3.1) and the facts that $p \mid r$ and $r \mid n$ imply that $p \mid n$. Moreover, because $p \mid r$ and both p and r are positive, we have that $p \leq r$ by Example 3.3.3 Finally, because $r \leq \sqrt{n}$, transitivity

of order (Appendix A, T17) implies that $p \leq \sqrt{n}$. Thus n is divisible by a prime number that is less than or equal to $\sqrt{n}$ [as was to be shown].

29. *c.* $\sqrt{527} \cong 22.96$, and so the prime factors to be checked are 2, 3, 5, 7, 11, 13, 17, and 19. Testing each in turn shows that 527 is not prime because 527=17·31.

   d. $\sqrt{613} \cong 24.76$, and so the prime factors to be checked are 2, 3, 5, 7, 11, 13, 17, 19, and 23. Testing each in turn shows that none divides 613. Therefore, 613 is prime.

30. After crossing out all multiples of 2, 3, 5, and 7 (the prime numbers less than $\sqrt{100}$), the remaining numbers are prime. They are circled in the following diagram.

②	③	4̸	⑤	6̸	⑦	8̸	9̸	1̸0̸	⑪	1̸2̸	⑬	1̸4̸	1̸5̸
1̸6̸	⑰	1̸8̸	⑲	2̸0̸	2̸1̸	2̸2̸	㉓	2̸4̸	2̸5̸	2̸6̸	2̸7̸	2̸8̸	㉙
3̸0̸	㉛	3̸2̸	3̸3̸	3̸4̸	3̸5̸	3̸6̸	㊲	3̸8̸	3̸9̸	4̸0̸	㊶	4̸2̸	㊸
4̸4̸	4̸5̸	4̸6̸	㊼	4̸8̸	4̸9̸	5̸0̸	5̸1̸	5̸2̸	㊽	5̸4̸	5̸5̸	5̸6̸	5̸7̸
5̸8̸	㊾	6̸0̸	㊿	6̸2̸	6̸3̸	6̸4̸	6̸5̸	6̸6̸	㊿	6̸8̸	6̸9̸	7̸0̸	㉛
7̸2̸	㊼	7̸4̸	7̸5̸	7̸6̸	7̸7̸	7̸8̸	㊾	8̸0̸	8̸1̸	8̸2̸	㊿	8̸4̸	8̸5̸
8̸6̸	8̸7̸	8̸8̸	㊾	9̸0̸	9̸1̸	9̸2̸	9̸3̸	9̸4̸	9̸5̸	9̸6̸	㊾	9̸8̸	9̸9̸

31. *c.* $\sqrt{8623} \cong 92.9$, and so prime factors to be checked are listed in the answer to exercise 30. Testing each in turn shows that none divides 8623, and so 8623 is prime.

   d. $\sqrt{7917} \cong 88.98$, and so prime factors to be checked are listed in the answer to exercise 30. Testing each in turn shows that $7917 = 7 \cdot 1131$, and so 7917 is not prime.

32. *Proof:* Let n be any integer greater than 11. Then each of the numbers $n - 4$, $n - 6$, and $n - 8$ is greater than 3. Observe that $n = (n - 4) + 4 = (n - 6) + 6 = (n - 8) + 8$ and that all three of 4, 6, and 8 are composite. Thus, if at least one of $n - 4$, $n - 6$, and $n - 8$ is composite, then n can be written as a sum of two composite numbers. In particular, in case either $n - 6$ or $n - 8$ is composite, we are done. Suppose, therefore, that neither $n - 6$ nor $n - 8$ is composite. [We will show that $n - 4$ is composite.] Observe that $n - 8$, $n - 7$, and $n - 6$ constitute a sequence of three consecutive integers. By exercise 28 of Section 3.4, in any such sequence one of the integers is divisible by 3. Now neither $n - 6$ nor $n - 8$ is divisible by 3 (because since $n > 11$, $n - 6$ and $n - 8$ are both greater than 3, and neither $n - 6$ nor $n - 8$ is prime). Consequently, $n - 7$ is divisible by 3, and so $n - 7 = 3k$ for some integer k. Thus $n - 4 = (n - 7) + 3 = 3k + 3 = 3(k + 1)$. Therefore $n - 4$ is composite because it is a product of 3 and $k + 1$. [We know that $k + 1 > 1$ because since $n > 11$, $3k = n - 7 > 4$, and so $k > 4/3$.] Hence in case neither $n - 6$ nor $n - 8$ is composite, then $n - 4$ is composite, and so in this case also n is a sum of two composite numbers, namely $n - 4$ and 4.

   Note: The solution to exercise 34, Section 3.4 provides a direct proof of the statement given in this exercise.

Section 3.7

2. You cannot be sure that the result of the calculation is a rational number because the calculator does not tell you anything about the decimal digits that are beyond its display range. If they were all zero after some point or if a pattern repeats forever, then the number would be rational. But the fact that there is a repeating pattern in the few digits that are shown is no guarantee that the pattern persists.

4. *Proof:* Suppose not. Suppose $3\sqrt{2} - 7$ is rational. *[We must derive a contradiction.]* By definition of rational, $\exists$ integers a and b with $3\sqrt{2} - 7 = a/b$ and $b \neq 0$. Solving for $\sqrt{2}$ gives $\sqrt{2} = (a/b + 7)/3 = (a + 7b)/3b$. But $a + 7b$ and $3b$ are integers (because products and sums of integers are integers) and $3b \neq 0$ (by the zero product property). Therefore by definition of rational, $\sqrt{2}$ is rational. This contradicts Theorem 3.7.1 which states that $\sqrt{2}$ is irrational. *[Hence the supposition is false and the statement is true.]*

Note: This result can also be deduced from exercise 11, Section 3.6.

6. False.

Proof 1: $\sqrt{2}/6 = (1/6) \cdot \sqrt{2}$, which is a product of a nonzero rational number and an irrational number. By exercise 10 of Section 3.6, such a product is irrational.

Proof 2: Suppose not. Suppose $\sqrt{2}/6$ is rational. *[We must derive a contradiction.]* By definition of rational, $\exists$ integers a and b with $\sqrt{2}/6 = a/b$ and $b \neq 0$. Solving for $\sqrt{2}$ gives $\sqrt{2} = 6a/b$. But $6a$ is an integer (because products of integers are integers) and b is a nonzero integer. Therefore by definition of rational, $\sqrt{2}$ is rational. This contradicts Theorem 3.7.1 which states that $\sqrt{2}$ is irrational.

8. *Counterexample:* $\sqrt{2}$ is irrational. Also $\sqrt{2} - \sqrt{2} = 0$ and 0 is rational because $0 = 0/1$. Thus $\exists$ irrational numbers whose difference is rational.

10. *Counterexample:* Let $r = 0$ and $s = \sqrt{2}$. Then r is rational and s is irrational and $r/s = 0/\sqrt{2} = 0$, which is rational because $0 = 0/1$.

11. *Counterexample:* Both $\sqrt{2}$ and $2 - \sqrt{2}$ are positive (because $2 > \sqrt{2}$) and both are irrational (by Theorem 3.7.1 and exercise 8 of Section 3.6). Furthermore, $\sqrt{2} + (2 - \sqrt{2}) = 2$, which is rational because $2 = 2/1$. Thus $\exists$ positive irrational numbers whose sum is rational.

12. *Counterexample:* $\sqrt{2}$ is irrational. Also $\sqrt{2} \cdot \sqrt{2} = 2$ and 2 is rational because $2 = 2/1$. Thus $\exists$ irrational numbers whose product is rational.

13. *Counterexample:* Let $n = 64$. Then n is a perfect square because $64 = 8^2$, but $\sqrt[3]{64} = 4$ which is not irrational because $4 = 4/1$.

14. The sentence is true when $x = 2$ because 2 is rational and $\sqrt{2}$ is irrational, but it is false when $x = 4$ because both 4 and $\sqrt{4} = 2$ are rational. Thus the sentence is sometimes true and sometimes false.

15. a. *Proof (by contraposition):* Let n be any integer such that n is not even. *[We must show that n^3 is not even.]* By Theorem 3.6.2 n is odd, and so n^3 is also odd (by Example 3.2.3 (#3) applied twice). Thus (again by Theorem 3.6.2), n^3 is not even *[as was to be shown]*.

b. *Proof:* Suppose not. That is, suppose $\sqrt[3]{2}$ is rational. By definition of rational, $\sqrt[3]{2} = a/b$ for some integers a and b with $b \neq 0$. By cancelling any common factors if necessary, we may assume that a and b have no common factors. Cubing both sides of the equation $\sqrt[3]{2} = a/b$ gives $2 = a^3/b^3$, and so $2b^3 = a^3$. Thus a^3 is even. By part (a) of this questions, a is even, and thus $a = 2k$ for some integer k. By substitution $a^3 = (2k)^3 = 8k^3 = 2b^3$, and so $b^3 = 4k^3 = 2(2k^3)$. It follows that b^3 is even, and hence (also by part (a)) b is even. Thus both a and b are even which contradicts the assumption that a and b have no common factor. Therefore, the supposition is false, and $\sqrt[3]{2}$ is irrational.

17. *Example:* Let $d = 4$ and $n = 2$. Then $d \mid n^2$ because $4 \mid 4$ (since $\frac{4}{4}$ is an integer), but $d \nmid n$ because $4 \nmid 2$ (since $\frac{2}{4}$ is not an integer).

18. *Proof:* Suppose that a and d are integers with $d > 0$ and that q_1, q_2, r_1, and r_2 are integers such that $a = dq_1 + r_1$ and $a = dq_2 + r_2$, where $0 \leq r_1 < d$ and $0 \leq r_2 < d$. *[We must show that $r_1 = r_2$ and $q_1 = q_2$.]* Then $dq_1 + r_1 = dq_2 + r_2$, and so $r_2 - r_1 = dq_1 - dq_2 = d(q_1 - q_2)$. This implies

that $d \mid (r_2 - r_1)$ because $q_1 - q_2$ is an integer (being a difference of integers). But both r_1 and r_2 lie between 0 and d. Thus the difference of $r_2 - r_1$ lies between $-d$ and d. *[For, by properties T22 and T25 of Appendix A, if $0 \le r_1 < d$ and $0 \le r_2 < d$, then multiplying the first inequality by -1 gives $0 \ge -r_1 > -d$ or, equivalently, $-d < -r_1 \le 0$. And adding $-d < -r_1 \le 0$ and $0 \le r_2 < d$ gives $-d < r_2 - r_1 < d$.]* Since $r_2 - r_1$ is a multiple of d and yet lies between $-d$ and d, the only possibility is that $r_2 - r_1 = 0$, or, equivalently, that $r_1 = r_2$. Substituting back into the original expressions for a and equating the two gives $dq_1 + r_1 = dq_2 + r_1$ [because $r_1 = r_2$]. Subtracting r_1 from both sides gives $dq_1 = dq_2$, and since $d \ne 0$, we have that $q_1 = q_2$. Hence, $r_1 = r_2$ and $q_1 = q_2$, as was to be shown.

19. *Lemma:* For all integers a, if $5 \mid a^2$ then $5 \mid a$.

    Proof by contradiction: Suppose there exists an integer a such that $5 \mid a^2$ and $5 \nmid a$. Because $5 \mid a^2$, $a^2 = 5q$ for some integer q, and by the quotient-remainder theorem with $d = 5$, we have that $a = 5k$ or $a = 5k + 1$ or $a = 5k + 2$ or $a = 5k + 3$ or $a = 5k + 4$. But $a \ne 5k$ for any integer k because $5 \nmid a$, and thus there are only four cases to consider.

    Case 1 ($a = 5k + 1$ for some integer k): In this case $a^2 = (5k + 1)^2 = 25k^2 + 10k + 1 = 5(5k^2 + 2k) + 1$. Let $s = 5k^2 + 2k$. Then s is an integer because it is a sum of products of integers. It follows that $a^2 = 5q = 5s + 1$ for some integers q and s. But this is contradicts the result of exercise 18.

    Case 2 ($a = 5k + 2$ for some integer k): In this case $a^2 = (5k + 2)^2 = 25k^2 + 20k + 4 = 5(5k^2 + 4k) + 4$. Let $s = 5k^2 + 4k$. Then s is an integer because it is a sum of products of integers. It follows that $a^2 = 5q = 5s + 4$ for some integers q and s. But this is contradicts the result of exercise 18.

    Case 3 ($a = 5k + 3$ for some integer k): In this case $a^2 = (5k + 3)^2 = 25k^2 + 30k + 9 = 25k^2 + 30k + 5 + 4 = 5(5k^2 + 6k + 1) + 4$. Let $s = 5k^2 + 6k + 1$. Then s is an integer because it is a sum of products of integers. It follows that $a^2 = 5q = 5s + 4$ for some integers q and s. But this is contradicts the result of exercise 18.

    Case 4 ($a = 5k + 4$ for some integer k): In this case $a^2 = (5k + 4)^2 = 25k^2 + 40k + 16 = 25k^2 + 40k + 15 + 1 = 5(5k^2 + 8k + 3) + 1$. Let $s = 5k^2 + 8k + 3$. Then s is an integer because it is a sum of products of integers. It follows that $a^2 = 5q = 5s + 1$ for some integers q and s. But this is contradicts the result of exercise 18.

    Hence in all four possible cases, a contradiction is reached, which shows that the supposition is false and the given statement is true.

    Proof that $\sqrt{5}$ is irrational: Suppose not. Suppose $\sqrt{5}$ is rational. *[We must derive a contradiction.]* By definition of rational, $\exists$ integers m and n with $\sqrt{5} = m/n$ and $n \ne 0$. Without loss of generality, we may assume that m and n have no common divisors. *[by dividing m and n by any common divisors if necessary.]* Squaring both sides of the equation above gives $5 = m^2/n^2$, or, equivalently, $m^2 = 5n^2$. Since n^2 is an integer, $5 \mid m^2$ by definition of divisibility. It follows that $5 \mid m$ (by the lemma), and so by definition of divisibility there exists an integer k such that $m = 5k$. Substituting into $m^2 = 5n^2$ gives $(5k)^2 = 5n^2$, and so $25k^2 = 5n^2$, which implies that $5k^2 = n^2$. Since k^2 is an integer, $5 \mid n^2$ by definition of divisibility. It follows that $5 \mid n$ (by the lemma). Thus 5 is a common divisor of m and n. But this contradicts the assumption that m and n have no common divisors. *[Hence the supposition is false and the statement is true.]*

20. *Proof:* Suppose not. That is, suppose $\exists$ an integer a such that $9 \mid (a^2 - 3)$. *[We must derive a contradiction.]* By definition of divisibility, $a^2 - 3 = 9b$ for some integer b. Then $a^2 = 9b + 3 = 3(3b + 1)$, and so a^2 is divisible by 3. Hence a is divisible by 3 (by exercise 16b). By definition of divisibility, $a = 3c$ for some integer c. Substituting into the equation $a^2 - 3 = 9b$ gives $(3c)^2 - 3 = 9c^2 - 3 = 9b$, and so $9c^2 = 9b + 3$. Dividing by 3 gives $3c^2 = 3b + 1$. Since c^2 is an integer, this implies that $3b + 1$ is divisible by 3, which contradicts the result of exercise 16a (and also of exercise18). *[Hence the supposition is false and the statement is true.]*

21. *b. Proof:* Suppose not. That is, suppose $\sqrt{2}$ is rational. *[We will show that this supposition leads to a contradiction.]* By definition of rational, we may write $\sqrt{2} = a/b$ for some integers a and b with $b \neq 0$. Then $2 = a^2/b^2$, and so $a^2 = 2b^2$. Consider the prime factorizations for a^2 and for $2b^2$. By the unique factorization theorem, these factorizations are unique except for the order in which the factors are written down. Now because every prime factor of a occurs twice in the prime factorization of a^2, the prime factorization of a^2 contains an even number of 2's. If 2 is a factor of a, then this even number is positive, and if 2 is not a factor of a, then this even number is 0. On the other hand, because every prime factor of b occurs twice in the prime factorization of b^2, the prime factorization of $2b^2$ contains an odd number of 2's. Therefore, the equation $a^2 = 2b^2$ cannot be true. So the supposition is false, and hence $\sqrt{2}$ is irrational.

22. *Proof:* Suppose not. Suppose $\exists$ an integer n such that n is not a perfect square and $\sqrt{n}$ is rational. *[We must derive a contradiction.]* By definition of rational, there exist integers a and b such that $\sqrt{n} = a/b$ (*) and $b \neq 0$. Without loss of generality, we may assume that a and b have no common divisors *[by dividing a and b by any common divisors if necessary]*. Squaring both sides of equation (*) gives $n = a^2/b^2$, and multiplying by b^2 gives $b^2 n = a^2$. By the unique factorization theorem, a, b, and n have representations as products of primes that are unique except for the order in which the prime factors are written down. By the laws of exponents, a^2 and b^2 are products of the same prime numbers as a and b respectively, each written twice. Consequently, each prime factor in a^2 and in b^2 occurs an even number of times. Since n is not a perfect square, some prime factor in n occurs an odd number of times (again by the laws of exponents). It follows that this same prime factor occurs an odd number of times in the product nb^2 (because all prime factors in b^2 occur an even number of times). Since $nb^2 = a^2$, a^2 contains a prime factor that occurs an odd number of times. This contradicts the fact that every prime factor of a^2 occurs an even number of times. *[Hence the supposition is false and the statement is true.]*

23. *Proof 1:* Suppose not. Suppose $\sqrt{2} + \sqrt{3}$ is rational. *[We must derive a contradiction.]* By definition of rational, $\sqrt{2} + \sqrt{3} = \dfrac{a}{b}$ for some integers a and b with $b \neq 0$. Squaring both sides gives $2 + 2 \cdot \sqrt{2} \cdot \sqrt{3} + 3 = \dfrac{a^2}{b^2}$. Then $2\sqrt{6} = \dfrac{a^2}{b^2} - 5$, and so $\sqrt{6} = \dfrac{a^2 - 5b^2}{2b^2}$. Now $a^2 - 5b^2$ and $2b^2$ are both integers (because products and differences of integers are integers) and $2b^2 \neq 0$ (by the zero product property). Therefore, $\sqrt{6}$ is rational by definition of rational. But $\sqrt{6}$ is irrational by exercise 22 (since 6 is not a perfect square), and so a contradiction has been reached. *[Hence the supposition is false and the statement is true.]*

    Proof 2: Suppose not. Suppose $\sqrt{2} + \sqrt{3}$ is rational. *[We must derive a contradiction.]* By definition of rational, $\sqrt{2} + \sqrt{3} = \dfrac{a}{b}$ for some integers a and b with $b \neq 0$. Also $a \neq 0$ because $a = b(\sqrt{2} + \sqrt{3})$ and both b and $\sqrt{2} + \sqrt{3}$ are nonzero. Subtracting $\sqrt{2}$ from both sides gives $\sqrt{3} = \dfrac{a}{b} - \sqrt{2}$, and squaring both sides of this equation yields $3 = \dfrac{a^2}{b^2} - 2\sqrt{2}\dfrac{a}{b} + 2$. Subtracting 2 from both sides and multiplying both sides by b^2 gives $b^2 = a^2 - 2ab\sqrt{2}$, and solving for $\sqrt{2}$ shows that $\sqrt{2} = \dfrac{a^2 - b^2}{2ab}$. But both the numerator and the denominator of this fraction are integers because products and differences of integers are integers, and the denominator is nonzero by the zero product property. Thus $\sqrt{2}$ is rational by definition of rational. But $\sqrt{2}$ is irrational by Theorem 3.7.1, and so a contradiction has been reached. *[Hence the supposition is false and the statement is true.]*

24. *Proof:* Suppose not. That is, suppose that $\log_5(2)$ is rational. *[We will show that this supposition leads to a contradiction.]* By definition of rational, $\log_5(2) = a/b$ for some integers a and b with $b \neq 0$. Since logarithms are always positive, we may assume that a and b are both positive. By definition of logarithm, $5^{a/b} = 2$. Raising both sides to the bth power gives

$5^a = 2^b$. Let $N = 5^a = 2^b$. Since $b \geq 0$, $N > 2^0 = 1$. Thus we may consider the prime factorization of N. Because $N = 5^a$, the prime factors of N are all 5. On the other hand, because $N = 2^b$, the prime factors of N are all 2. This contradicts the unique factorization theorem which states that the prime factors of any integer greater than 1 are unique except for the order in which they are written. Hence the supposition is false, and so $\log_5(2)$ is irrational.

25. The given equation shows that when N is divided by any of the numbers 2, 3, 5, or 7, the remainder is 1. $N = 211$, which is prime.

26. We can deduce that $p = 3$.
    Proof: Let a be any integer, and let p be any prime number such that $p \mid a$ and $p \mid (a+3)$. By definition of divisibility, $a = pr$ and $a + 3 = ps$ for some integers r and s. Then $3 = (a+3) - a = ps - pr = p(s - r)$. But $s - r$ is an integer (because it is a difference of integers), and so by definition of divisibility $p \mid 3$. But since 3 is a prime number, its only positive divisors are 1 and itself. So $p = 1$ or $p = 3$. However, since p is a prime number, $p \neq 1$. Hence $p = 3$.

27. *a.* The following are all prime numbers: $N_1 = 2 + 1 = 3$, $N_2 = 2 \cdot 3 + 1 = 7$, $N_3 = 2 \cdot 3 \cdot 5 + 1 = 31$, $N_4 = 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$, $N_5 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$. However, $N_6 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$. Thus the smallest non-prime integer of the given form is 30,031.

    b. Each of N_1, N_2, N_3, N_4, and N_5 is prime, and so each is its own smallest prime divisor. Thus $q_1 = N_1$, $q_2 = N_2$, $q_3 = N_3$, $q_4 = N_4$, and $q_5 = N_5$. However, N_6 is not prime and $N_6 = 30031 = 59 \cdot 509$. Since 59 and 509 are primes, the smallest prime divisor of N_6 is $q_6 = 59$.

28. *Proof:* Suppose there are only finitely many prime numbers. Then one is the largest. Call it p. Let $M = p! + 1$. We will show that there is a prime number q such that $q > p$. To see this, note that because all of the integers from 2 through p divide $p!$ and because $p! = M - 1$, then none of the integers from 2 through p divides M (by the same reasoning as in the proof of Proposition 3.7.3). But, by Theorem 3.3.2, some prime number q divides M. Now, since p is the largest prime number, every prime number is a factor of $p!$. So, since q is a prime number, q is a factor of $p!$ Hence q does not divide M. Thus q divides M and q does not divide M, which is a contradiction. Thus the supposition is false, and we conclude that there are infinitely many prime numbers.

29. *Proof:* Suppose $p_1, p_2, \ldots, p_n$ are distinct prime numbers with $p_1 = 2$ and $n > 1$. *[We must show that $p_1 p_2 \cdots p_n + 1 = 4k + 3$ for some integer k.]* Let $N = p_1 p_2 \cdots p_n + 1$. By the quotient-remainder theorem, N can be written in one of the forms $4k$, $4k + 1$, $4k + 2$, or $4k + 3$ for some integer k. Now N is odd (because $p_1 = 2$); hence N equals either $4k + 1$ or $4k + 3$ for some integer k. Suppose $N = 4k + 1$ for some integer k. *[We will show that this supposition leads to a contradiction.]* By substitution, $4k + 1 = p_1 p_2 \cdots p_n + 1$, and so $4k = p_1 p_2 \cdots p_n$. Hence $4 \mid p_1 p_2 \cdots p_n$. But $p_1 = 2$ and all of $p_2, p_3, \ldots, p_n$ are odd (being prime numbers that are greater than 2). Consequently, there is only one factor of 2 in the prime factorization of $p_1 p_2 \cdots p_n$, and so $4 \nmid p_1 p_2 \cdots p_n$. This is a contradiction. Hence the supposition that $N = 4k + 1$ for some integer k is false, and so *[by disjunctive syllogism!]* $N = 4k + 3$ for some integer k *[as was to be shown]*.

30. *Proof:* Suppose n is any integer that is greater than 2. Then $n! - 1$ is an integer that is greater than 2, and so by Theorem 3.3.2 there is a prime number p that divides $n! - 1$. Thus $p \leq n! - 1 < (n!)$. Now either $p > n$ or $p \leq n$. Suppose $p \leq n$. *[We will show that this supposition leads to a contradiction.]* Because $p \leq n$, then $p \mid (n!)$. So $p \mid (n!)$ and also $p \mid (n! - 1)$, and thus (by exercise 16 of Section 3.3) p divides $(n! - (n! - 1))$, which equals 1. But the only divisors of 1 are 1 and -1, and so $p = 1$ or $p = -1$. However since p is prime, $p > 1$. Thus we have reached a contradiction. Hence the supposition that $p \leq n$ is false, and so $p > n$. Therefore, p is a prime number such that $n < p < (n!)$.

31. *a. Proof (by contraposition):* Suppose there is an integer $n > 2$ that is not a power of 2 for which $x^n + y^n = z^n$ has a positive integer solution. Call the solution $x = x_0$, $y = y_0$, and

$z = z_0$. If n is prime, then for some prime number p (namely $p = n$), $x^p + y^p = z^p$ has a positive integer solution and we are done. If n is not prime, then n is divisible by a prime (by Theorem 3.3.2), and so, since n is not a power of 2, there exist a prime number $p > 2$ and an integer k such that $n = kp$. Also since $x = x_0$, $y = y_0$, and $z = z_0$ is a positive integer solution to $x^n + y^n = z^n$, then $x_0^n + y_0^n = z_0^n$. But $n = kp$, and so $x_0^{kp} + y_0^{kp} = z_0^{kp}$, or, equivalently (by the laws of exponents), $(x_0^k)^p + (y_0^k)^p = (z_0^k)^p$. Now x_0^k, y_0^k, and z_0^k are all positive integers (because they are integer powers of positive integers). Consequently, the equation $x^p + y^p = z^p$ has a positive integer solution (namely, x_0^k, y_0^k, and z_0^k).

b. We are to assume Fermat's result that for all integers x, y, and z, $x^4 + y^4 \neq z^4$.

Proof: Suppose the given statement is false. That is, suppose that there exist integers n, x, y, and z such that n is a power of 2, $n > 4$, and $x^n + y^n = z^n$. *[We will show that this supposition leads to a contradiction.]* Because n is a power of 2, $n = 2^k$ for some integer k, and because $n > 4$, $k > 2$. Hence, also, $k - 2 > 0$. By substitution, $x^{2^k} + y^{2^k} = z^{2^k}$. So

$$x^{2^{k-2} \cdot 2^2} + y^{2^{k-2} \cdot 2^2} = z^{2^{k-2} \cdot 2^2}$$

and thus

$$(x^{2^{k-2}})^{2^2} + (y^{2^{k-2}})^{2^2} = (z^{2^{k-2}})^{2^2}, \text{ or, equivalently, } (x^{2^{k-2}})^4 + (y^{2^{k-2}})^4 = (z^{2^{k-2}})^4.$$

Let $x_0 = x^{2^{k-2}}$, $y_0 = y^{2^{k-2}}$, and $z_0 = z^{2^{k-2}}$ Because $k - 2 > 0$, 2^{k-2} is a positive integer, and so each of x_0, y_0, and z_0 is a product of integers and thus is an integer. It follows that x_0, y_0, and z_0 are integers such that $(x_0)^4 + (y_0)^4 = (z_0)^4$, which contradicts the Fermat result we are to assume. Thus the supposition is false, and the given statement is true.

33. *Existence Proof*: When $n = 2$, then $n^2 + 2n - 3 = 2^2 + 2 \cdot 2 - 3 = 5$, which is prime. Thus there is a prime number of the form $n^2 + 2n - 3$, where n is a positive integer.

Uniqueness Proof (by contradiction): Suppose not. By the existence proof above, we know that when $n = 2$, then $n^2 + 2n - 3$ is prime. Suppose there is another positive integer m, not equal to 2, such that $m^2 + 2m - 3$ is prime. *[We must derive a contradiction.]* By factoring, we see that $m^2 + 2m - 3 = (m + 3)(m - 1)$. Now $m \neq 1$ because otherwise $m^2 + 2m - 3 = 0$, which is not prime. Also $m \neq 2$ by supposition. Thus $m > 2$. Consequently, $m + 3 > 5$ and $m - 1 > 1$, and so $m^2 + 2m - 3$ can be written as a product of two positive integers neither of which is 1 (namely $m + 3$ and $m - 1$). This contradicts the supposition that $m^2 + 2m - 3$ is prime. Hence the supposition is false: there is no integer m other than 2 such that $m^2 + 2m - 3$ is prime.

Uniqueness Proof (direct): Suppose m is any positive integer such that $m^2 + 2m - 3$ is prime. *[We must show that $m = 2$.]* By factoring, $m^2 + 2m - 3 = (m + 3)(m - 1)$. Since $m^2 + 2m - 3$ is prime, either $m + 3 = 1$ or $m - 1 = 1$. Now $m + 3 \neq 1$ because m is positive (and if $m + 3 = 1$ then $m = -2$). Thus $m - 1 = 1$, which implies that $m = 2$ *[as was to be shown]*.

35. *Proof (by contradiction)*: Suppose not. Suppose there exist two distinct real number b_1 and b_2 such that for all real numbers r, (1) $b_1 r = r$ and (2) $b_2 r = r$. Then $b_1 b_2 = b_2$ (by (1) with $r = b_1$) and $b_2 b_1 = b_1$ (by (2) with $r = b_2$). Consequently, $b_2 = b_1 b_2 = b_2 b_1 = b_1$ by substitution and the commutative law of multiplication. But this implies that $b_1 = b_2$, which contradicts the supposition that b_1 and b_2 are distinct. *[Thus the supposition is false and there exists at most one real number b such that $br = r$ for all real numbers r.]*

Proof (direct): Suppose b_1 and b_2 are real numbers such that (1) $b_1 r = r$ and (2) $b_2 r = r$ for all real numbers r. By (1) $b_1 b_2 = b_2$, and by the commutative law for multiplication and (2), $b_1 b_2 = b_2 b_1 = b_1$. Since both b_1 and b_2 are equal to $b_1 b_2$, we conclude that $b_1 = b_2$.

Section 3.8

2. $z = 2$

3. *b.* $z = 6$

5. $e = 41/48$

7.

a	59				
d	13				
q	0	1	2	3	4
r	59	46	33	20	7

8. *b.*

A	87	12	2	
q	3			
d		1		
n			0	
p				2

11. $\gcd(7, 21) = 7$

12. *Solution 1*: $\gcd(48, 54) = \gcd(6 \cdot 8, 6 \cdot 9) = 6$

   Solution 2: $\gcd(48, 54) = \gcd(2^4 \cdot 3, 2 \cdot 3^3) = 2 \cdot 3 = 6$

15.

$$\begin{array}{r} 13 \\ 832\overline{)10933} \\ \underline{10816} \\ 117 \end{array}$$ So $10933 = 832 \cdot 13 + 117$, and hence $\gcd(10933, 832) = \gcd(832, 117)$

$$\begin{array}{r} 7 \\ 117\overline{)832} \\ \underline{819} \\ 13 \end{array}$$ So $832 = 117 \cdot 7 + 13$, and hence $\gcd(832, 117) = \gcd(117, 13)$

$$\begin{array}{r} 9 \\ 13\overline{)117} \\ \underline{117} \\ 0 \end{array}$$ So $117 = 13 \cdot 9 + 0$, and hence $\gcd(117, 13) = \gcd(13, 0)$

But $\gcd(13, 0) = 13$. So $\gcd(10933, 832) = 13$.

16.

$$\begin{array}{r} 1 \\ 2431\overline{)4131} \\ \underline{2431} \\ 1700 \end{array}$$

So $4131 = 2431 \cdot 1 + 1700$, and hence $\gcd(4131, 2431) = \gcd(2431, 1700)$

$$\begin{array}{r} 1 \\ 1700\overline{)2431} \\ \underline{1700} \\ 731 \end{array}$$

So $2431 = 1700 \cdot 1 + 731$, and hence $\gcd(2431, 1700) = \gcd(1700, 731)$

$$\begin{array}{r} 2 \\ 731\overline{)1700} \\ \underline{1462} \\ 238 \end{array}$$

So $1700 = 731 \cdot 2 + 238$, and hence $\gcd(1700, 731) = \gcd(731, 238)$

$$\begin{array}{r} 3 \\ 238\overline{)731} \\ \underline{714} \\ 17 \end{array}$$

So $731 = 238 \cdot 3 + 17$, and hence $\gcd(731, 238) = \gcd(238, 17)$

$$\begin{array}{r} 14 \\ 17\overline{)238} \\ \underline{238} \\ 0 \end{array}$$

So $238 = 17 \cdot 14 + 0$, and hence $\gcd(238, 17) = \gcd(17, 0)$

But $\gcd(17, 0) = 17$. So $\gcd(4131, 2431) = 17$.

18.

A	5859						
B	1232						
r	1232	931	301	28	21	7	0
a	5859	1232	931	301	28	21	7
b	1232	931	301	28	21	7	0
gcd							7

19. *Proof*: Let a and b be any positive integers.

Part 1 (proof that if $\gcd(a, b) = a$ then $a \mid b$): Suppose that $\gcd(a, b) = a$. By definition of greatest common divisor, $\gcd(a, b) \mid b$, and so by substitution, $a \mid b$.

Part 2 (proof that if $a \mid b$ then $\gcd(a, b) = a$): Suppose that $a \mid b$. Then since it is also the case that $a \mid a$, a is a common divisor of a and b. Thus by definition of greatest common divisor, $a \leq \gcd(a, b)$. On the other hand, since no integer greater than a divides a, the greatest common divisor of a and b is less than or equal to a. In symbols, $\gcd(a, b) \leq a$. Therefore, since $a \leq \gcd(a, b)$ and $\gcd(a, b) \leq a$, then $\gcd(a, b) = a$.

20. *Lemma*: If a and b are integers, not both zero, and $d = \gcd(a, b)$, then a/d and b/d are integers with no common divisor that is greater than 1.

Proof: Let a and b be integers, not both zero, and let $d = \gcd(a, b)$. By definition of gcd, $d \mid a$ and $d \mid b$. Hence a/d and b/d are integers. Suppose a/d and b/d have a common divisor c that is greater than 1. *[We will derive a contradiction.]* Then $a/d = cr$ and $b/d = cs$ for some integers r and s. It follows that $a = (cd)r$ and $b = (cd)s$, and so $cd \mid a$ and $cd \mid b$. But d is positive because $d \geq 1$, and, since $c > 1$, we have that $cd > d$ *[by T19, Appendix A]*. Thus cd is a common divisor of a and b that is greater than the greatest common divisor of a and b. This is a contradiction. Hence the supposition that a/d and b/d have a common divisor that is greater than 1 is false, and so a/d and b/d have no common divisor that is greater than 1.

Algorithm: Reducing a Fraction
(Input: *A,B*; Output: *C,D*)

[Given two integers A and B with $B \neq 0$, this algorithm finds integers C and D so that $A/B = C/D$ and C and D have no common divisor that is greater than 1. The algorithm first adjusts for the fact that A/B may be negative by setting variables $a = |A|$ and $b = |B|$. Then it calls the Euclidean algorithm to compute $\gcd(a,b)$ and sets $c = a$ div $\gcd(a,b)$ and $d = b$ div $\gcd(a,b)$. By the lemma above, c and d are integers that are divisible by $\gcd(a,b)$. Consequently,

$$\frac{c}{d} = \frac{a \; div \; \gcd(a,b)}{b \; div \; \gcd(a,b)} = \frac{\dfrac{a}{\gcd(a,b)}}{\dfrac{b}{\gcd(a,b)}} = \frac{a}{b}.$$

It also follows from the lemma that c and d have no common factor that is greater than 1. Thus c/d is the reduced form of a/b. Finally the sign of the reduced fraction is adjusted: C is set equal to $-c$ if A/B is less than 0 and to c if A/B is greater than or equal to 0, and D is set equal to d.]

Input: A, B *[integers with $B \neq 0$]*

Algorithm Body:

> if $A/B < 0$ then *sign* $:= -1$ else *sign* $:= 1$
>
> if $A < 0$ then $a := -A$ else $a := A$
>
> if $B < 0$ then $b := -B$ else $b := B$
>
> $gcd := \gcd(a,b)$
>
> *[The value of gcd can be computed by calling the Euclidean algorithm.]*
>
> $c := a$ div gcd, $d := b$ div gcd
>
> *[The values of c and d can be computed by calling the division algorithm.]*
>
> *[When execution reaches this point, $a/b = c/d$ and c and d have no common divisors that are greater than 1.]*
>
> $C := sign\cdot c$, $D := d$
>
> *[When execution reaches this point, $A/B = C/D$ and C and D have no common divisors that are greater than 1.]*

Output: C, D *[integers with $D \neq 0$]*

21. *Proof:* Suppose a and b are any integers with $b \neq 0$, and suppose q and r are any integers such that $a = bq + r$. *[We must show that $\gcd(b,r) \leq \gcd(a,b)$.]*

    Step 1 (proof that any common divisor of b and r is also a common divisor of a and b): Let c be a common divisor of b and r. Then $c \mid b$ and $c \mid r$, and so by definition of divisibility, $b = nc$ and $r = mc$ for some integers n and m. Now substitute into the equation $a = bq + r$ to obtain $a = (nc)q + mc = c(nq + m)$. But $nq + m$ is an integer, and so by definition of divisibility $c \mid a$. Now we already know that $c \mid b$; hence c is a common divisor of a and b.

    Step 2 (proof that $\gcd(b,r) \leq \gcd(a,b)$): By step 1, every common divisor of b and r is a common divisor of a and b. It follows that the greatest common divisor of b and r is a common divisor of a and b. But then $\gcd(b,r)$ (being one of the common divisors of a and b) is less than or equal to the greatest common divisor of a and b: $\gcd(b,r) \leq \gcd(a,b)$.

22. *a.* Suppose a and d are positive integers and q and r are integers such that $a = dq + r$ and $0 < r < d$. Then $-a = -dq - r = -dq - d + d - r = d(-q-1) + (d-r) = d(-(q+1)) + (d-r)$. Also since $0 < r < d$, then $0 > -r > -d$ (by multiplying all parts of the inequality by

−1). Adding d to all parts of the inequality gives $d + 0 > d + (-r) > d + (-d)$, and hence $d > d - r > 0$.

b. If the input a is negative, then use the current algorithm with input $-a$ to obtain a quotient q and a remainder r so that $-a = dq+r$ and $0 \le r < d$. If $r = 0$, then $a = -(-a) = -dq = d(-q)$, and thus the quotient of the division of a by d is $-q$ and the remainder is 0. If $r > 0$, then by part (a), $a = -(-a) = d(-(q+1)) + (d - r)$ and $0 < d - r < d$, and thus the quotient of the division of a by d is $-(q + 1)$ and the remainder is $d - r$. Hence Algorithm 3.8.1 can be modified as follows.

Algorithm Body:

> **if** $a < 0$ **then** *sign* $:= -1$, $a := -a$ **else** *sign* $:= 1$
>
> *[Same steps as the body of Algorithm 3.8.1.]*
>
> **if** *sign* $= -1$ **then if** $r = 0$
>
> > > **then** $q := -q$
> > >
> > > **else** $q := -(q + 1)$, $r := d - r$

23. *a.* Note that this exercise statement is a converse to Theorem 3.5.3 (p. 169), but it is more general because a (n in Theorem 3.5.3) may be negative.

b. $r := B$, $a := A$, $b := B$

> **while** $(b \ne 0)$
>
> > $r := a - \lfloor a/b \rfloor \cdot b$
> >
> > $a := b$
> >
> > $b := r$
>
> **end while**
>
> $gcd := a$

24. *a. Proof:* Suppose a and b are integers and $a \ge b > 0$.   *[We first show that every common divisor of a and b is a common divisor of b and $a - b$, and conversely.]*

Part 1 (proof that every common divisor of a and b is a common divisor of b and $a - b$):

Suppose $d \mid a$ and $d \mid b$. Then $d \mid (a - b)$ by exercise 16 of Section 3.3. Hence d is a common divisor of a and $a - b$.

Part 2 (proof that every common divisor of b and $a - b$ is a common divisor of a and b):

Suppose $d \mid b$ and $d \mid (a - b)$. Then by exercise 15 of Section 3.3, $a \mid [b + (a - b)]$. But $b + (a - b) = a$, and so $d \mid a$. Hence d is a common divisor of a and b.

Part 3 (end of proof): Because every common divisor of a and b is a common divisor of b and $a - b$, the greatest common divisor of a and b is a common divisor of b and $a - b$ and so is less than or equal to the greatest common divisor of a and $a - b$. Thus $\gcd(a, b) \le \gcd(b, a - b)$. By similar reasoning, $\gcd(b, a - b) \le \gcd(a, b)$. Therefore, $\gcd(a, b) = \gcd(b, a - b)$.

c.

A	768											
B	348											
a	768	420	72					12				0
b	348			276	204	132	60		48	36	24	12
gcd												12

25. *b.* $\operatorname{lcm}(2^2 \cdot 3 \cdot 5 \, , \, 2^3 \cdot 3^2) = 2^3 \cdot 3^2 \cdot 5 = 360$

c. $\operatorname{lcm}(2800, 6125) = \operatorname{lcm}(2^4 \cdot 5^2 \cdot 7 \, , \, 5^3 \cdot 7^2) = 2^4 \cdot 5^3 \cdot 7^2 = 98,000$

26. The proof given in Appendix B shows that for all positive integers a and b, if $\gcd(a, b) =$ $\text{lcm}(a, b)$, then $a = b$. Thus, to complete the proof of the exercise statement, it remains only to show that for all positive integers a and b, if $a = b$, then $\gcd(a, b) = \text{lcm}(a, b)$. But given any positive integers a and b such that $a = b$, we have $\gcd(a, b) = \gcd(a, a) = a$ and $\text{lcm}(a, b) = \text{lcm}(a, a) = a$, and hence $\gcd(a, b) = \text{lcm}(a, b)$.

27. *Proof*: Let a and b be any positive integers.

    Part 1 (proof that if $\text{lcm}(a, b) = b$ then $a \mid b$): Suppose that $\text{lcm}(a, b) = b$. By definition of least common multiple, $a \mid \text{lcm}(a, b)$, and so by substitution, $a \mid b$.

    Part 2 (proof that if $a \mid b$ then $\text{lcm}(a, b) = b$): Suppose that $a \mid b$. Then since it is also the case that $b \mid b$, b is a common multiple of a and b. Moreover, because b divides any common multiple of both a and b, $\text{lcm}(a, b) = b$.

28. *Proof*: Let a and b be any integers. By definition of greatest common divisor, $\gcd(a, b) \mid a$, and by definition of least common multiple, $a \mid \text{lcm}(a, b)$. Hence by transitivity of divisibility, $\gcd(a, b) \mid \text{lcm}(a, b)$.

29. *Proof*: Let a and b be any positive integers.

    Part 1 (proof that $\gcd(a, b) \cdot \text{lcm}(a, b) \leq ab$): By definition of greatest common divisor, $\gcd(a, b) \mid a$. Hence by definition of divisibility, $a = \gcd(a, b) \cdot k$ for some integer k. Multiplying both sides by b gives $ab = \gcd(a, b) \cdot k \cdot b$, and so $\dfrac{ab}{\gcd(a, b)} = bk$. It follows by definition of divisibility that $b \ \left| \ \left[\dfrac{ab}{\gcd(a, b)}\right]\right.$. An almost exactly identical sequence of steps shows that $a \ \left| \ \left[\dfrac{ab}{\gcd(a, b)}\right]\right.$. Thus by definition of least common multiple, $\text{lcm}(a, b) \ \left| \ \dfrac{ab}{\gcd(a, b)}\right.$. It follows from Example 3.3.3 that $\text{lcm}(a, b) \leq \dfrac{ab}{\gcd(a, b)}$, or, equivalently (because $\gcd(a, b) > 0$), $\gcd(a, b) \cdot \text{lcm}(a, b) \leq ab$.

    Part 2 (proof that $ab \leq \gcd(a, b) \cdot \text{lcm}(a, b)$): By definition of least common multiple, $a \mid \text{lcm}(a, b)$. Hence by definition of divisibility, $\text{lcm}(a, b) = ak$ for some integer k. Multiplying both sides by b gives $b \cdot \text{lcm}(a, b) = ak \cdot b$, and so $b = \left[\dfrac{ab}{\text{lcm}(a, b)}\right] \cdot k$. It follows by definition of divisibility that $\left[\dfrac{ab}{\text{lcm}(a, b)}\right] \ \Big| \ b$. An almost exactly identical sequence of steps shows that $\left[\dfrac{ab}{\text{lcm}(a, b)}\right] \ \Big| \ a$. Thus by definition of greatest common divisor (because $\text{lcm}(a, b) > 0$), $\gcd(a, b) \geq \dfrac{ab}{\text{lcm}(a, b)}$, and so $\gcd(a, b) \cdot \text{lcm}(a, b) \geq ab$, or, equivalently, $ab \leq \gcd(a, b) \cdot \text{lcm}(a, b)$.

    By part 1, $\gcd(a, b) \cdot \text{lcm}(a, b) \leq ab$, and by part 2, $ab \leq \gcd(a, b) \cdot \text{lcm}(a, b)$. Therefore, $\gcd(a, b) \cdot \text{lcm}(a, b) = ab$.

Chapter 4: Sequences and Mathematical Induction

The first section of this chapter introduces the notation for sequences, summations, products, and factorial. Students have two main difficulties with this material. One is learning to recognize patterns so as to be able, for instance, to transform expanded versions of sums into summation notation. The other is learning how to handle subscripts, particularly to change variables for summations and to distinguish index variables from variables that are constant with respect to a summation.

The second, third, and fourth sections of this chapter treat mathematical induction. The ordinary form is discussed in Sections 4.2 and 4.3 and the strong form in Section 4.4. Because of the importance of mathematical induction in discrete mathematics, a wide variety of examples is given so that students will become comfortable with using the technique in many different situations. Section 8.4 introduces general recursive definitions and structural induction and can be covered along with chapter 4 if a few additional terms are defined.

Students may find it helpful for you to relate the logic of ordinary mathematical induction to the logic discussed in Chapters 1 and 2. The main point is that the inductive step establishes the truth of a sequence of if-then statements. Together with the basis step, this sequence gives rise to a chain of inferences that lead to the desired conclusion. More formally:

Suppose
1. $P(1)$ is true; and
2. for all integers $k \geq 1$, if $P(k)$ is true then $P(k+1)$ is true.

The truth of statement (2) implies, according to the law of universal instantiation, that no matter what particular integer $k \geq 1$ is substituted in place of k, the statement "If $P(k)$ then $P(k+1)$" is true. The following argument, therefore, has true premises, and so by modus ponens it has a true conclusion:

If $P(1)$ then $P(2)$.	by 2 and universal instantiation
$P(1)$	by 1
$\therefore \quad P(2)$	by modus ponens

Similar reasoning gives the following chain of arguments, each of which has a true conclusion by modus ponens:

$$\text{If } P(2) \text{ then } P(3).$$
$$P(2)$$
$$\therefore \quad P(3)$$
$$\text{If } P(3) \text{ then } P(4).$$
$$P(3)$$
$$\therefore \quad P(4)$$
$$\text{If } P(4) \text{ then } P(5).$$
$$P(4)$$
$$\therefore \quad P(5)$$
And so forth.

Thus no matter how large a positive integer n is specified, the truth of $P(n)$ can be deduced as the final conclusion of a (possibly very long) chain of arguments continuing those shown above.

Note that in Section 4.2 the formula for the sum of the geometric series is written as $\dfrac{r^{n+1} - 1}{r - 1}$ because in discrete mathematics r is commonly greater than one, making this version of the formula the more convenient.

The concluding section of the chapter applies the technique of mathematical induction to proving algorithm correctness. It is intended to be an introduction to the subject and contains references directing students to sources that treat it at length.

Comments on Exercises

Exercise Set 4.1: **#8** and **#9**: These exercises are designed for students already familiar with logarithms. In classes where such familiarity cannot be assumed, the exercises can simply be skipped or students can be referred to the definitions given in Section 7.1.

Exercise Set 4.1: **#49**: This exercise is particularly good preparation for the combinatorial manipulations in Chapter 6.

Exercise Set 4.2:. **#19-28**: These exercises develop skills needed in Section 8.2. **#29**: The mistake made in this proof fragment is surprisingly common.

Exercise Set 4.3 #24-27 and Exercise Set 4.4 #1-9: The skill developed in doing these exercises is used again in Sections 8.2 and 8.3.

Section 4.1

2. $b_1 = \dfrac{5-1}{5+1} = \dfrac{4}{6}, \quad b_2 = \dfrac{5-2}{5+2} = \dfrac{3}{7}, \quad b_3 = \dfrac{5-3}{5+3} = \dfrac{2}{8}, \quad b_4 = \dfrac{5-4}{5+4} = \dfrac{1}{9}$

4. $d_0 = 1 + \left(\dfrac{1}{2}\right)^0 = 1 + 1 = 2, \quad d_1 = 1 + \left(\dfrac{1}{2}\right)^1 = 1 + \dfrac{1}{2} = \dfrac{3}{2}, \quad d_2 = 1 + \left(\dfrac{1}{2}\right)^2 = 1 + \dfrac{1}{4} = \dfrac{5}{4},$

$d_3 = 1 + \left(\dfrac{1}{2}\right)^3 = 1 + \dfrac{1}{8} = \dfrac{9}{8}$

6. $f_1 = \left\lfloor \dfrac{1}{4} \right\rfloor \cdot 4 = 0 \cdot 4 = 0, \quad f_2 = \left\lfloor \dfrac{2}{4} \right\rfloor \cdot 4 = 0 \cdot 4 = 0, \quad f_3 = \left\lfloor \dfrac{3}{4} \right\rfloor \cdot 4 = 0 \cdot 4 = 4,$

$f_4 = \left\lfloor \dfrac{4}{4} \right\rfloor \cdot 4 = 1 \cdot 4 = 4$

7. $a_0 = 2 \cdot 0 + 1 = 1, \quad a_1 = 2 \cdot 1 + 1 = 3, \quad a_2 = 2 \cdot 2 + 1 = 5, \quad a_3 = 2 \cdot 3 + 1 = 7$
$b_0 = (0-1)^3 + 0 + 2 = 1, \quad b_1 = (1-1)^3 + 1 + 2 = 3, \quad b_2 = (2-1)^3 + 2 + 2 = 5,$
$b_3 = (3-1)^3 + 3 + 2 = 13$
So $a_0 = b_0, \quad a_1 = b_1,$ and $a_2 = b_2,$ but $a_3 \neq b_3.$

9.

h_1	$=$	$1 \cdot \lfloor \log_2 1 \rfloor$	$=$	$1 \cdot 0$
h_2	$=$	$2 \cdot \lfloor \log_2 2 \rfloor$	$=$	$2 \cdot 1$
h_3	$=$	$3 \cdot \lfloor \log_2 3 \rfloor$	$=$	$3 \cdot 1$
h_4	$=$	$4 \cdot \lfloor \log_2 4 \rfloor$	$=$	$4 \cdot 2$
h_5	$=$	$5 \cdot \lfloor \log_2 5 \rfloor$	$=$	$5 \cdot 2$
h_6	$=$	$6 \cdot \lfloor \log_2 6 \rfloor$	$=$	$6 \cdot 2$
h_7	$=$	$7 \cdot \lfloor \log_2 7 \rfloor$	$=$	$7 \cdot 2$
h_8	$=$	$8 \cdot \lfloor \log_2 8 \rfloor$	$=$	$8 \cdot 3$
h_9	$=$	$9 \cdot \lfloor \log_2 9 \rfloor$	$=$	$9 \cdot 3$
h_{10}	$=$	$10 \cdot \lfloor \log_2 10 \rfloor$	$=$	$10 \cdot 3$
h_{11}	$=$	$11 \cdot \lfloor \log_2 11 \rfloor$	$=$	$11 \cdot 3$
h_{12}	$=$	$12 \cdot \lfloor \log_2 12 \rfloor$	$=$	$12 \cdot 3$
h_{13}	$=$	$13 \cdot \lfloor \log_2 13 \rfloor$	$=$	$13 \cdot 3$
h_{14}	$=$	$14 \cdot \lfloor \log_2 14 \rfloor$	$=$	$14 \cdot 3$
h_{15}	$=$	$15 \cdot \lfloor \log_2 15 \rfloor$	$=$	$15 \cdot 3$

When n is an integral power of 2, h_n is n times the exponent of that power. For instance, $8 = 2^3$ and $h_8 = 8 \cdot 3$. If m and n are integers and $2^m \leq 2^n < 2^{m+1}$, then $h_n = n \cdot m$.

Exercises 10-16 have more than one correct answer.

13. $a_n = \dfrac{1}{n} - \dfrac{1}{n+1}$ for all integers $n \geq 1$

15. $a_n = (-1)^n \left(\dfrac{n-1}{n} \right)$ for all integers $n \geq 1$

16. $a_n = 3 \cdot 2^n$ for all integers $n \geq 0$

17. $a_n = \lfloor n/2 \rfloor$

18. e. $\prod_{k=2}^{2} a_k = a_2 = -2$

21. $\displaystyle\sum_{m=0}^{3} \dfrac{1}{2^m} = \dfrac{1}{2^0} + \dfrac{1}{2^1} + \dfrac{1}{2^2} + \dfrac{1}{2^3} = 1 + \dfrac{1}{2} + \dfrac{1}{4} + \dfrac{1}{8} = \dfrac{15}{8}$

22. $\prod_{j=0}^{4} (-1)^j = (-1)^0 \cdot (-1)^1 \cdot (-1)^2 \cdot (-1)^3 \cdot (-1)^4 = 1 \cdot (-1) \cdot 1 \cdot (-1) \cdot 1 = 1$

24. $\displaystyle\sum_{j=0}^{0} (j+1) \cdot 2^j = (0+1) \cdot 2^0 = 1 \cdot 1 = 1$

25. $\sum_{k=2}^{2} \left(1 - \frac{1}{k} \right) = 1 - \frac{1}{2} = \frac{1}{2}$

26. $\sum_{k=-1}^{1} (k^2 + 3) = ((-1)^2 + 3) + (0^2 + 3) + (1^2 + 3) = 4 + 3 + 4 = 11$

28. $\displaystyle\prod_{i=2}^{5} \dfrac{i(i+2)}{(i-1)(i+1)} = \dfrac{2 \cdot 4}{1 \cdot 3} \cdot \dfrac{3 \cdot 5}{2 \cdot 4} \cdot \dfrac{4 \cdot 6}{3 \cdot 5} \cdot \dfrac{5 \cdot 7}{4 \cdot 6} = \dfrac{5 \cdot 7}{1 \cdot 3} = \dfrac{35}{3}$

30. $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + n \cdot (n+1)$

31. $\dfrac{1}{0!} + \dfrac{1}{1!} + \dfrac{1}{2!} + \cdots + \dfrac{1}{n!}$

Exercises 29-41 have more than one correct answer.

33. $\displaystyle\sum_{k=1}^{5} (-1)^{k+1} (k^3 - 1)$

34. $\displaystyle\prod_{i=2}^{4} (i^2 - 1)$

37. $\displaystyle\prod_{j=1}^{4} (1 - t^j)$

39. $\displaystyle\sum_{k=1}^{n} \dfrac{k}{(k+1)!}$

41. $\displaystyle\sum_{k=0}^{n-1} \dfrac{n-k}{(k+1)!}$

43. $\dfrac{6!}{8!} = \dfrac{6!}{8 \cdot 7 \cdot 6!} = \dfrac{1}{56}$

44. $\dfrac{4!}{0!} = \dfrac{4!}{1} = 24$

47. $\dfrac{n!}{(n-2)!} = \dfrac{n(n-1)(n-2)!}{(n-2)!} = n(n-1)$ (assuming $n \geq 2$)

50. $$\frac{n!}{(n-k+1)!} = \frac{n(n-1)\cdots(n-k+2)(n-k+1)(n-k)\cdots3\cdot2\cdot1}{(n-k+1)(n-k)(n-k-1)\cdots3\cdot2\cdot1}$$

$$= n(n-1)\cdots(n-k+2) \qquad (\text{assuming } n-k+1 \geq 0)$$

51. *b. Proof*: Let n and k be integers with $n \geq 2$ and $2 \leq k \leq n$. Now $n!$ is the product of all the integers from 1 to n, and so since $n \geq 2$ and $2 \leq k \leq n$, k is a factor of $n!$. That is $n! = kr$ for some integer r. By substitution $n! + k = kr + k = k(r+1)$. But $r+1$ is an integer because r is. By definition of divisibility, therefore, $n! + k$ is divisible by k.

c. Yes. If m is any integer that is greater than or equal to 2, then none of the terms of the following sequence of integers is prime: $m! + 2, m! + 3, m! + 4, \ldots, m! + m$. The reason is that each has the form $m! + k$ for an integer k with $2 \leq k \leq m$, and for each such k, by part (b) $m! + k$ is divisible by k.

53. When $k = 1$, $i = 1 + 1 = 2$. When $k = n$, $i = n + 1$. Since $i = k + 1$, then $k = i - 1$. So $\frac{k^2}{k+4} = \frac{(i-1)^2}{(i-1)+4} = \frac{(i-1)^2}{i+3}$. Therefore, $\prod_{k=1}^{n}(\frac{k^2}{k+4}) = \prod_{i=2}^{n+1}(\frac{(i-1)^2}{i+3})$.

56. When $i = 1$, $j = 1 - 1 = 0$. When $i = n - 1$, $j = n - 2$. Since $j = i - 1$, then $i = j + 1$. So $\frac{i}{(n-i)^2} = \frac{j+1}{(n-(j+1))^2} = \frac{j+1}{(n-j-1)^2}$. Therefore, $\sum_{i=1}^{n-1}(\frac{i}{(n-i)^2}) = \sum_{j=0}^{n-2}(\frac{j+1}{(n-j-1)^2})$.

57. When $i = n$, $j = n - 1$. When $i = 2n$, $j = 2n - 1$. Since $j = i - 1$, then $i = j + 1$. So $\frac{n-i+1}{n+i} = \frac{n-(j+1)+1}{n+j+1} = \frac{n-j}{n+j+1}$. Therefore, $\prod_{i=n}^{2n}(\frac{n-i+1}{n+i}) = \prod_{j=n-1}^{2n-1}(\frac{n-j}{n+j+1})$.

59. By Theorem 4.1.1,

$$2 \cdot \sum_{k=1}^{n}(3k^2 + 4) + 5 \cdot \sum_{k=1}^{n}(2k^2 - 1) = \sum_{k=1}^{n}2(3k^2 + 4) + \sum_{k=1}^{n}5(2k^2 - 1)$$

$$= \sum_{k=1}^{n}(6k^2 + 8) + \sum_{k=1}^{n}(10k^2 - 5)$$

$$= \sum_{k=1}^{n}(6k^2 + 8 + 10k^2 - 5)$$

$$= \sum_{k=1}^{n}(16k^2 + 3).$$

60. By Theorem 4.1.1, $\left(\prod_{k=1}^{n}(\frac{k}{k+1})\right)\left(\prod_{k=1}^{n}(\frac{k+1}{k+2})\right) = \prod_{k=1}^{n}(\frac{k}{k+1})(\frac{k+1}{k+2}) = \prod_{k=1}^{n}(\frac{k}{k+2}).$

61. (1) For $m = 1$ and $n = 4$, the expanded form of the equation is

$$(a_1 + a_2 + a_3 + a_4) + (b_1 + b_2 + b_3 + b_4) = (a_1 + b_1) + (a_2 + b_2) + (a_3 + b_3) + (a_4 + b_4).$$

The two sides of this equation are equal by repeated application of the associative and commutative laws of addition.

(2) For $m = 1$ and $n = 4$, the expanded form of the equation is

$$c(a_1 + a_2 + a_3 + a_4) = ca_1 + ca_2 + ca_3 + ca_4.$$

The two sides of this equation are equal by repeated application of the associative law of addition and the distributive law.

(3) For $m = 1$ and $n = 4$, the expanded form of the equation is

$$(a_1 a_2 a_3 a_4)(b_1 b_2 b_3 b_4) = (a_1 b_1)(a_2 b_2)(a_3 b_3)(a_4 b_4).$$

The two sides of this equation are equal by repeated application of the associative and commutative laws of multiplication.

62. $b.$ $m + 1$, $sum + a[j - 1]$

64.

0		remainder $= r[6] = 1$
2⌐1		remainder $= r[5] = 1$
2⌐3		remainder $= r[4] = 0$
2⌐6		remainder $= r[3] = 0$
2⌐12		remainder $= r[2] = 0$
2⌐24		remainder $= r[1] = 1$
2⌐49		remainder $= r[0] = 0$
2⌐98		Hence $98_{10} = 1100010_2$.

65.

0		remainder $= r[7] = 1$
2⌐1		remainder $= r[6] = 1$
2⌐3		remainder $= r[5] = 0$
2⌐6		remainder $= r[4] = 0$
2⌐12		remainder $= r[3] = 1$
2⌐25		remainder $= r[2] = 1$
2⌐51		remainder $= r[1] = 0$
2⌐102		remainder $= r[0] = 1$
2⌐205		Hence $205_{10} = 11001101_2$.

67.

a	28					
i	0	1	2	3	4	5
q	28	14	7	3	1	0
$r[0]$	0					
$r[1]$		0				
$r[2]$			1			
$r[3]$				1		
$r[4]$					1	

68.

a	44						
i	0	1	2	3	4	5	6
q	44	22	11	5	2	1	0
$r[0]$	0						
$r[1]$		0					
$r[2]$			1				
$r[3]$				1			
$r[4]$					0		
$r[5]$						1	

69. Let a nonnegative integer a be given. Divide a by 16 using the quotient-remainder theorem to obtain a quotient $q[0]$ and a remainder $r[0]$. If the quotient is nonzero, divide by 16 again to obtain a quotient $q[1]$ and a remainder $r[1]$. Continue this process until a quotient of 0 is obtained. The remainders calculated in this way are the hexadecimal digits of a:

$$a_{10} = (r[k]r[k-1]\ldots r[2]r[1]r[0])_{16}.$$

71.

$$
\begin{array}{ll}
\overline{0} & \text{R. } 2 = 2_{16} \\
16\overline{2} & \text{R. } 11 = B_{16} \\
16\overline{43} & \text{R. } 5 = 5_{16} \\
16\overline{693} & \qquad \text{Hence } 693_{10} = 2B5_{16}.
\end{array}
$$

72.

$$
\begin{array}{ll}
\overline{0} & \text{R. } 8 = 8_{16} \\
16\overline{8} & \text{R. } 15 = F_{16} \\
16\overline{143} & \text{R. } 13 = D_{16} \\
16\overline{2301} & \qquad \text{Hence } 2301_{10} = 8FD_{16}.
\end{array}
$$

73.

Algorithm Decimal to Hexadecimal Conversion Using Repeated Division by 16

[In this algorithm the input is a nonnegative integer a. The aim of the algorithm is to produce a sequence of binary digits $r[0]$, $r[1]$, $r[2]$, $\ldots r[i-1]$ so that the hexadecimal representation of a is $(r[i-1]r[i-2]\ldots r[2]r[1]r[0])_{16}.$]

Input: a *[a nonnegative integer]*

Algorithm Body:

$\qquad q := a, \ i := 0$

$\qquad$ **while** $(i = 0 \text{ or } q \neq 0)$

$\qquad\qquad r[i] := q \bmod 16$

$\qquad\qquad q := q \ div \ 16$

$\qquad\qquad i := i + 1$

$\qquad$ **end while**

[After execution of this step, the values of $r[0]$, $r[1]$, $r[2]$,..., $r[i-1]$ are all integers from 0 to 15 inclusive, and $a_{10} = (r[i-1]r[i-2] \ldots r[2]r[1]r[0])_{16}.$]

Output: $r[0]$, $r[1]$, $r[2]$, $\ldots$, $r[i-1]$ *[a sequence of integers]*

end Algorithm

Section 4.2

2. Let $P(n)$ be the property "A postage of $n\cancel{c}$ can be obtained using $3\cancel{c}$ and $7\cancel{c}$ stamps."

Show that the property is true for $n = 12$: A postage of $12\cancel{c}$ can be obtained using four $3\cancel{c}$ stamps.

Show that for all integers $k \geq 12$, if the property is true for $n = k$ then it is true for $n = k + 1$: Suppose that for some integer $k \geq 12$, a postage of k cents can be obtained using $3\cancel{c}$ and $7\cancel{c}$ stamps . We must show that a postage of $k + 1$ cents can be obtained using $3\cancel{c}$ and $7\cancel{c}$ stamps. But if there are two $3\cancel{c}$ stamps among those used to make up the k cents of postage, replace them by one $7\cancel{c}$ stamps; the result will be $(k + 1)\cancel{c}$ of postage. And if there are not two $3\cancel{c}$ stamps making up the k cents of postage, then at least two $7\cancel{c}$ stamps must be used because $k \geq 12$. Remove two $7\cancel{c}$ stamps and replace them by five $3\cancel{c}$ stamps; the result will be $(k + 1)\cancel{c}$ of postage. Thus in either case $(k + 1)\cancel{c}$ of postage can be obtained using $3\cancel{c}$ and $7\cancel{c}$ stamps *[as was to be shown]*.

4. *a.* $P(2) : \displaystyle\sum_{i=1}^{2-1} i(i + 1) = \dfrac{2(2 - 1)(2 + 1)}{3}$

$P(2)$ is true because the left-hand side equals $1(1 + 1) = 2$ and the right-hand side equals $\dfrac{2 \cdot 1 \cdot 3}{3} = 2$ also.

b. $P(k) : \displaystyle\sum_{i=1}^{k-1} i(i + 1) = \dfrac{k(k - 1)(k + 1)}{3}$

c. $P(k + 1) : \displaystyle\sum_{i=1}^{(k+1)-1} i(i + 1) = \dfrac{(k + 1)((k + 1) - 1)((k + 1) + 1)}{3}$

Or, equivalently, $P(k + 1)$ is $\displaystyle\sum_{i=1}^{k} i(i + 1) = \dfrac{(k + 1)k(k + 2)}{3}$

d. Must show: If k is any integer with $k \geq 2$ and $\displaystyle\sum_{i=1}^{k-1} i(i + 1) = \dfrac{k(k - 1)(k + 1)}{3}$,

then $\displaystyle\sum_{i=1}^{k} i(i + 1) = \dfrac{(k + 1)k(k + 2)}{3}$.

7. *Proof (by mathematical induction)*: Let the property $P(n)$ be the equation

$$1 + 6 + 11 + \cdots + (5n - 4) = \frac{n(5n - 3)}{2}.$$

Show that the property is true for $n = 1$: The property is true for $n = 1$ because for $n = 1$ the left-hand side is 1 and the right-hand side is $\dfrac{1 \cdot (5 \cdot 1 - 3)}{2} = 1$ also.

Show that for all integers $k \geq 1$, if the property is true for $n = k$ then it is true for $n = k + 1$: Suppose $1 + 6 + 11 + \cdots + (5k - 4) = \dfrac{k(5k - 3)}{2}$ for some integer $k \geq 1$. *[This is the inductive hypothesis.]* We must show that $1 + 6 + 11 + \cdots + (5(k + 1) - 4) = \dfrac{(k + 1)(5(k + 1) - 3)}{2}$. But the left-hand side of this equation is

$$1 + 6 + 11 + \cdots + (5(k+1) - 4) = 1 + 6 + 11 + \cdots + (5k - 4) + (5(k+1) - 4)$$

by making the next-to-last term explicit

$$= \frac{k(5k - 3)}{2} + (5k + 1)$$

by inductive hypothesis

$$= \frac{k(5k - 3)}{2} + \frac{2(5k + 1)}{2}$$

by creating a common denominator

$$= \frac{5k^2 - 3k}{2} + \frac{10k + 2}{2}$$

by multiplying out

$$= \frac{5k^2 - 3k + 10k + 2}{2}$$

by adding the fractions

$$= \frac{5k^2 + 7k + 2}{2}$$

by combining like terms.

And the right-hand side of the equation is

$$\frac{(k+1)(5(k+1) - 3)}{2} = \frac{(k+1)(5k + 2)}{2} = \frac{5k^2 + 2k + 5k + 2}{2} = \frac{5k^2 + 7k + 2}{2}.$$

Thus the left-hand and right-hand sides of the equation are equal *[as was to be shown]*.

9. *Proof (by mathematical induction)*: Let the property $P(n)$ be the equation

$$4^3 + 4^4 + 4^5 + \cdots + 4^n = \frac{4(4^n - 16)}{3}.$$

Show that the property is true for $n = 3$: The property is true for $n = 3$ because for $n = 3$ the left-hand side is $4^3 = 64$ and the right-hand side is $\dfrac{4(4^3 - 16)}{3} = \dfrac{4(64 - 16)}{3} = \dfrac{4 \cdot 48}{3} = 64$ also.

Show that for all integers $k \geq 1$, if the property is true for $n = k$ then it is true for $n = k + 1$: Suppose $4^3 + 4^4 + 4^5 + \cdots + 4^k = \dfrac{4(4^k - 16)}{3}$ for some integer $k \geq 3$. *[This is the inductive hypothesis.]* We must show that $4^3 + 4^4 + 4^5 + \cdots + 4^{k+1} = \dfrac{4(4^{k+1} - 16)}{3}$. But the left-hand side of this equation is

$$4^3 + 4^4 + 4^5 + \cdots + 4^{k+1} = 4^3 + 4^4 + 4^5 + \cdots + 4^k + 4^{k+1}$$

by making the next-to-last term explicit

$$= \frac{4(4^k - 16)}{3} + 4^{k+1}$$

by inductive hypothesis

$$= \frac{4^{k+1} - 64}{3} + \frac{3 \cdot 4^{k+1}}{3}$$

by creating a common denominator

$$= \frac{4 \cdot 4^{k+1} - 64}{3}$$

by adding the fractions

$$= \frac{4(4^{k+1} - 16)}{3}$$

by factoring out the 4,

and this is the right-hand side of the equation *[as was to be shown]*.

11. *Proof (by mathematical induction)*: Let the property $P(n)$ be the equation

$$1^3 + 2^3 + \cdots + n^3 = \left(\frac{n(n+1)}{2}\right)^2.$$

Show that the property is true for $n = 1$: The property is true for $n = 1$ because the left-hand side is $1^3 = 1$ and the right-hand side is $\left(\dfrac{1(1+1)}{2}\right)^2 = \left(\dfrac{2}{2}\right)^2 = 1$ also.

Show that for all integers $k \geq 1$, if the property is true for $n = k$ then it is true for $n = k + 1$: Suppose $1^3 + 2^3 + \cdots + k^3 = \left(\dfrac{k(k+1)}{2}\right)^2$ for some integer $k \geq 1$. *[This is the inductive hypothesis.]* We must show that $1^3 + 2^3 + \cdots + (k+1)^3 = \left(\dfrac{(k+1)((k+1)+1)}{2}\right)^2$. But the left-hand side of this equation is

$$
\begin{aligned}
1^3 + 2^3 + \cdots + (k+1)^3 \quad &= \quad 1^3 + 2^3 + \cdots + k^3 + (k+1)^3 \\
&\qquad \text{by making the next-to-last term explicit} \\
&= \quad \left(\frac{k(k+1)}{2}\right)^2 + (k+1)^3 \\
&\qquad \text{by inductive hypothesis} \\
&= \quad \frac{k^2(k+1)^2}{4} + \frac{4(k+1)^3}{4} \\
&\qquad \text{by multiplying and creating a common denominator} \\
&= \quad \frac{k^2(k+1)^2 + 4(k+1)^3}{4} \\
&\qquad \text{by adding the fractions} \\
&= \quad \frac{(k+1)^2(k^2 + 4(k+1))}{4} \\
&\qquad \text{by factoring out } (k+1)^2 \\
&= \quad \frac{(k+1)^2(k^2 + 4k + 4)}{4} \\
&\qquad \text{by multiplying out.}
\end{aligned}
$$

The right-hand side of the equation is

$$
\begin{aligned}
\left(\frac{(k+1)((k+1)+1)}{2}\right)^2 \quad &= \quad \left(\frac{(k+1)(k+2)}{2}\right)^2 \\
&= \quad \frac{(k+1)^2(k+2)^2}{4} \\
&= \quad \frac{(k+1)^2(k^2 + 4k + 4)}{4}.
\end{aligned}
$$

Thus the left-hand side of the equation equals the right-hand side *[as was to be shown]*.

12. *Proof (by mathematical induction):* Let the property $P(n)$ be the equation

$$
\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}.
$$

Show that the property is true for $n = 1$: The property is true for $n = 1$ because the left-hand side equals $\dfrac{1}{1 \cdot 2} = \dfrac{1}{2}$ and the right-hand side equals $\dfrac{1}{1+1} = \dfrac{1}{2}$ also.

Show that for all integers $k \geq 1$, if the property is true for $n = k$ then it is true for $n = k + 1$: Suppose $\dfrac{1}{1 \cdot 2} + \dfrac{1}{2 \cdot 3} + \cdots + \dfrac{1}{k(k+1)} = \dfrac{k}{k+1}$ for some integer $k \geq 1$. *[This is the inductive hypothesis.]* We must show that $\dfrac{1}{1 \cdot 2} + \dfrac{1}{2 \cdot 3} + \cdots + \dfrac{1}{(k+1)((k+1)+1)} = \dfrac{k+1}{(k+1)+1}$, or, equivalently, $\dfrac{1}{1 \cdot 2} + \dfrac{1}{2 \cdot 3} + \cdots + \dfrac{1}{(k+1)(k+2)} = \dfrac{k+1}{k+2}$. But the left-hand side of this equation is

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{(k+1)(k+2)}$$

$$= \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{k(k+1)} + \frac{1}{(k+1)(k+2)}$$

by making the next-to-last term explicit

$$= \frac{k}{k+1} + \frac{1}{(k+1)(k+2)}$$

by inductive hypothesis

$$= \frac{k(k+2)}{(k+1)(k+2)} + \frac{1}{(k+1)(k+2)}$$

by creating a common denominator

$$= \frac{k^2 + 2k + 1}{(k+1)(k+2)}$$

by adding the fractions

$$= \frac{(k+1)^2}{(k+1)(k+2)}$$

because $k^2 + 2k + 1 = (k+1)^2$

$$= \frac{k+1}{k+2}$$

by cancelling $(k+1)$ from numerator and denominator,
and this is the right-hand side of the equation *[as was to be shown]*.

14. *Proof (by mathematical induction):* Let the property $P(n)$ be the equation

$$\sum_{i=1}^{n+1} i \cdot 2^i = n \cdot 2^{n+2} + 2.$$

Show that the property is true for $n = 0$: The property holds for $n = 0$ because $\sum_{i=1}^{0+1} i \cdot 2^i = 1 \cdot 2^1 = 2$ and $0 \cdot 2^{0+2} + 2 = 2$ also.

Show that for all integers $k \geq 0$, if the property is true for $n = k$ then it is true for $n = k + 1$: Suppose $\sum_{i=1}^{k+1} i \cdot 2^i = k \cdot 2^{k+2} + 2$ for some integer $k \geq 0$. *[This is the inductive hypothesis.]* We must show that $\sum_{i=1}^{(k+1)+1} i \cdot 2^i = (k+1) \cdot 2^{(k+1)+2} + 2$, or, equivalently, $\sum_{i=1}^{k+2} i \cdot 2^i = (k+1) \cdot 2^{k+3} + 2$. But the left-hand side of the equation is

$$
\begin{aligned}
\sum_{i=1}^{(k+1)+1} i \cdot 2^i &= \sum_{i=1}^{k+1} i \cdot 2^i + (k+2)2^{k+2} && \text{by writing the } (k+1)\text{st term separately} \\
&= (k \cdot 2^{k+2} + 2) + (k+2)2^{k+2} && \text{by inductive hypothesis} \\
&= (k + (k+2))2^{k+2} + 2 \\
&= (2k+2)2^{k+2} + 2 \\
&= (k+1)2^{k+3} + 2 && \text{by algebra,}
\end{aligned}
$$

and this is the right-hand side of the equation *[as was to be shown]*.

15. *Proof (by mathematical induction):* Let the property $P(n)$ be the equation

$$\sum_{i=1}^{n} i(i!) = (n+1)! - 1.$$

Show that the property is true for $n = 1$: We must show that $\sum_{i=1}^{1} i(i!) = (1+1)! - 1$. But the left-hand side of this equation is $\sum_{i=1}^{1} i(i!) = 1 \cdot (1!) = 1$ and the right-hand side is $(1+1)! - 1 = 2! - 1 = 2 - 1 = 1$ also. So the property is true for $n = 1$.

Show that for all integers $k \geq 1$, if the property is true for $n = k$ then it is true for $n = k + 1$: Suppose $\sum_{i=1}^{k} i(i!) = (k+1)! - 1$ for some integer $k \geq 1$. *[This is the inductive hypothesis.]* We must show that $\sum_{i=1}^{k+1} i(i!) = ((k+1)+1)! - 1$, or, equivalently, we must show that $\sum_{i=1}^{k+1} i(i!) = (k+2)! - 1$. But the left-hand side of the equation is

$$\sum_{i=1}^{k+1} i(i!) = \sum_{i=1}^{k} i(i!) + (k+1)((k+1)!)$$ by writing the $(k+1)$st term separately

$$= [(k+1)! - 1] + (k+1)((k+1)!)$$ by inductive hypothesis

$$= ((k+1)!)(1 + (k+1)) - 1$$ by combining the terms with the common factor $(k+1)!$

$$= (k+1)!(k+2) - 1$$

$$= (k+2)! - 1$$ by algebra,

and this is the right-hand side of the equation *[as was to be shown]*.

16. *Proof (by mathematical induction)*: Let the property $P(n)$ be the equation

$$\left(1 - \frac{1}{2^2}\right)\left(1 - \frac{1}{3^2}\right) \cdots \left(1 - \frac{1}{n^2}\right) = \frac{n+1}{2n}.$$

Show that the property is true for $n = 2$: The property holds for $n = 2$ because $1 - \frac{1}{2^2} = \frac{3}{4}$ and $\frac{2+1}{2 \cdot 2} = \frac{3}{4}$ also.

Show that for all integers $k \geq 2$, if the property is true for $n = k$ then it is true for $n = k + 1$: Suppose

$$\left(1 - \frac{1}{2^2}\right)\left(1 - \frac{1}{3^2}\right) \cdots \left(1 - \frac{1}{k^2}\right) = \frac{k+1}{2k}$$ for some integer $k \geq 2$. $\leftarrow$ inductive hypothesis

We must show that

$$\left(1 - \frac{1}{2^2}\right)\left(1 - \frac{1}{3^2}\right) \cdots \left(1 - \frac{1}{(k+1)^2}\right) = \frac{(k+1)+1}{2(k+1)},$$

or, equivalently, we must show that

$$\left(1 - \frac{1}{2^2}\right)\left(1 - \frac{1}{3^2}\right) \cdots \left(1 - \frac{1}{(k+1)^2}\right) = \frac{k+2}{2(k+1)}.$$

But the left-hand side of this equation is

$$\left(1 - \frac{1}{2^2}\right)\left(1 - \frac{1}{3^2}\right) \cdots \left(1 - \frac{1}{(k+1)^2}\right)$$

$$= \left(1 - \frac{1}{2^2}\right)\left(1 - \frac{1}{3^2}\right) \cdots \left(1 - \frac{1}{k^2}\right)\left(1 - \frac{1}{(k+1)^2}\right)$$ by making the next-to-last factor explicit

$$= \left(\frac{k+1}{2k}\right)\left(1 - \frac{1}{(k+1)^2}\right)$$ by inductive hypothesis

$$= \frac{k+1}{2k} - \frac{1}{2k(k+1)}$$

$$= \frac{(k+1)^2 - 1}{2k(k+1)}$$

$$= \frac{(k^2 + 2k + 1) - 1}{2k(k+1)}$$

$$= \frac{k+2}{2(k+1)}$$ by algebra,

and this is the right-hand side of the equation *[as was to be shown]*.

17. *Proof (by mathematical induction)*: Let the property $P(n)$ be the equation

$$\prod_{i=0}^{n}\left(\frac{1}{2i+1} \cdot \frac{1}{2i+2}\right) = \frac{1}{(2n+2)!}$$

Show that the property is true for $n = 0$: The property holds for $n = 0$ because
$$\prod_{i=0}^{0}\left(\frac{1}{2i+1}\cdot\frac{1}{2i+2}\right) = \frac{1}{1}\cdot\frac{1}{2} = \frac{1}{2} \text{ and } \frac{1}{(2\cdot 0+2)!} = \frac{1}{2} \text{ also.}$$

Show that for all integers $k \geq 0$, if the property is true for $n = k$ then it is true for $n = k + 1$: Suppose $\displaystyle\prod_{i=0}^{k}\left(\frac{1}{2i+1}\cdot\frac{1}{2i+2}\right) = \frac{1}{(2k+2)!}$ for some integer $k \geq 0$. *[This is the inductive hypothesis.]* We must show that $\displaystyle\prod_{i=0}^{k+1}\left(\frac{1}{2i+1}\cdot\frac{1}{2i+2}\right) = \frac{1}{(2\cdot(k+1)+2)!}$,
or, equivalently, $\displaystyle\prod_{i=0}^{k+1}\left(\frac{1}{2i+1}\cdot\frac{1}{2i+2}\right) = \frac{1}{(2k+4)!}$. But the left-hand side of this equation is

$$\prod_{i=0}^{k+1}\left(\frac{1}{2i+1}\cdot\frac{1}{2i+2}\right)$$

$$= \prod_{i=0}^{k}\left(\frac{1}{2i+1}\cdot\frac{1}{2i+2}\right)\cdot\left(\frac{1}{2(k+1)+1}\cdot\frac{1}{2(k+1)+2}\right)$$

by writing the $(k+1)$st factor separately

$$= \left(\frac{1}{(2k+2)!}\right)\cdot\left(\frac{1}{2(k+1)+1}\cdot\frac{1}{2(k+1)+2}\right)$$

by inductive hypothesis

$$= \frac{1}{(2k+2)!}\cdot\frac{1}{2k+3}\cdot\frac{1}{2k+4}$$

$$= \frac{1}{(2k+4)!}$$

by algebra,

and this is the right-hand side of the equation *[as was to be shown]*.

18. *Proof (by mathematical induction):* Let the property $P(n)$ be the equation

$$\sin x + \sin 3x + \cdots + \sin(2n-1)x = \frac{1-\cos 2nx}{2\sin x}.$$

Show that the property is true for $n = 1$: The property holds for $n = 1$ because the left-hand side equals $\sin x$, and the right-hand side equals $\dfrac{1-\cos 2x}{2\sin x} = \dfrac{1-\cos^2 + \sin^2 x}{2\sin x} = \dfrac{2\sin^2 x}{2\sin x} = \sin x$.

Show that for all integers $k \geq 1$, if the property is true for $n = k$ then it is true for $n = k + 1$: Suppose $\sin x + \sin 3x + \cdots + \sin(2k-1)x = \dfrac{1-\cos 2kx}{2\sin x}$ for some integer $k \geq 1$. *[This is the inductive hypothesis.]* We must show that $\sin x + \sin 3x + \cdots + \sin(2(k+1)-1)x = \dfrac{1-\cos 2(k+1)x}{2\sin x}$, or, equivalently, $\sin x + \sin 3x + \cdots + \sin(2k+1)x = \dfrac{1-\cos 2(k+1)x}{2\sin x}$. But when the next-to-last term of the the left-hand side of this equation is made explicit, the left-hand side becomes

$$\sin x + \sin 3x + \cdots + \sin(2k-1)x + \sin(2k+1)x$$

$$
\begin{aligned}
&= \frac{1-\cos 2kx}{2\sin x} + \sin(2k+1)x && \text{by inductive hypothesis} \\
&= \frac{1-\cos 2kx}{2\sin x} + \frac{2\sin x \sin(2kx+x)}{2\sin x} && \text{by creating a common denominator} \\
&= \frac{1-\cos 2kx + 2\sin x \sin(2kx+x)}{2\sin x} && \text{by adding fractions} \\
&= \frac{1-\cos 2kx + 2\sin x[\sin(2kx)\cos x + \cos(2kx)\sin x]}{2\sin x} && \text{by the addition formula for sine} \\
&= \frac{1-\cos 2kx + 2\sin x \sin(2kx)\cos x + 2\sin^2 x \cos(2kx)}{2\sin x} && \text{by multiplying out} \\
&= \frac{1+\cos 2kx(2\sin^2 x - 1) + 2\sin x \cos x \sin(2kx)}{2\sin x} && \text{by combining like terms} \\
&= \frac{1+\cos 2kx(-\cos 2x) + \sin 2x \sin(2kx)}{2\sin x} && \text{by the formulas for } \cos 2x \text{ and } \sin 2x \\
&= \frac{1-(\cos 2kx \cos 2x - \sin 2x \sin(2kx))}{2\sin x} && \text{by factoring out } -1 \\
&= \frac{1-\cos(2kx + 2x)}{2\sin x} && \text{by the addition formula for cosine} \\
&= \frac{1-\cos(2(k+1)x)}{2\sin x} && \text{by factoring out 2x,}
\end{aligned}
$$

and this is the right-hand side of the equation *[as was to be shown]*.

20. $5 + 10 + 15 + 20 + \cdots + 300 = 5(1 + 2 + 3 + \cdots + 60) = 5\left(\dfrac{60 \cdot 61}{2}\right) = 9150.$

22. $7+8+9+10+\cdots+600 = (1+2+3+\cdots+600)-(1+2+3+4+5+6) = \left(\dfrac{600 \cdot 601}{2}\right)-21 = 180,279$

25. $3 + 3^2 + 3^3 + \cdots + 3^n = 3(1 + 3 + 3^2 + \cdots + 3^{n-1}) = 3\left(\dfrac{3^{(n-1)+1}-1}{3-1}\right) = \dfrac{3(3^n-1)}{2}$

26. $5^3 + 5^4 + 5^5 + \cdots + 5^k = 5^3(1 + 5 + 5^2 + \cdots + 5^{k-3}) = 5^3\left(\dfrac{5^{(k-3)+1}-1}{5-1}\right) = \dfrac{5^3(5^{k-2}-1)}{4}$

28. $1 - 2 + 2^2 - 2^3 + \cdots + (-1)^n 2^n = 1 + (-2) + (-2)^2 + (-2)^3 + \cdots\cdots + (-2)^n$

$$= \frac{(-2)^{n+1}-1}{(-2)-1} = \frac{(-2)^{n+1}-1}{-3} = \frac{1}{3}\left(1 + (-1)^n 2^{n+1}\right)$$

29. $(a + md) + (a + (m+1)d) + (a + (m+2)d) + \cdots + (a + (m+n)d)$

$$
\begin{aligned}
&= (a + md) + (a + md + d) + (a + md + 2d) + \cdots + (a + md + nd) \\
&= \underbrace{((a + md) + (a + md) + \cdots + (a + md))}_{n+1 \text{ terms}} + d(1 + 2 + 3 + \cdots + n) \\
&= (n+1)(a + md) + d\left(\frac{n(n+1)}{2}\right) && \text{by Theorem 4.2.2} \\
&= (a + md + \frac{n}{2}d)(n+1) \\
&= [a + (m + \frac{n}{2})d](n+1)
\end{aligned}
$$

Any one of the last three equations or their algebraic equivalents could be considered a correct answer.

30. $ar^m + ar^{m+1} + ar^{m+2} + \cdots + ar^{m+n} = ar^m(1 + r + r^2 + \ldots + r^n) = ar^m\left(\dfrac{r^{n+1}-1}{r-1}\right)$ by Theorem 4.2.3

31. *a.* $2 + 4 + 8 + \ldots + 2^{40} = 2(1 + 2 + 2^2 + \cdots + 2^{39}) = 2\left(\dfrac{2^{39+1} - 1}{2 - 1}\right) = 2^{41} - 2$

    b. 40 generations $= 40 \cdot 25 = 1000$ years (at 25 years per generation)

    c. Since $2^{41} - 2 \cong 2.2 \times 10^{12} > 10^{10}$, not all ancestors are distinct: some ancestors on different branches of the family tree must be the same.

33. *Proof*: Suppose m and n are any positive integers such that m is odd. By definition of odd, $m = 2q + 1$ for some integer k, and so, by Theorems 4.1.1 and 4.2.2,

$$\sum_{k=0}^{m-1}(n+k) = \sum_{k=0}^{(2q+1)-1}(n+k) = \sum_{k=0}^{2q}(n+k) = \sum_{k=0}^{2q}n + \sum_{k=0}^{2q}k = (2q+1)n + \sum_{k=1}^{2q}k$$

$$= (2q+1)n + \frac{2q(2q+1)}{2} = (2q+1)n + q(2q+1) = (2q+1)(n+q) = m(n+q).$$

But $n + q$ is an integer because it is a sum of integers. Hence, by definition of divisibility, $\sum_{k=0}^{m-1}(n+k)$ is divisible by m.

Note: If m is even, the property is no longer true. For example, if $n = 1$ and $m = 2$, then $\sum_{k=0}^{m-1}(n+k) = \sum_{k=0}^{2-1}(1+k) = 1 + 2 = 3$, and 3 is not divisible by 2.

34. *Proof*: Suppose p is any prime number with $p \geq 5$. The sum of squares of any p consecutive integers may be represented as $n^2 + (n+1)^2 + (n+2)^2 + \cdots + (n+p)^2$, where n is some integer: Then

$$n^2 + (n+1)^2 + (n+2)^2 + (n+3)^2 + \cdots + (n+(p-1))^2$$
$$= n^2 + (n^2 + 2n + 1) + (n^2 + 4n + 4) + (n^2 + 6n + 9) + \cdots + (n^2 + 2(p-1)n + (p-1)^2)$$
$$= \underbrace{(n^2 + n^2 + n^2 + \cdots + n^2)}_{p \text{ terms}} + (2n+4n+6n+\cdots+2(p-1)n) + (1+4+9+\cdots+(p-1)^2)$$
$$= pn^2 + 2n(1 + 2 + 3 + \cdots + (p-1)) + (1^2 + 2^2 + 3^2 + \cdots + (p-1)^2)$$
$$= pn^2 + 2n\left(\frac{(p-1)((p-1)+1)}{2}\right) + \frac{(p-1)((p-1)+1)(2(p-1)+1)}{6} \quad \text{by algebra}$$
$$\text{by Theorem 4.2.2 and exercise 10}$$
$$= pn^2 + 2n\left(\frac{(p-1)p}{2}\right) + \frac{(p-1)p(2p-1)}{6}$$
$$= p\left(n^2 + n(p-1)\right) + \frac{p(p-1)(2p-1)}{6}$$

Now the right-hand side of this equation is an integer because it equals a sum of squares of integers, and, because $p\left(n^2 + n(p-1)\right)$ is also an integer, the other term on the right-hand side is a difference of integers and hence an integer. Thus 6 must divide $p(p-1)(2p-1)$. But because p is prime and $p \geq 5$, none of 2 or 3 or 6 is a factor of p and therefore, 6 is a factor of $(p-1)(2p-1)$. Hence $\dfrac{(p-1)(2p-1)}{6}$ is an integer, and so p is a factor of both terms on the right-hand side of the equation. It follows that p is a factor of the entire right-hand side *[exercise 15, Section 3.3]*, which implies that p is a factor of the sum of the p consecutive squares.

Note: An alternative solution to this exercise can be given using exercise 42 from Section 3.4. According to that exercise, if p is a prime number and $p \geq 5$, then p has the form $6q+1$ or $6q+5$ for some integer q. In case $p = 6q+1$, then $(p-1)(2p-1) = ((6q+1)-1)(2p-1) = 6q(2p-1)$, which is divisible by 6. In case $p = 6q+5$, then $(p-1)(2p-1) = ((6q+5)-1)(2(6q+5)-1) = (6q+4)(12q-9) = 2(3q+2)\cdot 3(4q+3) = 6(3q+2)(4q+3)$, which is also divisible by 6. So in either case $(p-1)(2p-1)$ is divisible by 6.

Section 4.3

2. *Formula*: $(1 + \frac{1}{1})(1 + \frac{1}{2}) \cdots (1 + \frac{1}{n}) = n + 1$ for all integers $n \geq 1$.

Proof (by mathematical induction): Let the property $P(n)$ be the equation

$$(1 + \frac{1}{1})(1 + \frac{1}{2}) \cdots (1 + \frac{1}{n}) = n + 1$$

Show that the property is true for $n = 1$: When $n = 1$, the left-hand side of the equation is $1 + \frac{1}{1} = 2$ and the right hand side is $1 + 1 = 2$ also. So the property is true for $n = 1$.

Show that for all integers $k \geq 1$, if the property is true for $n = k$ then it is true for $n = k + 1$: Suppose $(1 + \frac{1}{1})(1 + \frac{1}{2}) \cdots (1 + \frac{1}{k}) = k + 1$, for some integer $k \geq 1$. *[This is the inductive hypothesis.]* We must show that $(1 + \frac{1}{1})(1 + \frac{1}{2}) \cdots (1 + \frac{1}{k+1}) = (k + 1) + 1$. But the left-hand side of this equation is

$$(1 + \frac{1}{1})(1 + \frac{1}{2}) \cdots (1 + \frac{1}{k+1})$$

$$= (1 + \frac{1}{1})(1 + \frac{1}{2}) \cdots (1 + \frac{1}{k})(1 + \frac{1}{k+1}) \quad \text{by making the next-to-last factor explicit}$$

$$= (k + 1)(1 + \frac{1}{k+1}) \quad \text{by inductive hypothesis}$$

$$= (k + 1) + 1 \quad \text{by algebra,}$$

and this is the right-hand side of the equation *[as was to be shown]*.

4. *Formula*: $\sum_{i=1}^{n}(-1)^{i-1}i^2 = (-1)^{n-1}(1 + 2 + 3 + \cdots + n)$ or $\sum_{i=1}^{n}(-1)^{i-1}i^2 = (-1)^{n-1} \cdot \frac{n(n+1)}{2}$

(by Theorem 4.2.2) for all integers $n \geq 1$.

Proof (by mathematical induction): Let the property $P(n)$ be the equation

$$\sum_{i=1}^{n}(-1)^{i-1}i^2 = (-1)^{n-1} \cdot \frac{n(n+1)}{2}.$$

Show that the property is true for $n = 1$: The property is true for $n = 1$ because the left-hand side of the equation is $\sum_{i=1}^{1}(-1)^{i-1}i^2 = (-1)^0 \cdot 1^2 = 1$ and the right-hand side is $(-1)^{1-1} \cdot \frac{1(1+1)}{2} = 1$ also.

Show that for all integers $k \geq 1$, if the property is true for $n = k$ then it is true for $n = k + 1$: Suppose $\sum_{i=1}^{k}(-1)^{i-1}i^2 = (-1)^{k-1} \cdot \frac{k(k+1)}{2}$ for some integer $k \geq 1$. *[This is the inductive hypothesis.]* We must show that

$$\sum_{i=1}^{k+1}(-1)^{i-1}i^2 = (-1)^{(k+1)-1} \cdot \frac{(k+1)((k+1)+1)}{2},$$

or, equivalently, we must show that

$$\sum_{i=1}^{k+1}(-1)^{i-1}i^2 = (-1)^{k} \cdot \frac{(k+1)(k+2)}{2}.$$

But the left-hand side of this equation is

$$\sum_{i=1}^{k+1}(-1)^{i-1}i^2$$

$$= \sum_{i=1}^{k}(-1)^{i-1}i^2 + (-1)^{(k+1)-1}(k+1)^2 \qquad \text{by writing the } (k+1)\text{st term separately}$$

$$= (-1)^{k-1}\left(\frac{k(k+1)}{2}\right) + (-1)^k(k+1)^2 \qquad \text{by inductive hypothesis}$$

$$= (-1)^{k-1}(k+1)\left(\frac{k}{2} + (-1)(k+1)\right)$$

$$= (-1)^{k-1}(k+1)\left(\frac{k-2k-2}{2}\right)$$

$$= (-1)^{k-1}(k+1)\left(\frac{-k-2}{2}\right)$$

$$= (-1)^{k-1}(k+1)\left(\frac{-(k+2)}{2}\right)$$

$$= (-1)^k \cdot \frac{(k+1)(k+2)}{2} \qquad \text{by algebra,}$$

and this is the right-hand side of the equation *[as was to be shown]*.

5.

$$\sum_{k=1}^{1}\frac{k}{(k+1)!} = \frac{1}{2!} = \frac{1}{2}$$

$$\sum_{k=1}^{2}\frac{k}{(k+1)!} = \frac{1}{2} + \frac{1}{3!} = \frac{5}{6}$$

$$\sum_{k=1}^{3}\frac{k}{(k+1)!} = \frac{5}{6} + \frac{1}{4!} = \frac{23}{24}$$

$$\sum_{k=1}^{4}\frac{k}{(k+1)!} = \frac{23}{24} + \frac{1}{5!} = \frac{119}{120}$$

$$\sum_{k=1}^{5}\frac{k}{(k+1)!} = \frac{119}{120} + \frac{1}{6!} = \frac{719}{720}$$

Note that $\dfrac{1}{2} = \dfrac{2!-1}{2!}$, $\dfrac{5}{6} = \dfrac{3!-1}{3!}$, $\dfrac{23}{24} = \dfrac{4!-1}{4!}$, $\dfrac{119}{120} = \dfrac{5!-1}{5!}$, and $\dfrac{719}{720} = \dfrac{6!-1}{6!}$. So we conjecture that $\displaystyle\sum_{k=1}^{n}\frac{k}{(k+1)!} = \frac{(n+1)!-1}{(n+1)!}$.

Proof by mathematical induction: Let the property $P(n)$ be the equation

$$\sum_{k=1}^{n}\frac{k}{(k+1)!} = \frac{(n+1)!-1}{(n+1)!}.$$

Show that the property is true for $n = 1$: The calculation preceding the proof shows that

$$\sum_{k=1}^{1}\frac{k}{(k+1)!} = \frac{(1+1)!-1}{(1+1)!}.$$

Show that for all integers $r \geq 1$, if the property is true for $n = r$ then it is true for $n = r + 1$: Suppose that for some integer $r \geq 1$, $\displaystyle\sum_{k=1}^{r}\frac{k}{(k+1)!} = \frac{(r+1)!-1}{(r+1)!}$. *[This is the inductive hypothesis.]* We must show that $\displaystyle\sum_{k=1}^{r+1}\frac{k}{(k+1)!} = \frac{[(r+1)+1]!-1}{[(r+1)+1]!}$, or, equivalently,

that $\displaystyle\sum_{k=1}^{r+1} \frac{k}{(k+1)!} = \frac{(r+2)!-1}{(r+2)!}$.

But the left-hand side of this equation is

$$\sum_{k=1}^{r+1} \frac{k}{(k+1)!}$$

$$= \sum_{k=1}^{r} \frac{k}{(k+1)!} + \frac{r+1}{[(r+1)+1]!} \qquad \text{by making the next-to-last term explicit}$$

$$= \frac{(r+1)!-1}{(r+1)!} + \frac{r+1}{(r+2)!} \qquad \text{by inductive hypothesis}$$

$$= \frac{(r+1)!-1}{(r+1)!} \cdot \frac{(r+2)}{(r+2)} + \frac{r+1}{(r+2)!} \qquad \text{to create a common denominator}$$

$$= \frac{(r+2)!-(r+2)}{(r+2)!} + \frac{r+1}{(r+2)!}$$

$$= \frac{(r+2)!-1}{(r+2)!} \qquad \text{by algebra,}$$

and this is the right-hand side of the equation *[as was to be shown]*.

7. *a.* $P(n)$: $2^n < (n+1)!$

   $P(2)$ is true because $2^2 = 4 < 6 = (2+1)!$.

   b. $P(k)$: $2^k < (k+1)!$

   c. $P(k+1)$: $2^{k+1} < ((k+1)+1)!$

   d. Must show: If k is any integer with $k \geq 2$ and $2^k < (k+1)!$, then $2^{k+1} < ((k+1)+1)!$.

9. *Proof (by mathematical induction)*: Let the property $P(n)$ be the sentence "$7^n - 1$ is divisible by 6."

   Show that the property is true for $n = 0$: The property is true for $n = 0$ because $7^0 - 1 = 1 - 1 = 0$ and 0 is divisible by 6 (since $0 = 0 \cdot 6$).

   Show that for all integers $k \geq 0$, if the property is true for $n = k$ then it is true for $n = k + 1$: Suppose $7^k - 1$ is divisible by 6 for some integer $k \geq 0$. *[This is the inductive hypothesis.]* We must show that $7^{k+1} - 1$ is divisible by 6. By definition of divisibility, the inductive hypothesis is equivalent to the statement $7^k - 1 = 6r$ for some integer r. Then by the laws of algebra, $7^{k+1} - 1 = 7 \cdot 7^k - 1 = (6+1)7^k - 1 = 6 \cdot 7^k + (7^k - 1) = 6 \cdot 7^k + 6r$, where the last equality holds by inductive hypothesis. Thus, by factoring out the 6 from the extreme right-hand side and by equating the extreme left-hand and extreme right-hand sides, , we have $7^{k+1} - 1 = 6(7^k + r)$, which is divisible by 6 because $7^k + r$ is an integer (since products and sums of integers are integers). Therefore, $7^{k+1} - 1$ is divisible by 6 *[as was to be shown]*.

10. *Proof (by mathematical induction)*: Let the property $P(n)$ be the sentence "$n^3 - 7n + 3$ is divisible by 3."

    Show that the property is true for $n = 0$: The property is true for $n = 0$ because $0^3 - 7 \cdot 0 + 3 = 3$ and 3 is divisible by 3 (since $3 = 3 \cdot 1$).

    Show that for all integers $k \geq 0$, if the property is true for $n = k$ then it is true for $n = k + 1$: Suppose $k^3 - 7k + 3$ is divisible by 3 for some integer $k \geq 0$. *[This is the inductive hypothesis.]* We must show that $(k+1)^3 - 7(k+1) + 3$ is divisible by 3. By definition of divisibility, the inductive hypothesis is equivalent to the statement $k^3 - 7k + 3 = 3r$ for some integer r. Then by the laws of algebra, $(k+1)^3 - 7(k+1) + 3 = k^3 + 3k^2 + 3k + 1 - 7k - 7 + 3 = (k^3 - 7k + 3) + (3k^2 + 3k - 6) = 3r + 3(k^2 + k - 2)$, where the last equality holds by inductive hypothesis. Thus, by factoring out the 3 from the extreme right-hand side and by equating the extreme left-hand and extreme right-hand sides, , we have $(k+1)^3 - 7(k+1) + 3 = 3(r + k^2 + k - 2)$, which is divisible by 3 because $r + k^2 + k - 2$ is an integer (since products and sums of integers are integers).. Therefore, $(k+1)^3 - 7(k+1) + 3$ is divisible by 3 *[as was to be shown]*.

12. *Proof (by mathematical induction)*: Let the property $P(n)$ be the sentence "$7^n - 2^n$ is divisible by 5."

    Show that the property is true for $n = 1$: The property is true for $n = 1$ because $7^1 - 2^1 = 7 - 2 = 5$ and 5 is divisible by 5 (since $5 = 5 \cdot 1$).

    Show that for all integers $k \geq 1$, if the property is true for $n = k$ then it is true for $n = k + 1$: Suppose $7^k - 2^k$ is divisible by 5 for some integer $k \geq 0$. *[This is the inductive hypothesis.]* We must show that $7^{k+1} - 2^{k+1}$ is divisible by 5. By definition of divisibility, the inductive hypothesis is equivalent to the statement $7^k - 2^k = 5r$ for some integer r. Then by the laws of algebra, $7^{k+1} - 2^{k+1} = 7 \cdot 7^k - 2 \cdot 2^k = (5 + 2) \cdot 7^k - 2 \cdot 2^k = 5 \cdot 7^k + 2 \cdot 7^k - 2 \cdot 2^k = 5 \cdot 7^k + 2(7^k - 2^k) = 5 \cdot 7^k + 2 \cdot 5r$, where the last equality holds by inductive hypothesis. Thus, by factoring out the 5 from the extreme right-hand side and by equating the extreme left-hand and extreme right-hand sides, we have $7^{k+1} - 2^{k+1} = 5(7^k + 2r)$, which is divisible by 5 because $7^k + 2r$ is an integer (since products and sums of integers are integers). Therefore, $7^{k+1} - 2^{k+1}$ is divisible by 5 *[as was to be shown]*.

13. *Proof*: Suppose x and y are any integers with $x \neq y$. We show by mathematical induction on n that the property "$x^n - y^n$ is divisible by $x - y$" is true for all integers $n \geq 1$.

    Show that the property is true for $n = 1$: The property is true for $n = 1$ because $x^1 - y^1 = x - y$ and $x - y$ is divisible by $x - y$.

    Show that for all integers $k \geq 1$, if the property is true for $n = k$ then it is true for $n = k + 1$: Suppose $x^k - y^k$ is divisible by $x - y$ for some integer $k \geq 1$. *[This is the inductive hypothesis.]* We must show that $x^{k+1} - y^{k+1}$ is divisible by $x - y$. By rewriting the inductive hypothesis using the definition of divisibility, we have $x^k - y^k = (x - y)r$ for some integer r. Then by the laws of algebra, $x^{k+1} - y^{k+1} = x^{k+1} - xy^k + xy^k - y^{k+1} = x(x^k - y^k) + y^k(x - y) = x(x - y)r + y^k(x - y)$, where the last equality holds by inductive hypothesis. Thus, by factoring out $(x - y)$ from the extreme right-hand side and by equating the extreme left-hand and extreme right-hand sides, we have $x^{k+1} - y^{k+1} = x(x - y)(r + y^k)$, which is divisible by $x - y$ because $x(r + y^k)$ is an integer(since products and sums of integers are integers). Therefore, $x^{k+1} - y^{k+1}$ is divisible by $x - y$ *[as was to be shown]*.

14. *Proof (by mathematical induction)*: Let the property $P(n)$ be the sentence "$n^3 - n$ is divisible by 6."

    Show that the property is true for $n = 2$: The property is true for $n = 2$ because $2^3 - 2 = 6$ and 6 is divisible by 6.

    Show that for all integers $k \geq 2$, if the property is true for $n = k$ then it is true for $n = k + 1$: Suppose $k^3 - k$ is divisible by 6 for some integer $k \geq 2$. *[This is the inductive hypothesis.]* We must show that $(k + 1)^3 - (k + 1)$ is divisible by 6. By definition of divisibility $k^3 - k = 6r$ for some integer r. Then by the laws of algebra, $(k + 1)^3 - (k + 1) = k^3 + 3k^2 + 3k + 1 - k - 1 = (k^3 - k) + 3(k^2 + k) = 6r + 3(k(k + 1))$, where the last equality holds by inductive hypothesis. Now $k(k + 1)$ is a product of two consecutive integers. By Theorem 3.4.2 one of these is even, and so *[by Section 3.1, exercise 42 or Example 3.2.3]* the product $k(k + 1)$ is even. Hence $k(k + 1) = 2s$ for some integer s. Thus $6r + 3(k(k + 1)) = 6r + 3(2s) = 6(r + s)$, and so by substitution, $(k + 1)^3 - (k + 1) = 6(r + s)$, which is divisible by 6 because $r + s$ is an integer. Therefore, $(k + 1)^3 - (k + 1)$ is divisible by 6 *[as was to be shown]*.

15. *Proof (by mathematical induction)*: Let the property $P(n)$ be the sentence "$n(n^2 + 5)$ is divisible by 6."

    Show that the property is true for $n = 1$: The property is true for $n = 1$ because $1(1^2 + 5) = 6$ and 6 is divisible by 6.

    Show that for all integers $k \geq 1$, if the property is true for $n = k$ then it is true for $n = k + 1$: Suppose $k(k^2 + 5)$ is divisible by 6 for some integer $k \geq 1$. *[This is the inductive hypothesis.]* We must show that $(k+1)((k+1)^2 + 5)$ is divisible by 6. By definition of

divisibility $k(k^2+5) = 6r$ for some integer r. Then by the laws of algebra, $(k+1)((k+1)^2+5) = (k+1)(k^2+2k+1+5) = k(k^2+5)+(k(2k+1)+k^2+2k+1+5) = k(k^2+5)+(3k^2+3k+6) = 6r+3(k^2+k)+6$, where the last equality holds by inductive hypothesis. Now $k(k+1)$ is a product of two consecutive integers. By Theorem 3.4.2 one of these is even, and so *[by Section 3.1, exercise 42 or Example 3.2.3]* the product $k(k+1)$ is even. Hence $k(k+1) = 2s$ for some integer s. Thus $6r + 3(k^2+k)+6 = 6r+3(2s)+6 = 6(r+s+1)$. By substitution, then, $(k+1)((k+1)^2+5) = 6(r+s+1)$, which is divisible by 6 because $r+s+1$ is an integer. Therefore, $(k+1)((k+1)^2+5)$ is divisible by 6 *[as was to be shown]*.

17. *Proof (by mathematical induction)*: Let the property $P(n)$ be the inequality $1+3n \le 4^n$.

    Show that the property is true for $n = 0$: The property is true for $n = 0$ because the left-hand side is $1+3 \cdot 0 = 1$ and the right-hand side is $4^0 = 1$, and $1 \le 1$.

    Show that for all integers $k \ge 0$, if the property is true for $n = k$ then it is true for $n = k+1$: Suppose $1+3k \le 4^k$ for some integer $k \ge 0$. *[This is the inductive hypothesis.]* We must show that $1+3(k+1) \le 4^{k+1}$. Multiplying both sides of the inequality in the inductive hypothesis by 4 gives $4 \cdot (1+3k) \le 4 \cdot 4^k$, or, equivalently, $4+12k \le 4^{k+1}$. Now $1+3(k+1) = 1+3k+3 = 4+3k \le 4+12k$ because $k \ge 0$. Putting these together gives $1+3(k+1) = 1+3k+3 = 4+3k \le 4+12k \le 4^{k+1}$ Thus, by the transitive property of order, $1+3(k+1) \le 4^{k+1}$ *[as was to be shown]*.

18. *Proof (by mathematical induction)*: Let the property $P(n)$ be the inequality $5^n + 9 < 6^n$.

    Show that the property is true for $n = 2$: The property is true for $n = 2$ because the left-hand side is $5^2 + 9 = 25 + 9 = 34$ and the right-hand side is $6^2 = 36$, and $34 < 36$.

    Show that for all integers $k \ge 2$, if the property is true for $n = k$ then it is true for $n = k+1$: Suppose $5^k + 9 < 6^k$ for some integer $k \ge 2$. *[This is the inductive hypothesis.]* We must show that $5^{k+1} + 9 < 6^{k+1}$. Multiplying both sides of the inequality in the inductive hypothesis by 5 gives $5(5^k + 9) < 5 \cdot 6^k$. Note that $5(5^k + 9) = 5^{k+1} + 45$, $5 \cdot 6^k < 6^{k+1}$, and $5^{k+1} + 9 < 5^{k+1} + 45$. Putting these together gives $5^{k+1} + 9 < 5^{k+1} + 45 < 5 \cdot 6^k < 6^{k+1}$, and so, by transitivity of order, $5^{k+1} + 9 < 6^{k+1}$ *[as was to be shown]*.

20. *Proof (by mathematical induction)*: Let the property $P(n)$ be the inequality $2^n < (n+2)!$.

    Show that the property is true for $n = 0$: The property is true for $n = 0$ because the left-hand side is $2^0 = 1$ and the right-hand side is $(0+2)! = 2! = 2$ and $1 < 2$.

    Show that for all integers $k \ge 0$, if the property is true for $n = k$ then it is true for $n = k+1$: Suppose $2^k < (k+2)!$ for some integer $k \ge 0$. *[This is the inductive hypothesis.]* We must show that $2^{k+1} < ((k+1)+2)!$. But by the laws of algebra and substitution from the inductive hypothesis, $2^{k+1} = 2^k \cdot 2 < (k+2)! \cdot 2 < (k+2)! \cdot (k+3)$ *[2 < k+3 because $k \ge 0$]*. Thus $2^{k+1} < (k+2)! \cdot (k+3) = (k+3)!$ and so $2^{k+1} < ((k+1)+2)!$ *[as was to be shown]*.

21. *Proof (by mathematical induction)*: Let the property $P(n)$ be the inequality

    $$\sqrt{n} < \frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n}}.$$

    Show that the property is true for $n = 2$: To show that the property is true for $n = 2$ we must show that $\sqrt{2} < \frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}}$. But this inequality is true if, and only if, $2 < \sqrt{2} + 1$ (by multiplying/dividing both sides by $\sqrt{2}$). And this is true if, and only if, $1 < \sqrt{2}$ (by subtracting/adding 1 on both sides). But $1 < \sqrt{2}$, and so the inequality holds for $n = 2$.

    Show that for all integers $k \ge 2$, if the property is true for $n = k$ then it is true for $n = k+1$: Suppose $\sqrt{k} < \frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{k}}$ for some integer $k \ge 2$. *[This*

is the inductive hypothesis.] We must show that $\sqrt{k+1} < \dfrac{1}{\sqrt{1}} + \dfrac{1}{\sqrt{2}} + \dfrac{1}{\sqrt{3}} + \cdots + \dfrac{1}{\sqrt{k+1}}$. But for each integer $k \geq 2$, $\sqrt{k} < \sqrt{k+1}$ (*), and so (by multiplying both sides by $\sqrt{k}$) $k < \sqrt{k} \cdot \sqrt{k+1}$. Adding 1 to both sides gives $k + 1 < \sqrt{k} \cdot \sqrt{k+1} + 1$, and dividing both sides by $\sqrt{k+1}$ gives $\sqrt{k+1} < \sqrt{k} + \dfrac{1}{\sqrt{k+1}}$. By substitution from the inductive hypothesis, then, $\sqrt{k+1} < \dfrac{1}{\sqrt{1}} + \dfrac{1}{\sqrt{2}} + \dfrac{1}{\sqrt{3}} + \cdots + \dfrac{1}{\sqrt{k}} + \dfrac{1}{\sqrt{k+1}}$ *[as was to be shown].*

(*) *Note:* Strictly speaking, the reason for this claim is that $k < k + 1$ and for all positive real numbers a and b, if $a < b$, then $\sqrt{a} < \sqrt{b}$.

22. *Proof:* Suppose x is a *[particular but arbitrarily chosen]* real number that is greater than -1. We show by mathematical induction that the property $1 + nx \leq (1 + x)^n$ is true for all integers $n \geq 2$.

    Show that the property is true for $n = 2$: To show that the property is true for $n = 2$, we must show that $1 + 2x \leq (1 + x)^2$. But $(1 + x)^2 = 1 + 2x + x^2$, and $1 + 2x \leq 1 + 2x + x^2$ because $x^2 \geq 0$ for all real numbers x. Hence the property is true for $n = 2$.

    Show that for all integers $k \geq 2$, if the property is true for $n = k$ then it is true for $n = k + 1$: Suppose $1 + kx \leq (1 + x)^k$ for some integer $k \geq 2$. *[This is the inductive hypothesis.]* We must show that $1 + (k + 1)x \leq (1 + x)^{k+1}$. But the right-hand side of this inequality is $(1 + x)^{k+1} = (1 + x)^k(1 + x)$, and, by inductive hypothesis, $(1 + x)^k(1 + x) \geq (1 + kx)(1 + x)$ provided $1 + x > 0$, which is true because $x > -1$. Moreover, $(1 + kx)(1 + x) = 1 + kx + x + kx^2 = 1 + (k + 1)x + kx^2 \geq 1 + (k + 1)x$ *[because $kx^2 \geq 0$ for all real numbers x]*, and $1 + (k + 1)x$ is the left-hand side of the inequality to be shown. Thus, by the transitive property of order, $1 + (k + 1)x \leq (1 + x)^{k+1}$ *[which is what was to be shown].*

23. a. *Proof (by mathematical induction):* Let the property $P(n)$ be the inequality $n^3 > 2n + 1$.

    Show that the property is true for $n = 2$: The property is true for $n = 2$ because the left-hand side is $2^3 = 8$ and the right-hand side is $2 \cdot 2 + 1 = 5$, and $8 > 5$.

    Show that for all integers $k \geq 2$, if the property is true for $n = k$ then it is true for $n = k + 1$: Suppose $k^3 > 2k + 1$ for some integer $k \geq 2$. *[This is the inductive hypothesis.]* We must show that $(k + 1)^3 > 2(k + 1) + 1$. But the left-hand side of this inequality is $(k + 1)^3 = k^3 + (3k^2 + 3k + 1)$ $(^1)$, and, by inductive hypothesis, $k^3 + (3k^2 + 3k + 1) > (2k + 1) + (3k^2 + 3k + 1)$.$(^2)$ Now, since $k \geq 2$, we have $3k^2 + 3k + 1 > 3k > 3$ $(^3)$. And putting $(^2)$ and $(^3)$ together gives $k^3 + (3k^2 + 3k + 1) > (2k + 1) + 3 > 2(k + 1) + 1$ $(^4)$ Finally, combining the results from $(^1)$ and $(^4)$ yields $(k + 1)^3 > 2(k + 1) + 1$ *[as was to be shown].*

    b. *Proof (by mathematical induction):* Let the property $P(n)$ be the inequality $n! > n^2$.

    Show that the property is true for $n = 4$: The inequality is true for $n = 4$ because the left-hand side is $4! = 24$ and the right-hand side is $4^2 = 16$, and $24 > 16$.

    Show that for all integers $k \geq 4$, if the property is true for $n = k$ then it is true for $n = k + 1$: Suppose $k! > k^2$ for some integer $k \geq 4$. *[This is the inductive hypothesis.]* We must show that $(k+1)! > (k+1)^2$. But the left-hand side of this inequality is $(k+1)! = (k+1)k!$, and by inductive hypothesis, $(k + 1)k! > (k + 1)k^2 = k^3 + k^2$. By part (a) $k^3 > 2k + 1$. Hence $k^3 + k^2 > k^2 + 2k + 1 = (k + 1)^2$, and thus $(k + 1)! > (k + 1)^2$ *[as was to be shown].*

25. *Proof by mathematical induction:* According to the definition of $b_0, b_1, b_2, \ldots$, $b_0 = 5$ and $b_k = 4 + b_{k-1}$ for all integers $k \geq 1$. Consider the inequality.$(b_n)^2 > 16n^2$. Note that because all terms of the sequence are positive, if $b_n > 4n$ then $(b_n)^2 > 16n^2$. Thus we will let the property $P(n)$ be $b_n > 4n$ and show that this inequality is true for all integers $n \geq 0$.

    Show that the property is true for $n = 0$: We must show that $b_0 > 4 \cdot 0$. But $4 \cdot 0 = 0$ and $b_0 = 5$ by definition of $b_0, b_1, b_2, \ldots$ and $5 > 0$. So the property holds for $n = 0$.

Show that for all integers $k \geq 0$, if the property is true for $n = k$ then it is true for
$n = k + 1$: Suppose that for some integer $k \geq 0$, $b_k > 4k$. *[This is the inductive hypothesis.]*
We must show that $b_{k+1} > 4(k + 1)$. But

$$
\begin{array}{rcll}
b_{k+1} & = & 4 + b_k & \text{by definition of } b_0, b_1, b_2, \ldots \\
\Rightarrow \quad b_{k+1} & > & 4 + 4k & \text{because } b_k > 4k \text{ by inductive hypothesis} \\
\Rightarrow \quad b_{k+1} & > & 4(1 + k) & \text{by factoring out a 4} \\
\Rightarrow \quad b_{k+1} & = & 4(k + 1) & \text{by the commutative law of addition.}
\end{array}
$$

[This is what was to be shown].

26. *Proof by mathematical induction:* According to the definition of $c_0, c_1, c_2, \ldots$, $c_0 = 3$ and
$c_k = (c_{k-1})^2$ for all integers $k \geq 1$. Let the property $P(n)$ be the equation $c_n = 3^{2^n}$.

Show that the property is true for $n = 0$: We must show that $c_0 = 3^{2^0}$. But $3^{2^0} = 3^1 = 3$
and $c_0 = 3$ by definition of $c_0, c_1, c_2, \ldots$. So the property holds for $n = 0$.

Show that for all integers $k \geq 0$, if the property is true for $n = k$ then it is true for
$n = k + 1$: Suppose that for some integer $k \geq 0$, $c_k = 3^{2^k}$. *[This is the inductive hypothesis.]*
We must show that $c_{k+1} = 3^{2^{k+1}}$. But

$$
\begin{array}{rcll}
c_{k+1} & = & (c_k)^2 & \text{by definition of } c_0, c_1, c_2, \ldots \\
& = & (3^{2^k})^2 & \text{by inductive hypothesis} \\
& = & 3^{2^k \cdot 2} & \\
& = & 3^{2^{k+1}} & \text{by the laws of exponents.}
\end{array}
$$

[This is what was to be shown].

27. *Proof by mathematical induction:* According to the definition of $d_1, d_2, d_3, \ldots$, $d_1 = 2$ and
$d_k = \dfrac{d_{k-1}}{k}$ for all integers $k \geq 2$. Let the property $P(n)$ be the equation. $d_n = \dfrac{2}{n!}$.

Show that the property is true for $n = 1$: We must show that $d_1 = \dfrac{2}{1!}$. But $\dfrac{2}{1!} = 2$ and
$d_1 = 2$ by definition of $d_1, d_2, d_3, \ldots$. So the property holds for $n = 1$.

Show that for all integers $k \geq 1$, if the property is true for $n = k$ then it is true for
$n = k + 1$: Suppose that for some integer $k \geq 1$, $d_k = \dfrac{2}{k!}$. *[This is the inductive hypothesis.]*
We must show that $d_{k+1} = \dfrac{2}{(k + 1)!}$. But

$$
\begin{array}{rcll}
d_{k+1} & = & \dfrac{d_k}{k + 1} & \text{by definition of } d_1, d_2, d_3, \ldots \\[2ex]
& = & \dfrac{\frac{2}{k!}}{k + 1} & \text{by inductive hypothesis} \\[2ex]
& = & \dfrac{2}{(k + 1)k!} & \\[2ex]
& = & \dfrac{2}{(k + 1)!} & \text{by the algebra of fractions.}
\end{array}
$$

[This is what was to be shown].

28. *Proof by mathematical induction:* Let the property $P(n)$ be the equation

$$
\frac{1}{3} = \frac{1 + 3 + 5 + \cdots + (2n - 1)}{(2n + 1) + (2n + 3) + \cdots + (4n - 1)}.
$$

Show that the property is true for $n = 1$: For $n = 1$ the property simply asserts that $\frac{1}{3} = \frac{1}{3}$, which is true.

Show that for all integers $k \geq 1$, if the property is true for $n = k$ then it is true for $n = k + 1$: Suppose that for some integer $k \geq 1$, $\frac{1}{3} = \dfrac{1 + 3 + 5 + \cdots + (2k - 1)}{(2k + 1) + (2k + 3) + \cdots + (4k - 1)}$.

[This is the inductive hypothesis.] Cross-multiplying this equation gives $(2k + 1) + (2k + 3) + \cdots + (4k - 1) = 3[1 + 3 + 5 + \cdots + (2k - 1)]$, and thus the inductive hypothesis is equivalent to $(2k + 3) + \cdots + (4k - 1) = 3[1 + 3 + 5 + \cdots + (2k - 1)] - (2k + 1)$. We must show that

$$\frac{1}{3} = \frac{1 + 3 + 5 + \cdots + [2(k + 1) - 1]}{[2(k + 1) + 1] + [2(k + 1) + 3] + \cdots + [4(k + 1) - 1]},$$

or, equivalently,

$$\frac{1}{3} = \frac{1 + 3 + 5 + \cdots + (2k + 1)}{(2k + 3) + (2k + 5) + \cdots + (4k + 3)}.$$

Now the right-hand side of the equation to be shown is

$$\frac{1 + 3 + 5 + \cdots + (2k + 1)}{(2k + 3) + (2k + 5) + \cdots + (4k + 3)}$$

$$= \frac{1 + 3 + 5 + \cdots + (2k - 1) + (2k + 1)}{(2k + 3) + (2k + 5) + \cdots + (4k - 1) + (4k + 1) + (4k + 3)}$$

by making more terms explicit

$$= \frac{1 + 3 + 5 + \cdots + (2k - 1) + (2k + 1)}{[3(1 + 3 + 5 + \cdots + (2k - 1)) - (2k + 1)] + (4k + 1) + (4k + 3)}$$

by inductive hypothesis

$$= \frac{1 + 3 + 5 + \cdots + (2k - 1) + (2k + 1)}{3[1 + 3 + 5 + \cdots + (2k - 1)] + (6k + 3)}$$

$$= \frac{1 + 3 + 5 + \cdots + (2k - 1) + (2k + 1)}{3[1 + 3 + 5 + \cdots + (2k - 1)] + 3(2k + 1)}$$

$$= \frac{1 + 3 + 5 + \cdots + (2k - 1) + (2k + 1)}{3[1 + 3 + 5 + \cdots + (2k - 1) + (2k + 1)]}$$

$$= \frac{1}{3} \qquad \text{by basic algebra}$$

[as was to be shown].

29. Let $P(n)$ be the property "if n people come to the meeting and each shakes hands with all the others present, then $\dfrac{k(k - 1)}{2}$ handshakes occur." We show by mathematical induction that this property holds for all integers $n \geq 2$.

    Proof (by mathematical induction):

    Show that the property is true for $n = 2$: The property is true for $n = 2$ because on the one hand if two people come to the meeting and each shakes hands with each of the others present, then just one handshake occurs, and on the other hand $\dfrac{2 \cdot (2 - 1)}{2}$ equals 1 also.

    Show that for all integers $k \geq 2$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let k be an integer with $k \geq 2$, and suppose that if k people come to the meeting and each shakes hands with all the others present, then $\dfrac{k(k - 1)}{2}$ handshakes occur. *[This is the inductive hypothesis.]* We must show that if $k + 1$ people come to the meeting and each shakes hands with all the others present, then $\dfrac{(k + 1)((k + 1) - 1)}{2} = \dfrac{(k + 1)k}{2}$ handshakes

occur. But if $k+1$ people come to the meeting, then after the kth person has arrived and shaken hands all around, $\dfrac{k(k-1)}{2}$ handshakes have occurred (by inductive hypothesis). When the $(k+1)$st person arrives and shakes hands with all k others, k additional handshakes occur. Thus, as was to be shown, the total number of handshakes is

$$\frac{k(k-1)}{2} + k = \frac{k^2 - k + 2k}{2} = \frac{k^2 + k}{2} = \frac{(k+1)k}{2}$$

[as was to be shown].

32. *Proof (by mathematical induction)*: Let the property $P(n)$ be the sentence "If one square is removed from a $2^n \times 2^n$ checkerboard, then the remaining squares can be completely covered by trominos."

   Show that the property is true for $n = 1$: A $2^1 \times 2^1$ checkerboard just consists of four squares. If one square is removed, the remaining squares form an L, which can be covered with a tromino, as illustrated below.
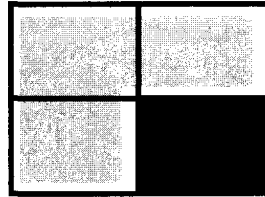
   Show that for all integers $k \geq 1$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let k be an integer with $k \geq 1$, and suppose that if one square is removed from a $2^k \times 2^k$ checkerboard, then the remaining squares can be completely covered by trominos. *[This is the inductive hypothesis.]* Consider a $2^{k+1} \times 2^{k+1}$ checkerboard with one square removed. Divide it into four equal quadrants, each consisting of a $2^k \times 2^k$ checkerboard. In one of the quadrants, one square will have been removed, and so, by inductive hypothesis, all the remaining squares in this quadrant can be completely covered by trominos. The other three quadrants meet at the center of the checkerboard, and the center of the checkerboard serves as a corner of a square from each of those quadrants. A tromino can, therefore, be placed on those three central squares. This situation is illustrated in the following figure:
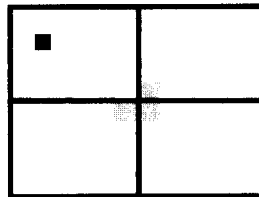
   By inductive hypothesis, the remaining squares in each of the three quadrants can be completely covered by trominos. Thus every square in the $2^{k+1} \times 2^{k+1}$ checkerboard except the one that was removed can be completely covered by trominos *[as was to be shown]*.

   Note: Proposition 4.3.1 can be deduced as a corollary to the result of this exercise.

33. Let $P(n)$ be the property that "in any round-robin tournament involving n teams, it is possible to label the teams $T_1, T_2, T_3, \ldots, T_n$ so that T_i beats T_{i+1} for all $i = 1, 2, 3, \ldots, n-1$." We will show by mathematical induction that this property is true for all integers $n \geq 2$.

   Show that the property is true for $n = 2$: Consider any round-robin tournament involving two teams. By definition of round-robin tournament, these teams play each other exactly once. Let T_1 be the winner and T_2 the loser of this game. Then T_1 beats T_2, and so the labeling is as required.

   Show that for all integers $k \geq 2$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let k be an integer with $k \geq 2$ and suppose that in any round-robin tournament

involving k teams it is possible to label the teams in the way described. *[This is the inductive hypothesis.]* We must show that in any round-robin tournament involving $k + 1$ teams it is possible to label the teams in the way described.

Consider any round-robin tournament with $k + 1$ teams. Pick one and call it T'. Temporarily remove T' and consider the remaining k teams. Since each of these teams plays each other team exactly once, the games played by these k teams form a round-robin tournament. It follows by inductive hypothesis that these k teams may be labeled $T_1, T_2, T_3, \ldots, T_k$ where T_i beats T_{i+1} for all $i = 1, 2, 3, \ldots, k - 1$.

Case 1 (T' beats T_1): In this case, relabel each T_i to be T_{i+1}, and let $T_1 = T'$. Then T_1 beats the newly labeled T_2 (because T' beats the old T_1), and T_i beats T_{i+1} for all $i = 2, 3, \ldots, k$ (by inductive hypothesis).

Case 2 (T' loses to $T_1, , T_2, T_3, \ldots, T_m$ and beats T_{m+1} where $1 \le m \le k - 1$): In this case, relabel teams $T_{m+1}, T_{m+2}, \ldots, T_k$ to be $T_{m+2}, T_{m+3}, \ldots, T_{k+1}$ and let $T_{m+1} = T'$. Then for each i with $1 \le i \le m - 1$, T_i beats T_{i+1} (by inductive hypothesis), T_m beats T_{m+1} (because T_m beats T'), T_{m+1} beats T_{m+2} (because T' beats the old T_{m+1}), and for each i with $m + 2 \le i \le k$, T_i beats T_{i+1} (by inductive hypothesis).

Case 3 (T' loses to T_i for all $i = 1, 2, \ldots, k$): In this case, let $T_{k+1} = T'$. Then for all $i = 1, 2, \ldots, k - 1$, T_i beats T_{i+1} (by inductive hypothesis) and T_k beats T_{k+1} (because T_k beats T').

Thus in all three cases the teams may be relabeled in the way specified *[as was to be shown]*.

34. *Proof by contradiction:* Suppose not. Suppose it is impossible to find three successive integers on the rim of the disk whose sum is at least 45. *[We must derive a contradiction.]* Then there is some ordering of the integers from 1 to 30, say $x_1, x_2, \ldots, x_{30}$ such that

$$x_1 + x_2 + x_3 < 45$$
$$x_2 + x_3 + x_4 < 45$$
$$x_3 + x_4 + x_5 < 45$$
$$\cdot$$
$$\cdot$$
$$\cdot$$
$$x_{29} + x_{30} + x_1 < 45$$
$$x_{30} + x_1 + x_2 < 45.$$

Adding all these inequalities gives $3 \sum_{i=1}^{30} x_i < 30 \cdot 45 = 1350$. But $\sum_{i=1}^{30} x_i = \sum_{i=1}^{30} i$ because the sequence $x_1, x_2, \ldots, x_{30}$ is a rearrangement of the integers from 1 to 30. Hence $3 \sum_{i=1}^{30} i < 1350$, and so by the formula for the sum of the first n integers, $3 \left(\dfrac{30 \cdot 31}{2} \right) < 1350$, or, equivalently, $1395 < 1350$. But $1395 \ge 1350$, and so we have arrived at a contradiction. *[Hence the supposition is false and the given statement is true.]*

Section 4.4

2. *Proof:* Let the property $P(n)$ be the sentence "b_n is divisible by 4." We prove by strong mathematical induction that this property is true for all integers $n \ge 1$.

Show that the property is true for $n = 1$ and $n = 2$: $b_1 = 4$ and $b_2 = 12$ and both 4 and 12 are divisible by 4. So the property is true for $n = 1$ and 2.

Show that if $k > 2$ and the property is true for all integers i with $1 \le i < k$, then it is true for $n = k$: Let $k > 2$ be an integer, and suppose b_i is divisible by 4 for all

integers i with $1 \le i < k$. [*This is the inductive hypothesis.*] We must show that b_k is divisible by 4. But by definition of $b_1, b_2, b_3, \ldots, b_k = b_{k-2} + b_{k-1}$. Since $k > 2$, $0 < k - 2 < k$ and $1 < k - 1 < k$, and so, by inductive hypothesis, both b_{k-2} and b_{k-1} are divisible by 4. But the sum of any two numbers that are divisible by 4 is also divisible by 4 [*exercise 15 of Section 3.3*], so the sum of b_{k-2} and b_{k-1}, which equals b_k, is also divisible by 4 [*as was to be shown*].

3. *Proof*: Let the property $P(n)$ be the sentence "c_n is even." We prove by strong mathematical induction that this property is true for all integers $n \ge 0$.

   Show that the property is true for $n = 0$, $n = 1$, and $n = 2$: $c_0 = 2$, $c_1 = 2$, and $c_2 = 6$ and 2, 2, and 6 are all even. So the property is true for $n = 0$, 1, and 2.

   Show that if $k > 2$ and the property is true for all integers i with $0 \le i < k$, then it is true for $n = k$: Let $k > 2$ be an integer, and suppose c_i is even for all integers i with $1 \le i < k$. [*This is the inductive hypothesis.*] We must show that c_k is even. But by definition of $c_0, c_1, c_2, \ldots, c_k = 3c_{k-3}$. Since $k > 2$, $0 \le k - 3 < k$, and so, by inductive hypothesis, c_{k-3} is even. But the product of an even integer with any integer is even [*exercise 42, Section 3.1 or Example 3.2.3*], and so $3c_{k-3}$, which equals c_k, is also even [*as was to be shown*].

5. *Proof*: Let the property $P(n)$ be the inequality $e_n \le 3^n$. We prove by strong mathematical induction that this property is true for all integers $n \ge 0$.

   Show that the property is true for $n = 0$, $n = 1$, and $n = 2$: $e_0 = 1$, $e_1 = 2$, and $e_2 = 3$ and $1 \le 3^0$, $2 \le 3^1$, and $3 \le 3^2$. So the property is true for $n = 0$, 1, and 2.

   Show that if $k > 2$ and the property is true for all integers i with $0 \le i < k$, then it is true for $n = k$: Let k be an integer with $k > 2$, and suppose the property is true for all integers i with $0 \le i < k$. We must show that the property is true for k. But

$$
\begin{array}{rlll}
& h_k & = & h_{k-1} + h_{k-2} + h_{k-3} \quad \text{by definition of } h_0, h_1, h_2, \ldots \\
\Rightarrow & h_k & \le & 3^{k-1} + 3^{k-2} + 3^{k-3} \quad \text{by inductive hypothesis} \\
\Rightarrow & h_k & \le & 3^{k-3}(3^2 + 3 + 1) \quad \text{because } 3^{k-3} \cdot 3^2 = 3^{k-1} \text{ and } 3^{k-3} \cdot 3 = 3^{k-2}.
\end{array}
$$

   But $3^2 + 3 + 1 = 13 \le 27 = 3^3$. Hence by order properties of the real numbers (Appendix A, T17 and T19),

$$
h_k \le 3^{k-3} \cdot 3^3 = 3^k
$$

   [*as was to be shown*].

6. *Proof*: Let the property $P(n)$ be the inequality $f_n \le n$. We prove by strong mathematical induction that this property is true for all integers $n \ge 1$.

   Show that the property is true for $n = 1$: $f_1 = 1$ and $1 \le 1$. So the property is true for $n = 1$.

   Show that if $k > 1$ and the property is true for all integers i with $1 \le i < k$, then it is true for $n = k$: Let $k > 1$ be an integer, and suppose $f_i \le i$ for all integers i with $1 \le i < k$. [*This is the inductive hypothesis.*] We must show that $f_k \le k$. But by definition of $f_1, f_2, f_3, \ldots, f_k = 2 \cdot f_{\lfloor k/2 \rfloor}$. Since $k > 1$, $1 \le \lfloor k/2 \rfloor < k$, and so, by inductive hypothesis, $f_{\lfloor k/2 \rfloor} \le \lfloor k/2 \rfloor$. Thus

$$
f_k = 2 \cdot f_{\lfloor k/2 \rfloor} \le 2 \cdot \lfloor k/2 \rfloor = \left\{ \begin{array}{l} 2 \cdot ((k-1)/2) \text{ if } k \text{ is odd} \\ 2 \cdot (k/2) \text{ if } k \text{ is even} \end{array} \right. = \left\{ \begin{array}{l} k - 1 \text{ if } k \text{ is odd} \\ k \text{ if } k \text{ is even} \end{array} \right. \le k,
$$

   and so $f_k \le k$ [*as was to be shown*].

8. Note that the proof for part (a) for this exercise is identical to the proof given as the answer to exercise 5.

   a. Proof: Let the property $P(n)$ be the inequality $h_n \le 3^n$. We prove by strong mathematical induction that this property is true for all integers $n \ge 0$.

Show that the property is true for $n = 0$, $n = 1$, and $n = 2$: Note that $h_0 = 1 \le 3^0$, $h_1 = 2 \le 3^1$, and $h_2 = 3 \le 3^2$. So the property is true for $n = 0, 1$, and 2.

Show that if $k > 2$ and the property is true for all integers i with $0 \le i < k$, then it is true for $n = k$: Let k be an integer with $k > 2$, and suppose the property is true for all integers i with $0 \le i < k$. We must show that the property is true for k. But

$$
\begin{aligned}
h_k &= h_{k-1} + h_{k-2} + h_{k-3} && \text{by definition of } h_0, h_1, h_2, \ldots \\
\Rightarrow h_k &\le 3^{k-1} + 3^{k-2} + 3^{k-3} && \text{by inductive hypothesis} \\
\Rightarrow h_k &\le 3^{k-3}(3^2 + 3 + 1) && \text{because } 3^{k-3} \cdot 3^2 = 3^{k-1} \text{ and } 3^{k-3} \cdot 3 = 3^{k-2}.
\end{aligned}
$$

But $3^2 + 3 + 1 = 13 \le 27 = 3^3$. Hence by order properties of the real numbers (Appendix A, T17 and T19),

$$ h_k \le 3^{k-3} \cdot 3^3 = 3^k $$

[as was to be shown].

b. Proof: Let s be any real number such that $s^3 \ge s^2 + s + 1$, and let $P(n)$ be the inequality $h_n \le s^n$. We prove by strong mathematical induction that this property is true for all integers $n \ge 2$.

Show that the property is true for $n = 2$, $n = 3$, and $n = 4$: Because $s \ge 1.83$, $h_2 = 3 \le 3.3489 = 1.83^2 < s^2$, $h_3 = h_0 + h_1 + h_2 = 1 + 2 + 3 = 6 \le 6.128487 = 1.83^3$, and $h_4 = h_1 + h_2 + h_3 = 2 + 3 + 6 = 11 \le 11.21513121 = 1.83^4$. So the property is true for $n = 2$, 3, and 4.

Show that if $k > 4$ and the property is true for all integers i with $2 \le i < k$, then it is true for $n = k$: Let k be an integer with $k > 4$, and suppose the property is true for all integers i with $2 \le i < k$. We must show that the property is true for k. But

$$
\begin{aligned}
h_k &= h_{k-1} + h_{k-2} + h_{k-3} \\
\Rightarrow h_k &\le s^{k-1} + s^{k-2} + s^{k-3} && \text{by inductive hypothesis} \\
\Rightarrow h_k &\le s^{k-3}(s^2 + s + 1) && \text{because } s^{k-3} \cdot s^2 = s^{k-1} \text{ and } s^{k-3} \cdot s = s^{k-2}. \\
\Rightarrow h_k &\le s^{k-3} \cdot s^3 = s^k && \text{by hypothesis about } s, s^2 + s + 1 \le s^3
\end{aligned}
$$

[as was to be shown].

9. *Proof:* Let the property $P(n)$ be the inequality $a_n \le \left(\dfrac{7}{4}\right)^n$. We prove by strong mathematical induction that this property is true for all integers $n \ge 1$.

Show that the property is true for $n = 1$ and $n = 2$: By definition of $a_1, a_2, a_3, \ldots$, $a_1 = 1$ and $a_2 = 3$. But $1 < \dfrac{7}{4}$ and $\left(\dfrac{7}{4}\right)^2 = \dfrac{49}{16} = 3\dfrac{1}{16} > 3$. So $a_1 \le \dfrac{7}{4}$ and $a_2 \le \left(\dfrac{7}{4}\right)^2$, and thus the property is true for $n = 1$ and $n = 2$.

Show that if $k > 2$ and the property is true for all integers i with $1 \le i < k$, then it is true for $n = k$: Let $k > 2$ be an integer, and suppose $a_i \le \left(\dfrac{7}{4}\right)^i$ for all integers i with $1 \le i < k$. *[This is the inductive hypothesis.]* We must show that $a_k \le \left(\dfrac{7}{4}\right)^k$. But by definition of $a_1, a_2, a_3, \ldots$, $a_k = a_{k-1} + a_{k-2}$. Since $k > 2$, $1 \le k - 2 < k - 1 < k$, and so by inductive hypothesis, $a_{k-1} \le \left(\dfrac{7}{4}\right)^{k-1}$ and $a_{k-2} \le \left(\dfrac{7}{4}\right)^{k-2}$. Adding the inequalities and using the laws of basic algebra gives

$$
a_{k-1} + a_{k-2} \le \left(\frac{7}{4}\right)^{k-1} + \left(\frac{7}{4}\right)^{k-2} = \left(\frac{7}{4}\right)^{k-2}\left(\frac{7}{4} + 1\right) = \left(\frac{7}{4}\right)^{k-2}\left(\frac{11}{4}\right)
$$

$$
= \left(\frac{7}{4}\right)^{k-2}\left(\frac{44}{16}\right) < \left(\frac{7}{4}\right)^{k-2}\left(\frac{49}{16}\right) = \left(\frac{7}{4}\right)^{k-2}\left(\frac{7}{4}\right)^2 = \left(\frac{7}{4}\right)^k.
$$

So $a_{k-1} + a_{k-2} \le \left(\dfrac{7}{4}\right)^k$ [as was to be shown].

11. *Proof*: Let the property $P(n)$ be the sentence "n is either a prime number or a product of prime numbers." We prove by strong mathematical induction that this property is true for all integers $n \ge 2$.

Show that the property is true for $n = 2$: When $n = 2$, the sentence is "2 is either a prime number or a product of prime numbers." This sentence is true because 2 is prime.

Show that if $k > 2$ and the property is true for all integers i with $1 \le i < k$, then it is true for $n = k$: Let $k > 2$ be an integer, and suppose that i is either a prime number or a product of prime numbers for all integers i with $1 \le i < k$. [This is the inductive hypothesis.] We must show that k is either a prime number or a product of prime numbers. In case k is prime, the sentence is true. So suppose k is not prime. Then, by definition of prime, $k = rs$ for some positive integers r and s with $r \ne 1$ and $s \ne 1$. By Example 3.3.3, $r \le k$ and $s \le k$, and, because neither r nor s equals 1, $r < k$ and $s < k$. Thus, by inductive hypothesis, each of r and s is either a prime number or a product of prime numbers. So, because k is the product of r and s, k is a product of prime numbers [as was to be shown].

13. *Proof*: Let the property $P(n)$ be the sentence "A sum of n even integers is even." We prove by strong mathematical induction that this property is true for all integers $n \ge 2$.

Show that the property is true for $n = 2$: The property is true for $n = 2$ because any sum of two even integers is even [Theorem 3.1.1].

Show that if $k > 2$ and the property is true for all integers i with $1 \le i < k$, then it is true for $n = k$: Let $k > 2$ be an integer, and suppose that for all integers i with $1 \le i < k$, any sum of i even integers is even. [This is the inductive hypothesis.] We must show that any sum of $i + 1$ even integers is even. Suppose $a_1 + a_2 + a_3 + \cdots + a_i + a_{i+1}$ is any sum of $i + 1$ even integers. By regrouping [for a formal justification of this step, see Section 8.4], we have $a_1 + a_2 + a_3 + \cdots + a_{k-1} + a_k = (a_1 + a_2 + a_3 + \cdots + a_{k-1}) + a_k$, and by inductive hypothesis $a_1 + a_2 + a_3 + \cdots + a_{k-1}$ is even. Thus $a_1 + a_2 + a_3 + \cdots + a_{k-1} + a_k$ equals a sum of two even integers and is, therefore, even by Theorem 3.1.1. [This is what was to be shown.]

14. *Proof*: Let the property $P(n)$ be the sentence "If n is even, a sum of n odd integers is even, and if n is odd, a sum of n odd integers is odd." We prove by strong mathematical induction that this property is true for all integers $n \ge 2$.

Show that the property is true for $n = 2$: The property is true for $n = 2$ because any sum of two odd integers is even [exercise 27, Section 3.1 or Example 3.2.3].

Show that if $k > 2$ and the property is true for all integers i with $1 \le i < k$, then it is true for $n = k$: Let $k > 2$ be an integer, and suppose that for all integers i with $1 \le i < k$, if i is even, any sum of i odd integers is even, and if i is odd, any sum of i odd integers is odd. [This is the inductive hypothesis.] We must show that if k is even, any sum of k odd integers is even, and if k is odd, any sum of k odd integers is odd. Suppose $a_1 + a_2 + a_3 + \cdots + a_{k-1} + a_k$ is any sum of k odd integers.

Case 1 (k is odd): In this case $k - 1$ is even, and so $a_1 + a_2 + a_3 + \cdots + a_{k-1}$ is even by inductive hypothesis. Then $a_1 + a_2 + a_3 + \cdots + a_{k-1} + a_k = (a_1 + a_2 + a_3 + \cdots + a_{k-1}) + a_k$ is a sum of an even integer and an odd integer. So it is odd [exercise 19, Section 3.1 or Example 3.2.3].

Case 2 (k is even): In this case $k - 1$ is odd, and so $a_1 + a_2 + a_3 + \cdots + a_{k-1}$ is odd by inductive hypothesis. Then $a_1 + a_2 + a_3 + \cdots + a_{k-1} + a_k = (a_1 + a_2 + a_3 + \cdots + a_{k-1}) + a_k$ is a sum of two odd integers. So it is even [exercise 27, Section 3.1 or Example 3.2.3].

Thus if k is even, any sum of k odd integers is even, and if k is odd, any sum of k odd integers is odd [as was to be shown].

16. *Conjecture*: For all integers $n \geq 0$, the units digit of 3^n is 1 if $n \bmod 4 = 0$, 3 if $n \bmod 4 = 1$, 9 if $n \bmod 4 = 2$, and 7 if $n \bmod 4 = 3$.

   Proof [by strong mathematical induction]: Let the property $P(n)$ be the sentence "The units digit of 3^n is 1 if $n \bmod 4 = 0$, 3 if $n \bmod 4 = 1$, 9 if $n \bmod 4 = 2$, and 7 if $n \bmod 4 = 3$."

   Show that the property is true for $n = 0$, $n = 1$, $n = 2$, and $n = 3$: When $n = 0$, $n \bmod 4 = 0$ and the units digit of $3^0 = 1$. When $n = 1$, $n \bmod 4 = 1$ and the units digit of $3^1 = 3$. When $n = 2$, $n \bmod 4 = 2$ and the units digit of $3^2 = 9$. And when $n = 3$, $n \bmod 4 = 2$ and since $3^3 = 27$, the units digit of $3^3 = 7$.

   Show that if $k > 3$ and the property is true for all integers i with $1 \leq i < k$, then it is true for $n = k$: Let $k > 3$ be an integer, and suppose that for all integers i with $1 \leq i < k$, the units digit of 3^i is 1 if $i \bmod 4 = 0$, 3 if $i \bmod 4 = 1$, 9 if $i \bmod 4 = 2$, and 7 if $i \bmod 4 = 3$. We must show that the units digit of 3^k is 1 if $k \bmod 4 = 0$, 3 if $k \bmod 4 = 1$, 9 if $k \bmod 4 = 2$, and 7 if $k \bmod 4 = 3$.

   Case 1 ($k \bmod 4 = 0$): In this case $k = 4r$ for some integer r, and so $k - 1 = 4r - 1 = 4(r-1) + 3$. Thus $(k-1) \bmod 4 = 3$, and, by inductive hypothesis, the units digit of 3^{k-1} is 7. So $3^{k-1} = 10s + 7$ for some integer s, and hence $3^k = 3 \cdot 3^{k-1} = 3(10s + 7) = 30s + 21 = 30s + 20 + 1 = (3s + 2) \cdot 10 + 1$. Because $3s + 2$ is an integer, it follows that the units digit of 3^k is 1.

   Case 2 ($k \bmod 4 = 1$): In this case $k = 4r + 1$ for some integer r, and so $k - 1 = (4r+1) - 1 = 4r$. Thus $(k-1) \bmod 4 = 0$, and, by inductive hypothesis, the units digit of 3^{k-1} is 1. So $3^{k-1} = 10s + 1$ for some integer s, and hence $3^k = 3 \cdot 3^{k-1} = 3(10s + 1) = 30s + 3 = (3s) \cdot 10 + 3$. Because $3s$ is an integer, it follows that the units digit of 3^k is 3.

   Case 3 ($k \bmod 4 = 2$): In this case $k = 4r + 2$ for some integer r, and so $k - 1 = (4r + 2) - 1 = 4r + 1$. Thus $(k-1) \bmod 4 = 1$, and, by inductive hypothesis, the units digit of 3^{k-1} is 3. So $3^{k-1} = 10s + 3$ for some integer s, and hence $3^k = 3 \cdot 3^{k-1} = 3(10s + 3) = 30s + 9 = (3s) \cdot 10 + 9$. Because $3s$ is an integer, it follows that the units digit of 3^k is 9.

   Case 4 ($k \bmod 4 = 3$): In this case $k = 4r + 3$ for some integer r, and so $k - 1 = (4r + 3) - 1 = 4r + 2$. Thus $(k-1) \bmod 4 = 9$, and, by inductive hypothesis, the units digit of 3^{k-1} is 9. So $3^{k-1} = 10s + 9$ for some integer s, and hence $3^k = 3 \cdot 3^{k-1} = 3(10s + 9) = 30s + 27 = 30s + 20 + 7 = (3s + 2) \cdot 10 + 7$. Because $3s + 2$ is an integer, it follows that the units digit of 3^k is 7.

   Hence in all four cases the units digit of 3^k is as specified *[as was to be shown]*.

17. The inductive step fails when $k = 1$. The reason is that to go from $k = 1$ to $k = 2$, one evaluates $\dfrac{r^{k-1} \cdot r^{k-1}}{r^{k-2}}$ for $k = 1$. But the inductive hypothesis only says that $r^i = 1$ for all i with $0 \leq i < k$ and when $k = 1$ then $k - 2 = -1 < 0$. Therefore one cannot deduce from the inductive hypothesis that $r^{k-2} = 1$.

19. *Proof*: Suppose n is any integer that is greater than 1. Let S be the set of all positive integers that are divisors of n. Then S has at least one element because n is a divisor of n. Hence by the well-ordering principle for the integers, S has a least element, say p. Suppose that p is not prime. Then $p = rs$ for some positive integers r and s with $r \neq 1$ and $s \neq 1$. Thus r is a divisor of p and p is a divisor of n, and so, by the transitivity of divisibility (Theorem 3.3.2), r is a divisor of n. Also, because $s > 1$ and $p = rs$, $r \neq p$. But by Example 3.3.3, $r \leq p$, and thus $r < p$. Therefore, r is in S and r is smaller than the least element of S, which is impossible. Hence the supposition that p is not prime is false, and we can conclude that p is prime and, thus, that n is divisible by the prime number p.

23. *Proof*: Suppose a and b are any integers that are not both zero. Let S be the set of all positive integers of the form $ua + vb$ for some integers u and v.

   We first show that S has one or more elements. Since a and b are not both zero, one of them

is nonzero. Without loss of generality, we may assume that $a \neq 0$. In case $a > 0$, let $u = 1$ and $v = 0$, and in case $a < 0$, let $u = -1$ and $v = 0$. In the first case, $ua + vb = a \in S$, and in the second case $ua + vb = -a \in S$. So in either case, S has one or more elements. Hence by the well-ordering principle for the integers, S has a least element, say m. Then $m = u_0 a + v_0 b$ for some particular integers u_0 and v_0.

We next show that $m \mid a$ and $m \mid b$. By the quotient-remainder theorem, $a = mq + r$ where $0 \leq r < m$. Then $r = a - mq = a - (u_0 a + v_0 b)q = (1 - u_0 q)a - (v_0 q)b$. Thus by definition of S, $r \in S$ (if r is positive) or else $r = 0$. But if $r \in S$, then $m \leq r$ (since m is the *least* element of S) which is impossible because $r < m$. Hence $r \notin S$, and so $r = 0$ and $m \mid a$. A similar argument shows that $m \mid b$. Hence m is a common divisor of a and b.

Finally we show that m is the *greatest* common divisor of a and b. Suppose c is any integer such that $c \mid a$ and $c \mid b$. Then $a = rc$ and $b = sc$ for some integers r and s, and so $u_0 a = u_0 rc = (u_0 r)c$ and $v_0 b = v_0 sc = (v_0 s)c$. Since u_0, r, v_0, and s are all integers, $c \mid u_0 a$ and $c \mid v_0 b$, and so $c \mid (u_0 a + v_0 b)$ *[by exercise 15 of Section 3.3]*. Hence, if $c \mid a$ and $c \mid b$ then $c \mid m$. But since $c \mid m$ and $m > 0$, then $c \leq m$. *[If c is positive, this is true by Example 3.3.3. If c is negative, it is true because each negative integer is less than each positive integer.]* Therefore, $m = \gcd(a, b)$.

24. No.

Counterexample 1: Let $P(n)$ be "$n \neq 4$." Then $P(0)$, $P(1)$, and $P(2)$ are all true (because $0 \neq 4$, $1 \neq 4$, and $2 \neq 4$,), and for all integers $k \geq 0$, if $P(k)$ is true then $P(3k)$ is true (because if $k \neq 4$ then $3k \neq 4$). But when $n = 4$, the statement $n \neq 4$ is false. So it is not the case that $P(n)$ is true for all integers $n \geq 0$

Counterexample 2: Let $P(n)$ be "$n + 24$ is composite." Then $P(0)$, $P(1)$, and $P(2)$ are all true (because 24, 25, and 26 are composite), and for all integers $k \geq 0$, if $P(k)$ is true then $P(3k)$ is true (because if $k + 24$ is composite then $3k + 24$ is also composite — in fact, $3k + 24$ is composite for *any* integer $k \geq 0$). But it is false that $n + 24$ is composite for all integers $n \geq 0$ (because, for instance, $5 + 24 = 29$ is prime).

Counterexample 3: Let $P(n)$ be "$n = 0$, or $n = 1$, or $n = 2$, or $n = 3r$ for some integer r." Then $P(0)$, $P(1)$, and $P(2)$ are all true (because an *or* statement is true if any component is true), and for all integers $k \geq 0$, if $P(k)$ is true then $P(3k)$ is true (also by definition of the truth value of an *or* statement and by definition of $P(n)$). But $P(n)$ is not true for all integers $n \geq 0$ (because, for instance, $P(4)$ is not true).

(There are many other counterexamples besides these two.)

25. Suppose $P(n)$ is a property that is defined for integers n and suppose the statement "$P(n)$ is true for all integers $n \geq a$" can be proved using strong mathematical induction. Then for some integer b the following two statements are true:

1. $P(a)$, $P(a + 1)$, $P(a + 2)$, ..., $P(b)$ are all true.

2. For any integer $k > b$, if $P(i)$ is true for all integers i with $a \leq i < k$, then $P(k)$ is true.

We will show that we can reach the conclusion that $P(n)$ is true for all integers $n \geq a$ using ordinary mathematical induction.

Proof: Let $Q(n)$ be the property "$P(j)$ is true for all integers j with $a \leq j \leq n$."

Show that the property is true for $n = b$: For $n = b$, the property is "$P(j)$ is true for all integers j with $a \leq j \leq b$." But this is true by (1) above.

Show that for all integers $k \geq b$, if the property is true for $n = k$, then it is true for $n = k + 1$: Let k be any integer with $k \geq b$ and suppose $Q(k)$ is true. By definition of Q this means that $P(j)$ is true for all integers j with $a \leq j \leq k$. It follows from (2) above that $P(k + 1)$ is also true. Hence $P(j)$ is true for all integers j with $a \leq j \leq k + 1$. By definition of Q this means that $Q(k + 1)$ is true.

It follows by the principle of ordinary mathematical induction that $Q(n)$ is true for all integers $n \geq b$. From this and from (1) above, we conclude that $P(n)$ is true for all integers $n \geq a$.

26. *Example 1 (k is even)*: Let $k = 42$. Then $k/2 = 21 = 16 + 4 + 1 = 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2 + 1$. To obtain the binary representation for k, multiply the representation for $k/2$ by 2 and add $0 \ (= 0 \cdot 1)$: $k = 2 \cdot (1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2 + 1) + 0 \cdot 1 = 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2 + 0 \cdot 1$. Thus $k_2 = 101010_2$.

Example 2 (k is odd): Let $k = 43$. Then $(k-1)/2 = 21 = 16 + 4 + 1 = 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2 + 1$. To obtain the binary representation for k, multiply the representation for $(k-1)/2$ by 2 and add $1 \ (= 1 \cdot 1)$: $k = 2 \cdot (1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2 + 1) + 1 \cdot 1 = 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2 + 1 \cdot 1$. Thus $k_2 = 101011_2$.

27. *Proof*: Consider the property "n can be written in the form

$$n = c_r \cdot 3^r + c_{r-1} 3^{r-1} + \cdots + c_2 \cdot 3^2 + c_1 \cdot 3 + c_0$$

where r is a nonnegative integer, $c_r = 1$ or 2 and $c_j = 0, 1,$ or 2 for all $j = 0, 1, 2, \ldots, r - 1$."

We will show that the property is true for all integers $n \geq 1$.

Show that the property is true for $n = 1$: Observe that $1 = c_r 3^r$ for $r = 0$ and $c_r = 1$. Thus 1 can be written in the required form.

Show that if $k > 1$ and the property is true for all integers i with $1 \leq i < k$, then it is true for $n = k$: Let k be an integer with $k > 1$, and suppose that for all integers i with $1 \leq i < k$, i can be written in the required form:

$$i = c_r \cdot 3^r + c_{r-1} 3^{r-1} + \cdots + c_2 \cdot 3^2 + c_1 \cdot 3 + c_0$$

where r is a nonnegative integer, $c_r = 1$ or 2 and $c_j = 0, 1,$ or 2 for all $j = 0, 1, 2, , \ldots, r - 1$.

We must show that k can be written in the required form. By the quotient-remainder theorem, k can be written as $3m$, $3m+1$, or $3m+2$ for some integer m. In each case m satisfies $0 \leq m < k$, and so m can be written in the required form:

$$m = c_r \cdot 3^r + c_{r-1} 3^{r-1} + \cdots + c_2 \cdot 3^2 + c_1 \cdot 3 + c_0$$

where r is a nonnegative integer, $c_r = 1$ or 2 and $c_j = 0, 1,$ or 2 for all $j = 0, 1, 2, , \ldots, r - 1$. Then

$$3m = c_r \cdot 3^{r+1} + c_{r-1} 3^r + \cdots + c_2 \cdot 3^3 + c_1 \cdot 3^2 + c_0 \cdot 3 + 0$$
$$3m + 1 = c_r \cdot 3^{r+1} + c_{r-1} 3^r + \cdots + c_2 \cdot 3^3 + c_1 \cdot 3^2 + c_0 \cdot 3 + 1$$
$$3m + 2 = c_r \cdot 3^{r+1} + c_{r-1} 3^r + \cdots + c_2 \cdot 3^3 + c_1 \cdot 3^2 + c_0 \cdot 3 + 2$$

which all have the required form. Hence k can be written in the required form *[as was to be shown]*.

28. *Theorem*: Given any nonnegative integer n and any positive integer d, there exist integers q and r such that $n = dq + r$ and $0 \leq r < d$.

Proof: Let a nonnegative integer d be given, and for each integer n let $P(n)$ be the property "$\exists$ integers q and r such that $n = dq + r$ and $0 \leq r < d$."

Show that the property is true for $n = 0$: We must show that there exist nonnegative integers q and r such that $0 = dq + r$ and $0 \leq r < d$. Let $q = r = 0$. Then $0 = d \cdot 0 + 0$ and $0 \leq 0 < d$. Hence the theorem is true for $n = 0$.

Show that for all integers $k \geq 0$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let $k \geq 0$ be given, and suppose there exist integers q' and r' such that

$k = dq' + r'$ and $0 \le r' < d$. *[We must show that there exist nonnegative integers q and r such that $k + 1 = dq + r$ and $0 \le r < d$.]* Then $k + 1 = (dq' + r') + 1$. Note that since r' is an integer and $0 \le r' < d$, then either $r' < d - 1$ or $r' = d - 1$.

Case 1 ($r' < d - 1$): In this case, $k + 1 = (dq' + r') + 1 = dq' + (r' + 1)$. Let $q = q'$ and $r = r' + 1$. Then by substitution, $k + 1 = dq + r$. Since $r' < d - 1$ then $r = r' + 1 < d$, and since $r = r' + 1$ and $r' \ge 0$, then $r \ge 0$. Hence $0 \le r < d$.

Case 2 ($r' = d - 1$): In this case, $k + 1 = (dq' + r') + 1 = dq' + (r' + 1) = dq' + ((d - 1) + 1) = dq' + d = d(q' + 1)$. Let $q = q' + 1$ and $r = 0$. Then by substitution $k + 1 = dq + r$, and since $r = 0$ and $d > 0$, $0 \le r < d$.

Thus in either case there exist nonnegative integers q and r such that $k + 1 = dq + r$ and $0 \le r < d$ *[as was to be shown]*.

29. *Proof:* Let $P(n)$ be a property that is defined for integers n, and let a be a fixed integer. Suppose the statement "$P(n)$ is true for all integers $n \ge a$" can be proved using ordinary mathematical induction. Then the following two statements are true:

(1) $P(a)$ is true;

(2) For all integers $k \ge a$, if $P(k)$ is true then $P(k + 1)$ is true.

We will show that we can use the well-ordering principle to deduce the truth of the statement "$P(n)$ is true for all integers $n \ge a$." Let S be the set of all integers greater than or equal to a for which $P(n)$ is false. Suppose S has one or more elements. *[We will derive a contradiction.]* By the well-ordering principle, S has a least element, b, and by definition of S, $P(b)$ is false. Now $b - 1 \ge a$ because S consists entirely of integers greater than or equal to a and $b \ne a$ because $P(a)$ is true and $P(b)$ is false. Also $P(b - 1)$ is true because $b - 1 < b$ and b is the *least* element greater than or equal to a for which $P(n)$ is false. Thus $b - 1 \ge a$ and $P(b - 1)$ is true, and so by (2) above, $P((b - 1) + 1)$, which equals $P(b)$, is true. Hence $P(b)$ is both true and false, which is a contradiction. This contradiction shows that the supposition is false, and so S has no elements. But this means that $P(n)$ is true for all integers $n \ge a$.

30. *Proof:* We first use the principle of ordinary mathematical induction to prove the well-ordering principle for the integers. Let S be a set of integers with one or more elements all of which are greater than or equal to some integer a, and suppose S does not have a least element. Let $P(n)$ be the property "$i \notin S$ for any integer i with $a \le i \le n$."

Show that the property is true for $n = a$: If a were in S, then it would be the least element of S because every element of S is greater than or equal to a. So, since S is assumed not to have a least element, $a \notin S$.

Show that for all integers $k \ge a$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let an integer $k \ge a$ be given, and suppose that $i \notin S$ for any integer i with $a \le i \le k$. *[This is the inductive hypothesis.]* It follows that if $k + 1$ were an element of S, it would be the least element of S. But this is impossible because S is assumed not to have a least element. Thus $i \notin S$ for any integer i with $a \le i \le k + 1$.

Hence, by ordinary mathematical induction, $i \notin S$ for any integer i with $a \le i \le n$, and, therefore, S does not contain any integer greater than or equal to a. But this contradicts the fact that S consists entirely of integers greater than or equal to a and has one or more elements. Thus the supposition that S does not have a least element is false, and so S has a least element.

This shows that the well-ordering principle for the integers follows from the principle of ordinary mathematical induction, and, therefore, that any statement that can be proved by the well-ordering principle for the integers can be proved by first using the principle of ordinary mathematical induction to deduce the well-ordering principle for the integers and then using the well-ordering principle for the integers to deduce the given statement.

Section 4.5

2. *Proof*: Suppose the condition $m + n$ is odd is true before entry to the loop. Then $m_{old} + n_{old}$ is odd. After execution of the loop, $m_{new} = m_{old} + 4$ and $n_{new} = n_{old} - 2$. So $m_{new} + n_{new} = (m_{old} + 4) + (n_{old} - 2) = m_{old} + n_{old} + 2$. But $m_{old} + n_{old}$ is odd and 2 is even, and the sum of an odd and an even integer is odd *[see exercise 19 of Section 3.1 or Example 3.2.3]*. Hence $m_{new} + n_{new}$ is odd.

4. *Proof*: Suppose the condition $2^n < (n + 2)!$ is true before entry to the loop. Then $2^{n_{old}} < (n_{old} + 2)!$. After execution of the loop, $n_{new} = n_{old} + 1$. So $2^{n_{new}} = 2^{n_{old}+1} = 2 \cdot 2^{n_{old}} < 2 \cdot (n_{old} + 2)! < (n_{old} + 3) \cdot (n_{old} + 2)!$ *[because $n_{old} \geq 0$]* $= (n_{old} + 3)! = (n_{new} + 2)!$. Hence $2^{n_{new}} < (n_{new} + 2)!$.

5. *Proof*: Suppose the condition $2n + 1 \leq 2^n$ is true before entry to the loop. Then $2n_{old} + 1 \leq 2^{n_{old}}$. After execution of the loop, $n_{new} = n_{old} + 1$. So $2n_{new} + 1 = 2(n_{old} + 1) + 1 = (2n_{old} + 1) + 2 \leq 2^{n_{old}} + 2$. But since $n_{old} \geq 3$, $2 \leq 2^{n_{old}}$, and so $2^{n_{old}} + 2 \leq 2^{n_{old}} + 2^{n_{old}} = 2 \cdot 2^{n_{old}} = 2^{n_{old}+1} = 2^{n_{new}}$. Putting the inequalities together gives $2n_{new} + 1 \leq 2^{n_{old}} + 2 \leq 2^{n_{new}}$ *[as was to be shown]*.

7. *Proof*:

I. Basis Property: $I(0)$ is the statement *"largest = the maximum value of $A[1]$ and $i = 1$."* According to the pre-condition this statement is true.

II. Inductive Property: Suppose k is a nonnegative integer such that $G \wedge I(k)$ is true before an iteration of the loop. Then when execution comes to the top of the loop, $i \neq m$, *largest* = the maximum value of $A[1], A[2], \ldots, A[k + 1]$, and $i = k + 1$. Since $i \neq m$, the guard is passed and statement 1 is executed. Now before execution of statement 1, $i_{old} = k + 1$. So after execution of statement 1, $i_{new} = i_{old} + 1 = (k + 1) + 1 = k + 2$. Also before statement 2 is executed, *largest*$_{old}$ = the maximum value of $A[1], A[2], \ldots, A[k + 1]$. Statement 2 checks whether $A[i_{new}] = A[k + 2] > largest_{old}$. If the condition is true, then *largest*$_{new}$ is set equal to $A[k + 2]$ which is the maximum value of $A[1], A[2], \ldots, A[k + 1], A[k + 2]$. If the condition is false then $A[k + 2] \leq largest_{old}$, and so *largest*$_{old}$ is the maximum value of $A[1], A[2], \ldots, A[k + 1], A[k + 2]$. Now in this case since the condition is false, the variable *largest* retains its previous value, and so *largest*$_{new}$ = *largest*$_{old}$. Thus in either case *largest*$_{new}$ is the maximum value of $A[1], A[2], \ldots, A[k + 1], A[k + 2]$ and $i_{new} = k + 2$. Hence $I(k + 1)$ is true.

III. Eventual Falsity of Guard: The guard G is the condition $i \neq m$. By I and II, it is known that for all integers $n \geq 1$, after n iterations of the loop $I(n)$ is true. Hence after $m - 1$ iterations of the loop $I(m)$ is true, which implies that $i = m$ and G is false.

IV. Correctness of the Post-Condition: Suppose that N is the least number of iterations after which G is false and $I(N)$ is true. Then (since G is false) $i = m$ and (since $I(N)$ is true) *largest* = the maximum value of $A[1], A[2], \ldots, A[N + 1]$ and $i = N + 1$. Putting these together gives $m = N + 1$ and so *largest* = *the* maximum value of $A[1], A[2], \ldots, A[m]$, which is the post-condition.

9. *Proof*:

I. Basis Property: $I(0)$ is the statement "both a and A are even integers or both are odd integers and $a \geq -1$." According to the pre-condition this statement is true.

II. Inductive Property: Suppose k is a nonnegative integer such that $G \wedge I(k)$ is true before an iteration of the loop. Then when execution comes to the top of the loop, $a_{old} > 0$ and a_{old} and A are both even integers or both are odd integers, and $a_{old} \geq -1$. Execution of statement 1 sets a_{new} equal to $a_{old} - 2$. Hence a_{new} has the same parity as a_{old} which is the same as A. Also since $a_{old} > 0$, then $a_{new} = a_{old} - 2 > 0 - 2 = -2$. But a_{new} is an integer. So since $a_{new} > -2$, $a_{new} \geq -1$. Hence after the loop iteration, $I(k + 1)$ is true.

III. Eventual Falsity of Guard: The guard G is the condition $a > 0$. After each iteration of the loop, $a_{\text{new}} = a_{\text{old}} - 2 < a_{\text{old}}$, and so successive iterations of the loop give a strictly decreasing sequence of integer values of a which eventually becomes less than or equal to zero, at which point G becomes false.

IV. Correctness of the Post-Condition: Suppose that N is the least number of iterations after which G is false and $I(N)$ is true. Then (since G is false) $a \leq 0$ and (since $I(N)$ is true) both a and A are even integers or both are odd integers, and $a \geq -1$. Putting the inequalities together gives $-1 \leq a \leq 0$, and so since a is an integer, $a = -1$ or $a = 0$. Since a and A have the same parity, then, $a = 0$ if A is even and $a = -1$ if A is odd. This is the post-condition.

10. **I. Basis Property**: $I(0)$ is the statement "(1) a and b are nonnegative integers with $\gcd(a, b) = \gcd(A, B)$, and (2) at most one of a and b equals 0, and (3) $0 \leq a + b \leq A + B - 0$." According to the pre-condition, A and B are positive integers and $a = A$ and $b = B$, and so $I(0)$ is true.

II. Inductive Property: Suppose k is a nonnegative integer such that $G \wedge I(k)$ is true before an iteration of the loop. Then when execution comes to the top of the loop, $a_{\text{old}} \neq 0$, $b_{\text{old}} \neq 0$ and

(1) a_{old} and b_{old} are nonnegative integers with $\gcd(a_{\text{old}}, b_{\text{old}}) = \gcd(A, B)$,
(2) at most one of a_{old} and b_{old} equals 0, and
(3) $0 \leq a_{\text{old}} + b_{\text{old}} \leq A + B - k$.

After execution of the statement **"if $a \geq b$ then $a := a - b$ else $b := b - a$"**, we have the following:

(1) *Case 1* ($a_{\text{old}} \geq b_{\text{old}}$): In this case $a_{\text{new}} = a_{\text{old}} - b_{\text{old}} \geq 0$ and $b_{\text{new}} = b_{\text{old}} > 0$, and so both a_{new} and b_{new} are nonnegative. Also $\gcd(a_{\text{new}}, b_{\text{new}}) = \gcd(a_{\text{old}} - b_{\text{old}}, b_{\text{old}}) = \gcd(a_{\text{old}}, b_{\text{old}})$ by Lemma 3.8.3. But $\gcd(a_{\text{old}}, b_{\text{old}}) = \gcd(A, B)$ by (1) above. Hence $\gcd(a_{\text{new}}, b_{\text{new}}) = \gcd(A, B)$.

Case 2 ($a_{\text{old}} < b_{\text{old}}$): In this case $b_{\text{new}} = b_{\text{old}} - a_{\text{old}} > 0$ and $a_{\text{new}} = a_{\text{old}} > 0$, and so both a_{new} and b_{new} are nonnegative. Also $\gcd(a_{\text{new}}, b_{\text{new}}) = \gcd(a_{\text{old}}, b_{\text{old}} - a_{\text{old}}) = \gcd(a_{\text{old}}, b_{\text{old}})$ by Lemma 3.8.3. But $\gcd(a_{\text{old}}, b_{\text{old}}) = \gcd(A, B)$ by (1) above. Hence $\gcd(a_{\text{new}}, b_{\text{new}}) = \gcd(A, B)$.

(2) Because G is true $a_{\text{old}} \neq 0$ and $b_{\text{old}} \neq 0$, and by (1) above both a_{old} and b_{old} are nonnegative. Hence $a_{\text{old}} > 0$ and $b_{\text{old}} > 0$. Since either $a_{\text{new}} = a_{\text{old}}$ or $b_{\text{new}} = b_{\text{old}}$, at most one of a_{new} or b_{new} equals zero.

(3) Observe that

$$a_{\text{new}} + b_{\text{new}} = \begin{cases} a_{\text{old}} - b_{\text{old}} + b_{\text{old}} & \text{if} \quad a_{\text{old}} \geq b_{\text{old}} \\ a_{\text{old}} + b_{\text{old}} - a_{\text{old}} & \text{if} \quad b_{\text{old}} > a_{\text{old}} \end{cases} = \begin{cases} a_{\text{old}} & \text{if} \quad a_{\text{old}} \geq b_{\text{old}} \\ b_{\text{old}} & \text{if} \quad b_{\text{old}} > a_{\text{old}} \end{cases}.$$

But since $a_{\text{old}} \neq 0$ and $b_{\text{old}} \neq 0$ and a_{old} and b_{old} are nonnegative integers, then $a_{\text{old}} \geq 1$ and $b_{\text{old}} \geq 1$. Hence $a_{\text{old}} - 1 \geq 0$ and $b_{\text{old}} - 1 \geq 0$, and so $a_{\text{old}} \leq a_{\text{old}} + b_{\text{old}} - 1$ and $b_{\text{old}} \leq b_{\text{old}} + a_{\text{old}} - 1$. But by (3) above $a_{\text{old}} + b_{\text{old}} \leq A + B - k$. It follows that $a_{\text{new}} + b_{\text{new}} \leq a_{\text{old}} + b_{\text{old}} - 1 \leq A + B - k - 1 = A + B - (k + 1)$. Hence after the loop iteration, $I(k + 1)$ is true.

III. Eventual Falsity of Guard: The guard G is the condition $a \neq 0$ and $b \neq 0$. By II above, for all integers n, after n iterations of the loop, $a \geq 0$, $b \geq 0$, at most one of a and b equals 0, and $0 \leq a + b \leq A + B - n$. Thus if $A + B$ iterations of the loop occur, $0 \leq a + b \leq A + B - (A + B) = 0$, and, since $a \geq 0$ and $b \geq 0$, it would follow that both a and b are 0, which would mean that G is false. Therefore, G becomes false either after $A + B$ iterations of the loop or, possibly, after some fewer number of iterations.

IV. Correctness of the Post-Condition: Suppose that N is the least number of iterations after which G is false and $I(N)$ is true. Then (since G is false) $a = 0$ or $b = 0$, and (since $I(N)$ is true) both a and b are nonnegative, at most one of a and b equals 0, and $\gcd(a, b) = \gcd(A, B)$.

Thus $\gcd(a,b) = \begin{cases} \gcd(0,b) & \text{if} & a = 0 \\ \gcd(a,0) & \text{if} & b = 0 \end{cases}$. By Lemma 3.8.1, $\gcd(0,b) = b$ and $\gcd(a,0) = a$. Hence one of a or b is zero and the other is nonzero, and $\gcd(A,B)$ equals whichever of a or b is nonzero.

Alternative Solution to Part III: Omit part (3) of the loop invariant, and change the proof in III to the following: The guard G is the condition $a \neq 0$ and $b \neq 0$. Observe that after each iteration of the loop

$$a_{\text{new}} + b_{\text{new}} = \begin{cases} a_{\text{old}} - b_{\text{old}} + b_{\text{old}} & \text{if} & a_{\text{old}} \geq b_{\text{old}} \\ a_{\text{old}} + b_{\text{old}} - a_{\text{old}} & \text{if} & b_{\text{old}} > a_{\text{old}} \end{cases} = \begin{cases} a_{\text{old}} & \text{if} & a_{\text{old}} \geq b_{\text{old}} \\ b_{\text{old}} & \text{if} & b_{\text{old}} > a_{\text{old}} \end{cases} < a_{\text{old}} + b_{\text{old}}.$$

Therefore, the values of $a + b$ form a strictly decreasing sequence of nonnegative integers (since a and b are nonnegative). By the well-ordering principle, this sequence has a least value. Let N be the least integer for which this value is attained, and let $a_N + b_N$ be this least value. Suppose G is true after the Nth iteration of the loop. *[We will derive a contradiction.]* Then the loop iterates another time, which results in new values a_{N+1} and b_{N+1} for a and b. But by the argument above, $a_{N+1} + b_{N+1} < a_N + b_N$. This contradicts the fact that $a_N + b_N$ is the least value of the sum $a + b$. Hence the supposition is false, and so G is false after the Nth iteration of the loop.

11. **I. Basis Property**: $I(0)$ is the statement "$xy + product = A \cdot B$. According to the precondition, A and B are positive integers, $x = A$ and $y = B$, and $product = 0$. So $I(0)$ is true.

II. Inductive Property: Suppose k is a nonnegative integer such that $G \wedge I(k)$ is true before an iteration of the loop. Then when execution comes to the top of the loop, $x_{\text{old}} \cdot y_{\text{old}} + product_{\text{old}} = A \cdot B$.

After execution of the statement "$r := y \bmod 2$," there are two possibilities: $r = 0$ or $r = 1$.

(1) *Case 1 ($r = 0$)*: In this case, $y_{\text{old}} = 2q$, for some integer q, and $x_{\text{new}} = 2 \cdot x_{\text{old}}$ and $y_{\text{new}} = y_{\text{old}}$ div $2 = y_{\text{old}}/2 = q$. Also, because the value of *product* is unchanged, $product_{\text{new}} = product_{\text{old}}$. Hence, $x_{\text{new}} \cdot y_{\text{new}} + product_{\text{new}} = (2 \cdot x_{\text{old}}) \cdot (y_{\text{old}}/2) + product_{\text{old}} = x_{\text{old}} \cdot y_{\text{old}} + product_{\text{old}} = A \cdot B$.

Case 2 (($r = 1$): In this case, $y_{\text{old}} = 2q+1$, for some integer q, $product_{\text{new}} = product_{\text{old}} + x_{\text{old}}$, and $y_{\text{new}} = y_{\text{old}} - 1$. Also, because the value of x is unchanged, $x_{\text{new}} = x_{\text{old}}$. Hence, $x_{\text{new}} \cdot y_{\text{new}} + product_{\text{new}} = x_{\text{old}} \cdot (y_{\text{old}} - 1) + (product_{\text{old}} + x_{\text{old}}) = x_{\text{old}} \cdot y_{\text{old}} - x_{\text{old}} + product_{\text{old}} + x_{\text{old}} = x_{\text{old}} \cdot y_{\text{old}} + product_{\text{old}} = A \cdot B$.

Thus, in either case, $x_{\text{new}} \cdot y_{\text{new}} + product_{\text{new}} = A \cdot B$. Hence after the loop iteration, $I(k+1)$ is true.

III. Eventual Falsity of Guard: The guard G is the condition $y \neq 0$. Let S be the set of all values of y that result from an iteration of the loop. Now the initial value of y is a positive integer and each iteration of the loop either cuts the value of y in half or reduces it by 1. Thus all elements of S are integers, and the only way a value of y can become negative is for a previous value to be 0. But $y = 0$ would prevent the iteration of the loop that could make y negative. Hence all elements of S are nonnegative integers. By the well-ordering principle, S has a least element, m. If $m > 0$, then after the iteration in which y would obtain the value m, the loop would iterate again and a new value of y would be obtained that would be less than m. This would contradict m's being the least element of S. It follows that the least element of S equals 0, and so the guard condition is eventually false.

IV. Correctness of the Post-Condition: Suppose that N is the least number of iterations after which G is false and $I(N)$ is true. Then (since G is false) $y = 0$, and (since $I(N)$ is true) $x \cdot y + product = A \cdot B$. But because $y = 0$, this equation becomes $product = A \cdot B$, which is the post-condition of the loop.

12. *a.* Suppose the following condition is satisfied before entry to the loop:"there exist integers u, v, s, and t such that $a = uA + vB$ and $b = sA + tB$." Then

$$a_{\text{old}} = u_{\text{old}}A + v_{\text{old}}B \qquad \text{and} \qquad b_{\text{old}} = s_{\text{old}}A + t_{\text{old}}B,$$

for some integers u_{old}, v_{old}, s_{old}, and t_{old}. Observe that $b_{\text{new}} = r_{\text{new}} = a_{\text{old}} \bmod b_{\text{old}}$. So by the quotient-remainder theorem, there exists a unique integer q_{new} with $a_{\text{old}} = b_{\text{old}} \cdot q_{\text{new}} + r_{\text{new}} = b_{\text{old}} \cdot q_{\text{new}} + b_{\text{new}}$. Solving for b_{new} gives

$$\begin{aligned} b_{\text{new}} &= a_{\text{old}} - b_{\text{old}} \cdot q_{\text{new}} = (u_{\text{old}}A + v_{\text{old}}B) - (s_{\text{old}}A + t_{\text{old}}B)q_{\text{new}} \\ &= (u_{\text{old}} - s_{\text{old}}q_{\text{new}})A + (v_{\text{old}} - t_{\text{old}}q_{\text{new}})B. \end{aligned}$$

Therefore, let $s_{\text{new}} = u_{\text{old}} - s_{\text{old}}q_{\text{new}}$ and $t_{\text{new}} = v_{\text{old}} - t_{\text{old}}q_{\text{new}}$. Also since $a_{\text{new}} = b_{\text{old}} = s_{\text{old}}A + t_{\text{old}}B$, let $u_{\text{new}} = s_{\text{old}}$ and $v_{\text{new}} = t_{\text{old}}$. Hence $a_{\text{new}} = u_{\text{new}} \cdot A + v_{\text{new}} \cdot B$ and $b_{\text{new}} = s_{\text{new}} \cdot A + t_{\text{new}} \cdot B$, and so the condition is true after each iteration of the loop and hence after exit from the loop.

b. Initially $a = A$ and $b = B$. Let $u = 1$, $v = 0$, $s = 0$, and $t = 1$. Then before the first iteration of the loop, $a = uA + vB$ and $b = sA + tB$ as was to be shown.

c. By part (b) there exist integers u, v, s, and t such that before the first iteration of the loop, $a = uA + vB$ and $b = sA + tB$. So by part (a), after each subsequent iteration of the loop, there exist integers u, v, s, and t such that $a = uA + vB$ and $b = sA + tB$. Now after the final iteration of the **while** loop in the Euclidean algorithm, the variable *gcd* is given the current value of a. (See page 196.) But by the correctness proof for the Euclidean algorithm, $gcd = \gcd(A, B)$. Hence there exist integers u and v such that $\gcd(A, B) = uA + vB$.

d. The method discussed in part (a) gives the following formulas for u, v, s, and t:

$$u_{\text{new}} = s_{\text{old}}, \qquad v_{\text{new}} = t_{\text{old}}, \qquad s_{\text{new}} = u_{\text{old}} - s_{\text{old}}q_{\text{new}}, \qquad \text{and} \qquad t_{\text{new}} = v_{\text{old}} - t_{\text{old}}q_{\text{new}},$$

where in each iteration q_{new} is the quotient obtained by dividing a_{old} by b_{old}. The trace table below shows the values of a, b, r, q, *gcd*, and u, v, s, and t for the iterations of the **while** loop from the Euclidean algorithm. By part (b) the initial values of u, v, s, and t are $u = 1$, $v = 0$, $s = 0$, and $t = 1$.

r		18	12	6	0
q		2	8	1	2
a	330	156	18	12	6
b	156	18	12	6	0
gcd					6
u	1	0	1	-8	9
v	0	1	-2	17	-19
s	0	1	-8	9	-26
t	1	-2	17	-19	55

Since the final values of *gcd*, u, and v are 6, 9 and -19 and since $A = 330$ and $B = 156$, we have $\gcd(330, 156) = 6 = 330u + 156v = 330 \cdot 9 + 156 \cdot (-19)$, which is true.

Chapter 5: Set Theory

The first section of this chapter introduces the structures of set and ordered set and illustrates them with a variety of examples. The aim of this section is to provide a solid basis of experience for deriving the set properties discussed in the remainder of the chapter.

Students of computer science may be motivated to take seriously the formal structures and notation of set theory if they are shown a relation between them and the formal structures and notation of computer science. In programming, for instance, it is important to distinguish among different kinds of data structures and to respect the notations that are used to refer to them. Similarly, in set theory it is important to distinguish between, say, $\{1, 2, 3\}$ and $(1, 2, 3)$ or between $((u, v), w)$ and $(u, (v, w))$.

The reason for delaying discussion of set theory to this chapter is that considerable sophistication is needed to understand the derivations of set properties. Even after having studied the first four chapters of the book, many students have difficulty constructing simple element proofs. One reason for the difficulty is a tendency for students to interpret "if $x \in A$ then $x \in B$" as "$x \in A$ and $x \in B$". I have found this tendency to be quite strong. For example, even when I tell students that part of a test will be on definitions, specifically warn them against this error, and repeatedly emphasize the dynamic if-then nature of the definition of subset, there are always students who write the definition as an *and* statement anyway. Part of the reason for the misunderstanding may be that if it is true for a particular x that "if $x \in A$ then $x \in B$" and if $x \in A$, then the statement "$x \in A$ and $x \in B$" is also true. In any case, you may be taken aback by the confusion some of your students manifest in tackling the proofs of Section 5.2. However, many students who have difficulty at the outset catch on to the idea of element proof eventually, particularly if given feedback on their work through discussion of student presentations of proofs at the board or if allowed to resubmit some homework problems for a better grade. And at this stage of the course, most students actually enjoy the "algebraic" derivation of set theory properties, often negotiating to use this method rather than the element method on tests.

It is possible to cover the material of this chapter lightly and still give students a bare introduction to the idea of element proof. One way to do so is to start with Section 5.1, making sure to assign some of exercises 14–17. Then you would simply state the various set properties from Section 5.2, perhaps giving a proof or two using element arguments but not asking students to write such proofs themselves. Instead you could assign the "algebraic" proofs from Section 5.3.

Some of the set theory properties developed in Section 5.2 are used to derive counting principles in Chapter 6. However, you can cover Chapter 6 before Chapter 5 by referring to those properties in informal terms. For instance, if you are on the quarter system, you might consider covering Chapters 1-4 and 6 during the first quarter and leaving Chapter 5 to start the second quarter. This allows time for the more abstract ideas of Chapters 3 and 4 to settle in before the final examination, while ending the course with material that is concrete and of obviously practical use. Then the second quarter could start with sets and move on to other discrete structures such as functions, relations, and graphs.

Comments on Exercises

Exercise Set 5.1: #14-17 are useful for introducing students to the idea of element argument as preparation for Section 5.2. #16 and #17 are also preparation for understanding the equivalence of various representations of congruence classes, which are discussed in Section 10.3. The discussion of partitions in Section 5.1 is also part of the groundwork for the discussion of equivalence relations. #23 and #25 are especially helpful as background for understanding congruence classes of integers modulo n.

Exercise Set 5.3: #21 is a warm-up exercise for the proof of the theorem that a set with n elements has 2^n subsets. You might assign this exercise the day before you present the theorem in class.

Section 5.1

2. No. $\{4\}$ is the set whose only element is 4. This does not equal the number 4.

3. $A = D$

4. *b.* $T = \{0, 2\}$

   e. $W = \emptyset$ (There are no integers that are both greater than -1 and less than -3.)

   f. $X = \mathbf{Z}$ (Every integer u satisfies at least one of the conditions $u \leq 4$ or $u \geq 1$.)

5. *c.* Yes, because $\{\emptyset\}$ is the set that contains the one element $\emptyset$.

   d. No, because $\emptyset$ has no elements and thus it cannot contain the element $\emptyset$.

6. *b. In words*: The set of all x in the universal set U such that x is in A or x is in B.
   Shorthand notation: $A \cup B$.

   c. In words: The set of all x in the universal set U such that x is in A and x is not in B.
   Shorthand notation: $A - B$.

   d. In words: The set of all x in the universal set U such that x is not in A.
   Shorthand notation: A^c.

7. *b.* Yes. Every element in C is in A.

   c. Yes. Every element in C is in C.

8. *c.* No.   *d.* Yes   *e.* Yes.   *g.* Yes   *h.* No   *j.* Yes

9. *f.* $B - A = \{6\}$ *g.* $B \cup C = \{2, 3, 4, 6, 8, 9\}$ *h.* $B \cap C = \{6\}$

11.

   a. $A \cup B = \{x \in \mathbf{R} \mid -3 \leq x < 2\}$ *b.* $A \cap B = \{x \in \mathbf{R} \mid -1 < x \leq 0\}$
   c. $A^c = \{x \in \mathbf{R} \mid x < -3 \text{ or } x > 0\}$ *d.* $A \cup C = \{x \in \mathbf{R} \mid -3 \leq x \leq 0 \text{ or } 6 < x \leq 8\}$
   e. $A \cap C = \emptyset$ *f.* $B^c = \{x \in \mathbf{R} \mid x \leq -1 \text{ or } x \geq 2\}$
   g. $A^c \cap B^c = \{x \in \mathbf{R} \mid x < -3 \text{ or } x \geq 2\}$ *h.* $A^c \cup B^c = \{x \in \mathbf{R} \mid x \leq -1 \text{ or } x > 0\}$
   i. $(A \cap B)^c = \{x \in \mathbf{R} \mid x \leq -1 \text{ or } x > 0\}$ *j.* $(A \cup B)^c = \{x \in \mathbf{R} \mid x < -3 \text{ or } x \geq 2\}$

   Note that $(A \cap B)^c = A^c \cup B^c$ and that $(A \cup B)^c = A^c \cap B^c$.

12. *a.* True: Every positive integer is a rational number.

   c. False: There are many rational numbers that are not integers. For instance, $1/2 \in \mathbf{Q}$ but $1/2 \notin \mathbf{Z}$.

   e. True: No integers are both positive and negative.

   f. True: Every rational number is real. So the set of all numbers that are both rational and real is the same as the set of all numbers that are rational.

   g. True: Every integer is a rational number, and so the set of all numbers that are integers or rational numbers is the same as the set of all rational numbers.

   h. True: Every positive integer is a real number, and so the set of all numbers that are both positive integers and real numbers is the same as the set of all positive integers.

   i. False: Every integer is a rational number, and so the set of all numbers that are integers or rational numbers is the same as the set of all rational numbers. However there are many rational numbers that are not integers, and so $\mathbf{Z} \cup \mathbf{Q} = \mathbf{Q} \neq \mathbf{Z}$.

13. *b. Negation*: $\exists$ a set S such that $S \subseteq \mathbf{Q}^+$ and $S \nsubseteq \mathbf{Q}^-$. The negation is true. For example let $S = \{1/2\}$. Then $S \subseteq \mathbf{Q}^+$ and $S \nsubseteq \mathbf{Q}^-$.

14. *c.* Yes. Every integer that is divisible by 6 is also divisible by 3.

   d. $R \cap S = \{u \in \mathbf{Z} \mid u \text{ is divisible by 2 and } u \text{ is divisible by 3}\}$
      $= \{u \in \mathbf{Z} \mid u \text{ is divisible by 6}\} = T$

15. *a.* No. For example, $5 \in A$ because $5 = 5 \cdot 1$, but $5 \neq 20k$ for any integer k, and so $5 \notin B$.

   b. Yes: If n is any element of B, then $n = 20k$ for some integer k. Thus $n = 5(4k)$ and so, since $4k$ is an integer, $n \in A$.

17. *c.* No. For example, $8 \in D$ because $8 = 3 \cdot 3 - 1$. But $8 \notin A$ because $8 \neq 5i - 1$ for any integer i. (For if $8 = 5i - 1$ for some integer i, solving for i would give $5i = 9$, or $i = 9/5$, which is not an integer.)

   d. Yes.
   Suppose $n \in B$. By definition of B, $n = 3j + 2$ for some integer j. But then $n = 3j + 2 = 3j + 3 - 1 = 3(j + 1) - 1$. Let $s = j + 1$. Then s is an integer and $n = 3s - 1$. So by definition of D, $n \in D$. Hence any element of B is in D, or, symbolically, $B \subseteq D$.
   Conversely, suppose $q \in D$. By definition of D, $q = 3s - 1$ for some integer s. But then $q = 3s - 1 = 3s - 3 + 2 = 3(s - 1) + 2$ for some integer s. Let $j = s - 1$. Then j is an integer and $q = 3j + 2$. So by definition of B, $q \in B$. Hence any element of D is in B, or, symbolically, $D \subseteq B$.
   Since $B \subseteq D$ and $D \subseteq B$, by definition of set equality $B = D$.

18. *b.*

19. *b.*

   c.
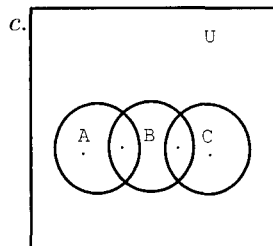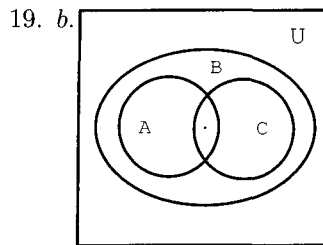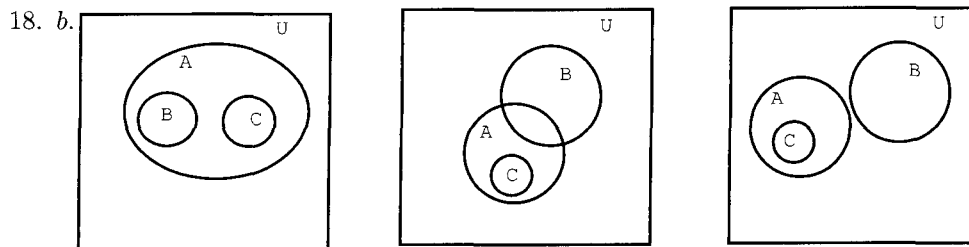
20. *b.* $A \cap (B \cup C) = \{a, b, c\} \cap \{b, c, d, e\} = \{b, c\}$, $(A \cap B) \cup C = \{b, c\} \cup \{b, c, e\} = \{b, c, e\}$, and $(A \cap B) \cup (A \cap C) = \{b, c\} \cup \{b, c\} = \{b, c\}$. Hence $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

   d. $(A - B) - C = \{a\} - \{b, c, e\} = \{a\}$ and $A - (B - C) = \{a, b, c\} - \{d\} = \{a, b, c\}$. These sets are not equal.

21.

b

c

d

e

f

Region shaded | | | *is* A^c
Region shaded $\equiv$ *is* B^c

Cross-hatched region is $A^c \cap B^c$
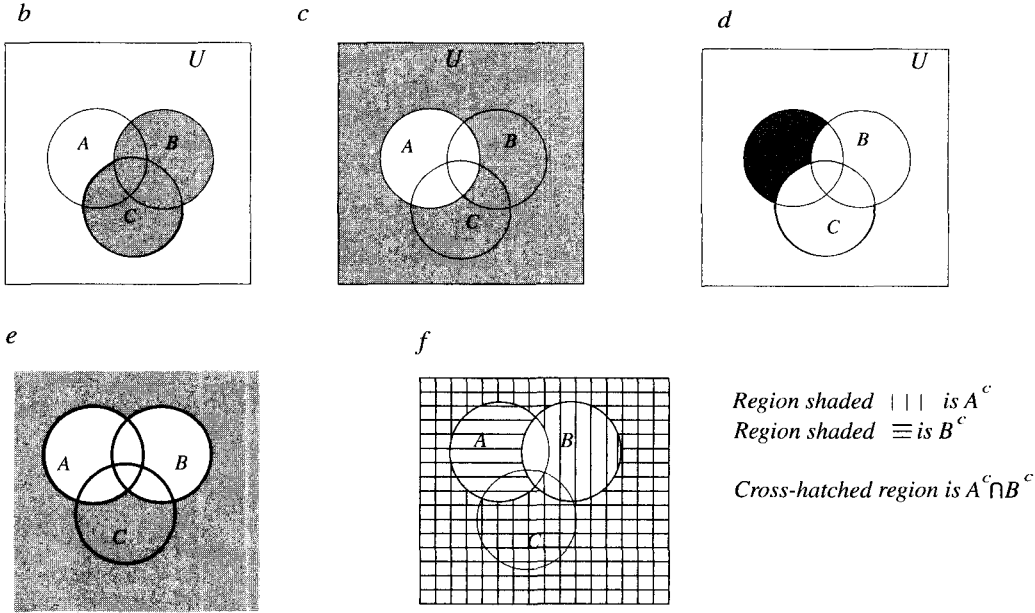
22. *b.* Yes. Every element in $\{p, q, u, v, w, x, y, z\}$ is in one of the sets of the partition and no element is in more than one set of the partition.

c. No. The number 4 is in both sets $\{5, 4\}$ and $\{1, 3, 4\}$.

e. Yes. Every element in $\{1, 2, 3, 4, 5, 6, 7, 8\}$ is in one of the sets of the partition and no element is in more than one set of the partition.

24. Yes. Every real number x satisfies exactly one of the conditions: $x > 0$ or $x = 0$ or $x < 0$. (See property T16 of Appendix A.)

25. Yes. By the quotient-remainder theorem, every integer can be represented in exactly one of the following forms: $4k$ or $4k + 1$ or $4k + 2$ or $4k + 3$ for some integer k.

27. *b.* $X \times Y = \{(a, x), (a, y), (b, x), (b, y)\}$

$\mathscr{P}(X \times Y) = \{\emptyset, \{(a, x)\}, \{(a, y)\}, \{(b, x)\}, \{(b, y)\}, \{(a, x), (a, y)\}, \{(a, x), (b, x)\},$
$\{(a, x), (b, y)\}, \{(a, y), (b, x)\}, \{(a, y), (b, y)\}, \{(b, x), (b, y)\},$
$\{(a, x), (a, y), (b, x)\}, \{(a, x), (a, y), (b, y)\}, \{(a, x), (b, x), (b, y)\},$
$\{(a, y), (b, x), (b, y)\}, \{(a, x), (a, y), (b, x), (b, y)\}\}$

28. *a.* $\mathscr{P}(\emptyset) = \{\emptyset\}$

c. $\mathscr{P}(\mathscr{P}(\mathscr{P}(\emptyset))) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$

29. *b.* $B \times A = \{(a, x), (a, y), (a, z), (a, w), (b, x), (b, y), (b, z), (b, w)\}$

c. $A \times A = \{(x, x), (x, y), (x, z), (x, w), (y, x), (y, y), (y, z), (y, w), (z, x), (z, y), (z, z), (z, w),$
$(w, x), (w, y), (w, z), (w, w)\}$

d. $B \times B = \{(a, a), (a, b), (b, a), (b, b)\}$

30. *b.* $(A \times B) \times C = \{((1, u), m), ((1, u), n), ((1, v), m), ((1, v), n), ((2, u), m), ((2, u), n), ((2, v), m),$
$((2, v), n), ((3, u), m), ((3, u), n), ((3, v), m), ((3, v), n)\}$

c. $A \times B \times C = \{(1, u, m), (1, u, n), (1, v, m), (1, v, n), (2, u, m), (2, u, n), (2, v, m), (2, v, n),$
$(3, u, m), (3, u, n), (3, v, m), (3, v, n)\}$

32.

i	1			2					3
j	1	2	3	1	2	3	4	5	
found	no	yes		no					
answer	$A \subseteq B$							$A \nsubseteq B$	

33. Algorithm: Testing Whether $x \in A$

[This algorithm checks whether an element x is in a set A, which is represented as a one-dimensional array $a[1], a[2], \ldots, a[n]$. Initially answer is set equal to "$x \notin A$." Then for successive integers i from 1 to n, x is compared to $a[i]$. If at any stage $x=a[i]$, the value of answer is changed to "$x \in A$" and iteration of the loop ceases.]

Input: $a[1], a[2], \ldots, a[n]$ *[a one-dimensional array]*, x *[an element of the same data type as the elements of the array]*

Algorithm Body:

$$i := 1, \ answer := \text{``}x \notin A\text{''}$$

while ($i \leq n$ and $answer = $ "$x \notin A$")

    if $x = a[i]$ **then** $answer := $ "$x \in A$"

    $i := i + 1$

end while

Output: *answer [a string]*

Section 5.2

1. *c*. (1) A (2) $B \cap C$

4. *a*. $A \cup B \subseteq B$ *b*. $A \cup B$ *c*. $x \in B$ *d*. A *e*. or   *f*. B *g*. A *h*. B *i*. B

7. *Proof*:

Suppose A and B are sets.

$(A \cap B)^c \subseteq A^c \cup B^c$: Suppose $x \in (A \cap B)^c$. By definition of complement, $x \notin A \cap B$, which means that it is false that (x is in A and x is in B). By De Morgan's laws of logic, this implies that x is not in A or x is not in B, which can be written $x \notin A$ or $x \notin B$. Hence $x \in A^c$ or $x \in B^c$ by definition of complement. It follows by definition of union that $x \in A^c \cup B^c$. *[Thus $(A \cap B)^c \subseteq A^c \cup B^c$ by definition of subset.]*

$A^c \cup B^c \subseteq (A \cap B)^c$: Suppose $x \in A^c \cup B^c$. Then by definition of union $x \in A^c$ or $x \in B^c$. By definition of complement $x \notin A$ or $x \notin B$. In other words, x is not in A or x is not in B. By De Morgan's laws of logic this implies that it is false that (x is in A and x is in B), which can be written $x \notin A \cap B$ by definition of intersection. Hence by definition of complement, $x \in (A \cap B)^c$. *[Thus $A^c \cup B^c \subseteq (A \cap B)^c$ by definition of subset.]*

[Since both set containments have been proved, $(A \cap B)^c = A^c \cup B^c$ by definition of set equality.]

9. *Proof*: Let A, B, and C be any sets.

$(A - B) \cap (C - B) \subseteq (A \cap C) - B$: Suppose $x \in (A - B) \cap (C - B)$. By definition of intersection, $x \in A - B$ and $x \in C - B$, and so, by definition of set difference, $x \in A$ and $x \notin B$ and $x \in C$ and $x \notin B$. To summarize: $x \in A$ and $x \in C$ and $x \notin B$. Hence, by definition of intersection, $x \in A \cap C$ and $x \notin B$, and by definition of set difference, $x \in (A \cap C) - B$. *[Thus $(A - B) \cap (C - B) \subseteq (A \cap C) - B$ by definition of subset.]*

$(A \cap C) - B \subseteq (A - B) \cap (C - B)$: Suppose $x \in (A \cap C) - B$. By definition of set difference, $x \in (A \cap C)$ and $x \notin B$, and by definition of intersection, $x \in A$ and $x \in C$ and $x \notin B$. Thus it is true that $x \in A$ and $x \notin B$ and $x \in C$ and $x \notin B$, and so by definition of set difference, $x \in A - B$ and $x \in C - B$. Therefore by definition of intersection, $x \in (A - B) \cap (C - B)$. *[Thus $(A \cap C) - B \subseteq (A - B) \cap (C - B)$ by definition of subset.]*

[Since both subset containments have been proved, $(A - B) \cap (C - B) = (A \cap C) - B$ by definition of set equality.]

10. *Proof*: Let A and B be any sets.

$A \cup (A \cap B) \subseteq A$: Suppose $x \in A \cup (A \cap B)$. By definition of union, $x \in A$ or $x \in A \cap B$. In case $x \in A$, then clearly $x \in A$. In case $x \in A \cap B$, then, by definition of intersection, $x \in A$ and $x \in B$, and so, in particular, $x \in A$. Hence in either case $x \in A$. *[Thus $A \cup (A \cap B) \subseteq A$ by definition of subset.]*

$A \subseteq A \cup (A \cap B)$: Suppose $x \in A$. Then by definition of union, $x \in A \cup (A \cap B)$. *[Thus $A \subseteq A \cup (A \cap B)$ by definition of subset.]*

[Since both subset containments have been proved, $A \cup (A \cap B) = A$ by definition of set equality.

13. *Proof*: Suppose A, B, and C are sets and $A \subseteq B$. Let $x \in A \cup C$. Then by definition of union, $x \in A$ or $x \in C$. In case $x \in A$, then since $A \subseteq B$, we have that $x \in B$, and so it is true that $x \in B$ or $x \in C$, and hence, by definition of union, $x \in B \cup C$. In case $x \in C$, then it is true that $x \in B$ or $x \in C$, and so, by definition of union, $x \in B \cup C$. Therefore, in either case, $x \in B \cup C$. *[Thus $A \cup C \subseteq B \cup C$ by definition of subset.]*

14. *Proof*: Suppose A and B are sets and $A \subseteq B$. Let $x \in B^c$. By definition of complement, $x \notin B$. It follows that $x \notin A$ *[because if $x \in A$ then $x \in B$ (since $A \subseteq B$), and this would contradict the fact that $x \notin B$]*. Hence by definition of complement $x \in A^c$. *[Thus $B^c \subseteq A^c$ by definition of subset.]*

15. *Proof*: Suppose A, B, and C are sets and $A \subseteq B$ and $A \subseteq C$. Let $x \in A$. Since $x \in A$ and $A \subseteq B$, then $x \in B$ (by definition of subset). Similarly, since $x \in A$ and $A \subseteq C$, then $x \in C$. Hence $x \in B$ and $x \in C$, and so by definition of intersection, $x \in B \cap C$. *[By definition of subset, therefore, $A \subseteq B \cap C$.]*

17. *Proof*: Suppose A, B, and C are sets.

$A \times (B \cap C) \subseteq (A \times B) \cap (A \times C)$: Suppose $(x, y) \in A \times (B \cap C)$. By definition of Cartesian product, $x \in A$ and $y \in B \cap C$. By definition of intersection, $y \in B$ and $y \in C$. It follows that both statements "$x \in A$ and $y \in B$" and "$x \in A$ and $y \in C$" are true. Hence by definition of Cartesian product, $(x, y) \in A \times B$ and $(x, y) \in A \times C$, and so by definition of intersection, $(x, y) \in (A \times B) \cap (A \times C)$. *[Thus $A \times (B \cap C) \subseteq (A \times B) \cap (A \times C)$ by definition of subset.]*

$(A \times B) \cap (A \times C) \subseteq A \times (B \cap C)$: Suppose $(x, y) \in (A \times B) \cap (A \times C)$. By definition of intersection, $(x, y) \in A \times B$ and $(x, y) \in A \times C$, and so by definition of Cartesian product $x \in A$ and $y \in B$ and also $x \in A$ and $y \in C$. Consequently, the statement "$x \in A$ and both $y \in B$ and $y \in C$" is true. It follows by definition of intersection that $x \in A$ and $y \in B \cap C$, and so by definition of Cartesian product, $(x, y) \in A \times (B \cap C)$. *[Thus $(A \times B) \cap (A \times C) \subseteq A \times (B \cap C)$ by definition of subset.]*

[Since both subset containments have been proved, $A \times (B \cap C) = (A \times B) \cap (A \times C)$ by definition of set equality.]

19. The "proof" claims that because $x \notin A$ or $x \notin B$, it follows that $x \notin A \cup B$. But it is possible for "$x \notin A$ or $x \notin B$" to be true and "$x \notin A \cup B$" to be false. For example, let $A = \{1, 2\}$, $B = \{2, 3\}$, and $x = 3$. Then since $3 \notin \{1, 2\}$, the statement "$x \notin A$ or $x \notin B$" is true. But since $A \cup B = \{1, 2, 3\}$ and $3 \in \{1, 2, 3\}$, the statement "$x \notin A \cup B$" is false.

20. A correct proof of the given statement must show that if $x \in (A - B) \cup (A \cap B)$ then $x \in A$. This incorrect proof uses the assumption that $x \in A$ as a basis for concluding that $x \in A$. In other words, this incorrect proof begs the question.

Another mistake is that the assertion "If $x \in A$ then $x \in A - B$" is not necessarily true. In fact, it is often false. For example, if $A = \{1, 2\}$ and $B = \{2\}$, then $A - B = \{1\}$, and so the statement "$2 \in A$" is true but the statement "$2 \in A - B$" is false.

21.

b
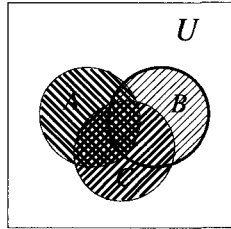
darkly shaded region is $A \cap (B \cup C)$
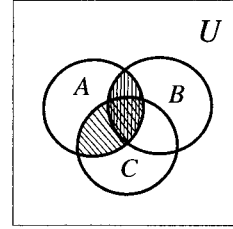
entire shaded region is $(A \cap B) \cup (A \cap C)$

c
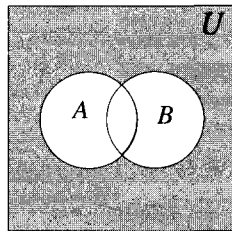
shaded region is $(A \cup B)^c$
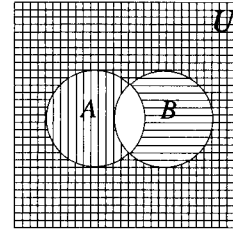
cross-hatched region is $A^c \cap B^c$

d
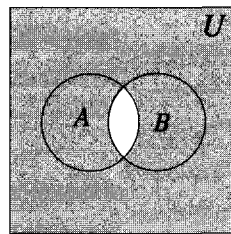
shaded region is $(A \cap B)^c$
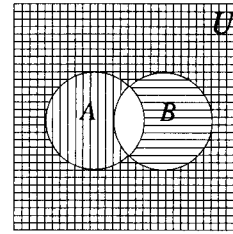
entire shaded region is $A^c \cup B^c$

24. *Proof*: Let A, B, and C be any sets, and suppose that $(A - B) \cap (B - C) \cap (A - C) \neq \emptyset$. Then there is an element x such that $x \in (A - B) \cap (B - C) \cap (A - C)$. By definition of intersection, $x \in A - B$ and $x \in B - C$ and $x \in A - C$, and so by definition of set difference, $x \in A$ and $x \notin B$ and $x \in B$ and $x \notin C$ and $x \in A$ and $x \notin C$. In particular, $x \notin B$ and $x \in B$, which is a contradiction. Hence the supposition is false. That is, $(A - B) \cap (B - C) \cap (A - C) = \emptyset$.

26. *Proof*: Let U be a universal set. Suppose $U^c \neq \emptyset$; that is, suppose there were an element x in U^c. Then by definition of complement $x \notin U$. But, by definition, a universal set contains all elements under discussion, and thus it is impossible that $x \notin U$. *[Hence the supposition is false, and so $U^c = \emptyset$.]*

29. *Proof*: Let A and B be sets with $B \subseteq A^c$. Suppose $A \cap B \neq \emptyset$; that is, suppose there were an element x in $A \cap B$. Then by definition of intersection, $x \in A$ and $x \in B$. But $B \subseteq A^c$, and so by definition of subset, $x \in A^c$. By definition of complement this means that $x \notin A$. Hence $x \in A$ and $x \notin A$, which is a contradiction. *[Thus the supposition is false, and we conclude that $A \cap B = \emptyset$.]*

30. *Proof*: Let A, B, and C be any sets such that $A \subseteq B$ and $B \cap C = \emptyset$. Suppose $A \cap C \neq \emptyset$; that is, suppose there were an element x in $A \cap C$. Then by definition of intersection, $x \in A$ and $x \in C$. But by hypothesis $A \subseteq B$, and so since $x \in A$, $x \in B$ also. Hence $x \in B \cap C$, which implies that $B \cap C \neq \emptyset$. But this contradicts the hypothesis that $B \cap C = \emptyset$. Hence the supposition is false, and so $A \cap C = \emptyset$.

31. *Proof*: Let A, B, and C be any sets such that $B \subseteq C$ and $A \cap C = \emptyset$. Suppose $A \cap B \neq \emptyset$. Then there is an element x such that $x \in A \cap B$. By definition of intersection, $x \in A$ and $x \in B$. Since $B \subseteq C$, then, $x \in C$. So $x \in A$ and $x \in C$, and thus $x \in A \cap C$ by definition of intersection. But this contradicts the assumption that $A \cap C = \emptyset$. Hence the supposition is false, and so $A \cap B = \emptyset$.

33. *Proof*: Let A, B, and C be any sets such that $B \cap C \subseteq A$. Suppose $(C - A) \cap (B - A) \neq \emptyset$. Then there is an element x such that $x \in (C - A) \cap (B - A)$. By definition of intersection, $x \in C - A$ and $x \in B - A$, and so by definition of set difference, $x \in C$ and $x \notin A$ and $x \in B$ and $x \notin A$. Since $x \in C$ and $x \in B$, $x \in B \cap C$ by definition of intersection. But $B \cap C \subseteq A$, and so $x \in A$. Thus $x \notin A$ and $x \in A$, which is a contradiction. Hence the supposition is false, and so $(C - A) \cap (B - A) = \emptyset$.

34. *Proof*: Let A, B, C, and D be any sets such that $A \cap C = \emptyset$. Suppose $(A \times B) \cap (C \times D) \neq \emptyset$. Then there is an ordered pair (x, y) such that $(x, y) \in (A \times B) \cap (C \times D)$. By definition of intersection, $(x, y) \in A \times B$ and $(x, y) \in C \times D$, and by definition of Cartesian product, $x \in A$ and $x \in C$. By definition of intersection, then, $x \in A \cap C$. But this implies that $A \cap C \neq \emptyset$, which contradicts the fact that $A \cap C = \emptyset$. Hence the supposition is false, and so $(A \times B) \cap (C \times D) = \emptyset$.

36. *Proof (by mathematical induction)*: Let the property $P(n)$ be the equation

$$(A_1 - B) \cup (A_2 - B) \cup \cdots \cup (A_n - B) = (A_1 \cup A_2 \cup \cdots \cup A_n) - B.$$

Show that the property is true for $n = 1$: For $n = 1$ the property is the equation $A_1 - B = A_1 - B$, which is clearly true.

Show that for all integers $k \geq 1$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let k be an integer with $k \geq 1$, and suppose $A_1, A_2, \ldots, A_k, A_{k+1}$, and B are any sets such that

$$(A_1 - B) \cup (A_2 - B) \cup \cdots \cup (A_k - B) = (A_1 \cup A_2 \cup \cdots \cup A_k) - B. \qquad \leftarrow \text{inductive hypothesis}$$

We must show that

$$(A_1 - B) \cup (A_2 - B) \cup \cdots \cup (A_{k+1} - B) = (A_1 \cup A_2 \cup \cdots \cup A_{k+1}) - B.$$

But the left-hand side of this equation is

$(A_1 - B) \cup (A_2 - B) \cup \cdots \cup (A_{k+1} - B)$

$$
\begin{aligned}
&= [(A_1 - B) \cup (A_2 - B) \cup \cdots \cup (A_k - B)] \cup (A_{k+1} - B) &&\text{by definition}\\
&= [(A_1 \cup A_2 \cup \cdots \cup A_k) - B] \cup (A_{k+1} - B) &&\text{by inductive hypothesis}\\
&= [(A_1 \cup A_2 \cup \cdots \cup A_k) \cup A_{k+1}] - B &&\text{by exercise 8}\\
&= (A_1 \cup A_2 \cup \cdots \cup A_{k+1}) - B &&\text{by definition}
\end{aligned}
$$

and this is the right-hand side of the equation *[as was to be shown]*.

37. *Proof (by mathematical induction)*: Let the property $P(n)$ be the equation

$$(A_1 - B) \cap (A_2 - B) \cap \cdots \cap (A_n - B) = (A_1 \cap A_2 \cap \cdots \cap A_n) - B.$$

Show that the property is true for $n = 1$: For $n = 1$ the property is the equation $A_1 - B = A_1 - B$, which is clearly true.

Show that for all integers $k \geq 1$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let k be an integer with $k \geq 1$, and suppose $A_1, A_2, \ldots, A_k, A_{k+1}$, and B are any sets such that

$$(A_1 - B) \cap (A_2 - B) \cap \cdots \cap (A_k - B) = (A_1 \cap A_2 \cap \cdots \cap A_k) - B. \qquad \leftarrow \text{inductive hypothesis}$$

We must show that

$$(A_1 - B) \cap (A_2 - B) \cap \cdots \cap (A_{k+1} - B) = (A_1 \cap A_2 \cap \cdots \cap A_{k+1}) - B.$$

But the left-hand side of this equation is

$(A_1 - B) \cap (A_2 - B) \cap \cdots \cap (A_{k+1} - B)$

$\begin{aligned}
&= [(A_1 - B) \cap (A_2 - B) \cap \cdots \cap (A_k - B)] \cap (A_{k+1} - B) && \text{by definition} \\
&= [(A_1 \cap A_2 \cap \cdots \cap A_k) - B] \cap (A_{k+1} - B) && \text{by inductive hypothesis} \\
&= [(A_1 \cap A_2 \cap \cdots \cap A_k) \cap A_{k+1}] - B && \text{by exercise 9} \\
&= (A_1 \cap A_2 \cap \cdots \cap A_{k+1}) - B && \text{by definition}
\end{aligned}$

and this is the right-hand side of the equation *[as was to be shown]*.

Section 5.3

2. *Counterexample*: Let $U = \{1, 2, 3, 4\}$, $A = \{1, 2\}$, $B = \{1, 2, 3\}$, and $C = \{2\}$. Then $A \subseteq B$, $B \cap C = \{2\}$, and $(B \cap C)^c = \{1, 3, 4\}$. So $A \cap (B \cap C)^c = \{1, 2\} \cap \{1, 3, 4\} = \{1\} \neq \emptyset$.

4. *Counterexample*: Let $A = \{1, 2, 3\}$, $B = \{2\}$, and $C = \{3\}$. Then $B \cap C = \emptyset \subseteq A$, and $A - B = \{1, 3\}$ and $A - C = \{1, 2\}$, and so $(A - B) \cap (A - C) = \{1, 3\} \cap \{1, 2\} = \{1\} \neq \emptyset$.

7. False. *Counterexample*: Let $A = \{1, 2, 3\}$, $B = \{2\}$, and $C = \{1\}$. Then $A - B = \{1, 2, 3\} - \{2\} = \{1, 3\}$ and $C - B = \{1\} - \{2\} = \{1\}$, and so $(A - B) \cap (C - B) = \{1\} \cap \{1\} = \{1\}$. On the other hand, $B \cup C = \{1, 2\}$, and so $A - (B \cup C) = \{1, 2, 3\} - \{1, 2\} = \{3\}$. Hence $(A - B) \cap (C - B) \neq A - (B \cup C)$.

8. True. *Proof*: Let A and B be sets with $A^c \subseteq B$. By definition of union, $A \cup B$ is the set of all elements x in U such that x is in A or x is in B. So every element x in $A \cup B$ is in U, and hence $A \cup B \subseteq U$. *[Therefore, $A \cup B \subseteq U$.]* To prove that $U \subseteq A \cup B$, suppose $x \in U$. It is certainly true that $x \in A$ or $x \notin A$ (a tautology), and so by definition of complement $x \in A$ or $x \in A^c$. In case $x \in A$, then $x \in A \cup B$ by definition of union. In case $x \in A^c$, then $x \in B$ because $A^c \subseteq B$ by hypothesis, and so $x \in A \cup B$ by definition of union. Thus in either case $x \in A \cup B$. *[Therefore, $U \subseteq A \cup B$.]* *[Since both set containments $A \cup B \subseteq U$ and $U \subseteq A \cup B$ have been proved, $A \cup B = U$ by definition of set equality.]*

10. True. *Proof*: Let A and B be sets with $A \subseteq B$. *[We must show that $A \cap B^c = \emptyset$.]* Suppose $A \cap B^c \neq \emptyset$, that is, suppose there were an element x in $A \cap B^c$. By definition of intersection, $x \in A$ and $x \in B^c$, and so by definition of complement $x \in A$ and $x \notin B$. But $A \subseteq B$ by hypothesis. Hence since $x \in A$, by definition of subset, $x \in B$. Thus $x \in B$ and $x \notin B$, which is a contradiction. Therefore the supposition that $A \cap B^c \neq \emptyset$ is false, and so $A \cap B^c = \emptyset$ *[as was to be shown]*.

11. True. *Proof*: Let A, B, and C be any sets such that $A \subseteq B$ and $B \cap C = \emptyset$. *[We must show that $A \cap C = \emptyset$.]* Suppose $A \cap C \neq \emptyset$; that is, suppose there were an element x in $A \cap C$. By definition of intersection, $x \in A$ and $x \in C$. By hypothesis $A \subseteq B$, and so since $x \in A$, $x \in B$ also. Hence $x \in B \cap C$, which implies that $B \cap C \neq \emptyset$. But $B \cap C = \emptyset$ by hypothesis. This is a contradiction. Therefore the supposition that $A \cap C \neq \emptyset$ is false, and so $A \cap C = \emptyset$ *[as was to be shown]*.

12. False. *Counterexample*: Let $A = \{1\}$ and $B = \{2\}$. Then $A \cap B = \emptyset$ but $A \times B = \{(1, 2)\} \neq \emptyset$.

15. True. *Proof*: Let A and B be sets and suppose $X \in \mathscr{P}(A) \cup \mathscr{P}(B)$. Then $X \in \mathscr{P}(A)$ or $X \in \mathscr{P}(B)$ *[by definition of union]*. In case $X \in \mathscr{P}(A)$, then $X \subseteq A$ *[by definition of power set]*, and so $X \subseteq A \cup B$ *[by definition of union]*. In case $X \in \mathscr{P}(B)$, then $X \subseteq B$ *[by definition of power set]*, and so $X \subseteq A \cup B$ *[by definition of union]*. Thus in either case, $X \subseteq A \cup B$, and so $X \in \mathscr{P}(A \cup B)$ *[by definition of power set]*. Hence $\mathscr{P}(A) \cup \mathscr{P}(B) \subseteq \mathscr{P}(A \cup B)$ *[by definition of subset]*.

16. True. *Proof*: Let A and B be sets.

    $\mathscr{P}(A \cap B) \subseteq \mathscr{P}(A) \cap \mathscr{P}(B)$: Let $X \in \mathscr{P}(A \cap B)$. Then X is a subset of $A \cap B$ *[by definition of power set]*, and so every element in X is in both A and B. Thus $X \subseteq A$ and $X \subseteq B$ *[by definition of subset]*, and so $X \in \mathscr{P}(A)$ and $X \in \mathscr{P}(B)$ *[by definition of power set]*. Hence $X \in \mathscr{P}(A) \cap \mathscr{P}(B)$ *[by definition of intersection]*. Consequently, $\mathscr{P}(A \cap B) \subseteq \mathscr{P}(A) \cap \mathscr{P}(B)$ *[by definition of subset]*.

    $\mathscr{P}(A) \cap \mathscr{P}(B) \subseteq \mathscr{P}(A \cap B)$: Let $X \in \mathscr{P}(A) \cap \mathscr{P}(B)$. Then $X \in \mathscr{P}(A)$ and $X \in \mathscr{P}(B)$ *[by definition of intersection]*. Hence $X \subseteq A$ and $X \subseteq B$ *[by definition of power set]*. So every element of X is in both A and B, and thus $X \subseteq A \cap B$ *[by definition of subset]*. It follows that $X \in \mathscr{P}(A \cap B)$ *[by definition of power set]*, and so $\mathscr{P}(A) \cap \mathscr{P}(B) \subseteq \mathscr{P}(A \cap B)$ *[by definition of subset]*.

    [Since both subset containments have been proved, $\mathscr{P}(A \cap B) = \mathscr{P}(A) \cap \mathscr{P}(B)$ by definition of set equality.]

17. False. The elements of $\mathscr{P}(A \times B)$ are subsets of $A \times B$, whereas the elements of $\mathscr{P}(A) \times \mathscr{P}(B)$ are ordered pairs whose first element is a subset of A and whose second element is a subset of B. *Counterexample*: Let $A = B = \{1\}$. Then $\mathscr{P}(A) = \{\emptyset, \{1\}\}$, $\mathscr{P}(B) = \{\emptyset, \{1\}\}$, and $\mathscr{P}(A) \times \mathscr{P}(B) = \{(\emptyset, \emptyset), (\emptyset, \{1\}), (\{1\}, \emptyset), (\{1\}, \{1\})\}$. On the other hand, $A \times B = \{(1, 1)\}$, and so $\mathscr{P}(A \times B) = \{\emptyset, \{(1, 1)\}\}$. By inspection $\mathscr{P}(A) \times \mathscr{P}(B) \neq \mathscr{P}(A \times B)$.

18. *b*. *Negation*: $\forall$ sets S, $\exists$ a set T such that $S \cup T \neq \emptyset$. The negation is true. For example, given any set S, let $T = \{1\}$. Then $S \cup T = S \cup \{1\}$. Since $1 \in S \cup \{1\}$, $S \cup \{1\} \neq \emptyset$.

19. $S_0 = \{\emptyset\}$, $S_1 = \{\{a\}, \{b\}, \{c\}\}$, $S_2 = \{\{a, b\}, \{a, c\}, \{b, c\}\}$, $S_3 = \{\{a, b, c\}\}$. Yes, $\{S_0, S_1, S_2, S_3\}$ is a partition of $\mathscr{P}(S)$ because the sets S_0, S_1, S_2, and S_3 are mutually disjoint and their union is $\mathscr{P}(S)$.

20. No. The sets S_a, S_b, S_c, and $S_\emptyset$ do not form a partition of $\mathscr{P}(S)$ because they are not mutually disjoint. For example, $\{a, b\} \in S_a$ and $\{a, b\} \in S_b$.

21. *d*. S_1 and S_2 each have eight elements.

    e. $S_1 \cup S_2$ has sixteen elements.

    f. $S_1 \cup S_2 = \mathscr{P}(A)$.

22. True. *Proof*: For any positive integer $n \geq 2$, let S be the set of all nonempty subsets of $\{2, 3, \ldots, n\}$, and for each $S_i \in S$, let P_i be the product of all the elements in S_i. Let the property $P(n)$ be the equation

$$\sum_{i=1}^{2^{n-1}-1} P_i = \frac{(n+1)!}{2} - 1.$$

Note: S has $2^{n-1} - 1$ elements, and $\sum_{i=1}^{2^{n-1}-1} P_i$ equals the sum of all products of elements of nonempty subsets of $\{2, 3, \ldots, n\}$. We will prove by mathematical induction that the property is true for all integers $n \geq 2$.

Show that the property is true for $n = 2$: For $n = 2$, $S = \{\{2\}\}$ and there is only one element of S, namely $S_1 = \{2\}$. Then $P_1 = 2$, and so the left-hand side of the equation equals

$\sum_{i=1}^{2^1-1} P_i = \sum_{i=1}^{1} P_i = P_1 = 2$. The right-hand side of the equation is $\dfrac{(2+1)!}{2} - 1 = \dfrac{3!}{2} - 1 = 3 - 1 = 2$ also. Hence the property is true for $n = 2$.

Show that for all integers $k \geq 2$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let k be an integer such that $k \geq 2$, let S be the set of all nonempty subsets of $\{2, 3, \ldots, k\}$, and for each $S_i \in S$, let P_i be the product of all the elements in S_i. Suppose the equation holds for $n = k$. In other words, suppose $\sum_{i=1}^{2^{k-1}-1} P_i = \dfrac{(k+1)!}{2} - 1$. *[This is the inductive hypothesis.]* Let S' be the set of all nonempty subsets of $\{2, 3, \ldots, k+1\}$, and for each $S_i' \in S'$, let P_i' be the product of all the elements in S_i'. Now any subset of $\{2, 3, \ldots, k+1\}$ either contains $k + 1$ or does not contain $k + 1$. Any subset of $\{2, 3, \ldots, k+1\}$ that does not contain $k + 1$ is a subset of $\{2, 3, \ldots, k\}$, and any subset of $\{2, 3, \ldots, k+1\}$ that contains $k + 1$ is the union of a subset of $\{2, 3, \ldots, k\}$ and $\{k+1\}$. Also by Theorem 5.3.1, there are $2^{k-1} - 1$ nonempty subsets of $\{2, 3, \ldots, k\}$ *[because there are $k-1$ elements in the set $\{2, 3, \ldots, k\}$]*, and by the same reasoning there are $2^k - 1$ nonempty subsets of $\{2, 3, \ldots, k+1\}$. Thus

$$\sum_{i=1}^{2^k-1} P_i' = \sum_{i=1}^{2^{k-1}-1} P_i + \begin{bmatrix} \text{the sum of all products of elements of nonempty} \\ \text{subsets of } \{\, 2, 3, \ldots, k+1 \text{ that contain } k+1 \,\} \end{bmatrix}.$$

But given any nonempty subset A of $\{2, 3, \ldots, k+1\}$ that contains $k + 1$, the product of all the elements of A equals $k + 1$ times the product of the elements of $A - \{k+1\}$. Thus the sum of all products of elements of nonempty subsets of $\{2, 3, \ldots, k+1\}$ that contain $k + 1$ equals the product of $k + 1$ times the sum of all products of elements of nonempty subsets of $\{2, 3, \ldots, k\}$ plus 1 *[for the case $A = \{k+1\}$ for which $A - \{k+1\}$ equals the empty set]*. Hence the left-hand side of the equation is

$$\begin{aligned}
\sum_{i=1}^{2^k-1} P_i' &= \sum_{i=1}^{2^{k-1}-1} P_i + (k+1)\left(\sum_{i=1}^{2^{k-1}-1} P_i + 1 \right) \\
&= (1 + (k+1))\left(\sum_{i=1}^{2^{k-1}-1} P_i \right) + (k+1) \\
&= (k+2)\left(\frac{(k+1)!}{2} - 1 \right) + (k+1) \qquad \text{by inductive hypothesis} \\
&= \frac{(k+2)!}{2} - (k+2) + (k+1) \\
&= \frac{(k+2)!}{2} - 1
\end{aligned}$$

which is the right-hand side of the equation. Thus the property is true for $n = k + 1$ *[as was to be shown]*.

24. *e.* double complement law   *f.* distributive law   *g.* set difference law

27. *Proof:* Let sets A, B, and C be given. Then

$$\begin{aligned}
(A - B) - C &= (A \cap B^c) \cap C^c && \text{by the set difference law (used twice)} \\
&= A \cap (B^c \cap C^c) && \text{by the associative law for } \cap \\
&= A \cap (B \cup C)^c && \text{by De Morgan's law} \\
&= A - (B \cup C) && \text{by the set difference law.}
\end{aligned}$$

28. *Proof*: Let A and B be sets. Then

$$
\begin{aligned}
A - (A - B) &= A \cap (A \cap B^c)^c & \text{by the set difference law (used twice)} \\
&= A \cap (A^c \cup (B^c)^c) & \text{by De Morgan's law} \\
&= A \cap (A^c \cup B) & \text{by the double complement law} \\
&= (A \cap A^c) \cup (A \cap B) & \text{by the distributive law} \\
&= \emptyset \cup (A \cap B) & \text{by the complement law for } \cap \\
&= (A \cap B) \cup \emptyset & \text{by the commutative law for } \cup \\
&= A \cap B & \text{by the identity law for } \cup.
\end{aligned}
$$

30. *Proof*: Let sets A and B be given. Then

$$
\begin{aligned}
(B^c \cup (B^c - A))^c &= (B^c \cup (B^c \cap A^c))^c & \text{by the set difference law} \\
&= (B^c)^c \cap (B^c \cap A^c)^c & \text{by De Morgan's law} \\
&= B \cap (B^c \cap A^c)^c & \text{by the double complement law} \\
&= B \cap ((B^c)^c \cup (A^c)^c) & \text{by De Morgan's law} \\
&= B \cap (B \cup A) & \text{by the double complement law (used twice)} \\
&= B & \text{by the absorption law.}
\end{aligned}
$$

31. *Proof*: Let A and B be sets. Then

$$
\begin{aligned}
A - (A \cap B) &= A \cap (A \cap B)^c & \text{by the set difference law} \\
&= A \cap (A^c \cup B^c) & \text{by De Morgan's law} \\
&= (A \cap A^c) \cup (A \cap B^c) & \text{by the distributive law} \\
&= \emptyset \cup (A \cap B^c) & \text{by the complement law for } \cap \\
&= (A \cap B^c) \cup \emptyset & \text{by the commutative law for } \cup \\
&= A \cap B^c & \text{by the identity law for } \cup \\
&= A - B & \text{by the set difference law.}
\end{aligned}
$$

32. *Proof*: Let A and B be any sets. Then $(A - B) \cup (B - A)$

$$
\begin{aligned}
&= (A \cap B^c) \cup (B \cap A^c) & \text{by the set difference law (used twice)} \\
&= [(A \cap B^c) \cup B] \cap [(A \cap B^c) \cup A^c)] & \text{by the distributive law} \\
&= [B \cup (A \cap B^c)] \cap [A^c \cup (A \cap B^c)] & \text{by the commutative law for } \cup \text{ (used twice)} \\
&= [(B \cup A) \cap (B \cup B^c)] \cap [(A^c \cup A) \cap (A^c \cup B^c)] & \text{by the distributive law (used twice)} \\
&= [(A \cup B) \cap (B \cup B^c)] \cap [(A \cup A^c) \cap (A^c \cup B^c)] & \text{by the commutative law for } \cup \text{ (used twice)} \\
&= [(A \cup B) \cap U] \cap [U \cap (A^c \cup B^c)] & \text{by the complement law for } \cup \text{ (used twice)} \\
&= [(A \cup B) \cap U] \cap [(A^c \cup B^c) \cap U] & \text{by the commutative law for } \cap \\
&= (A \cup B) \cap (A^c \cup B^c) & \text{by the identity law for } \cap \text{ (used twice)} \\
&= (A \cup B) \cap (A \cap B)^c & \text{by De Morgan's law} \\
&= (A \cup B) - (A \cap B) & \text{by the set difference law.}
\end{aligned}
$$

33. *Proof*: Let A, B, and C be any sets. Then

$(A - B) - (B - C)$

$$
\begin{aligned}
&= (A \cap B^c) \cap (B \cap C^c)^c & \text{by the set difference law (used three times)} \\
&= (A \cap B^c) \cap (B^c \cup (C^c)^c) & \text{by De Morgan's law} \\
&= (A \cap B^c) \cap (B^c \cup C) & \text{by the double complement law} \\
&= ((A \cap B^c) \cap B^c) \cup ((A \cap B^c) \cap C) & \text{by the distributive law} \\
&= (A \cap (B^c \cap B^c)) \cup ((A \cap B^c) \cap C) & \text{by the associative law for } \cap \\
&= (A \cap B^c) \cup ((A \cap B^c) \cap C) & \text{by the idempotent law for } \cap \\
&= A \cap B^c & \text{by the absorption law} \\
&= A - B & \text{by the set difference law.}
\end{aligned}
$$

34. Let A and B be any sets. Then

$A \cap ((B \cup A^c) \cap B^c)$

$$
\begin{aligned}
&= A \cap (B^c \cap (B \cup A^c)) && \text{by the commutative law for } \cap \\
&= A \cap ((B^c \cap B) \cup (B^c \cap A^c)) && \text{by the distributive law} \\
&= A \cap ((B \cap B^c) \cup (B^c \cap A^c)) && \text{by the commutative law for } \cap \\
&= A \cap (\emptyset \cup (B^c \cap A^c)) && \text{by the complement law for } \cap \\
&= A \cap ((B^c \cap A^c) \cup \emptyset) && \text{by the commutative law for } \cup \\
&= A \cap (B^c \cap A^c) && \text{by the identity law for } \cup \\
&= A \cap (A^c \cap B^c) && \text{by the commutative law for } \cap \\
&= (A \cap A^c) \cap B^c && \text{by the associative law for } \cap \\
&= \emptyset \cap B^c && \text{by the complement law for } \cap \\
&= B^c \cap \emptyset && \text{by the commutative law for } \cap \\
&= \emptyset && \text{by the universal bound law for } \cap.
\end{aligned}
$$

Alternate derivation:

$A \cap ((B \cup A^c) \cap B^c)$

$$
\begin{aligned}
&= A \cap (B^c \cap (B \cup A^c)) && \text{by the commutative law for } \cap \\
&= (A \cap B^c) \cap (B \cup A^c) && \text{by the associative law for } \cap \\
&= (A \cap B^c) \cap (A^c \cup B) && \text{by the commutative law for } \cup \\
&= (A \cap B^c) \cap (A^c \cup (B^c)^c) && \text{by the double complement law} \\
&= (A \cap B^c) \cap (A \cap B^c)^c && \text{by De Morgan's law} \\
&= \emptyset && \text{by the complement law for } \cap.
\end{aligned}
$$

35. Let A and B be any sets. Then

$(A - (A \cap B)) \cap (B - (A \cap B))$

$$
\begin{aligned}
&= (A \cap (A \cap B)^c) \cap (B \cap (A \cap B)^c) && \text{by the set difference law (used twice)} \\
&= A \cap ((A \cap B)^c \cap (B \cap (A \cap B)^c)) && \text{by the associative law for } \cap \\
&= A \cap (((A \cap B)^c \cap B) \cap (A \cap B)^c) && \text{by the associative law for } \cap \\
&= A \cap ((B \cap (A \cap B)^c) \cap (A \cap B)^c) && \text{by the commutative law for } \cap \\
&= A \cap (B \cap ((A \cap B)^c \cap (A \cap B)^c)) && \text{by the associative law for } \cap \\
&= A \cap (B \cap (A \cap B)^c) && \text{by the idempotent law for } \cap \\
&= (A \cap B) \cap (A \cap B)^c && \text{by the associative law for } \cap \\
&= \emptyset && \text{by the complement law for } \cap.
\end{aligned}
$$

36. Let A, B, and C be any sets. Then $((A \cap (B \cup C)) \cap (A - B)) \cap (B \cup C^c)$

$$
\begin{aligned}
&= ((A \cap (B \cup C)) \cap (A \cap B^c)) \cap (B \cup C^c) && \text{by the set difference law} \\
&= ((A \cap B^c) \cap (A \cap (B \cup C))) \cap (B \cup C^c) && \text{by the commutative law for } \cap \\
&= (((A \cap B^c) \cap A) \cap (B \cup C)) \cap (B \cup C^c) && \text{by the associative law for } \cap \\
&= ((A \cap (A \cap B^c)) \cap (B \cup C)) \cap (B \cup C^c) && \text{by the commutative law for } \cap \\
&= (((A \cap A) \cap B^c) \cap (B \cup C)) \cap (B \cup C^c) && \text{by the associative law for } \cap \\
&= ((A \cap B^c) \cap (B \cup C)) \cap (B \cup C^c) && \text{by the idempotent law for } \cap \\
&= (A \cap B^c) \cap ((B \cup C) \cap (B \cup C^c)) && \text{by the associative law for } \cap \\
&= (A \cap B^c) \cap (B \cup (C \cap C^c)) && \text{by the distributive law} \\
&= (A \cap B^c) \cap (B \cup \emptyset) && \text{by the complement law for } \cap \\
&= (A \cap B^c) \cap B && \text{by the identity law for } \cup \\
&= A \cap (B^c \cap B) && \text{by the associative law for } \cap \\
&= A \cap (B \cap B^c) && \text{by the commutative law for } \cap \\
&= A \cap \emptyset && \text{by the complement law for } \cap \\
&= \emptyset && \text{by the universal bound law for } \cap.
\end{aligned}
$$

37. *c.* There is no single correct answer to this question, but students might notice that the main idea of the element proof is simply that no element can be simultaneously in B and in $A - B$ (because for it to be in $A - B$ means that it is not in B). On the other hand the algebraic proof involves five rather formal steps, which could reasonably be viewed as more complicated.

38. *a. Proof:* Let A, B, and C be any sets.

$(A - B) \cup (B - C) \subseteq (A \cup B) - (B \cap C)$: Suppose $x \in (A - B) \cup (B - C)$. By definition of union, $x \in A - B$ or $x \in B - C$.

Case 1 ($x \in A - B$): In this case, by definition of set difference, $x \in A$ and $x \notin B$. Then since $x \in A$, by definition of union, $x \in A \cup B$. Also, since $x \notin B$, then $x \notin B \cap C$ (for otherwise, by definition of intersection, x would be in B, which it is not). Thus $x \in A \cup B$ and $x \notin B \cap C$, and so, by definition of set difference, $x \in (A \cup B) - (B \cap C)$.

Case 2 ($x \in B - C$): In this case, by definition of set difference, $x \in B$ and $x \notin C$. Then since $x \in B$, by definition of union, $x \in A \cup B$. Also, since $x \notin C$, then $x \notin B \cap C$ (for otherwise, by definition of intersection, x would be in C, which it is not). Thus $x \in A \cup B$ and $x \notin B \cap C$, and so, by definition of set difference, $x \in (A \cup B) - (B \cap C)$.

Therefore, in either case, $x \in (A \cup B) - (B \cap C)$, and so, by definition of subset, $(A - B) \cup (B - C) \subseteq (A \cup B) - (B \cap C)$.

$(A \cup B) - (B \cap C) \subseteq (A - B) \cup (B - C)$: Suppose $x \in (A \cup B) - (B \cap C)$. By definition of set difference, $x \in A \cup B$ and $x \notin B \cap C$. Note that either $x \in B$ or $x \notin B$.

Case 1 ($x \in B$): In this case $x \notin C$ because otherwise x would be in both B and C, which would contradict the fact that $x \notin B \cap C$. Thus, in this case, $x \in B$ and $x \notin C$, and so $x \in B - C$ by definition of set difference. Then $x \in (A - B) \cup (B - C)$ by definition of union.

Case 2 ($x \notin B$): In this case, since $x \in A \cup B$, then $x \in A$. Hence $x \in A$ and $x \notin B$, and so $x \in A - B$ by definition of set difference. Then $x \in (A - B) \cup (B - C)$ by definition of union.

Hence, in both cases, $x \in (A - B) \cup (B - C)$, and so, by definition of subset, $(A \cup B) - (B \cap C) \subseteq (A - B) \cup (B - C)$.

Therefore, since both set containments have been proved, we conclude that $(A - B) \cup (B - C) = (A \cup B) - (B \cap C)$ by definition of set equality.

b. Proof: Let A, B, and C be any sets. Then

$(A - B) \cup (B - C)$

$=$	$(A \cap B^c) \cup (B \cap C^c)$	by the set difference law (used twice)
$=$	$((A \cap B^c) \cup B) \cap ((A \cap B^c) \cup C^c)$	by the distributive law
$=$	$(B \cup (A \cap B^c)) \cap ((A \cap B^c) \cup C^c)$	by the commutative law for $\cup$
$=$	$((B \cup A) \cap (B \cup B^c)) \cap ((A \cap B^c) \cup C^c)$	by the distributive law
$=$	$((B \cup A) \cap U) \cap ((A \cap B^c) \cup C^c)$	by the complement law for $\cup$
$=$	$(B \cup A) \cap ((A \cap B^c) \cup C^c)$	by the identity law for $\cap$
$=$	$(A \cup B) \cap ((A \cap B^c) \cup C^c)$	by the commutative law for $\cup$
$=$	$((A \cup B) \cap (A \cap B^c)) \cup ((A \cup B) \cap C^c)$	by the distributive law
$=$	$(((A \cup B) \cap A) \cap B^c) \cup ((A \cup B) \cap C^c)$	by the associative law for $\cap$
$=$	$((A \cap (A \cup B)) \cap B^c) \cup ((A \cup B) \cap C^c)$	by the commutative law for $\cap$
$=$	$(A \cap B^c) \cup ((A \cup B) \cap C^c)$	by the absorption law
$=$	$((A \cap B^c) \cup \emptyset) \cup ((A \cup B) \cap C^c)$	by the identity law for $\cup$
$=$	$((A \cap B^c) \cup (B \cap B^c)) \cup ((A \cup B) \cap C^c)$	by the complement law for $\cap$
$=$	$((B^c \cap A) \cup (B^c \cap B)) \cup ((A \cup B) \cap C^c)$	by the commutative law for $\cap$
$=$	$(B^c \cap (A \cup B)) \cup ((A \cup B) \cap C^c)$	by the distributive law
$=$	$((A \cup B) \cap B^c)) \cup ((A \cup B) \cap C^c)$	by the commutative law for $\cap$
$=$	$(A \cup B) \cap (B^c \cup C^c)$	by the distributive law
$=$	$(A \cup B) \cap (B \cap C)^c$	by De Morgan's law
$=$	$(A \cup B) - (B \cap C)$	by the set difference law.

c. Although writing down every detail of the element proof is somewhat tedious, its basic idea is not hard to see. In this case the element proof is probably easier than the algebraic proof.

39. *b.* $B \triangle C = (\{3,4,5,6\} - \{5,6,7,8\}) \cup (\{5,6,7,8\} - \{3,4,5,6\}) = \{3,4\} \cup \{7,8\} = \{3,4,7,8\}$

c. $A \triangle C = (\{1,2,3,4\} - \{5,6,7,8\}) \cup (\{5,6,7,8\} - \{1,2,3,4\}) = \{1,2,3,4\} \cup \{5,6,7,8\} = \{1,2,3,4,5,6,7,8\}$

d. By part (a), $A \triangle B = \{1,2,5,6\}$. So $(A \triangle B) \triangle C = (\{1,2,5,6\} - \{5,6,7,8\}) \cup (\{5,6,7,8\} - \{1,2,5,6\}) = \{1,2\} \cup \{7,8\} = \{1,2,7,8\}$.

42. *Proof*: Let A be any subset of a universal set U. Then

$$
\begin{aligned}
A \triangle A^c &= (A - A^c) \cup (A^c - A) && \text{by definition of } \triangle \\
&= (A \cap (A^c)^c) \cup (A^c \cap A^c) && \text{by the set difference law (used twice)} \\
&= (A \cap A) \cup (A^c \cap A^c) && \text{by the double complement law} \\
&= A \cup A^c && \text{by the idempotent law for } \cap \text{ (used twice)} \\
&= U && \text{by the complement law for } \cup.
\end{aligned}
$$

43. *Proof 1*: Let A be any subset of a universal set U. Then

$$
\begin{aligned}
A \triangle A &= (A - A) \cup (A - A) && \text{by definition of } \triangle \\
&= (A \cap A^c) \cup (A \cap A^c) && \text{by the set difference law (used twice)} \\
&= \emptyset \cup \emptyset && \text{by the complement law for } \cap \text{ (used twice)} \\
&= \emptyset && \text{by the identity law for } \cup.
\end{aligned}
$$

Proof 2: Let A be any subset of a universal set U. Then

$$
\begin{aligned}
A \triangle A &= (A - A) \cup (A - A) && \text{by definition of } \triangle \\
&= A - A && \text{by the idempotent law} \\
&= A \cap A^c && \text{by the set difference law} \\
&= \emptyset && \text{by the complement law for } \cap.
\end{aligned}
$$

44. *Lemma*: For any subsets A and B of a universal set U and for any element x,

(1) $x \in A \triangle B \Leftrightarrow (x \in A \text{ and } x \notin B) \text{ or } (x \notin A \text{ and } x \in B)$

(2) $x \notin A \triangle B \Leftrightarrow (x \notin A \text{ and } x \notin B) \text{ or } (x \in A \text{ and } x \in B)$.

Proof:

(1) Suppose A and B are any sets and x is any element. Then

$$
\begin{aligned}
x \in A \triangle B &\Leftrightarrow x \in (A - B) \cup (B - A) && \text{by definition of } \triangle \\
&\Leftrightarrow x \in A - B \text{ or } x \in B - A && \text{by definition of } \cup \\
&\Leftrightarrow (x \in A \text{ and } x \notin B) \text{ or } (x \in B \text{ and } x \notin A) && \text{by definition of } \cap.
\end{aligned}
$$

(2) Suppose A and B are any sets and x is any element. Observe that there are only four mutually exclusive possibilities for the relationship of x to A and B: $(x \in A \text{ and } x \notin B)$ or $(x \in B \text{ and } x \notin A)$ or $(x \in A \text{ and } x \in B)$ or $(x \notin A \text{ and } x \notin B)$. By part (1), the condition that $x \in A \triangle B$ is equivalent to the first two possibilities. So the condition that $x \notin A \triangle B$ is equivalent to the second two possibilities. In other words, $x \notin A \triangle B \Leftrightarrow (x \notin A \text{ and } x \notin B)$ or $(x \in A \text{ and } x \in B)$.

Theorem: For all subsets A, B, and C of a universal set U, if $A \triangle C = B \triangle C$ then $A = B$.

Proof: Let A, B, and C be any subsets of a universal set U, and suppose that $A \triangle C = B \triangle C$. *[We will show that $A = B$.]*

$A \subseteq B$: Suppose $x \in A$. Either $x \in C$ or $x \notin C$. If $x \in C$, then $x \in A$ and $x \in C$ and so by the lemma, $x \notin A \triangle C$. But $A \triangle C = B \triangle C$. Thus $x \notin B \triangle C$ either. Hence, again by the lemma, since $x \in C$ and $x \notin B \triangle C$, then $x \in B$. On the other hand, if $x \notin C$, then by the lemma, since $x \in A$, $x \in A \triangle C$. But $A \triangle C = B \triangle C$. So, again by the lemma, since $x \notin C$ and $x \in B \triangle C$, then $x \in B$. Hence in either case, $x \in B$ *[as was to be shown]*.

$B \subseteq A$: The proof is exactly the same as for $A \subseteq B$ with the letters A and B reversed.

Since $A \subseteq B$ and $B \subseteq A$, by definition of set equality $A = B$.

45. *Proof 1*: Suppose A, B, and C are any subsets of a universal set U. Then

$$x \in (A \triangle B) \triangle C \quad \Leftrightarrow \quad (x \in A \triangle B \text{ and } x \notin C) \text{ or } (x \in C \text{ and } x \notin A \triangle B)$$
by the lemma from the solution to 44
$$\Leftrightarrow \quad ([(x \in A \text{ and } x \notin B) \text{ or } (x \in B \text{ and } x \notin A)] \text{ and } x \notin C) \text{ or}$$
$$(x \in C \text{ and } [(x \in A \text{ and } x \in B) \text{ or } (x \notin A \text{ and } x \notin B)])$$
by the lemma from the solution to 44
$$\Leftrightarrow \quad ([x \in A \text{ and } x \notin B \text{ and } x \notin C] \text{ or } [x \in B \text{ and } x \notin A \text{ and } x \notin C]) \text{ or}$$
$$([x \in C \text{ and } x \in A \text{ and } x \in B] \text{ or } [x \in C \text{ and } x \notin A \text{ and } x \notin B])$$
by the distributive and associative laws of logic
$$\Leftrightarrow \quad x \text{ is in exactly one of the sets } A, B, \text{ and } C, \text{ or}$$
$$x \text{ is in all three of the sets } A, B, \text{ and } C.$$

On the other hand,

$$x \in A \triangle (B \triangle C) \quad \Leftrightarrow \quad (x \in A \text{ and } x \notin B \triangle C) \text{ or } (x \in B \triangle C \text{ and } x \notin A)$$
by the lemma from the solution to 44
$$\Leftrightarrow \quad (x \in B \triangle C \text{ and } x \notin A) \text{ or } (x \in A \text{ and } x \notin B \triangle C)$$
by the commutative law for *or*.

By exactly the same sequence of steps as in the first part of this proof but with B in place of A, C in place of B, and A in place of C, we deduce that

$$x \in A \triangle (B \triangle C) \quad \Leftrightarrow \quad x \text{ is in exactly one of the sets } A, B, \text{ and } C, \text{ or}$$
$$x \text{ is in all three of the sets } A, B, \text{ and } C.$$

So $x \in (A \triangle B) \triangle C \Leftrightarrow x \in A \triangle (B \triangle C)$, and hence $(A \triangle B) \triangle C = A \triangle (B \triangle C)$.

Proof 2: Suppose A, B, and C are any subsets of a universal set U. Then

$(A \triangle B) \triangle C$

$$= \quad ((A \triangle B) - C) \cup (C - (A \triangle B))$$
by definition of symmetric difference
$$= \quad (((A - B) \cup (B - A)) - C) \cup (C - ((A - B) \cup (B - A)))$$
by definition of symmetric difference (used twice)
$$= \quad (((A \cap B^c) \cup (B \cap A^c)) \cap C^c) \cup (C \cap ((A \cap B^c) \cup (B \cap A^c))^c)$$
by the set difference law (used six times)
$$= \quad (((A \cap B^c) \cap C^c) \cup ((B \cap A^c) \cap C^c)) \cup (C \cap ((A \cap B^c) \cup (B \cap A^c))^c)$$
by the commutative law for $\cap$ and the distributive law
$$= \quad (((A \cap B^c) \cap C^c) \cup ((A^c \cap B) \cap C^c)) \cup (C \cap ((A \cap B^c)^c \cap (B \cap A^c)^c))$$
by the commutative law for $\cap$ and De Morgan's law
$$= \quad (((A \cap B^c) \cap C^c) \cup ((A^c \cap B) \cap C^c)) \cup (C \cap ((A^c \cup B) \cap (B^c \cup A)))$$
by De Morgan's law and the double complement law
$$= \quad ((A \cap B^c \cap C^c) \cup (A^c \cap B \cap C^c)) \cup ((C \cap (A^c \cup B)) \cap (B^c \cup A))$$
by the associative law for $\cap$
$$= \quad ((A \cap B^c \cap C^c) \cup (A^c \cap B \cap C^c)) \cup (((C \cap A^c) \cup (C \cap B)) \cap (B^c \cup A))$$
by the distributive law
$$= \quad ((A \cap B^c \cap C^c) \cup (A^c \cap B \cap C^c)) \cup (((C \cap A^c) \cap (B^c \cup A)) \cup ((C \cap B) \cap (B^c \cup A)))$$
by the commutative law for $\cap$ and the distributive law
$$= \quad ((A \cap B^c \cap C^c) \cup (A^c \cap B \cap C^c)) \cup$$
$$(((C \cap A^c) \cap B^c) \cup ((C \cap A^c) \cap A)) \cup ((C \cap B) \cap B^c) \cup ((C \cap B) \cap A)))$$
by the distributive law (used twice)

$$\begin{aligned}
= \;& ((A \cap B^c \cap C^c) \cup (A^c \cap B \cap C^c)) \cup \\
& (((A^c \cap B^c \cap C) \cup (C \cap (A^c \cap A))) \cup ((C \cap (B \cap B^c)) \cup (A \cap B \cap C)))
\end{aligned}$$
by the commutative and associative laws for $\cap$
$$\begin{aligned}
= \;& ((A \cap B^c \cap C^c) \cup (A^c \cap B \cap C^c)) \cup \\
& (((A^c \cap B^c \cap C) \cup (C \cap \emptyset)) \cup ((C \cap \emptyset) \cup (A \cap B \cap C)))
\end{aligned}$$
by the complement law for $\cap$ (used twice)
$$= ((A \cap B^c \cap C^c) \cup (A^c \cap B \cap C^c)) \cup (((A^c \cap B^c \cap C) \cup \emptyset) \cup (\emptyset \cup (A \cap B \cap C)))$$
by the universal bound law for $\cap$ (used twice)
$$= ((A \cap B^c \cap C^c) \cup (A^c \cap B \cap C^c)) \cup ((A^c \cap B^c \cap C) \cup (A \cap B \cap C))$$
by the commutative and identity laws for $\cup$
$$= (A \cap B^c \cap C^c) \cup (A^c \cap B \cap C^c) \cup (A^c \cap B^c \cap C) \cup (A \cap B \cap C)$$
by the associative law for $\cup$.

A similar set of steps shows that $A \triangle (B \triangle C) = (A \cap B^c \cap C^c) \cup (A^c \cap B \cap C^c) \cup (A^c \cap B^c \cap C) \cup (A \cap B \cap C)$ also. Hence $(A \triangle B) \triangle C = A \triangle (B \triangle C)$.

46. *Proof*: Suppose A and B are any subsets of a universal set U. By the universal bound law for $\cup$, $B \cup U = U$, and so, by the commutative law for $\cup$, $U \cup B = U$. Take the intersection of both sides with A to obtain $A \cap (U \cup B) = A \cap U$. But the left-hand side of this equation is $A \cap (U \cup B) = (A \cap U) \cup (A \cap B) = A \cup (A \cap B)$ by the distributive law and the identity law for $\cap$. And the right-hand side of the equation equals A by the identity law for $\cap$. Hence $A \cup (A \cap B) = A$ *[as was to be shown]*.

47. *Proof*: Suppose A and B are any subsets of a universal set U. By the universal bound law for $\cap$, $B \cap \emptyset = \emptyset$, and so, by the commutative law for $\cap$, $\emptyset \cap B = \emptyset$. Take the union of both sides with A to obtain $A \cup (\emptyset \cap B) = A \cup \emptyset$. But the left-hand side of this equation is $A \cup (\emptyset \cap B) = (A \cup \emptyset) \cap (A \cup B) = A \cap (A \cup B)$ by the distributive law and the identity law for $\cup$. And the right-hand side of the equation equals A by the by the identity law for $\cup$. Hence $A \cap (A \cup B) = A$ *[as was to be shown]*.

49. *a*. complement law for $+$ *b*. associative law for $+$ *c*. complement law for $+$

50. *a*. commutative law for $\cdot$ *b*. distributive law for $\cdot$ over $+$

c. idempotent law for $\cdot$ (exercise 48)   *d*. identity law for $\cdot$

e. distributive law for $\cdot$ over $+$ *f*. commutative law for $+$ *g*. identity law for $\cdot$

Note that once Theorem 5.3.2(5b) has been proved (exercise 51), the proof of this property (Theorem 5.3.2(7a)) can be streamlined as shown below.

Proof: For all elements a and b in B,
$$\begin{aligned}
(a + b) \cdot a &= (a + b) \cdot (a + 0) && \text{by the identity law for } + \\
&= a + (b \cdot 0) && \text{by the distributive law for } + \text{ over } \cdot \\
&= a + 0 && \text{by exercise 51} \\
&= a && \text{by the identity law for } +.
\end{aligned}$$

52. *Proof*: For all elements a and b in B,
$$\begin{aligned}
(a \cdot b) + a &= (a \cdot b) + (a \cdot 1) && \text{by the identity law for } \cdot \\
&= a \cdot (b + 1) && \text{by the distributive law for } \cdot \text{ over } + \\
&= a \cdot 1 && \text{by exercise 49} \\
&= a && \text{by the identity law for } \cdot.
\end{aligned}$$

54. *Proof*: By the uniqueness of the complement law, to show that $\overline{1} = 0$, it suffices to show that $1 + 0 = 1$ and $1 \cdot 0 = 0$. But the first equation is true by the identity law for $+$, and the second equation is true by exercise 51 (the universal bound law for $\cdot$). Thus $\overline{1} = 0$.

56. *Proof 1*: By exercise 55, we know that for all x and y in B, $\overline{x \cdot y} = \overline{x} + \overline{y}$. So suppose a and b are any elements in B. Substitute $\overline{a}$ and $\overline{b}$ in place of x and y in this equation to obtain $\overline{\overline{a} \cdot \overline{b}} = \overline{\overline{a}} + \overline{\overline{b}}$, and since $\overline{\overline{a}} + \overline{\overline{b}} = a + b$ by the double complement law, we have $\overline{\overline{a} \cdot \overline{b}} = a + b$. Hence by the uniqueness of the complement law, the complement of $\overline{a} \cdot \overline{b}$ is $a + b$. It follows by definition of complement that

$$(\overline{a} \cdot \overline{b}) + (a + b) = 1 \qquad \text{and} \qquad (\overline{a} \cdot \overline{b}) \cdot (a + b) = 0.$$

By the commutative laws for $+$ and $\cdot$,

$$(a + b) + (\overline{a} \cdot \overline{b}) = 1 \qquad \text{and} \qquad (a + b) \cdot (\overline{a} \cdot \overline{b}) = 0,$$

and thus by the uniqueness of the complement law, the complement of $a + b$ is $\overline{a} \cdot \overline{b}$. In other words, $\overline{a + b} = \overline{a} \cdot \overline{b}$.

Proof 2: An alternative proof can be obtained by taking the proof for exercise 55 in Appendix B and changing every $+$ sign to a $\cdot$ sign and every $\cdot$ sign to a $+$ sign.

57. *Proof*: Let x, y, and z be any elements in B such that $x + y = x + z$ and $x \cdot y = x \cdot z$. Then

$$
\begin{aligned}
y &= (y + x) \cdot y && \text{by exercise 50} \\
&= (x + y) \cdot y && \text{by the commutative law for } + \\
&= (x + z) \cdot y && \text{by hypothesis} \\
&= y \cdot (x + z) && \text{by the commutative law for } \cdot \\
& y \cdot x + y \cdot z && \text{by the distributive law for } \cdot \text{ over } + \\
&= (x \cdot y) + (z \cdot y) && \text{by the commutative law for } \cdot \text{ (used twice)} \\
&= (x \cdot z) + (z \cdot y) && \text{by hypothesis} \\
&= (z \cdot x) + (z \cdot y) && \text{by the commutative law for } \cdot \\
&= z \cdot (x + y) && \text{by the distributive law for } \cdot \text{ over } + \\
&= z \cdot (x + z) && \text{by hypothesis} \\
&= (z + x) \cdot z && \text{by the commutative laws for } \cdot \text{ and } + \\
&= z && \text{by exercise 50.}
\end{aligned}
$$

58. *a.* (ii) $1 \cdot 0 = 0 \cdot 1 = 0$

The following verifications check all possible cases.

(iii)

$0 + (0 + 0) = 0 + 0 = 0 = 0 + 0 = (0 + 0) + 0$

$0 + (0 + 1) = 0 + 1 = 1 = 0 + 1 = (0 + 0) + 1$

$0 + (1 + 0) = 0 + 1 = 1 = 1 + 0 = (0 + 1) + 0$

$1 + (0 + 0) = 1 + 0 = 1 = 1 + 0 = (1 + 0) + 0$

$0 + (1 + 1) = 0 + 1 = 1 = 1 + 1 = (0 + 1) + 1$

$1 + (0 + 1) = 1 + 1 = 1 = 1 + 1 = (1 + 0) + 1$

$1 + (1 + 0) = 1 + 1 = 1 = 1 + 1 = (1 + 1) + 0$

$1 + (1 + 1) = 1 + 1 = 1 = 1 + 1 = (1 + 1) + 1$

(iv)

$0 \cdot (0 \cdot 0) = 0 \cdot 0 = 0 = 0 \cdot 0 = (0 \cdot 0) \cdot 0$

$0 \cdot (0 \cdot 1) = 0 \cdot 0 = 0 = 0 \cdot 1 = (0 \cdot 0) \cdot 1$

$0 \cdot (1 \cdot 0) = 0 \cdot 0 = 0 = 0 \cdot 0 = (0 \cdot 1) \cdot 0$

$1 \cdot (0 \cdot 0) = 1 \cdot 0 = 0 = 0 \cdot 0 = (1 \cdot 0) \cdot 0$

$0 \cdot (1 \cdot 1) = 0 \cdot 1 = 0 = 0 \cdot 1 = (0 \cdot 1) \cdot 1$

$1 \cdot (0 \cdot 1) = 1 \cdot 0 = 0 = 0 \cdot 1 = (1 \cdot 0) \cdot 1$

$1 \cdot (1 \cdot 0) = 1 \cdot 0 = 0 = 1 \cdot 0 = (1 \cdot 1) \cdot 0$

$1 \cdot (1 \cdot 1) = 1 \cdot 1 = 1 = 1 \cdot 1 = (1 \cdot 1) \cdot 1$

(v)

$0 + (0 \cdot 0) = 0 + 0 = 0 = 0 \cdot 0 = (0 + 0) \cdot (0 + 0)$

$0 + (0 \cdot 1) = 0 + 0 = 0 = 0 \cdot 1 = (0 + 0) \cdot (0 + 1)$

$0 + (1 \cdot 0) = 0 + 0 = 0 = 1 \cdot 0 = (0 + 1) \cdot (0 + 0)$

$1 + (0 \cdot 0) = 1 + 0 = 1 = 1 \cdot 1 = (1 + 0) \cdot (1 + 0)$

$0 + (1 \cdot 1) = 0 + 1 = 1 = 1 \cdot 1 = (0 + 1) \cdot (0 + 1)$

$1 + (0 \cdot 1) = 1 + 0 = 1 = 1 \cdot 1 = (1 + 0) \cdot (1 + 1)$

$1 + (1 \cdot 0) = 1 + 0 = 1 = 1 \cdot 1 = (1 + 1) \cdot (1 + 0)$

$1 + (1 \cdot 1) = 1 + 1 = 1 = 1 \cdot 1 = (1 + 1) \cdot (1 + 1)$

(vi)

$0 \cdot (0 + 0) = 0 \cdot 0 = 0 = 0 + 0 = (0 \cdot 0) + (0 \cdot 0)$

$0 \cdot (0 + 1) = 0 \cdot 1 = 0 = 0 + 0 = (0 \cdot 0) + (0 \cdot 1)$

$0 \cdot (1 + 0) = 0 \cdot 1 = 0 = 0 + 0 = (0 \cdot 1) + (0 \cdot 0)$

$1 \cdot (0 + 0) = 1 \cdot 0 = 0 = 0 + 0 = (1 \cdot 0) + (1 \cdot 0)$

$0 \cdot (1 + 1) = 0 \cdot 1 = 0 = 0 + 0 = (0 \cdot 1) + (0 \cdot 1)$

$1 \cdot (0 + 1) = 1 \cdot 1 = 1 = 0 + 1 = (1 \cdot 0) + (1 \cdot 1)$

$1 \cdot (1 + 0) = 1 \cdot 1 = 1 = 1 + 0 = (1 \cdot 1) + (1 \cdot 0)$

$1 \cdot (1 + 1) = 1 \cdot 1 = 1 = 1 + 1 = (1 \cdot 1) + (1 \cdot 1)$

b. Because $0 + 0 = 0$ and $1 + 0 = 1$, 0 is an identity element for $+$. Similarly, because $0 \cdot 1 = 0$ and $1 \cdot 1 = 1$, 1 is an identity element for $\cdot$.

c. $0 + \overline{0} = 0 + 1 = 1$ and $0 \cdot \overline{0} = 0 \cdot 1 = 0$

$1 + \overline{1} = 1 + 0 = 1$ and $1 \cdot \overline{1} = 1 \cdot 0 = 0$

59. *Proof*: The proofs of the absorption law and the idempotent law do not use the associative law. See, for example, Example 5.3.6 and the solutions to exercises 48, 50, and 52. Thus we may make free use of the absorption and idempotent laws in this proof.

Part 1: We first prove that for all x, y, and z in B, (1) $(x + (y + z)) \cdot x = x$ and (2) $((x + y) + z) \cdot x = x$. So suppose x, y, and z are any elements in B. It follows immediately from the absorption law that (1) $(x + (y + z)) \cdot x = x$. Also,

$$
\begin{aligned}
((x + y) + z)) \cdot x &= x \cdot ((x + y) + z) && \text{by the commutative law for } \cdot \\
&= x \cdot (x + y) + x \cdot z && \text{by the distributive law for } \cdot \text{ over } + \\
&= (x + y) \cdot x + x \cdot z && \text{by the commutative law for } \cdot \\
&= x + x \cdot z && \text{by the absorption law} \\
&= x \cdot x + x \cdot z && \text{by the idempotent law for } \cdot \\
&= x \cdot (x + z) && \text{by the distributive law for } \cdot \text{ over } + \\
&= (x + z) \cdot x && \text{by the commutative law for } \cdot \\
&= x && \text{by the absorption law.}
\end{aligned}
$$

Hence (2) $((x + y) + z) \cdot x = x$.

Part 2: By the commutative law for $+$ and equation (2), for all x, y, and z in B, $((x + y) + z) \cdot y = ((y + x) + z) \cdot y = y$. And by the commutative law for $+$ and equation (2), for all x, y, and z in B, $(x + (y + z)) \cdot y = ((y + x) + z) \cdot y = y$. Thus we have (3) $((x + y) + z) \cdot y = y$ and (4) $(x + (y + z)) \cdot y = y$. By similar reasoning we can also conclude that (5) $((x + y) + z) \cdot z = z$ and (6) $(x + (y + z)) \cdot z = z$.

Part 3: We next prove that for all a, b, and c in B, (7) $a + (b+c) = ((a+b)+c) \cdot (a+(b+c))$ and (8) $(a+b)+c = ((a+b)+c) \cdot (a+(b+c))$. To prove (7), suppose a, b, and c are any elements in B. Then

$$((a+b)+c) \cdot (a+(b+c))$$

$$
\begin{aligned}
&= ((a+b)+c) \cdot a + ((a+b)+c) \cdot (b+c)) && \text{by the distributive law for } \cdot \text{ over } + \\
&= a + ((a+b)+c) \cdot (b+c)) && \text{by equation (2)} \\
&= a + [((a+b)+c) \cdot b + ((a+b)+c) \cdot c] && \text{by the distributive law for } \cdot \text{ over } + \\
&= a + (b+c) && \text{by equations (3) and (5).}
\end{aligned}
$$

Similarly, if a, b, and c are any elements in B. Then we can prove equation (8) as follows:

$$((a+b)+c) \cdot (a+(b+c))$$

$$
\begin{aligned}
&= (a+(b+c)) \cdot ((a+b)+c) && \text{by the commutative law for } \cdot \\
&= (a+(b+c)) \cdot (a+b) + (a+(b+c)) \cdot c && \text{by the distributive law for } \cdot \text{ over } + \\
&= (a+(b+c)) \cdot (a+b) + c && \text{by equation (6)} \\
&= [(a+(b+c)) \cdot a + (a+(b+c)) \cdot b] + c && \text{by the distributive law for } \cdot \text{ over } + \\
&= (a+b) + c && \text{by equations (1) and (4).}
\end{aligned}
$$

Therefore, since both $a + (b+c)$ and $(a+b) + c$ are equal to the same quantity, they are equal to each other: $a + (b+c) = (a+b) + c$.

Part 4: In the last part of the proof, we deduce the associative law for $\cdot$. Suppose a, b, and c are any elements in B. Then

$$
\begin{aligned}
\overline{(a \cdot b) \cdot c} &= \overline{(a \cdot b)} + \overline{c} && \text{by De Morgan's law} \\
&= (\overline{a} + \overline{b}) + \overline{c} && \text{by De Morgan's law} \\
&= \overline{a} + (\overline{b} + \overline{c}) && \text{by } \textit{Part 3} \\
&= \overline{a} + \overline{(b \cdot c)} && \text{by De Morgan's law} \\
&= \overline{a \cdot (b \cdot c)} && \text{by De Morgan's law.}
\end{aligned}
$$

Take the complement of both sides to obtain $\overline{\overline{(a \cdot b) \cdot c}} = \overline{\overline{a \cdot (b \cdot c)}}$, and so, by the double complement law, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

Section 5.4

3. This statement contradicts itself. If it were true, then because it declares itself to be a lie, it would be false. Consequently, it is not true. On the other hand, if it were false, then it would be false that "the sentence in this box is a lie," and so the sentence would be true. Consequently, the sentence is not false. Thus the sentence is neither true nor false, which contradicts the definition of a statement. Hence the sentence is not a statement.

4. Since there are no real numbers with negative squares, this sentence is vacuously true, and hence it is a statement.

6. In order for an *and* statement to be true, both components must be true. So if the given sentence is a true statement, the first component "this sentence is false" is true. But this implies that the sentence is false. In other words, the sentence is not true. On the other hand, if the sentence is false, then at least one component is false. But because the second component "$1 + 1 = 2$" is true, the first component must be false. Thus it is false that "this sentence is false," and so the sentence is true. In other words, the sentence is not false. Thus the sentence is neither true nor false, which contradicts the definition of a statement. Hence the sentence is not a statement.

7. *a.* Assuming that the sentence "If this sentence is true, then $1+1 = 3$" is a statement, then the sentence is either true or false. By definition of truth values for an if-then statement, the only way the sentence can be false is for its hypothesis to be true and its conclusion false. But if

its hypothesis is true, then the sentence is true and therefore it is not false. So it is impossible for the sentence to be false, and hence it is true. Consequently, what its hypothesis asserts is true, and so (again by definition of truth values for if-then statements) its conclusion must also be true. Therefore, $1 + 1 = 3$.

b. We can deduce that "This sentence is true" is not a statement. For if it were a statement, then since $1 + 1 = 3$ is also a statement, the sentence "If this sentence is true, then $1 + 1 = 3$" would also be a statement. It would then follow by part (a) that $1 + 1 = 3$, which we know to be false. So "This sentence is true" is not a statement.

8. Suppose Nixon says (ii) and the only utterance Jones makes about Watergate is (i). Suppose also that apart from (ii) all of Nixon's other assertions about Watergate are evenly split between true and false.

Case 1 (Statement (i) is true): In this case, more than half of Nixon's assertions about Watergate are false, and so (since all of Nixon's other assertions about Watergate are evenly split between true and false) statement (ii) must be false (because it is an assertion about Watergate). So at least one of Jones' statements about Watergate is false. But the only statement Jones makes about Watergate is (i). So statement (i) is false.

Case 2 (Statement (i) is false): In this case, half or more of Nixon's assertions about Watergate are true, and so (since all of Nixon's other assertions about Watergate are evenly split between true and false) statement (ii) must be true. But statement (ii) asserts that everything Jones says about Watergate is true. And so, in particular, statement (i) is true.

The above arguments show that under the given circumstances, statements (i) and (ii) are contradictory.

10. No. Suppose there were such a book. If such a book did not refer to itself, then it would belong to the set of all books that do not refer to themselves. But it is supposed to refer to all books in this set, and so it would refer to itself. On the other hand, if such a book referred to itself, then it would belong to the set of books to which it refers and this set only contains books that do not refer to themselves. Thus it would not refer to itself. It follows that the assumption that such a book exists leads to a contradiction, and so there is no such book.

11. The answer is neither yes nor no. (In other words, the definition of heterological is inherently contradictory.) For if heterological were heterological, then it would describe itself. But by definition of heterological, this would mean that it would not describe itself. Hence it is impossible for heterological to be heterological. On the other hand, if heterological were not heterological, then it would not describe itself. But by definition of heterological this would mean that it would be a heterological word, and so it would be heterological. Hence it is impossible for heterological to be not heterological. These arguments show that heterological is neither heterological nor not heterological.

12. Because the total number of strings consisting of 11 or fewer English words is finite, the number of such strings that describe integers must be also finite. Thus the number of integers described by such strings must be finite, and hence there is a largest such integer, say m. Let $n = m + 1$. Then n is "the smallest integer not describable in fewer than 12 English words." But this description of n contains only 11 words. So n is describable in fewer than 12 English words, which is a contradiction. (*Comment*: This contradiction results from the self-reference in the description of n.)

13. There is no such algorithm.

Proof: Suppose there were an algorithm, call it CheckPrint, such that if a fixed quantity a, an algorithm X, and a data set D are input to it, then

   CheckPrint(a, X, D) prints

      "yes" if X prints a when it is run with data set D

"no" if X does not print a when it is run with data set D.

Let SignalHalt be an algorithm that operates on an algorithm X and a data set D as follows: SignalHalt runs X with D and prints "halts" if X terminates. If X does not terminate, SignalHalt does not terminate either. Observe that

CheckPrint("halt", SignalHalt, (X, D)) prints

"yes" if SignalHalt prints "halts" when it is run with data set (X, D)

"no" if SignalHalt does not print "halts" when it is run with data set (X, D).

Thus, we may define a new algorithm CheckHalt, whose input is an algorithm X and a data set D, as follows:

CheckHalt(X, D) prints

"halts" if CheckPrint("halts", SignalHalt, (X, D)) prints "yes"

"loops forever" if CheckPrint("halts", SignalHalt, (X, D)) prints "no".

The above discussion shows that if there is an algorithm CheckPrint which, for a fixed quantity a, an input algorithm X, and a data set D, can determine whether X prints a when run with data set D, then there is an algorithm CheckHalt that solves the halting problem. Since there is no algorithm that solves the halting problem, there is no algorithm with the property described.

14. *Proof*: Suppose there exists a set A such that $\mathscr{P}(A) \subseteq A$. Let $B = \{x \in A \mid x \notin x\}$. Then $B \subseteq A$, and so $B \in \mathscr{P}(A)$. But then, because $\mathscr{P}(A) \subseteq A$, by definition of subset $B \in A$. Either $B \in B$ or $B \notin B$. Now if $B \in B$, then, by definition of B, $B \notin B$, but if $B \notin B$, then B satisfies the defining property for B, and so $B \in B$. Thus both $B \notin B$ and $B \in B$, which is a contradiction. Hence the supposition is false, and we conclude that there is no set that contains its power set.

Chapter 6: Counting and Probability

The primary aim of this chapter is to help students develop an intuitive understanding for fundamental principles of counting and probability and an ability to apply them in a wide variety of situations.

Students seem most successful in solving counting problems when they have a clear mental image of the objects they are counting. It is helpful to encourage them to get into the habit of beginning a counting problem by listing (or at least imagining) some of the objects they are trying to count. If they see that all the objects to be counted can be matched up with the integers from m to n inclusive, then the total is $n - m + 1$ (Section 6.1). If they see that all the objects can be produced by a multi-step process, then the total can be found by counting the distinct paths from root to leaves in a possibility tree that shows the outcomes of each successive step (Section 6.2). And in case each step of the process can be performed in a fixed number of ways (regardless of how the previous steps were performed), the total can be calculated by applying the multiplication rule (Section 6.2). If they see that the objects to be counted can be separated into disjoint categories, then the total is just the sum of the subtotals for each category (Section 6.3). And in case the categories are not disjoint, the total can be counted using the inclusion/exclusion rule (Section 6.3). If they see that the objects to be counted can be represented as all the subsets of size r of a set with n elements, then the total is $\binom{n}{r}$ for which there is a computational formula (Section 6.4). And if the objects can be represented as all the multisets of size r of a set with n elements, then the total is $\binom{n+r-1}{r}$.

Pascal's formula is discussed in Section 6.6 and the binomial theorem in Section 6.7. Each is proved both algebraically and combinatorially. Exercise 21 of Section 6.4 is a warm-up for the combinatorial proof of the binomial theorem, and exercise 10 of Section 6.7 is intended to help students perceive how Pascal's formula is applied in the algebraic proof of the binomial theorem.

Note that exercise 20 of Section 6.1 should have been placed in Section 6.9. It is best to wait to assign it until that section is covered.

Section 6.1

4. $\{2\clubsuit, 4\clubsuit, 6\clubsuit, 8\clubsuit, 10\clubsuit, 2\spadesuit, 4\spadesuit, 6\spadesuit, 8\spadesuit, 10\spadesuit\}$ Probability $= 10/52 = 5/26 \cong 19.2\%$

6. $\{2\clubsuit, 3\clubsuit, 4\clubsuit, 2\diamondsuit, 3\diamondsuit, 4\diamondsuit, 2\heartsuit, 3\heartsuit, 4\heartsuit, 2\spadesuit, 3\spadesuit, 4\spadesuit\}$ Probability $= 12/52 = 3/13 \cong 23.1\%$

8. $\{11, 22, 33, 44, 55, 66\}$ Probability $= 6/36 = 1/6 \cong 16.7\%$

10. $\{36, 45, 46, 54, 55, 56, 63, 64, 65, 66\}$ Probability $= 10/36 = 5/18 \cong 27.8\%$

11. *b.* (ii) $\{HHT, HTH, THH, HHH\}$ Probability $= 4/8 = 1/2 = 50\%$
    (iii) $\{TTT\}$ Probability $= 1/8 = 12.5\%$

12. *b.* (ii) $\{GGB, GBG, BGG, GGG\}$ Probability $= 4/8 = 1/2 = 50\%$
    (iii) $\{BBB\}$ Probability $= 1/8 = 12.5\% \cap B)$

13. *b.* (ii) $\{CCW, CWC, WCC, CCC\}$ Probability $= 4/8 = 1/2 = 50\%$
    (iii) $\{WWW\}$ Probability $= 1/8 = 12.5\%$

14. *b.* $4/8 = 1/2 = 50\%$
    c. $1/8 = 12.5\%$

15. The methods used to compute the probabilities in exercises 12, 13, and 14 are exactly the same as those in exercise 11. The only difference in the solutions are the symbols used to denote the outcomes; the probabilities are identical. These exercises illustrate the fact that computing

various probabilities that arise in connection with tossing a coin is mathematically identical to computing probabilities in other, more realistic situations. So if the coin tossing model is completely understood, many other probabilities can be computed without difficulty.

17. *a.* $\{RBB, RBY, RYB, RYY, BRB, BRY, YRB, YRY, BBR, BYR, YBR, YYR\}$

     Probability $= 12/27 \cong 44.4\%$

    b. Out of the 27 possible outcomes, there are only 8 in which none of the faces is red: $\{BBB, BBY, BYB, YBB, BYY, YBY, YYB, YYY\}$. So the event that at least one face is red consists of the remaining $27 - 8 = 19$ outcomes. This event has probability $= 19/27 \cong 70.4\%$

19. *a.* $\{B_1B_1, B_1B_2, B_1W_1, B_1W_2, B_1W_3, B_2B_1, B_2B_2, B_2W_1, B_2W_2, B_2W_3, W_1B_1, W_1B_2, W_1W_1,$
    $W_1W_2, W_1W_3, W_2B_1, W_2B_2, W_2W_1, W_2W_2, W_2W_3, W_3B_1, W_3B_2, W_3W_1, W_3W_2, W_3W_3\}$

    b. $\{B_1B_1, B_1B_2, B_1W_1, B_1W_2, B_1W_3, B_2B_1, B_2B_2, B_2W_1, B_2W_2, B_2W_3\}$

     Probability $= 10/25 = 2/5 \cong 40\%$

    c. $\{W_1W_1, W_1W_2, W_1W_3, W_2W_1, W_2W_2, W_2W_3, W_3W_1, W_3W_2, W_3W_3\}$

     Probability $= 9/25 \cong 36\%$

20. *a.* $1/5 = 20\%$

    b. When there are five doors, as described in the exercise statement, there are 16 possible sets of outcomes if you switch doors. These are shown in the table below. For each set of outcomes, the door with the prize is marked with an asterisk. There are fewer possible sets of outcomes if the prize is not behind door A, because in that case the host will not open the door with the prize.

Prize is behind door	You choose one of			
A^*	BCD	BCE	BDE	CDE
B	B^*CD	B^*CE	B^*DE	
C	BC^*D	BC^*E	BC^*D	
D	BCD^*	CD^*E	BD^*E	
E	BCE^*	BDE^*	CDE^*	

In 12 sets of outcomes you would increase your chance of winning the prize by switching, and only 4 sets of outcomes would you not increase your chance of winning by switching. So, if all 16 sets of outcomes were equally likely, you would increase your chance of winning the prize in 12/16 of the sets of outcomes by switching. In fact, however, the 16 sets of outcomes are not equally likely. Because it is just as likely for the prize to be behind door A as it is for the prize to be behind one of the other doors, each of the four sets of outcomes for when the prize is behind door A is less likely than each of the three sets of outcomes for when the prize is behind another door. This implies that your chance of winning by switching is even greater than it would be if all 16 sets of outcomes were equally likely. So the probability of your winning the prize increases if you switch.

Another way to arrive at the conclusion that you are more likely to win the prize by switching is to reason as follows: If the prize is not behind door A and you switch, you have a 1/3 chance of choosing correctly and there is a 4/5 chance that the prize is not behind door A. So the probability of winning the prize if you switch is $(1/3)(4/5) = 4/15 \cong 26.7\%$. This reasoning is formalized using the concept of conditional probability, which is discussed in Section 6.9: Let A be the event that the prize is not behind door A. Then $P(A) = 4/5$ because it is assumed that the prize is equally likely to be behind any of the five doors. Let B be the event that you choose the door with the prize. Then $P(B|A) = 1/3$ because given that the prize is behind one of doors B, C, D, or E, once the host has opened one door, the prize is equally likely to be behind any of the other three doors. Thus the event that you win by switching is the intersection of the event that the prize is not behind door A and the event that you chose the right door out of the three that remain. So the probability that you win by switching is $P(A \cap B) = P(A)P(B|A) = (4/5)(1/3) = 4/15 \cong 26.7\%$.

22. *a.*

100 101 102 103 104 105 106 107 108 ... 990 991 992 993 994 995 996 997 998 999

$\updownarrow$

6 · 17

$\updownarrow$

6 · 18

$\updownarrow$

6 · 165

$\updownarrow$

6 · 166
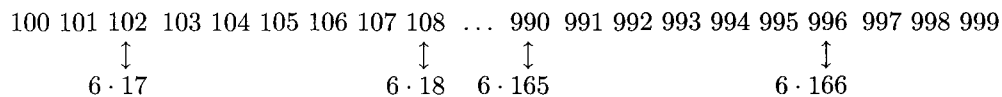
The above diagram shows that there are as many three-digit integers that are multiples of 6 as there are integers from 17 to 166 inclusive. But by Theorem 6.1.1, there are $166 - 17 + 1 = 150$ such integers.

b. The probability that a randomly chosen three-digit integer is a multiple of 6 is

$$150/(999\text{-}100\text{+}1) = 150/900 = 1/6 \cong 16.7\%.$$

23. *a.* n

b. $39 - 4 + 1 = 36$

25. *a.* (i) When n is even, $\left\lfloor \dfrac{n}{2} \right\rfloor = \dfrac{n}{2}$, so the answer is $n - \dfrac{n}{2} + 1 = \dfrac{n}{2} + 1 = \dfrac{n+2}{2}$.

(ii) When n is odd, $\left\lfloor \dfrac{n}{2} \right\rfloor = \dfrac{n-1}{2}$, so the answer is $n - \dfrac{n-1}{2} + 1 = \dfrac{2n-n+1+2}{2} = \dfrac{n+3}{2}$.

b. (i) $\dfrac{\frac{n+2}{2}}{n} = \dfrac{n+2}{2n} = \dfrac{1}{2} + \dfrac{1}{n}$ (ii) $\dfrac{\frac{n+3}{2}}{n} = \dfrac{n+3}{2n} = \dfrac{1}{2} + \dfrac{3}{2n}$

27. Let k be the 62nd element in the array. By Theorem 6.1.1, $k - 29 + 1 = 62$, so $k = 62 + 29 - 1 = 90$. Thus the 62nd element in the array is $B[90]$.

29. Let m be the smallest of the integers. By Theorem 6.1.1, $326 - m + 1 = 87$, so $m = 326 - 87 + 1 = 240$.

30.

1   2   3   4   5   6   ...   998   999   1000   1001

$\updownarrow$ $\updownarrow$ $\updownarrow$ $\updownarrow$ $\updownarrow$

2 · 1   2 · 2   2 · 3   2 · 499   2 · 500
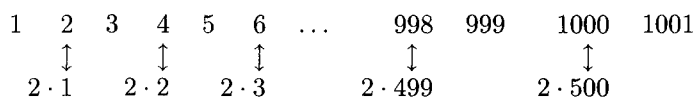
The diagram above shows that there are as many even integers between 1 and 1001 as there are integers from 1 to 500 inclusive. There are 500 such integers.

32. *b.*

M	Tu	W	Th	F	Sa	Su	M	Tu	...	F	Sa	Su	M
1	2	3	4	5	6	7	8	9		362	363	364	365
$\updownarrow$							$\updownarrow$						$\updownarrow$
7 · 0 + 1							7 · 1 + 1						7 · 52 + 1
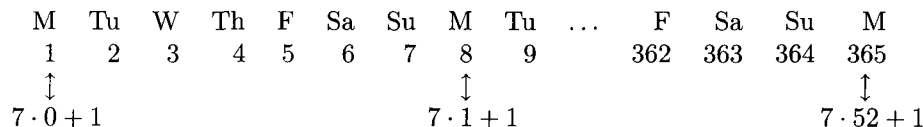
In the diagram above, Mondays occur on days numbered $7k + 1$ where k is an integer from 0 to 52 inclusive. Thus there are as many Mondays in the year as there are such integers, namely $52 - 0 + 1 = 53$ of them.

33. *Proof*: Let m be any integer, and let the property $P(n)$ be the sentence "The number of integers from m to n inclusive is $n - m + 1$." We will prove by mathematical induction that the property is true for all integers $n \geq m$.

Show that the property is true for $n = m$: There is just one integer, namely m, from m to m inclusive. Substituting m in place of n in the formula $n - m + 1$ gives $m - m + 1 = 1$, which is correct.

Show that for all integers $k \geq m$, if the property is true for $n = k$ then it is true for $n = k + 1$: Suppose k is an integer with $k \geq m$, and suppose the number of integers from m to k inclusive is $k - m + 1$. *[This is the inductive hypothesis.]* We must show that the number of integers from m to $k + 1$ inclusive is $m - (k + 1) + 1$.

Consider the sequence of integers from m to $k + 1$ inclusive:

$$\underbrace{m, \quad m + 1, \quad m + 2, \quad \ldots, \quad k,}_{k - m + 1} \quad (k + 1).$$

By inductive hypothesis there are $k - m + 1$ integers from m to k inclusive. So there are $(k - m + 1) + 1$ integers from m to $k + 1$ inclusive. But $(k - m + 1) + 1 = (k + 1) - m + 1$. So there are $(k + 1) - m + 1$ integers from m to $k + 1$ inclusive *[as was to be shown]*.

Section 6.2

2.
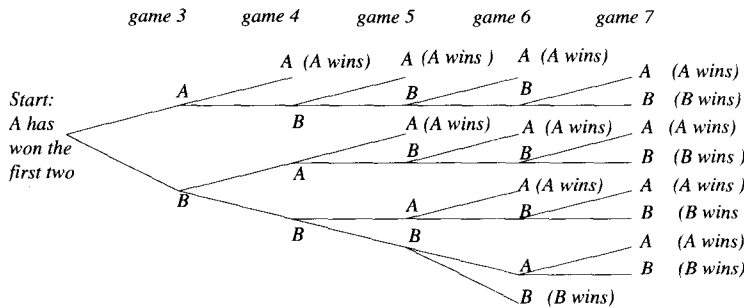
The number of ways to complete the series equals the number of branches on this possibility tree, namely 15. So there are fifteen ways to complete the series.

5.
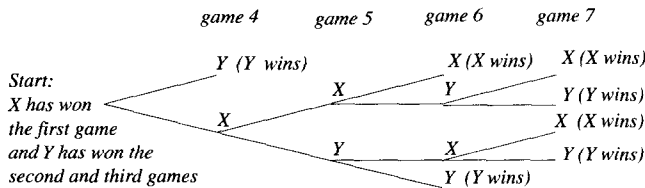
The number of ways to play the competition equals the number of branches on this possibility tree, namely 7. So there are seven ways to play the competition.

7. *a.*
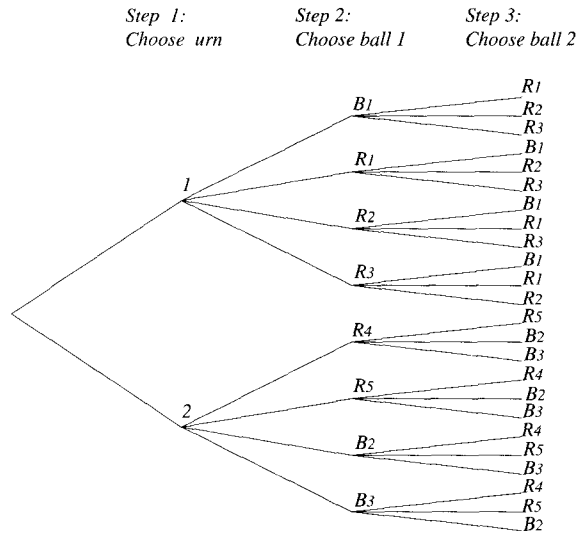
b. There are 24 outcomes of this experiment.

c. The probability that two red balls are chosen is $8/24 = 1/3$.

10. Sketch:
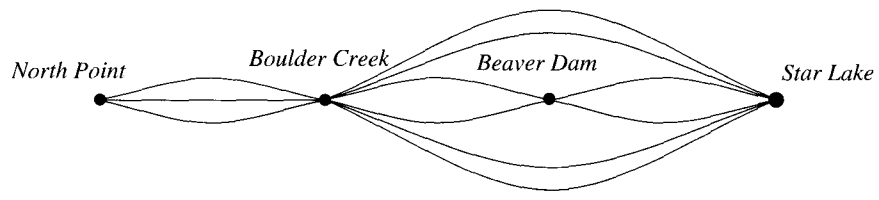
a. Think of creating a route from North Point to Star Lake that passes through Beaver Dam as a 3-step process. Step 1 is to choose a route from North Point to Boulder Creek, step 2 is to choose a route from Boulder Creek to Beaver Dam, and step 3 is to choose a route from Beaver Dam to Star Lake. There are 3 choices for step 1 and 2 choices for each of steps 2 and 3. Thus, the number of routes from North Point to Star Lake that pass through Beaver Dam is $3 \cdot 2 \cdot 2 = 12$.

b. Imagine the following 2-step process for creating a route from North Point to Star Lake that bypasses Beaver Dam: Step 1 is to choose a route from North Point to Boulder Creek, step 2 is to choose a direct route from Boulder Creek to Star Lake. There are 3 choices for step 1 and 4 choices for step 2. Thus, the number of routes from North Point to Star Lake that bypass Beaver Dam is $3 \cdot 4 = 12$.

11. *c.* If a bit string of length 8 begins and ends with a 1, then the six middle positions can be filled with any bit string of length 6. Hence there are $2^6 = 64$ such strings.

d. $2^8 = 256$

12. *b.* Think of creating a string of hexadecimal digits that satisfies the given requirements as a 6-step process. Step 1 is to choose the first hexadecimal digit. It can be any hexadecimal digit from 4 through D (which equals 13) There are $13 - 4 + 1 = 10$ of these. Steps 2–5 are to choose

the second through the fifth hexadecimal digits. Each can be any one of the 16 hexadecimal digits. Step 6 is to choose the last hexadecimal digit. It can be any hexadecimal digit from 2 through E (which equals 14) There are $14 - 2 + 1 = 13$ of these. So the total number of the specified hexadecimal numbers is $10 \cdot 16 \cdot 16 \cdot 16 \cdot 16 \cdot 13 = 8,519,680$.

13. *c.* There are four outcomes in which exactly one head occurs: $HTTT, THTT, TTHT, TTTH$. Since there are 16 outcomes in all, the probability of obtaining exactly one head is $4/16 = 1/4$.

14. Think of creating license plates that satisfy the given requirements as multi-step processes.

c. Because the license plate begins with *TGIF* positions 1–4 in the plate are already taken. Let steps 1–3 be to choose digits for each of positions 5-7. There are 10 ways to perform each of these steps, so there are $10 \cdot 10 \cdot 10 = 1000$ license plates satisfying the given requirements.

e. Because the license plate begins with *AB*, positions 1 and 2 in the plate are already taken. Let steps 1 and 2 be to choose letters for positions 3 and 4, and let steps 3–5 be to choose digits for positions 5–7. Because all letters and digits must be distinct, there are 24 ways to perform step 1 (choose any letter but *A* or *B*), 23 ways to perform step 2 (choose any letter but *A* or *B* or the letter chosen in step 1), 10 ways to perform step 3 (choose any digit), 9 ways to perform step 4 (choose any digit but the one chosen in step 3), and 8 ways to perform step 5 (choose any digit but one chosen in a previous step). Thus there are $24 \cdot 23 \cdot 10 \cdot 9 \cdot 8 = 397,440$ license plates satisfying the given requirements.

15. Think of creating combinations that satisfy the given requirements as multi-step processes in which steps 1-3 are to choose a number from 1 to 30, inclusive.

a. Because there are 30 choices of numbers in each of steps 1–3, there are $30^3 = 27,000$ possible combinations for the lock.

b. In this case we are given that no number may be repeated. So there are 30 choices for step 1, 29 for step 2, and 28 for step 3. Thus there are $30 \cdot 29 \cdot 28 = 24,360$ possible combinations for the lock.

16. *b.* Constructing a PIN that is obtainable by the same keystroke sequence as 5031 can be thought of as the following four-step process. Step 1 is to choose either the digit 5 or one of the three letters on the same key as the digit 5, step 2 is to choose the digit 0, step 3 is to choose the digit 3 or one of the three letters on the same key as the digit 3, and step 4 is to choose either the digit 1 or one of the two letters on the same key as the digit 1. There are four ways to perform steps 1 and 3, one way to perform step 2, and three ways to perform step 4. So by the multiplication rule there are $4 \cdot 1 \cdot 4 \cdot 3 = 48$ different PINs that are keyed the same as 5031.

c. Constructing a numeric PIN with no repeated digit can be thought of as the following four-step process. Steps 1–4 are to choose the digits in position 1-4 (counting from the left). Because no digit may be repeated, there are 10 ways to perform step one, 9 ways to perform step two, 8 ways to perform step three, and 7 ways to perform step four. Thus the number of numeric PINs with no repeated digit is $10 \cdot 9 \cdot 8 \cdot 7 = 5040$.

18. *b.* There are 10 ways to perform step one, 22 ways to perform step two *[because we may choose any of the thirteen letters from N through Z or any of the nine digits not chosen in step 1]*, 34 ways to perform step three *[because we may not use either of the two previously used symbols]*, and 33 ways to perform step four (because we may not use any of the three previously used symbols). So the total number of PINs is $10 \cdot 22 \cdot 34 \cdot 33 = 246,840$.

20. In parts *a–c*, think of constructing a 4-digit integer as a 4-step process where step *i* is to choose the *i*th digit (counting from the left) for $i = 1, 2, 3, 4$.

a. There are 9 choices for step 1 *[because the first digit cannot be 0]*, and 10 choices for each of steps 2–4 *[because any digits can be in positions 2–4]*. So the number of integers from 1000 through 9999 is $9 \cdot 10 \cdot 10 \cdot 10 = 9000$.

(An alternative solution is to use Theorem 6.1.1 to say that the number of integers from 1000 through 9999 is $9999 - 1000 + 1 = 9000$.)

b. There are 9 choices for step 1 *[because the first digit cannot be 0]*, 10 choices for steps 2 and 3 *[because any digits can be in positions 2–3]*, and 5 choices for step 4 *[because the last digit must be 1, 3, 5, 7, or 9]*. So the number of odd integers from 1000 through 9999 is $9 \cdot 10 \cdot 10 \cdot 5 = 4500$.

c. There are 9 choices for step 1 *[because the first digit cannot be 0]*, 9 choices for step 2 *[because the digit chosen in step 1 cannot be used]*, 8 choices for step 3 *[because the digits chosen in steps 1 and 2 cannot be used]*, and and 7 choices for step 4 *[because the digits chosen in steps 1–3 cannot be used]* So the number of integers from 1000 through 9999 with distinct digits is $9 \cdot 9 \cdot 8 \cdot 7 = 4536$.

d. Think of constructing a 4-digit integer as a 4-step process where step 1 is to pick the right-most digit, step 2 is to pick the left-most digit, step 3 is to pick the second digit from the left, and step 4 is to pick the third digit from the left. There are 5 choices for step 1 *[because the right-most digit must be 1,3,5,7, or 9]*, 8 choices for the left-most digit *[because it cannot be 0 or the digit chosen to be right-most]*, 8 choices for step 3 *[because it cannot be either of the digits chosen in steps 1 and 2]*, and 7 choices for step 4 *[because it cannot be any of the digits chosen in steps 1–3]*. Thus the number of odd integers from 1000 through 9999 with distinct digits is $5 \cdot 8 \cdot 8 \cdot 7 = 2240$.

e. The probability that a randomly chosen four-digit integer has distinct digits is $4536/9000 = 50.4\%$. The probability that a randomly chosen four-digit integer has distinct digits and is odd is $2240/9000 \cong 24.9\%$.

22. *mn*

23. *mnp*

25. $(b - a + 1)(d - c + 1)$

26. Use five digits to represent each number from 1 through 99,999 by adding leading 0's as necessary. Constructing a five-digit number can then be thought of as placing five digits into five adjacent positions. Imagine constructing a number containing one each of the digits 2, 3, 4, and 5 as the following five-step process: Step one is to choose a position for the 2, step two is to choose a position for the 3, step three is to choose a position for the 4, step four is to choose a position for the 5, and step five is to choose an unused digit to fill in the remaining position. There are 5 ways to perform step one, 4 ways to perform step two, 3 ways to perform step three, 2 ways to perform step four, and 6 ways to perform step five (because there are six digits not equal to 2, 3, 4, or 5). So there are $5 \cdot 4 \cdot 3 \cdot 2 \cdot 6 = 720$ numbers containing one each of the digits 2, 3, 4, and 5.

27. *a.* Call one of the integers r and the other s. Since r and s have no common factors, if p_i is a factor of r, then p_i is not a factor of s. So for each $i = 1, 2, \ldots, m$, either $p_i{}^{k_i}$ is a factor of r or $p_i{}^{k_i}$ is a factor of s. Thus, constructing r can be thought of as an m-step process in which step i is to decide whether $p_i{}^{k_i}$ is a factor of r or not. There are two ways to perform each step, and so the number of different possible r's is 2^m. Observe that once r is specified, s is completely determined because $s = n/r$. Hence the number of ways n can be written as a product of two positive integers rs which have no common factors is 2^m. Note that this analysis assumes that order matters because, for instance, $r = 1$ and $s = n$ will be counted separately from $r = n$ and $s = 1$.

b. Each time that we can write n as rs, where r and s have no common factors, we can also write $n = sr$. So if order matters, there are twice as many ways to write n as a product of two integers with no common factors as there are if order does not matter. Thus if order does not matter, there are $2^m/2 = 2^{m-1}$ ways to write n as a product of two integers with no common factors.

28. *c.* A divisor of $p^a q^b r^c$ is any one of the $(a+1)(b+1)$ divisors of $p^a q^b$ counted in part (b) times any one of the $c+1$ numbers $1, r, r^2, \ldots, r^c$. So by the multiplication rule, there are $(a+1)(b+1)(c+1)$ divisors in all.

d. By the multiplication rule, the answer is $(a_1+1)(a_2+1)(a_3+1)\cdots(a_m+1)$. (A full formal proof would use mathematical induction.)

e. Let n be the smallest positive integer with exactly 12 divisors, and suppose $n = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$, where all the p_i are prime numbers with $p_1 < p_2 < \cdots < p_m$ and where all the a_i are integers with $a_i \geq 1$. By the result of part (d), $12 = (a_1+1)(a_2+1)(a_3+1)\cdots(a_m+1)$. Then each $(a_i+1) \geq 2$, and so, because the prime factorization of 12 is $12 = 2^2 \cdot 3$, $m \leq 3$.

In case $m = 1$, then $a_1 = 11$ and $n = p_1^{11} \geq 2^{11} = 2048$.

In case $m = 2$, then because $12 = 3 \cdot 4 = 2 \cdot 6$, either $a_1 = 3$ and $a_2 = 2$, in which case $n = p_1^3 p_2^2 \geq 2^3 3^2 = 8 \cdot 9 = 72$, or $a_1 = 5$ and $a_2 = 1$, in which case $n = p_1^5 p_2^1 \geq 2^5 3^1 = 32 \cdot 3 = 96$.

In case $m = 3$, then because $12 = 3 \cdot 2 \cdot 2$, $a_1 = 2$, $a_2 = 1$, and $a_3 = 1$, and $n = p_1^2 p_2^1 p_3^1 \geq 2^2 3^1 5^1 = 4 \cdot 3 \cdot 5 = 60$.

Therefore, the smallest positive integer with exactly 12 divisors is 60.

Because $12 = 2 \cdot 2 \cdot 3 = 4 \cdot 3 = 6 \cdot 2$, by part (d) the possibilities are $a_1 = 1$, $a_2 = 1$, and $a_3 = 2$ (of which the smallest example is $2^2 \cdot 3^1 \cdot 5^1 = 60$), or $a_1 = 3$, $a_2 = 2$ (of which the smallest example is $2^3 \cdot 3^2 = 72$), or $a_1 = 5$, $a_2 = 1$ (of which the smallest example is $2^5 \cdot 3^1 = 96$). The smallest of the numbers obtained is 60, and so the answer is 60. (The twelve divisors of 60 are 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, and 60.)

29. *c.* Because the letters GOR remain together as an ordered unit, there are 7 items that can be arranged in order: A, L, GOR, I, T, H, and M. Thus the number of arrangements is $7! = 5040$.

30. *a.* The number of ways the 6 people can be seated equals the number or permutations of a set of 6 elements, namely, $6! = 720$.

b. Assuming that the row is bounded by two aisles, the answer is $2 \cdot 5! = 240$. Under this assumption, arranging the people in the row can be regarded as a 2-step process where step 1 is to choose the aisle seat for the doctor *[there are 2 ways to do this]* and step 2 is to choose an ordering for the remaining people *[there are 5! ways to do this]*. (If it is assumed that one end of the row is against a wall, then there is only one aisle seat and the answer is $5! = 120$.)

c. Each married couple can be regarded as a single item, so the number of ways to order the 3 couples is $3! = 6$.

33. *stu, stv, sut, suv, svt, svu, tsu, tsv, tus, tuv, tvs, tvu, ust, usv, uts, utv, uvs, uvt, vst, vsu, vts, vtu, vus, vut*

34. *b.* $P(6,6) = 6!/(6-6)! = 6!/0! = 6!/1 = 720$

c. $P(6,3) = 6!/(6-3)! = 6!/3! = 6 \cdot 5 \cdot 4 = 120$

d. $P(6,1) = 6!/(6-1)! = 6!/5! = 6$

35. *b.* $P(8,2) = 8!/(8-2)! = 8!/6! = 8 \cdot 7 = 56$

36. *b.* $P(9,6) = 9!/(9-6)! = 9!/3! = 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 = 60,480$

    d. $P(7,4) = 7!/(7-4)! = 7!/3! = 7 \cdot 6 \cdot 5 \cdot 4 = 840$

37. *Proof 1*: Let n be any integer such that $n \geq 2$. By the first version of the formula in Theorem 6.2.3,
$$P(n+1,3) = \frac{(n+1)!}{((n+1)-3)!} = \frac{(n+1)n(n-1)(n-2)!}{(n-2)!} = n^3 - n.$$

Proof 2: Let n be any integer such that $n \geq 2$. By the second version of the formula in Theorem 6.2.3,
$$P(n+1,3) = (n+1)(n)\cdots((n+1)-3+1) = (n+1)(n)(n-1) = n^3 - n.$$

39. *Proof 1*: Let n be any integer such that $n \geq 3$. By the first version of the formula in Theorem 6.2.3,

$$
\begin{aligned}
P(n+1,3) - P(n,3) &= \frac{(n+1)!}{((n+1)-3)!} - \frac{n!}{(n-3)!} \\[2mm]
&= \frac{(n+1)!}{(n-2)!} - \frac{n!}{(n-3)!} \\[2mm]
&= \frac{(n+1) \cdot n!}{(n-2)!} - \frac{(n-2) \cdot n!}{(n-2) \cdot (n-3)!} \\[2mm]
&= \frac{n!((n+1)-(n-2))}{(n-2)!} \\[2mm]
&= \frac{n!}{(n-2)!} \cdot 3 \\[2mm]
&= 3P(n,2).
\end{aligned}
$$

Proof 2: Let n be any integer such that $n \geq 3$. By the second version of the formula in Theorem 6.2.3,

$$
\begin{aligned}
P(n+1,3) - P(n,3) &= (n+1)n(n-1) - n(n-1)(n-2) \\[2mm]
&= n(n-1)[(n+1)-(n-2)] \\[2mm]
&= n(n-1)(n+1-n+2) \\[2mm]
&= 3n(n-1) \\[2mm]
&= 3P(n,2).
\end{aligned}
$$

40. *Proof*: Let n be any integer such that $n \geq 2$. By Theorem 6.2.3,
$$P(n,n) = \frac{n!}{(n-n)!} = \frac{n!}{0!} = \frac{n!}{1} = n!.$$

On the other hand,
$$P(n,n-1) = \frac{n!}{(n-(n-1))!} = \frac{n!}{1!} = \frac{n!}{1} = n!$$

also. Hence $P(n,n) = P(n,n-1)$.

41. *Proof*: Let the property $P(k)$ be the sentence "If an operation consists of k steps and the first step can be performed in n_1 ways, the second step can be performed in n_2 ways, ..., and the kth step can be performed in n_k ways, then the entire operation can be performed in $n_1 n_2 \cdots n_k$ ways." We will show that the property is true for $k = 1$ and then use mathematical induction to show that that the property is true for all integers $k \geq 2$.

Show that the property is true for $k = 1$: If an operation consists of one step that can be performed in n_1 ways, then the entire operation can be performed in n_1 ways.

Show that the property is true for $k = 2$: Suppose an operation consists of two steps and the first step can be performed in n_1 ways and the second step can be performed in n_2 ways. Each of the n_1 ways of performing the first step can be paired with one of the n_2 ways of performing the second step. Thus the total number of ways to perform the entire operation is $\underbrace{n_2 + n_2 + \cdots + n_2}_{n_1 \text{ terms}}$, which equals $n_1 n_2$.

Show that for all integers $i \geq 2$, if the property is true for $k = i$ then it is true for $k = i + 1$: Let i be an integer such that $i \geq 2$ and suppose that $P(i)$ is true. *[This is the inductive hypothesis.]* Consider an operation that consists of $i + 1$ steps where the first step can be performed in n_1 ways, the second step can be performed in n_2 ways, ..., the ith step can be performed in n_i ways, and the $(i + 1)$st step can be performed in n_{i+1} ways. This operation can be regarded as a two-step operation in which the first step is an i-step operation that consists of the original first i steps and the second step is the original $(i + 1)st$ step. By inductive hypothesis, the first step of the operation can be performed in $n_1 n_2 \cdots n_i$ ways and by assumption the second step can be performed in n_{i+1} ways. Therefore, by the same argument used to establish the case $k = 2$ above, the entire operation can be performed in $(n_1 n_2 \cdots n_i) n_{i+1} = n_1 n_2 \cdots n_i n_{i+1}$ ways. *[This is what was to be shown.]*

42. *Proof*: For each integer $n \geq 1$, let the property $P(n)$ be the sentence "The number of permutations of a set with n elements is $n!$." We will prove by mathematical induction that the property is true for all integers $n \geq 1$.

Show that the property is true for $n = 1$: If a set consists of one element there is just one way to order it, and $1! = 1$.

Show that for all integers $k \geq 1$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let k be an integer with $k \geq 1$ and suppose that the number of permutations of a set with k elements is $k!$. *[This is the inductive hypothesis.]* Let X be a set with $k + 1$ elements. The process of forming a permutation of the elements of X can be considered a two-step operation where step 1 is to choose the element to write first and step 2 is to write the remaining elements of X in some order. Since X has $k + 1$ elements, there are $k + 1$ ways to perform step 1, and by inductive hypothesis there are $k!$ ways to perform step 2. Hence by the product rule there are $(k + 1)k! = (k + 1)!$ ways to form a permutation of the elements of X. But this means that there are $(k + 1)!$ permutations of X *[as was to be shown]*.

43. *Proof*: Let n be any integer with $n \geq 1$, and let the property $P(r)$ be the equation $P(n, r) = n!/(n - r)!$. We will prove by mathematical induction that the property is true for all integers r with $1 \leq r \leq n$.

Show that the property is true for $r = 1$: For $r = 1$, $P(n, r)$ is the number of 1-permutations of a set with n elements which equals n because there are n ways to place one element from a set with n elements into one position. But when $r = 1$, $n!/(n - r)! = n!/(n - 1)! = n$ also. Hence the formula holds for $r = 1$.

Show that for all integers $1 \leq k \leq n - 1$, if the property is true for $r = k$ then it is true for $r = k + 1$: Let k be an integer with $1 \leq k \leq n - 1$ and suppose $P(n, k) = \dfrac{n!}{(n - k)!}$. *[We must show that $P(n, k+1) = \dfrac{n!}{(n - (k + 1))!}$.]* Consider the process of forming a $(k + 1)$-permutation of a set X of n elements. This process can be thought of as a two-step

operation as follows: Imagine $k+1$ positions spread out in a row. Step 1 is to place k elements from X into the left-most k positions and step 2 is to place one element into the right-most position. By inductive hypothesis, there are $n!/(n-k)!$ ways to perform step 1. After step 1 has been performed there are $n-k$ elements left to choose from to place in the $(k+1)$st position. It follows that there are $n-k$ ways to perform step 2. Thus by Theorem 6.2.1, there are $\dfrac{n!}{(n-k)!} \cdot (n-k)$ ways to perform the entire operation, or, in other words, to form a $(k+1)$-permutation of X. But

$$\frac{n!}{(n-k)!} \cdot (n-k) = \frac{n!(n-k)}{(n-k)(n-k-1)!} = \frac{n!}{(n-k-1)!} = \frac{n!}{(n-(k+1))!}.$$

Thus the number of $(k+1)$-permutations of X equals $n!/(n-(k+1))!$, or, equivalently, $P(n, k+1) = \dfrac{n!}{(n-(k+1))!}$ *[as was to be shown]*.

Section 6.3

2. *a.* $16 + 16^2 + 16^3 = 4,368$

   b. $16^2 + 16^3 + 16^4 + 16^5 = 1,118,464$

5. *a.* Such integers must end in a 0 or a 5. Therefore, the answer is $9 \cdot 10 \cdot 10 \cdot 10 \cdot 2 = 18,000$.

   b. The total number of five-digit integers is $99999 - 10000 + 1 = 90000$. By part (a), 18,000 of these are divisible by 5. So the probability that a randomly chosen five-digit integer is divisible by 5 is $18000/90000 = 1/5 = 20\%$.

7. *Solution 1*: As indicated in the problem statement, certain numbers are equal and should therefore not be counted twice. For instance, $001.90 = 1.9 = 1.90$ and so forth.

   Numbers that consist of one significant digit: Excluding zero, there are 9 such numbers that have the form "x." and 9 that have the form ".x". Thus, including zero, there are $2 \cdot 9 + 1 = 19$ such numbers.

   Numbers that consist of two significant digits: There are $9 \cdot 10$ such numbers of the form "xx.", $9 \cdot 9$ such numbers of the form $x.x$, and $10 \cdot 9$ such numbers of the form ".xx". Thus there are $90 + 81 + 90 = 261$ such numbers in all.

   Numbers that consist of three significant digits: There are $9 \cdot 10^2$ such numbers of the form "xxx.", $9 \cdot 10 \cdot 9$ such numbers of the form "$xx.x$", $9 \cdot 10 \cdot 9$ such numbers of the form "$x.xx$" and $10^2 \cdot 9$ such numbers of the form ".xxx". Thus there are $2 \cdot 900 + 2 \cdot 810 = 3420$ such numbers in all.

   Similar analysis shows that there are $2 \cdot 9 \cdot 10^3 + 3 \cdot 9^2 \cdot 10^2 = 42,300$ such numbers with four significant digits, $2 \cdot 9 \cdot 10^4 + 4 \cdot 9^2 \cdot 10^3 = 504,000$ such numbers with five significant digits, $2 \cdot 9 \cdot 10^5 + 5 \cdot 9^2 \cdot 10^4 = 5,850,000$ such numbers with six significant digits, $2 \cdot 9 \cdot 10^6 + 6 \cdot 9^2 \cdot 10^5 = 66,600,000$ such numbers with seven significant digits, and $2 \cdot 9 \cdot 10^7 + 7 \cdot 9^2 \cdot 10^6 = 747,000,000$ such numbers with eight significant digits. Adding gives that there are 820,000,000 distinct numbers that can be displayed. Note that if the calculator has a $\pm$ indicator, the total is $2 \cdot 820000000 - 1 = 1,639,999,999$ (so as not to count zero twice).

   Solution 2 [with thanks to a student of Norton Starr at Amherst College]: Note that there are 99,999,999 distinct positive integers that can be represented on the calculator described in the exercise, 99,999,999 distinct negative integers, and zero. Thus the total number of distinct integers that can be represented on the calculator is $99,999,999 + 99,999,999 + 1 = 199,999,999$. Note also that a number that is not an integer has a left-most or an interior decimal point, and to count only distinct such numbers, trailing 0's should be ignored (because,

for example, $12.90 = 12.9 = 12.900$ and so forth). Thus we may assume that the right-most digit of any such number is not zero. Hence constructing a number that is not an integer can be regarded as a process of filling in 10 positions in the calculator display: first the left-most (which is either blank or contains a minus sign), second the right-most position (which is a nonzero digit), and finally the middle eight positions (seven of which are digits and one of which is a decimal point). So step 1 is to choose whether the left-most position will be blank or have a minus sign, step 2 is to choose one of the 9 nonzero digits for the right-most position, step 3 is to choose one of 8 positions for the decimal point, and each of steps 4-10 is to choose one of 10 digits to place into the empty positions, moving from left to right along the display. Therefore there are $2 \cdot 9 \cdot 8 \cdot 10^7 = 1,440,000,000$ numbers that are not integers and that can be represented on the display, and hence, by the addition rule, there are $199,999,999 + 1,440,000,000 = 1,639,999,999$ distinct numbers that can be represented.

8. *b.* On the ith iteration of the outer loop, there are i iterations of the inner loop, and this is true for each $i = 1, 2, \ldots, n$. Therefore, the total number of iterations of the inner loop is $1 + 2 + 3 + \cdots + n = n(n+1)/2$.

10. *a.* The number of ways to arrange the 6 letters of the word *THEORY* in a row is $6! = 720$

   b. When the *TH* in the word *THEORY* are treated as an ordered unit, there are only 5 items to arrange, *TH, E, O, R,* and *Y.* and so there are 5! orderings. Similarly, there are 5! orderings for the symbols *HT, E, O, R,* and *Y.* Thus, by the addition rule, the total number of orderings is $5! + 5! = 120 + 120 = 240$.

13. The set of all possible identifiers may be divided into 30 non-overlapping subsets depending on the number of characters in the identifier. Constructing one of the identifies in the kth subset can be regarded as a k-step process, where each step consists in choosing a symbol for one of the characters (say, going from left to right). Because the first character must be a letter, there are 26 choices for step 1, and because subsequent letters can be letters or digits or underscores there are 37 choices for each subsequent step. By the addition rule, we add up the number of identifiers in each subset to obtain a total. But because 82 of the resulting strings cannot be used as identifiers, by the difference rule, we subtract 82 from the total to obtain the final answer. Thus we have

$$(26 + 26 \cdot 37 + 26 \cdot 37^2 + \cdots + 26 \cdot 37^{29}) - 82 = 26(1 + 37 + 37^2 + \cdots + 37^{29}) - 82$$

$$= 26 \cdot \sum_{k=0}^{29} 37^k - 82 = 26 \left(\frac{37^{30} - 1}{37 - 1} \right) - 82 \cong 8.030 \times 10^{46} \cong.$$

15. *a.* Imagine the process of constructing a string of four distinct hexadecimal digits as a 4-step operation:

   Step 1: Choose a hexadecimal digit to place into the first position in the string.

   Step 2: Choose another hexadecimal digit to place into the second position in the string.

   Step 3: Choose yet another hexadecimal digit to place into the third position in the string.

   Step 4: Choose yet another hexadecimal digit to place into the fourth position in the string.

   The total number of ways to construct the string (and hence the total number of such strings) is $16 \cdot 15 \cdot 14 \cdot 13 = 43,680$.

   b. The process of constructing an arbitrary string of four hexadecimal digits (including those in which not all the digits are distinct) can also be regarded as a 4-step operation with 16 ways to perform each step. So the total number of strings of four hexadecimal digits is $16^4 = 65,536$. Note that if not all the digits in a string are distinct, then at least one is repeated, and so by the difference rule, we may subtract the number that consist of four distinct digits from the total to obtain the number with at least one repeated digit. Thus the answer is $16^4 - 16 \cdot 15 \cdot 14 \cdot 13 = 21,856$.

c. Because there are $16^4 = 65,536$ strings of four hexadecimal digits and because, by part (b), 21,856 of these have at least one repeated digit, the probability that a randomly chosen string of four hexadecimal digits has at least one repeated digit is $21856/65536 \cong 33.3\%$.

16. *b.* *Proof*: Let A and B be events in a sample space S. By the inclusion/exclusion rule (Theorem 6.3.3), $N(A \cup B) = N(A) + N(B) - N(A \cap B)$. So by the equally likely probability formula,

$$P(A \cup B) = \frac{N(A \cup B)}{N(S)} = \frac{N(A) + N(B) - N(A \cap B)}{N(S)} = \frac{N(A)}{N(S)} + \frac{N(B)}{N(S)} - \frac{N(A \cap B)}{N(S)}$$
$$= P(A) + P(B) - P(A \cap B).$$

17. Imagine the process of constructing a combination that satisfies the given conditions as a 3-step operation: step 1 is to choose an integer from 1 through 39 to use second, step 2 is to choose an integer to use first (any integer but the one chosen to use second may be chosen), and step 3 is to choose an integer to use third (again, any integer but the one chosen to use second may be chosen). There are 39 ways to perform step 1 and 38 ways to perform steps 2 and 3. Thus the number of ways to perform the entire operation (which equals the number of possible combinations for the lock) is $39 \cdot 38 \cdot 38 = 56,316$.

18. *b.* As in part (a), represent each integer from 1 through 99,999 as a string of five digits. The number of integers from 1 through 99,999 that do not contain the digit 6 is $9^5 - 1$ because there are 9 choices of digit for each of the five positions (namely, all ten digits except 6), except that 000000 is excluded. In addition, 100,000 does not contain the digit 6. So there are $(9^5 - 1) + 1 = 9^5$ integers from 1 through 100,000 that do not contain the digit 6. Therefore, by the difference rule, there are $100,000 - 9^5 = 40,951$ integers from 1 through 100,000 that contain at least one occurrence of the digit 6.

c. By parts (a) and (b) and the difference rule, the number of integers from 1 through 100,000 that contain two or more occurrences of the digit 6 is the difference between the number that contain at least one occurrence and the number that contain exactly one occurrence, namely, $40,951 - 32,805 = 8146$. Since there are 100,000 integers from 1 through 100,000, the probability that a randomly chosen integer in this range contains two or more occurrences of the digit 6 is $8146/100000 = 8.146\%$.

19. Call the employees U, V, W, X, Y, and Z, and suppose that U and V are the married couple. Let A be the event that U and V have adjacent desks. Since the desks of U and V can be adjacent either in the order UV or in the order VU, the number of desk assignments with U and V adjacent is the same as the sum of the number of permutations of the symbols $\boxed{UV}$, W, X, Y, Z plus the number of permutations of the symbols $\boxed{VU}$, W, X, Y, Z. By the multiplication rule each of these is $5!$, and so by the addition rule the sum is $2 \cdot 5!$. Since the total number of permutations of U, V, W, X, Y, Z is $6!$, $P(A) = 2 \cdot 5!/6! = 2/6 = 1/3$. Hence by the formula for the probability of the complement of an event, $P(A^c) = 1 - P(A) = 1 - 1/3 = 2/3$. So the probability that the married couple have nonadjacent desks is $2/3$.

20. *a.* By the multiplication rule, the number of strings of length n over $\{a, b, c, d\}$ with no two adjacent characters the same is $4 \cdot \underbrace{3 \cdot 3 \cdots 3}_{n-1} = 4 \cdot 3^{n-1}$ because any of the four letters may be chosen for the first character and for each subsequent character any letter except the one directly to its left may be chosen. The total number of strings over $\{a, b, c, d\}$ of length n is 4^n, and so by the difference rule the number of such strings with at least two adjacent characters the same is $4^n - 4 \cdot 3^{n-1}$.

b. The probability is $\dfrac{4^{10} - 4 \cdot 3^9}{4^{10}} = 1 - \left(\dfrac{3}{4}\right)^9 \cong 92.5\%$.

21. *b.* By part (a) and the equally likely probability formula, the probability that an integer chosen at random from 1 through 1000 is a multiple of 4 or a multiple of 7 is $\dfrac{N(A \cup B)}{1000} = \dfrac{357}{1000} =$ 35.7%.

   c. By the difference rule the number of integers from 1 through 1000 that are neither multiples of 4 nor multiples of 7 is $1000 - 357 = 643$.

22. *a.* Let A and B be the sets of all integers from 1 through 1,000 that are multiples of 2 and 9 respectively. Then $N(A) = 500$ and $N(B) = 111$ (because $9 = 9 \cdot 1$ is the smallest integer in B and $999 = 9 \cdot 111$ is the largest). Also $A \cap B$ is the set of all integers from 1 through 1,000 that are multiples of 18, and $N(A \cap B) = 55$ (because $18 = 18 \cdot 1$ is the smallest integer in $A \cap B$ and $990 = 18 \cdot 55$ is the largest). It follows from the inclusion/exclusion rule that the number of integers from 1 through 1,000 that are multiples of 2 or 9 equals $N(A \cup B) = N(A) + N(B) - N(A \cup B) = 500 + 111 - 55 = 556$.

   b. The probability is $556/1000 = 55.6\%$.

   c. $1000 - 556 = 444$

23. *e.* The first 3 bits in a Class C network address are 110 and the remaining 21 bits can be any ordering of 0's and 1's. So the number of network ID's for Class C networks is $2^{21} = 2,097,152$.

   f. The first eight bits in a Class C network address go from 11000000 (which equals 192) to 11011111 (which equals 223). The second two 8-bit sections of the network address go from 00000000 (which equals 0) to 11111111 (which equals 255). The final 8 bits, which are used for individual host ID's, go from 00000001 (which equals 1) to 11111110 (which equals 254). So the dotted decimal form of a computer in a Class C network has the form $w.x.y.z$, where $192 \le w \le 223$, $0 \le x \le 255$, $0 \le y \le 255$, and $1 \le z \le 254$.

   g. The host ID's for a Class C network go from 1 to 254, so there can be 254 hosts in a Class C network.

   h. If the first of the four numbers in the dotted decimal form of an IP address is between 1 and 126 inclusive, the network is Class A. If the first number is between 128 and 191, the network is Class B. If the first number is between 192 and 223, the network is Class C.

   j. Because $192 \le 202 \le 223$, the IP address comes from a Class C network.

25. Given a group of n people, imagine them lined up alphabetically by name. Assuming that each year has 365 days, the number of assignments of birthdays to individual people with repetition allowed is 365^n *[because any one of 365 birthdays can be assigned to each position in the line]*, and the number of assignments of birthdays to individual people without repetition is $365 \cdot 364 \cdot 363 \cdots (365 - n + 1)$. Assuming that all birthdays are equally likely, each of the 365^n assignments of birthdays to individual people is as likely as any other. So the probability that no two people have the same birthday is $\dfrac{365 \cdot 364 \cdot 363 \cdot \ldots \cdot (365 - n + 1)}{365^n}$, and thus by the formula for the probability of the complement of an event, the probability that at least two people have the same birthday is $p = 1 - \left(\dfrac{365 \cdot 364 \cdot 363 \cdot \ldots \cdot (365 - n + 1)}{365^n} \right)$. If $n = 22$, then $p \cong 1 - .5243 = .4757 < 1/2$, and if $n = 23$, then $p \cong 1 - .4927 = .5073 \ge 1/2$. Moreover, the greater n is, the greater the probability that two people in a group of n will have the same birthday. Therefore n must be 23 (or more) in order for the probability to be at least 50% that two or more people in the group have the same birthday.

26. $N(T) = 28$, $N(N) = 26$, $N(U) = 14$, $N(T \cap N) = 8$, $N(T \cap U) = 4$, $N(N \cap U) = 3$, $N(T \cap N \cap U) = 2$.

   a. $N(T \cup N \cup U) = N(T) + N(N) + N(U) - N(T \cap N) - N(T \cap U) - N(N \cap U) + N(T \cap N \cap U) = 28 + 26 + 14 - 8 - 4 - 3 + 2 = 55$

   b. $N((T \cup N \cup U)^c) = 100 - N(T \cup N \cup U) = 100 - 55 = 45$

c.

Sample of Students

T, 18, 6, 17, N, 2, 1, 2, 9, U
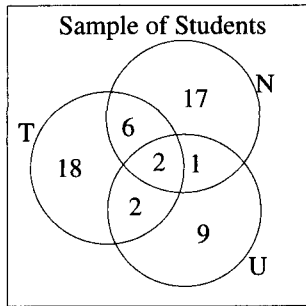
e. 1   *f.* 17

27. Let **A**, **B**, and **C** be the sets of all people who reported relief from drugs *A*, *B*, and *C* respectively. Then $N(\mathbf{A}) = 21$, $N(\mathbf{B}) = 21$, $N(\mathbf{C}) = 31$, $N(\mathbf{A} \cap \mathbf{B}) = 9$, $N(\mathbf{A} \cap \mathbf{C}) = 14$, $N(\mathbf{B} \cap \mathbf{C}) = 15$, and $N(\mathbf{A} \cup \mathbf{B} \cup \mathbf{C}) = 41$.

a. $N((\mathbf{A} \cup \mathbf{B} \cup \mathbf{C})^c) = 50 - N(\mathbf{A} \cup \mathbf{B} \cup \mathbf{C}) = 50 - 41 = 9$

b. $N(\mathbf{A} \cap \mathbf{B} \cap \mathbf{C}) = N(\mathbf{A} \cup \mathbf{B} \cup \mathbf{C}) - N(\mathbf{A}) - N(\mathbf{B}) - N(\mathbf{C}) + N(\mathbf{A} \cap \mathbf{B}) + N(\mathbf{A} \cap \mathbf{C}) + N(\mathbf{B} \cap \mathbf{C}) = 41 - 21 - 21 - 31 + 9 + 14 + 15 = 6$

c.

Sample of Subjects

A, 4, 3, 3, B, 6, 9, 8, 9, 8, C
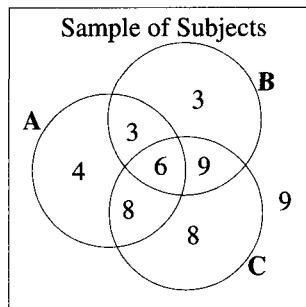
d. Solution 1: From the picture in part (c), it is clear that the number who got relief from *A* only is 4.

Solution 2: Because $(\mathbf{A} \cap \mathbf{B}) \cup (\mathbf{A} \cap \mathbf{C}) = \mathbf{A}$ and $(\mathbf{A} \cap \mathbf{B}) \cap (\mathbf{A} \cap \mathbf{C}) = \mathbf{A} \cap \mathbf{B} \cap \mathbf{C}$, we may apply the inclusion/exclusion rule to **A** to obtain the result that the number who got relief from *A* only equals $N(\mathbf{A}) - N(\mathbf{A} \cap \mathbf{B}) - N(\mathbf{A} \cap \mathbf{C}) + N(\mathbf{A} \cap \mathbf{B} \cap \mathbf{C}) = 21 - 9 - 14 + 6 = 4$.

29. *a.* by the difference rule   *b.* by De Morgan's law   *c.* by the inclusion/exclusion rule

31. *Solution 1*: Let *U* be the set of all permutations of *a*, *b*, *c*, *d*, and *e*, let *A* be the set of all permutations of *a*, *b*, *c*, *d*, and *e* in which the left-most character is *a*, *b*, or *c*, and let *B* be the set of all permutations in which the right-most character is *c*, *d*, or *e*. By the formula from exercise 29, $N(A \cap B) = N(U) - (N(A^c) + N(B^c) - N(A^c \cap B^c))$. Now by the multiplication rule, $N(U) = 5! = 120$. Also the number of permutations of *a*, *b*, *c*, *d*, and *e* in which the left-most character is neither *a*, *b*, or *c* is $2 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 48$ (because only *d* or *e* may be chosen as the left-most character). And the number of permutations of *a*, *b*, *c*, *d*, and *e* in which the right-most character is neither *c*, *d*, or *e* is $2 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 48$ (because only *a* or *b* may be chosen as the right-most character — imagine choosing the right-most character first and then the four on the left one after another). Thus $N(A^c) = 2 \cdot 4! = N(B^c)$. Furthermore, $A^c \cap B^c$ is the set of permutations of *a*, *b*, *c*, *d*, and *e* in which the left-most character is neither *a*, *b*, nor *c* and the right-most character is neither *c*, *d*, nor *e*. In other words, the left-most character

is d or e and the right-most character is a or b. Imagine constructing such a permutation as a five-step process in which the first step is to choose the left-most character, the second step is to choose the right-most character, and the third through fifth steps are to choose the middle characters one after another. By the multiplication rule there are $2 \cdot 2 \cdot 3 \cdot 2 \cdot 1 = 24$ such permutations, and so $N(A^c \cap B^c) = 24$. Thus the number of permutations of $abcde$ in which the first character is a, b, or c and the last character is c, d, or e is

$$N(A \cap B) = N(U) - (N(A^c) + N(B^c) - N(A^c \cap B^c)) = 120 - (48 + 48 - 24) = 48.$$

Solution 2: An alternative solution to this exercise does not use the inclusion/exclusion rule. The number of permutations in which the first character is an a or a b and the last character is a c, d, or e is $2 \cdot 3 \cdot 3! = 36$ *[the number of choices for the first position times the number of choices for the last position times the number of ways to order the characters in the middle three positions]*. The number of permutations in which the first character is a c and the last character is a d or an e is $1 \cdot 2 \cdot 3! = 12$ *[the number of choices for the first position times the number of choices for the last position times the number of ways to order the characters in the middle three positions]*. Thus, by the addition rule, the number of permutations of $abcde$ in which the first character is a, b, or c and the last character is c, d, or e is $36 + 12 = 48$.

32. Imagine each integer from 1 through 999,999 as a string of six digits with leading 0's allowed. For each $i = 1, 2, 3$, let A_i be the set of all integers from 1 through 999,999 that do not contain the digit i. We want to compute $N(A_1{}^c \cap A_2{}^c \cap A_3{}^c)$. By De Morgan's law,

$$A_1{}^c \cap A_2{}^c \cap A_3{}^c = (A_1 \cup A_2)^c \cap A_3{}^c = (A_1 \cup A_2 \cup A_3)^c = U - (A_1 \cup A_2 \cup A_3),$$

and so by the difference rule

$$N(A_1{}^c \cap A_2{}^c \cap A_3{}^c) = N(U) - N(A_1 \cup A_2 \cup A_3).$$

By the inclusion/exclusion rule,

$N(A_1 \cup A_2 \cup A_3) = N(A_1) + N(A_2) + N(A_3) - N(A_1 \cap A_2) - N(A_1 \cap A_3) - N(A_2 \cap A_3) + N(A_1 \cap A_2 \cap A_3)$.

Now $N(A_1) = N(A_2) = N(A_3) = 9^6$ because in each case any of nine digits may be chosen for each character in the string (for A_i these are all the ten digits except i). Also each $N(A_i \cap A_j) = 8^6$ because in each case any of eight digits may be chosen for each character of the string (for $A_i \cap A_j$ these are all the ten digits except i and j). Similarly, $N(A_1 \cap A_2 \cap A_3) = 7^6$ because any digit except 1, 2, and 3 may be chosen for each character in the string. Thus

$$N(A_1 \cup A_2 \cup A_3) = 3 \cdot 9^6 - 3 \cdot 8^6 + 7^6,$$

and so

$$N(A_1{}^c \cap A_2{}^c \cap A_3{}^c) = N(U) - N(A_1 \cup A_2 \cup A_3) = 10^6 - (3 \cdot 9^6 - 3 \cdot 8^6 + 7^6) = 74,460.$$

33. *Proof (by mathematical induction)*: Let $P(k)$ be the property "If a finite set A equals the union of k distinct mutually disjoint subsets $A_1, A_2, \ldots, A_k$, then $N(A) = N(A_1) + N(A_2) + \cdots + N(A_k)$."

Show that the property is true for $k = 1$: Suppose a finite set A equals the "union" of one subset A_1, then $A = A_1$, and so $N(A) = N(A_1)$.

Show that for all integers $i \geq 1$, if the property is true for $k = i$ then it is true for $k = i + 1$: Let i be an integer with $i \geq 1$ and suppose the property is true for $n = i$. *[This is the inductive hypothesis.]* Let A be a finite set that equals the union of $i + 1$ distinct mutually disjoint subsets $A_1, A_2, \ldots, A_{i+1}$. Then $A = A_1 \cup A_2 \cup \cdots \cup A_{i+1}$ and $A_i \cap A_j = \emptyset$ for all integers i and j with $i \neq j$. Let B be the set $A_1 \cup A_2 \cup \cdots \cup A_i$. Then $A = B \cup A_{i+1}$ and $B \cap A_{i+1} = \emptyset$. *[For if $x \in B \cap A_{i+1}$, then $x \in A_1 \cup A_2 \cup \cdots \cup A_i$ and $x \in A_{i+1}$, which*

implies that $x \in A_j$, for some j with $1 \le j \le i$, and $x \in A_{i+1}$. But A_j and A_i are disjoint. Thus no such x exists.] Hence A is the union of the two mutually disjoint sets B and A_{i+1}. Since B and A_{i+1} have no elements in common, the total number of elements in $B \cup A_{i+1}$ can be obtained by first counting the elements in B, next counting the elements in A_{i+1}, and then adding the two numbers together. It follows that $N(B \cup A_{i+1}) = N(B) + N(A_{i+1})$ which equals $N(A_1) + N(A_2) + \cdots + N(A_i) + N(A_{i+1})$ by inductive hypothesis. Hence $P(i+1)$ is true *[as was to be shown]*.

34. *Proof*: Let A and B be sets. We first show that $A \cup B$ can be partitioned into $A - (A \cap B)$, $B - (A \cap B)$, and $A \cap B$.

1. $A \cup B \subseteq (A - (A \cap B)) \cup (B - (A \cap B)) \cup (A \cap B)$: Let $x \in A \cup B$. Then $x \in A$ or $x \in B$.

Case 1 ($x \in A$): Either $x \in B$ or $x \notin B$. If $x \in B$, then $x \in A \cap B$ by definition of intersection, and so by definition of union $x \in (A - (A \cap B)) \cup (B - (A \cap B)) \cup (A \cap B)$. If $x \notin B$, then $x \notin A \cap B$ either *[by definition of intersection]* and so $x \in A - (A \cap B)$. Hence by definition of union, $x \in (A - (A \cap B)) \cup (B - (A \cap B)) \cup (A \cap B)$.

Case 2 ($x \in B$): Either $x \in A$ or $x \notin A$. If $x \in A$, then $x \in A \cap B$ by definition of intersection, and so by definition of union $x \in (A - (A \cap B)) \cup (B - (A \cap B)) \cup (A \cap B)$. If $x \notin A$, then $x \notin A \cap B$ either *[by definition of intersection]* and so $x \in B - (A \cap B)$. Hence by definition of union, $x \in (A - (A \cap B)) \cup (B - (A \cap B)) \cup (A \cap B)$.

Thus in either case $x \in (A - (A \cap B)) \cup (B - (A \cap B)) \cup (A \cap B)$ *[and so $A \cup B \subseteq (A - (A \cap B)) \cup (B - (A \cap B)) \cup (A \cap B)$ by definition of subset]*.

$(A - (A \cap B)) \cup (B - (A \cap B)) \cup (A \cap B) \subseteq A \cup B$: Let $x \in (A - (A \cap B)) \cup (B - (A \cap B)) \cup (A \cap B)$. By definition of union, $x \in (A - (A \cap B))$ or $x \in (B - (A \cap B))$ or $x \in (A \cap B)$. If $x \in (A - (A \cap B))$, then by definition of set difference $x \in A$ and $x \notin A \cap B$. In particular, $x \in A$, and so by definition of union, $x \in A \cup B$. If $x \in (B - (A \cap B))$, then by definition of set difference $x \in B$ and $x \notin A \cap B$. In particular, $x \in B$, and so by definition of union, $x \in A \cup B$. If $x \in (A \cap B)$, then by definition of intersection $x \in A$ and $x \in B$. In particular, $x \in A$, and so by definition of union, $x \in A \cup B$. Hence in all cases, $x \in A \cup B$ *[and so by definition of subset $(A - (A \cap B)) \cup (B - (A \cap B)) \cup (A \cap B) \subseteq A \cup B$.]*

[Since both set containments $A \cup B \subseteq (A - (A \cap B)) \cup (B - (A \cap B)) \cup (A \cap B)$ and $(A - (A \cap B)) \cup (B - (A \cap B)) \cup (A \cap B) \subseteq A \cup B$ have been proved, $A \cup B = (A - (A \cap B)) \cup (B - (A \cap B)) \cup (A \cap B)$ by definition of set equality.]

2. The sets $(A - (A \cap B))$, $(B - (A \cap B))$, and $(A \cap B)$ are mutually disjoint because if $x \in A \cap B$ then $x \notin A - (A \cap B)$ and $x \notin B - (A \cap B)$ by definition of set difference. Next if $x \in A - (A \cap B)$, then $x \notin A \cap B$ and so $x \notin B$; consequently $x \notin B - (A \cap B)$. Finally, if $x \in B - (A \cap B)$, then $x \notin A \cap B$ and so $x \notin A$; consequently $x \notin A - (A \cap B)$.

Next we derive the inclusion/exclusion formula from this partition. Since $A \cup B$ can be partitioned into $A - (A \cap B)$, $B - (A \cap B)$, and $A \cap B$, then

$$
\begin{aligned}
N(A \cup B) &= N(A - (A \cap B)) + N(B - (A \cap B)) + N(A \cap B) \\
&\qquad \text{by the addition rule} \\
&= N(A) - N(A \cap B) + N(B) - N(A \cap B) + N(A \cap B) \\
&\qquad \text{by the difference rule and the fact} \\
&\qquad \text{that } A \cap B \text{ is a subset of both } A \text{ and } B \\
&= N(A) + N(B) - N(A \cap B) \\
&\qquad \text{by basic algebra.}
\end{aligned}
$$

Note: An alternative way to show that $A \cup B$ is the union of the three sets $A - (A \cap B)$, $B - (B \cap A)$, and $A \cap B$ begins by showing that for all sets U and V, $U = (U - (U \cap V)) \cup (U \cap V)$. It then follows that $A \cup B = [(A - (A \cap B)) \cup (A \cap B)] \cup [(B - (B \cap A)) \cup (B \cap A)] = (A - (A \cap B)) \cup (B - (B \cap A)) \cup (A \cap B)$.

35. Proof: Suppose A, B, and C are finite sets.

$$
\begin{aligned}
N(A \cup B \cup C) &= N(A \cup (B \cup C)) && \text{by the associative law for } \cup \\
&= N(A) + N(B \cup C) - N(A \cap (B \cup C)) && \text{by the inclusion/exclusion rule} \\
& && \text{for two sets} \\
&= N(A) + N(B) + N(C) - N(B \cap C) && \text{by the inclusion/exclusion rule} \\
& \quad - N(A \cap (B \cup C)) && \text{for two sets} \\
&= N(A) + N(B) + N(C) - N(B \cap C) && \\
& \quad - N((A \cap B) \cup (A \cap C)) && \text{by the distributive law for sets} \\
&= N(A) + N(B) + N(C) - N(B \cap C) && \\
& \quad - [N(A \cap B) + N(A \cap C) && \\
& \quad\quad - N((A \cap B) \cap (A \cap C))] && \text{by the inclusion/exclusion rule} \\
& && \text{for two sets} \\
&= N(A) + N(B) + N(C) - N(A \cap B) && \text{by basic algebra and because} \\
& \quad - N(A \cap C) - N(B \cap C) && (A \cap B) \cap (A \cap C) \\
& \quad + N(A \cap B \cap C) && = (A \cap A) \cap B \cap C \\
& && = A \cap B \cap C.
\end{aligned}
$$

36. *Proof (by mathematical induction):*

Show that the property is true for $n = 2$: This was proved in one way in the text preceding Theorem 6.3.3 and in another way in the solution to exercise 34.

Show that for all integers $r \geq 2$, if the property is true for $n = r$ then it is true for $n = r + 1$: Let r be an integer with $r \geq 2$, and suppose that the formula holds for any collection of r finite sets. *[This is the inductive hypothesis.]* Let $A_1, A_2, \ldots, A_{r+1}$ be finite sets. Then

$N(A_1 \cup A_2 \cup \cdots \cup A_{r+1})$

$= N(A_1 \cup (A_2 \cup A_3 \cup \cdots \cup A_{r+1}))$ by the associative law for $\cup$

$= N(A_1) + N(A_2 \cup A_3 \cup \cdots \cup A_{r+1}) - N(A_1 \cap (A_2 \cup A_3 \cup \cdots \cup A_{r+1}))$

     by the inclusion/exclusion rule for two sets

$= N(A_1) + N(A_2 \cup A_3 \cup \cdots \cup A_{r+1}) - N((A_1 \cap A_2) \cup (A_1 \cap A_3) \cup \cdots \cup (A_1 \cap A_{r+1}))$

     by the generalized distributive law for sets
     (exercise 35, Section 5.2)

$= N(A_1) + \left(\sum_{2 \leq i \leq r+1} N(A_i) - \sum_{2 \leq i < j \leq r+1} N(A_i \cap A_j) \right.$

$\quad\quad \left. + \sum_{2 \leq i < j < k \leq r+1} N(A_i \cap A_j \cap A_k) - \cdots + (-1)^{r+1} N(A_2 \cap A_3 \cap \cdots \cap A_{r+1}) \right)$

$\quad\quad - \left(\sum_{2 \leq i \leq r+1} N(A_1 \cap A_i) - \sum_{2 \leq i < j \leq r+1} N((A_1 \cap A_i) \cap (A_1 \cap A_j)) + \cdots \right.$

$\quad\quad\quad \left. + (-1)^{r+1} N((A_1 \cap A_2) \cap (A_1 \cap A_3) \cap \cdots \cap (A_1 \cap A_{r+1})) \right)$

     by inductive hypothesis

$= N(A_1) + \left(\sum_{2 \leq i \leq r+1} N(A_i) - \sum_{2 \leq i < j \leq r+1} N(A_i \cap A_j) \right.$

$\quad\quad \left. + \sum_{2 \leq i < j < k \leq r+1} N(A_i \cap A_j \cap A_k) - \cdots + (-1)^{r+1} N(A_2 \cap A_3 \cap \cdots \cap A_{r+1}) \right)$

$\quad\quad - \left(\sum_{2 \leq i \leq r+1} N(A_1 \cap A_i) - \sum_{2 \leq i < j \leq r+1} N(A_1 \cap A_i \cap A_j) + \cdots \right.$

$\quad\quad\quad \left. + (-1)^{r+1} N(A_1 \cap A_2 \cap A_3 \cap \cdots \cap A_{r+1}) \right)$

$= \sum_{1 \leq i \leq r+1} N(A_i) - \sum_{1 \leq i < j \leq r+1} N(A_i \cap A_j) + \sum_{1 \leq i < j < k \leq r+1} N(A_i \cap A_j \cap A_k)$

$\quad\quad - \cdots + (-1)^{r+2} N(A_1 \cap A_3 \cap \cdots \cap A_{r+1}).$

[This is what was to be proved.]

Section 6.4

2. *a.* The 3-combinations are $x_1x_2x_3$, $x_1x_2x_4$, $x_1x_2x_5$, $x_1x_3x_4$, $x_1x_3x_5$, $x_1x_4x_5$, $x_2x_3x_4$, $x_2x_3x_5$, $x_2x_4x_5$, $x_3x_4x_5$. Therefore, $\dbinom{5}{3} = 10$.

b. The unordered selections of two elements are x_1x_2, x_1x_3, x_1x_4, x_1x_5, x_1x_6, x_2x_3, x_2x_4, x_2x_5, x_2x_6, x_3x_4, x_3x_5, x_3x_6, x_4x_5, x_4x_6, x_5x_6. Therefore, $\dbinom{6}{2} = 15$.

4. $\dbinom{8}{3} = \dfrac{P(8,3)}{3!}$

5. *c.* $\dbinom{5}{2} = \dfrac{5!}{2!(5-2)!} = \dfrac{5!}{2! \cdot 3!} = \dfrac{5 \cdot 4 \cdot 3!}{2 \cdot 1 \cdot 3!} = 10$ *d.* $\dbinom{5}{3} = \dfrac{5!}{3!(5-3)!} = \dfrac{5 \cdot 4 \cdot 3!}{3! \cdot 2 \cdot 1} = 10$

   e. $\dbinom{5}{4} = \dfrac{5!}{4!(5-4)!} = \dfrac{5!}{4! \cdot 1!} = \dfrac{5 \cdot 4!}{4!} = 5$ *f.* $\dbinom{5}{5} = \dfrac{5!}{5!(5-5)!} = \dfrac{5!}{5! \cdot 0!} = 1$

7. *a.* $\dbinom{13}{7} = \dfrac{13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7!}{6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \cdot 7!} = 1716$

   b. (i) $\dbinom{7}{4} \cdot \dbinom{6}{3} = \dfrac{7 \cdot 6 \cdot 5 \cdot 4!}{3 \cdot 2 \cdot 1 \cdot 4!} \cdot \dfrac{6 \cdot 5 \cdot 4}{3 \cdot 2} = 700$ *[the number of subsets of four women chosen from seven women times the number of subsets of three men chosen from six men]*

   (ii) $\dbinom{13}{7} - \dbinom{7}{7} = 1716 - 1 = 1715$ *[the total number of groups minus the number that contain no men]*

   (iii) $\dbinom{7}{1}\dbinom{6}{6} + \dbinom{7}{2}\dbinom{6}{5} + \dbinom{7}{3}\dbinom{6}{4} = 7 \cdot 1 + \dfrac{7 \cdot 6 \cdot 5!}{2 \cdot 1 \cdot 5!} \cdot \dfrac{6 \cdot 5!}{1 \cdot 5!} + \dfrac{7 \cdot 6 \cdot 5 \cdot 4!}{4! \cdot 3 \cdot 2 \cdot 1} \cdot \dfrac{6 \cdot 5 \cdot 4!}{4! \cdot 2 \cdot 1} =$
   $7 + 126 + 525 = 658$ *[the number of groups with one woman and six men plus the number with two women and five men plus the number with three women and four men — there are no groups with no women because there are only six men]*

   c. $\dbinom{11}{6} + \dbinom{11}{6} + \dbinom{11}{7} = 2\left(\dfrac{11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6!}{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \cdot 6!}\right) + \left(\dfrac{11 \cdot 10 \cdot 9 \cdot 8 \cdot 7!}{4 \cdot 3 \cdot 2 \cdot 1 \cdot 7!}\right) = 924 + 330 =$
   1254 *[Let the people be A and B. The number of groups that do not contain both A and B equals the number of groups with A and six others (none B) plus the number of groups with B and six others (none A) plus the number of groups with neither A nor B.]*

   d. $\dbinom{11}{5} + \dbinom{11}{7} = 462 + 330 = 792$ *[the number of groups with both A and B and five others plus the number of groups with neither A nor B]*

8. *a.* $\dbinom{12}{10} = 66$

   b. (i) $\dbinom{5}{4} \cdot \dbinom{7}{6} = 5 \cdot 7 = 35$

   (ii) Because there are only seven questions that do not require proof, any group of ten questions contains at least three that require proof. Thus the answer is the same as for part (a):
   $\dbinom{12}{10} = 66$.

   (iii) Because there are only seven questions that do not require proof, the only groups of ten questions with three or fewer questions requiring proof are those groups with exactly three questions requiring proof. Thus the number is $\dbinom{7}{7}\dbinom{5}{3} = 1 \cdot 10 = 10$.

c. Any set of questions containing at most one of questions 1 and 2 can be split into three subsets: (1) those that contain question 1 and not 2, (2) those that contain question 2 and not 1, and (3) those that contain neither question 1 nor 2. There are $\binom{10}{9}$ choices of questions in the first set, $\binom{10}{9}$ choices of questions in the second set, and $\binom{10}{10}$ choices of questions in the third set. So there are $2 \cdot \binom{10}{9} + \binom{10}{10} = 2 \cdot 10 + 1 = 21$ choices of ten questions containing at most one of questions 1 and 2.

d. There are $\binom{10}{8}$ choices of questions that contain both questions 1 and 2, and there are $\binom{10}{10}$ choices of questions that contain neither question 1 nor 2. So by the addition rule, there are $\binom{10}{8} + \binom{10}{10} = 45 + 1 = 46$ choices of questions that contain either both questions 1 and 2 or neither question 1 nor 2.

9. *a.* $\binom{40}{6} = 3,838,380$

10. $\binom{60}{22}\binom{38}{22} = \dfrac{60!}{22!38!} \cdot \dfrac{38!}{22!16!} \cong 3.148 \times 10^{26}$

[The assignment of treatments to mice can be considered a two-step operation. Step 1 is to choose 22 mice out of the 60 to receive treatment A, step 2 is to choose 22 mice out of the remaining 38 to receive treatment B. The remaining 16 mice are the controls.]

11. *b.* (1) The number of hands with a straight flush is $4 \cdot 9 = 36$ *[the number of suits, namely 4, times the number of lowest denominated card in the straight, namely 9, because aces can be low]*

(2) probability $= \dfrac{36}{\binom{52}{5}} = \dfrac{36}{2,598,960} \cong 0.0000139$

d. (1) The number of hands with a full house is $\binom{13}{1}\binom{4}{3}\binom{12}{1}\binom{4}{2} = 3744$ *[because constructing a full house can be thought of as a four-step process where step one is to choose the denomination for the three of a kind, step two is to choose three cards out of the four of that denomination, step three is to choose the denomination for the pair, and step four is to choose two cards of that denomination].*

(2) probability $= \dfrac{3744}{\binom{52}{5}} = \dfrac{3744}{2,598,960} \cong 0.00144$

e. (1) The number of hands with a flush (including a royal or a straight flush) is $4 \cdot \binom{13}{5} = 5148$ *[the number of suits times the number of ways to pick five cards from a suit].* Forty of these are royal or straight flushes, and so there are 5108 hands with a flush.

(2) probability $= \dfrac{5108}{\binom{52}{5}} = \dfrac{5108}{2,598,960} \cong 0.00197$

g. (1) The number of hands with three of a kind is $\binom{13}{1}\binom{4}{3}\binom{12}{2}\binom{4}{1}\binom{4}{1} = 54,912$ *[the number of ways to choose the denomination for the three of a kind times the number of ways*

three cars from that denomination can be chosen times the number of ways to choose two other denominations for the other two cards times the number of ways a card can be chosen from the lower ranked of the two denominations times the number of ways a card can be chosen from the higher ranked of the two denominations].

(2) probability $= \dfrac{54912}{\dbinom{52}{5}} = \dfrac{54912}{2,598,960} \cong 0.021$

h. (1) The number of hands with one pair is $\dbinom{13}{1}\dbinom{4}{2}\dbinom{12}{3}\dbinom{4}{1}\dbinom{4}{1}\dbinom{4}{1} = 1,098,240$ *[the number of ways to choose the denomination for the pair times the number of ways two cars from that denomination can be chosen times the number of ways to choose three other denominations for the other three cards times the number of ways a card can be chosen from the lowest ranked of the three denominations times the number of ways a card can be chosen from the middle ranked of the three denominations times the number of ways a card can be chosen from the highest ranked of the three denominations].*

(2) probability $= \dfrac{1,098,240}{\dbinom{52}{5}} = \dfrac{1,098,240}{2,598,960} \cong 0.4226$

i. (1) The sum of the answers from (a)–(h) plus the answer from Example 6.4.9 (the number of poker hands with two pairs) is 1,296,420, and so by the difference rule there are $\dbinom{52}{5} - 1,296,420 = 2,598,960 - 1,296,420 = 1,302,540$ hands whose cards neither contain a repeated denomination nor five adjacent denominations.

(2) probability $= \dfrac{1,302,540}{\dbinom{52}{5}} = \dfrac{1,302,540}{2,598,960} \cong 0.5012$

The results of this exercise are summarized in the following table.

Type of Hand	Probability
royal flush	0.0000015 = 0.00015%
straight flush	0.000014 = 0.0014%
four of a kind	0.00024 = 0.024%
full house	0.00144 = 0.144%
flush	0.00197 = 0.197%
straight	0.00392 = 0.392%
three of a kind	0.02113 = 2.113%
two pairs	0.0475 = 4.75%
one pair	0.4226 = 42.26%
none of the above	0.5012 = 50.12%

12. The sum of two integers is even if, and only if, either both integers are even or both are odd *[see Example 3.2.3]*. Because $2 = 2 \cdot 1$ and $100 = 2 \cdot 50$, there are 50 even integers and thus 51 odd integers from 1 to 101 inclusive. Hence the number of distinct pairs is $\dbinom{50}{2} + \dbinom{51}{2} = 1225 + 1275 = 2500$.

13. *b.* $\dbinom{10}{5} = \dfrac{10 \cdot 9 \cdot 8 \cdot 7 \cdot 5 \cdot 5!}{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \cdot 5!} = 252$

c. $\dbinom{10}{8} + \dbinom{10}{9} + \dbinom{10}{10} = 45 + 10 + 1 = 56$

e. $\dbinom{10}{0} + \dbinom{10}{1} = 1 + 10 = 11$

14. $a.$ $\dbinom{16}{7} = \dfrac{16 \cdot 15 \cdot 14 \cdot 13 \cdot 12 \cdot 11 \cdot 10 \cdot 9!}{9! \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} = 11,440$

$b.$ $\dbinom{16}{13} + \dbinom{16}{14} + \dbinom{16}{15} + \dbinom{16}{16} = \dfrac{16 \cdot 15 \cdot 14 \cdot 13!}{13! \cdot 3 \cdot 2 \cdot 1} + \dfrac{16 \cdot 15 \cdot 14!}{14! \cdot 2 \cdot 1} + \dfrac{16 \cdot 15!}{15! \cdot 1} + \dfrac{16!}{16! \cdot 1} =$
$560 + 120 + 16 + 1 = 697$

$c.$ $2^{16} - 1 = 65,535$ $d.$ $\dbinom{16}{0} + \dbinom{16}{1} = 1 + 16 = 17$

16. $a.$ $\dbinom{40}{5} = 658,008$

$b.$ $Solution\ 1$: $\dbinom{40}{5} - \dbinom{37}{5} = 658008 - 435897 = 222,111$ *[The number of samples with at least one defective equals the total number of samples minus the number with no defectives.]*

$Solution\ 2$: $\dbinom{37}{4}\dbinom{3}{1} + \dbinom{37}{3}\dbinom{3}{2} + \dbinom{37}{2}\dbinom{3}{3} = 198135 + 23310 + 666 = 222,111$ *[The number of samples with at least one defective equals the number with one defective plus the number with two defectives plus the number with three defectives.]*

$c.$ probability $= \frac{222111}{658008} \cong 0.337550 \cong 33.8\%$

17. $b.$ $\dbinom{9}{2} = \dfrac{9 \cdot 8}{2} = 36$ $c.$ $\dbinom{10}{3} = \dfrac{10 \cdot 9 \cdot 8}{3 \cdot 2} = 120$ $d.$ $\dbinom{9}{3} = \dfrac{9 \cdot 8 \cdot 7}{3 \cdot 2} = 84$

18. $\dbinom{11}{1}\dbinom{10}{4}\dbinom{6}{4}\dbinom{2}{2} = \dfrac{11!}{1! \cdot 10!} \cdot \dfrac{10!}{4! \cdot 6!} \cdot \dfrac{6!}{4! \cdot 2!} \cdot \dfrac{2!}{2! \cdot 0!} = \dfrac{11!}{1! \cdot 4! \cdot 4! \cdot 2!} = 34,650$ *[which agrees with the result in Example 6.4.11]*

20. $a.$ $\dbinom{11}{2}\dbinom{9}{3}\dbinom{6}{2}\dbinom{4}{1}\dbinom{3}{1}\dbinom{2}{1}\dbinom{1}{1} = 55 \cdot 84 \cdot 15 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 1,663,200.$

[The word MILLIMICRON has 2 M's, 3 I's, 2 L's, 1 C, 1R, 1O, and 1 N. To construct an ordering of the letters, choose 2 positions for the M's, then 3 positions for the I's, then 2 positions for the L's, then 1 position for the C, 1 position for the R, 1 for the O, and 1 for the N. If the groups of letters are chosen in a different order, the same answer is obtained.]

Note also that one could use the formula
$\dbinom{11}{2}\dbinom{9}{3}\dbinom{6}{2}\dbinom{4}{1}\dbinom{3}{1}\dbinom{2}{1}\dbinom{1}{1} = \dfrac{11!}{2! \cdot 3! \cdot 2! \cdot 1! \cdot 1! \cdot 1! \cdot 1!} = 1,663,200$

$b.$ $\dbinom{9}{1}\dbinom{8}{3}\dbinom{5}{2}\dbinom{3}{1}\dbinom{2}{1}\dbinom{1}{1} = 9 \cdot 56 \cdot 10 \cdot 3 \cdot 2 \cdot 1 = 30,240 \ (= \dfrac{9!}{1! \cdot 3! \cdot 2! \cdot 1! \cdot 1! \cdot 1!})$

[Once the M and the N have been fixed, there are 9 positions left to fill in.]

$c.$ $\dbinom{9}{1}\dbinom{8}{1}\dbinom{7}{2}\dbinom{5}{3}\dbinom{2}{2} = 9 \cdot 8 \cdot 21 \cdot 10 \cdot 1 = 15,120 \ (= \dfrac{9!}{1! \cdot 1! \cdot 2! \cdot 3! \cdot 2!})$

[There are 9 symbol groups to arrange in order: 1 CR, 1 ON, 2 M's, 3 I's, and 2 L's.]

21. $c.$ There are as many strings of length 4 with 2 a's and 2 b's as there are ways to choose 2 positions out of 4 into which to place the a's. Thus the answer is $\dbinom{4}{2} = \dfrac{4 \cdot 3}{2 \cdot 1} = 6$.
[Alternatively, one could think of choosing 2 positions (out of 4) for the a's and then 2 positions (out of the remaining 2) for the b's, and write the answer as $\dbinom{4}{2}\dbinom{2}{2} = 6$.]

22. $2 + 2^2 + 2^3 + 2^4 + 2^5 + 2^6 + 2^7 = 2(1 + 2 + 2^2 + 2^3 + 2^4 + 2^5 + 2^6) = 2\left(\dfrac{2^7 - 1}{2 - 1}\right) = 254$

23. $\binom{6}{1} + \binom{6}{2} + \binom{6}{3} + \binom{6}{4} + \binom{6}{5} + \binom{6}{6} = 6 + 15 + 20 + 15 + 6 + 1 = 63$

25. *a.* $210 = 2 \cdot 3 \cdot 5 \cdot 7$, distinct factorizations: $1 \cdot 210, \ 2 \cdot 105, \ 3 \cdot 70, \ 5 \cdot 42, \ 7 \cdot 30, \ 6 \cdot 35, 10 \cdot 21, 14 \cdot 15$, answer $= 8$

    c. As in the answer to part (b), there are two apparently different ways to look at the solution to this problem.

    Solution 1: Separate the factorizations into categories: one category consists only of the factorization in which one factor is 1 and the other factor is all five given primes *[there is* $1 = \binom{5}{0}$ *such factorization]*, a second category consists of those factorizations in which one factor is a single prime and the other factor is a product of the four other primes *[there are* $\binom{5}{1}$ *such factorizations]*, and the third category contains those factorizations in which one factor is a product of two of the primes and the other factor is a product of the other three primes *[there are* $\binom{5}{2}$ *such factorizations]*. All possible factorizations are included among these categories, and so the answer is $\binom{5}{0} + \binom{5}{1} + \binom{5}{2} = 1 + 5 + 10 = 16$.

    Solution 2: Let $S = \{p_1, p_2, p_3, p_4, p_5\}$, let $p_1 p_2 p_3 p_4 p_5 = P$, and let $f_1 f_2$ be any factorization of P. The product of the numbers in any subset $A \subseteq S$ can be used for f_1, with the product of the numbers in A^c being f_2.. Thus there are as many ways to write $f_1 f_2$ as there are subsets of S, namely $2^5 = 32$ (by Theorem 5.3.1). But given any factors f_1 and f_2, we have that $f_1 f_2 = f_2 f_1$. Thus counting the number of ways to write $f_1 f_2$ counts each factorization twice. So the answer is $\dfrac{32}{2} = 16$.

    Note: In Section 6.6 we will show that $\binom{n}{r} = \binom{n}{n-r}$ whenever $n \geq r \geq 0$. Thus, for example, the answer can be written as $\binom{5}{0} + \binom{5}{1} + \binom{5}{2} = \frac{1}{2}\left(\binom{5}{0} + \binom{5}{1} + \binom{5}{2} + \binom{5}{3} + \binom{5}{4} + \binom{5}{5}\right)$. In Section 6.7 we will show that for all integers $n \geq 0$, $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n-2} + \binom{n}{n-1} + \binom{n}{n} = 2^n$, and so, in particular, $\frac{1}{2}\left(\binom{5}{0} + \binom{5}{1} + \binom{5}{2} + \binom{5}{3} + \binom{5}{4} + \binom{5}{5}\right) = \frac{1}{2} \cdot 2^5 = \frac{32}{2} = 16$. These facts illustrate the relationship between the two solutions to this part of the exercise.

    d. Because the second solution given in parts (b) and (c) is the simplest, we give a general version of it as the answer to this part of the exercise. Let $S = \{p_1, p_2, p_3, \ldots, p_n\}$, let $p_1 p_2 p_3 \cdots p_n = P$, and let $f_1 f_2$ be any factorization of P. The product of the numbers in any subset $A \subseteq S$ can be used for f_1, with the product of the numbers in A^c being f_2.. Thus there are as many ways to write $f_1 f_2$ as there are subsets of S, namely 2^n (by Theorem 5.3.1). But given any factors f_1 and f_2, we have that $f_1 f_2 = f_2 f_1$. Thus counting the number of ways to write $f_1 f_2$ counts each factorization twice. So the answer is $\dfrac{2^n}{2} = 2^{n-1}$.

26. The answer is the total number of committees (which equals $\binom{16}{8} = 12,870$) minus the number of committees that have no members from at least one class. Let A_1 be the set of committees with no freshmen, A_2 the set of committees with no sophomores, A_3 the set of committees with no juniors, and A_4 the set of committees with no seniors. Then the set of committees with no members from at least one class is $A_1 \cup A_2 \cup A_3 \cup A_4$. By the inclusion/exclusion rule for four sets (see exercise 36 of Section 6.3),

$$N(A_1 \cup A_2 \cup A_3 \cup A_4) = \sum_{1 \le i \le 4} N(A_i) - \sum_{1 \le i < j \le 4} N(A_i \cap A_j)$$
$$+ \sum_{1 \le i < j < k \le 4} N(A_i \cap A_j \cap A_k)$$
$$- \sum_{1 \le i < j < k < l \le 4} N(A_i \cap A_j \cap A_k \cap A_l).$$

Now $N(A_1) = \binom{13}{8}$ [because a committee that contains no freshmen has its entire membership of eight taken from the $4 + 4 + 5 = 13$ sophomores, juniors, and seniors]. Similarly, $N(A_2) = \binom{12}{8}$, $N(A_3) = \binom{12}{8}$, $N(A_4) = \binom{11}{8}$, $N(A_1 \cap A_2) = \binom{9}{8}$ [because a committee that contains no freshmen or sophomores has its entire membership of eight taken from the $4 + 5 = 9$ juniors and seniors], $N(A_1 \cap A_3) = \binom{9}{8}$, $N(A_1 \cap A_4) = \binom{8}{8}$, $N(A_2 \cap A_3) = \binom{8}{8}$, $N(A_2 \cap A_4) = 0$ [because if students from the sophomore and senior classes are taken away, not enough students remain to form a committee of eight], $N(A_3 \cap A_4) = 0$, $N(A_i \cap A_j \cap A_k) = 0$ for all possible i, j, and k [because if students from three of the classes are taken away, not enough students remain to form a committee of eight], and $N(A_1 \cap A_2 \cap A_3 \cap A_4) = 0$ [because every committee must contain students from some class]. Consequently,

$$N(A_1 \cup A_2 \cup A_3 \cup A_4) = \binom{13}{8} + \binom{12}{8} + \binom{12}{8} + \binom{11}{8} - \binom{9}{8} - \binom{9}{8} - \binom{8}{8} - \binom{8}{8}$$

$$= 1287 + 495 + 495 + 165 - 9 - 9 - 1 - 1 = 2422.$$

So the answer is $\binom{16}{8} - 2422 = 12,870 - 2422 = 10,428$.

27. Given nonnegative integers r and n with $r \le n$, $P(n, r)$ is the set of r-permutations that can be formed from a set of n elements. Partition this set of r-permutations into subsets so that all the r-permutations in each subset are permutations of the same collection of elements. For instance, if $n = 5$ and $r = 3$ and $X = \{a, b, c, d, e\}$ is a set of $n = 5$ elements, then acd, adc, cda, cad, dac, and dca are all permutations of the same collection of elements, namely $\{a, c, d\}$. Thus each subset of the partition corresponds to a subset of X of size r. Furthermore, all subsets of the partition have the same size, namely $r!$ [because there are $r!$ permutations of a set of r elements]. Hence the number of subsets of X of size r equals the number of subsets of the partition. By the division rule, this equals the number of elements in the partition divided by the number of elements in each set of the partition, or $\dfrac{P(n, r)}{r!}$.

28. The error is that the "solution" overcounts the number of poker hands with two pairs. In fact, it counts every such hand twice. For instance, consider the poker hand $\{4\clubsuit, 4\diamondsuit, J\heartsuit, J\spadesuit, 9\clubsuit\}$. If the steps outlined in the false solution in the exercise statement are followed, this hand is first counted when the denomination 4 is chosen in step one, the cards $4\clubsuit$ and $4\diamondsuit$ are chosen in step two, the denomination J is chosen in step three, the cards J $\heartsuit$ and J$\spadesuit$ are chosen in step four, and $9\clubsuit$ is chosen in step five. The hand is counted a second time when the denomination J is chosen in step one, the cards J$\heartsuit$ and J $\spadesuit$ are chosen in step two, the denomination 4 is chosen in step three, the cards $4\clubsuit$ and $4\diamondsuit$ are chosen in step four, and $9\clubsuit$ is chosen in step five.

Section 6.5

2. b. $[x, x, x, x]$, $[x, x, x, y]$, $[x, x, x, z]$, $[x, x, y, y]$, $[x, x, y, z]$, $[x, x, z, z]$, $[x, y, y, y]$, $[x, y, y, z]$, $[x, y, z, z]$, $[x, z, z, z]$, $[y, y, y, y]$, $[y, y, y, z]$, $[y, y, z, z]$, $[y, z, z, z]$, $[z, z, z, z]$

4. a. $\binom{30 + 8 - 1}{30} = \binom{37}{30} = 10,295,472$

b. $\dbinom{26+8-1}{26} = \dbinom{33}{26} = 4,272,048$

c. $\dfrac{\dbinom{33}{26}}{\dbinom{37}{30}} = \dfrac{4,272,048}{10,295,472} \cong 41.5\%$

d. $\dfrac{\dbinom{26+7-1}{26}}{\dbinom{37}{30}} = \dfrac{\dbinom{32}{26}}{\dbinom{37}{30}} = \dfrac{906192}{10,295,472} \cong 0.088 = 8.8\%$

6. $\dbinom{5+n-1}{5} = \dbinom{n+4}{5} = \dfrac{(n+4)(n+3)(n+2)(n+1)n}{120}$

7. Consider any nonnegative integral solution $x_1, x_2, \ldots, x_n$ of the equation $x_1 + x_2 + \cdots + x_n = m$. For each $i = 1, 2, \ldots n$, let $y_i = x_1 + x_2 + \cdots + x_i$. Then $0 \le y_1 \le y_2 \le \cdots \le y_n = m$. Conversely, suppose $(y_1, y_2, \ldots, y_n)$ is any n-tuple of nonnegative integers such that $0 \le y_1 \le y_2 \le \cdots \le y_n = m$, and let $x_1 = y_1$, and $x_i = y_i - y_{i-1}$ for all integers $i = 1, 2, \ldots, n$. Then $x_1 + x_2 + \cdots + x_n = y_1 + (y_2 - y_1) + (y_3 - y_2) + \cdots + (y_n - y_{n-1}) = y_n = m$, and so $x_1 + x_2 + \cdots + x_n = m$. Consequently, the number of nonnegative integral solutions of the equation $x_1 + x_2 + \cdots + x_n = m$ is the same as the number of n-tuples of nonnegative integers $(y_1, y_2, \ldots, y_n)$ such that $0 \le y_1 \le y_2 \le \cdots \le y_n = m$. Since $y_n = m$, this is the same as the number of $(n-1)$-tuples of nonnegative integers $(y_1, y_2, \ldots, y_{n-1})$ where $0 \le y_1 \le y_2 \le \cdots \le y_{n-1} \le m$. By reasoning similar to that of Example 6.5.3, this number is the same as the number of ways of placing $m+1$ objects (the integers from 0 through m) into $n-1$ categories (the elements of the $(n-1)$-tuple), which is $\dbinom{(n-1)+(m+1)-1}{n-1} = \dbinom{(n-1)+m}{n-1}$. Thus the number of nonnegative integral solutions of $x_1 + x_2 + \cdots + x_n = m$ is $\dbinom{(n-1)+m}{n-1}$. (In Section 6.6 we show that this number equals $\dbinom{(n-1)+m}{m}$, and so this result agrees with the one obtained in Example 6.5.5.

9. The number of iterations of the inner loop is the same as the number of integer triples (i, j, k) where $1 \le k \le j \le i \le n$. By reasoning similar to that of Example 6.5.3, the number of such triples is $\dbinom{n+2}{3} = \dfrac{n(n+1)(n+2)}{6}$.

12. Think of the number 30 as divided into 30 individual units and the variables (y_1, y_2, y_3, y_4) as four categories into which these units are placed. The number of units in category y_i indicates the value of y_i in a solution of the equation. By Theorem 6.5.1, the number of ways to place 30 objects into four categories is $\dbinom{30+4-1}{30} = \dbinom{33}{30} = 5456$. So there are 5456 nonnegative integral solutions of the equation.

13. The analysis for this exercise is the same as for exercise 12 except that since each $y_i \ge 2$, we can imagine taking eight of the 30 units, placing two in each category (y_1, y_2, y_3, y_4), and then distributing the remaining 22 units among the four categories. The number of ways to do this is $\dbinom{22+4-1}{22} = \dbinom{25}{22} = 2300$. So there are 2300 integral solutions of the equation where each integer in the solution is at least two.

14. By reasoning similar to that of Example 6.5.6 or exercise 13, after ten units have been placed in each category a, b, c, d, and e, 450 units remain to distribute among the five categories.

The number of ways to do this is $\binom{450 + 5 - 1}{450} = \binom{454}{450} = 1,746,858,751$. So there are $1,746,858,751$ solutions to $a + b + c + d + e = 500$ for which each of a, b, c, d, and e is at least ten.

15. *a.* Think of the 30 kinds of balloons as the n categories and the 12 balloons to be chosen as the r objects. Each choice of 12 balloons is represented by a string of $30 - 1 = 29$ vertical bars (to separate the categories) and 12 crosses (to represent the chosen balloons). The total number of choices of 12 balloons of the 30 different kinds is the number of strings of 41 symbols (29 vertical bars and 12 crosses), namely, $\binom{12 + 30 - 1}{12} = \binom{41}{12} = 7,898,654,920$.

b. By the same reasoning as in part (a), the total number of choices of 50 balloons of the 30 different kinds is the number of strings that consist of $30 - 1 = 29$ vertical bars (to separate the categories) and 50 crosses (to represent the balloons that are chosen), namely, $\binom{50 + 30 - 1}{50} = \binom{79}{50} \cong 3.326779701 \times 10^{21}$. If at least one balloon of each kind is chosen, we can imagine choosing those 30 first and then choosing $50 - 30 = 20$ additional balloons. Again, by the same reasoning as in part (a), the number of ways to do this is the number of strings that consist of 29 vertical bars and 20 crosses, namely, $\binom{20 + 30 - 1}{20} = \binom{49}{20} \cong 2.827752735 \times 10^{13}$. Thus the probability that a combination of 50 balloons will contain at least one balloon of each kind is $\dfrac{\binom{(50 - 30) + 30 - 1}{50 - 30}}{\binom{50 + 30 - 1}{50}} = \dfrac{\binom{49}{20}}{\binom{79}{50}} \cong 8.5 \times 10^{-9}$.

16. *a.* $\binom{30 + 4 - 1}{30} = \binom{33}{30} = 5456$

b. probability $= \dfrac{\binom{(30 - 4 \cdot 4) + 4 - 1}{30 - 4 \cdot 4}}{5456} = \dfrac{\binom{17}{14}}{5456} = \dfrac{680}{5456} \cong 0.125 = 12.5\%$

17. Any number from 1 through 99,999 whose digits add up to 9 can be thought of as a 5-digit number with leading zeroes allowed. Imagine that the 5 digits are categories into which we place 9 crosses. (For instance, $\times \times \mid \quad \mid \times \times \times \times \times \mid \times \mid \times \times$ corresponds to the number 20512.) By Theorem 6.5.1, there are $\binom{9 + 5 - 1}{9} = \binom{13}{9} = 715$ ways to place the crosses into the categories.

19. *a.* For each selection of k A76 batteries (where $0 \le k \le 10$), $30 - k$ other batteries are obtained from the 7 remaining types. The number of ways to select these other batteries is $\binom{(30 - k) + 7 - 1}{30 - k} = \binom{36 - k}{30 - k}$. So the total number of ways the inventory can be distributed is

$$\sum_{k=0}^{10} \binom{36 - k}{30 - k}$$

$$= \binom{36}{30} + \binom{35}{29} + \binom{34}{28} + \binom{33}{27} + \binom{32}{26} + \binom{31}{25} + \binom{30}{24} + \binom{29}{23} + \binom{28}{22} + \binom{27}{21} + \binom{26}{20}$$

$$= 9,637,672.$$

b. For each selection of k A76 batteries (where $0 \le k \le 10$) and m D303 batteries (where $0 \le m \le 6$), $30 - k - m$ other batteries are obtained from the 6 remaining types. The number

of ways to select these other batteries is $\binom{(30-k-m)+6-1}{30-k-m} = \binom{35-k-m}{30-k-m}$. So the

total number of ways the inventory can be distributed is $\sum_{m=0}^{6} \sum_{k=0}^{10} \binom{35-k-m}{30-k-m} = 7,652,260$.

20. Consider those columns of a trace table corresponding to an arbitrary value of k. The values of j go from 1 to k, and for each value of j, the values of i go from 1 to j.

k	k										
j	1	2		3			. . .	k			
i	1	1	2	1	2	3	. . .	1	2	3	. . . k

So for each value of k, there are $1 + 2 + 3 + \cdots + k$ columns of the table. Since k goes from 1 to n, the total number of columns in the table is

$$1 + (1+2) + (1+2+3) + \cdots + (1+2+3+\cdots+n)$$

$$
\begin{aligned}
&= \sum_{k=1}^{1} k + \sum_{k=1}^{2} k + \cdots + \sum_{k=1}^{n-1} k + \sum_{k=1}^{n} k \\
&= \frac{1 \cdot 2}{2} + \frac{2 \cdot 3}{2} + \cdots + \frac{(n-1) \cdot n}{2} + \frac{n \cdot (n+1)}{2} \\
&= \frac{1}{2}[1 \cdot 2 + 2 \cdot 3 + \cdots + (n-1) \cdot n + n \cdot (n+1)] \\
&= \frac{1}{2}\left(\frac{n(n+1)(n+2)}{3}\right) \qquad \text{by exercise 13 of Section 4.2} \\
&= \frac{n(n+1)(n+2)}{6},
\end{aligned}
$$

which agrees with the result of Example 6.5.4.

Section 6.6

2. $\binom{n}{1} = \frac{n!}{1!(n-1)!} = \frac{n \cdot (n-1)!}{(n-1)!} = n$

4. $\binom{n}{3} = \frac{n!}{3! \cdot (n-3)!} = \frac{n \cdot (n-1) \cdot (n-2) \cdot (n-3)!}{3 \cdot 2 \cdot 1 \cdot (n-3)!} = \frac{n(n-1)(n-2)}{6}$

7. By formula (6.6.3), $\binom{n}{n-2} = \frac{n(n-1)}{2}$ for $n \geq 2$. If $n \geq -1$, then $n+3 \geq 2$, and so substituting $n+3$ for n gives $\binom{n+3}{n+1} = \frac{(n+3)((n+3)-1)}{2} = \frac{(n+3)(n+2)}{2}$.

8. By (6.6.1), $\binom{n}{n} = 1$ for $n \geq 0$. If $k-r \geq 0$, then $k-r$ may be substituted for n giving $\binom{k-r}{k-r} = 1$.

10. We first compute the values in the row of Pascal's triangle that corresponds to $n = 6$.
$\binom{6}{0} = 1$, $\binom{6}{1} = 1+5 = 6$, $\binom{6}{2} = 5+10 = 15$, $\binom{6}{3} = 10+10 = 20$, $\binom{6}{4} = 10+5 = 15$,
$\binom{6}{5} = 5+1 = 6$, $\binom{6}{6} = 1 = 7$

Then we compute the values for $n = 7$.

$$\binom{7}{0} = 1, \binom{7}{1} = 1+6 = 7, \binom{7}{2} = 6+15 = 21, \binom{7}{3} = 15+20 = 35, \binom{7}{4} = 20+15 = 35,$$

$$\binom{7}{5} = 15+6 = 21, \binom{7}{6} = 6+1 = 7, \binom{7}{7} = 1$$

11. $\binom{9}{0} = 1, \binom{9}{1} = 1+8 = 9, \binom{9}{2} = 8+28 = 36, \binom{9}{3} = 28+56 = 84, \binom{9}{4} = 56+70 = 126,$

$$\binom{9}{5} = 70+56 = 126, \binom{9}{6} = 56+28 = 84, \binom{9}{7} = 28+8 = 36, \binom{9}{8} = 8+1 = 9, \binom{9}{9} = 1$$

12.

$$\begin{aligned}
\binom{n+3}{r} &= \binom{n+2}{r-1} + \binom{n+2}{r} \\
&= \left(\binom{n+1}{r-2} + \binom{n+1}{r-1}\right) + \left(\binom{n+1}{r-1} + \binom{n+1}{r}\right) \\
&= \binom{n+1}{r-2} + 2\cdot\binom{n+1}{r-1} + \binom{n+1}{r} \\
&= \left(\binom{n}{r-3} + \binom{n}{r-2}\right) + 2\cdot\left(\binom{n}{r-2} + \binom{n}{r-1}\right) + \left(\binom{n}{r-1} + \binom{n}{r}\right) \\
&= \binom{n}{r-3} + 3\cdot\binom{n}{r-2} + 3\cdot\binom{n}{r-1} + \binom{n}{r}
\end{aligned}$$

13. *Proof*: Suppose n and r are nonnegative integers with $r+1 \le n$. Then

$$\begin{aligned}
\frac{n-r}{r+1}\cdot\binom{n}{r} &= \frac{n-r}{r+1}\cdot\frac{n!}{r!(n-r)!} \\
&= \frac{n-r}{r+1}\cdot\frac{n!}{r!(n-r)\cdot(n-r-1)!} \\
&= \frac{n!}{(r+1)!\cdot(n-r-1)!} \\
&= \frac{n!}{(r+1)!\cdot(n-(r+1))!} \\
&= \binom{n}{r+1}
\end{aligned}$$

[This is what was to be shown.]

15. *Proof*: Let n be an integer with $n \ge 1$. By exercise 14, $\sum_{i=1}^{n+1}\binom{i}{2} = \binom{n+2}{3}$. But for each $i = 2, 3, \ldots, n+1$,

$$\binom{i}{2} = \frac{i!}{i!\cdot(i-2)!} = \frac{i\cdot(i-1)}{2} = \frac{(i-1)\cdot i}{2}.$$

So

$$\begin{aligned}
\binom{n+2}{3} &= \sum_{i=2}^{n+1}\binom{i}{2} \\
&= \frac{1\cdot 2}{2} + \frac{2\cdot 3}{2} + \frac{3\cdot 4}{2} + \cdots + \frac{n(n+1)}{2} \\
&= \frac{1\cdot 2 + 2\cdot 3 + 3\cdot 4 + \cdots + n(n+1)}{2}.
\end{aligned}$$

Multiplying both sides by 2 gives

$$1\cdot 2 + 2\cdot 3 + 3\cdot 4 + \cdots + n(n+1) = 2\binom{n+2}{3}.$$

[as was to be shown].

16. *Proof by mathematical induction* : Let r be a fixed nonnegative integer, and let the property $P(n)$ be the formula

$$\sum_{i=r}^{n} \binom{i}{r} = \binom{n+1}{r+1}.$$

Show that this property is true for $n = r$: To prove this property for $n = r$, we must show that

$$\sum_{i=r}^{r} \binom{i}{r} = \binom{r+1}{r+1}.$$

But the left-hand side of this equation is $\binom{r}{r} = 1$, and the right-hand side is $\binom{r+1}{r+1}$, which also equals 1. So the property is true for $n = r$.

Show that for all integers $k \geq r$, if the property is true for $n = k$ then it is true for $n = k+1$: Let k be any integer with $k \geq r$, and suppose that

$$\sum_{i=r}^{k} \binom{i}{r} = \binom{k+1}{r+1}. \qquad \textit{[inductive hypothesis]}$$

We must show that

$$\sum_{i=r}^{k+1} \binom{i}{r} = \binom{(k+1)+1}{r+1}. \qquad (*)$$

But the left-hand side of equation (*) is

$$
\begin{aligned}
\sum_{i=r}^{k+1} \binom{i}{r} &= \sum_{i=r}^{k} \binom{i}{r} + \binom{k+1}{r} & \text{by writing the last term separately} \\
&= \binom{k+1}{r+1} + \binom{k+1}{r} & \text{by inductive hypothesis} \\
&= \binom{(k+1)+1}{r+1} & \text{by Pascal's formula,}
\end{aligned}
$$

and this is the right-hand side of equation (*) *[as was to be shown].*

17. *b. Proof* : Let n be an integer with $n \geq 1$. Then

$$
\begin{aligned}
\frac{1}{4n+2} \binom{2n+2}{n+1} &= \left(\frac{1}{2(2n+1)} \right) \left(\frac{(2n+2)!}{(n+1)!((2n+2)-(n+1))!} \right) \\
&= \left(\frac{1}{2(2n+1)} \right) \left(\frac{(2n+2)!}{(n+1)!(n+1)!} \right) \\
&= \left(\frac{1}{2(2n+1)} \right) \left(\frac{(2n+2)(2n+1)(2n)!}{(n+1) \cdot n! \cdot (n+1) \cdot n!} \right) \\
&= \frac{1}{2} \left(\frac{2(n+1)}{(n+1) \cdot (n+1)} \right) \left(\frac{(2n)!}{n! \cdot n!} \right) \\
&= \frac{1}{n+1} \binom{2n}{n} \\
&= C_n.
\end{aligned}
$$

18. Suppose m and n are positive integers and r is a nonnegative integer that is less than or equal to the minimum value of m and n. Let S be a set of $m + n$ elements, and write $S = A \cup B$, where A is a subset of S with m elements, B is a subset of S with n elements, and $A \cap B = \emptyset$. The collection of subsets of r elements chosen from S can be partitioned as follows: those consisting of 0 elements chosen from A and r elements chosen from B, those consisting of 1 element chosen from A and $r - 1$ elements chosen from B, those consisting of 2 elements chosen from A and $r - 2$ elements chosen from B, and so forth, up to those consisting of r elements chosen from A and 0 elements chosen from B. By the multiplication rule, there are $\binom{m}{i}\binom{n}{r-i}$ ways to choose i objects from m and $r - i$ objects from n, and so the number of subsets of size r in which i elements are from A and $r - i$ objects are from B is $\binom{m}{i}\binom{n}{r-i}$. Hence by the addition rule, the total number of subsets of S of size r is

$$\binom{m}{0}\binom{n}{r} + \binom{m}{1}\binom{n}{r-1} + \binom{m}{2}\binom{n}{r-2} + \cdots + \binom{m}{r}\binom{n}{0}.$$

But also since S has $m + n$ elements, the number of subsets of size r of S is $\binom{m+n}{r}$. So

$$\binom{m+n}{r} = \binom{m}{0}\binom{n}{r} + \binom{m}{1}\binom{n}{r-1} + \binom{m}{2}\binom{n}{r-2} + \cdots + \binom{m}{r}\binom{n}{0}.$$

19. *Proof*: Let n be any integer with $n \geq 0$. By exercise 18 with $m = r = n$,

$$\binom{n+n}{n} = \binom{n}{0}\binom{n}{n} + \binom{n}{1}\binom{n}{n-1} + \binom{n}{2}\binom{n}{n-2} + \cdots + \binom{n}{n}\binom{n}{0}.$$

But by Example 6.6.2, $\binom{n}{n-k} = \binom{n}{k}$ for all $k = 0, 1, 2, \ldots, n$. Hence

$$\binom{2n}{n} = \binom{n}{0}^2 + \binom{n}{1}^2 + \binom{n}{2}^2 + \cdots + \binom{n}{n}^2,$$

[as was to be shown].

20. *Proof*: Let m be any nonnegative integer, and let the property $P(n)$ be the equation

$$\binom{m}{0} + \binom{m+1}{1} + \binom{m+2}{2} + \cdots + \binom{m+n}{n} = \binom{m+n+1}{n}.$$

We will show by mathematical induction that the property is true for all integers $n \geq 0$.

Show that the property is true for $n = 0$: For $n = 0$, the equation states that $\binom{m}{0} = \binom{m+0+1}{0} = \binom{m+1}{0}$. But this is true because by exercise 1 both sides of the equation equal 1.

Show that for all integers $k \geq 0$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let k be an integer with $k \geq 0$, and suppose

$$\binom{m}{0} + \binom{m+1}{1} + \binom{m+2}{2} + \cdots + \binom{m+k}{k} = \binom{m+k+1}{k}.$$

[This is the inductive hypothesis.]

We must show that

$$\binom{m}{0} + \binom{m+1}{1} + \binom{m+2}{2} + \cdots + \binom{m+(k+1)}{k+1} = \binom{m+(k+1)+1}{k+1},$$

or, equivalently,

$$\binom{m}{0} + \binom{m+1}{1} + \binom{m+2}{2} + \cdots + \binom{m+k+1}{k+1} = \binom{m+k+2}{k+1}.$$

But

$$\binom{m}{0} + \binom{m+1}{1} + \binom{m+2}{2} + \cdots + \binom{m+k+1}{k+1} = \binom{m+k+1}{k} + \binom{m+k+1}{k+1}$$

by inductive hypothesis

$$= \binom{m+k+2}{k+1}$$

by Pascal's formula ($m + k + 1$ in place of n and $k + 1$ in place of r).

[This is what was to be shown.]

21. *Proof*: Let p be a prime number and r an integer with $0 < r < p$. Then $\binom{p}{r} = \dfrac{p!}{r!(p-r)!} = \dfrac{p(p-1)!}{r!(p-r)!}$, or, equivalently, $p(p-1)! = \binom{p}{r}(r!(p-r)!)$. Now $\binom{p}{r}$ is an integer because it equals the number of subsets of size r that can be formed from a set with p elements. Thus we can apply the unique factorization theorem to express each side of this equation as a product of prime numbers. Clearly, p is a factor of the left-hand side, and so p must also be a factor of the right-hand side. But $0 < r < p$, and so p does not appear as one of the prime factors in either $r!$ or $(p-r)!$. Therefore, p must occur as one of the prime factors of $\binom{p}{r}$, and hence $\binom{p}{r}$ is divisible by p.

Section 6.7

2. $(p+q)^6 = \binom{6}{0}p^6q^0 + \binom{6}{1}p^5q^1 + \binom{6}{2}p^4q^2 + \binom{6}{3}p^3q^3 + \binom{6}{4}p^2q^4 + \binom{6}{5}p^1q^5 + \binom{6}{6}p^0q^6$

$= p^6 + 6p^5q + 15p^4q^2 + 20p^3q^3 + 15p^2q^4 + 6pq^5 + q^6$

4. $(u-v)^5$

$= \binom{5}{0}u^5(-v)^0 + \binom{5}{1}u^4(-v)^1 + \binom{5}{2}u^3(-v)^2 + \binom{5}{3}u^2(-v)^3 + \binom{5}{4}u^1(-v)^4 + \binom{5}{5}u^0(-v)^5$

$= u^5 - 5u^4v + 10u^3v^2 - 10u^2v^3 + 5u^1v^4 - v^5$

6. *Solution 1*: $(u^2 - 3v)^4 = \binom{4}{0}(u^2)^4(-3v)^0 + \binom{4}{1}(u^2)^3(-3v)^1 + \binom{4}{2}(u^2)^2(-3v)^2$

$\qquad\qquad\qquad + \binom{4}{3}(u^2)^1(-3v)^3 + \binom{4}{4}(u^2)^0(-3v)^4$

$\qquad\quad = u^8 - 12u^6v + 54u^4v^2 - 108u^2v^3 + 81v^4$

Solution 2: An alternative solution is to first expand and simplify the expression $(a + b)^4$ and then substitute u^2 in place of a and $(-3v)$ in place of b and further simplify the result. Using this approach, we first apply the binomial theorem with $n = 4$ to obtain

$$(a+b)^4 = \binom{4}{0}a^4b^0 + \binom{4}{1}a^3b^1 + \binom{4}{2}a^2b^2 + \binom{4}{3}a^1b^3 + \binom{4}{4}b^4$$
$$= a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4.$$

Substituting u^2 in place of a and $(-3v)$ in place of b gives

$$(u^2 - 3v)^4 = (u^2 + (-3v))^4 = (u^2)^4 + 4(u^2)^3(-3v) + 6(u^2)^2(-3v)^2 + 4(u^2)(-3v)^3 + (-3v)^4$$
$$= u^8 - 12u^6v + 54u^4v^2 - 108u^2v^3 + 81v^4.$$

8. $\left(\dfrac{3}{a} - \dfrac{a}{3}\right)^5$

$= \left(\dfrac{3}{a}\right)^5 + \binom{5}{1}\left(\dfrac{3}{a}\right)^4\left(-\dfrac{a}{3}\right)^1 + \binom{5}{2}\left(\dfrac{3}{a}\right)^3\left(-\dfrac{a}{3}\right)^2 + \binom{5}{3}\left(\dfrac{3}{a}\right)^2\left(-\dfrac{a}{3}\right)^3$

$\qquad\qquad\qquad\qquad + \binom{5}{4}\left(\dfrac{3}{a}\right)^1\left(-\dfrac{a}{3}\right)^4 + \left(-\dfrac{a}{3}\right)^5$

$= \dfrac{243}{a^5} - \dfrac{135}{a^3} + \dfrac{30}{a} - \dfrac{10}{3}a + \dfrac{5}{27}a^3 - \dfrac{a^5}{243}$

9. $\left(x^2 - \dfrac{1}{x}\right)^5$

$= (x^2)^5 + \binom{5}{1}(x^2)^4\left(-\dfrac{1}{x}\right)^1 + \binom{5}{2}(x^2)^3\left(-\dfrac{1}{x}\right)^2 + \binom{5}{3}(x^2)^2\left(-\dfrac{1}{x}\right)^3$

$\qquad\qquad\qquad\qquad + \binom{5}{4}(x^2)^1\left(-\dfrac{1}{x}\right)^4 + \left(-\dfrac{1}{x}\right)^5$

$= x^{10} - 5x^7 + 10x^4 - 10x + \dfrac{5}{x^2} - \dfrac{1}{x^5}$

10. $(a+b)^6 = (a+b)\cdot(a+b)^5$

$\qquad = (a+b)\cdot(a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5)$

$\qquad = a^6 + 5a^5b + 10a^4b^2 + 10a^3b^3 + 5a^2b^4 + ab^5 + a^5b + 5a^4b^2 + 10a^3b^3 + 10a^2b^4 + 5ab^5 + b^6$

$\qquad = a^6 + (5+1)a^5b + (10+5)a^4b^2 + (10+10)a^3b^3 + (5+10)a^2b^4 + (1+5)ab^5 + b^6$

$\qquad = a^6 + 6a^5b + 15a^4b^2 + 20a^3b^3 + 15a^2b^4 + 6ab^5 + b^6$

12. Term is $\binom{10}{3}(2x)^7 3^3$. Coefficient is $\dfrac{10!}{3!\cdot 7!}\cdot 2^7\cdot 3^3 = 120\cdot 128\cdot 27 = 414,720.$

14. Term is $\binom{10}{2}(u^2)^8(-v^2)^2$. Coefficient is $\dfrac{10!}{2!\cdot 8!}\cdot(-1)^2 = 45.$

16. Term is $\binom{14}{5}(2x)^{14-5}(-3y^2)^5$. Coefficient is $\dfrac{14!}{5!\cdot 9!}\cdot 2^9\cdot(-3)^5 = 2002\cdot 512\cdot(-243) = -249,080,832.$

18. *Proof*: Let n be an integer with $n \geq 0$. Apply the binomial theorem with $a = 1$ and $b = 2$ to obtain

$\quad 3^n \quad = \quad (1+2)^n$

$\qquad = \quad \binom{n}{0}1^n2^0 + \binom{n}{1}1^{n-1}2^1 + \cdots + \binom{n}{k}1^{n-k}2^k + \cdots + \binom{n}{n}1^{n-n}2^n$

$\qquad = \quad \binom{n}{0} + 2\binom{n}{1} + 2^2\binom{n}{2} + \cdots + 2^n\binom{n}{n}$

because $2^0 = 1$ and $1^{n-k} = 1$ for all integers k.

20. *Proof*: Let n be an integer with $n \geq 0$. Apply the binomial theorem with $a = 3$ and $b = -1$ to obtain

$$
\begin{aligned}
2^n &= (3 + (-1))^n \\
&= \binom{n}{0}3^n(-1)^0 + \binom{n}{1}3^{n-1}(-1)^1 + \cdots + \binom{n}{i}3^{n-i}(-1)^i + \cdots + \binom{n}{n}3^{n-n}(-1)^n \\
&= \sum_{i=0}^{n}(-1)^i\binom{n}{i}3^{n-i}.
\end{aligned}
$$

21. *Proof*: Let n be an integer with $n \geq 0$ and suppose x is any nonnegative real number. Apply the binomial theorem with $a = 1$ and $b = x$ to obtain

$$
\begin{aligned}
(1 + x)^n &= \binom{n}{0}1^n x^0 + \binom{n}{1}1^{n-1}x^1 + \cdots + \binom{n}{k}1^{n-k}x^k + \cdots + \binom{n}{n}1^{n-n}x^n \\
&= \binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n \quad \text{because 1 raised to any power is 1} \\
&= 1 + nx + \frac{n(n-1)}{2}x^2 + \cdots + x^n.
\end{aligned}
$$

But each term to the right of nx is nonnegative. Hence $(1 + x)^n \geq 1 + nx$.

22. *Proof*: Let n be an integer with $n \geq 0$. Apply the binomial theorem with $a = 1$ and $b = -1/2$ and use the fact that 1 to any power equals 1 to obtain

$$
\left(\frac{1}{2}\right)^n = (1 + (-\frac{1}{2}))^n
$$

$$
= \sum_{k=0}^{n}\binom{n}{k}1^{n-k}\left(-\frac{1}{2}\right)^k
$$

$$
= \sum_{k=0}^{n}\binom{n}{k}\left(-\frac{1}{2}\right)^k
$$

$$
= \begin{cases} \displaystyle\sum_{k=0}^{n-1}\binom{n}{k}\left(-\frac{1}{2}\right)^k + \left(\frac{1}{2}\right)^n & \text{if } n \text{ is even} \\[3mm] \displaystyle\sum_{k=0}^{n-1}\binom{n}{k}\left(-\frac{1}{2}\right)^k - \left(\frac{1}{2}\right)^n & \text{if } n \text{ is odd} \end{cases}
$$

Subtracting $\left(\frac{1}{2}\right)^n$ from both sides of the first equation and adding $\left(\frac{1}{2}\right)^n$ to both sides of the second equation gives

$$
\sum_{k=0}^{n-1}\binom{n}{k}\left(-\frac{1}{2}\right)^k = \begin{cases} 0 & \text{if } n \text{ is even} \\ 2\left(\frac{1}{2}\right)^n & \text{if } n \text{ is odd} \end{cases}
$$

Thus, in expanded form,

$$
\binom{n}{0} - \frac{1}{2}\binom{n}{1} + \frac{1}{2^2}\binom{n}{2} - \frac{1}{2^3}\binom{n}{3} + \cdots + (-1)^{n-1}\binom{n}{n-1} = \begin{cases} 0 & \text{if } n \text{ is even} \\ \dfrac{1}{2^{n-1}} & \text{if } n \text{ is odd} \end{cases}.
$$

23. *Proof by mathematical induction*: Let the property $P(n)$ be the sentence "For any set S with n elements, S has 2^{n-1} subsets with an even number of elements and 2^{n-1} subsets with an odd number of elements."

Show that the property is true for $n = 1$: Any set S with just 1 element, say x, has two subsets: $\emptyset$, which has 0 elements, and $\{x\}$, which has 1 element. Since 0 is even and 1 is odd, the number of subsets of S with an even number of elements equals the number of subsets of S with an odd number of elements, namely, 1; and $1 = 2^0 = 2^{1-1}$.

Show that for all integers $k \geq 1$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let k be an integer with $k \geq 1$, and suppose that for any set S with k elements, S has 2^{k-1} subsets with an even number of elements and 2^{k-1} subsets with an odd number

of elements. *[This is the inductive hypothesis.]* We must show that for any set S with $k+1$ elements, S has $2^{(k+1)-1} = 2^k$ subsets with an even number of elements and $2^{(k+1)-1} = 2^k$ subsets with an odd number of elements. Call the elements of $S = \{x_1, x_2, \ldots, x_k, x_{k+1}\}$. By inductive hypothesis, $\{x_1, x_2, \ldots, x_k\}$ has 2^{k-1} subsets with an even number of elements and 2^{k-1} subsets with an odd number of elements. Now every subset of $\{x_1, x_2, \ldots, x_k\}$ is also a subset of S, and the only other subsets of S are obtained by taking the union of a subset of $\{x_1, x_2, \ldots, x_k\}$ with $\{x_{k+1}\}$. Moreover, if a subset of $\{x_1, x_2, \ldots, x_k\}$ has an even number of elements, then the union of that subset with $\{x_{k+1}\}$ has an odd number of elements. So 2^{k-1} of the subsets of S that are obtained by taking the union of a subset of $\{x_1, x_2, \ldots, x_k\}$ with $\{x_{k+1}\}$ have an even number of elements and 2^{k-1} have an odd number of elements. Thus the total number of subsets of S with an even number of elements is $2^{k-1} + 2^{k-1} = 2 \cdot 2^{k-1} = 2^{1+(k-1)} = 2^k$. Similarly, the total number of subsets of S with an odd number of elements is also $2^{k-1} + 2^{k-1} = 2^k$ *[as was to be shown]*.

Justification for the identity in exercise 17: Let n be any positive integer, let E be the largest even integer less than or equal to n, and let O be the largest odd integer less than or equal to n. Let S be any set with n elements. Then the number of subsets of S with an even number of elements is $\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots + \binom{n}{E}$, and the number of subsets of S with an odd number of elements is $\binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \cdots + \binom{n}{O}$. But there are as many subsets with an even number of elements as there are subsets with an odd number of elements, so if we subtract the second of these quantities from the first we obtain 0:

$$
\begin{aligned}
0 &= \left[\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots + \binom{n}{E} \right] - \left[\binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \cdots + \binom{n}{O} \right] \\
&= \binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \cdots + (-1)^n \binom{n}{n}.
\end{aligned}
$$

25. Let m be an integer with $m \geq 0$. Then

$$
\begin{aligned}
\sum_{i=0}^{m} \binom{m}{i} 4^i &= \sum_{i=0}^{m} \binom{m}{i} 1^{m-i} 4^i && \text{because 1 raised to any power is 1} \\
&= (1 + 4)^m && \text{by the binomial theorem with } a = 1 \text{ and } b = 4 \\
&= 5^m.
\end{aligned}
$$

27. Let m be an integer with $m \geq 0$. Then

$$
\sum_{k=0}^{m} \binom{m}{k} 2^{m-k} x^k = (2 + x)^m \quad \text{by the binomial theorem with } a = 2 \text{ and } b = x.
$$

29. Let n be an integer with $n \geq 0$. Then

$$
\begin{aligned}
\sum_{r=0}^{n} \binom{n}{r} x^{2r} &= \sum_{r=0}^{n} \binom{n}{r} 1^{n-r} (x^2)^r \\
& \qquad \text{by the laws of exponents and because 1 raised to any power is 1} \\
&= (1 + x^2)^n \\
& \qquad \text{by the binomial theorem with } a = 1 \text{ and } b = x^2.
\end{aligned}
$$

30. Let m be an integer with $m \geq 0$. Then

$$
\begin{aligned}
\sum_{i=0}^{m} \binom{m}{i} p^{m-i} q^{2i} &= \sum_{i=0}^{m} \binom{m}{i} p^{m-i} (q^2)^i && \text{by the laws of exponents} \\
&= (p + q^2)^m && \text{by the binomial theorem with } a = p \text{ and } b = q^2.
\end{aligned}
$$

31. Let n be an integer with $n \geq 0$. Then

$$\sum_{k=0}^{n}\binom{n}{k}\frac{1}{2^k} = \sum_{k=0}^{n}\binom{n}{k}1^{n-k}(\frac{1}{2})^k$$

by the laws of exponents and because 1 raised to any power is 1

$$= (1+\frac{1}{2})^n$$

by the binomial theorem with $a = 1$ and $b = \dfrac{1}{2}$

$$= (\frac{3}{2})^n.$$

33. Let n be an integer with $n \geq 0$. Then

$$\sum_{k=0}^{n}\binom{n}{k}3^{2n-2k}2^{2k} = \sum_{k=0}^{n}\binom{n}{k}(3^2)^{n-k}(2^2)^k$$

by the laws of exponents

$$= \sum_{k=0}^{n}\binom{n}{k}9^{n-k}4^k$$

because $3^2 = 9$ and $2^2 = 4$

$$= (9+4)^n$$

by the binomial theorem with $a = 9$ and $b = 4$

$$= 13^n.$$

35. Let n be an integer with $n \geq 0$. Then

$$\sum_{k=0}^{n}(-1)^k\binom{n}{k}3^{2n-2k}2^{2k} = \sum_{k=0}^{n}(-1)^k\binom{n}{k}(3^2)^{n-k}(2^2)^k$$

by the laws of exponents

$$= \sum_{k=0}^{n}\binom{n}{k}9^{n-k}(-4)^k$$

by the laws of exponents and because $3^2 = 9$ and $2^2 = 4$

$$= (9-4)^n$$

by the binomial theorem with $a = 9$ and $b = -4$

$$= 5^n.$$

36. *a.* Let n be an integer with $n \geq 0$. Apply the binomial theorem with $a = 1$ and $b = x$ to obtain

$$(1+x)^n = \sum_{k=0}^{n}\binom{n}{k}1^{n-k}x^k = \sum_{k=0}^{n}\binom{n}{k}x^k \qquad \text{because any power of 1 is 1.}$$

c. (ii) Let n be an integer with $n \geq 1$. Apply the formula from part (b) with $x = -1$ to obtain

$$0 = n(1+(-1))^{n-1} = \sum_{k=1}^{n}\binom{n}{k}k(-1)^{k-1}.$$

d. Apply the formula of part (b) with $x = 3$ to obtain

$$n \cdot 4^{n-1} = n(1+3)^{n-1} = \sum_{k=1}^{n}\binom{n}{k}k3^{k-1} = \sum_{k=1}^{n}\binom{n}{k}k3^k3^{-1} = \frac{1}{3}\sum_{k=1}^{n}\binom{n}{k}k3^k.$$

So $\displaystyle\sum_{k=1}^{n}\binom{n}{k}k3^k = 3n4^{n-1}.$

Section 6.8

3. *a.* $P(A \cup B) = 0.4 + 0.2 = 0.6$

   b. By the formula for the probability of a general union and because $S = A \cup B \cup C$,
   $$P(S) = ((A \cup B) \cup C) = P(A \cup B) + P(C) - P((A \cup B) \cap C).$$
   Suppose $P(C) = 0.2$. Then, since $P(S) = 1$,
   $$1 = 0.6 + 0.2 - P((A \cup B) \cap C) = 0.8 - P((A \cup B) \cap C).$$
   Solving for $P((A \cup B) \cap C)$ gives $P((A \cup B) \cap C) = -0.2$, which is impossible. Hence $P(C) \neq 0.2$.

5. We apply the formula for the probability of the complement of an event to obtain $P(B^c) = 0.4 = 1 - P(B)$. Solving for $P(B)$ gives $P(B) = 0.6$. So, by the formula for the probability of a general union, $P(A \cup B) = P(A) + P(B) - P(A \cap B) = 0.6 + 0.6 - 0.2 = 1$.

6. First note that we can apply the formula for the probability of the complement of an event to obtain $0.3 = P(U^c) = 1 - P(U)$. Solving for $P(U)$ gives $P(U) = 0.7$. Second, observe that by De Morgan's law $U^c \cup V^c = (U \cap V)^c$. Thus $0.4 = P(U^c \cup V^c) = P((U \cap V)^c) = 1 - P(U \cap V)$. Solving for $P(U \cap V)$ gives $P(U \cap V) = 0.6$. So, by the formula for the union of two events, $P(U \cup V) = P(U) + P(V) - P(U \cap V) = 0.7 + 0.6 - 0.6 = 0.7$.

8. *a.* Because $A \cap B = \emptyset$, $P(A \cup B) = P(A) + P(B) = 0.5 + 0.4 = 0.9$.

   b. Note that $C = (A \cup B)^c$. Thus $P(C) = 1 - P(A \cup B) = 1 - 0.9 = 0.1$.

   c. Because $A \cap C = \emptyset$, $P(A \cup C) = P(A) + P(C) = 0.5 + 0.1 = 0.6$.

   d. $P(A^c) = 1 - P(A) = 1 - 0.5 = 0.5$

   e. By De Morgan's law $A^c \cap B^c = (A \cup B)^c$. Thus, by part (a) and the formula for the probability of the complement of an event, $P(A^c \cap B^c) = P((A \cup B)^c) = 1 - P(A \cup B) = 1 - 0.9 = 0.1$

   f. By De Morgan's law $A^c \cup B^c = (A \cap B)^c$. Thus by the formula for the probability of the complement of an event and because $A \cap B = \emptyset$ and $P(\emptyset) = 0$, $P(A^c \cup B^c) = P((A \cap B)^c) = 1 - P(A \cap B) = 1 - 0 = 1$.

9. *b.* By part (a), $P(A \cup B) = 0.7$. So, since $C = (A \cup B)^c$, by the formula for the probability of the complement of an event, $P(C) = 1 - P(A \cup B) = 1 - 0.7 = 0.3$.

   c. By the formula for the probability of the complement of an event, $P(A^c) = 1 - P(A) = 1 - 0.4 = 0.6$.

   e. By De Morgan's law $A^c \cup B^c = (A \cap B)^c$. Thus, the formula for the probability of the complement of an event, $P(A^c \cup B^c) = P((A \cap B)^c) = 1 - P(A \cap B) = 1 - 0.2 = 0.8$.

   f. Solution 1: Because $C = S - (A \cup B)$, $C = (A \cup B)^c$. Thus by substitution, De Morgan's law, and the associative, commutative, and idempotent properties of $\cap$,
   $$B^c \cap C = B^c \cap (A \cup B)^c = B^c \cap (A^c \cap B^c) = (B^c \cap A^c) \cap B^c = (A^c \cap B^c) \cap B^c = A^c \cap (B^c \cap B^c) = A^c \cap B^c = (A \cup B)^c = C.$$ Hence, by part (b),
   $$P(B^c \cap C) = P(C) = 0.3.$$
   Solution 2: Because $C = S - (A \cup B)$, $C = (A \cup B)^c$. Thus by De Morgan's law, $C = A^c \cap B^c$. Now $A^c \cap B^c \subseteq B^c$ (by Theorem 5.2.1(1)a) and hence $B^c \cap C = C$ (by Theorem 5.2.3a). Therefore $P(B^c \cap C) = P(C) = 0.3$.

10. *a.* By the formula for the probability of a general union, $P(A \cup B) = P(A) + P(B) - P(A \cap B) = 0.7 + 0.3 - 0.1 = 0.9$.

    b. By part (a), $P(A \cup B) = 0.9$. So, since $C = (A \cup B)^c$, by the formula for the probability of the complement of an event, $P(C) = 1 - P(A \cup B) = 1 - 0.9 = 0.1$.

c. By the formula for the probability of the complement of an event, $P(A^c) = 1 - P(A) = 1 - 0.7 = 0.3$.

d. By De Morgan's law $A^c \cap B^c = (A \cup B)^c = C$. Thus, by part (b), $P(A^c \cap B^c) = P(C) = 0.1$.

e. By De Morgan's law $A^c \cup B^c = (A \cap B)^c$. Thus, by the formula for the probability of the complement of an event, $P(A^c \cup B^c) = P((A \cap B)^c) = 1 - P(A \cap B) = 1 - 0.1 = 0.9$.

f. Because $C = S - (A \cup B)$, $C = (A \cup B)^c$. Thus by substitution, De Morgan's law, and the associative, commutative, and idempotent laws for $\cap$,

$B^c \cap C = B^c \cap (A \cup B)^c = B^c \cap (A^c \cap B^c) = (B^c \cap A^c) \cap B^c = (A^c \cap B^c) \cap B^c = A^c \cap (B^c \cap B^c) = A^c \cap B^c = (A \cup B)^c = C$. Hence, by part (b),

$P(B^c \cap C) = P(C) = 0.1$.

11. *Proof:* Suppose S is any sample space and U and V are events in S with $U \subseteq V$. *[We will show that $P(U) \leq P(V)$.]* First note that by the set difference, distributive, identity, and universal bound laws and the definition of union, $U \cup (V - U) = U \cup (V \cap U^c) = (U \cup V) \cap (U \cup U^c) = (U \cup V) \cap S = U \cup V = V$. Also by the set difference law, and the associative, commutative, and universal bound laws for $\cap$, $U \cap (V - U) = U \cap (V \cap U^c) = U \cap (U^c \cap V) = (U \cap U^c) \cap V = \emptyset \cap V = \emptyset$. Thus, by probability axiom 3 (the formula for the probability of mutually disjoint events), $P(V) = P(U \cup (V - U)) = P(U) + P(V - U)$. But $V - U$ is an event in S, so $P(V - U) \geq 0$. Hence $P(U) \leq P(V)$.

12. *Proof 1:* Suppose S is any sample space and U and V are any events in S. First note that by the set difference, distributive, universal bound, and identity laws, $(V \cap U) \cup (V - U) = (V \cap U) \cup (V \cap U^c) = V \cap (U \cup U^c) = V \cap S = V$. Next, observe that if $x \in (V \cap U) \cap (V - U)$, then, by definition of intersection, $x \in (V \cap U)$ and $x \in (V - U)$, and so, by definition of intersection and set difference, $x \in V$, $x \in U$, $x \in V$, and $x \notin U$, and hence, in particular, $x \in U$ and $x \notin U$, which is impossible. It follows that $(V \cap U) \cap (V - U) = \emptyset$. Thus, by substitution and by probability axiom 3 (the formula for the probability of mutually disjoint events), $P(V) = P((V \cap U) \cup (V - U)) = P(V \cap U) + P(V - U)$. Solving for $P(V - U)$ gives $P(V - U) = P(V) - P(U \cap V)$.

Proof 2: Suppose S is any sample space and U and V are any events in S. First note that by the set difference, distributive, universal bound, and identity laws, $U \cup (V - U) = U \cup (V \cap U^c) = (U \cup V) \cap (U \cup U^c) = (U \cup V) \cap S = U \cup V$. Next, observe that, by the same sequence of steps as in the solution to exercise 11, $U \cap (V - U) = \emptyset$. Thus, by substitution, $P(U \cup V) = P(U \cup (V - U)) = P(U) + P(V - U)$. But also by the formula for the probability of a general union, $P(U \cup V) = P(U) + P(V) - P(U \cap V)$. Equating the two expressions for $P(U \cup V)$ gives $P(U) + P(V - U) = P(U) + P(V) - P(U \cap V)$. Subtracting $P(U)$ from both sides gives $P(V - U) = P(V) - P(U \cap V)$.

13. We precede the proof of the statement in the exercise with a technically necessary, but slightly pedantic, lemma.

Lemma: For any positive integer n, $\underbrace{\emptyset \cup \emptyset \cup \cdots \cup \emptyset}_{n \text{ terms}} = \emptyset$.

Proof (by mathematical induction): Let $P(n)$ be the property "$\underbrace{\emptyset \cup \emptyset \cup \cdots \cup \emptyset}_{n \text{ terms}} = \emptyset$."

Show that the property is true for $n = 1$: When $n = 1$, the property is $\emptyset = \emptyset$, which is true.

Show that for all integers $k \geq 1$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let k be an integer with $k \geq 1$, and suppose that $\underbrace{\emptyset \cup \emptyset \cup \cdots \cup \emptyset}_{k \text{ terms}} = \emptyset$. *[This is the inductive hypothesis.]* We must show that $\underbrace{\emptyset \cup \emptyset \cup \cdots \cup \emptyset}_{k+1 \text{ terms}} = \emptyset$. But by the definition of

a general union of sets given in the directions for exercise 35 of Section 5.2 and by inductive hypothesis, $\underbrace{\emptyset \cup \emptyset \cup \cdots \cup \emptyset}_{k+1 \text{ terms}} = (\underbrace{\emptyset \cup \emptyset \cup \cdots \cup \emptyset}_{k \text{ terms}}) \cup \emptyset = \emptyset \cup \emptyset = \emptyset$ *[as was to be shown]*.

Proof of the statement in the exercise (by mathematical induction): Let $P(n)$ be the property "If $A_1, A_2, \ldots, A_n$ are any mutually disjoint events in a sample space S, then $P(A_1 \cup A_2 \cup \cdots \cup A_n) = \sum_{k=1}^{n} P(A_k)$."

Show that the property is true for $n = 2$: If A_1 and A_2 are any two mutually disjoint events in a sample space S, then, by probability axiom 3 (the formula for the probability of mutually disjoint events), $P(A_1 \cup A_2) = P(A_1) + P(A_2) = \sum_{k=1}^{2} P(A_k)$.

Show that for all integers $k \geq 2$, if the property is true for $n = i$ then it is true for $n = i + 1$: Let k be an integer with $k \geq 2$, and suppose that if $A_1, A_2, \ldots, A_i$ are any mutually disjoint events in a sample space S, then $P(A_1 \cup A_2 \cup \cdots \cup A_i) = \sum_{k=1}^{i} P(A_k)$. *[This is the inductive hypothesis.]* We will show that if $A_1, A_2, \ldots, A_{i+1}$ are any mutually disjoint events in a sample space S, then $P(A_1 \cup A_2 \cup \cdots \cup A_{i+1}) = \sum_{k=1}^{i+1} P(A_k)$. According to the definition of a general union of sets given in exercise 35 in Section 5.2 (the directions for the proof of the generalized distributive law for sets), $A_1 \cup A_2 \cup \cdots \cup A_{i+1} = (A_1 \cup A_2 \cup \cdots \cup A_i) \cup A_{i+1}$. Also, because $A_1, A_2, \ldots, A_{i+1}$ are mutually disjoint, by the commutative and generalized distributive laws for sets and by the lemma, $(A_1 \cup A_2 \cup \cdots \cup A_i) \cap A_{i+1} = A_{i+1} \cap (A_1 \cup A_2 \cup \cdots \cup A_i) = (A_{i+1} \cap A_1) \cup (A_{i+1} \cap A_2) \cup \cdots \cup (A_{i+1} \cap A_i) = \underbrace{\emptyset \cup \emptyset \cup \cdots \cup \emptyset}_{i \text{ terms}} = \emptyset$. Thus, by probability axiom 3 (the formula for the probability of mutually disjoint events) and the inductive hypothesis, $P(A_1 \cup A_2 \cup \cdots \cup A_{i+1}) = P((A_1 \cup A_2 \cup \cdots \cup A_i) \cup A_{i+1}) = P(A_1 \cup A_2 \cup \cdots \cup A_i) + P(A_{i+1}) = \sum_{k=1}^{i} P(A_k) + P(A_{i+1}) = \sum_{k=1}^{i+1} P(A_k)$ *[as was to be shown]*.

15. *Solution 1*: The net gain for the first prize winner is $\$10,000,000 - \$0.60 = \$9,999,999.40$, that for the second prize winner is $\$1,000,000 - \$0.60 = \$999,999.40$, and that for the third prize winner is $\$50,000 - \$0.60 = 49,999.40$. Each of the other 29,999,997 million people who mail back an entry form has a net loss of $\$0.60$. Because all of the 30 million entry forms have an equal chance of winning the prizes, the expected gain or loss is

$$\$9999999.40 \cdot \frac{1}{30000000} + \$999999.40 \cdot \frac{1}{30000000} + \$49999.40 \cdot \frac{1}{30000000} - \$0.60 \cdot \frac{29999997}{30000000}) \cong -\$0.23,$$

or an expected loss of about 23 cents per person.

Solution 2: The total amount spent by the 30 million people who return entry forms is $30,000,000 \cdot \$0.60 = \$18,000,000$. The total amount of prize money awarded is $\$10,000,000 + \$1,000,000 + \$50,000 = \$11,050,000$. Thus the net loss is $\$18,000,000 - \$11,050,000 = \$6,950,000$, and so the expected loss per person is $6950000/30000000 \cong -\$0.23$, or about 23 cents per person.

17. Let 2_1 and 2_2 denote the two balls with the number 2, let 8_1 and 8_2 denote the two balls with the number 8, and let 1 denote the other ball. There are $\binom{5}{2} = 10$ subsets of 2 balls that can be chosen from the urn. The following table shows the sums of the numbers on the balls in each set and the corresponding probabilities:

Subset	Sum s	Probability of s
$\{1, 2_1\}, \{1, 2_2\}$	3	2/10
$\{2_1, 2_2\}$	4	1/10
$\{1, 8_1\}, \{1, 8_2\}$	9	2/10
$\{2_1, 8_1\}, \{2_1, 8_2\}, \{2_2, 8_1\}, \{2_2, 8_2\}$	10	4/10
$\{8_1, 8_2\}$	16	1/10

Thus the expected value is $3 \cdot \dfrac{2}{10} + 4 \cdot \dfrac{1}{10} + 9 \cdot \dfrac{2}{10} + 10 \cdot \dfrac{4}{10} + 16 \cdot \dfrac{1}{10} = \dfrac{84}{10} = 8.4$.

18. Let 2_1 and 2_2 denote the two balls with the number 2, let 8_1 and 8_2 denote the two balls with the number 8, and let 1 denote the other ball. There are $\binom{5}{3} = 10$ subsets of 3 balls that can be chosen from the urn. The following table shows the sums of the numbers on the balls in each set and the corresponding probabilities:

Subset	Sum s	Probability of s
$\{1, 2_1, 2_2\}$	5	1/10
$\{1, 2_1, 8_1\}, \{1, 2_2, 8_1\}, \{1, 2_1, 8_2\}, \{1, 2_2, 8_2\}$	11	4/10
$\{2_1, 2_2, 8_1\}, \{2_1, 2_2, 8_2\}$	12	2/10
$\{1, 8_1, 8_2\}$	17	1/10
$\{2_1, 8_1, 8_2\}, \{2_2, 8_1, 8_2\}$	18	2/10

Thus the expected value is $5 \cdot \dfrac{1}{10} + 11 \cdot \dfrac{4}{10} + 12 \cdot \dfrac{2}{10} + 17 \cdot \dfrac{1}{10} + 18 \cdot \dfrac{2}{10} = \dfrac{126}{10} = 12.6$.

20. The probability of drawing a face card is $\dfrac{12}{52}$. So the probability of not drawing a face card is $\dfrac{40}{52}$, and the expected gain or loss is $\dfrac{12}{52} \cdot 3 - \dfrac{40}{52} \cdot 1 = -\dfrac{4}{52} \cong -0.077$. Hence the expected loss is about 7.7 cents per game.

21. When a coin is tossed 4 times, there are $2^4 = 16$ possible outcomes and there are $\binom{4}{h}$ ways to obtain exactly h heads (as shown by the technique illustrated in Example 6.4.10). The following table shows the possible outcomes of the tosses, the amount gained or lost for each outcome, the number of ways the outcomes can occur, and the probabilities of the outcomes.

Number of Heads	Net Gain (or Loss)	Number of Ways	Probability
0	$-\$3$	$\binom{4}{0} = 1$	1/16
1	$-\$2$	$\binom{4}{1} = 4$	4/16
2	$-\$1$	$\binom{4}{2} = 6$	6/16
3	$\$2$	$\binom{4}{3} = 4$	4/16
4	$\$3$	$\binom{4}{4} = 1$	1/16

Thus the expected value is $(-\$3) \cdot \dfrac{1}{16} + (-\$2) \cdot \dfrac{4}{16} + (-\$1) \cdot \dfrac{6}{16} + \$2 \cdot \dfrac{4}{16} + \$3 \cdot \dfrac{1}{16} = -\$\dfrac{6}{16} = -\$0.375$. So this game has an expected loss of 37.5 cents.

22. For $i = 1, 2, 3, 4$, let A_i be the event that a head comes up on the ith toss but not before, and let A_5 be the event that all four tosses produce tails. Because the coin is fair, there is a 50-50 chance that heads will come up on the first toss, and so $P(A_1) = 1/2$. For heads to come up on the second toss and not before, implies that 2 tosses occurred with 4 possible outcomes, and that in only 1 of the 4 was the outcome TH. Thus $P(A_2) = 1/4$. Similar reasoning shows that $P(A_3) = 1/8$ because in only 1 of the 8 equally likely outcomes of tossing a coin three

times does TTH occur. Finally, both $P(A_4)$ and $P(A_5)$ equal $1/16$ because when a coin is tossed 4 times, in only 1 of the 16 equally likely outcomes does $TTTH$ occur and in only 1 of the 16 does $TTTT$ occur.

Thus the expected number of tosses until either a head comes up or four tails are obtained is
$$1 \cdot \frac{1}{2} + 2 \cdot \frac{1}{4} + 3 \cdot \frac{1}{8} + 4 \cdot \frac{1}{16} + 4 \cdot \frac{1}{16} = 1.875.$$

Section 6.9

2. $P(X \cap Y) = P(X \mid Y)P(Y) = \frac{1}{3} \cdot \frac{1}{4} = \frac{1}{12}$

3. *b.* Let A be the event that a randomly chosen person tests positive for a condition, let B_1 be the event that the person has the condition, and let B_2 be the event that the person does not have the condition. The event that a randomly chosen person tests negative for the condition is A^c. Then the probability of a false positive is $P(A \mid B_2)$, the probability of a false negative is $P(A^c \mid B_1)$, the probability that a person who actually has the condition tests positive for it is $P(A \mid B_1)$, and the probability that a person who does not have the condition tests negative for it is $P(A^c \mid B_2)$.

   (1) Suppose the probability of a false positive is 4%. This means that $P(A \mid B_2) = 4\% = 0.04$. By part (a), $P(A^c \mid B_2) = 1 - P(A \mid B_2) = 1 - 0.04 = 0.96$, and so the probability that a person who does not have the condition tests negative for it is 96%.

   (2) Suppose the probability of a false negative is 1%. This means that $P(A^c \mid B_1) = 1\% = 0.01$. By part (a), $P(A^c \mid B_1) = 1 - P(A \mid B_1)$, and so $P(A \mid B_1) = 1 - P(A^c \mid B_1) = 1 - 0.01 = 0.99$. Thus the probability that a person who has the condition tests positive for it is 99%.

4. By definition of conditional probability, $P(A \mid B^c) = \dfrac{P(A \cap B^c)}{P(B^c).}$. Now by the solution to Example 6.9.5, $A = (A \cap B) \cup (A \cap B^c)$ and $(A \cap B) \cap (A \cap B^c) = \emptyset$, and thus, by probability axiom 3, $P(A) = P(A \cap B) + P(A \cap B^c)$. Solving for $P(A \cap B^c)$ gives $P(A \cap B^c) = P(A) - P(A \cap B)$, and using formula 6.9.2 to substitute $P(A \mid B)P(B)$ in place of $P(A \cap B)$ gives $P(A \cap B^c) = P(A) - P(A \mid B)P(B)$. Also, by the formula for the complement of an event, $P(B^c) = 1 - P(B)$. Hence, by substitution, $P(A \mid B^c) = \dfrac{P(A \cap B^c)}{P(B^c).} = \dfrac{P(A) - P(A \mid B)P(B)}{1 - P(B)}$.

6. Let R_1 be the event that the first ball is red, R_2 the event that the second ball is red, B_1 the event that the first ball is blue, and B_2 the event that the second ball is blue. Then $P(R_1) = \dfrac{30}{70}$, $P(B_1) = \dfrac{40}{70}$, $P(R_2 \mid R_1) = \dfrac{29}{69}$, $P(R_2 \mid B_1) = \dfrac{30}{69}$, and $P(B_2 \mid B_1) = \dfrac{39}{69}$.

   a. The probability that both balls are red is $P(R_1 \cap R_2) = P(R_2 \mid R_1)P(R_1) = \dfrac{29}{69} \cdot \dfrac{30}{70} = \dfrac{29}{161} \cong 18.0\%$.

   b. The probability that the second ball is red but the first ball is not is $P(B_1 \cap R_2) = P(R_2 \mid B_1)P(B_1) = \dfrac{30}{69} \cdot \dfrac{40}{70} = \dfrac{40}{161} \cong 24.8\%$.

   c. Because $B_1 \cap R_1 = \emptyset$ and $B_1 \cup R_1$ is the entire sample space S, $R_2 = S \cap R_2 = (B_1 \cap R_2) \cup (R_1 \cap R_2)$ and $(B_1 \cap R_2) \cap (R_1 \cap R_2) = \emptyset$. Thus the probability that the second ball is red is $P(R_2) = P((B_1 \cap R_2) \cup (R_1 \cap R_2)) = P(B_1 \cap R_2) + P(R_1 \cap R_2) = \dfrac{40}{161} + \dfrac{29}{161} = \dfrac{69}{161} \cong 0.42857 \cong 42.9\%$.

   d. *Solution 1:* The probability that at least one of the balls is red is $P(R_1 \cup R_2) = P(R_1) + P(R_2) - P(R_1 \cap R_2) = \dfrac{30}{70} + \dfrac{69}{161} - \dfrac{29}{161} = \dfrac{109}{161} \cong 67.7\%$.

Solution 2: The event that at least one of the balls is red is the complement of the event that both balls are blue. Thus $P(R_1 \cup R_2) = 1 - P(B_1 \cap B_2) = 1 - P(B_2 \mid B_1)P(B_1) = 1 - \dfrac{39}{69} \cdot \dfrac{40}{70} = 1 - \dfrac{52}{161} \cong 67.7\%$

7. *b.* Let W_1 be the event that a woman is chosen on the first draw, W_2 the event that a woman is chosen on the second draw, M_1 the event that a man is chosen on the first draw, and M_2 the event that a man is chosen on the second draw. Then $P(W_1) = \dfrac{3}{10}$, $P(M_1) = \dfrac{7}{10}$, $P(W_2 \mid W_1) = \dfrac{2}{9}$, $P(W_2 \mid M_1) = \dfrac{3}{9} = \dfrac{1}{3}$, and $P(M_2 \mid M_1) = \dfrac{6}{9} = \dfrac{2}{3}$, and $P(M_2 \mid W_1) = \dfrac{7}{9}$. Then the probability that both finalists are men is $P(M_1 \cap M_2) = P(M_2 \mid M_1)P(M_1) = \dfrac{2}{3} \cdot \dfrac{7}{10} = \dfrac{7}{15} \cong 46.7\%$.

c. Solution 1: The event that one finalist is a woman and the other is a man is $(W_1 \cap M_2) \cup (W_2 \cap M_1)$ and $W_1 \cap M_2$ and $W_2 \cap M_1$ are mutually disjoint because W_1 and M_1 are mutually disjoint. Hence the probability that one finalist is a woman and the other is a man is $P((W_1 \cap M_2) \cup (W_2 \cap M_1)) = P(W_1 \cap M_2) + P(W_2 \cap M_1) = P(M_2 \mid W_1)P(W_1) + P(W_2 \mid M_1)P(M_1) = \dfrac{7}{9} \cdot \dfrac{3}{10} + \dfrac{1}{3} \cdot \dfrac{7}{10} = \dfrac{7}{15} \cong 46.7\%$.

Solution 2: The event that one finalist is a woman and the other is a man is the complement of the event that either both are women or both are men. Because those events are mutually disjoint, the probability that one finalist is a woman and the other is a man is $1 - P(W_1 \cap W_2) - P(M_1 \cup M_2) = 1 - P(W_2 \mid W_1)P(W_1) - P(M_2 \mid M_1)P(M_1) = 1 - \dfrac{2}{9} \cdot \dfrac{3}{10} - \dfrac{2}{3} \cdot \dfrac{7}{10} = \dfrac{7}{15} \cong 46.7\%$.

8. *Proof*: Suppose that a sample space S is a union of two disjoint events B_1 and B_2, that A is an event in S with $P(A) \neq 0$, and that $P(B_k) \neq 0$ for $k = 1$ and $k = 2$. Because B_1 and B_2 are disjoint, the same reasoning as in Example 6.9.5 establishes that $A = (A \cap B_1) \cup (A \cap B_2)$ and $(A \cap B_1) \cap (A \cap B_2) = \emptyset$. Thus $P(A) = P(A \cap B_1) + P(A \cap B_2)$. Moreover, for each $k = 1$ or 2, by definition of conditional probability, we have both that $P(B_k \mid A) = \dfrac{P(B_k \cap A)}{P(A)} = \dfrac{P(A \cap B_k)}{P(A)}$ and that $P(A \cap B_k) = P(A \mid B_k)P(B_k)$. Putting these results together gives that for each $k = 1$ or 2,

$$P(B_k \mid A) = \frac{P(A \cap B_k)}{P(A)} = \frac{P(A \mid B_k)P(B_k)}{P(A \cap B_1) + P(A \cap B_2)} = \frac{P(A \mid B_k)P(B_k)}{P(A \mid B_1)P(B_1) + P(A \mid B_2)P(B_2)},$$

which is Bayes' theorem for $n = 2$.

9. *Proof*: Let S be a sample space, let A be an event in S with $P(A) \neq 0$, and suppose that $B_1, B_2, \ldots, B_n$ are mutually disjoint events in S such that $S = B_1 \cup B_2 \cup \cdots \cup B_n$. By the generalized distributive law for sets, $A = A \cap S = A \cap (B_1 \cup B_2 \cup \cdots \cup B_n) = (A \cap B_1) \cup (A \cap B_2) \cup \cdots \cup (A \cap B_n)$. Also because $B_1, B_2, \ldots, B_n$ are mutually disjoint and by the associative, commutative, and universal bound laws for sets, $(A \cap B_i) \cap (A \cap B_j) = (A \cap A) \cap (B_i \cap B_j) = (A \cap A) \cap \emptyset = \emptyset$ for all integers i and j with $1 \leq i \leq n$, $1 \leq j \leq n$, and $i \neq j$. Thus the sets $(A \cap B_1), (A \cap B_2), \ldots, (A \cap B_n)$ are also mutually disjoint, and so, by substitution and the definition of conditional probability,

$$
\begin{aligned}
P(A) &= P((A \cap B_1) \cup (A \cap B_2) \cup \cdots \cup (A \cap B_n)) \\
&= P(A \cap B_1) + P(A \cap B_2) + \cdots + P(A \cap B_n) \\
&= P(A \mid B_1)P(B_1) + P(A \mid B_2)P(B_2) + \cdots + P(A \mid B_n)P(B_n).
\end{aligned}
$$

Also by definition of conditional probability,

$$P(A \mid B_k)P(B_k) = \frac{P(A \cap B_k)}{P(B_k)}P(B_k) = P(A \cap B_k).$$

Putting these results together gives

$$P(B_k \mid A) = \frac{P(A \cap B_k)}{P(A)} = \frac{P(A \mid B_k)P(B_k)}{P(A \mid B_1)P(B_1) + P(A \mid B_2)P(B_2) + \cdots + P(A \mid B_n)P(B_n)}$$

[as was to be shown].

11. *a.* Let B_1 be the event that the first urn is chosen, B_2 the event that the second urn is chosen, and A the event that the chosen ball is blue. Then

$$P(A \mid B_1) = \frac{4}{20} \quad \text{and} \quad P(A \mid B_2) = \frac{10}{19}.$$

$$P(A \cap B_1) = P(A \mid B_1)P(B_1) = \frac{4}{20} \cdot \frac{1}{2} = \frac{1}{10}.$$

Also

$$P(A \cap B_2) = P(A \mid B_2)P(B_2) = \frac{10}{19} \cdot \frac{1}{2} = \frac{5}{19}.$$

Now A is the disjoint union of $A \cap B_1$ and $A \cap B_2$. So

$$P(A) = P(A \cap B_1) + P(A \cap B_2) = \frac{1}{10} + \frac{5}{19} = \frac{69}{190} \cong 36.3\%.$$

So the probability that the chosen ball is blue is approximately 36.3%.

b. Solution 1 (using Bayes' theorem): Given that the chosen ball is blue, the probability that it came from the first urn is $P(B_1 \mid A)$. By Bayes' theorem and the computations in part (a),

$$P(B_1 \mid A) = \frac{P(A \mid B_1)P(B_1)}{P(A \mid B_1)P(B_1) + P(A \mid B_2)P(B_2)} = \frac{\dfrac{1}{10}}{\dfrac{1}{10} + \dfrac{5}{19}} = \frac{19}{69} \cong 27.5\%.$$

Solution 2 (without explicit use of Bayes' theorem): Given that the chosen ball is blue, the probability that it came from the first urn is $P(B_1 \mid A)$. By the results of part (a), $P(B_1 \mid A) = \dfrac{P(A \cap B_1)}{P(A)} = \dfrac{\dfrac{1}{10}}{\dfrac{69}{190}} = \dfrac{19}{69} \cong 27.5\%.$

12. *a.* Let B_1 be the event that the first urn is chosen, B_2 the event that the second urn is chosen, and A the event that the chosen ball is green. Then

$$P(B_1) = \frac{4}{10} = \frac{2}{5}, \qquad P(B_2) = \frac{6}{10} = \frac{3}{5}, \qquad P(A \mid B_1) = \frac{25}{35} \quad \text{and} \quad P(A \mid B_2) = \frac{15}{37}.$$

$$P(A \cap B_1) = P(A \mid B_1)P(B_1) = \frac{25}{35} \cdot \frac{2}{5} = \frac{2}{7}.$$

Also

$$P(A \cap B_2) = P(A \mid B_2)P(B_2) = \frac{15}{37} \cdot \frac{3}{5} = \frac{9}{37}.$$

Now A is the disjoint union of $A \cap B_1$ and $A \cap B_2$. So

$$P(A) = P(A \cap B_1) + P(A \cap B_2) = \frac{2}{7} + \frac{9}{37} = \frac{137}{259} \cong 52.9\%.$$

So the probability that the chosen ball is green is approximately 52.9%.

b. Solution 1 (using Bayes' theorem): Given that the chosen ball is green, the probability that it came from the first urn is $P(B_1 \mid A)$. By Bayes' theorem and the computations in part (a),

$$P(B_1 \mid A) = \frac{P(A \mid B_1)P(B_1)}{P(A \mid B_1)P(B_1) + P(A \mid B_2)P(B_2)} = \frac{\dfrac{2}{7}}{\dfrac{2}{7} + \dfrac{9}{37}} = \frac{74}{137} \cong 54.0\%.$$

Solution 2 (without explicit use of Bayes' theorem): Given that the chosen ball is green, the probability that it came from the first urn is $P(B_1 \mid A)$. By the results of part (a),

$$P(B_1 \mid A) = \frac{P(A \cap B_1)}{P(A)} = \frac{\dfrac{2}{7}}{\dfrac{137}{259}} = \frac{74}{137} \cong 54.0\%.$$

14. Let B_1 be the event that the part came from the first factory, B_2 the event that the part came from the second factory, and A the event that a part chosen at random from the 180 is defective.

a. The probability that a part chosen at random from the 180 is from the first factory is $P(B_1) = \frac{100}{180}$.

b. The probability that a part chosen at random from the 180 is from the second factory is $P(B_2) = \frac{80}{180}$.

c. The probability that a part chosen at random from the 180 is defective is $P(A)$. Because 2% of the parts from the first factory and 5% of the parts from the second factory are defective, $P(A \mid B_1) = \dfrac{2}{100}$ and $P(A \mid B_2) = \dfrac{5}{100}$. By definition of conditional probability,

$$P(A \cap B_1) = P(A \mid B_1)P(B_1) = \frac{2}{100} \cdot \frac{100}{180} = \frac{1}{90}$$
$$P(A \cap B_2) = P(A \mid B_2)P(B_2) = \frac{5}{100} \cdot \frac{80}{180} = \frac{2}{90}.$$

Now because B_1 and B_2 are disjoint and because their union is the entire sample space, A is the disjoint union of $A \cap B_1$ and $A \cap B_2$. Thus the probability that

$$P(A) = P(A \cap B_1) + P(A \cap B_2) = \frac{1}{90} + \frac{2}{90} = \frac{3}{90} \cong 3.3\%.$$

d. Solution 1 (using Bayes' theorem): Given that the chosen part is defective, the probability that it came from the first factory is $P(B_1 \mid A)$. By Bayes' theorem and the computations in part (a),

$$P(B_1 \mid A) = \frac{P(A \mid B_1)P(B_1)}{P(A \mid B_1)P(B_1) + P(A \mid B_2)P(B_2)} = \frac{\dfrac{1}{90}}{\dfrac{1}{90} + \dfrac{2}{90}} = \frac{1}{3} \cong 33.3\%.$$

Solution 2 (without explicit use of Bayes' theorem): Given that the chosen ball is green, the probability that it came from the first urn is $P(B_1 \mid A)$. By the results of part (a),

$$P(B_1 \mid A) = \frac{P(A \cap B_1)}{P(A)} = \frac{\dfrac{1}{90}}{\dfrac{3}{90}} = \frac{1}{3} \cong 33.3\%.$$

15. Let B_1 be the event that a randomly chosen piece of produce is from supplier X, B_2 the event that a randomly chosen piece of produce is from supplier Y, B_3 the event that a randomly chosen piece of produce is from supplier Z, and A the event that a randomly chosen piece of

produce purchased from the store is superior grade. From the information given in the problem statement, we know that $P(B_1) = 20\% = 0.2$, $P(B_2) = 45\% = 0.45$, $P(B_3) = 35\% = 0.35$, $P(A \mid B_1) = 12\% = 0.12$, $P(A \mid B_2) = 8\% = 0.08$, and $P(A \mid B_3) = 15\% = 0.15$.

a. By definition of conditional probability,

$$P(A \cap B_1) = P(A \mid B_1)P(B_1) = 0.12 \cdot 0.2 = 0.024,$$
$$P(A \cap B_2) = P(A \mid B_2)P(B_2) = 0.08 \cdot 0.45 = 0.036,$$
$$P(A \cap B_3) = P(A \mid B_3)P(B_3) = 0.15 \cdot 0.35 = 0.0525.$$

Now because B_1, B_2, and B_3 are disjoint and because their union is the entire sample space, A is the disjoint union of $A \cap B_1$, $A \cap B_2$, and $A \cap B_3$. Thus

$$P(A) = P(A \cap B_1) + P(A \cap B_2) + P(A \cap B_3) = 0.024 + 0.036 + 0.0525 = 0.1125 = 11.25\%.$$

b. Solution 1 (by direct application of Bayes' theorem): Given that the chosen part is defective, the probability that it came from the first factory is $P(B_1 \mid A)$. By Bayes' theorem,

$$
\begin{aligned}
P(B_1 \mid A) &= \frac{P(A \mid B_1)P(B_1)}{P(A \mid B_1)P(B_1) + P(A \mid B_2)P(B_2) + P(A \mid B_3)P(B_3)} \\[2mm]
&= \frac{0.12 \cdot 0.2}{0.12 \cdot 0.2 + 0.08 \cdot 0.45 + 0.15 \cdot 0.35} \\[2mm]
&\cong 21.3\%.
\end{aligned}
$$

Solution 2 (without explicit use of Bayes' theorem): Given that the chosen ball is green, the probability that it came from the first urn is $P(B_1 \mid A)$. By definition of conditional probability and the results of part (a), $P(B_1 \mid A) = \dfrac{P(A \cap B_1)}{P(A)} = \dfrac{0.024}{0.1125} \cong 21.3\%$.

17. *Proof*: Suppose A and B are events in a sample space S, and $P(A \cap B) = P(A) \cdot P(B)$, $P(A) \neq 0$, and $P(B) \neq 0$. Applying the hypothesis to the definition of conditional probability gives $P(A \mid B) = \dfrac{P(A \cap B)}{P(B)} = \dfrac{P(A) \cdot P(B)}{P(B)} = P(A)$ and $P(B \mid A) = \dfrac{P(A \cap B)}{P(A)} = \dfrac{P(A) \cdot P(B)}{P(A)} = P(B)$.

19. The sample space $S = \{HHH, HHT, HTH, HTT, THH, THT, TTH, TTT\}$, $A = \{HHH, HHT, HTH, HTT\}$, $B = \{HHT, HTH, THH, TTT\}$, and $A \cap B = \{HHT, HTH\}$. Then $P(A) = \dfrac{4}{8} = \dfrac{1}{2}$, $P(B) = \dfrac{4}{8} = \dfrac{1}{2}$, and $P(A \cap B) = \dfrac{2}{8} = \dfrac{1}{4}$. Hence $P(A \mid B) = \dfrac{P(A \cap B)}{P(B)} = \dfrac{1/4}{1/2} = \dfrac{1}{2} = P(A)$ and $P(B \mid A) = \dfrac{P(A \cap B)}{P(A)} = \dfrac{1/4}{1/2} = \dfrac{1}{2} = P(B)$.

20. If A and B are events in a sample space and $A \cap B = \emptyset$ and A and B are independent, then (by definition of independence) $P(A \cap B) = P(A)P(B)$, and (because $A \cap B = \emptyset$) $P(A \cap B) = 0$. Hence $P(A)P(B) = 0$, and so (by the zero product property) either $P(A) = 0$ or $P(B) = 0$.

21. *Alternative proof to that given in Appendix B*: Suppose A and B are independent events in a sample space S. Then $P(A \cap B) = P(A)P(B)$. In case $P(B) = 0$, then, by the result of exercise 11, Section 6.8, $P(A^c \cap B) = 0$ (because $A^c \cap B \subseteq B$). Thus, $P(A^c \cap B) = 0 = P(A^c) \cdot 0 = P(A^c)P(B)$. In case $P(B) \neq 0$,

$$
\begin{aligned}
P(A^c \cap B) &= P(A^c|B)P(B) && \text{by formula 6.9.2} \\
&= [1 - P(A|B)]P(B) && \text{by exercise 3a} \\
&= [1 - P(A)]P(B) && \text{by the result of exercise 17} \\
&= P(A^c)P(B) && \text{by the formula for the complement of an event (6.8.1).}
\end{aligned}
$$

It follows by definition of independence that in either case A^c and B are independent.

22. *Proof 1*: Suppose A and B are independent events in a sample space S. By Example 6.9.5, A and B^c are independent. Now, in general, if events C and D are independent then so are events D and C (because $P(C)P(D) = P(D)P(C)$), and hence B^c and A are independent. Thus, by Example 6.9.5 a second time (with B^c playing the role of A and A playing the role of B) B^c and A^c are independent, and so A^c and B^c are independent.

    Proof 2: Suppose A and B are independent events in a sample space S. It follows by definition of independence, De Morgan's law, and the formulas for the probability for the complement of an event and the probability of a general union of two events that

    $$P(A^c \cap B^c) = P((A \cup B)^c) = 1 - P(A \cup B) = 1 - [P(A) + P(B) - P(A \cap B)]$$

    $$= 1 - [P(A) + P(B) - P(A)P(B)] = 1 - P(A) - P(B) + P(A)P(B) = (1 - P(A)) - P(B)(1 - P(A))$$

    $$= P(A^c)(1 - P(B)) = P(A^c)P(B^c).$$

    Hence A^c and B^c are independent.

24. Let A be the event that a randomly chosen error is missed by proofreader X, and let B be the event that the error is missed by proofreader Y. Then $P(A) = 0.12$ and $P(B) = 0.15$.

    a. Because the proofreaders work independently, $P(A \cap B) = P(A)P(B)$. Hence the probability that the error is missed by both proofreaders is $P(A \cap B) = P(A)P)B) = (0.12)(0.15) = 0.018 = 1.8\%$.

    b. Assuming that the manuscript contains 1000 typographical errors, the expected number of missed errors is $1000 \cdot 0.018\% = 18$.

25. Let H_i be the event that the result of toss i is heads, and let T_i be the event that the result of toss i is tails. Then $P(H_i) = 0.7$ and $P(T_i) = 0.3$ for $i = 1, 2$.

    a. Because the results of the tosses are independent, the probability of obtaining exactly two heads is $P(H_1 \cap H_2) = P(H_1)P(H_2) = 0.7 \cdot 0.7 = 0.49 = 49\%$.

    c. Because the results of the tosses are independent, the probability of obtaining no heads is $P(T_1 \cap T_2) = P(T_1)P(T_2) = 0.3 \cdot 0.3 = 0.09 = 9\%$.

    d. By the formula for the complement of an event, the probability of obtaining at least one head is $P(T_1 \cap T_2)^c) = 1 - P(T_1 \cap T_2) = 1 - 0.09 = 0.91 = 91\%$.

26. *One possible example among many*: Consider the possible outcomes obtained when a coin is tossed three times. Let A be the event that a head occurred on the first toss, B the event that at least two heads were obtained, and C the event that an odd number of heads were obtained. Then $A = \{HHH, HHT, HTH, HTT\}$, $B = \{HHH, HHT, HTH, THH\}$, and $C = \{HHH, HTT, THT, TTH\}$. Thus $A \cap B = \{HHH, HHT, HTH\}$ and $A \cap B \cap C = \{HHH\}$. Hence $P(A) = P(B) = P(C) = 4/8 = 1/2$, $P(A \cap B) = 3/8$, and $P(A \cap B \cap C) = 1/8$. But $1/8 = (1/2)(1/2)(1/2)$, and so $P(A \cap B \cap C) = P(A)P(B)P(C)$. However, $P(A \cap B) = 3/8 \neq (1/2)(1/2) = P(A)P(B)$, and so A and B are not pairwise independent.

27. *Solution*: The family could have two boys, two girls, or one boy and one girl. Let the subscript 1 denote the firstborn child (understanding that in the case of twins this might be by only a few moments), and let the subscript 2 denote the secondborn child. Then we can let $(B_1 G_2, B_1)$ denote the outcome that the firstborn child is a boy, the secondborn is a girl, and the child you meet is the boy. Similarly, we can let $(B_1 B_2, B_2)$ denote the outcome that both the firstborn and the secondborn are boys and the child you meet is the secondborn boy. When this notational scheme is used for the entire set of possible outcomes for the genders of the children and the gender of the child you meet, all outcomes are equally likely and the sample space is denoted by

    $$\{(B_1 B_2, B_1), (B_1 B_2, B_2), (B_1 G_2, B_1), (B_1 G_2, G_2), (G_1 B_2, G_1), (G_1 B_2, B_2), (G_1 G_2, G_1), (G_1 G_2, G_2)\}.$$

    The event that you meet one of the children and it is a boy is

$$\{(B_1 B_2, B_1), (B_1 B_2, B_2), (B_1 G_2, B_1), (G_1 B_2, B_2)\}.$$

The probability of this event is $4/8 = 1/2$.

Discussion: An intuitive way to see this conclusion is to realize that the fact that you happen to meet one of the children see that it is a boy gives you no information about the gender of the other child. Because each of the children is equally likely to be a boy, the probability that the other child is a boy is $1/2$. Consider the following situation in which the probabilities are identical to the situation described in the exercise. A person tosses two fair coins and immediately covers them so that you cannot see which faces are up. The person then reveals one of the coins, and you see that it is heads. This action on the person's part has given you no information about the other coin; the probability that the other coin has also landed heads up is $1/2$.

28. *b.* Let H_i be the event that the result of toss i is heads, and let T_i be the event that the result of toss i is tails for $i = 1, 2, \ldots, 10$. By definition of mutual independence,

$P(\text{obtaining exactly ten heads}) = P(H_1 H_2 H_3 H_4 H_5 H_6 H_7 H_8 H_9 H_{10})$
$= P(H_1)P(H_2)P(H_3)P(H_4)P(H_5)P(H_6)P(H_7)P(H_8)P(H_9)P(H_{10}) = (0.7)^{10} \cong 0.028 = 2.8\%.$

c. The event of obtaining no heads is the same as the event of obtaining all tails:

$$P(T_1 T_2 T_3 T_4 T_5 T_6 T_7 T_8 T_9 T_{10}) = \prod_{i=1}^{10} P(T_i) = (0.3)^{10} \cong 0.000006 = 0.0006\%.$$

d. The probability of obtaining at least one head is the complement of the event of obtaining all tails. So, by the formula for the complement of an event, $P(\text{obtaining no heads}) = 1 - P(\text{obtaining all tails}) = 1 - P(T_1 T_2 T_3 T_4 T_5 T_6 T_7 T_8 T_9 T_{10}) = 1 - (0.3)^{10} \cong 0.999994 = 99.9994\%.$

29. *b.* The event that at least one of the ten items is defective is the complement of the event that none is defective, which, by part (a) is approximately 73.7%. So $P(\text{at least one is defective}) \cong 1 - 73.7\% = 26.3\%.$

c. $P(4 \text{ defectives}) = \begin{bmatrix} \text{the number of ways 4} \\ \text{defectives can be obtained} \\ \text{in a sample of 10 items} \end{bmatrix} P(\text{defective})^4 P(\text{not defective})^6$

$= \binom{10}{4} 0.03^4 \cdot 0.97^6 = 210 \cdot 0.03^4 \cdot 0.97^6 \cong 0.000142$

d. By part (a), $P(\text{no defectives}) \cong 0.737.$

$P(1 \text{ defective}) = \begin{bmatrix} \text{the number of ways 1} \\ \text{defective can be obtained} \\ \text{in a sample of 10 items} \end{bmatrix} P(\text{defective})^1 P(\text{not defective})^9$

$= \binom{10}{1} 0.03^1 \cdot 0.97^9 = 10 \cdot 0.03^1 \cdot 0.97^9 \cong 0.228$

$P(2 \text{ defectives}) = \begin{bmatrix} \text{the number of ways 2} \\ \text{defectives can be obtained} \\ \text{in a sample of 10 items} \end{bmatrix} P(\text{defective})^2 P(\text{not defective})^8$

$= \binom{10}{2} 0.03^2 \cdot 0.97^8 = 45 \cdot 0.03^2 \cdot 0.97^8 \cong 0.032$

$P(\text{at most 2 defectives}) = P(0 \text{ defectives}) + P(1 \text{ defective}) + P(2 \text{ defectives}) = 0.737 + 0.228 + 0.032 \cong 0.997$

30. *a.* $P(0 \text{ false positives}) = \begin{bmatrix} \text{the number of ways 0 false} \\ \text{positives can be obtained} \\ \text{over a ten-year period} \end{bmatrix} \left(P\left(\begin{array}{c} \text{false} \\ \text{positive} \end{array} \right) \right)^0 \left(P\left(\begin{array}{c} \text{not a false} \\ \text{positive} \end{array} \right) \right)^{10}$

$= \binom{10}{0} 0.96^{10} = 1 \cdot 0.96^{10} \cong 0.665 = 66.5\%$

$$c. \ P(2 \text{ false positives}) = \begin{bmatrix} \text{the number of ways 2 false} \\ \text{positives can be obtained} \\ \text{over a ten-year period} \end{bmatrix} \left(P \begin{pmatrix} \text{false} \\ \text{positive} \end{pmatrix} \right)^2 \left(P \begin{pmatrix} \text{not a false} \\ \text{positive} \end{pmatrix} \right)^8$$

$$= \binom{10}{2} 0.04^2 \cdot 0.96^8 = 45 \cdot 0.04^2 \cdot 0.96^8 = 0.0594 \cong 5.2\%$$

d. Let T be the event that a woman's test result is positive one year, and let C be the event that the woman has breast cancer.

(i) By Bayes' formula, the probability of C given T is

$$\begin{aligned} P(C|T) &= \frac{P(T|C)P(C)}{P(T|C)P(C) + P(T|C^c)P(C^c)} \\ &= \frac{(0.98)(0.0002)}{(0.98)(0.0002) + (0.04)(0.9998)} \\ &\cong 0.00488 = 4.88\%. \end{aligned}$$

(ii) The event that a woman's test result is negative one year is T^c. By Bayes formula, the probability of C given T^c is

$$\begin{aligned} P(C|T^c) &= \frac{P(T^c|C)P(C)}{P(T^c|C)P(C) + P(T^c|C^c)P(C^c)} \\ &= \frac{(0.02)(0.0002)}{(0.02)(0.0002) + (0.98)(0.9998)} \\ &\cong 0.000004 = 0.0004\%. \end{aligned}$$

Chapter 7: Functions

Students often come out of high school mathematics courses identifying functions with formulas. The aim of Section 7.1 is to promote a broader view of the function concept and to give students experience with the wide variety of functions that arise in discrete mathematics. Representation of functions by arrow diagrams is emphasized to prepare the way for the discussion of one-to-one and onto functions in Section 7.2. Students do not usually find Section 7.1 difficult, but many seem to need the practice working with functions defined on, say, power sets or sets of strings to be able to reason effectively with such functions in later sections of the chapter. For instance, if you are planning to assign exercise 24 in Section 7.2, it is desirable to have previously assigned exercise 13 in Section 7.1.

Section 7.2 focuses on function properties. As they are learning about one-to-one and onto functions in this section, a significant number of students benefit from some explicit review of logical principles such as the negation of $\forall$, $\exists$, and if-then statements and the equivalence of a conditional statement and its contrapositive. These logical principles are needed, of course, to understand the equivalence of the two forms of the definition of one-to-one and what it means for a function not to be one-to-one or onto. This is a good opportunity to solicit student participation since at this point in the course students, in theory, know the logic, and so you can ask them to recall it and apply it to the study of function properties themselves. Because the techniques used to test for injectivity and surjectivity and to find inverse functions are quite different for functions with finite and infinite domains, examples involving both kinds of functions are discussed in this section.

Section 7.3 on the pigeonhole principle provides a break from the emphasis on theory in the other sections of the chapter, and many students appreciate the change of focus at this point. The range of difficulty of the problems is deliberately broad to enable you to tailor your choice of exercises to the abilities of your students.

Sections 7.4 and 7.5 go together in the sense that the relations between one-to-one and onto functions and composition of functions developed in Section 7.4 are used to prove the fundamental theorem about cardinality in Section 7.5. The proofs that a composition of one-to-one functions is one-to-one or that a composition of onto functions is onto (and the related exercises) test the degree to which students have learned to instantiate mathematical definitions in abstract contexts, apply the method of generalizing from the generic particular in a sophisticated setting, develop mental models of mathematical concepts that are both vivid and generic enough to reason with, and create moderately complex chains of deductions.

There are always students who respond with enthusiasm to the idea of different sizes of infinity discussed in Section 7.5. When covering the proof of the uncountablity of the reals in this section, it is of interest to point out the connections that link Russell's paradox, the halting problem, and the Cantor diagonalization argument.

Comments on Exercises:

Exercises #6 in Section **7.1** and #10 and #11 in Section **7.2** explore the question of how many functions of certain types there are from a finite set of one size to a finite set of a (possibly different) size. Exercise #11 in Section **7.1** on the identity function is a warm-up for #13 of **Section 7.4**. Exercise #13 in Section **7.1** on a function defined on a power set prepares students for #24 and #46 in Section **7.2**. Exercise #14 in Section **7.1** on values of a function defined on a set of strings leads students into #22, #23, #25, #26, #44, #45 and #47 in Section **7.2**. Exercise #27 in Section **7.1** integrates topics from Chapters 6 and 7 by relating permutations and functions. The results of exercises #29-31 in Section **7.2** are used for some calculations in Sections **8.2, 9.4,** and **9.5**. Exercises #2-4 and #15 in Section **7.2** are designed to counteract a common linguistic misunderstanding about the definition of one-to-one (that a function $f: X \to Y$ is one-to-one if each element of X is sent to exactly one element of Y). Exercise #52 in Section **7.2** integrates topics from Chapters 5, 6, and 7. The fact that a set with n elements has 2^n subsets is first proved by

induction in Section 5.3. In Section 6.7 a second proof is given using the binomial theorem. This exercise leads students through a third proof that works by setting up a one-to-one correspondence between subsets and strings of 0's and 1's of length n.

Section 7.1

2. *a.* domain of $g = \{1, 3, 5\}$, co-domain of $g = \{a, b, c, d\}$ *b.* $g(1) = g(3) = g(5) = b$

    c. range of $g = \{b\}$ *d.* no, yes   *e.* inverse image of $b = \{1, 3, 5\}$, inverse image of $c = \emptyset$

    f. $\{(1, b), (3, b), (5, b)\}$

3. *c.* This arrow diagram associates both 1 and 2 to 4. So this diagram does not define a function.

    d. This arrow diagram determines a function. Each element in X is related to one and only one element in Y.

    e. In this arrow diagram, the element 2 in X is not related to any element in Y. So this diagram does not define a function.

4. *b* False. The definition of function does not allow an element of the domain to be associated to two different elements of the co-domain, but it does allow an element of the co-domain to be the image of more than one element in the domain. For example, let $X = \{1, 2\}$ and $Y = \{a\}$ and define $f \colon X \rightarrow Y$ by specifying that $f(1) = f(2) = a$. Then f defines a function from X to Y for which a has two unequal preimages.

    d. This statement is false. Each input to a function is related to only one output.

5. *b.* There is just one function from X to Y. It is represented by the arrow diagram shown below.
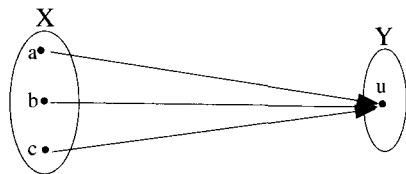
    c. There are eight functions from X to Y. They are represented by the arrow diagrams shown below.
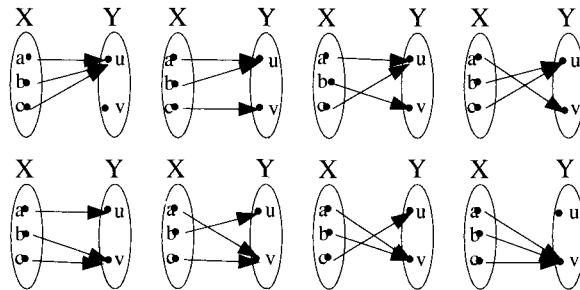
6. *b.* The answer is $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^5 = 32$. The explanation is the same as that in the answer to part (c) below, but with $n = 2$ and $m = 5$.

    c. The answer is n^m because the m elements of the domain can be placed in order and the process of constructing a function can be thought of as an m-step operation where, for each i from 1 to m, the ith step is to choose one of the n elements of the co-domain to be the image of the ith element of the domain. Since there are n ways to perform each of the m steps of the operation, the entire operation can be performed in $n \cdot n \cdots n$ (m factors) ways. (*Brief version of this explanation*: The answer is n^m because each of the m elements of the domain can be sent to any one of n possible elements in the co-domain.)

8. No. For instance, $H(3) = \lfloor 3 \rfloor + 1 = 3 + 1 = 4$, whereas $K(3) = \lceil 3 \rceil = 3$. In fact, $H(x) = K(x) \Leftrightarrow x$ is not an integer.

10. No. For instance, let F and G be defined by the rules $F(x) = x$ and $G(x) = 0$ for all real numbers x. Then $(F - G)(2) = F(2) - G(2) = 2 - 0 = 2$, whereas $(G - F)(2) = G(2) - F(2) = 0 - 2 = -2$, and $2 \neq -2$. In fact, $G - F = F - G \Leftrightarrow F = G$.

11. *c.* $i_{\mathbf{Z}}(K(t)) = K(t)$ *d.* $i_{\mathbf{Z}}(U_{kj}) = U_{kj}$

12. *b.* Define $F \colon \mathbf{Z}^{nonneg} \to \mathbf{R}$ as follows: for each nonnegative integer n, $F(n) = (-1)^n(2n)$.

13. *b.* $F(\emptyset) = 0$ (because 0 is an even number)   *d.* $F(\{2,3,4,5\}) = 0$

14. *b.* $g(aba) = aba$, $g(bbab) = babb$, $g(b) = b$ The range of g is the set of all strings of a's and b's, which equals S.

15. *b.* $5^{-2} = 1/25$

    d. the exponent to which 3 must be raised to obtain 3^n is n

    e. $4^0 = 1$

16. *b.* $\log_2 1024 = 10$ because $2^{10} = 1024$

    d. $\log_2 1 = 0$ because $2^0 = 1$

    e. $\log_{10} \dfrac{1}{10} = -1$ because $10^{-1} = \dfrac{1}{10}$

    f. $\log_3 3 = 1$ because $3^1 = 3$

    g. $\log_2 2^k = k$ because the exponent to which 2 must be raised to obtain 2^k is k

18. *Proof*: Let b be any positive real number with $b \neq 1$. Then $b^0 = 1$, and so $\log_b 1 = 0$. (Note that we do not allow b to equal 1 here because $\log_b$ is not defined for $b = 1$.)

20. *Proof*: Suppose that $\log_3(7)$ is rational. Then $\log_3(7) = a/b$ for some integers a and b with $b \neq 0$. Since logarithms are always positive, we may assume that a and b are both positive. By definition of logarithm, $3^{a/b} = 7$. Raising both sides to the bth power gives $3^a = 7^b$. Let $N = 3^a = 7^b$, and consider the prime factorization of N. Since $N = 3^a$, the prime factors of N are all 3. On the other hand, since $N = 7^b$, the prime factors of N are all 7. This contradicts the unique factorization theorem which states that the prime factors of any integer greater than 1 are unique except for the order in which they are written. Hence the supposition is false, and so $\log_3(7)$ is irrational.

22. Since $\log_b y = 2$, then $b^2 = y$. Hence $(b^2)^1 = y$, and so $log_{b^2}(y) = 1$.

23. *b.* $p_2(2, y) = y$, $p_2(5, x) = x$ The range of p_2 is $\{x, y\}$.

24. *b.* $mod(59, 8) = 3$, $div(59, 8) = 7$ *c.* $mod(30, 5) = 0$, $div(30, 5) = 6$

25. *b.* $E(1010) = 111000111000$, $D(000000111111) = 0011$

26. *b.* $H(00110, 10111) = 2$

27. *b.*

1	2	3	4		1	2	3	4
↓	↓	↓	↓		↓	↓	↓	↓
1	2	3	4		3	2	1	4

    d.

1	2	3	4		1	2	3	4		1	2	3	4
↓	↓	↓	↓		↓	↓	↓	↓		↓	↓	↓	↓
2	3	4	1		3	4	1	2		4	1	2	3

```
1  2  3  4       1  2  3  4       1  2  3  4
↓  ↓  ↓  ↓       ↓  ↓  ↓  ↓       ↓  ↓  ↓  ↓
2  1  4  3       3  1  4  2       4  3  1  2

1  2  3  4       1  2  3  4       1  2  3  4
↓  ↓  ↓  ↓       ↓  ↓  ↓  ↓       ↓  ↓  ↓  ↓
2  4  1  3       3  4  2  1       4  3  2  1
```
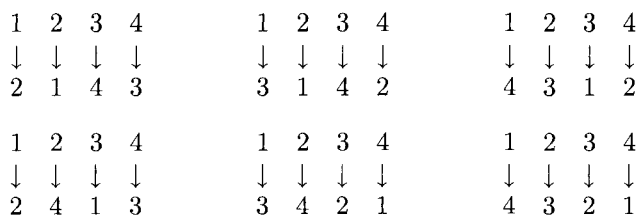
28. *b.*
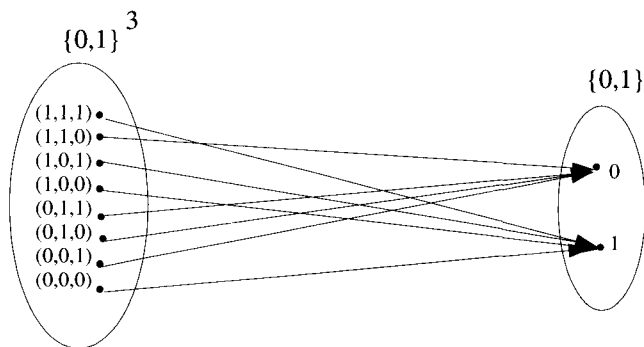
29.

input	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}
1 1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
1 0	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
0 1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1 1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

30. *b.*

input			output
x_1	x_2	x_3	f
1	1	1	1
1	1	0	1
1	0	1	0
1	0	0	0
0	1	1	1
0	1	0	1
0	0	1	0
0	0	0	0

32. Student D is correct. Suppose h were well-defined. Then $h(\frac{1}{2}) = h(\frac{2}{4})$ because $\frac{1}{2} = \frac{2}{4}$. But $h(\frac{1}{2}) = \frac{1}{2}$ and $h(\frac{2}{4}) = \frac{2^2}{4} = 1$, and $\frac{1}{2} \neq 1$. *[This contradiction shows that the supposition that h is well-defined is false, and so h is not well-defined.]*

33. f is not well defined because $f(n) \notin S$ for many values of n in S. For instance, $f(100\,000) = (100\,000)^2 = 10\,000\,000\,000 \notin S$.

34. *a.*

$$\chi_A(u) \cdot \chi_B(u) = \begin{cases} 1 \cdot 1 & \text{if } u \in A \text{ and } u \in B \\ 1 \cdot 0 & \text{if } u \in A \text{ and } u \notin B \\ 0 \cdot 1 & \text{if } u \notin A \text{ and } u \in B \\ 0 \cdot 0 & \text{if } u \notin A \text{ and } u \notin B \end{cases}$$

$$= \begin{cases} 1 & \text{if } u \in A \cap B \\ 0 & \text{if } u \notin A \cap B \end{cases}$$

$$= \chi_{A \cap B}(u)$$

b.

$$\chi_A(u) + \chi_B(u) - \chi_A(u) \cdot \chi_B(u) = \begin{cases} 1 + 1 - 1 \cdot 1 & \text{if } u \in A \text{ and } u \in B \\ 1 + 0 - 1 \cdot 0 & \text{if } u \in A \text{ and } u \notin B \\ 0 + 1 - 0 \cdot 1 & \text{if } u \notin A \text{ and } u \in B \\ 0 + 0 - 0 \cdot 0 & \text{if } u \notin A \text{ and } u \notin B \end{cases}$$

$$= \begin{cases} 1 & \text{if } u \in A \text{ and } u \in B \\ 1 & \text{if } u \in A \text{ and } u \notin B \\ 1 & \text{if } u \notin A \text{ and } u \in B \\ 0 & \text{if } u \notin A \text{ and } u \notin B \end{cases}$$

$$= \begin{cases} 1 & \text{if } u \in A \cup B \\ 0 & \text{if } u \notin A \cup B \end{cases}$$

$$= \chi_{A \cup B}(u)$$

35. *d.* $\phi(12) = 4$ *[because 1, 5, 7, and 11 have no common factors with 12 other than ± 1]*

e. $\phi(11) = 10$ *[because 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, and 11 have no common factors with 11 other than ± 1]*

f. $\phi(1) = 1$ *[because 1 is the only positive integer which has no common factors with 1 other than ± 1]*

37. *Proof:* By exercise 36 with $p = 2$, if n is and integer with $n \geq 1$, then $\phi(2^n) = 2^n - 2^{n-1} = 2^{n-1}(2-1) = 2^{n-1}$. Given any odd integer $n \geq 3$, $n = 2k + 1$ for some integer $k \geq 1$. Hence $\phi(2^n) = 2^{n-1} = 2^{(2k+1)-1} = 2^{2k} = (2^k)^2$, which is a perfect square. Thus $\phi(2^n)$ is a perfect square for each of the infinitely many odd integers $n \geq 3$.

38. *Proof:* Given any integer n with $n = pq$, where p and q are distinct prime numbers, let A be the set of all positive integers less than or equal to n that are divisible by p and let B be the set of all positive integers less than or equal to n that are divisible by q. Note that $A = \{p, 2p, 3p, \ldots, qp\}$, $B = \{q, 2q, 3q, \ldots, pq\}$, and $A \cap B = \{pq\}$. By definition of ϕ,

$$\phi(n) = n - [n(A \cup B)]$$

$$= n - [n(A) + n(B) - n(A \cap B)] \quad \text{by the inclusion/exclusion formula}$$

$$= pq - [q + p - 1]$$

$$= (p-1)(q-1)$$

39. *Proof:* Given any integer n with $n = pqr$, where p, q, and r are distinct prime numbers, let A be the set of all positive integers less than or equal to n that are divisible by p, B the set of all positive integers less than or equal to n that are divisible by q, and C the set of all positive integers less than or equal to n that are divisible by r. Note that $A = \{p, 2p, 3p, \ldots, qr \cdot p\}$, $B = \{q, 2q, 3q, \ldots, pr \cdot q\}$, $C = \{r, 2r, 3r, \ldots, pq \cdot r\}$, $A \cap B = \{pq, 2pq, 3pq, \ldots, r \cdot pq\}$, $A \cap C = \{pr, 2pr, 3pr, \ldots, q \cdot pr\}$, $B \cap C = \{qr, 2qr, 3qr, \ldots, p \cdot qr\}$, and $A \cap B \cap C = \{pqr\}$. By definition of ϕ,

$$\phi(n) \quad = \quad n - [n(A \cup B \cup C)]$$

$$= \quad n - [n(A) + n(B) + n(C) - n(A \cap B) - n(A \cap C) - n(B \cap C) + n(A \cap B \cap C)]$$

by the inclusion/exclusion formula

$$= \quad pqr - [qr + pr + pq - r - q - p + 1]$$

$$= \quad pqr - qr - pr - pq + r + q + p - 1$$

$$= \quad (p-1)(q-1)(r-1)$$

41. This property is true. *Proof*: Let $f\colon X \to Y$ be any function, and suppose $A \subseteq X$ and $B \subseteq X$.

$\boldsymbol{f(A \cup B) \subseteq f(A) \cup f(B)}$: Let $y \in f(A \cup B)$. Then $y = f(x)$ for some $x \in A \cup B$. By definition of union, $x \in A$ or $x \in B$. So $y = f(x)$ for some $x \in A$ (in which case $y \in f(A)$) or $y = f(x)$ for some $x \in B$ (in which case $y \in f(B)$). Hence by definition of union, $y \in f(A) \cup f(B)$.

$\boldsymbol{f(A) \cup f(B) \subseteq f(A \cup B)}$: Let $y \in f(A) \cup f(B)$. By definition of union, $y \in f(A)$ or $y \in f(B)$. If $y \in f(A)$, then $y = f(x)$ for some $x \in A$. In this case, by definition of union, $x \in A \cup B$, and so $y \in f(A \cup B)$. If $y \in f(B)$, then $y = f(x)$ for some $x \in B$. In this case, by definition of union, $x \in A \cup B$, and so $y \in f(A \cup B)$. Hence, in either case, $y \in f(A \cup B)$.

43. This property is false. *Counterexample*: Let $X = \{1,2,3\}$, $Y = \{a,b\}$, $A = \{1,2\}$, $B = \{3\}$, and let $f(1) = f(3) = a$ and $f(2) = b$. Then $f(A) = \{a,b\}$, $f(B) = \{a\}$, $f(A - B) = f(\{1,2\}) = \{a,b\}$, and $f(A) - f(B) = \{a,b\} - \{a\} = \{b\}$. So $f(A - B) \neq f(A) - f(B)$.

45. This statement is true. *Proof*: Let $f\colon X \to Y$ be any function, and suppose that $C \subseteq Y$ and $D \subseteq Y$. For any element x in X, by definition of inverse image and union,

$$x \in f^{-1}(C \cup D) \Leftrightarrow f(x) \in C \cup D \Leftrightarrow f(x) \in C \text{ or } f(x) \in D$$

$$\Leftrightarrow x \in f^{-1}(C) \text{ or } \in f^{-1}(D) \Leftrightarrow x \in f^{-1}(C) \cup f^{-1}(D).$$

Hence $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$.

46. This statement is true. *Proof*: Let $f\colon X \to Y$ be any function, and suppose that $C \subseteq Y$ and $D \subseteq Y$. For any element x in X, by definition of inverse image and intersection,

$$x \in f^{-1}(C \cap D) \Leftrightarrow f(x) \in C \cap D \Leftrightarrow f(x) \in C \text{ and } f(x) \in D$$

$$\Leftrightarrow x \in f^{-1}(C) \text{ and } x \in f^{-1}(D) \Leftrightarrow x \in f^{-1}(C) \cap f^{-1}(D).$$

Hence $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$.

47. This statement is true. *Proof*: Let $f\colon X \to Y$ be any function, and suppose that $C \subseteq Y$ and $D \subseteq Y$. For any element x in X, by definition of inverse image and set difference,

$$x \in f^{-1}(C - D) \Leftrightarrow f(x) \in C - D \Leftrightarrow f(x) \in C \text{ and } f(x) \notin D$$

$$\Leftrightarrow x \in f^{-1}(C) \text{ and } x \notin f^{-1}(D) \Leftrightarrow x \in f^{-1}(C) - f^{-1}(D).$$

Hence $f^{-1}(C - D) = f^{-1}(C) - f^{-1}(D)$.

Section 7.2

4. True. Suppose x_1 and x_2 are elements of X such that $f(x_1) = f(x_2)$. Let $y = f(x_1) = f(x_2)$. According to the exercise statement, there is at most one element of X that has y as its image. So $x_1 = x_2$.

5. The statement in (b) is incorrect. The condition that every element in the domain of a function have a corresponding image in the function's co-domain is part of the definition for all functions, not just functions that are onto.

The statement in part (d) is just a formal way of expressing the statement in part (b). So it is incorrect for the same reason that the statement in part (b) is incorrect.

7. *b.* G is not one-to-one because, for example, $G(a) = y = G(b)$ and $a \neq b$. G is not onto because z is in Y but $z \neq G(r)$ for any r in X.

8. *a.* H is not one-to-one because $H(b) = y = H(c)$ and $b \neq c$. H is not onto because, for example, $x \in Y$ and $x \neq H(r)$ for any $r \in X$.

b. K is one-to-one because no two elements of X are sent by K to the same element of Y. K is not onto because z is in Y and $z \neq K(r)$ for any r in X.

9. In each case below there are a number of correct answers.
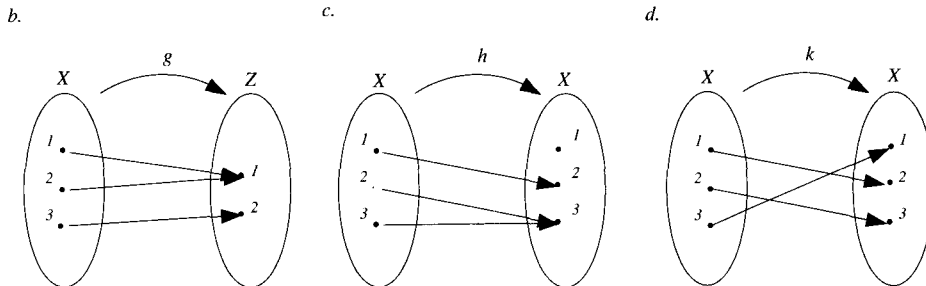
10. *c.* $3 \cdot 2 \cdot 1 = 6$ *[There are three choices for where to send the first element of the domain, two choices for where to send the second element (since the function is one-to-one, the second element cannot go to the same place as the first), and one choice for where to send the third, which cannot go to the same place as either of the first two.]*

d. $5 \cdot 4 \cdot 3 = 60$ *[There are five choices for where to send the first element of the domain, four choices for where to send the second element(since the function is one-to-one, the second element cannot go to the same place as the first), and three choices for where to send the third, which cannot go to the same place as either of the first two.]*

e. The answer is $n(n-1)(n-2)\cdots(n-m+1)$ because there are n choices for where to send the first element of the domain, $n-1$ for where to send the second (since it cannot go the same place as the first), $n-2$ for where to send the third (since it cannot go the same place as either of the first two), and so forth. At the time an image is chosen for the mth element of the domain, the other $m-1$ elements of the domain have all been sent to $m-1$ distinct elements of the co-domain, and so there are $n-(m-1) = n-m+1$ choices for where to send the mth element.

11. *b.* None.

c. $3 \cdot 2 \cdot 1 = 6$ *[For any such function, the three elements of the domain must go to three different elements of the co-domain because otherwise the function will not be onto. Thus any such function is also one-to-one, and so the number of such functions can be counted in the same way as was shown in the answer to 10(c): there are three choices for where to send the first element of the domain, two choices for where to send the second, and one choice for where to send the third.]*

e. Consider onto functions from a set with four elements to a set with three elements. Denote the set of four elements by $X = \{a, b, c, d\}$ and the set with three elements by $Y = \{u, v, w\}$. Divide the set of onto functions f from X to Y into two disjoint categories: (1) those that send at least two elements of X to $f(d)$, and (2) those that do not.

An onto function in category 1 can be constructed by the following two-step operation: Step 1 is to choose an image for d. There are three ways to do this because there are three elements of Y. Step 2 is to choose an onto function from $X - \{d\}$ to Y. (This ensures that at least two elements of X are sent to $f(d)$.) By part (c), there are 6 such onto functions. Thus the number of functions in category 1 is $3 \cdot 6 = 18$.

An onto function in category 2 can be constructed by the following two-step operation: Step 1 is to choose an image for d. (As above, there are three ways to do this.) Step 2 is to choose an onto function from $X - \{d\}$ to $Y - \{f(d)\}$. (This ensures that the only element of X that is sent to $f(d)$ is d.) By part (a), there are 6 such onto functions. Thus the number of functions in category 2 is $3 \cdot 6 = 18$.

Therefore, by the addition rule, the number of onto functions from a set with four elements to a set with three elements is $18 + 18 = 36$.

f. Let X be a set with m elements, let Y be a set with n elements, where $m \geq n \geq 1$, and let x be any particular element of X. Divide the set of onto functions f from X to Y into two disjoint categories: (1) those for which $f^{-1}(f(x))$ has more than one element (i.e., those functions that send at least two elements of X to $f(x)$), and (2) those for which $f^{-1}(f(x))$ contains only the single element x. Because these categories are non-overlapping, by the addition rule, the number of onto functions from X to Y equals the sum of the numbers of onto functions in the two categories.

Constructing an onto function in category 1 can be regarded as a two-step operation: Step 1 is to choose where to send x and Step 2 is to choose an onto function from $X - \{x\}$ to Y. This ensures that at least two elements are sent to $f(x)$. Thus the number of such functions equals the number of choices for where to send x times the number of onto functions from $X - \{x\}$ to Y, which equals $n \cdot c_{m-1, n}$.

Constructing an onto function in category 2 can also be regarded as a two-step operation: Step 1 is to choose where to send x and Step 2 is to choose an onto function from $X - \{x\}$ to $Y - \{f(x)\}$. This ensures that only one element is sent to $f(x)$. The number of such functions equals the number of choices for where to send x times the number of onto functions from $X - \{x\}$ to $Y - \{f(x)\}$, which equals $n \cdot c_{m-1, n-1}$.

By the addition rule, $c_{m,n}$, the total number of onto functions from X to Y, satisfies the formula $c_{m,n} = n \cdot c_{m-1, n} + n \cdot c_{m-1, n-1}$.

13. *a.* (i) *g is one-to-one:* Suppose n_1 and n_2 are in $\mathbf{Z}$ and $g(n_1) = g(n_2)$. By definition of g, $4n_1 - 5 = 4n_2 - 5$. Adding 5 to both sides and dividing by 4 gives $n_1 = n_2$.

(ii). *g is not onto:* Let $m = 0$. Then m is in $\mathbf{Z}$ but $m \neq g(n)$ for any integer n. *[For if $m = g(n)$ then $0 = 4n - 5$, and so $n = 5/4$. But $5/4$ is not in $\mathbf{Z}$.]*

b. G is onto: Suppose y is any element of $\mathbf{R}$. Let $x = (y + 5)/4$. Then $G(x) = G((y + 5)/4) = 4[(y + 5)/4] - 5 = (y + 5) - 5 = y$ *[as was to be shown]*.

14. *b. K is onto:* Suppose y is any element of $\mathbf{R}^{nonneg}$. Let $x = \sqrt{y}$. Then x is a real number because $y \geq 0$, and by definition of K, $K(x) = K(\sqrt{y}) = (\sqrt{y})^2 = y$.

18. *f is one-to-one.* *Proof:* Let x_1 and x_2 be any nonzero real numbers such that $f(x_1) = f(x_2)$. By definition of f, $\dfrac{3x_1 - 1}{x_1} = \dfrac{3x_2 - 1}{x_2}$. Cross-multiplying gives $(3x_1 - 1)x_2 = (3x_2 - 1)x_1$, or, equivalently, $3x_1 x_2 - x_2 = 3x_1 x_2 - x_1$. Subtracting $3x_1 x_2$ from both sides gives $-x_1 = -x_2$, and multiplying both sides by -1 gives $x_1 = x_2$.

19. *f is one-to-one.* *Proof:* Let x_1 and x_2 be any real numbers other than -1, and suppose that $f(x_1) = f(x_2)$. By definition of f, $\dfrac{x_1 + 1}{x_1 - 1} = \dfrac{x_2 + 1}{x_2 - 1}$. Cross-multiplying gives $(x_1 + 1)(x_2 - 1) = (x_2 + 1)(x_1 - 1)$, or, equivalently, $x_1 x_2 - x_1 + x_2 - 1 = x_1 x_2 - x_2 + x_1 - 1$. Adding $1 - x_1 x_2$

to both sides gives $-x_1 + x_2 = -x_2 + x_1$, or, equivalently, $2x_1 = 2x_2$. Dividing both sides by 2 gives $x_1 = x_2$.

20. *b.* $h(364\text{-}98\text{-}1703) = 2$. Since position 2 is occupied, the next position is examined. That also is occupied, but the following position is free. So 364-98-1703 is placed in position 4.

   c. $h(283\text{-}09\text{-}0787) = 0$. Since position 0 is occupied but the next position is free, 283-09-0787 is placed in position 1.

23. *a. D is not one-to-one*: Let $s = 10$ and let $t = 1100$. Then $D(s) = 1 - 1 = 0$ and $D(t) = 2 - 2 = 0$. So $D(s) = D(t)$ but $s \neq t$.

   b. D is onto: *Proof*: Let m be any integer. In case m is positive, let s be the string consisting of m 1's and no 0's. Then $D(s) = m$. In case m is 0, let s be the null string. Then $D(s) = 0 = m$. In case m is negative, let s be the string consisting of no 1's and $|m|$ 0's. Then $D(s) = -|m| = m$.

24. *b. F is not onto*: The number 4 is in $\mathbf{Z}$ but $F(A) \neq 4$ for any set A in $\mathscr{P}(\{a, b, c\})$ because no subset of $\{a, b, c\}$ has four elements.

25. *a. N is not one-to-one*: Let $s_1 = a$ and $s_2 = ab$. Then $N(s_1) = N(s_2) = 1$ but $s_1 \neq s_2$.

26. Let S be the set of all strings of a's and b's.

   a. C is one-to-one: Suppose s_1 and s_2 are strings in S and $C(s_1) = C(s_2)$. By definition of C, this means that $as_1 = as_2$. But strings are just n-tuples written without parentheses or commas. By definition of equality of ordered n-tuples, therefore, for each integer $n \geq 0$, the nth character from the left in as_1 equals the nth character from the left in as_2. It follows that for each integer $n \geq 0$, the nth character from the left in s_1 equals the nth character from the left in s_2, and so $s_1 = s_2$.

   b. C is not onto: The string b is in S but $b \neq as$ for any string a in S. Hence $b \neq C(s)$ for any s in S.

27. *a. F is one-to-one*: Suppose $F(a, b) = F(c, d)$ for some ordered pairs (a, b) and (c, d) in $\mathbf{Z}^+ \times \mathbf{Z}^+$. By definition of F, $3^a 5^b = 3^c 5^d$. Thus, by the unique factorization theorem (Theorem 3.3.3), $a = b$ and $c = d$; in other words, $(a, b) = (c, d)$.

   b. G is one-to-one: Suppose $G(a, b) = G(c, d)$ for some ordered pairs (a, b) and (c, d) in $\mathbf{Z}^+ \times \mathbf{Z}^+$. By definition of G, $3^a 6^b = 3^c 6^d$, and so $3^a 3^b 2^b = 3^c 2^d 3^d$, or, equivalently, $3^{a+b} 2^b = 3^{c+d} 3^d$. Thus, by the unique factorization theorem (Theorem 3.3.3), $a + b = c + d$ and $b = d$. Solving these equations gives $a = b$ and $c = d$; in other words, $(a, b) = (c, d)$.

28. *b.* Let $x = \log_{16} 9$ and $y = \log_4 3$. By definition of logarithm, $16^x = 9$ and $4^y = 3$. Since $16 = 4^2$ and $9 = 3^2$, substitution gives $(4^2)^x = 9 = 3^2 = (4^y)^2$. So by one of the laws of exponents (property (7.2.2)), $4^{2x} = 4^{2y}$. Hence by property (7.2.4), $2x = 2y$, and thus $x = y$. Therefore the answer is yes.

30. Suppose b, x, and y are any positive real numbers with $b \neq 1$. Let $u = \log_b(x)$ and $v = \log_b(y)$. By definition of logarithm, $x = b^u$ and $y = b^v$. Then $x \cdot y = b^u \cdot b^v = b^{u+v}$ by property (7.2.1). Applying the definition of logarithm to the extreme parts of this last equation gives $\log_b(x \cdot y) = u + v = \log_b(x) + \log_b(y)$.

33. When $f \colon \mathbf{R} \to \mathbf{R}$ and $g \colon \mathbf{R} \to \mathbf{R}$ are both onto, it need not be the case that $f + g$ is onto. *Counterexample*: Let $f \colon \mathbf{R} \to \mathbf{R}$ and $g \colon \mathbf{R} \to \mathbf{R}$ be defined by $f(x) = x$ and $g(x) = -x$ for all $x \in \mathbf{R}$. Then both f and g are onto, but $(f + g)(x) = f(x) + g(x) = x + (-x) = 0$ for all x, and so $f + g$ is not onto.

35. If $f\colon \mathbf{R} \to \mathbf{R}$ is onto and c is any nonzero real number, then $c \cdot f$ is also onto.

Proof: Suppose $f\colon \mathbf{R} \to \mathbf{R}$ is onto and c is any nonzero real number. Let $y \in \mathbf{R}$. Since $c \neq 0$, y/c is a real number, and since f is onto, there is an $x \in \mathbf{R}$ with $f(x) = y/c$. Then $y = c \cdot f(x) = (c \cdot f)(x)$. So $c \cdot f$ is onto.

37.
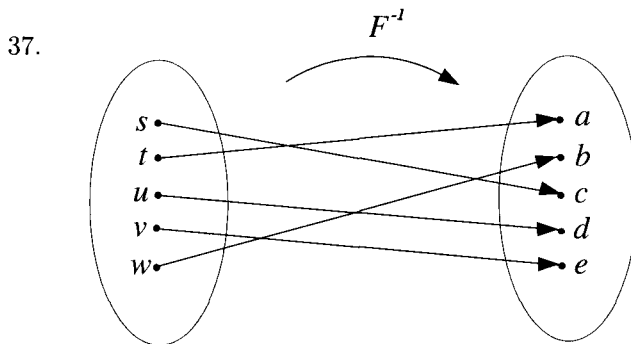
41. The answer to exercise 13(b) shows that G is onto. It is also the case that G is one-to-one. To see why this is so, suppose $G(x_1) = G(x_2)$ for some x_1 and x_2 in $\mathbf{R}$. *[We must show that $x_1 = x_2$.]* Then, by definition of G, $4x_1 - 5 = 4x_2 - 5$. Add 5 to both sides of this equation and divide both sides by 4 to obtain $x_1 = x_2$, *[as was to be shown]*. Note also that given any real number y, we may let $x = (y + 5)/4$. Then x is a real number, and by definition of G, $G(x) = G((y + 5)/4) = 4((y + 5)/4) - 5 = (y + 5) - 5 = y$. Hence for all $y \in \mathbf{R}$, $G^{-1}(y) = (y + 5)/4$.

42. The answer to exercise 14b shows that K is onto. It is also the case that K is one-to-one. To see why this is so, suppose x_1 and x_2 are any nonnegative real numbers such that $K(x_1) = K(x_2)$. *[We must show that $x_1 = x_2$.]* Then by definition of K, $x_1^2 = x_2^2$. But each nonnegative real number has a unique nonnegative square root. So since both x_1 and x_2 are nonnegative square roots of the same number, $x_1 = x_2$ *[as was to be shown]*. Therefore K is both one-to-one and onto, and thus K is a one-to-one correspondence. For all $y \in \mathbf{R}^{nonneg}$, $K^{-1}(y) = \sqrt{y}$ because $K(\sqrt{y}) = (\sqrt{y})^2 = y$.

45. Because D is not one-to-one, D is not a one-to-one correspondence.

46. F is neither one-to-one nor onto. Hence it is not a one-to-one correspondence.

47. N is neither one-to-one nor onto. Hence it is not a one-to-one correspondence.

49. This function is not a one-to-one correspondence because it is not one-to-one.

50. By the result of exercise 18, f is one-to-one. f is also onto for the following reason. Given any real number y other than 3, let $x = \dfrac{1}{3 - y}$. Then x is a real number (because $y \neq 3$) and

$$f(x) = f(\frac{1}{3 - y}) = \frac{3\left(\frac{1}{3-y}\right) - 1}{\frac{1}{3-y}} = \frac{3\left(\frac{1}{3-y}\right) - 1}{\frac{1}{3-y}} \cdot \frac{(3 - y)}{(3 - y)} = \frac{3 - (3 - y)}{1} = 3 - 3 + y = y.$$

This calculation also shows that $f^{-1}(y) = \dfrac{1}{3 - y}$ for all real numbers $y \neq 3$.

51. By the result of exercise 19, f is one-to-one. f is also onto for the following reason. Given any real number y other than 1, let $x = \dfrac{1+y}{1-y}$. Then x is a real number (because $y \neq 1$) and

$$f(x) = f(\frac{y+1}{y-1}) = \frac{\left(\frac{y+1}{y-1}\right)+1}{\left(\frac{y+1}{y-1}\right)-1} = \frac{\left(\frac{y+1}{y-1}\right)+1}{\left(\frac{y+1}{y-1}\right)-1} \cdot \frac{(y-1)}{(y-1)} = \frac{y+1+(y-1)}{y+1-(y-1)} = \frac{y+1+y-1}{y+1-y+1} = y.$$

This calculation also shows that $f^{-1}(y) = \dfrac{y+1}{y-1}$ for all real numbers $y \neq 1$.

52. *a.* Let $X = \{x_1, x_2, \ldots, x_n\}$ and let S be the set of all strings of 0's and 1's that have length n. Define a function $F: \mathscr{P}(X) \to S$ as follows: for each A in $\mathscr{P}(X)$, $F(A) =$ the string of 0's and 1's for which the character in the ith position is a 1 if $x_i \in A$ and the character in the ith position is a 0 if $x_i \notin A$. For instance, if $n = 10$ and $A = \{x_2, x_4, x_9\}$, then $F(A) = 0101000010$; the 1's in positions 2, 4, and 9 indicate that $x_2, x_4,$ and x_9 are the elements in A.

F is one-to-one: Suppose $F(A_1) = F(A_2)$ for some sets A_1 and A_2 in $\mathscr{P}(X)$. By definition of equality of strings, for each integer $i = 1, 2, \ldots, n$, the ith character of $F(A_1)$ is a 1 if, and only if, the ith character of $F(A_2)$ is a 1. By definition of F, this implies that $x_i \in A_1$ if, and only if, $x_i \in A_2$. It follows that every element of A_1 is in A_2 and every element of A_2 is in A_1. Consequently, $A_1 = A_2$ by definition of set equality.

F is onto: Suppose y is a string of 0's and 1's of length n. Define a subset A of X as follows: Let A consist of the set of all x_i in X for which the character in position i of y is a 1; otherwise $x \notin A$. (For instance, if $n = 10$ and $y = 0001110100$, then $A = \{x_4, x_5, x_6, x_8\}$ because there are 1's in positions 4, 5, 6, and 8 and 0's in all other positions.) Then $F(A) = y$ by definition of F.

Since F is one-to-one and onto, F is a one-to-one correspondence.

53. **Algorithm 7.2.1   Checking Whether a Function is One-to-One**

[For a given function F with domain $X = \{a[1], a[2], \ldots, a[n]\}$, this algorithm discovers whether or not F is one-to-one. Initially, answer is set equal to "one-to-one". Then the values of $F(a[i])$ and $F(a[j])$ are systematically compared for indices i and j with $1 \leq i < j \leq n$. If at any point it is found that $F(a[i]) = F(a[j])$ and $a[i] \neq a[j]$, then F is not one-to-one, and so answer is set equal to "not one-to-one" and execution ceases. If after all possible values of i and j have been examined, the value of answer is still "one-to-one", then F is one-to-one.]

Input: n *[a positive integer]*, $a[1], a[2], \ldots, a[n]$ *[a one-dimensional array representing the set X]*, F *[a function with domain X]*

Algorithm Body:

   answer := *"one-to-one"*

   $i := 1$

   while $(i \leq n - 1$ and *answer* = *"one-to-one"*$)$

      $j := i + 1$

      while $(j \leq n$ and *answer* = *"one-to-one"*$)$

         if $(F(a[i]) = F(a[j])$ and $a[i] \neq a[j])$ **then** *answer* := *"not one-to-one"*

         $j := j + 1$

      end while

      $i := i + 1$

   end while

Output: *answer [a string]*

54. **Algorithm 7.2.2   Checking Whether a Function is Onto**

[For a given function F with domain X = {a[1], a[2], ..., a[n]} and co-domain Y = {b[1], b[2], ..., b[m]}, this algorithm discovers whether or not F is onto. Initially, answer is set equal to "onto", and then successive elements of Y are considered. For each such element, b[i], a search is made through elements of the domain to determine if any is sent to b[i]. If not, the value of answer is changed to "not onto" and execution of the algorithm ceases. If so, the next successive element of Y is considered. If all elements of Y have been considered and the value of answer has not been changed from its initial value, then F is onto.]

Input: *n [a positive integer], a[1], a[2], ..., a[n] [a one-dimensional array representing the set X], m [a positive integer], b[1], b[2], ..., b[m] [a one-dimensional array representing the set Y], F [a function with domain X]*

Algorithm Body:

answer := "onto"

$i := 1$

while ($i \leq m$ and *answer* = "onto")

    $j := 1$

    found := "no"

    while ($j \leq n$ and *found* = "no")

        if $F(a[j]) = b[i]$ **then** *found* := "yes"

        $j := j + 1$

    end while

    if *found* = "no" **then** *answer* := "not onto"

    $i := i + 1$

end while

Output: *answer [a string]*

Section 7.3

2. *a.* No. For example, thirteen hearts could be selected: $2, 3, 4, 5, 6, 7, 8, 9, 10, J, Q, K, A$. No two of these are of the same denomination.

    b. Yes. Let X be the set consisting of the 20 selected cards, and let Y be the 13 possible denominations of cards. Define a function D from X (the pigeons) to Y (the pigeonholes) by specifying that for all x in X, $D(x) =$ the denomination of x. Now X has 20 elements and Y has 13 and $20 > 13$. So by the pigeonhole principle, D is not one-to-one. Hence $D(x_1) = D(x_2)$ for some cards x_1 and x_2 with $x_1 \neq x_2$. Then x_1 and x_2 are two distinct cards out of the 20 selected cards that have the same denomination.

4. Yes. Let X be the set of the 700 people and Y the set of all of the possible ordered pairs of first and last initials, and consider the function I from X (the pigeons) to Y (the pigeonholes) defined by specifying that $I(x) =$ the ordered pair of initials of person x. By the multiplication rule, $n(Y)$, the number of all of the possible ordered pairs of initials, is $26 \cdot 26 = 676$. By the pigeonhole principle, since $700 > 676$, I is not one-to-one, and so at least two people must have the same first and last initials.

6. *a.* Yes. Let X be the set of seven integers and Y the set of all possible remainders obtained through division by 6, and consider the function R from X (the pigeons) to Y (the pigeonholes) defined by the rule: $R(n) = n \bmod 6$ (= the remainder obtained by the integer division of

n by 6). Now *X* has 7 elements and *Y* has 6 elements (0, 1, 2, 3, 4, and 5). Hence by the pigeonhole principle, *R* is not one-to-one: $R(n_1) = R(n_2)$ for some integers n_1 and n_2 with $n_1 \neq n_2$. But this means that n_1 and n_2 have the same remainder when divided by 6.

b. No. Consider the set $\{1, 2, 3, 4, 5, 6, 7\}$. This set has seven elements no two of which have the same remainder when divided by 8.

7. Yes. Let *Y* be the set of all pairs of integers from *S* that add up to 15. There are 5 elements in $Y - \{3, 12\}, \{4, 11\}, \{5, 10\}, \{6, 9\}, \{7, 8\}-$ and each integer in *S* occurs in exactly one such pair. Let *X* be the set of six integers chosen from *S*, and consider the function from *X* to *Y* defined by the rule: $P(x) =$ the pair to which *x* belongs. Since *X* has 6 elements and *Y* has 5 elements and $6 > 5$, then by the pigeonhole principle, *P* is not one-to-one. Thus $P(x_1) = P(x_2)$ for some integers x_1 and x_2 in *X* with $x_1 \neq x_2$. This means that x_1 and x_2 are distinct integers in the same pair, which implies that $x_1 + x_2 = 15$.

8. No. For instance, the five integers 1, 2, 3, 4, 5 could be chosen. The sum of any two of these is less than 10 and so no two have a sum of 10.

11. Yes. There are *n* odd integers in the set $\{1, 2, \ldots, 2n\}$, namely, 1 $(= 2 \cdot 1 - 1)$, 3 $(= 2 \cdot 2 - 1)$, ..., $2n - 1$ $(= 2 \cdot n - 1)$. So the maximum number of odd integers that can be chosen is *n*. Thus if $n + 1$ integers are chosen, at least one of them must be even.

13. Seven. Since there are only six pairs of boots in the pile, if at most one boot is chosen from each pair, the maximum number of boots chosen would be six. It follows that if seven boots are chosen, at least two must be from the same pair.

15. There are $n + 1$ even integers from 0 to 2*n* inclusive: $0 (= 2 \cdot 0), 2 (= 2 \cdot 1), 4 (= 2 \cdot 2), \ldots, 2n (= 2 \cdot n)$. So a maximum of $n + 1$ even integers can be chosen. Thus if at least $n + 2$ integers are chosen, one is sure to be odd. Similarly, there are *n* odd integers from 0 to 2*n* inclusive, namely 1 $(= 2 \cdot 1 - 1), 3 (= 2 \cdot 2 - 1), \ldots, 2n - 1 (= 2 \cdot n - 1)$. It follows that if at least $n + 1$ integers are chosen, one is sure to be even. (An alternative way to reach the second conclusion is to note that there are $2n + 1$ integers from 0 to 2*n* inclusive. Because $n + 1$ of them are even, the number of odd integers is $(2n + 1) - (n + 1) = n$.)

16. There are 20 integers from 1 to 100 inclusive that are divisible by 5: $5 (= 5 \cdot 1), 10 (= 5 \cdot 2), 15 (= 5 \cdot 3), \ldots, 100 (= 5 \cdot 20)$. Hence there are 80 that are not divisible by 5, and so it is necessary to pick at least 81 in order to be sure to get one that is divisible by 5.

18. There are 15 distinct remainders that can be obtained through integer division by 15 (0, 1, 2, ..., 14). Hence at least 16 integers must be chosen in order to be sure that at least two have the same remainder when divided by 15.

19. Each number from 100 through 999 contains at least one of the nine digits 1, 2, 3, 4, 5, 6, 7, 8, or 9. Therefore, if ten such numbers are selected, at least two of them must have a digit in common. In fact, at least two must have a first digit in common because there are only nine possible first digits.

21. The length of the repeating section of the decimal representation of 5/20483 is less than or equal to the number of possible remainders that can be obtained when a number is divided by 20,483, , namely 20,483. The reason is that in the long-division process of dividing 5.0000... by 20,483, either some remainder is 0 and the decimal expansion terminates (in which case the length of the repeating section is 0) or, at some point within the first 20,483 successive divisions in the long-division process, a nonzero remainder is repeated. At that point the digits in the developing decimal expansion begin to repeat because the sequence of successive remainders repeats those previously obtained.

23. Irrational. The decimal expansion of a rational number must either terminate or repeat, and the decimal expansion of this number does neither because the numbers of 5's and 6's continually increase.

27. Yes. Let X be the set of 2,000 people (the pigeons) and Y the set of all 366 possible birthdays (the pigeonholes). Define a function $B\colon X \to Y$ by specifying that $B(x) = x$'s birthday. Now $2000 > 4 \cdot 366 = 1464$, and so by the generalized pigeonhole principle, there must be some birthday y such that $B^{-1}(y)$ has at least $4 + 1 = 5$ elements. Hence at least 5 people must share the same birthday.

28. Yes. This follows from the generalized pigeonhole principle with 500 pigeons (the lines of code), 17 pigeonholes (the days), and $k = 29$, using the fact that $500 > 29 \cdot 17 = 493$.

30. Consider the maximum number of pennies that can be chosen without getting at least five from the same year. This maximum, which is 12, is obtained when four pennies are chosen from each of the three years. Hence at least thirteen pennies must be chosen to be sure of getting at least five from the same year.

31. *Proof (by contradiction)*: Suppose that two or fewer secretaries are each assigned to three or more executives. Then the remaining secretaries are each assigned to two or fewer executives. Since the maximum number of executives to which any secretary can be assigned is four, the maximum number of executives that can be served by the secretaries occurs when 2 secretaries (the maximum possible) are each assigned to 4 executives (the maximum possible) and the remaining 3 secretaries are each assigned to 2 executives (the maximum possible for that group). The maximum number of executives that can be served by the secretaries is, therefore, $2 \cdot 4 + 3 \cdot 2 = 14$. Thus the five secretaries are assigned to at most 14 executives. It follows that at least one executive does not have a secretary, which contradicts the fact that each executive is assigned a secretary. Consequently, the supposition that two or fewer secretaries are assigned to three or more executives is false *[and so at least three secretaries are assigned to three or more executives]*.

    Proof (direct – with thanks to E. W. Dijkstra): Let k be the number of secretaries assigned to three or more executives. Because no secretary is assigned to more than four executives, these secretaries are assigned to at most $4k$ executives. Each of the remaining $5 - k$ secretaries is assigned to at most two executives, and so together they are assigned to at most $2(5 - k) = 10 - 2k$ executives. Therefore the number of executives assigned secretaries is at most $4k + (10 - 2k) = 10 + 2k$. Since 15 executives are assigned secretaries, $15 \le 10 + 2k$, or $k \ge 5/2$. So, since k is an integer, $k \ge 3$. Hence at least three secretaries are assigned to three or more executives.

32. *Proof*: Let S be the set of all possible sums of elements of subsets of A and define a function F from $\mathscr{P}(A)$ to S as follows: for each subset X of A, let $F(X)$ be the sum of the elements of X. By Theorem 5.3.1, $\mathscr{P}(A)$ has $2^6 = 64$ elements. Moreover, because A has six elements each of which is less than thirteen, the maximum possible sum of elements of any subset of A is 57 $(= 12 + 11 + 10 + 9 + 8 + 7)$. The minimum possible sum of elements of any subset of A is 21 $(= 1 + 2 + \cdots + 6)$. Hence S has 37 elements (the numbers from 21 to 57 inclusive). Since $64 > 37$, the pigeonhole principle guarantees that F is not one-to-one. Thus there exist distinct subsets S_1 and S_2 of S such that $F(S_1) = F(S_2)$, which implies that the elements of S_1 add up to the same sum as the elements of S_2.

    Additional Note: In fact, it can be shown that it is always possible to find disjoint subsets of S with the same sum. A proof is given at the end of the answer to exercise 33.

33. *Proof*: Let T be the set of all possible sums of elements of subsets of S and define a function F from $\mathscr{P}(S)$ to T as follows: for each subset X of A, let $F(X)$ be the sum of the elements of X. By Theorem 5.3.1, $\mathscr{P}(S)$ has $2^{10} = 1024$ elements. Moreover, because S has 10 elements each of which is less than 50, the maximum possible sum of elements of any subset of S is

$41 + 42 + \cdots + 50 = 455$. The minimum possible sum of elements of any subset of S is $1 + 2 + \cdots + 10 = 55$. Hence T has $455 - 55 + 1 = 401$ elements (the numbers from 55 to 455 inclusive). Because $1024 > 401$, the pigeonhole principle guarantees that F is not one-to-one. Thus there exist distinct subsets S_1 and S_2 of S such that $F(S_1) = F(S_2)$, which implies that the elements of S_1 add up to the same sum as the elements of S_2.

Additional Note: In fact, it can be shown that it is always possible to find disjoint subsets of S with the same sum. To see why this is true, consider again the sets S_1 and S_2 found in the proof given above. Then $S_1 \neq S_2$ and $F(S_1) = F(S_2)$. By definition of F, $F(S_1 - S_2) + F(S_1 \cap S_2) =$ the sum of the elements in $S_1 - S_2$ plus the sum of the elements in $S_1 \cap S_2$. But $S_1 - S_2$ and $S_1 \cap S_2$ are disjoint and their union is S_1. So $F(S_1 - S_2) + F(S_1 \cap S_2) = F(S_1)$. By the same reasoning, $F(S_2 - S_1) + F(S_1 \cap S_2) = F(S_2)$. Since $F(S_1) = F(S_2)$, we have that $F(S_1 - S_2) = F(S_1) - F(S_1 \cap S_2) = F(S_2) - F(S_1 \cap S_2) = F(S_2 - S_1)$. Hence the elements in $S_1 - S_2$ add up to the same sum as the elements in $S_2 - S_1$. But $S_1 - S_2$ and $S_2 - S_1$ are disjoint because $S_1 - S_2$ contains no elements of S_2 and $S_2 - S_1$ contains no elements of S_1.

34. *Proof*: Let X be the set consisting of the given 52 positive integers and let Y be the set containing the following elements: $\{00\}, \{50\}, \{01, 99\}, \{02, 98\}, \{03, 97\}, \ldots, \{49, 51\}$. Define a function F from X to Y by the rule $F(x) =$ the set containing the right-most two digits of x. Now X has 52 elements and Y has 51 elements. So by the pigeonhole principle, F is not one-to-one: there exist elements x_1 and x_2 in X such that $F(x_1) = F(x_2)$ and $x_1 \neq x_2$.

Case 1 (x_1 and x_2 have the same right-most two digits): In this case that right-most two digits of $x_1 - x_2$ are 00, and so $x_1 - x_2$ is divisible by 100.

Case 2 (x_1 and x_2 do not have the same right-most two digits): In this case since $F(x_1) = F(x_2)$ and $x_1 \neq x_2$, $F(x_1) = F(x_2)$ must be one of the two-element sets in Y, and since x_1 and x_2 do not have the same right-most two digits, the last two digits of x_1 must be one of the numbers in this set and the last two digits of x_2 must be the other number in this set. But the numbers in each of the two-element sets of Y add up to 100. Consequently the sum of the last two digits of x_1 and x_2 add up to 100, which implies that $x_1 + x_2$ is divisible by 100.

35. *Proof*: Suppose that 101 integers are chosen from 1 to 200 inclusive. Call them $x_1, x_2, \ldots, x_{101}$. Represent each of these integers in the form $x_i = 2^{k_i} \cdot a_i$ where a_i is the uniquely determined odd integer obtained by dividing x_i by the highest possible power of 2. Because each x_i satisfies the condition $1 \leq x_i \leq 200$, each a_i satisfies the condition $1 \leq a_i \leq 199$. Define a function F from $X = \{x_1, x_2, \ldots, x_{101}\}$ to the set Y of all odd integers from 1 to 199 inclusive by the rule $F(x_i) =$ that odd integer a_i such that x_i equals $2^{k_i} \cdot a_i$. Now X has 101 elements and Y has 100 elements ($1 = 2 \cdot 1 - 1$, $3 = 2 \cdot 2 - 1$, $5 = 2 \cdot 3 - 1$, $\ldots$, $199 = 2 \cdot 100 - 1$). Hence by the pigeonhole principle, F is not one-to-one: $F(x_i) = F(x_j)$ and $x_i \neq x_j$. But $x_i = 2^{k_i} \cdot a_i$ and $x_j = 2^{k_j} \cdot a_j$ and $F(x_i) = a_i$ and $F(x_j) = a_j$. Thus $x_i = 2^{k_i} \cdot a_i$ and $x_j = 2^{k_j} \cdot a_i$. If $k_j > k_i$, then $x_j = 2^{k_j} \cdot a_i = 2^{k_j - k_i} \cdot 2^{k_i} \cdot a_i = 2^{k_j - k_i} \cdot x_i$, and so x_j is divisible by x_i. Similarly, if $k_j < k_i$, x_i is divisible by x_j. Thus in either case, one of the numbers is divisible by another.

36. *a. Proof*: Suppose $a_1, a_2, \ldots, a_n$ is a sequence of n integers none of which is divisible by n. Define a function F from $X = \{a_1, a_2, \ldots, a_n\}$ to $Y = \{1, 2, \ldots, n-1\}$ by the rule $F(x) = x \bmod n$ (the remainder obtained through integer division of x by n). Since no element of X is divisible by n, F is well-defined. Now X has n elements and Y has $n - 1$ elements, and so by the pigeonhole principle $F(a_i) = F(a_j)$ for some elements a_i and a_j in X with $a_i \neq a_j$. By definition of F, both a_i and a_j have the same remainder when divided by n, and so $a_i - a_j$ is divisible by n. *[More formally, by the quotient-remainder theorem we can write $a_i = nq_i + r_i$ and $a_j = nq_j + r_j$ where $0 \leq r_i < n$ and $0 \leq r_j < n$, and since $F(a_i) = F(a_j)$, $r_i = r_j$. Thus $a_i - a_j = (nq_i + r_i) - (nq_j + r_j) = n(q_i - q_j) + (r_i - r_j) = n(q_i - q_j)$ because $r_i = r_j$. So by definition of divisibility, $a_i - a_j$ is divisible by n.]*

b. Proof: Suppose $x_1, x_2, \ldots, x_n$ is a sequence of n integers. For each $k = 1, 2, \ldots, n$, let $a_k = x_1 + x_2 + \ldots + x_k$. If some a_k is divisible by n, the problem is solved: the sum of the

numbers in the consecutive subsequence $x_1, x_2, \ldots, x_k$ is divisible by n. If no a_k is divisible by n, then $a_1, a_2, \ldots, a_n$ satisfies the hypothesis of part a, and so $a_j - a_i$ is divisible by n for some integers i and j with $j > i$. But $a_j - a_i = x_{i+1} + x_{i+2} + \ldots + x_j$. Thus the sum of the numbers in the consecutive subsequence $x_{i+1}, x_{i+2}, \ldots, x_j$ is divisible by n.

37. Let $a_1, a_2, \ldots, a_{n^2+1}$ be any sequence of $n^2 + 1$ distinct real numbers, and suppose that $a_1, a_2, \ldots, a_{n^2+1}$ does not contain a strictly increasing or a strictly decreasing subsequence of length at least $n + 1$. That is, suppose that every subsequence that is strictly increasing or strictly decreasing has length at most n. Let S be the set of ordered pairs of integers (i, d) where $1 \leq i \leq n$ and $1 \leq d \leq n$. Then we may define $F \colon \{a_1, a_2, \ldots, a_{n^2+1}\} \to S$ as follows:

$$F(a_k) = (i_k, d_k)$$

where

$\quad$ i_k is the length of the longest increasing subsequence starting at a_k,

and

$\quad$ d_k is the length of the longest decreasing subsequence starting at a_k.

Since there are $n^2 + 1$ elements in $\{a_1, a_2, \ldots, a_{n^2+1}\}$ and n^2 elements in S, by the pigeonhole principle F is not one-to-one. So $F(a_k) = F(a_m)$ for some integers k and m with $k \neq m$. Without loss of generality, we may assume that $k < m$. It follows by definition of F that $i_k = i_m$ and $d_k = d_m$. Now if $a_k < a_m$, then the longest strictly increasing subsequence starting at a_k is at least one more than the longest strictly increasing subsequence starting at a_m (because a_k can be added onto the front of any increasing subsequence that starts at a_m). So, in this case, $i_k > i_m$, which is a contradiction. Similarly, if $a_k > a_m$, then the longest strictly decreasing subsequence starting at a_k is at least one more than the longest strictly decreasing subsequence starting at a_m (because a_k can be added onto the front of any decreasing subsequence that starts at a_m). So, in this case, $d_k > d_m$, which is a contradiction. Hence $a_k \not< a_m$ and $a_k \not> a_m$, and so $a_k = a_m$. But this also is impossible because all the numbers in $\{a_1, a_2, \ldots, a_{n^2+1}\}$ are distinct. Thus the supposition is false, and so $\{a_1, a_2, \ldots, a_{n^2+1}\}$ contains a strictly increasing or a strictly decreasing subsequence of length at least $n + 1$.

38. Let S be any set consisting entirely of integers from 1 through 100, and suppose that no integer in S divides any other integer in S. Factor out the highest power of 2 to write each integer in S as $2^k \cdot m$, where m is an odd integer. Now consider any two such integers in S, say $2^r \cdot a$ and $2^s \cdot b$. Observe that $a \neq b$. The reason is that if $a = b$, then whichever integer contains the fewer number of factors of 2 divides the other integer. (For example, $2^2 \cdot 3 \mid 2^4 \cdot 3$.) Thus there can be no more integers in S than there are distinct odd integers from 1 through 100, namely 50. Furthermore, it is possible to find a set T of 50 integers from 1 through 100 no one of which divides any other. For instance, $T = 51, 52, 53, \ldots, 99, 100$. Hence the largest number of elements that a set of integers from 1 through 100 can have so that no one element in the set is divisible by any other is 50.

39. **Algorithm 7.3.1   Finding Pigeons in the Same Pigeonhole**

[For a given function F with domain $X = \{x[1], x[2], \ldots, x[n]\}$ and co-domain $Y = \{y[1], y[2], \ldots, y[m]\}$ with $n > m$, this algorithm finds elements a and b so that $F(a) = F(b)$ and $a \neq b$. The existence of such elements is guaranteed by the pigeonhole principle because $n > m$. Initially, the variable done is set equal to "no". Then the values of $F(x[i])$ and $F(x[j])$ are systematically compared for indices i and j with $1 \leq i < j \leq n$. When it is found that $F(x[i]) = F(x[j])$ and $x[i] \neq x[j]$, a is set equal to $x[i]$, b is set equal to $x[j]$, done is set equal to "yes", and execution ceases.]

Input: *n [a positive integer], m [a positive integer with $m < n$], $x[1], x[2], \ldots, x[n]$ [a one-dimensional array representing the set X], $y[1], y[2], \ldots, y[m]$ [a one-dimensional array representing the set Y], F [a function from X to Y]*

Algorithm Body:

$$done := \text{``no''}$$

$$i := 1$$

while $(i \le n - 1$ and $done = \text{``no''})$

    $j := i + 1$

    while $(j \le n$ and $done = \text{``no''})$

        if $(F(x[i]) = F(x[j])$ and $x[i] \ne x[j])$

            then do $a := x[i]$, $b := x[j]$, $done := \text{``yes''}$ **end do**

        $j := j + 1$

    end while

    $i := i + 1$

end while

Output: a, b *[positive integers]*

Section 7.4

2.
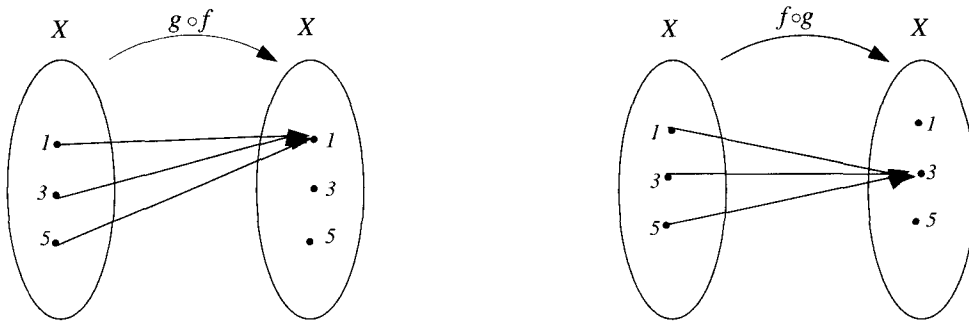
Then $f \circ g \ne g \circ f$ because, for instance, $(g \circ f)(1) = 1$ whereas $(f \circ g)(1) = 3$.

4. $G \circ F$ is defined by $(G \circ F)(x) = x$, for all $x \in \mathbf{R}$, because for any real number x, $(G \circ F)(x) = G(F(x)) = G(x^5) = (x^5)^{1/5} = x^1 = x$. $F \circ G$ is defined by $(F \circ G)(x) = x$, for all $x \in \mathbf{R}$, because for any real number x, $(F \circ G)(x) = F(G(x)) = F(x^{1/5}) = (x^{1/5})^5 = x^1 = x$. Thus $G \circ F = F \circ G$.

6. $G \circ F$ is defined by $(G \circ F)(x) = \lfloor x \rfloor$, for all real numbers x, because for any real number x, $(G \circ F)(x) = G(F(x)) = G(3x) = \left\lfloor \dfrac{3x}{3} \right\rfloor = \lfloor x \rfloor$. $F \circ G$ is defined by $(F \circ G)(n) = 3 \cdot \left\lfloor \dfrac{x}{3} \right\rfloor$, for all real numbers x, because for any real number x, $(F \circ G)(x) = F(G(x)) = F(\left\lfloor \dfrac{x}{3} \right\rfloor) = 3 \cdot \left\lfloor \dfrac{x}{3} \right\rfloor$. Then $G \circ F \ne F \circ G$ because, for instance, $(G \circ F)(1) = \lfloor 1 \rfloor = 1$, whereas $(F \circ G)(1) = 3 \cdot \left\lfloor \dfrac{1}{3} \right\rfloor = 3 \cdot 0 = 0$.

8. $(G \circ F)(2) = G(2^2/3) = G(4/3) = \lfloor 4/3 \rfloor = 1$

   $(G \circ F)(-3) = G((-3)^2/3) = G(3) = \lfloor 3 \rfloor = 3$

   $(G \circ F)(5) = G(5^2/3) = G(25/3) = \lfloor 25/3 \rfloor = 8$

10. For each x in $\mathbf{R}^+$, $(G \circ G^{-1})(x) = G(G^{-1}(x)) = G(\sqrt{x}) = (\sqrt{x})^2 = x$ because $x > 0$. Hence $G \circ G^{-1} = i_{\mathbf{R}^+}$ by definition of equality of functions.

For each x in $\mathbf{R}^+$, $(G^{-1} \circ G)(x) = G^{-1}(G(x)) = G(x^2) = \sqrt{x^2} = x$ because $x > 0$. Hence $G^{-1} \circ G = i_{\mathbf{R}^+}$ by definition of equality of functions.

11. Since $H = H^{-1}$, for all real numbers $x \neq 1$,

$$
\begin{aligned}
(H^{-1} \circ H)(x) \;=\; (H \circ H^{-1})(x) \;&=\; H\left(\frac{x+1}{x-1}\right) \\[2mm]
&=\; \frac{\left(\frac{x+1}{x-1}\right)+1}{\left(\frac{x+1}{x-1}\right)-1} \;=\; \frac{\left(\frac{x+1}{x-1}\right)+1}{\left(\frac{x+1}{x-1}\right)-1} \cdot \frac{(x-1)}{(x-1)} \\[2mm]
&=\; \frac{(x+1)+(x-1)}{(x+1)-(x-1)} \;=\; \frac{2x}{2} \;=\; x.
\end{aligned}
$$

12. *b.* For all positive real numbers b and x, $\log_b x$ is the exponent to which b must be raised to obtain x. So if b is raised to this exponent, x is obtained. In other words, $b^{\log_b x} = x$.

13. *Proof*: Suppose f is a function from a set X to a set Y. For each x in X, $(i_Y \circ f)(x) = i_Y(f(x)) = f(x)$ by definition of i_Y. Hence $i_Y \circ f = f$.

14. *Proof*: Suppose $f \colon X \to Y$ is a one-to-one and onto function with inverse function $f^{-1} \colon Y \to X$. Then for all $y \in Y$, $(f \circ f^{-1})(y) = f(f^{-1}(y)) = f$ (that element x in X for which $f(x)$ equals y) $= y = i_Y(y)$. Hence $f \circ f^{-1} = i_Y$.

15. *b.* $z/2 = t/2$ *c.* $f(x_1) = f(x_2)$

17. No. *Counterexample*: For the functions f and g defined by the arrow diagrams below, $g \circ f$ is onto but f is not onto.
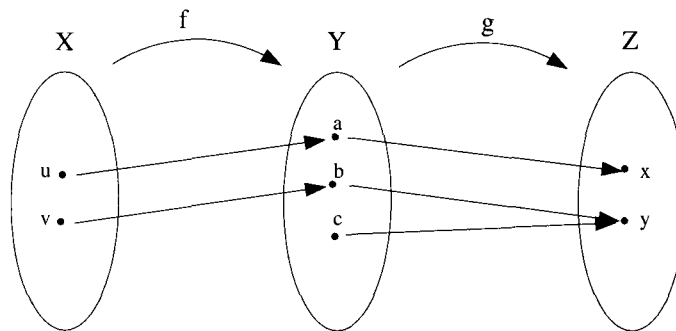
18. Yes. *Proof*: Suppose $f \colon X \to Y$ and $g \colon Y \to Z$ are functions and $g \circ f \colon X \to Z$ is one-to-one. To show that f is one-to-one, suppose x_1 and x_2 are in X and $f(x_1) = f(x_2)$. *[We must show that $x_1 = x_2$.]* Then $g(f(x_1)) = g(f(x_2))$, and so $g \circ f(x_1) = g \circ f(x_2)$. But $g \circ f$ is one-to-one. Hence $x_1 = x_2$ *[as was to be shown]*.

19. Yes. *Proof*: Suppose $f \colon X \to Y$ and $g \colon Y \to Z$ are functions and $g \circ f \colon X \to Z$ is onto. To show that g is onto, let $z \in Z$. *[We must show that $z = g(y)$ for some $y \in Y$.]* Since $g \circ f$ is onto, there is an x in X such that $g \circ f(x) = z$. But $g \circ f(x) = g(f(x))$; so if $y = f(x)$ then $g(y) = z$. Hence there is an element y in Y such that $g(y) = z$ *[as was to be shown]*.

20. Yes. *Proof*: Suppose $f \colon W \to X$, $g \colon X \to Y$, and $h \colon Y \to Z$ are functions. For each $w \in W$, $[h \circ (g \circ f)](w) = h((g \circ f)(w)) = h(g(f(w))) = h \circ g(f(w)) = [(h \circ g) \circ f](w)$. Hence $h \circ (g \circ f) = (h \circ g) \circ f$ by definition of equality of functions.

22. False. *Counterexample*: Define f, g, and h from $\mathbf{Z}$ to $\mathbf{Z}$ as follows: for all integers n, $f(n) = 2\left\lfloor \dfrac{n}{2} \right\rfloor$, $g(n) = n$, and $h(n) = 2n$. Then h is one-to-one (by the answer to exercise 12a from Section 7.2). Also $(f \circ h)(n) = f(h(n)) = f(2n) = 2\left\lfloor \dfrac{2n}{2} \right\rfloor = 2\lfloor n \rfloor = 2n$, and $(g \circ h)(n) = g(h(n)) = g(2n) = 2n$. But $f(1) = 2\left\lfloor \dfrac{1}{2} \right\rfloor = 2 \cdot 0 = 0$, whereas $g(1) = 1$. So $f \neq g$.

24. $g \circ f \colon \mathbf{R} \to \mathbf{R}$ is defined by $(g \circ f)(x) = g(f(x)) = g(x + 3) = -(x + 3)$ for all $x \in \mathbf{R}$.

    Since $z = -(x + 3)$ if, and only if, $x = -z - 3$, $(g \circ f)^{-1} \colon \mathbf{R} \to \mathbf{R}$ is defined by $(g \circ f)^{-1}(z) = -z - 3$ for all $z \in \mathbf{R}$.

    Since $z = -y$ if, and only if, $y = -z$, $g^{-1} \colon \mathbf{R} \to \mathbf{R}$ is defined by $g^{-1}(z) = -z$ for all $z \in \mathbf{R}$.

    Since $y = x + 3$ if, and only if, $x = y - 3$, $f^{-1} \colon \mathbf{R} \to \mathbf{R}$ is defined by $f^{-1}(y) = y - 3$.

    $f^{-1} \circ g^{-1} \colon \mathbf{R} \to \mathbf{R}$ is defined by $(f^{-1} \circ g^{-1})(z) = f^{-1}(g^{-1}(z)) = f^{-1}(-z) = (-z) - 3 = -z - 3$ for all $z \in \mathbf{R}$.

    By the above and the definition of equality of functions, $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

25. *Proof*: Suppose $f \colon X \to Y$ and $g \colon Y \to X$ are functions such that $g \circ f = i_X$ and $f \circ g = i_Y$. Since both i_X and i_Y are one-to-one and onto, by the results of exercises 18 and 19, both f and g are one-to-one and onto, and so by Theorem 7.2.1 and the definition of inverse function, both have inverse functions. By Theorem 7.4.2(b), $f \circ f^{-1} = i_Y$. Since $f \circ g = i_Y$ also, $f \circ f^{-1} = f \circ g$, and so for all $y \in Y$, $(f \circ f^{-1})(y) = (f \circ g)(y)$. This implies that for all $y \in Y$, $f(f^{-1}(y)) = f(g(y))$. Since f is one-to-one, it follows that $f^{-1}(y) = g(y)$ for all $y \in Y$, and so by definition of equality of functions $f^{-1} = g$.

26. *Proof*: Suppose $f \colon X \to Y$ and $g \colon Y \to Z$ are functions that are both one-to-one and onto. By Theorems 7.4.3 and 7.4.4, $g \circ f$ is one-to-one and onto, and so by Theorem 7.2.1 and the definition of inverse function, $g \circ f$ has an inverse function $(g \circ f)^{-1} \colon Z \to X$. To show that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$, let z be any element of Z and let $x = (g \circ f)^{-1}(z)$. By definition of inverse function, $(g \circ f)^{-1}(z) = x$ if, and only if, $g \circ f(x) = z$. Hence $z = g \circ f(x) = g(f(x))$. Let $f(x) = y$. Then $z = g(y)$. Now since f and g are one-to-one and onto, by Theorem 7.2.1 and the definition of inverse function, f and g have inverse functions $f^{-1} \colon Y \to X$ and $g^{-1} \colon Z \to Y$. Then $g^{-1}(z) = y$ because $g(y) = z$ and $f^{-1}(y) = x$ because $f(x) = y$. Consequently, $f^{-1} \circ g^{-1}(z) = f^{-1}(g^{-1}(z)) = f^{-1}(y) = x$. But then $(g \circ f)^{-1}(z) = x = (f^{-1} \circ g^{-1})(z)$. Since the choice of z was arbitrary, $(g \circ f)^{-1}(z) = x = (f^{-1} \circ g^{-1})(z)$ for all $z \in Z$, and so $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ by definition of equality of functions.

28. True. *Proof*: Suppose $f \colon X \to Y$ is any function, suppose A is any subset of X, and suppose x_0 is any element of A. *[We must show that $x_0 \in f^{-1}(f(A))$.]* Then $f(x_0) \in f(A)$ by definition of $f(A)$. Now according to the definition of inverse image, $f^{-1}(f(A)) = \{x \in A \mid f(x) \in f(A)\}$. So, since $x_0 \in A$ and $f(x_0) \in f(A)$, then $x_0 \in f^{-1}(f(A))$ *[as was to be shown]*. Hence, by definition of subset, $A \subseteq f^{-1}(f(A))$.

30. False. *One counterexample among many*: Let $X = Y = C = \{1, 2\}$, and define $f \colon X \to Y$ by specifying that $f(1) = f(2) = 1$. Then $f(f^{-1}(C)) = f(\{1, 2\}) = \{1\}$. So $C \nsubseteq f(f^{-1}(C))$ because $\{1, 2\} \nsubseteq \{1\}$.

31. True. *Proof*: Let X, Y, and Z be any sets, let $f \colon X \to Y$ and $g \colon Y \to Z$ be any functions, and let E be any subset of Z.

    1. *Proof that $(g \circ f)^{-1}(E) \subseteq f^{-1}(g^{-1}(E))$*: Suppose $x \in (g \circ f)^{-1}(E)$. By definition of inverse image (for $g \circ f$), $(g \circ f)(x) \in E$, and by definition of composition of functions, $g(f(x)) \in E$. Then by definition of inverse image (for g), $f(x) \in g^{-1}(E)$, and by definition of inverse image (for f), $x \in f^{-1}(g^{-1}(E))$. So by definition of subset, $(g \circ f)^{-1}(E) \subseteq f^{-1}(g^{-1}(E))$.

2. *Proof that $f^{-1}(g^{-1}(E)) \subseteq (g \circ f)^{-1}(E)$*: Suppose $x \in f^{-1}(g^{-1}(E))$. By definition of inverse image (for f), $f(x) \in g^{-1}(E)$, and by definition of inverse image (for g), $g(f(x)) \in E$. So by definition of composition of functions, $(g \circ f)(x) \in E$. Then by definition of inverse image (for $g \circ f$), $x \in (g \circ f)^{-1}(E)$. So by definition of subset, $f^{-1}(g^{-1}(E)) \subseteq (g \circ f)^{-1}(E)$.

Therefore, since each set is a subset of the other, the two sets are equal.

Alternative proof (using the logic of if-and-only-if statements): Let X, Y, and Z be any sets, let $f : X \to Y$ and $g : Y \to Z$ be any functions, and let E be any subset of Z. $x \in (g \circ f)^{-1}(E) \Leftrightarrow (g \circ f)(x) \in E$ *[by definition of inverse image for $g \circ f$]* $\Leftrightarrow g(f(x)) \in E$ *[by definition of composition of functions]* $\Leftrightarrow f(x) \in g^{-1}(E)$ *[by definition of inverse image for g]* $\Leftrightarrow x \in f^{-1}(g^{-1}(E))$ *[by definition of inverse image for f]*. So by definition of set equality, $(g \circ f)^{-1}(E) = f^{-1}(g^{-1}(E))$.

Section 7.5

4. *Proof*: Define a function $f \colon \mathbf{O} \to 2\mathbf{Z}$ as follows: $f(n) = n - 1$ for all odd integers n. Observe that since n is odd, $n = 2k + 1$ for some integer k, and so $n - 1 = 2k$, which is even. Thus f is well-defined. Now f is one-to-one because for all odd integers n_1 and n_2, if $f(n_1) = f(n_2)$ then $n_1 - 1 = n_2 - 1$ and hence $n_1 = n_2$. Moreover f is onto because given any even integer m, then $m = 2k$ for some integer k, and so $m + 1 = 2k + 1$, which is odd. But $f(m+1) = (m+1) - 1 = m$ by definition of f. Thus, because there is a function $f \colon \mathbf{O} \to 2\mathbf{Z}$ that is one-to-one and onto, $\mathbf{O}$ has the same cardinality as $2\mathbf{Z}$.

5. Define $f \colon 2\mathbf{Z} \to 25\mathbf{Z}$ by the rule $f(n) = 25(n/2)$ for all even integers n. The function f is one-to-one because for any even integers n_1 and n_2, if $f(n_1) = f(n_2)$ then $25(n_1/2) = 25(n_2/2)$ and so *[by multiplying both sides by 2 and dividing by 25]* $n_1 = n_2$. Also f is onto because if m is any element in $25\mathbf{Z}$, then $m = 25k$ for some integer k. But then $2k$ is an even integer and $f(2k) = 25(2k/2) = 25k = m$ by definition of f. So since there is a function $f \colon 2\mathbf{Z} \to 25\mathbf{Z}$ that is one-to-one and onto, $2\mathbf{Z}$ has the same cardinality as $25\mathbf{Z}$.

6. The function $I \colon 2\mathbf{Z} \to \mathbf{Z}$ is defined as follows: $I(n) = n$ for all even integers n. I is clearly one-to-one because if $I(n_1) = I(n_2)$ then by definition of I, $n_1 = n_2$. But I is not onto because the range of I consists only of even integers. In other words, if m is any odd integer, then $I(n) \neq m$ for any even integer n.

The function $J \colon \mathbf{Z} \to 2\mathbf{Z}$ is defined as follows $J(n) = 2\lfloor n/2 \rfloor$ for all integers n. Then J is onto because for any even integer m, $m = 2k$ for some integer k. Let $n = 2k$. Then $J(n) = J(2k) = 2\lfloor 2k/2 \rfloor = 2\lfloor k \rfloor = 2k = m$. But J is not one-to-one because, for example, $J(2) = 2\lfloor 2/2 \rfloor = 2 \cdot 1 = 2$ and $J(3) = 2\lfloor 3/2 \rfloor = 2 \cdot 1 = 2$, so $J(2) = J(3)$ but $2 \neq 3$.

(More generally, given any integer k, if $m = 2k$, then $J(m) = 2\lfloor m/2 \rfloor = 2\lfloor 2k/2 \rfloor = 2\lfloor k \rfloor = J(m)$ and $J(m+1) = 2\lfloor (m+1)/2 \rfloor = 2\lfloor (2k+1)/2 \rfloor = 2\lfloor k + 1/2 \rfloor = 2k$. So $J(m) = J(m+1)$ but $m \neq m + 1$.)

7. *a.* $f(1) = -(1-1)/2 = 0$, $f(2) = 2/2 = 1$, $f(3) = -(3-1)/2 = -1$, $f(4) = 4/2 = 2$. All these values agree with those indicated in Figure 7.5.2.

9. Define a function $f \colon \mathbf{Z}^+ \to \mathbf{Z}^{nonneg}$ as follows: $f(n) = n - 1$ for all positive integers n. Observe that if $n \geq 1$ then $n - 1 \geq 0$, so f is well-defined. In addition, f is one-to-one because for all positive integers n_1 and n_2, if $f(n_1) = f(n_2)$ then $n_1 - 1 = n_2 - 1$ and hence $n_1 = n_2$. Moreover f is onto because if m is any nonnegative integer, then $m + 1$ is a positive integer and $f(m+1) = (m+1) - 1 = m$ by definition of f. Thus, because there is a function $f \colon \mathbf{Z}^+ \to \mathbf{Z}^{nonneg}$ that is one-to-one and onto, $\mathbf{Z}^+$ has the same cardinality as $\mathbf{Z}^{nonneg}$. It follows that $\mathbf{Z}^{nonneg}$ is countably infinite and hence countable.

11. *Proof*: Define $h: S \to V$ by the rule $h(x) = 3x + 2$ for all real numbers x in S. Then h is one-to-one because if x_1 and x_2 are in S and $h(x_1) = h(x_2)$, then $3x_1 + 2 = 3x_2 + 2$ and so *[by subtracting 2 and dividing by 3]* $x_1 = x_2$. Furthermore, h is onto because if y is any element in V, then $2 < y < 5$ and so $0 < (y-2)/3 < 1$. Consequently, $(y-2)/3 \in S$ and $h((y-2)/3) = 3((y-2)/3) + 2 = y$. Hence h is a one-to-one correspondence, and so S and V have the same cardinality.

12. *Proof*: Define $F: S \to W$ by the rule $F(x) = (b-a)x + a$ for all real numbers x in S. Then F is well-defined because if $0 < x < 1$, then $a < (b-a)x + a < b$. In addition, F is one-to-one because if x_1 and x_2 are in S and $F(x_1) = F(x_2)$, then $(b-a)x_1 + a = (b-a)x_2 + a$ and so *[by subtracting a and dividing by $b-a$]* $x_1 = x_2$. Furthermore, F is onto because if y is any element in W, then $a < y < b$ and so $0 < (y-a)/(b-a) < 1$. Consequently, $(y-a)/(b-a) \in S$ and $h((y-a)/(b-a)) = (b-a)[(y-a)/(b-a)] + a = y$. Hence F is a one-to-one correspondence, and so S and W have the same cardinality.

14. *Proof (without calculus)*: The function g is defined by the rule $g(x) = \frac{1}{2} \cdot \left(\frac{x}{1 + |x|} \right) + \frac{1}{2}$ for all real numbers x. To show that g is one-to-one, suppose x_1 and x_2 are in $\mathbf{R}$ and $g(x_1) = g(x_2)$. It follows that x_1 and x_2 have the same sign because if $x_1 < 0$ and $x_2 > 0$, then $g(x_1) < \frac{1}{2}$ and $g(x_2) > \frac{1}{2}$ and if $x_1 > 0$ and $x_2 < 0$, then $g(x_1) > \frac{1}{2}$ and $g(x_2) < \frac{1}{2}$. Now if $x_1 > 0$ and $x_2 > 0$, then $|x_1| = x_1$ and $|x_2| = x_2$, and so the condition $g(x_1) = g(x_2)$ implies that $\frac{x_1}{1 + x_1} = \frac{x_2}{1 + x_2}$. Cross multiplying gives $x_1 + x_1 x_2 = x_2 + x_1 x_2$, which implies that $x_1 = x_2$. Furthermore, if $x_1 < 0$ and $x_2 < 0$, then $|x_1| = -x_1$ and $|x_2| = -x_2$, and so the condition $g(x_1) = g(x_2)$ implies that $\frac{x_1}{1 - x_1} = \frac{x_2}{1 - x_2}$. Cross multiplying gives $x_1 - x_1 x_2 = x_2 - x_1 x_2$, which implies that $x_1 = x_2$. Therefore, in all cases if $g(x_1) = g(x_2)$ then $x_1 = x_2$, and so g is one-to-one.

To show that g is onto, let $y \in S = \{x \in \mathbf{R} \mid 0 < x < 1\}$. In case $0 < y < \frac{1}{2}$, let $x = \frac{2y - 1}{2y}$ and note that $x < 0$. Then

$$
\begin{aligned}
g(x) &= g\left(\frac{2y-1}{2y}\right) \\
&= \frac{1}{2}\left(\frac{\frac{2y-1}{2y}}{1 + \left|\frac{2y-1}{2y}\right|} \right) + \frac{1}{2} \\
&= \frac{1}{2}\left(\frac{\frac{2y-1}{2y}}{1 - \frac{2y-1}{2y}} \right) + \frac{1}{2} \\
&= \frac{1}{2}\left(\frac{2y-1}{2y - 2y - 1} \right) + \frac{1}{2} = y - \frac{1}{2} + \frac{1}{2} = y.
\end{aligned}
$$

In case $\frac{1}{2} \le y < 1$, let $x = \frac{2y - 1}{2(1 - y)}$ and note that $x \ge 0$. Then

$$g(x) = g\left(\frac{2y-1}{2(1-y)}\right)$$

$$= \frac{1}{2} \cdot \left(\frac{\frac{2y-1}{2(1-y)}}{1 + \left|\frac{2y-1}{2(1-y)}\right|}\right) + \frac{1}{2}$$

$$= \frac{1}{2} \cdot \left(\frac{\frac{2y-1}{2(1-y)}}{1 + \frac{2y-1}{2(1-y)}}\right) + \frac{1}{2}$$

$$= \frac{1}{2} \cdot \left(\frac{2y-1}{2 - 2y + 2y - 1}\right) + \frac{1}{2}$$

$$= y - \frac{1}{2} + \frac{1}{2}$$

$$= y.$$

Therefore, in either case there exists a real number x such that $g(x) = y$, and so g is onto. Since g is both one-to-one and onto, g is a one-to-one correspondence. It follows that the set of all real numbers and S have the same cardinality.

Proof (with calculus): To show that g is one-to-one, note that for all $x > 0$,

$$g(x) = \frac{1}{2} \cdot \frac{x}{1+x} + \frac{1}{2}.$$

Then

$$g'(x) = \frac{1}{2}\left(\frac{(1+x)-x}{(1+x)^2}\right) = \frac{1}{2(1+x)^2} > 0.$$

Hence g is increasing on the interval $(0, \infty)$. In addition, for all $x < 0$,

$$g(x) = \frac{1}{2} \cdot \frac{x}{1-x} + \frac{1}{2}.$$

Then

$$g'(x) = \frac{1}{2}\left(\frac{(1-x)-x}{(1-x)^2}\right) = \frac{1-2x}{2(1-x)^2} > 0.$$

Hence g is increasing on the interval $(-\infty, 0)$. Now if $x < 0$, then $g(x) < 1/2$, and if $x \geq 0$, then $g(x) \geq 1/2$. Putting this information together with the fact that g is increasing on the intervals $(-\infty, 0)$ and $(0, \infty)$ gives that g is increasing on the entire set of real numbers, and so g is one-to-one. (See the solution to exercise 18 of Section 9.1 for a proof of this last fact.) To show g is onto, note that $\lim_{x \to \infty} g(x) = 1$ and $\lim_{x \to -\infty} g(x) = 0$. Also g is continuous on its entire domain (because g is obviously differentiable for all $x \neq 0$ and $\lim_{x \to 0^-} g(x) = \frac{1}{2} = \lim_{x \to 0^+} g(x)$). Hence by definition of limit and the intermediate value theorem, g takes every value strictly between 0 and 1. So g is onto. Since g is also one-to-one, g is a one-to-one correspondence. It follows that the set of all real numbers and S have the same cardinality.

15. Let B be the set of all bit strings (strings of 0's and 1's). Define a function $F: \mathbf{Z}^+ \to B$ as follows: $F(1) = \epsilon$, $F(2) = 0$, $F(3) = 1$, $F(4) = 00$, $F(5) = 01$, $F(6) = 10$, $F(7) = 11$, $F(8) = 000$, $F(9) = 001$, $F(10) = 010$, and so forth. At each stage, all the strings of length k are counted before the strings of length $k+1$, and the strings of length k are counted in order of increasing magnitude when interpreted as binary representations of integers. Thus the set of all bit strings is countably infinite and hence countable.

Note: A more formal definition for F is the following:

$$F(n) = \begin{cases} \epsilon & \text{if } n = 1 \\ \text{the } k\text{-bit binary representation of } n - 2^k & \text{if } \lfloor \log_2 n \rfloor = k. \end{cases}$$

For example, $F(7) = 11$ because $\lfloor \log_2 7 \rfloor = 2$ and the two-bit binary representation of $7 - 2^2$ ($= 3$) is 11.

17. Suppose r_1 and r_2 are any two rational numbers with $r_1 < r_2$. Let $x = (r_1 + r_2)/2$. Now $r_1 + r_2$ is rational by Theorem 3.2.2, and so $x = (r_1 + r_2)/2$ is rational by exercise 17 of Section 3.2. Furthermore, since $r_1 < r_2$, $r_1 + r_1 < r_2 + r_1$, which implies that $2r_1 < r_1 + r_2$, or equivalently $r_1 < (r_1 + r_2)/2$. Similarly, since $r_1 < r_2$, $r_1 + r_2 < r_2 + r_2$, which implies that $r_1 + r_2 < 2r_2$, or equivalently $(r_1 + r_2)/2 < r_2$. Putting the inequalities together gives $r_1 < x < r_2$.

18. No. For instance, both $\sqrt{2}$ and $-\sqrt{2}$ are irrational (by Theorem 3.7.1 and exercise 21 in Section 3.6), and yet their average is $(\sqrt{2} + (-\sqrt{2}))/2$ which equals 0 and is rational.

    More generally: If r is any rational number and x is any irrational number, then both $r + x$ and $r - x$ are irrational (by the result of exercise 11 in Section 3.6 or by the combination of Theorem 3.6.3 and exercise 9 in Section 3.6). Yet the average of these numbers is $((r+x)+(r-x))/2 = r$, which is rational.

19. *Proof*: Suppose r and s are real numbers with $0 < r < s$. Let n be an integer such that $\dfrac{\sqrt{2}}{s - r} < n$. Then $\dfrac{\sqrt{2}}{n} < s - r$. Let $m = \dfrac{nr}{\sqrt{2}} + 1$. Then m is an integer and $m - 1 \le \dfrac{nr}{\sqrt{2}} < m$. Multiply all parts of the inequality by $\sqrt{2}$ and divide by n to obtain $\dfrac{\sqrt{2}(m - 1)}{n} \le r < \dfrac{\sqrt{2}m}{n}$. Now since $s = r + (s - r)$ and $\dfrac{\sqrt{2}}{n} < s - r$, then $\dfrac{\sqrt{2}m}{n} = \dfrac{\sqrt{2}(m - 1)}{n} + \dfrac{\sqrt{2}}{n} \le r + \dfrac{\sqrt{2}}{n} < s$. Hence, *[by transitivity of order]* $r < \dfrac{\sqrt{2}m}{n} < s$. Note that $\dfrac{\sqrt{2}m}{n}$ is irrational because m and n are integers, $\dfrac{\sqrt{2}m}{n} = \dfrac{m}{n} \cdot \sqrt{2}$, and the product of a nonzero rational number and an irrational number is irrational (exercise 10 of Section 3.6).

20. *Two examples of many*: Define f and g from $\mathbf{Z}$ to $\mathbf{Z}$ as follows: $f(n) = 2n$ and $g(n) = 4n - 5$ for all integers n. By exercises 12 and 13 of Section 7.2, these functions are one-to-one but not onto.

21. *Two examples of many*: Define $F \colon \mathbf{Z} \to \mathbf{Z}$ by the rule $F(n) = \begin{cases} n/2 & \text{if } n \text{ is even} \\ 0 & \text{if } n \text{ is odd} \end{cases}$. Then F is onto because given any integer m, $m = F(2m)$. But F is not one-to-one because, for instance, $F(1) = F(3) = 0$.

    Define $G \colon \mathbf{Z} \to \mathbf{Z}$ by the rule $G(n) = \lfloor n/2 \rfloor$ for all integers n. Then G is onto because given any integer m, $m = \lfloor m \rfloor = \lfloor (2m)/2 \rfloor = G(2m)$. But G is not one-to-one because, for instance, $G(2) = \lfloor 2/2 \rfloor = 1$ and $G(3) = \lfloor 3/2 \rfloor = 1$ and $2 \ne 3$.

22. First note that g is one-to-one. For suppose $g(a, b) = g(c, d)$ for some ordered pairs (a, b) and (c, d) in $\mathbf{Z}^+ \times \mathbf{Z}^+$. By definition of g, $2^a 3^b = 2^c 3^d$, and so by the unique factorization theorem (Theorem 3.3.3), $a = b$ and $c = d$, or, equivalently, $(a, b) = (c, d)$. Hence there is a one-to-one correspondence between $\mathbf{Z}^+ \times \mathbf{Z}^+$ and a subset S (the range of g) of $\mathbf{Z}^+$. But by Theorem 7.5.3, any subset of a countable set is countable, and thus S is countable. It follows from the transitive property of cardinality that $\mathbf{Z}^+ \times \mathbf{Z}^+$ is also countable.

23. *b*. The fundamental observation is that if one adds up the numbers of ordered pairs along successive diagonals starting from the upper left corner, one obtains a sum of successive integers.

The reason is that the number of pairs in the $(m+1)$st diagonal is 1 more than the number in the mth diagonal. We show below that the value of H for a given pair (m,n) in the diagram is the sum of the numbers of pairs in the diagonals preceding the one containing (m,n) plus the number of the position of (m,n) in its diagonal counting down from the top starting from 0.

Starting in the upper left corner, number the diagonals of the diagram so that the diagonal containing only $(0,0)$ is 0, the diagonal containing $(1,0)$ and $(0,1)$ is 1, the diagonal containing $(2,0)$, $(1,1)$, and $(0,2)$ is 2, and so forth. Within each diagonal, number each ordered pair starting at the top. Thus within diagonal 2, for example, the pair $(2,0)$ is 0, the pair $(1,1)$ is 1 and the pair $(0,2)$ is 2. Each ordered pair of nonnegative integers can be uniquely specified by giving the number of the diagonal that contains it and stating its numerical position within that diagonal. For instance, the pair $(1,1)$ is in position 1 of diagonal 2, and the pair $(0,1)$ is in position 0 of diagonal 1. In general, each pair of the form (m,n) lies in diagonal $m+n$, and its position within diagonal $m+n$ is n. Observe that if the arrows in the diagram of exercise 23(a) are followed, the number of ordered pairs that precede $(m+n,0)$, the top pair of the $(m+n)$th diagonal, is the sum of the numbers of pairs in each of the diagonals from the zeroth through the $(m+n-1)$st. Since there are k pairs in the diagonal numbered $k-1$, the number of pairs that precede $(m+n,0)$ is

$$1 + 2 + 3 + \cdots + (m+n) = \frac{(m+n)(m+n+1)}{2}$$

by Theorem 4.2.2. Then $\dfrac{(m+n)(m+n+1)}{2} + n$ is the sum of the number of pairs that precede the top pair of the $(m+n)$th diagonal plus the numerical position of the pair (m,n) within the $(m+n)$th diagonal. Hence $H(n) = n + \dfrac{(m+n)(m+n+1)}{2}$ is the numerical position of the pair (m,n) in the total ordering of all the pairs if the ordering is begun with 0 at $(0,0)$ and is continued by following the arrows in the diagram of exercise 23(a).

24. The proof given below is adapted from one in *Foundations of Modern Analysis* by Jean Dieudonné, New York: Academic Press, 1969, page 14.

Proof: Suppose (a,b) and (c,d) are in $\mathbf{Z}^+ \times \mathbf{Z}^+$ and $(a,b) \neq (c,d)$.

Case 1, $a + b \neq c + d$: By interchanging (a,b) and (c,d) if necessary, we may assume that $a + b < c + d$. Then

$$
\begin{array}{lll}
H(a,b) & = & b + \dfrac{(a+b)(a+b+1)}{2} \qquad\qquad \text{by definition of } H \\[2mm]
\Rightarrow \quad H(a,b) & \leq & a + b + \dfrac{(a+b)(a+b+1)}{2} \qquad \text{because } a \geq 0 \\[2mm]
\Rightarrow \quad H(a,b) & < & (a+b+1) + \dfrac{(a+b)(a+b+1)}{2} \qquad \text{because } a+b < a+b+1 \\[2mm]
\Rightarrow \quad H(a,b) & < & \dfrac{2(a+b+1)}{2} + \dfrac{(a+b)(a+b+1)}{2} \\[2mm]
\Rightarrow \quad H(a,b) & < & \dfrac{(a+b+1)(a+b+2)}{2} \qquad \text{by factoring out } (a+b+1) \\[2mm]
\Rightarrow \quad H(a,b) & < & \dfrac{(c+d)(c+d+1)}{2} \qquad \text{since } a+b < c+d \text{ and } a, b, c, \\
 & & \qquad\qquad\qquad \text{and } d \text{ are integers, } a+b+1 \leq c+d \\[2mm]
\Rightarrow \quad H(a,b) & < & d + \dfrac{(c+d)(c+d+1)}{2} \qquad \text{because } d \geq 0 \\[2mm]
\Rightarrow \quad H(a,b) & < & H(c,d) \qquad \text{by definition of } H.
\end{array}
$$

Therefore, $H(a,b) \neq H(c,d)$.

Case 2, $a + b = c + d$: First observe that in this case $b \neq d$. For if $b = d$, then subtracting b from both sides of $a + b = c + d$ gives $a = c$, and so $(a, b) = (c, d)$, which contradicts our assumption that $(a, b) \neq (c, d)$. Hence,

$$H(a, b) = b + \frac{(a + b)(a + b + 1)}{2} = b + \frac{(c + d)(c + d + 1)}{2} \neq d + \frac{(c + d)(c + d + 1)}{2} = H(c, d),$$

and so $H(a, b) \neq H(c, d)$.

Thus both in case 1 and in case 2, $H(a, b) \neq H(c, d)$, and hence H is one-to-one.

25. There are many proofs of this fact, some more rigorous and some less rigorous.

Proof 1: Let $x = 0.199999\ldots$. Then $10x = 1.99999\ldots$, and so $10x - x = 1.8$. But also $10x - x = 9x$. Hence $9x = 1.8$, or equivalently $x = 0.2$.

Proof 2: We start by assuming that $1/3 = 0.33333\ldots$. Then $1 = 3(1/3) = 3(0.33333\ldots) = 0.99999\ldots$. Multiplying both sides by 0.1 gives $0.1 = (0.1)(0.99999\ldots) = 0.099999\ldots$. Adding 0.1 to both sides of the resulting equation gives $0.2 = 0.199999\ldots$.

Proof 3 (by contradiction): Let $x = 0.199999\ldots$ and suppose $x \neq 0.2$. This means that there is a little distance between $0.199999\ldots$ and 2 on the number line. In other words, $0.2 - x = \varepsilon$ for some positive number ε. *[We will show that this assumption leads to a contradiction by showing that however small the distance ε might be, we can construct a number of the form $0.19999\ldots 9$ with two contradictory properties: (1) its distance from 0.2 is greater than ε because it is farther from 0.2 than $0.199999\ldots$ and (2) its distance from 0.2 is less than ε by the way we constructed it.]* Let n be a positive integer such that $10^n > \frac{1}{\varepsilon}$, or equivalently such that $\varepsilon > \frac{1}{10^n}$, and let $a = 0.199999\ldots 9$ ($n - 1$ *nines*). Then $a < x < 0.2$, and so $0.2 - x < 0.2 - a$. This implies that $0.2 - a > \varepsilon$. But $0.2 - a = 0.2 - 0.199999\ldots 9$ ($n - 1$ *nines* $) = 0.000000\ldots 01$ (*n decimal places*) $= \frac{1}{10^n} < \varepsilon$. Thus $0.2 - a > \varepsilon$ and $0.2 - a < \varepsilon$, which is a contradiction. Hence the supposition is false, and so $x = 0.2$.

Proof 4 (by calculus): By the formal definition of infinite decimals using infinite series and by the formula for the sum of an infinite geometric series,

$0.199999\ldots = 0.1 + 0.09 + 0.009 + 0.0009 + \cdots$

$\qquad = 0.1 + 0.09 \left(\sum_{n=0}^{\infty} (\frac{1}{10})^n \right) = 0.1 + 0.09 \left(\frac{1}{1 - \frac{1}{10}} \right)$

$\qquad = 0.1 + 0.09 \left(\frac{1}{\frac{9}{10}} \right) = 0.1 + 0.09 \left(\frac{10}{9} \right) = 0.1 + 0.1 = 0.2.$

28. *Proof:* Suppose A and B are any two disjoint countably infinite sets. Then $A \cap B = \emptyset$ and there are one-to-one correspondences $f : \mathbf{Z}^+ \to A$ and $g : \mathbf{Z}^+ \to B$. Define $h : \mathbf{Z}^+ \to A \cup B$ as follows:

$$\text{For all integers } n \geq 1, \ h(n) = \begin{cases} f(n/2) & \text{if } n \text{ is even} \\ g((n+1)/2) & \text{if } n \text{ is odd} \end{cases} .$$

Observe that h is one-to-one because if $h(n_1) = h(n_2)$ then (since $A \cap B = \emptyset$) either both n_1 and n_2 are even or both n_1 and n_2 are odd. If both n_1 and n_2 are even, it follows by definition of h that $f(n_1/2) = f(n_2/2)$, and so since f is one-to-one, $n_1/2 = n_2/2$, which implies that $n_1 = n_2$. If both n_1 and n_2 are odd, it follows by definition of h that $g((n_1 + 1)/2) = g((n_2 + 1)/2)$, and so since g is one-to-one, $(n_1 + 1)/2 = (n_2 + 1)/2$, which implies that $n_1 = n_2$. Hence in either case $n_1 = n_2$, and so h is one-to-one.

To show that h is onto, let $y \in A \cup B$ be given. By definition of union, $y \in A$ or $y \in B$. If $y \in A$, then since f is onto, there is a positive integer m such that $f(m) = y$, and so by definition of h, $y = h(2m)$. If $y \in B$, then since g is onto, there is a positive integer m such that $g(m) = y$, and so by definition of h, $y = h(2m - 1)$. Now when m is a positive integer,

then both $2m$ and $2m - 1$ are positive integers. Thus in either case, there is a positive integer whose image under h is y. So h is onto.

The above arguments show that there is a one-to-one correspondence from $\mathbf{Z}^+$ to $A \cup B$, and so $A \cup B$ is countably infinite.

29. *Proof*: Suppose not. That is, suppose the set of all irrational numbers were countable. Then the set of all real numbers could be written as a union of two disjoint countably infinite sets: the set of all rational numbers and the set of all irrational numbers. By exercise 28 this union is countably infinite, and so the set of all real numbers would be countably infinite and hence countable. But this contradicts the fact that the set of all real numbers is uncountable (which follows immediately from Theorems 7.5.2 and 7.5.3 or Corollary 7.5.4). Hence the set of all irrational number is uncountable.

30. *Proof*: Suppose A is any finite set and B is any countably infinite set and A and B are disjoint. In case $A = \emptyset$, then $A \cup B = B$, which is countably infinite. So we may assume that for some positive integer m there are one-to-one correspondences $f\colon \{1, 2, \ldots, m\} \to A$ and $g\colon \mathbf{Z}^+ \to B$. Define a function $h\colon \mathbf{Z}^+ \to A \cup B$ as follows:
$$\text{For all integers } n,\ h(n) = \begin{cases} f(n) & \text{if } 1 \le n \le m \\ g(n - m) & \text{if } n \ge m + 1 \end{cases}.$$

Then h is one-to-one because $A \cap B = \emptyset$ and f and g are one-to-one. And h is onto because both f and g are onto and every positive integer can be written in the form $n - m$ for some integer $n \ge m + 1$. Since h is one-to-one and onto, h is a one-to-one correspondence. Therefore, $A \cup B$ is countably infinite.

31. *Proof*: Suppose A and B are any two countable sets. If A and B are both finite, then, by Theorem 6.3.1, $A \cup B$ is finite and hence countable. If at least one of A or B is countably infinite, then we consider two cases.

Case 1 ($A \cap B = \emptyset$): In this case, if A and B are both countably infinite, then, by exercise 28, $A \cup B$ is countably infinite and hence countable. If A is finite and B is countably infinite, then, by exercise 30, $A \cup B$ is countably infinite and hence countable.

Case 2 ($A \cap B \ne \emptyset$): In this case, $A \cup B = (A - B) \cup (B - A) \cup (A \cap B)$ and the sets $A - B$, $B - A$, and $A \cap B$ are mutually disjoint. Because A and B are both countable, then, by Theorem 7.5.3, each of $A - B$, $B - A$, and $A \cap B$ is also countable. Thus, by case 1, $(A - B) \cup (B - A)$ is countable and so $((A - B) \cup (B - A)) \cup (A \cap B)$ is countable. But $((A - B) \cup (B - A)) \cup (A \cap B) = A \cup B$, and thus $A \cup B$ is countable.

32. *Proof*: Use the one-to-one correspondence $F\colon \mathbf{Z}^+ \to \mathbf{Z}$ of Example 7.5.2 to define a function $G\colon \mathbf{Z}^+ \times \mathbf{Z}^+ \to \mathbf{Z} \times \mathbf{Z}$ by the equation: $G(m, n) = (F(m), F(n))$.

G *is one-to-one*: Suppose $G(a, b) = G(c, d)$. Then $(F(a), F(b)) = (F(c), F(d))$ by definition of G. So $F(a) = F(c)$ and $F(b) = F(d)$ by definition of equality of ordered pairs. Since F is one-to-one, then, $a = c$ and $b = d$, and so $(a, b) = (c, d)$.

G *is onto*: Suppose $(r, s) \in \mathbf{Z} \times \mathbf{Z}$. Then $r \in \mathbf{Z}$ and $s \in \mathbf{Z}$. Since F is onto, there exist an $m \in \mathbf{Z}^+$ and an $n \in \mathbf{Z}^+$ with $F(m) = r$ and $F(n) = s$. But, then, by definition of G, $G(m, n) = (r, s)$.

So G is a one-to-one correspondence from $\mathbf{Z}^+ \times \mathbf{Z}^+$ to $\mathbf{Z} \times \mathbf{Z}$, and thus the two sets have the same cardinality. But by exercise 22, $\mathbf{Z}^+ \times \mathbf{Z}^+$ has the same cardinality as $\mathbf{Z}^+$. So by the transitive property of cardinality, $\mathbf{Z} \times \mathbf{Z}$ has the same cardinality as $\mathbf{Z}^+$, and hence $\mathbf{Z} \times \mathbf{Z}$ is countably infinite.

33. *Proof*: First note that there are as many equations of the form $x^2 + bx + c = 0$ as there are pairs (b, c) where b and c are in $\mathbf{Z}$. By exercise 32, the set of all such pairs is countably infinite, and so the set of equations of the form $x^2 + bx + c = 0$ is countably infinite.

Next observe that, by the quadratic formula, each equation $x^2 + bx + c = 0$ has at most two solutions (which may be complex numbers):

$$x = \frac{-b + \sqrt{b^2 - 4c}}{2} \quad \text{and} \quad x = \frac{-b - \sqrt{b^2 - 4c}}{2}.$$

Let

$$R_1 = \left\{ x \mid x = \frac{-b + \sqrt{b^2 - 4c}}{2} \quad \text{for some integers } b \text{ and } c \right\},$$

$$R_2 = \left\{ x \mid x = \frac{-b - \sqrt{b^2 - 4c}}{2} \quad \text{for some integers } b \text{ and } c \right\},$$

and $R = R_1 \cup R_2$. Then R is the set of all solutions of equations of the form $x^2 + bx + c = 0$ where b and c are integers.

Define functions F_1 and F_2 from the set of equations of the form $x^2 + bx + c = 0$ to the sets R_1 and R_2 as follows:

$$F_1(x^2 + bx + c = 0) = \frac{-b + \sqrt{b^2 - 4c}}{2} \quad \text{and} \quad F_2(x^2 + bx + c = 0) = \frac{-b - \sqrt{b^2 - 4c}}{2}.$$

Then F_1 and F_2 are onto functions defined on countably infinite sets, and so, by exercise 27, R_1 and R_2 are countable. Since any union of two countable sets is countable (exercise 31), $R = R_1 \cup R_2$ is countable.

34. *Proof 1*: Define a function $f\colon \mathscr{P}(S) \to T$ as follows: For each subset A of S, let $f(A) = \chi_A(x)$, the characteristic function of A, where for all $x \in S$

$$\chi_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases}.$$

Then f is one-to-one because if $f(A_1) = f(A_2)$ then $\chi_{A_1}(x) = \chi_{A_2}(x)$ for all $x \in S$, which implies that $x \in A_1$ if, and only if, $x \in A_2$ *[for instance, if $x \in A_1$, then $\chi_{A_1}(x) = 1 = \chi_{A_2}(x)$ and so $x \in A_2$]*, or equivalently $A_1 = A_2$. Furthermore, f is onto because given any function $g\colon S \to \{0,1\}$, let A be the set of all x in S such that $g(x) = 1$. Then $g = \chi_A = f(A)$. Since f is one-to-one and onto, $\mathscr{P}(S)$ and T have the same cardinality.

Proof 2: Define $H\colon T \to \mathscr{P}(S)$ by letting $H(f) = \{ x \in S \mid f(x) = 1 \}$.

H is one-to-one: Suppose $H(f_1) = H(f_2)$. By definition of H, $\{ x \in S \mid f_1(x) = 1 \} = \{ x \in S \mid f_2(x) = 1 \}$. So for all $x \in S$, $f_1(x) = 1 \Leftrightarrow f_2(x) = 1$. This implies that for all $x \in S$, $f_1(x) = f_2(x)$ (because f_1 and f_2 only take the values 1 and 0, and so if they do not have the value 1 they must have the value 0). Thus $f_1 = f_2$.

H is onto: Suppose $A \subseteq S$. Define $g\colon A \to \{0,1\}$ as follows: for all $x \in S$,

$$g(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases}$$

Then $x \in A$ if, and only if, $g(x) = 1$, and so $A = H(g)$.

Since we have found a function $H\colon T \to \mathscr{P}(S)$ that is one-to-one and onto, we conclude that T and $\mathscr{P}(S)$ have the same cardinality.

35. *Proof (by contradiction)*: Suppose not. Suppose S and $\mathscr{P}(S)$ have the same cardinality. This means that there is a one-to-one, onto function $f\colon S \to \mathscr{P}(S)$. Let $A = \{x \in S \mid x \notin f(x)\}$. Then $A \in \mathscr{P}(S)$, and since f is onto, there is a $z \in S$ such that $A = f(z)$. Now either $z \in A$ or $z \notin A$. In case $z \in A$, then by definition of A, $z \notin f(z) = A$. Hence in this case $z \in A$ and

$z \notin A$ which is impossible. In case $z \notin A$, then since $A = f(z)$, $z \notin f(z)$ and so z satisfies the condition of membership for the set A which implies that $z \in A$. Hence in this case $z \notin A$ and $z \in A$ which is impossible. Thus in both cases a contradiction is obtained. It follows that the supposition is false, and so S and $\mathscr{P}(S)$ do not have the same cardinality.

36. *Proof*: Let B be the set of all functions from $\mathbf{Z}^+$ to $\{0, 1\}$ and let D be the set of all functions from $\mathbf{Z}^+$ to $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Elements of B can be represented as infinite sequences of 0's and 1's (for instance, 01101010110...) and elements of D can be represented as infinite sequences of digits from 0 to 9 inclusive (for instance, 20775931124...).

We define a function $H: B \to D$ as follows: For each function f in B, consider the representation of f as an infinite sequence of 0's and 1's. Such a sequence is also an infinite sequence of digits chosen from 0 to 9 inclusive (one formed without using 2,3,...,9), which represents a function in D. We define this function to be $H(f)$. More formally, for each $f \in B$, let $H(f)$ be the function in D defined by the rule $H(f)(n) = f(n)$ for all $n \in \mathbf{Z}^+$. It is clear from the definition that H is one-to-one.

We define a function $K: D \to B$ as follows: For each function g in D, consider the representation of g as a sequence of digits from 0 to 9 inclusive. Replace each of these digits by its 4-bit binary representation adding leading 0's if necessary to make a full four bits. (For instance, 2 would be replaced by 0010.) The result is an infinite sequence of 0's and 1's, which represents a function in B. This function is defined to be $K(g)$. Note that K is one-to-one because if $g_1 \neq g_2$ then the sequences representing g_1 and g_2 must have different digits in some position m, and so the corresponding sequences of 0's and 1's will differ in at least one of the positions $4m - 3, 4m - 2, 4m - 1$, or $4m$, which are the locations of the 4-bit binary representations of the digits in position m.

It can be shown that whenever there are one-to-one functions from one set to a second and from the second set back to the first, then the two sets have the same cardinality. This fact is known as the Schröder-Bernstein theorem after its two discoverers. For a proof see, for example, *Set Theory and Metric Spaces* by Irving Kaplansky, *A Survey of Modern Algebra*, Third Edition, by Garrett Birkhoff and Saunders MacLane, *Naive Set Theory* by Paul Halmos, or *Topology* by James R. Munkres. The above discussion shows that there are one-to-one functions from B to D and from D to B, and hence by the Schröder-Bernstein theorem the two sets have the same cardinality.

37. *Proof*: Let A and B be countably infinite sets and represent the distinct elements of A and the distinct elements of B as infinite sequences $A: a_1, a_2, a_3, \ldots$ and $B: b_1, b_2, b_3, \ldots$. Then all the distinct elements of $A \times B$ are listed in the following rectangular array.
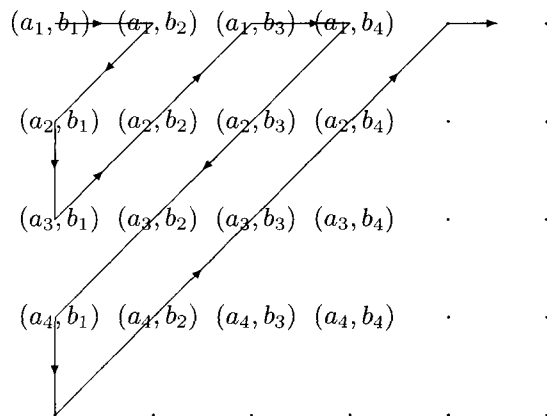
Define a function F from $\mathbf{Z}^+$ to $A \times B$ as follows: Let $F(1) = (a_1, b_1)$ and let each successive value of $F(n)$ be the next successive ordered pair obtained by following the arrows. Thus $F(2) = (a_1, b_2)$, $F(3) = (a_2, b_1)$, $F(4) = (a_3, b_1)$, $F(5) = (a_2, b_2)$, and so forth. It is clear that F is one-to-one because the elements of $A \times B$ are all distinct, and F is onto because every ordered pair in $A \times B$ appears in the array. Hence F is a one-to-one correspondence from $\mathbf{Z}^+$ to $A \times B$, and so $A \times B$ is countably infinite.

38. *Proof*: Let $A_1, A_2, A_3, \ldots$ be countable sets. Represent the elements of each A_i as an infinite sequence $A_i : a_{i1}, a_{i2}, a_{i3}, \ldots$ where if any A_i is finite, the sequence is filled out by repeating one of the elements forever. Consider the rectangular array of elements whose ith row is the sequence representing A_i for each $i = 1, 2, 3, \ldots$.
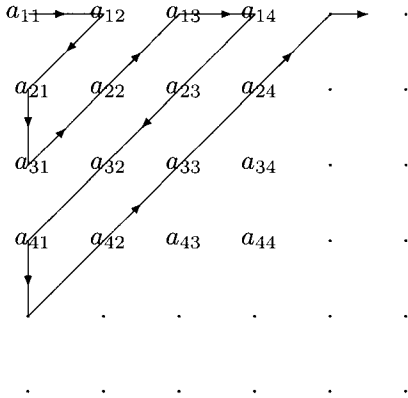
Let $\displaystyle\bigcup_{i=1}^{\infty} A_i = \{x \mid x \in A_i$ for at least one value of $i\}$, and note that each element of the array is in $\displaystyle\bigcup_{i=1}^{\infty} A_i$. Define a function G from $\mathbf{Z}^+$ to $\displaystyle\bigcup_{i=1}^{\infty} A_i$ as follows: Let $G(1) = a_{11}$ and let each successive value of $G(n)$ be the next successive element of the array obtained by following the arrows unless that element has already been made the image of some integer, in which case it is skipped. Thus (if there is no repetition) $G(2) = a_{12}$, $G(3) = a_{21}$, $G(4) = a_{31}$, $G(5) = a_{22}$, and so forth. It is clear that G is one-to-one because elements are skipped if they have already been used as function values, and G is onto because every element in $\displaystyle\bigcup_{i=1}^{\infty} A_i$ appears in the array. Hence G is a one-to-one correspondence from $\mathbf{Z}^+$ to $\displaystyle\bigcup_{i=1}^{\infty} A_i$, and so $\displaystyle\bigcup_{i=1}^{\infty} A_i$ is countably infinite and hence countable.

Chapter 8: Recursion

This chapter can be covered at any time after Chapter 4. The first three sections discuss sequences that are defined recursively and the fourth section explores recursively defined sets and functions and recursive definitions for sum, product, union, and intersection.

Section 8.1 has two aims. The primary one is to introduce students to the idea of "recursive thinking," namely assuming the answer to a problem is known for certain smaller cases and expressing the answer for a given case in terms of the answers to these smaller cases. The other related aim is simply to familiarize students with the concept and notation of a recursively defined sequence. Because the notation causes problems for some students, to help them distinguish recursive definitions from explicit formulas, the letter k is used to denote the variable in a recursive definition and the letter n is used to denote the variable in an explicit formula.

Sections 8.2 and 8.3 treat the questions of how to find an explicit formula for a sequence that has been defined recursively and how to use mathematical induction to verify that this explicit formula correctly describes the given sequence. In Section 8.2, the method used is "iteration," which consists of writing down successive terms of the sequence and looking for a pattern. In Section 8.3, explicit formulas for second-order linear homogeneous recurrence relations are derived. The main difficulty students have with these sections is related to a lack of understanding of the extent to which definitions are universal. For instance, given a recurrence relation that expresses a_k for general k in terms of a_{k-1} and a_{k-2}, quite a few students have difficulty writing, say, a_{k-1} in terms of a_{k-2} and a_{k-3}. In addition, more students than you might expect get tripped up by the algebra of successive substitution, neglecting to substitute carefully and/or making errors in multiplying out or in regrouping terms. A number of exercises are designed to address these difficulties.

Section 8.4 is not difficult for students, and at this point in the course many are able to appreciate the elegance and effectiveness of recursive definitions for describing sets that they are familiar with from other contexts. Structural induction is introduced in this section as a method for proving properties of recursively defined sequences.

Comments on Exercises

Section 8.1: #1–17, #22–26, and #46–47 develop students' skill in handling the notation and verifying properties of recursively defined sequences. Exercises #18–23, #34–43, and #53–55 explore recursive thinking. Exercises #44–50 are intended to help students develop facility with Stirling numbers of the second kind.

Section 8.2: #1 and #2 are warm-up exercises which review formulas used to simplify expressions that arise in solving recurrence relations by iteration.

Section 8.3: A number of exercises in this section are designed to give students practice in the kind of thinking used to derive the main theorems of the section. They are meant to bridge the gap between mechanical application of the theorems and formal derivation of the theorems themselves.

Section 8.4: Exercises in this section ask students to explore recursive definitions for Boolean expressions, parenthesis structures, Douglas Hofstadter's MIU-system, and other general sets of strings. Exercises are also included on McCarthy's 91 function, the Ackermann function, and Collatz's 3n+1 problem. In addition, a number of exercises give practice using structural induction.

Section 8.1

2. $b_1 = 1$, $b_2 = b_1 + 3 \cdot 2 = 7$, $b_3 = b_2 + 3 \cdot 3 = 16$, $b_4 = b_3 + 3 \cdot 4 = 28$

4. $d_0 = 3$, $d_1 = 1 \cdot d_0{}^2 = 9$, $d_2 = 2 \cdot d_1{}^2 = 162$, $d_3 = 3 \cdot d_2{}^2 = 78,732$

6. $t_0 = -1$, $t_1 = 2$, $t_2 = t_1 + 2 \cdot t_0 = 2 + 2 \cdot (-1) = 0$, $t_3 = t_2 + 2 \cdot t_1 = 0 + 2 \cdot 2 = 4$

8. $v_1 = 1$, $v_2 = 3$, $v_3 = v_2 + v_1 + 1 = 3 + 1 + 1 = 5$, $v_4 = v_3 + v_2 + 1 = 5 + 3 + 1 = 9$

10. By definition of $b_0, b_1, b_2, \ldots$, for all integers $k \geq 1$, $b_k = 4^k$ and $b_{k-1} = 4^{k-1}$. So for all integers $k \geq 1$, $4 \cdot b_{k-1} = 4 \cdot 4^{k-1} = 4^k = b_k$.

12. Call the nth term of the sequence s_n. Then $s_n = \dfrac{(-1)^n}{n!}$ for all integers $n \geq 0$. So for all integers $k \geq 1$, $s_k = \dfrac{(-1)^k}{k!}$ and $s_{k-1} = \dfrac{(-1)^{k-1}}{(k-1)!}$. It follows that for all integers $k \geq 1$,

$$\frac{-s_{k-1}}{k} = \frac{-\frac{(-1)^{k-1}}{(k-1)!}}{k} = \frac{-(-1)^{k-1}}{k \cdot (k-1)!} = \frac{(-1)^k}{k!} = s_k.$$

14. Call the nth term of the sequence d_n. Then $d_n = 3^n - 2^n$ for all integers $n \geq 0$. So for all integers $k \geq 2$, $d_k = 3^k - 2^k$, $d_{k-1} = 3^{k-1} - 2^{k-1}$, and $d_{k-2} = 3^{k-2} - 2^{k-2}$. It follows that for all integers $k \geq 2$, $5d_{k-1} - 6d_{k-2} = 5(3^{k-1} - 2^{k-1}) - 6(3^{k-2} - 2^{k-2}) = 5 \cdot 3^{k-1} - 5 \cdot 2^{k-1} - 2 \cdot 3 \cdot 3^{k-2} + 2 \cdot 3 \cdot 2^{k-2}$
$= 5 \cdot 3^{k-1} - 5 \cdot 2^{k-1} - 2 \cdot 3^{k-1} + 3 \cdot 2^{k-1} = (5-2) \cdot 3^{k-1} + (-5+3) \cdot 2^{k-1} = 3 \cdot 3^{k-1} - 2 \cdot 2^{k-1} = 3^k - 2^k = d_k$.

16. According to exercise 17 of Section 6.6, for each integer $n \geq 1$, $C_n = \dfrac{1}{4n+2}\dbinom{2n+2}{n+1}$. Substituting $k - 1$ in place of n gives

$$C_{k-1} = \frac{1}{4(k-1)+2}\binom{2(k-1)+2}{(k-1)+1} = \frac{1}{4k-2}\binom{2k}{k}.$$

Then for each integer $k \geq 2$,

$$C_k = \frac{1}{k+1}\binom{2k}{k} = \frac{1}{k+1} \cdot \frac{4k-2}{4k-2}\binom{2k}{k} = \frac{4k-2}{k+1}C_{k-1}.$$

17. $m_7 = 2m_6 + 1 = 2 \cdot 63 + 1 = 127$, $m_8 = 2m_7 + 1 = 2 \cdot 127 + 1 = 255$

18. *b.* $a_4 = 26 + 1 + 26 + 1 + 26 = 80$

19. *a.* $b_1 = 1$, $b_2 = 1 + 1 + 1 + 1 = 4$, $b_3 = 4 + 4 + 1 + 4 = 13$

c. Note that it takes just as many moves to move a stack of disks from the middle pole to an outer pole as from an outer pole to the middle pole: the moves are the same except that their order and direction are reversed. For all integers $k \geq 2$,

$b_k \quad = \quad a_{k-1}$ (moves to transfer the top $k-1$ disks from pole A to pole C)

$\qquad\qquad +1$ (move to transfer the bottom disk from pole A to pole B)

$\qquad\qquad +b_{k-1}$ (moves to transfer the top $k-1$ disks from pole C to pole B).

$\qquad = \quad a_{k-1} + 1 + b_{k-1}.$

d. One way to transfer a tower of k disks from pole A to pole B is first to transfer the top $k-1$ disks from pole A to pole B [*this requires b_{k-1} moves*], then transfer the top $k-1$ disks from pole B to pole C [*this also requires b_{k-1} moves*], then transfer the bottom disk from pole A to pole B [*this requires one move*], and finally transfer the top $k-1$ disks from pole C to pole B [*this again requires b_{k-1} moves*]. This sequence of steps need not necessarily, however, result in a minimum number of moves. Therefore, at this point, all we can say for sure is that for all integers $k \geq 2$,

$$b_k \leq b_{k-1} + b_{k-1} + 1 + b_{k-1} = 3b_{k-1} + 1.$$

e. Proof 1: In part 1 of the proof, we show that for any integer $k \geq 1$, in a tower of Hanoi with adjacency requirement, when a transfer of k disks from one end pole to the other end pole is performed, at some point all the disks are piled on the middle pole. In part 2 of the proof, we use the result of part 1 together with the result of part (c) of the problem to deduce the equation $b_k = 3b_{k-1} + 1$ for all integers $k \geq 2$.

Part 1 *(by mathematical induction)*: Let the property $P(k)$ be the sentence "In a tower of Hanoi with adjacency requirement, when a transfer of k disks from one end pole to the other end pole is performed, at some point all the disks are piled on the middle pole."

Show that the property is true for $k = 1$: The property is true for $k = 1$ because when one disk is transferred from one end pole to the other end pole with an adjacency requirement, it must first be placed on the middle pole before it can be moved to the pole at the other end.

Show that for all integers $k \geq 1$, if the property is true for $k = i$, then it is true for $k = i + 1$: Let i be an integer with $i \geq 1$, and suppose that in a tower of Hanoi with adjacency requirement, when a tower of i disks is transferred from one end pole to the other end pole, at some point all the disks are piled on the middle pole. *[This is the inductive hypothesis.]* We must show that in a tower of Hanoi with adjacency requirement, when a tower of $i + 1$ disks is transferred from one end pole to the other end pole, at some point all the disks are piled on the middle pole. So suppose $i + 1$ disks are piled on one end pole, say pole A. Call the middle pole B and the third pole C. In order to move the bottom disk from pole A, the top i disks must previously have been moved to pole C. Because of the adjacency requirement, the bottom disk must then be moved to the middle pole. Furthermore, to transfer the entire tower of $i + 1$ disks to pole C, the bottom disk must be moved to pole C. To achieve this, the top i disks must be transferred back to pole A. By inductive hypothesis, at some point while making this transfer, the top i disks will all be piled on the middle pole. But at that time, the bottom disk will be at the bottom of the middle pole *[because if it were back on pole A, transferring the top $i - 1$ disks to pole A would simply recreate the initial position of the disks]*, and so the entire tower of $i + 1$ disks will be on the middle pole. *[This is what was to be shown.]*

Part 2: By part (c) of this exercise, we know that $b_k = a_{k-1} + 1 + b_{k-1}$. Now a_{k-1} is the minimum number of moves needed to transfer a tower of $k - 1$ disks from end pole A to end pole C. By part 1 of this proof, we know that at some point during the transfer all $k - 1$ disks will be on the middle pole. But the minimum number of moves needed to put them there is, by definition, b_{k-1}. Moreover, from their position on the middle pole, the top $k - 1$ disks must be moved to pole C in order to be able to place the bottom disk on the middle pole. By symmetry, the minimum number of moves needed to transfer the top $k - 1$ disks from pole B to pole C is also b_{k-1}. Thus $a_{k-1} = b_{k-1} + b_{k-1}$, and so $b_k = b_{k-1} + b_{k-1} + 1 + b_{k-1} = 3b_{k-1} + 1$.

Proof 2 (by mathematical induction): Let the property $P(k)$ be the equation $b_k = 3b_{k-1} + 1$.

Show that the property is true for $k = 2$: The property is true for $k = 2$ because for $k = 2$ the left-hand side is 4 (by part (a)) and the right-hand side is $3 \cdot 1 + 1 = 4$ also.

Show that for all integers $i \geq 2$, if the property is true for $k = i$ then it is true for $k = i + 1$: Let i be an integer with $i \geq 2$, and suppose that $b_i = 3b_{i-1} + 1$. *[This is the inductive hypothesis.]* We must show that $b_{i+1} = 3b_i + 1$. But $b_{i+1} = a_i + 1 + b_i$ *[by part (c)]* $= a_i + 1 + 3b_{i-1} + 1$ *[by inductive hypothesis]* $= (3a_{i-1} + 2) + 1 + 3b_{i-1} + 1$ *[by exercise 18(c)]* $= 3a_{i-1} + 3 + 3b_{i-1} + 1 = 3(a_{i-1} + 1 + b_{i-1}) + 1 = 3b_i + 1$ *[by part (c) of this exercise]*. *[This is what was to be shown.]*

20. *c.* Name the poles A, B, C, and D going from left to right. Because disks can be moved from one pole to any other pole, the number of moves needed to transfer a tower of disks from any one pole to any other pole is the same for any two poles. One way to transfer a tower of k disks from pole A to pole D is to first transfer the top $k - 2$ disks from pole A to pole B, then transfer the second largest disk from pole A to pole C, then transfer the largest disk from pole A to pole D, then transfer the second largest disk from pole C to pole D, and finally transfer

the top $k - 2$ disks from pole B to pole D. This might not result in a minimal number of moves, however. So for all integers $k \geq 3$,

$$
\begin{aligned}
s_k \quad \leq \quad & s_{k-2} && \text{(moves to transfer the top } k-2 \text{ disks from pole } A \text{ to pole } B) \\
& +1 && \text{(move to transfer the second largest disk from pole } A \text{ to pole } C) \\
& +1 && \text{(move to transfer the largest disk from pole } A \text{ to pole } D) \\
& +1 && \text{(move to transfer the second largest disk from pole } C \text{ to pole } D) \\
& +s_{k-2} && \text{(moves to transfer the top } k-2 \text{ disks from pole } B \text{ to pole } D) \\
\leq \quad & 2s_{k-2} + 3.
\end{aligned}
$$

21. *a.* $t_1 = 2, \quad t_2 = 2 + 2 + 2 = 6$

c. For all integers $k \geq 2$,

$$
\begin{aligned}
t_k \quad = \quad & t_{k-1} && \text{(moves to transfer the top } 2k-2 \text{ disks from pole } A \text{ to pole } B) \\
& +2 && \text{(moves to transfer the bottom two disks from pole } A \text{ to pole } C) \\
& +t_{k-1} && \text{(moves to transfer the top } 2k-2 \text{ disks from pole } B \text{ to pole } C) \\
= \quad & 2t_{k-1} + 2.
\end{aligned}
$$

Note that transferring the stack of $2k$ disks from pole A to pole C requires at least two transfers of the top $2(k-1)$ disks: one to transfer them off the bottom two disks to free the bottom disks so that they can be moved to pole C and another to transfer the top $2(k-1)$ disks back on top of the bottom two disks. Thus at least $2t_{k-1}$ moves are needed to effect these two transfers. Two more moves are needed to transfer the bottom two disks from pole A to pole C, and this transfer cannot be effected in fewer than two moves. It follows that the sequence of moves indicated in the description of the equation above is, in fact, minimal.

22. *a.* $r_k = r_{k-1} + 4r_{k-2}$ for all integers $k \geq 3$

c. $r_7 = r_6 + 4r_5 = 181 + 4 \cdot 65 = 441$; $r_8 = r_7 + 4r_6 = 441 + 4 \cdot 181 = 1,165$; $r_9 = r_8 + 4r_7 = 1165 + 4 \cdot 441 = 2,929$; $r_{10} = r_9 + 4r_8 = 2929 + 4 \cdot 1165 = 7,589$; $r_{11} = r_{10} + 4r_9 = 7589 + 4 \cdot 2929 = 19,305$; $r_{12} = r_{11} + 4r_{10} = 19305 + 4 \cdot 7589 = 49,661$

At the end of the year there will be $r_{12} = 49,661$ rabbit pairs or 99,322 rabbits.

23. *a.* $s_k = s_{k-1} + 3s_{k-3}$ for all integers $k \geq 3$

b. $s_0 = 1, s_1 = 1, s_2 = 1, s_3 = 1 + 3 \cdot 1 = 4, s_4 = 4 + 3 \cdot 1 = 7, s_5 = 7 + 3 \cdot 1 = 10$

c. $s_6 = s_5 + 3s_3 = 22, s_7 = s_6 + 3s_4 = 43, s_8 = s_7 + 3s_5 = 73, s_9 = s_8 + 3s_6 = 139, s_{10} = s_9 + 3s_7 = 268, s_{11} = s_{10} + 3s_9 = 487, s_{12} = s_{11} + 3s_{10} = 904.$

24. $F_{13} = F_{12} + F_{11} = 233 + 144 = 377, \quad F_{14} = F_{13} + F_{12} = 377 + 233 = 610$

25. *b.* $F_{k+2} = F_{k+1} + F_k$ *c.* $F_{k+3} = F_{k+2} + F_{k+1}$

28. By definition of the Fibonacci sequence, for any integer $k \geq 1$, $F_{k+1}^2 - F_k{}^2 - F_{k-1}^2 = (F_k + F_{k-1})^2 - F_k{}^2 - F_{k-1}^2 = F_k{}^2 + 2F_kF_{k-1} + F_{k-1}^2 - F_k{}^2 - F_{k-1}^2 = 2F_kF_{k-1}$.

29. By definition of the Fibonacci sequence, for any integer $k \geq 1$, $F_{k+1}^2 - F_k{}^2 = (F_{k+1} - F_k)(F_{k+1} + F_k) = (F_{k+1} - F_k)F_{k+2}$. But since $F_{k+1} = F_k + F_{k-1}$, then $F_{k+1} - F_k = F_{k-1}$. By substitution, $F_{k+1}^2 - F_k{}^2 = F_{k-1}F_{k+2}$.

30. *d. Proof (by mathematical induction):* Let the property $P(n)$ be the equation $F_{n+2}F_n - F_{n+1}^2 = (-1)^n$.

Show that the property is true for $n = 0$: The property is true for $n = 0$ because for $n = 0$ the left-hand side is $F_{0+2}F_0 - F_1{}^2 = 2 \cdot 1 - 1^2 = 1$, and the right-hand side is $(-1)^0 = 1$ also.

Show that for all integers $k \geq 0$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let k be an integer with $k \geq 0$, and suppose that $F_{k+2}F_k - F_{k+1}^2 = (-1)^k$ for some integer $k \geq 0$. *[This is the inductive hypothesis.]* We must show that $F_{k+3}F_{k+1} - F_{k+2}^2 = (-1)^k$. But by inductive hypothesis,

$$F_{k+1}^2 = F_{k+2}F_k - (-1)^k = F_{k+2}F_k + (-1)^{k+1}. \quad \text{(We call this equation } (*).)$$

Hence,

$$
\begin{aligned}
F_{k+3}&F_{k+1} - F_{k+2}^2 \\
&= (F_{k+1} + F_{k+2})F_{k+1} - F_{k+2}^2 && \text{by definition of the Fibonacci sequence} \\
&= F_{k+1}^2 + F_{k+2}F_{k+1} - F_{k+2}^2 \\
&= F_{k+2}F_k + (-1)^{k+1} + F_{k+2}F_{k+1} - F_{k+2}^2 && \text{by substitution from equation } (*) \\
&= F_{k+2}(F_k + F_{k+1} - F_{k+2}) + (-1)^{k+1} && \text{by factoring out } F_{k+2} \\
&= F_{k+2}(F_{k+2} - F_{k+2}) + (-1)^{k+1} && \text{by definition of the Fibonacci sequence} \\
&= F_{k+2} \cdot 0 + (-1)^{k+1} \\
&= (-1)^{k+1}.
\end{aligned}
$$

32. *Proof:* In part 1 of the proof, we will show that $\displaystyle\lim_{n\to\infty} \frac{F_{2n}}{F_{2n+1}}$ exists and $\displaystyle\lim_{n\to\infty} \frac{F_{2n}}{F_{2n+1}} \geq 0$. In part 2 of the proof, we will show that $\displaystyle\lim_{n\to\infty} \frac{F_{2n+1}}{F_{2n+2}}$ exists and $\displaystyle\lim_{n\to\infty} \frac{F_{2n+1}}{F_{2n+2}} \leq 1$. In part 3, we will show that because both $\displaystyle\lim_{n\to\infty} \frac{F_{2n}}{F_{2n+1}}$ and $\displaystyle\lim_{n\to\infty} \frac{F_{2n+1}}{F_{2n+2}}$ exist and are finite, $\displaystyle\lim_{n\to\infty} \frac{F_n}{F_{n+1}}$ exists and equals $\dfrac{\sqrt{5}-1}{2}$. In parts 1 and 2, we use the result of exercise 30 that $F_{m+2}F_m - F_{m+1}^2 = (-1)^m$ for all integers $m \geq 0$. Adding F_{m+1}^2 to both sides of the equation gives that for all integers $m \geq 0$,

$$F_{m+2}F_m = F_{m+1}^2 + (-1)^m \quad \text{(We call this equation (1).)}$$

Part 1: Because all values of the Fibonacci sequence are positive, we may apply properties of inequalities, the definition of the Fibonacci sequence, and equation (1) to obtain the following sequence of if-and-only-if statements: For any integer $n \geq 0$,

$$\frac{F_{2n}}{F_{2n+1}} > \frac{F_{2n+2}}{F_{2n+3}} \Leftrightarrow F_{2n}F_{2n+3} > F_{2n+1}F_{2n+2} \quad \text{[by cross-multiplying]}$$

$$\Leftrightarrow F_{2n}(F_{2n+2} + F_{2n+1}) > F_{2n+1}(F_{2n+1} + F_{2n})$$

$$\Leftrightarrow F_{2n}F_{2n+2} > F_{2n+1}^2 \Leftrightarrow F_{2n+1}^2 + (-1)^{2n} > F_{2n+1}^2 \quad \text{[by equation (1) with } m = 2n]$$

$$\Leftrightarrow F_{2n+1}^2 + 1 > F_{2n+1}^2 \quad \text{[because } 2n \text{ is even]} \Leftrightarrow 1 > 0, \text{ which is true.}$$

Thus, since the original inequality is equivalent to an inequality that is true, the original inequality is also true. Therefore, $\dfrac{F_{2n}}{F_{2n+1}} > \dfrac{F_{2n+2}}{F_{2n+3}}$ for all integers $n \geq 0$, and hence the infinite sequence $\left\{\dfrac{F_{2n}}{F_{2n+1}}\right\}_{n=0}^{\infty}$ is strictly decreasing. Because the terms of the sequence are bounded below by 0, this implies (by a theorem from calculus) that $\displaystyle\lim_{n\to\infty} \frac{F_{2n}}{F_{2n+1}}$ exists and is greater than or equal to 0.

Part 2: As in part 1, because all values of the Fibonacci sequence are positive, we may apply properties of inequalities, the definition of the Fibonacci sequence, and equation (1) to obtain the following sequence of if-and-only-if statements: For any integer $n \geq 0$,

$\dfrac{F_{2n+1}}{F_{2n+2}} < \dfrac{F_{2n+3}}{F_{2n+4}} \Leftrightarrow F_{2n+1}F_{2n+4} < F_{2n+2}F_{2n+3}$ *[by cross-multiplying]*

$\Leftrightarrow F_{2n+1}(F_{2n+3} + F_{2n+2}) < F_{2n+2}(F_{2n+2} + F_{2n+1}) \Leftrightarrow F_{2n+1}F_{2n+3} < F_{2n+2}^2$

$\Leftrightarrow F_{2n+2}^2 + (-1)^{2n+1} < F_{2n+2}^2$ *[by equation (1) with $m = 2n + 1$]*

$\Leftrightarrow F_{2n+2}^2 - 1 < F_{2n+2}^2$ *[because $2n + 1$ is odd]* $\Leftrightarrow -1 < 0$, which is true.

Thus, since the original inequality is equivalent to an inequality that is true, the original inequality is also true. Therefore, $\dfrac{F_{2n+1}}{F_{2n+2}} < \dfrac{F_{2n+3}}{F_{2n+4}}$ for all integers $n \geq 0$, and hence the infinite sequence $\left\{ \dfrac{F_{2n+1}}{F_{2n+2}} \right\}_{n=0}^{\infty}$ is strictly increasing. Because the terms of the sequence are bounded above by 1, this implies (by a theorem from calculus) that $\displaystyle\lim_{n \to \infty} \dfrac{F_{2n+1}}{F_{2n+2}}$ exists and is less than or equal to 1.

Part 3: Let $L_1 = \displaystyle\lim_{n \to \infty} \dfrac{F_{2n}}{F_{2n+1}}$ and $L_2 = \displaystyle\lim_{n \to \infty} \dfrac{F_{2n+1}}{F_{2n+2}}$. Then

$$L_1 = \lim_{n \to \infty} \frac{F_{2n}}{F_{2n+1}} = \lim_{n \to \infty} \frac{1}{\dfrac{F_{2n+1}}{F_{2n}}} = \lim_{n \to \infty} \frac{1}{\dfrac{F_{2n} + F_{2n-1}}{F_{2n}}} = \lim_{n \to \infty} \frac{1}{1 + \dfrac{F_{2n-1}}{F_{2n}}}$$

$$= \frac{1}{1 + \displaystyle\lim_{n \to \infty} \dfrac{F_{2n-1}}{F_{2n}}} = \frac{1}{1 + L_2}.$$

Multiplying both sides by $1 + L_2$ gives that

$$L_1 + L_1 L_2 = 1. \qquad \text{(Call this equation (2).)}$$

Now $L_2 = \displaystyle\lim_{n \to \infty} \dfrac{F_{2n+1}}{F_{2n+2}} = \lim_{n \to \infty} \dfrac{1}{\dfrac{F_{2n+2}}{F_{2n+1}}} = \lim_{n \to \infty} \dfrac{1}{\dfrac{F_{2n+1} + F_{2n}}{F_{2n+1}}}$

$$= \lim_{n \to \infty} \frac{1}{1 + \dfrac{F_{2n}}{F_{2n+1}}} = \frac{1}{1 + \displaystyle\lim_{n \to \infty} \dfrac{F_{2n}}{F_{2n+1}}} = \frac{1}{1 + L_1}.$$

Multiplying both sides by $1 + L_1$ gives that

$$L_2 + L_1 L_2 = 1. \qquad \text{(Call this equation (3).)}$$

By substituting from equation (3) into equation (2), we have

$$L_1 + L_1 L_2 = L_2 + L_1 L_2$$

and subtracting $L_1 L_2$ from both sides gives that $L_1 = L_2$. Thus both subsequences $\left\{ \dfrac{F_{2n}}{F_{2n+1}} \right\}_{n=0}^{\infty}$ and $\left\{ \dfrac{F_{2n+1}}{F_{2n+2}} \right\}_{n=0}^{\infty}$ have the same limit and this is the limit for the entire sequence.

To discover the value of the limit, substitute L_1 in place of L_2 in equation (2) to obtain

$$L_1 + L_1^2 = 1, \text{ or equivalently, } L_1^2 + L_1 - 1 = 0.$$

Solving this equation with the quadratic formula and using the fact that $L_1 \geq 0$ gives that $L_1 = \dfrac{\sqrt{5} - 1}{2}$. So the limit of the sequence is $\dfrac{\sqrt{5} - 1}{2}$.

33. Let $L = \lim_{n \to \infty} x_n$. By definition of $x_0, x_1, x_2, \ldots$ and by the continuity of the square root function,

$$L = \lim_{n \to \infty} x_n = \lim_{n \to \infty} \sqrt{2 + x_{n-1}} = \sqrt{2 + \lim_{n \to \infty} x_{n-1}} = \sqrt{2 + L}.$$

Hence $L^2 = 2 + L$, and so $L^2 - L - 2 = 0$. Factoring gives $(L-2)(L+1) = 0$, and so $L = 2$ or $L = -1$. But $L \geq 0$ because each $x_i \geq 0$. Thus $L = 2$.

35. *a.* When 3% interest is compounded monthly, the interest rate per month is $0.03/12 = 0.0025$. If S_k is the amount on deposit at the end of month k, then $S_k = S_{k-1} + 0.0025 S_{k-1} = (1 + 0.0025)S_{k-1} = (1.0025)S_{k-1}$ for each integer $k \geq 1$.

b. $S_{12} = (1.0025)S_{11}$

$= (1.0025)[(1.0025)S_{10}] = (1.0025 S_{10} = (1.0025)^2[(1.0025)S_9] = (1.0025)^3 S_9$

$= (1.0025)^3[(1.0025)S_8] = (1.0025)^4 S_8 = (1.0025)^4[(1.0025)S_7] = (1.0025)^5 S_7$

$= (1.0025)^5[(1.0025)S_6] = (1.0025)^6 S_6 = (1.0025)^6[(1.0025)S_5] = (1.0025)^7 S_5$

$= (1.0025)^7[(1.0025)S_4] = (1.0025)^8 S_4 = (1.0025)^8[(1.0025)S_3] = (1.0025)^9 S_3$

$= (1.0025)^9[(1.0025)S_2] = (1.0025)^{10} S_2 = (1.0025)^{10}[(1.0025)S_1] = (1.0025)^{11} S_1$

$= (1.0025)^{11}[(1.0025)S_0] = (1.0025)^{12} S_0 = (1.0025)^{12} \cdot 10000 \cong 10,304.16$ dollars.

c. The APR $= \dfrac{10304.16 - 10000}{10000} = 0.030416 = 3.0416\%$.

37. *a.* length 0: ϵ
length 1: a, b, c
length 2: $ab, ac, ba, bb, bc, ca, cb, cc$
length 3: $aba, abb, abc, aca, acb, acc, bab, bac, bba, bbb, bbc, bca, bcb, bcc, cab, cac$
$\quad\quad\quad cba, cbb, cbc, cca, ccb, ccc$

b. By part (a), $s_0 = 1$, $s_1 = 3$, $s_2 = 8$, and $s_3 = 22$

c. Let k be an integer with $k \geq 2$. Any string of length k that does not contain the pattern aa starts with an a, with a b, or with a c. If it starts with an b or a c, this can be followed by any string of length $k - 1$ that does not contain the pattern aa. There are s_{k-1} such strings, and so there are $2s_{k-1}$ strings that start either with a b or with a c. If the string starts with an a, then the first two characters must be ab or ac. In either case, the remaining $k - 2$ characters can be any string of length $k - 2$ that does not contain the pattern aa. There are s_{k-2} such strings, and so there are $2s_{k-2}$ strings that start either ab or ac. It follows that for all integers $k \geq 2$, $s_k = 2s_{k-1} + 2s_{k-2}$.

c. By part (b) $s_2 = 8$ and $s_3 = 22$, and so $s_4 = 2s_3 + 2s_2 = 44 + 16 = 60$.

38. *a.* Let k be an integer with $k \geq 3$. The set of bit strings of length k that do not contain the pattern 101 can be partitioned into $k + 1$ subsets: the subset of strings that start with 0 and continue with any bit string of length $k - 1$ not containing 101 *[there are a_{k-1} of these]*, the subset of strings that start with 100 and continue with any bit string of length $k - 3$ not containing 101 *[there are a_{k-3} of these]*, the subset of strings that start with 1100 and continue with any bit string of length $k - 4$ not containing 101 *[there are a_{k-4} of these]*, the subset of strings that start with 11100 and continue with any bit string of length $k - 5$ not containing 101 *[there are a_{k-5} of these]*, until the following subset of strings is obtained: $\{\underbrace{11\ldots1}_{k-3 \; 1's}001, \underbrace{11\ldots1}_{k-3 \; 1's}000\}$ *[there are 2 of these and a_1 equals 2]*. In addition, the three single-element sets $\{\underbrace{11\ldots1}_{k-2 \; 1's}00\}$, $\{\underbrace{11\ldots1}_{k-1 \; 1's}0\}$, and $\{\underbrace{11\ldots1}_{k-1 \; 1's}1\}$ are in the partition, and since $a_0 = 1$

(because the only bit string of length zero that satisfies the condition is ϵ), $3 = a_0 + 2$. Thus by the addition rule,

$$a_k = a_{k-1} + a_{k-3} + a_{k-4} + \cdots + a_1 + a_0 + 2.$$

b. By part (a), if $k \geq 4$,

$$\begin{aligned}
a_k &= a_{k-1} + a_{k-3} + a_{k-4} + \cdots + a_1 + a_0 + 2 \\
a_{k-1} &= a_{k-2} + a_{k-4} + a_{k-5} + \cdots + a_1 + a_0 + 2.
\end{aligned}$$

Subtracting the second equation from the first gives

$$\begin{aligned}
a_k - a_{k-1} &= a_{k-1} + a_{k-3} - a_{k-2} \\
\Rightarrow \qquad a_k &= 2a_{k-1} + a_{k-3} - a_{k-2}. \quad \text{(Call this equation (*).)}
\end{aligned}$$

Note that $a_2 = 4$ (because all four bit strings of length 2 satisfy the condition) and $a_3 = 7$ (because all eight bit strings of length 3 satisfy the condition except 101). Thus equation (*) is also satisfied when $k = 3$ because in that case the right-hand side of the equation becomes $2a_2 + a_0 - a_1 = 2 \cdot 4 + 1 - 2 = 7$, which equals the left-hand side of the equation.

40. Imagine a tower of height k inches. If the bottom block has height one inch, then the remaining blocks make up a tower of height $k - 1$ inches. There are t_{k-1} such towers. If the bottom block has height two inches, then the remaining blocks make up a tower of height $k - 2$ inches. There are t_{k-2} such towers. If the bottom block has height four inches, then the remaining blocks make up a tower of height $k - 4$ inches. There are t_{k-4} such towers. Therefore, $t_k = t_{k-1} + t_{k-2} + t_{k-4}$ for all integers $k \geq 5$.

41. b. Let $k \geq 3$ and consider a permutation of $\{1, 2, \ldots, k\}$ that does not move any number more than one place from its "natural" position. Such a permutation either leaves 1 fixed or it interchanges 1 and 2. If it leaves 1 fixed, then the remaining $k - 1$ numbers can be permuted in any way except that they must not be moved more than one place from their natural positions. There are a_{k-1} ways to do this. If it interchanges 1 and 2, then the remaining $k - 2$ numbers can be permuted in any way except that they must not be moved more than one place from their natural positions. There are a_{k-2} ways to do this. Therefore, $a_k = a_{k-1} + a_{k-2}$ for all integers $k \geq 2$.

42. To get a sense of the problem, we compute s_4 directly. If there are four seats in the row, there can be a single student in any one of the four seats or there can be a pair of students in seats 1&3, 1&4, or 2&4. No other arrangements are possible because with more than two students, two would have to sit next to each other. Thus $s_4 = 4 + 3 = 7$. In general, if there are k chairs in a row, then

$$\begin{aligned}
s_k \;=\; & s_{k-1} \quad \text{(the number of ways a nonempty set of students can sit} \\
& \qquad \text{in the row with no two students adjacent and chair } k \text{ empty)} \\[4pt]
& +s_{k-2} \quad \text{(the number of ways students can sit in the row with chair } k \\
& \qquad \text{occupied, chair } k - 1 \text{ empty, and chairs 1 through} \\
& \qquad k - 2 \text{ occupied by a nonempty set of students in such a} \\
& \qquad \text{way that no two students are adjacent)} \\[4pt]
& +1 \quad\;\; \text{(for the seating in which chair } k \text{ is occupied} \\
& \qquad \text{and all the other chairs are empty} \\[4pt]
=\; & s_{k-1} + s_{k-2} + 1 \text{ for all integers } k \geq 3.
\end{aligned}$$

44. The partitions are

$\{x_1\}\{x_2\}\{x_3\}\{x_4,x_5\}$ $\{x_1\}\{x_2\}\{x_4\}\{x_3,x_5\}$ $\{x_1\}\{x_3\}\{x_4\}\{x_2,x_5\}$ $\{x_2\}\{x_3\}\{x_4\}\{x_1,x_5\}$
$\{x_1\}\{x_2\}\{x_5\}\{x_3,x_4\}$ $\{x_1\}\{x_3\}\{x_5\}\{x_2,x_4\}$ $\{x_2\}\{x_3\}\{x_5\}\{x_1,x_4\}$ $\{x_1\}\{x_4\}\{x_5\}\{x_2,x_3\}$
$\{x_2\}\{x_4\}\{x_5\}\{x_1,x_3\}$ $\{x_3\}\{x_4\}\{x_5\}\{x_1,x_2\}$

So $S_{5,4} = 10$.

46. By the recurrence relation from Example 8.1.11 and the values computed in Example 8.1.10, $S_{5,3} = S_{4,2} + 3 \cdot S_{4,3} = 7 + 3 \cdot 6 = 25$.

47. By the definition and initial conditions for Stirling numbers of the second kind and the results of exercises 44–46, the total number of partitions of a set with five elements is $S_{5,1} + S_{5,2} + S_{5,3} + S_{5,4} + S_{5,5} = 1 + 15 + 25 + 10 + 1 = 52$.

49. *Proof (by mathematical induction)*: Let the property $P(n)$ be the equation $\sum_{k=2}^{n} 3^{n-k} S_{k,2} = S_{n+1,3}$.

    Show that the property is true for $n = 2$: The property is true for $n = 2$ because for $n = 2$ the left-hand side of the equation is $\sum_{k=2}^{2} 3^{2-k} S_{k,2} = 3^{2-2} S_{2,2} = 1$, and the right-hand side is $S_{2+1,3} = S_{3,3} = 1$ also.

    Show that for all integers $m \geq 2$, if the property is true for $n = m$ then it is true for $n = m + 1$: Let m be an integer with $m \geq 2$, and suppose that $\sum_{k=2}^{m} 3^{m-k} S_{k,2} = S_{m+1,3}$. *[This is the inductive hypothesis.]* We must show that

$$\sum_{k=2}^{m+1} 3^{(m+1)-k} S_{k,2} = S_{m+2,3}.$$

But

$$
\begin{aligned}
\sum_{k=2}^{m+1} 3^{(m+1)-k} S_{k,2} &= \sum_{k=2}^{m} 3 \cdot 3^{m-k} S_{k,2} + 3^0 S_{m+1,2} \\
&= 3 \sum_{k=2}^{m} 3^{m-k} S_{k,2} + S_{m+1,2} \\
&= S_{m+1,2} + 3 S_{m+1,3} \qquad \text{by inductive hypothesis} \\
&= S_{m+2,3} \qquad \begin{array}{l}\text{by the recurrence relation for}\\ \text{Stirling numbers of the second kind.}\end{array}
\end{aligned}
$$

50. If X is a set with n elements and Y is a set with m elements, then the number of onto functions from X to Y is $m! S_{n,m}$, where $S_{n,m}$ is a Stirling number of the second kind. The reason is that we can construct all possible onto functions from X to Y as follows: For each partition of X into m subsets, order the subsets of the partition; call them, say, $S_1, S_2, \ldots, S_m$. Define an onto function from X to Y by first choosing an element of Y to be the image of all the elements in S_1 (there are m ways to do this), then choosing another element of Y to be the image of all the elements in S_2 (there are $m - 1$ ways to do this), then choosing another element of Y to be the image of all the elements in S_3 (there are $m - 2$ ways to do this), and so forth. Each of the $m!$ functions constructed in this way is onto because since Y has m elements and there are m subsets in the partition, eventually every element in Y will be the image of at least one element in X. Thus for each partition of X into m subsets, there are $m!$ onto functions, and so the total number of onto functions is the number of partitions, $S_{n,m}$, times $m!$, or $m! S_{n,m}$.

51. *Proof (by strong mathematical induction)*: Let the property $P(n)$ be the inequality $F_n < 2^n$ where F_n is the nth Fibonacci number.

    Show that the property is true for $n = 1$ and $n = 2$: $F_1 = 1 < 2 = 2^1$ and $F_2 = 3 < 4 = 2^2$.

Show that for all integers $k > 2$, if the property is true for all integers i with $1 \le i < k$ then it is true for k: Let k be an integer with $k > 2$, and suppose that $F_i < 2^i$ for all integers i with $0 \le i < k$. *[This is the inductive hypothesis.]* We must show that $F_k < 2^k$. Now by definition of the Fibonacci numbers, $F_k = F_{k-1} + F_{k-2}$. But by inductive hypothesis *[since $k > 2$]*, $F_{k-1} < 2^{k-1}$ and $F_{k-2} < 2^{k-2}$. Hence $F_k = F_{k-1} + F_{k-2} < 2^{k-1} + 2^{k-2} = 2^{k-2} \cdot (2 + 1) = 3 \cdot 2^{k-2} < 4 \cdot 2^{k-2} = 2^k$. Thus $F_k < 2^k$ *[as was to be shown]*.

[Since both the basis and inductive steps have been proved, we conclude that $F_n < 2^n$ for all integers $n \ge 1$.]

52. *Proof (by mathematical induction):* Let the property $P(n)$ be the equation $\gcd(F_{n+1}, F_n) = 1$.

    Show that the property is true for $n = 0$: To prove the property for $n = 0$, we must show that $\gcd(F_1, F_0) = 1$. But $F_1 = 1$ and $F_0 = 1$ and $\gcd(1, 1) = 1$.

    Show that for all integers $k \ge 0$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let k be an integer with $k \ge 0$, and suppose that $\gcd(F_{k+1}, F_k) = 1$. *[This is the inductive hypothesis.]* We must show that $\gcd(F_{k+2}, F_{k+1}) = 1$. But by definition of the Fibonacci sequence $F_{k+2} = F_{k+1} + F_k$. It follows from Lemma 3.8.2 that $\gcd(F_{k+2}, F_{k+1}) = \gcd(F_{k+1}, F_k)$. But by inductive hypothesis, $\gcd(F_{k+1}, F_k) = 1$. Hence $\gcd(F_{k+2}, F_{k+1}) = 1$ *[as was to be shown]*.

    [Since both the basis and the inductive steps have been proved, we conclude that $\gcd(F_{n+1}, F_n) = 1$ for all integers $n \ge 0$.]

53. *a.* $g_3 = 1$, $g_4 = 1$, $g_5 = 2$ (*LWLLL* and *WWLLL*)

    b. $g_6 = 4$ (*WWWLLL, WLWLLL, LWWLLL, LLWLLL*)

    c. If $k \ge 6$, then any sequence of k games must begin with exactly one of the possibilities: W, LW, or LLW. The number of sequences of k games that begin with W is g_{k-1} because the succeeding $k - 1$ games can consist of any sequence of wins and losses except that the first sequence of three consecutive losses occurs at the end. Similarly, the number of sequences of k games that begin with LW is g_{k-2} and the number of sequences of k games that begin with LLW is g_{k-3}. Therefore, $g_k = g_{k-1} + g_{k-2} + g_{k-3}$ for all integers $k \ge 6$.

54. *a.* $d_1 = 0$, $d_2 = 1$, $d_3 = 2$ (231 and 312)

    b. $d_4 = 9$ (2143, 3412, 4321, 3142, 4123, 2413, 4312, 2341, 3421)

    c. Divide the set of all derangements into two subsets: one subset, S, consists of all derangements in which the number 1 changes places with another number, and the other subset, T, consists of all derangements in which the number 1 goes to position $i \ne 1$ but i does not go to position 1. Forming a derangement in S can be regarded as a two-step process: step 1 is to choose a position i and to interchange 1 and i and step 2 is to derange the remaining $k - 2$ numbers. Now there are $k - 1$ numbers with which 1 can trade places in step 1, and so by the product rule there are $(k-1)d_{k-2}$ derangements in S. Forming a derangement in T can also be regarded as a two-step process: step 1 is to derange the $k - 1$ numbers $2, 3, \ldots, k$ in positions $2, 3, \ldots, k$, and step 2 is to interchange the number 1 in position 1 with any of the numbers in the derangement. Now there are $k - 1$ choices of numbers to interchange 1 with in step 2, and so by the multiplication rule there are $d_{k-1}(k - 1)$ derangements in T. It follows that the total number of derangements of the given k numbers is $d_k = (k - 1)d_{k-1} + (k - 1)d_{k-2}$ for all integers $k \ge 3$.

55. For each integer $k = 1, 2, \ldots, n - 1$, consider the product $(x_1 x_2 \ldots x_k)(x_{k+1} x_{k+2} \ldots x_n)$. The factor $x_1 x_2 \ldots x_k$ can be parenthesized in P_k ways, and the factor $x_{k+1} x_{k+2} \ldots x_n$ can be parenthesized in P_{n-k} ways. Therefore, the product $x_1 x_2 x_3 \ldots x_{n-1} x_n$ can be parenthesized in $P_k P_{n-k}$ ways if the final multiplication is $(x_1 x_2 \ldots x_k) \cdot (x_{k+1} x_{k+2} \ldots x_n)$. Now when $x_1 x_2 x_3 \ldots x_{n-1} x_n$ is fully parenthesized, the final multiplication can be any one of the following: $(x_1) \cdot (x_2 x_3 \ldots x_n), (x_1 x_2) \cdot (x_3 x_4 \ldots x_n), (x_1 x_2 x_3) \cdot (x_4 x_5 \ldots x_n), \ldots, (x_1 x_2 \ldots x_{n-2}) \cdot (x_{n-1} x_n),$

$(x_1 x_2 \ldots x_{n-1}) \cdot (x_n)$. So the total number of ways to parenthesize the product is the sum of all the numbers $P_k P_{n-k}$ for $k = 1, 2, \ldots, n-1$. In symbols: $P_n = \sum_{k=1}^{n-1} P_k P_{n-k}$.

Section 8.2

1. *c.* $3 + 3 \cdot 2 + 3 \cdot 3 + \cdots + 3 \cdot n + n = 3(1 + 2 + 3 + \ldots + n) + n = 3\left(\dfrac{n(n+1)}{2}\right) + n =$
$\dfrac{3n(n+1)}{2} + \dfrac{2n}{2} = \dfrac{3n^2 + 5n}{2}$.

2. *b.* $3^{n-1} + 3^{n-2} + \cdots + 3^2 + 3 + 1 = 1 + 3 + 3^2 + \cdots + 3^{n-2} + 3^{n-1} = \dfrac{3^{(n-1)+1} - 1}{3 - 1} = \dfrac{3^n - 1}{2}$.

d. Note that $\dfrac{1}{(-1)^n} = (-1)^n$ and $\dfrac{1}{(-1)^n} \cdot (-1)^k = \dfrac{1}{(-1)^{n-k}} = (-1)^{n-k}$. Thus

$2^n - 2^{n-1} + 2^{n-2} - 2^{n-3} + \cdots + (-1)^{n-2} \cdot 2^2 + (-1)^{n-1} \cdot 2 + (-1)^n$

$\begin{aligned}
&= \frac{1}{(-1)^n}\left((-1)^n 2^n + (-1)^{n-1} 2^{n-1} + (-1)^{n-2} 2^{n-2} + \cdots + (-1)^2 \cdot 2^2 + (-1)^1 \cdot 2^1 + 1\right) \\
&= \frac{1}{(-1)^n}\left(1 - 2 + 2^2 + \cdots + (-1)^{n-1} 2^{n-1} + (-1)^n 2^n\right) \\
&= (-1)^n\left(1 + (-2) + (-2)^2 + \cdots + (-2)^{n-1} + (-2)^n\right) \\
&= (-1)^n\left(\frac{(-2)^{n+1} - 1}{(-2) - 1}\right) \\
&= (-1)^n\left(\frac{1 - (-2)^{n+1}}{3}\right) \\
&= \frac{(-1)^n + 2^{n+1}}{3}.
\end{aligned}$

4. $\begin{aligned}
b_0 &= 1 \\
b_1 &= \frac{b_0}{1 + b_0} = \frac{1}{1 + 1} = \frac{1}{2} \\
b_2 &= \frac{b_1}{1 + b_1} = \frac{\frac{1}{2}}{1 + \frac{1}{2}} = \frac{1}{2 + 1} = \frac{1}{3} \\
b_3 &= \frac{b_2}{1 + b_2} = \frac{\frac{1}{3}}{1 + \frac{1}{3}} = \frac{1}{3 + 1} = \frac{1}{4} \\
b_4 &= \frac{b_3}{1 + b_3} = \frac{\frac{1}{4}}{1 + \frac{1}{4}} = \frac{1}{4 + 1} = \frac{1}{5} \\
&\vdots
\end{aligned}$

Guess: $b_n = \dfrac{1}{n+1}$ for all integers $n \geq 0$

6. $\begin{aligned}
d_1 &= 2 \\
d_2 &= 2d_1 + 3 = 2 \cdot 2 + 3 = 2^2 + 3 \\
d_3 &= 2d_2 + 3 = 2(2^2 + 3) + 3 = 2^3 + 2 \cdot 3 + 3 \\
d_4 &= 2d_3 + 3 = 2(2^3 + 2 \cdot 3 + 3) + 3 = 2^4 + 2^2 \cdot 3 + 2 \cdot 3 + 3 \\
d_5 &= 2d_4 + 3 = 2(2^4 + 2^2 \cdot 3 + 2 \cdot 3 + 3) + 3 = 2^5 + 2^3 \cdot 3 + 2^2 \cdot 3 + 2 \cdot 3 + 3 \\
&\vdots
\end{aligned}$

$$
\begin{aligned}
\text{Guess: } d_n &= 2^n + 2^{n-2} \cdot 3 + 2^{n-3} \cdot 3 + \cdots + 2^2 \cdot 3 + 2 \cdot 3 + 3 \\
&= 2^n + 3(2^{n-2} + 2^{n-3} + \cdots + 2^2 + 2 + 1) \\
&= 2^n + 3\left(\frac{2^{(n-2)+1} - 1}{2 - 1}\right) \quad \textit{[by Theorem 4.2.3]} \\
&= 2^n + 3(2^{n-1} - 1) \\
&= 2^{n-1}(2 + 3) - 3 = 5 \cdot 2^{n-1} - 3 \quad \text{for all integers } n \geq 1
\end{aligned}
$$

7.
$$
\begin{aligned}
e_0 &= 2 \\
e_1 &= 4e_0 + 5 = 4 \cdot 2 + 5 \\
e_2 &= 4e_1 + 5 = 4(4 \cdot 2 + 5) + 5 = 4^2 \cdot 2 + 4 \cdot 5 + 5 \\
e_3 &= 4e_2 + 5 = 4(4^2 \cdot 2 + 4 \cdot 5 + 5) + 5 = 4^3 \cdot 2 + 4^2 \cdot 5 + 4 \cdot 5 + 5 \\
e_4 &= 4e_3 + 5 = 4(4^3 \cdot 2 + 4^2 \cdot 5 + 4 \cdot 5 + 5) + 5 = 4^4 \cdot 2 + 4^3 \cdot 5 + 4^2 \cdot 5 + 4 \cdot 5 + 5
\end{aligned}
$$

$$
\begin{aligned}
\text{Guess: } e_n &= 4^n \cdot 2 + 4^{n-1} \cdot 5 + 4^{n-2} \cdot 5 + \cdots + 4^2 \cdot 5 + 4 \cdot 5 + 5 \\
&= 4^n \cdot 2 + 5(4^{n-1} + 4^{n-2} + \cdots + 4^2 + 4 + 1) \\
&= 4^n \cdot 2 + 5\left(\frac{4^{(n-1)+1} - 1}{4 - 1}\right) \quad \textit{[by Theorem 4.2.3]} \\
&= 4^n \cdot 2 + 5\left(\frac{4^n - 1}{3}\right) = 4^n\left(\frac{6}{3}\right) + 4^n\left(\frac{5}{3}\right) - \frac{5}{3} \\
&= \frac{11}{3} \cdot 4^n - \frac{5}{3} = \frac{1}{3}(11 \cdot 4^n - 5) \quad \text{for all integers } n \geq 1
\end{aligned}
$$

8.
$$
\begin{aligned}
f_1 &= 1 \\
f_2 &= f_1 + 2^2 = 1 + 2^2 \\
f_3 &= f_2 + 2^3 = 1 + 2^2 + 2^3 \\
f_4 &= f_3 + 2^4 = 1 + 2^2 + 2^3 + 2^4 \\
f_5 &= f_4 + 2^5 = 1 + 2^2 + 2^3 + 2^4 + 2^5
\end{aligned}
$$

$$
\begin{aligned}
\text{Guess: } f_n &= 1 + 2^2 + 2^3 + \cdots + 2^n \\
&= \left(\frac{2^{n+1} - 1}{2 - 1}\right) - 2 \quad \textit{[by Theorem 4.2.3]} \\
&= 2^{n+1} - 3 \quad \text{for all integers } n \geq 1
\end{aligned}
$$

9.
$$
\begin{aligned}
g_1 &= 1 \\
g_2 &= \frac{g_1}{g_1 + 2} = \frac{1}{1 + 2} = \frac{1}{1 + 2} \\
g_3 &= \frac{g_2}{g_2 + 2} = \frac{\dfrac{1}{1+2}}{\dfrac{1}{1+2} + 2} = \frac{1}{1 + 2(1 + 2)} = \frac{1}{1 + 2 + 2^2} \\
g_4 &= \frac{g_3}{g_3 + 2} = \frac{\dfrac{1}{1+2+2^2}}{\dfrac{1}{1+2+2^2} + 2} = \frac{1}{1 + 2(1 + 2 + 2^2)} = \frac{1}{1 + 2 + 2^2 + 2^3} \\
g_5 &= \frac{g_4}{g_4 + 2} = \frac{\dfrac{1}{1+2+2^2+2^3}}{\dfrac{1}{(1+2+2^2+2^3)} + 2} = \frac{1}{1 + 2 + 2^2 + 2^3 + 2^4}
\end{aligned}
$$

$$\vdots$$

$$
\begin{aligned}
\text{Guess: } g_n &= \frac{1}{1 + 2 + 2^2 + 2^3 + \cdots + 2^{n-1}} \\
&= \frac{1}{2^n - 1} \quad \text{[by Theorem 4.2.3)]} \quad \text{for all integers } n \geq 1
\end{aligned}
$$

11.

$$
\begin{aligned}
p_1 &= 2 \\
p_2 &= p_1 + 2 \cdot 3^2 = 2 + 2 \cdot 3^2 \\
p_3 &= p_2 + 2 \cdot 3^3 = 2 + 2 \cdot 3^2 + 2 \cdot 3^3 \\
p_4 &= p_3 + 2 \cdot 3^4 = 2 + 2 \cdot 3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 \\
p_5 &= p_4 + 2 \cdot 3^5 = 2 + 2 \cdot 3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 + 2 \cdot 3^5
\end{aligned}
$$

$$\vdots$$

$$
\begin{aligned}
\text{Guess: } p_n &= 2 + 2 \cdot 3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 + \cdots + 2 \cdot 3^n \\
&= 2 + 2 \cdot 3^2 (1 + 3 + 3^2 + \cdots + 3^{n-2}) \\
&= 2 + 18 \left(\frac{3^{n-1} - 1}{3 - 1} \right) \quad \text{[by Theorem 4.2.3]} \\
&= 2 + 18 \left(\frac{3^{n-1} - 1}{2} \right) = 2 + 9(3^{n-1} - 1) \\
&= 2 + 3^2 \cdot 3^{n-1} - 9 = 3^{n+1} - 7 \quad \text{for all integers } n \geq 1
\end{aligned}
$$

13.

$$
\begin{aligned}
t_0 &= 0 \\
t_1 &= t_0 + 3 \cdot 1 + 1 = 3 + 1 \\
t_2 &= t_1 + 3 \cdot 2 + 1 = (3 + 1) + 3 \cdot 2 + 1 = 3 + 3 \cdot 2 + 2 \\
t_3 &= t_2 + 3 \cdot 3 + 1 = ((3 + 3 \cdot 2) + 2) + 3 \cdot 3 + 1 = 3 + 3 \cdot 2 + 3 \cdot 3 + 3 \\
t_4 &= t_3 + 3 \cdot 4 + 1 = (3 + 3 \cdot 2 + 3 \cdot 3 + 3) + 3 \cdot 4 + 1 = 3 + 3 \cdot 2 + 3 \cdot 3 + 3 \cdot 4 + 4
\end{aligned}
$$

$$\vdots$$

$$
\begin{aligned}
\text{Guess: } t_n &= 3 + 3 \cdot 2 + 3 \cdot 3 + 3 \cdot 4 + \cdots + 3 \cdot n + n \\
&= 3(1 + 2 + 3 + 4 + \cdots + n) + n = 3 \left(\frac{n(n+1)}{2} \right) + n \quad \text{[by Theorem 4.2.2]} \\
&= \frac{3n^2 + 3n + 2n}{2} = \frac{3n^2 + 5n}{2} \quad \text{for all integers } n \geq 0
\end{aligned}
$$

15.

$$
\begin{aligned}
y_1 &= 1 \\
y_2 &= y_1 + 2^2 = 1 + 2^2 \\
y_3 &= y_2 + 3^2 = (1 + 2^2) + 3^2 = 1 + 2^2 + 3^2 \\
y_4 &= y_3 + 4^2 = (1 + 2^2 + 3^2) + 4^2 = 1^2 + 2^2 + 3^2 + 4^2
\end{aligned}
$$

$$\vdots$$

Guess:

$$
y_n = 1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6} \quad \text{by exercise 10 of Section 4.2}
$$

16. The recurrence relation in exercise 18(c) of Section 8.1 is $a_k = 3a_{k-1} + 2$. The initial condition is $a_1 = 2$.

$$a_1 = 2$$
$$a_2 = 3a_1 + 2 = 3 \cdot 2 + 2$$
$$a_3 = 3a_2 + 2 = 3(3 \cdot 2 + 2) + 2 = 3^2 \cdot 2 + 2 \cdot 3 + 2$$
$$a_4 = 3a_3 + 2 = 3(3^2 \cdot 2 + 2 \cdot 3 + 2) + 2 = 3^3 \cdot 2 + 3^2 \cdot 2 + 2 \cdot 3 + 2$$

$$\vdots$$

Guess:

$$a_n = 2(1 + 3 + 3^2 + \cdots + 3^{n-1}) = 2\left(\frac{3^n - 1}{3 - 1}\right) \text{ [by Theorem 4.2.3]}$$
$$= 3^n - 1 \quad \text{for all integers } n \geq 1$$

17. The recurrence relation in exercise $21(c)$ of Section 8.1 is $t_k = 2t_{k-1} + 2$. The initial condition is $t_1 = 2$.

$$t_1 = 2$$
$$t_2 = 2t_1 + 2 = 2 \cdot 2 + 2 = 2^2 + 2$$
$$t_3 = 2t_2 + 2 = 2(2^2 + 2) + 2 = 2^3 + 2^2 + 2$$
$$t_4 = 2t_3 + 2 = 2(2^3 + 2^2 + 2) + 2 = 2^4 + 2^3 + 2^2 + 2$$
$$t_5 = 2t_4 + 2 = 2(2^4 + 2^3 + 2^2 + 2) + 2 = 2^5 + 2^4 + 2^3 + 2^2 + 2$$

$$\vdots$$

Guess: $t_n = 2^n + 2^{n-1} + 2^{n-2} + \cdots + 2^2 + 2$
$$= 2(2^{n-1} + 2^{n-2} + \cdots + 2^2 + 2 + 1)$$
$$= 2\left(\frac{2^{(n-1)+1} - 1}{2 - 1}\right) = 2(2^n - 1) = 2^{n+1} - 2 \quad \text{for all integers } n \geq 1$$

20. Let t_n be the runner's target time on day n. Then $t_k = t_{k-1} - 3$ seconds for all integers $k \geq 1$. Hence $t_0, t_1, t_2, \ldots$ is an arithmetic sequence with constant adder -3. It follows that $t_n = t_0 + n(-3)$ for all integers $n \geq 0$. Now $t_0 = 3$ minutes, and 3 minutes equals 180 seconds. Hence the runner's target time on day 14 is $t_{14} = 180 + (-3)14 = 180 - 42 = 138$ seconds $= 2$ minutes 18 seconds.

21. *Proof*: Let r be a fixed constant and $a_0, a_1, a_2, \ldots$ a sequence that satisfies the recurrence relation $a_k = ra_{k-1}$ for all integers $k \geq 1$ and the initial condition $a_0 = a$. Let the property $P(n)$ be the equation $a_n = ar^n$.

    Show that the property is true for $n = 0$: For $n = 0$ the right-hand side of the equation is $ar^0 = a \cdot 1 = a$, which is also the left-hand side of the equation.

    Show that for all integers $k \geq 0$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let k be an integer with $k \geq 0$, and suppose that $a_k = ar^k$. *[This is the inductive hypothesis.]* We must show that $a_{k+1} = ar^{k+1}$. But

$$a_{k+1} = ra_k \quad \text{by definition of } a_0, a_1, a_2, \ldots$$
$$= r(ar^k) \quad \text{by substitution from the inductive hypothesis}$$
$$= ar^{k+1} \quad \text{by the laws of exponents.}$$

    [This is what was to be shown.]

22. The recurrence relation $P_k = (1 + i/m)P_{k-1}$ defines a geometric sequence with constant multiplier $1 + i/m$. Therefore, $P_n = P_0(1 + i/m)^n$ for all integers $n \geq 0$.

23. For each integer $n \geq 0$, let P_n be the population at the end of year n. Then for all integers $k \geq 1$, $P_k = P_{k-1} + (0.03)P_{k-1} = (1.03)P_{k-1}$. Hence $P_0, P_1, P_2, \ldots$ is a geometric sequence with constant multiplier 1.03, and so $P_n = P_0 \cdot (1.03)^n$ for all integers $n \geq 0$. Since $P_0 = 50$

million, it follows that the population at the end of 25 years is $P_{25} = 50 \cdot (1.03)^{25} \cong 104.7$ million.

25. For each integer $n \geq 1$, let s_{n-1} be the number of operations the algorithm executes when it is run with an input of size n. Then $s_0 = 7$ and $s_k = 2s_{k-1}$ for each integer $k \geq 1$. Therefore, $s_0, s_1, s_2, \ldots$ is a geometric sequence with constant multiplier 2, and so $s_n = s_0 \cdot 2^n = 7 \cdot 2^n$ for all integers $n \geq 0$. For an input of size 25, the number of operations executed by the algorithm is $s_{25-1} = s_{24} = 7 \cdot 2^{24} = 117,440,512$.

26. *a.* For each integer $k \geq 1$, the amount in the account at the end of k months equals the amount in the account at the end of the $(k-1)$st month plus the interest earned on that amount during the month plus the \$200 monthly addition to the account. Therefore, $A_k = A_{k-1} + (0.03/12)A_{k-1} + 200 = (1.0025)A_{k-1} + 200$.

b.

$$A_0 = 1000$$
$$A_1 = (1.0025)A_0 + 200 = 1000(1.0025) + 200$$
$$A_2 = (1.0025)A_1 + 200 = (1.0025)[1000(1.0025) + 200] + 200$$
$$= 1000(1.0025)^2 + 200(1.0025) + 200$$
$$A_3 = (1.0025)A_2 + 200 = (1.0025)[1000(1.0025)^2 + 200(1.0025) + 200] + 200$$
$$= 1000(1.0025)^3 + 200(1.0025)^2 + 200(1.0025) + 200$$
$$A_4 = (1.0025)A_3 + 200$$
$$= (1.0025)[1000(1.0025)^3 + 200(1.0025)^2 + 200(1.0025) + 200] + 200$$
$$= 1000(1.0025)^4 + 200(1.0025)^3 + 200(1.0025)^2 + 200(1.0025) + 200$$
$$\vdots$$

Guess:
$$A_n = 1000(1.0025)^n + [200(1.0025)^{n-1} + 200(1.0025)^{n-2} + \ldots$$
$$+ 200(1.0025)^2 + 200(1.0025) + 200]$$
$$= 1000(1.0025)^n + 200[(1.0025)^{n-1} + (1.0025)^{n-2} + \cdots + (1.0025)^2 + 1.0025 + 1]$$
$$= 1000(1.0025)^n + 200\left(\frac{(1.0025)^n - 1}{1.0025 - 1}\right)$$
$$= (1.0025)^n(1000) + \frac{200}{0.0025}((1.0025)^n - 1)$$
$$= (1.0025)^n(1000) + 80000((1.0025)^n - 1)$$
$$= (1000 + 80000)(1.0025)^n - 80000 = 81000(1.0025)^n - 80000$$

c. Proof (by mathematical induction): Let $A_0, A_1, A_2, \ldots$ be a sequence that satisfies the recurrence relation $A_k = (1.0025)A_{k-1} + 200$ for all integers $k \geq 1$, with initial condition $A_0 = 1000$. and let the property $P(n)$ be the equation $A_n = 81000(1.0025)^n - 80000$.

Show that the property is true for $n = 0$: For $n = 0$ the right-hand side of the equation is $81000(1.0025)^0 - 80000 = 1000$, which equals A_0, the left-hand side of the equation

Show that for all integers $k \geq 0$, if the property is true for $n = k$ then it is true for $n = k+1$: Let k be an integer with $k \geq 0$, and suppose that $A_k = 81000(1.0025)^k - 80000$. *[This is the inductive hypothesis.]* We must show that $A_{k+1} = 81000(1.0025)^{k+1} - 80000$. But

A_{k+1}	$= (1.0025)A_k + 200$	by definition of $A_0, A_1, A_2, \ldots$
	$= (1.0025)[81000(1.0025)^k - 80000] + 200$	by substitution from the inductive hypothesis
	$= 81000(1.0025)^{k+1} - 80200 + 200$	
	$= 81000(1.0025)^{k+1} - 80000$	by the laws of algebra.

[This is what was to be shown.]

e. By parts (b) and (c), $A_n = 81000(1.0025)^n - 80000$, and so we need to find the value of n for which

$$81000(1.0025)^n - 80000 = 10000.$$

But this equation holds

$$\Leftrightarrow \quad 81000(1.0025)^n = 90000$$

$$\Leftrightarrow \quad (1.0025)^n = \frac{90000}{81000} = \frac{10}{9}$$

$$\Leftrightarrow \quad \log_{10}(1.0025)^n = \log_{10}\left(\frac{10}{9}\right) \quad \text{by property (7.2.5)}$$

$$\Leftrightarrow \quad n\log_{10}(1.0025) = \log_{10}\left(\frac{10}{9}\right) \quad \text{by exercise 31 of Section 7.2}$$

$$\Leftrightarrow \quad n = \frac{\log_{10}(10/9)}{\log_{10}(1.0025)} \cong 42.2.$$

So $n \cong 42.2$ months. If interest is only paid at the end of each month, then after about 42.2 months, or about 3 1/2 years, the account will have grown to more than $10,000$.

27. *a.* Let the original balance in the account be A dollars, and let A_n be the amount owed in month n assuming the balance is not reduced by making payments during the year. The annual interest rate is 18%, and so the monthly interest rate is $(18/12)\% = 1.5\% = 0.015$. The sequence $A_0, A_1, A_2, \ldots$ satisfies the recurrence relation $A_k = A_{k-1} + 0.015A_{k-1} = 1.015A_{k-1}$. Thus $A_1 = 1.015A_0 = 1.015A$, $A_2 = 1.015A_1 = 1.015(1.015A) = (1.015)^2A$, ..., $A_{12} = 1.015A_{11} = 1.015(1.015)^{11}A = (1.015)^{12}A$. So the amount owed at the end of the year is $(1.015)^{12}A$. It follows that the APR is $\dfrac{(1.015)^{12}A - A}{A} = \dfrac{A((1.015)^{12} - 1)}{A} = (1.015)^{12} - 1 \cong$ 19.6%.

Note: Because $A_k = 1.015A_{k-1}$ for each integer $k \geq 1$, we could have immediately concluded that the sequence is geometric and, therefore, satisfies the equation $A_n = A_0(1.015)^n = A(1.015)^n$.

b. Because the person pays $150 per month to pay off the loan, the balance at the end of month k is $B_k = 1.015B_{k-1} - 150$. We use iteration to find an explicit formula for $B_0, B_1, B_2, \ldots$.

$$B_0 = 3000$$
$$B_1 = (1.015)B_0 - 150 = 1.015(3000) - 150$$
$$B_2 = (1.015)B_1 - 150 = (1.015)[1.015(3000) - 150] - 150$$
$$\quad = 3000(1.015)^2 - 150(1.015) - 150$$
$$B_3 = (1.015)B_2 - 150 = (1.015)[3000(1.015)^2 - 150(1.015) - 150] - 150$$
$$\quad = 3000(1.015)^3 - 150(1.015)^2 - 150(1.015) - 150$$
$$B_4 = (1.015)B_3 - 150$$
$$\quad = (1.015)[3000(1.015)^3 - 150(1.015)^2 - 150(1.015) - 150] - 150$$
$$\quad = 3000(1.015)^4 - 150(1.015)^3 - 150(1.015)^2 - 150(1.015) - 150$$
$$\vdots$$

Guess: $B_n = 3000(1.015)^n + [150(1.015)^{n-1} - 150(1.015)^{n-2} + \ldots$
$$\qquad\qquad\qquad\qquad\qquad -150(1.015)^2 - 150(1.015) - 150]$$

$$= 3000(1.015)^n - 150[(1.015)^{n-1} + (1.015)^{n-2} + \cdots + (1.015)^2 + 1.015 + 1]$$

$$= 3000(1.015)^n - 150\left(\frac{(1.015)^n - 1}{1.015 - 1}\right)$$

$$= (1.015)^n(3000) - \frac{150}{0.015}((1.015)^n - 1)$$

$$= (1.015)^n(3000) - 10000((1.015)^n - 1)$$

$$= (1.015)^n (3000 - 10000) + 10000$$
$$= (-7000)(1.015)^n + 10000$$

So it appears that $B_n = (-7000)(1.015)^n + 10000$. We use mathematical induction to confirm this guess.

Proof (by mathematical induction): Let $B_0, B_1, B_2, \ldots$ be a sequence that satisfies the recurrence relation $B_k = (1.015)B_{k-1} - 150$ for all integers $k \geq 1$, with initial condition $B_0 = 3000$, and let the property $P(n)$ be the equation $B_n = (-7000)(1.015)^n + 10000$.

Show that the property is true for $n = 0$: For $n = 0$ the right-hand side of the equation is $(-7000)(1.015)^n + 10000 = 3000$, which equals B_0, the left-hand side of the equation

Show that for all integers $k \geq 0$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let k be an integer with $k \geq 0$, and suppose that $B_k = (-7000)(1.015)^k + 10000$. *[This is the inductive hypothesis.]* We must show that $B_{k+1} = (-7000)(1.015)^{k+1} + 10000$. But

$$
\begin{aligned}
B_{k+1} &= (1.015)B_k - 150 && \text{by definition of } B_0, B_1, B_2, \ldots \\
&= (1.015)[(-7000)(1.015)^k + 10000] - 150 && \text{by substitution from} \\
& && \text{the inductive hypothesis} \\
&= (-7000)(1.015)^{k+1} + 10150 - 150 \\
&= (-7000)(1.015)^{k+1} + 10000 && \text{by the laws of algebra.}
\end{aligned}
$$

[This is what was to be shown.]

c. By part (b), $B_n = (-7000)(1.015)^n + 10000$, and so we need to find the value of n for which

$$(-7000)(1.015)^n + 10000 = 0.$$

But this equation holds

$$
\begin{aligned}
\Leftrightarrow \quad & 7000(1.015)^n = 10000 \\
\Leftrightarrow \quad & (1.015)^n = \frac{10000}{7000} = \frac{10}{7} \\
\Leftrightarrow \quad & \log_{10}(1.015)^n = \log_{10}\left(\frac{10}{7}\right) && \text{by property (7.2.5)} \\
\Leftrightarrow \quad & n \log_{10}(1.015) = \log_{10}\left(\frac{10}{7}\right) && \text{by exercise 31 of Section 7.2} \\
\Leftrightarrow \quad & n = \frac{\log_{10}(10/7)}{\log_{10}(1.015)} \cong 24.
\end{aligned}
$$

So $n \cong 24$ months $= 2$ years. It will require approximately 2 years to pay off the balance, assuming that payments of \$150 are made each month and the balance is not increased by any additional purchases.

d. Assuming that the person makes no additional purchases and pays \$150 each month, the person will have made 24 payments of \$150 each, for a total of \$3600 to pay off the initial balance of \$3000.

29. *Proof (by mathematical induction)*: Let $b_0, b_1, b_2, \ldots$ be a sequence that satisfies the recurrence relation $b_k = \dfrac{b_{k-1}}{1 + b_{k-1}}$ for all integers $k \geq 1$, with initial condition $b_0 = 1$, and let the property $P(n)$ be the equation $b_n = \dfrac{1}{n+1}$.

Show that the property is true for $n = 0$: For $n = 0$ the right-hand side of the equation is $\dfrac{1}{0+1} = 1$, which equals b_0, the left-hand side of the equation

Show that for all integers $k \geq 0$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let k be an integer with $k \geq 0$, and suppose that $b_k = \dfrac{1}{k+1}$. *[This*

is the inductive hypothesis.] We must show that $b_{k+1} = \dfrac{1}{(k+1)+1}$, or, equivalently, that $b_{k+1} = \dfrac{1}{k+2}$. But

$$
\begin{aligned}
b_{k+1} &= \frac{b_k}{1+b_k} && \text{by definition of } b_0, b_1, b_2, \ldots \\[2mm]
&= \frac{\frac{1}{k+1}}{1 + \frac{1}{k+1}} && \text{by substitution from the inductive hypothesis} \\[2mm]
&= \frac{1}{(k+1)+1} \\[2mm]
&= \frac{1}{k+2}.
\end{aligned}
$$

[This is what was to be shown.]

31. *Proof (by mathematical induction):* Let $d_1, d_2, d_3, \ldots$. be a sequence that satisfies the recurrence relation $d_k = 2d_{k-1} + 3$ for all integers $k \geq 2$, with initial condition $d_1 = 2$, and let the property $P(n)$ be the equation $d_n = 5 \cdot 2^{n-1} - 3$.

    Show that the property is true for $n = 1$: For $n = 1$ the right-hand side of the equation is $5 \cdot 2^{1-1} - 3 = 5 - 3 = 2$, which equals d_1, the left-hand side of the equation

    Show that for all integers $k \geq 1$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let k be an integer with $k \geq 1$, and suppose that $d_k = 5 \cdot 2^{k-1} - 3$. *[This is the inductive hypothesis.]* We must show that $d_{k+1} = 5 \cdot 2^{(k+1)-1} - 3$. But

$$
\begin{aligned}
d_{k+1} &= 2d_k + 3 && \text{by definition of } d_1, d_2, d_3, \ldots \\
&= 2(5 \cdot 2^{k-1} - 3) + 3 && \text{by substitution from the inductive hypothesis} \\
&= 5 \cdot 2^k - 6 + 3 \\
&= 5 \cdot 2^{(k+1)-1} - 3 && \text{by the laws of algebra.}
\end{aligned}
$$

    [This is what was to be shown.]

32. *Proof (by mathematical induction):* Let $e_0, e_1, e_2, \ldots$ be a sequence that satisfies the recurrence relation $e_k = 4e_{k-1} + 5$ for all integers $k \geq 1$, with initial condition $e_0 = 2$, and let the property $P(n)$ be the equation $e_n = \dfrac{1}{3}(11 \cdot 4^n - 5)$.

    Show that the property is true for $n = 0$: For $n = 0$ the right-hand side of the equation is $\frac{1}{3}(11 \cdot 4^0 - 5) = \frac{1}{3}(11 - 5) = 2$, which equals e_0, the left-hand side of the equation.

    Show that for all integers $k \geq 0$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let k be an integer with $k \geq 0$, and suppose that $e_k = \dfrac{1}{3}(11 \cdot 4^k - 5)$. *[This is the inductive hypothesis.]* We must show that $e_{k+1} = \dfrac{1}{3}(11 \cdot 4^{k+1} - 5)$. But

$$
\begin{aligned}
e_{k+1} &= 4e_k + 5 && \text{by definition of } e_0, e_1, e_2, \ldots \\[2mm]
&= 4 \cdot \frac{1}{3}(11 \cdot 4^k - 5) + 5 && \text{by substitution from the inductive hypothesis} \\[2mm]
&= 4 \cdot \frac{1}{3} \cdot 11 \cdot 4^k - 4 \cdot \frac{1}{3} \cdot 5 + 5 \\[2mm]
&= \frac{1}{3} \cdot 11 \cdot 4^{k+1} - \frac{20}{3} + \frac{15}{3} \\[2mm]
&= \frac{1}{3} \cdot 11 \cdot 4^{k+1} - \frac{5}{3} \\[2mm]
&= \frac{1}{3}(11 \cdot 4^{k+1} - 5) && \text{by the laws of algebra.}
\end{aligned}
$$

    [This is what was to be shown.]

33. *Proof (by mathematical induction)*: Let $f_1, f_2, f_3, \ldots$ be a sequence that satisfies the recurrence relation $f_k = f_{k-1} + 2^k$ for all integers $k \geq 2$, with initial condition $f_1 = 1$, and let the property $P(n)$ be the equation $f_n = 2^{n+1} - 3$.

    Show that the property is true for $n = 1$: For $n = 1$ the right-hand side of the equation is $2^{1+1} - 3 = 4 - 3 = 1$, which equals f_1, the left-hand side of the equation.

    Show that for all integers $k \geq 1$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let k be an integer with $k \geq 1$, and suppose that $f_k = 2^{k+1} - 3$. *[This is the inductive hypothesis.]* We must show that $f_{k+1} = 2^{(k+1)+1} - 3$, or, equivalently, that $f_{k+1} = 2^{k+2} - 3$. But

    $$
    \begin{aligned}
    f_{k+1} &= f_k + 2^{k+1} && \text{by definition of } f_1, f_2, f_3, \ldots \\
    &= 2^{k+1} - 3 + 2^{k+1} && \text{by substitution from the inductive hypothesis} \\
    &= 2 \cdot 2^{k+1} - 3 && \\
    &= 2^{k+2} - 3 && \text{by the laws of algebra.}
    \end{aligned}
    $$

    [This is what was to be shown.]

34. *Proof (by mathematical induction)*: Let $g_1, g_2, g_3, \ldots$ be a sequence that satisfies the recurrence relation $g_k = \dfrac{g_{k-1}}{g_{k-1} + 2}$ for all integers $k \geq 2$, with initial condition $g_1 = 1$, and let the property $P(n)$ be the equation $g_n = \dfrac{1}{2^n - 1}$.

    Show that the property is true for $n = 1$: For $n = 1$ the right-hand side of the equation is $\dfrac{1}{2^1 - 1} = 1$, which equals g_1, the left-hand side of the equation.

    Show that for all integers $k \geq 1$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let k be an integer with $k \geq 1$, and suppose that $g_k = \dfrac{1}{2^k - 1}$. *[This is the inductive hypothesis.]* We must show that $g_{k+1} = \dfrac{1}{2^{k+1} - 1}$. But

    $$
    \begin{aligned}
    g_{k+1} &= \frac{g_k}{g_k + 2} && \text{by definition of } g_1, g_2, g_3, \ldots \\[2mm]
    &= \frac{\dfrac{1}{2^k - 1}}{\dfrac{1}{2^k - 1} + 2} && \text{by substitution from the inductive hypothesis} \\[2mm]
    &= \frac{1}{1 + 2(2^k - 1)} && \\[2mm]
    &= \frac{1}{1 + 2^{k+1} - 2} && \\[2mm]
    &= \frac{1}{2^{k+1} - 1} && \text{by the laws of algebra.}
    \end{aligned}
    $$

    [This is what was to be shown.]

35. *Proof by mathematical induction*: Let $h_0, h_1, h_2, \ldots$ be a sequence that satisfies the recurrence relation $h_k = 2^k - h_{k-1}$ for all integers $k \geq 1$, with initial condition $h_0 = 1$, and let the property $P(n)$ be the equation $h_n = \dfrac{2^{n+1} - (-1)^{n+1}}{3}$.

    Show that the property is true for $n = 0$: For $n = 0$ the right-hand side of the equation is $\dfrac{2^{0+1} - (-1)^{0+1}}{3} = \dfrac{2 - (-1)}{3} = 1$, which equals h_0, the left-hand side of the equation.

    Show that for all integers $k \geq 0$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let k be an integer with $k \geq 0$, and suppose that

    $$
    h_k = \frac{2^{k+1} - (-1)^{k+1}}{3}. \qquad \textit{[This is the inductive hypothesis.]}
    $$

We must show that

$$h_{k+1} = \frac{2^{(k+1)+1} - (-1)^{(k+1)+1}}{3},$$

or, equivalently, that

$$h_{k+1} = \frac{2^{k+2} - (-1)^{k+2}}{3}.$$

But

$$
\begin{aligned}
h_{k+1} &= 2^{k+1} - h_k && \text{by definition of } h_0, h_1, h_2, \ldots \\[1mm]
&= 2^{k+1} - \frac{2^{k+1} - (-1)^{k+1}}{3} && \text{by substitution from the inductive hypothesis} \\[1mm]
&= \frac{3 \cdot 2^{k+1} - 2^{k+1} + (-1)^{k+1}}{3} \\[1mm]
&= \frac{2 \cdot 2^{k+1} - (-1)^{k+2}}{3} \\[1mm]
&= \frac{2^{k+2} - (-1)^{k+2}}{3} && \text{by the laws of algebra.}
\end{aligned}
$$

[This is what was to be shown.]

36. *Proof by mathematical induction*: Let $p_1, p_2, p_3, \ldots$. be a sequence that satisfies the recurrence relation $p_k = p_{k-1} + 2 \cdot 3^k$ for all integers $k \geq 2$, with initial condition $p_1 = 2$, and let the property $P(n)$ be the equation $p_n = 3^{n+1} - 7$.

    Show that the property is true for $n = 1$: For $n = 1$ the right-hand side of the equation is $3^{1+1} - 7 = 3^2 - 7 = 9 - 7 = 2$, which equals p_1, the left-hand side of the equation.

    Show that for all integers $k \geq 1$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let k be an integer with $k \geq 1$, and suppose that $p_k = 3^{k+1} - 7$. *[This is the inductive hypothesis.]* We must show that $p_{k+1} = 3^{(k+1)+1} - 7 = 3^{k+2} - 7$. But

$$
\begin{aligned}
p_{k+1} &= p_k + 2 \cdot 3^{k+1} && \text{by definition of } p_1, p_2, p_3, \ldots \\
&= (3^{k+1} - 7) + 2 \cdot 3^{k+1} && \text{by substitution from the inductive hypothesis} \\
&= 3^{k+1}(1 + 2) - 7 \\
&= 3 \cdot 3^{k+1} - 7 \\
&= 3^{k+2} - 7 && \text{by the laws of algebra.}
\end{aligned}
$$

    [This is what was to be shown.]

37. *Proof by mathematical induction*: Let $s_0, s_1, s_2, \ldots$. be a sequence that satisfies the recurrence relation $s_k = s_{k-1} + 2k$ for all integers $k \geq 1$, with initial condition $s_0 = 3$, and let the property $P(n)$ be the equation $s_n = 3 + n(n + 1)$.

    Show that the property is true for $n = 0$: For $n = 0$ the right-hand side of the equation is $3 + 0(0 + 1) = 3$, which equals s_0.

    Show that for all integers $k \geq 0$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let k be an integer with $k \geq 0$, and suppose that $s_k = 3 + k(k + 1)$. *[This is the inductive hypothesis.]* We must show that $s_{k+1} = 3 + (k + 1)((k + 1) + 1)$, or, equivalently, that $s_{k+1} = 3 + (k + 1)(k + 2)$. But

$$
\begin{aligned}
s_{k+1} &= s_k + 2(k + 1) && \text{by definition of } s_0, s_1, s_2, \ldots \\
&= (3 + k(k + 1)) + 2(k + 1) && \text{by substitution from the inductive hypothesis} \\
&= 3 + k^2 + 3k + 2 \\
&= 3 + (k + 1)(k + 2) && \text{by the laws of algebra.}
\end{aligned}
$$

    [This is what was to be shown.]

38. *Proof by mathematical induction*: Let $t_0, t_1, t_2, \ldots$ be a sequence that satisfies the recurrence relation $t_k = t_{k-1} + 3k + 1$ for all integers $k \geq 1$, with initial condition $t_0 = 0$, and let the property $P(n)$ be the equation $t_n = \dfrac{3n^2 + 5n}{2}$.

   Show that the property is true for $n = 0$: For $n = 0$ the right-hand side of the equation is $\dfrac{3 \cdot 0^2 + 5 \cdot 0}{2} = 0$, which equals t_0.

   Show that for all integers $k \geq 0$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let k be an integer with $k \geq 0$, and suppose that $t_k = \dfrac{3k^2 + 5k}{2}$. *[This is the inductive hypothesis.]* We must show that $t_{k+1} = \dfrac{3(k+1)^2 + 5(k+1)}{2}$. But the left-hand side of this equation is

$$
\begin{aligned}
t_{k+1} &= t_k + 3(k+1) + 1 && \text{by definition of } t_0, t_1, t_2, \ldots \\
&= \frac{3k^2 + 5k}{2} + 3(k+1) + 1 && \text{by substitution from the inductive hypothesis} \\
&= \frac{3k^2 + 5k + 6k + 6 + 2}{2} \\
&= \frac{3k^2 + 11k + 8}{2} && \text{by the laws of algebra.}
\end{aligned}
$$

And the right-hand side of the equation is

$$
\frac{3(k+1)^2 + 5(k+1)}{2} = \frac{3(k^2 + 2k + 1) + 5k + 5}{2} = \frac{3k^2 + 11k + 8}{2}, \text{ also. Thus, both sides of}
$$

the equation are equal to the same quantity, and so they are equal to each other *[as was to be shown]*.

40. *Proof by mathematical induction*: Let $y_1, y_2, y_3, \ldots$ be a sequence that satisfies the recurrence relation $y_k = y_{k-1} + k^2$ for all integers $k \geq 2$, with initial condition $y_1 = 1$, and let the property $P(n)$ be the equation $y_n = \dfrac{n(n+1)(2n+1)}{6}$.

   Show that the property is true for $n = 1$: For $n = 1$ the right-hand side of the equation is $\dfrac{1 \cdot (1+1) \cdot (2 \cdot 1 + 1)}{6} = 1$, which equals y_1.

   Show that for all integers $k \geq 1$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let k be an integer with $k \geq 1$, and suppose that

$$
y_k = \frac{k(k+1)(2k+1)}{6} \text{ for some integer } k \geq 1.
$$

[This is the inductive hypothesis.]

We must show that

$$
y_{k+1} = \frac{(k+1)((k+1)+1)(2(k+1)+1)}{6},
$$

or, equivalently, that $y_{k+1} = \dfrac{(k+1)(k+2)(2k+3)}{6}$. But

$$
\begin{aligned}
y_{k+1} &= y_k + (k+1)^2 && \text{by definition of } y_1, y_2, y_3, \dots \\
&= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 && \text{by substitution from the inductive hypothesis} \\
&= \frac{k(k+1)(2k+1) + 6(k+1)^2}{6} \\
&= \frac{(k+1)[k(2k+1) + 6(k+1)]}{6} \\
&= \frac{(k+1)(2k^2 + 7k + 6)}{6} \\
&= \frac{(k+1)(k+2)(2k+3)}{6} && \text{by the laws of algebra.}
\end{aligned}
$$

[This is what was to be shown.]

41. *Proof by mathematical induction:* Let $a_1, a_2, a_3, \dots$. be a sequence that satisfies the recurrence relation $a_k = 3a_{k-1} + 2$ for all integers $k \geq 2$, with initial condition $a_1 = 2$, and let the property $P(n)$ be the equation $a_n = 3^n - 1$.

    Show that the property is true for $n = 1$: For $n = 1$ the right-hand side of the equation is $3^1 - 1 = 2$, which equals a_1.

    Show that for all integers $k \geq 1$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let k be an integer with $k \geq 1$, and suppose that $a_k = 3^k - 1$ for some integer $k \geq 1$. *[This is the inductive hypothesis.]* We must show that $a_{k+1} = 3^{k+1} - 1$. But

$$
\begin{aligned}
a_{k+1} &= 3a_k + 2 && \text{by definition of } a_1, a_2, a_3, \dots \\
&= 3(3^k - 1) + 2 && \text{by substitution from the inductive hypothesis} \\
&= 3^{k+1} - 3 + 2 \\
&= 3^{k+1} - 1 && \text{by the laws of algebra.}
\end{aligned}
$$

    [This is what was to be shown.]

42. *Proof by mathematical induction:* Let $t_1, t_2, t_3, \dots$. be a sequence that satisfies the recurrence relation $t_k = 2t_{k-1} + 2$ for all integers $k \geq 2$, with initial condition $t_1 = 2$, and let the property $P(n)$ be the equation $t_n = 2^{n+1} - 2$.

    Show that the property is true for $n = 1$ For $n = 1$ the right-hand side of the equation is $t_1 = 2^2 - 2 = 2$, which is true.

    Show that for all integers $k \geq 1$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let k be an integer with $k \geq 1$, and suppose that $t_k = 2^{k+1} - 2$. *[This is the inductive hypothesis.]* We must show that $t_{k+1} = 2^{(k+1)+1} - 2$, or, equivalently, $t_{k+1} = 2^{k+2} - 2$. But

$$
\begin{aligned}
t_{k+1} &= 2t_k + 2 && \text{by definition of } t_1, t_2, t_3, \dots \\
&= 2(2^{k+1} - 2) + 2 && \text{by inductive hypothesis} \\
&= 2^{k+2} - 4 + 2 \\
&= 2^{k+2} - 2
\end{aligned}
$$

    [This is what was to be shown.]

44. *a.*
$$
\begin{aligned}
b_1 &= 1 \\
b_2 &= 2 \\
b_3 &= \frac{2}{b_2} = \frac{2}{2} = 1 \\
b_4 &= \frac{2}{b_3} = \frac{2}{1} = 2
\end{aligned}
$$

$$b_5 = \frac{2}{b_4} = \frac{2}{2} = 1$$

$$b_6 = \frac{2}{b_5} = \frac{2}{1} = 2$$

$$b_7 = \frac{2}{b_6} = \frac{2}{2} = 1$$

.
.
.

Guess: $b_n = \begin{cases} 1 & \text{if } n \text{ is odd} \\ 2 & \text{if } n \text{ is even} \end{cases}$

b. *Proof by strong mathematical induction*: Let $b_1, b_2, b_3, \ldots$ be a sequence that satisfies the recurrence relation $b_k = \dfrac{2}{b_{k-1}}$ for all integers $k \geq 3$, with initial conditions $b_1 = 1$ and $b_2 = 2$, and let the property $P(n)$ be the equation

$$b_n = \begin{cases} 1 & \text{if } n \text{ is odd} \\ 2 & \text{if } n \text{ is even} \end{cases} .$$

Show that the property is true for $n = 1$ and $n = 2$: For $n = 1$ and $n = 2$ the right-hand sides of the equation are 1 and 2, which equal b_1 and b_2 respectively.

Show that for all integers $k > 2$, if the property is true for all i with $1 \leq i < k$ then it is true for k: Let k be an integer with $k > 2$ and suppose

$$b_i = \begin{cases} 1 & \text{if } i \text{ is odd} \\ 2 & \text{if } i \text{ is even} \end{cases} \quad \text{for all integers } i \text{ with } 1 \leq i < k.$$

[This is the inductive hypothesis.] We must show that

$$b_k = \begin{cases} 1 & \text{if } k \text{ is odd} \\ 2 & \text{if } k \text{ is even.} \end{cases}$$

But

$$
\begin{aligned}
b_k &= \frac{2}{b_{k-1}} && \text{by definition of } b_1, b_2, b_3, \ldots \\[2mm]
&= \begin{cases} \dfrac{2}{1} & \text{if } k-1 \text{ is odd} \\[2mm] \dfrac{2}{2} & \text{if } k-1 \text{ is even} \end{cases} && \text{by substitution from the inductive hypothesis} \\[2mm]
&= \begin{cases} 2 & \text{if } k \text{ is even} \\ 1 & \text{if } k \text{ is odd} \end{cases} && \text{because } k \text{ has opposite parity from } k-1.
\end{aligned}
$$

[This is what was to be shown.]

46. a.
$$
\begin{aligned}
s_0 &= 1 \\
s_1 &= 2 \\
s_2 &= 2s_0 = 2 \\
s_3 &= 2s_1 = 2 \cdot 2 = 2^2 \\
s_4 &= 2s_2 = 2 \cdot 2 = 2^2 \\
s_5 &= 2s_3 = 2 \cdot 2^2 = 2^3 \\
s_6 &= 2s_4 = 2 \cdot 2^2 = 2^3
\end{aligned}
$$

$$s_7 = 2s_5 = 2 \cdot 2^3 = 2^4$$
$$s_8 = 2s_6 = 2 \cdot 2^3 = 2^4$$

.
.
.

Guess:
$$s_{2m+1} = 2^{m+1} \qquad \text{for all integers } m \geq 0$$
$$s_{2m} = 2^m \qquad \text{for all integers } m \geq 1$$

or, equivalently,

$$s_n = \left\{ \begin{array}{ll} 2^{(n+1)/2} & \text{if } n \text{ is odd} \\ 2^{n/2} & \text{if } n \text{ is even} \end{array} \right\} = 2^{\lceil n/2 \rceil} \text{ for all integers } n \geq 0.$$

b. Proof by strong mathematical induction: Let $s_0, s_1, s_2, \ldots$ be a sequence that satisfies the recurrence relation $s_k = 2s_{k-2}$ for all integers $k \geq 2$, with initial conditions $s_0 = 1$ and $s_1 = 2$, and let the property $P(n)$ be the equation

$$s_n = 2^{\lceil n/2 \rceil} = \left\{ \begin{array}{ll} 2^{(n+1)/2} & \text{if } n \text{ is odd} \\ 2^{n/2} & \text{if } n \text{ is even} \end{array} \right. .$$

Show that the property is true for $n = 0$ and $n = 1$: For $n = 0$ and $n = 1$ the right-hand sides of the equation are $2^{0/2} = 2^0 = 1$ and $2^{(1+1)/2} = 2^1 = 2$, which equal s_0 and s_1 respectively.

Show that for all integers $k > 1$, if the property is true for all i with $0 \leq i < k$ then it is true for k: Let k be an integer with $k > 1$ and suppose

$$s_i = \left\{ \begin{array}{ll} 2^{(i+1)/2} & \text{if } i \text{ is odd} \\ 2^{i/2} & \text{if } i \text{ is even} \end{array} \right. \quad \text{for all integers } i \text{ with } 1 \leq i < k.$$

[This is the inductive hypothesis.] We must show that

$$s_k = \left\{ \begin{array}{ll} 2^{(k+1)/2} & \text{if } k \text{ is odd} \\ 2^{k/2} & \text{if } k \text{ is even.} \end{array} \right.$$

But

$$\begin{aligned}
s_k &= 2s_{k-2} &&\text{by definition of } s_0, s_1, s_2, \ldots \\
&= \left\{ \begin{array}{ll} 2 \cdot 2^{((k-2)+1)/2} & \text{if } k - 2 \text{ is odd} \\ 2 \cdot 2^{(k-2)/2} & \text{if } k - 2 \text{ is even} \end{array} \right. &&\text{by substitution from the inductive hypothesis} \\
&= \left\{ \begin{array}{ll} 2^{(k-1)/2+1} & \text{if } k \text{ is odd} \\ 2^{(k-2)/2+1} & \text{if } k \text{ is even} \end{array} \right. &&\text{because } k - 2 \text{ and } k \text{ have the same parity} \\
&= \left\{ \begin{array}{ll} 2^{(k+1)/2} & \text{if } k \text{ is odd} \\ 2^{k/2} & \text{if } k \text{ is even.} \end{array} \right.
\end{aligned}$$

[This is what was to be shown.]

47. *a.*

$$\begin{aligned}
t_0 &= 0 \\
t_1 &= 1 - t_0 = 1 - 0 = 1 \\
t_2 &= 2 - t_1 = 2 - 1 = 1 \\
t_3 &= 3 - t_2 = 3 - 1 = 2 \\
t_4 &= 4 - t_3 = 4 - 2 = 2 \\
t_5 &= 5 - t_4 = 5 - 2 = 3 \\
t_6 &= 6 - t_5 = 6 - 3 = 3
\end{aligned}$$

.
.
.

Guess: $t_n = \lceil n/2 \rceil$ for all integers $n \geq 0$

b. *Proof (by strong mathematical induction):* Let $t_0, t_1, t_2, \ldots$ be a sequence that satisfies the recurrence relation $t_k = k - t_{k-1}$ for all integers $k \geq 1$, with initial condition $t_0 = 0$, and let the property $P(n)$ be the equation $t_n = \lceil n/2 \rceil$.

Show that the property is true for $n = 0$: For $n = 0$ the right-hand side of the equation is $\lceil 0/2 \rceil = 0$, which equals t_0.

Show that for all integers $k > 0$, if the property is true for all i with $0 \leq i < k$ then it is true for k: Let k be an integer with $k > 0$ and suppose $t_i = \lceil i/2 \rceil$ for all integers i with $1 \leq i < k$. *[This is the inductive hypothesis.]* We must show that $t_k = \lceil k/2 \rceil$. But

$$
\begin{aligned}
t_k &= k - t_{k-1} && \text{by definition of } t_0, t_1, t_2, \ldots \\
&= k - \lceil (k-1)/2 \rceil && \text{by substitution from the inductive hypothesis} \\
&= \begin{cases} k - k/2 & \text{if } k \text{ is even} \\ k - (k-1)/2 & \text{if } k \text{ is odd} \end{cases} \\
&= \begin{cases} k/2 & \text{if } k \text{ is even} \\ (k+1)/2 & \text{if } k \text{ is odd} \end{cases} && \text{by the laws of algebra} \\
&= \lceil k/2 \rceil && \text{by definition of ceiling.}
\end{aligned}
$$

[This is what was to be shown.]

48. a.
$$
\begin{aligned}
w_1 &= 1 \\
w_2 &= 2 \\
w_3 &= w_1 + 3 = 1 + 3 \\
w_4 &= w_2 + 4 = 2 + 4 \\
w_5 &= w_3 + 5 = 1 + 3 + 5 \\
w_6 &= w_4 + 6 = 2 + 4 + 6 \\
w_7 &= w_5 + 7 = 1 + 3 + 5 + 7
\end{aligned}
$$

$\vdots$

Guess:
$$
\begin{aligned}
w_n &= \begin{cases} 1 + 3 + 5 + \cdots + n & \text{if } n \text{ is odd} \\ 2 + 4 + 6 + \cdots + n & \text{if } n \text{ is even} \end{cases} \\[2mm]
&= \begin{cases} \left(\dfrac{n+1}{2}\right)^2 & \text{if } n \text{ is odd} \\ 2\left(1 + 2 + 3 + \cdots + \dfrac{n}{2}\right) & \text{if } n \text{ is even} \end{cases} && \text{by exercise 5 of Section 4.2} \\[2mm]
&= \begin{cases} \left(\dfrac{n+1}{2}\right)^2 & \text{if } n \text{ is odd} \\ 2\left(\dfrac{\frac{n}{2}\left(\frac{n}{2}+1\right)}{2}\right) & \text{if } n \text{ is even} \end{cases} && \text{by Theorem 4.2.2} \\[2mm]
&= \begin{cases} \dfrac{(n+1)^2}{4} & \text{if } n \text{ is odd} \\ \dfrac{n(n+2)}{4} & \text{if } n \text{ is even} \end{cases} && \text{by the laws of algebra.}
\end{aligned}
$$

b. *Proof by strong mathematical induction:* Let $w_1, w_2, w_3, \ldots$ be a sequence that satisfies the recurrence relation $w_k = w_{k-2} + k$ for all integers $k \geq 3$, with initial conditions $w_1 = 1$ and $w_2 = 2$, and let the property $P(n)$ be the equation

$$w_n = \begin{cases} \dfrac{(n+1)^2}{4} & \text{if } n \text{ is odd} \\ \dfrac{n(n+2)}{4} & \text{if } n \text{ is even} \end{cases} \quad \text{for all integers } n \geq 1.$$

Show that the property is true for $n = 1$ ***and*** $n = 2$: For $n = 1$ and $n = 2$ the right-hand sides of the equation are $(1+1)^2/4 = 1$ and $2(2+2)/4 = 2$, which equal w_1 and w_2 respectively.

Show that for all integers $k > 2$, ***if the property is true for all*** i ***with*** $1 \leq i < k$ ***then it is true for*** k: Let k be an integer with $k > 2$ and suppose

$$w_i = \begin{cases} \dfrac{(i+1)^2}{4} & \text{if } i \text{ is odd} \\ \dfrac{i(i+2)}{4} & \text{if } i \text{ is even} \end{cases} \quad \text{for all integers } i \text{ with } 1 \leq i < k.$$

[This is the inductive hypothesis.]

We must show that

$$w_k = \begin{cases} \dfrac{(k+1)^2}{4} & \text{if } k \text{ is odd} \\ \dfrac{k(k+2)}{4} & \text{if } k \text{ is even.} \end{cases}$$

But

$$
\begin{aligned}
w_k \;=\;& w_{k-2} + k && \text{by definition of } w_1, w_2, w_3, \dots \\[4pt]
=\;& \begin{cases} \dfrac{((k-2)+1)^2}{4} + k & \text{if } k-2 \text{ is odd} \\ \dfrac{(k-2)((k-2)+2)}{4} + k & \text{if } k-2 \text{ is even} \end{cases} && \begin{array}{l}\text{by substitution from the in-} \\ \text{ductive hypothesis}\end{array} \\[4pt]
=\;& \begin{cases} \dfrac{(k-1)^2}{4} + \dfrac{4k}{4} & \text{if } k \text{ is odd} \\ \dfrac{(k-2)\cdot k}{4} + \dfrac{4k}{4} & \text{if } k \text{ is even} \end{cases} && \begin{array}{l}\text{because } k-2 \text{ and } k \text{ have the} \\ \text{same parity}\end{array} \\[4pt]
=\;& \begin{cases} \dfrac{k^2 - 2k + 1 + 4k}{4} & \text{if } k \text{ is odd} \\ \dfrac{k^2 - 2k + 4k}{4} & \text{if } k \text{ is even} \end{cases} \\[4pt]
=\;& \begin{cases} \dfrac{k^2 + 2k + 1}{4} & \text{if } k \text{ is odd} \\ \dfrac{k^2 + 2k}{4} & \text{if } k \text{ is even} \end{cases} \\[4pt]
=\;& \begin{cases} \dfrac{(k+1)^2}{4} & \text{if } k \text{ is odd} \\ \dfrac{k(k+2)}{4} & \text{if } k \text{ is even} \end{cases} && \text{by the laws of algebra.}
\end{aligned}
$$

[This is what was to be shown.]

49.

$$
\begin{aligned}
u_0 &= 2 \\
u_1 &= 2 \\
u_2 &= u_0 \cdot u_1 = 2 \cdot 2 = 2^{1+1} = 2^2 \\
u_3 &= u_1 \cdot u_2 = 2 \cdot 2^2 = 2^{1+2} = 2^3 \\
u_4 &= u_2 \cdot u_3 = 2^2 \cdot 2^3 = 2^{2+3} = 2^5 \\
u_5 &= u_3 \cdot u_4 = 2^3 \cdot 2^5 = 2^{3+5} = 2^8 \\
u_6 &= u_4 \cdot u_5 = 2^5 \cdot 2^8 = 2^{5+8} = 2^{13}
\end{aligned}
$$

Guess: $u_n = 2^{F_n}$, where F_n is the nth Fibonacci number, for all integers $n \geq 0$.

b. Proof by strong mathematical induction: Let $u_0, u_1, u_2, \ldots$ be a sequence that satisfies the recurrence relation $u_k = u_{k-2} \cdot u_{k-1}$ for all integers $k \geq 2$, with initial conditions $u_0 = 2$ and $u_1 = 2$, and let the property $P(n)$ be the equation $u_n = 2^{F_n}$, where F_n is the nth Fibonacci number.

Show that the property is true for $n = 0$ and $n = 1$: For $n = 0$ and $n = 1$, $F_0 = 1$ and $F_1 = 1$, and so the left-hand sides of the equation are $2^1 = 2$ and $2^1 = 2$, which equal u_0 and u_1 respectively.

Show that for all integers $k > 1$, if the property is true for all integers i with $0 \leq i < k$ then it is true for k: Let k be an integer with $k > 1$ and suppose $u_i = 2^{F_i}$, where F_i is the ith Fibonacci number, for all integers i with $1 \leq i < k$. *[This is the inductive hypothesis.]* We must show that $u_k = 2^{F_k}$, where F_k is the kth Fibonacci number. But

$$
\begin{aligned}
u_k &= u_{k-2} \cdot u_{k-1} & \text{by definition of } u_0, u_1, u_2, \ldots \\
&= 2^{F_{k-2}} \cdot 2^{F_{k-1}} & \text{by substitution from the inductive hypothesis} \\
&= 2^{F_{k-2}+F_{k-1}} & \text{by the laws of exponents} \\
&= 2^{F_k} & \text{by definition of the Fibonacci sequence.}
\end{aligned}
$$

[This is what was to be shown.]

51. The sequence does not satisfy the formula. By definition of $a_1, a_2, a_3, \ldots$, $a_1 = 0$, $a_2 = (a_1 + 1)^2 = 1^2 = 1$, $a_3 = (a_2 + 1)^2 = (1 + 1)^2 = 4$, $a_4 = (a_3 + 1)^2 = (4 + 1)^2 = 25$. But according to the formula $a_4 = (4 - 1)^2 = 9 \neq 25$.

52. *a.* Suppose there are $k - 1$ lines already drawn in the plane in such a way that they divide the plane into a maximum number P_{k-1} of regions. If addition of a new line is to create a maximum number of regions, it must cross all the $k - 1$ lines that are already drawn. But if all $k - 1$ lines are crossed by the new line, then one can imagine traveling along the new line from a point before it reaches the first line it crosses to a point after it reaches the last line it crosses. One sees that for each integer $i = 1, 2, \ldots, k - 1$, the region just before the ith line is reached is divided in half. This creates $k - 1$ new regions. But the final region after the last line is passed is also divided in half. This creates one additional new region, which brings the total number of new regions to k. Therefore, $P_k = P_{k-1} + k$ for all integers $k \geq 1$.

b.
$$
\begin{aligned}
P_1 &= 2 \\
P_2 &= P_1 + 2 = 2 + 2 \\
P_3 &= P_2 + 3 = 2 + 2 + 3 \\
P_4 &= P_3 + 4 = 2 + 2 + 3 + 4 = \\
P_5 &= P_4 + 5 = 2 + 2 + 3 + 4 + 5
\end{aligned}
$$

Guess:
$$
\begin{aligned}
P_n &= 2 + 2 + 3 + 4 + \cdots + n = 1 + 1 + 2 + 3 + 4 + \cdots + n \\
&= 1 + \frac{n(n+1)}{2} & \text{[by Theorem 4.2.2]} \\
&= \frac{2}{2} + \frac{n^2 + n}{2} = \frac{n^2 + n + 2}{2} & \text{for all integers } n \geq 1
\end{aligned}
$$

53.

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^2 = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} F_2 & F_1 \\ F_1 & F_0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^3 = \begin{bmatrix} 3 & 2 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} F_3 & F_2 \\ F_2 & F_1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^4 = \begin{bmatrix} 5 & 3 \\ 3 & 2 \end{bmatrix} = \begin{bmatrix} F_4 & F_3 \\ F_3 & F_2 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^5 = \begin{bmatrix} 8 & 5 \\ 5 & 3 \end{bmatrix} = \begin{bmatrix} F_5 & F_4 \\ F_4 & F_3 \end{bmatrix}$$

Guess: For all integers $n \geq 1$,

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^n = \begin{bmatrix} F_n & F_{n-1} \\ F_{n-1} & F_{n-2} \end{bmatrix}$$

Proof by mathematical induction: Let $A_2, A_3, A_4, \ldots$ be a sequence of 2×2 matrices that satisfies the recurrence relation

$$A_k = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^k = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^{k-1} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} A_{k-1}$$

for all integers $k \geq 3$, with initial condition $A_2 = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$, and let the property $P(n)$ be the equation

$$A_n = \begin{bmatrix} F_n & F_{n-1} \\ F_{n-1} & F_{n-2} \end{bmatrix},$$

where F_m is the mth Fibonacci number for $m \geq 0$.

Show that the property is true for $n = 2$: For $n = 2$, the property states that

$$A_2 = \begin{bmatrix} F_2 & F_1 \\ F_1 & F_0 \end{bmatrix}.$$

But $A_2 = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$, and the first calculation above shows that $\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} F_2 & F_1 \\ F_1 & F_0 \end{bmatrix}$. So the property is true for $n = 2$.

Show that for all integers $k \geq 2$, if the property is true for $n = k$ then it is true for $n = k + 1$: Suppose that for some integer $k \geq 2$,

$$A_k = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^k = \begin{bmatrix} F_k & F_{k-1} \\ F_{k-1} & F_{k-2} \end{bmatrix}. \qquad \text{[This is the inductive hypothesis.]}$$

Then

$$\begin{aligned}
A_{k+1} &= \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} A_k & \text{by definition of } A_2, A_3, A_4, \ldots \\[2mm]
&= \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} F_k & F_{k-1} \\ F_{k-1} & F_{k-2} \end{bmatrix} & \text{by inductive hypothesis} \\[2mm]
&= \begin{bmatrix} F_k + F_{k-1} & F_{k-1} + F_{k-2} \\ F_k & F_{k-1} \end{bmatrix} & \text{by definition of matrix multiplication} \\[2mm]
&= \begin{bmatrix} F_{k+1} & F_k \\ F_k & F_{k-1} \end{bmatrix}. & \text{by definition of the Fibonacci sequence.}
\end{aligned}$$

[This is what was to be shown.]

54. *a.*

$$Y_1 = E + c + mY_0$$

$$Y_2 = E + c + mY_1 = E + c + m(E + c + mY_0) = (E + c) + m(E + c) + m^2Y_0$$

$$Y_3 = E + c + mY_2 = E + c + m((E+c) + m(E+c) + m^2Y_0) = (E+c) + m(E+c) + m^2(E+c) + m^3Y_0$$

$$Y_4 = E + c + mY_3 = E + c + m((E + c) + m(E + c) + m^2(E + c) + m^3Y_0)$$

$$= (E + c) + m(E + c) + m^2(E + c) + m^3(E + c) + m^4Y_0$$

$$.$$
$$.$$
$$.$$

Guess: $Y_n = (E + c) + m(E + c) + m^2(E + c) + \cdots + m^{n-1}(E + c) + m^nY_0$

$$= (E + c)[1 + m + m^2 + \cdots + m^{n-1}] + m^nY_0$$

$$= (E + c)\left(\frac{m^n - 1}{m - 1}\right) + m^nY_0, \text{ for all integers } n \geq 1.$$

b. Suppose $0 < m < 1$. Then

$$\lim_{n \to \infty} Y_n = \lim_{n \to \infty} \left((E + c)\left(\frac{m^n - 1}{m - 1}\right) + m^nY_0\right)$$

$$= (E + c)\left(\frac{\lim_{n \to \infty} m^n - 1}{m - 1}\right) + \lim_{n \to \infty} m^nY_0$$

$$= (E + c)\left(\frac{0 - 1}{m - 1}\right) + 0 \cdot Y_0 \qquad \text{because when } 0 < m < 1,$$
$$\text{then } \lim_{n \to \infty} m^n = 0$$

$$= \frac{E + c}{1 - m}.$$

Section 8.3

2. *b* and *f*

3. *b.*

$$\left\{ \begin{array}{l} a_0 = C \cdot 2^0 + D = C + D = 0 \\ a_1 = C \cdot 2^1 + D = 2C + D = 2 \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} D = -C \\ 2C + (-C) = 2 \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} D = -C \\ C = 2 \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} C = 2 \\ D = -2 \end{array} \right\}$$

$$a_2 = C \cdot 2^2 + D = 2 \cdot 2^2 + (-2) = 6$$

4. *b.*

$$\left\{ \begin{array}{l} b_0 = C \cdot 3^0 + D(-2)^0 = C + D = 3 \\ b_1 = C \cdot 3^1 + D(-2)^1 = 3C - 2D = 4 \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} 2C + 2D = 6 \\ 3C - 2D = 4 \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} C = 2 \\ D = 3 - 2 = 1 \end{array} \right\}$$

$$b_2 = C \cdot 3^2 + D(-2)^2 = 2 \cdot 3^2 + 1 \cdot (-2)^2 = 18 + 4 = 22$$

6. *Proof*: Given that $b_n = C \cdot 3^n + D(-2)^n$, then for any choice of C and D and integer $k \geq 2$, $b_k = C \cdot 3^k + D(-2)^k$, $b_{k-1} = C \cdot 3^{k-1} + D(-2)^{k-1}$, and $b_{k-2} = C \cdot 3^{k-2} + D(-2)^{k-2}$. Hence, $b_{k-1} + 6b_{k-2} = \left(C \cdot 3^{k-1} + D(-2)^{k-1}\right) + 6\left(C \cdot 3^{k-2} + D(-2)^{k-2}\right) = C \cdot \left(3^{k-1} + 6 \cdot 3^{k-2}\right) + D\left((-2)^{k-1} + 6(-2)^{k-2}\right) = C \cdot 3^{k-2}(3+6) + D(-2)^{k-2}(-2+6) = C \cdot 3^{k-2} \cdot 3^2 + D(-2)^{k-2}2^2 = C \cdot 3^k + D(-2)^k = b_k.$

7.

$$\left\{ \begin{array}{l} C + D = 1 \\ C\left(\dfrac{1+\sqrt{5}}{2}\right) + D\left(\dfrac{1-\sqrt{5}}{2}\right) = 1 \end{array} \right\}$$

$$\Leftrightarrow \left\{ \begin{array}{l} C\left(\dfrac{1+\sqrt{5}}{2}\right) + D\left(\dfrac{1+\sqrt{5}}{2}\right) = \dfrac{1+\sqrt{5}}{2} \\ C\left(\dfrac{1+\sqrt{5}}{2}\right) + D\left(\dfrac{1-\sqrt{5}}{2}\right) = 1 \end{array} \right\}$$

$$\Leftrightarrow \left\{ \begin{array}{l} D\left(\dfrac{1+\sqrt{5}}{2} - \dfrac{1-\sqrt{5}}{2}\right) = \dfrac{1+\sqrt{5}}{2} - 1 \\ C + D = 1 \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} D \cdot \sqrt{5} = \dfrac{1+\sqrt{5}-2}{2} \\ C + D = 1 \end{array} \right\}$$

$$\Leftrightarrow \left\{ \begin{array}{l} D = \dfrac{-(1-\sqrt{5})}{2\sqrt{5}} \\ C + \dfrac{-(1-\sqrt{5})}{2\sqrt{5}} = 1 \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} D = \dfrac{-(1-\sqrt{5})}{2\sqrt{5}} \\ C = \dfrac{2\sqrt{5} + (1-\sqrt{5})}{2\sqrt{5}} = \dfrac{1+\sqrt{5}}{2\sqrt{5}} \end{array} \right\}$$

9. *a.* If for all integers $k \geq 2$, $t^k = 7t^{k-1} - 10t^{k-2}$ and $t \neq 0$, then $t^2 = 7t - 10$ and so $t^2 - 7t + 10 = 0$. But $t^2 - 7t + 10 = (t-2)(t-5)$. Thus $t = 2$ or $t = 5$.

b. It follows from part (a) and the distinct roots theorem that for some constants C and D, $b_0, b_1, b_2, \ldots$. satisfies the equation $b_n = C \cdot 2^n + D \cdot 5^n$ for all integers $n \geq 0$. Since $b_0 = 2$ and $b_1 = 2$, then

$$\left\{ \begin{array}{l} b_0 = C \cdot 2^0 + D \cdot 5^0 = C + D = 2 \\ b_1 = C \cdot 2^1 + D \cdot 5^1 = 2C + 5D = 2 \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} D = 2 - C \\ 2C + 5(2 - C) = 2 \end{array} \right\}$$

$$\Leftrightarrow \left\{ \begin{array}{l} D = 2 - C \\ C = 8/3 \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} D = 2 - (8/3) = -(2/3) \\ C = 8/3 \end{array} \right\}$$

Thus $b_n = \dfrac{8}{3} \cdot 2^n - \dfrac{2}{3} \cdot 5^n$ for all integers $n \geq 0$.

10. *a.* If for all integers $k \geq 2$, $t^k = t^{k-1} + 6t^{k-2}$ and $t \neq 0$, then $t^2 = t + 6$ and so $t^2 - t - 6 = 0$. But $t^2 - t - 6 = (t-3)(t+2)$. Thus $t = 3$ or $t = -2$.

b. It follows from part (a) and the distinct roots theorem that for some constants C and D, $c_0, c_1, c_2, \ldots$. satisfies the equation $c_n = C \cdot 3^n + D(-2)^n$ for all integers $n \geq 0$. Since $c_0 = 0$ and $c_1 = 3$, then

$$\left\{ \begin{array}{l} c_0 = C \cdot 3^0 + D(-2)^0 = C + D = 0 \\ c_1 = C \cdot 3^1 + D(-2)^1 = 3C - 2D = 3 \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} D = -C \\ 3C - 2(-C) = 3 \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} D = -3/5 \\ C = 3/5 \end{array} \right\}$$

Thus $c_n = \dfrac{3}{5} \cdot 3^n - \dfrac{3}{5}(-2)^n$ for all integers $n \geq 0$.

12. The characteristic equation is $t^2 - 9 = 0$. Since $t^2 - 9 = (t-3)(t+3)$, the roots are $t = 3$ and $t = -3$. By the distinct roots theorem, for some constants C and D, $e_n = C \cdot 3^n + D(-3)^n$ for all integers $n \geq 0$. Since $e_0 = 0$ and $e_1 = 2$, then

$$\left\{ \begin{array}{l} e_0 = C \cdot 3^0 + D(-3)^0 = C + D = 0 \\ e_1 = C \cdot 3^1 + D(-3)^1 = 3C - 3D = 2 \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} D = -C \\ 3C - 3(-C) = 2 \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} D = -1/3 \\ C = 1/3 \end{array} \right\}$$

Thus $e_n = \dfrac{1}{3} 3^n - \dfrac{1}{3}(-3)^n = 3^{n-1} + (-3)^{n-1} = 3^{n-1}(1 + (-1)^{n-1}) = \left\{ \begin{array}{ll} 2 \cdot 3^{n-1} & \text{if } n \text{ is odd} \\ 0 & \text{if } n \text{ is even} \end{array} \right.$

for all integers $n \geq 0$.

14. The characteristic equation is $t^2 + 4t + 4 = 0$. Since $t^2 + 4t + 4 = (t+2)^2$, there is only one root, $t = -2$. By the single root theorem, for some constants C and D,

$$s_n = C(-2)^n + D \cdot n(-2)^n \qquad \text{for all integers } n \geq 0.$$

Since $s_0 = 0$ and $s_1 = -1$, then

$$\left\{ \begin{array}{l} s_0 = C(-2)^0 + D \cdot 0(-2)^0 = C = 0 \\ s_1 = C(-2)^1 + D \cdot 1(-2)^1 = -2C - 2D = -1 \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} C = 0 \\ -2D = -1 \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} C = 0 \\ D = 1/2 \end{array} \right\}$$

Thus $s_n = 0(-2)^n + \dfrac{1}{2} \cdot n(-2)^n = -n \cdot 2^{n-1}$ for all integers $n \geq 0$.

15. The characteristic equation is $t^2 - 6t + 9 = 0$. Since $t^2 - 6t + 9 = (t-3)^2$, there is only one root, $t = 3$. By the single root theorem, for some constants C and D, $t_n = C \cdot 3^n + D \cdot n \cdot 3^n$ for all integers $n \geq 0$. Since $t_0 = 1$ and $t_1 = 3$, then

$$\left\{ \begin{array}{l} t_0 = C \cdot 3^0 + D \cdot 0 \cdot 3^0 = C = 1 \\ t_1 = C \cdot 3^1 + D \cdot 1 \cdot 3^1 = 3C + 3D = 3 \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} C = 1 \\ C + D = 1 \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} C = 1 \\ D = 0 \end{array} \right\}$$

Thus $t_n = 1 \cdot 3^n + 0 \cdot n \cdot 3^n = 3^n$ for all integers $n \geq 0$.

16. Given the set-up of exercise 37 from Section 8.1, $s_k = 2s_{k-1} + 2s_{k-2}$ for all integers $k \geq 2$. Thus the characteristic equation is $t^2 - 2t - 2 = 0$. By the quadratic formula, the roots are $t = \dfrac{2 \pm \sqrt{4+8}}{2} = \dfrac{2 \pm 2\sqrt{3}}{2} = 1 \pm \sqrt{3}$. By the distinct roots theorem, for some constants C and D, $s_n = C(1+\sqrt{3})^n + D(1-\sqrt{3})^n$ for all integers $n \geq 0$. Since $s_0 = 1$ and $s_1 = 3$, then

$$\left\{ \begin{array}{l} s_0 = C(1+\sqrt{3})^0 + D(1-\sqrt{3})^0 = C + D = 1 \\ s_1 = C(1+\sqrt{3})^1 + D(1-\sqrt{3})^1 = 3 \end{array} \right\}$$

$$\Leftrightarrow \left\{ \begin{array}{l} D = 1 - C \\ C(1+\sqrt{3}) + (1-C)(1-\sqrt{3}) = 3 \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} D = 1 - C \\ C(1+\sqrt{3} - 1 + \sqrt{3}) = 3 - 1 + \sqrt{3} \end{array} \right\}$$

$$\Leftrightarrow \left\{ \begin{array}{l} D = 1 - \dfrac{2+\sqrt{3}}{2\sqrt{3}} = \dfrac{\sqrt{3}-2}{2\sqrt{3}} \\ C = \dfrac{\sqrt{3}+2}{2\sqrt{3}} \end{array} \right\}$$

Thus $s_n = C(1+\sqrt{3})^n + D(1-\sqrt{3})^n = \dfrac{\sqrt{3}+2}{2\sqrt{3}}(1+\sqrt{3})^n + \dfrac{\sqrt{3}-2}{2\sqrt{3}}(1-\sqrt{3})^n$ for all integers $n \geq 0$.

17. Given the set-up of exercise 39 from Section 8.1, $c_1 = 1$ and $c_2 = 2$ and $c_k = c_{k-1} + c_{k-2}$ for all integers $k \geq 3$. Define $c_0 = 1$. Then $c_2 = c_0 + c_1$ and so the recurrence relation holds for all integers $k \geq 2$. The characteristic equation is, therefore, $t^2 - t - 1 = 0$, which is the same as the characteristic equation for the Fibonacci sequence. In addition, the first two terms of this sequence are the same as the Fibonacci sequence. Hence $c_0, c_1, c_2, \ldots$ satisfies the same explicit formula as the Fibonacci sequence, namely, $c_n = \dfrac{1}{\sqrt{5}} \left(\dfrac{1+\sqrt{5}}{2} \right)^{n+1} - \dfrac{1}{\sqrt{5}} \left(\dfrac{1-\sqrt{5}}{2} \right)^{n+1}$ (equation (8.3.8)).

An alternative solution is to substitute the roots of the characteristic equation into the formula $c_n = C \left(\dfrac{1+\sqrt{5}}{2} \right)^n + D \left(\dfrac{1-\sqrt{5}}{2} \right)^n$ for $n = 1$ and $n = 2$ and solve for C and D from the resulting set of simultaneous equations.

18. *Proof:* Suppose that $s_0, s_1, s_2, \ldots$ and $t_0, t_1, t_2, \ldots$ are sequences such that $s_k = 5s_{k-1} - 4s_{k-2}$ and $t_k = 5t_{k-1} - 4t_{k-2}$ for all integers $k \geq 2$. Then for all integers $k \geq 2$, $5(2s_{k-1} + 3t_{k-1}) - 4(2s_{k-2} + 3t_{k-2}) = (5 \cdot 2s_{k-1} - 4 \cdot 2s_{k-2}) + (5 \cdot 3t_{k-1} - 4 \cdot 3t_{k-2}) = 2(5s_{k-1} - 4s_{k-2}) + 3(5t_{k-1} - 4t_{k-2}) = 2s_k + 3t_k$. *[This is what was to be shown.]*

20. *Proof*: Suppose that r is a nonzero real number, k and m are distinct integers, and a_k and a_m are any real numbers. Consider the system of equations

$Cr^k + kDr^k = a_k$

$Cr^m + mDr^m = a_m.$

Without loss of generality, we may assume that $k > m$. Multiply the bottom equation by r^{k-m} to obtain the equivalent system

$Cr^k + kDr^k = a_k$

$Cr^m \cdot r^{k-m} + mDr^m \cdot r^{k-m} = Cr^k + mDr^k = a_m \cdot r^{k-m}.$

Subtracting the bottom equation from the top one gives $(k-m)Dr^k = a_k - a_m \cdot r^{k-m}$, or

$D = \dfrac{a_k - a_m \cdot r^{k-m}}{(k-m)r^k}$ since $k-m \neq 0$ and $r \neq 0$. Substituting into the top equation gives $Cr^k +$

$k\left(\dfrac{a_k - a_m \cdot r^{k-m}}{(k-m)r^k}\right)r^k = a_k$, and solving for C gives $C = \dfrac{1}{r^k}\left(a_k - k\left(\dfrac{a_k - a_m \cdot r^{k-m}}{(k-m)}\right)\right)$.

These calculations show that the given system of equations has the unique solutions C and D that are shown.

Alternatively, the determinant of the given system of two linear equations in the two unknowns C and D is $r^k \cdot m \cdot r^m - r^m \cdot k \cdot r^k = r^{k+m}(m-k)$. This is nonzero because $m \neq k$ and $r \neq 0$, and therefore the given system has a unique solution.

21. Let $a_0, a_1, a_2, \ldots$ be any sequence that satisfies the recurrence relation $a_k = Aa_{k-1} + Ba_{k-2}$ for some real numbers A and B with $B \neq 0$ and for all integers $k \geq 2$. Furthermore, suppose that the equation $t^2 - At - B = 0$ has a single real root r. First note that $r \neq 0$ because otherwise we would have $0^2 - A \cdot 0 - B = 0$, which would imply that $B = 0$ and contradict the hypothesis. Second, note that the following system of equations with unknowns C and D has a unique solution.

$$a_0 = Cr^0 + 0 \cdot Dr^0 = 1 \cdot C + 0 \cdot D$$
$$a_1 = Cr^1 + 1 \cdot Dr^1 = C \cdot r + D \cdot r$$

One way to reach this conclusion is to observe that the determinant of the system is $1 \cdot r - r \cdot 0 = r \neq 0$. Another way to reach the conclusion is to write the system as

$$a_0 = C$$
$$a_1 = Cr + Dr$$

and let $C = a_0$ and $D = (a_1 - Cr)/r$. It is clear by substitution that these values of C and D satisfy the system. Conversely, if any numbers C and D satisfy the system, then $C = a_0$ and substituting C into the second equation and solving for D yields $D = (a_1 - Cr)/r$.

Proof of the exercise statement by strong mathematical induction: Let $a_0, a_1, a_2, \ldots$ be any sequence that satisfies the recurrence relation $a_k = Aa_{k-1} + Ba_{k-2}$ for some real numbers A and B with $B \neq 0$ and for all integers $k \geq 2$. Furthermore, suppose that the equation $t^2 - At - B = 0$ has a single real root r. Let the property $P(n)$ be the equation $a_n = Cr^n + nDr^n$ where C and D are the unique real numbers such that $a_0 = Cr^0 + 0 \cdot Dr^0$ and $a_1 = Cr^1 + 1 \cdot Dr^1$.

Show that the property is true for $n = 0$ and $n = 1$: The fact that the property is true for $n = 0$ and $n = 1$ is automatic because C and D are exactly those numbers for which $a_0 = Cr^0 + 0 \cdot Dr^0$ and $a_1 = Cr^1 + 1 \cdot Dr^1$.

Show that for all integers $k > 1$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let k be an integer with $k > 1$ and suppose $a_i = Cr^i + iDr^i$, for all integers i with $1 \leq i < k$. *[This is the inductive hypothesis.]* We must show that $a_k = Cr^k + kDr^k$. Now by the inductive hypothesis, $a_{k-1} = Cr^{k-1} + (k-1)Dr^{k-1}$ and $a_{k-2} = Cr^{k-2} + (k-2)Dr^{k-2}$. So

$$
\begin{aligned}
a_k &= Aa_{k-1} + Ba_{k-2} && \text{by definition of } a_0, a_1, a_2, \ldots \\
&= A(Cr^{k-1} + (k-1)Dr^{k-1}) + B(Cr^{k-2} + (k-2)Dr^{k-2}) \\
& && \text{by substitution from the inductive hypothesis} \\
&= C(Ar^{k-1} + Br^{k-2}) + D(A(k-1)r^{k-1} + B(k-2)r^{k-2}) \\
& && \text{by algebra} \\
&= Cr^k + Dkr^k && \text{by Lemma 8.3.4.}
\end{aligned}
$$

[This is what was to be shown.]

23. The characteristic equation is $t^2 - 2t + 5 = 0$. By the quadratic formula the roots of this equation are $t = \dfrac{2 \pm \sqrt{4-20}}{2} = \begin{cases} 1+2i \\ 1-2i \end{cases}$. By the distinct roots theorem, for some constants C and D, $b_n = C(1+2i)^n + D(1-2i)^n$ for all integers $n \geq 0$. Since $b_0 = 1$ and $b_1 = 1$, then

$$
\begin{cases} b_0 = C(1+2i)^0 + D(1-2i)^0 = C + D = 1 \\ b_1 = C(1+2i)^1 + D(1-2i)^1 = 1 \end{cases}
\Leftrightarrow
\begin{cases} (1-2i)C + (1-2i)D = 1 - 2i \\ (1+2i)C + (1-2i)D = 1 \end{cases}
$$

$$
\Leftrightarrow \begin{cases} C + D = 1 \\ [(1+2i)-(1-2i)]C = 1 - (1-2i) = 2i \end{cases}
\Leftrightarrow \begin{cases} C + D = 1 \\ C = 2i/4i = 1/2 \end{cases}
$$

$$
\Leftrightarrow \begin{cases} D = 1 - 1/2 = 1/2 \\ C = 1/2 \end{cases}
$$

Thus $b_n = (1/2)(1+2i)^n + (1/2)(1-2i)^n$ for all integers $n \geq 0$.

24. *a.* If $\dfrac{\phi}{1} = \dfrac{1}{\phi - 1}$, then $\phi(\phi - 1) = 1$, or, equivalently, $\phi^2 - \phi - 1 = 0$ and so ϕ satisfies the equation $t^2 - t - 1 = 0$.

b. By the quadratic formula, the solutions to $t^2 - t - 1 = 0$ are $t = \dfrac{1 \pm \sqrt{1+4}}{2} = \begin{cases} (1+\sqrt{5})/2 \\ (1-\sqrt{5})/2 \end{cases}$.

Let $\phi_1 = (1+\sqrt{5})/2$ and $\phi_2 = (1-\sqrt{5})/2$.

c. $F_n = \dfrac{1}{\sqrt{5}} \cdot \phi_1^{n+1} - \dfrac{1}{\sqrt{5}} \cdot \phi_2^{n+1} = \dfrac{1}{\sqrt{5}}(\phi_1^{n+1} - \phi_2^{n+1})$

This equation is an alternative way to write equation (8.3.8).

25. The given recurrence relation can be rewritten in the form $\dfrac{1}{6}P_k = P_{k-1} - \dfrac{5}{6}P_{k-2}$, or $P_k = 6P_{k-1} - 5P_{k-2}$. Thus the characteristic equation is $t^2 - 6t + 5 = 0$. Since $t^2 - 6t + 5 = (t-1)(t-5)$, this equation has roots $t = 1$ and $t = 5$. By the distinct roots theorem, for some constants C and D, $P_n = C \cdot 1^n + D \cdot 5^n = C + D \cdot 5^n$ for all integers $n \geq 0$. Since $P_0 = 1$ and $P_{300} = 0$, then

$$
\begin{cases} P_0 = C + D \cdot 5^0 = C + D = 1 \\ P_{300} = C + D \cdot 5^{300} = C + 5^{300} \cdot D = 0 \end{cases}
\Leftrightarrow
\begin{cases} C + D = 1 \\ (1 - 5^{300})D = 1 \end{cases}
$$

$$
\Leftrightarrow
\begin{cases} C = 1 - D = 1 - \dfrac{1}{1 - 5^{300}} \\ D = \dfrac{1}{1 - 5^{300}} \end{cases}
\Leftrightarrow
\begin{cases} C = \dfrac{-5^{300}}{1 - 5^{300}} \\ D = \dfrac{1}{1 - 5^{300}} \end{cases}
$$

Thus $P_n = \left(\dfrac{-5^{300}}{1 - 5^{300}}\right) + \left(\dfrac{1}{1 - 5^{300}}\right) \cdot 5^n = \left(\dfrac{5^{300} - 5^n}{5^{300} - 1}\right)$ for all integers $n \geq 0$.

$P_{20} = \left(\dfrac{5^{300} - 5^{20}}{5^{300} - 1}\right) \cong 1$

26. *a.* Let k be an integer with $k \geq 3$, call the k distinct sectors of the disk $1, 2, 3, \ldots, k$, and suppose that the values of $S_1, S_2, \ldots, S_{k-1}$ are known. Note that $S_1 = 4$ and $S_2 = 4 \cdot 3 = 12$.

Case 1, Sectors 1 and 3 are painted the same color: In this case $k > 3$ because otherwise sectors 1 and 3 would be both adjacent and painted the same color which is not allowed. Imagine sectors 1 through 3 made into a single unit painted the color of sectors 1 and 3. Then

the disk would contain a total of $k-2$ sectors: $1-3, 4, 5, \ldots, k$, and the number of ways to paint the disk would be S_{k-2}. Each of these ways corresponds to exactly three ways to paint the disk when sectors 1-3 are not united, for that is the number of choices of colors to paint sector 2 to contrast with sectors 1 and 3. Hence there are $3S_{k-2}$ ways to paint the disk in this case.

Case 2, Sectors 1 and 3 are painted different colors: In this case, imagine shrinking sector 2 to nothing. Then there would be S_{k-1} ways to paint the resulting disk. Now imagine expanding sector 2 back to its original size and giving it a color. Since there are two ways that sector 2 could be colored that would contrast with the colors of both sectors 1 and 3, each way to paint the disk leaving sector 2 out corresponds to exactly two ways to paint the disk when sector 2 is present. Hence there are $2S_{k-1}$ ways to paint the disk in this case.

If $k = 3$, then case 1 does not occur, and so $S_3 = 2S_2 = 24$. If $k \geq 4$, then the total number of ways to paint the disk is the sum of the ways counted in cases 1 and 2. Therefore, $S_k = 2S_{k-1} + 3S_{k-2}$ for all integers $k \geq 4$.

b. Let $T_0, T_1, T_2, \ldots$ be the sequence defined by $T_n = S_{n+2}$ for all integers $n \geq 0$. Then for all integers $k \geq 2$, $T_k = 2T_{k-1} + 3T_{k-2}$ and $T_0 = 12$ and $T_1 = 24$. The characteristic equation of the relation is $t^2 - 2t - 3 = 0$. Since $t^2 - 2t - 3 = (t - 3)(t + 1)$, the roots of this equation are $t = 3$ and $t = -1$. By the distinct roots theorem, for some constants C and D, $T_n = C \cdot 3^n + D(-1)^n$ for all integers $n \geq 0$. Since $T_0 = 12$ and $T_1 = 24$, then

$$\left\{ \begin{array}{l} T_0 = C \cdot 3^0 + D(-1)^0 = C + D = 12 \\ T_1 = C \cdot 3^1 + D(-1)^1 = 3C - D = 24 \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} 4C = 36 \\ C + D = 12 \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} C = 9 \\ D = 3 \end{array} \right\}$$

Thus $T_n = 9 \cdot 3^n + 3(-1)^n = 3(3 \cdot 3^n + (-1)^n) = 3(3^{n+1} + (-1)^n)$ for all integers $n \geq 0$, and hence $S_n = T_{n-2} = 3(3^{(n-2)+1} + (-1)^{n-2}) = 3(3^{n-1} + (-1)^n)$ for all integers $n \geq 2$.

Section 8.4

1. *b.* (1) p, q, r, and s are Boolean expressions by I.

    (2) $(p \vee q)$ and $\sim s$ are Boolean expressions by (1), *II(b)*, and *II(c)*

    (3) $(p\wedge \sim s)$ is a Boolean expression by (1), (2), and II(a)

    (4) $((p\wedge \sim s) \wedge r)$ is a Boolean expression by (1), (3), and II(a)

    (5) $\sim ((p\wedge \sim s) \wedge r)$ is a Boolean expression by (4) and *II(c)*

    (6) $(p \vee q)\vee \sim ((p\wedge \sim s) \wedge r)$ is a Boolean expression by (2), (5) and *II(b)*

2. *b.* (1) $\epsilon \in \Sigma^*$ by I.

    (2) $b = \epsilon b \in \Sigma^*$ by (1) and *II(b)*.

    (3) $bb \in \Sigma^*$ by (2) and *II(b)*

3. *b.* (1) MI is in the MIU-system by I.

    (2) MII is in the MIU-system by (1) and *II(b)*.

    (3) $MIIII$ is in the MIU-system by (2) and *II(b)*.

    (4) $MIIIIIIII$ is in the MIU-system by (3) and *II(b)*.

    (5) $MUIIIII$ is in the MIU-system by (4) and *II(c)*.

    (6) $MUIIU$ is in the MIU-system by (5) and *II(c)*.

4. The string MU is not in the system because the number of I's in MU is 0, which is divisible by 3, and for all strings in the MIU-system, the number of I's in the string is not divisible by 3.

   Proof (by structural induction): Let the property be the following sentence: The number of I's in the string is not divisible by 3.

Show that each object in the BASE for the MIU-system satisfies the property: The only object in the base is MI, which has one I, and the number 1 is not divisible by 3.

Show that for each rule in the RECURSION for the MIU-system , if the rule is applied to objects in the system that satisfy the property, then the objects defined by the rule also satisfy the property: The recursion for the MIU-system consists of four rules, denoted II(a)–(d). Let s be a string, let n be the number of I's in s, and suppose $3 \nmid n$. Consider the effect of acting upon s by each recursion rule in turn.

In case rule II(a) is applied to s, s has the form xI, where x is a string. The result is the string xIU. This string has the same number of I's as xI, namely n, and n is not divisible by 3.

In case rule II(b) is applied to s, s has the form Mx, where x is a string. The result is the string Mxx. This string has twice the number of I's as Mx. Because n is the number of I's in Mx and $3 \nmid n$, we have $n = 3k + 1$ or $n = 3k + 2$ for some integer k. In case $n = 3k + 1$, the number of I's in Mxx is $2(3k + 1) = 3(2k) + 2$, which is not divisible by 3. In case $n = 3k + 2$, the number of I's in Mxx is $2(3k + 2) = 6k + 4 = 3(2k + 1) + 1$, which is not divisible by 3 either.

In case rule II(c) is applied to s, s has the form $xIIIy$, where x and y are strings. The result is the string xUy. This string has three fewer I's than the number of I's in s. Because n is the number of I's in $xIIIy$ and $3 \nmid n$, we have that $3 \nmid (n - 3)$ either *[for if $3 \mid (n -- 3)$ then $n - 3 = 3k$, for some integer k. Hence $n = 3k + 3 = 3(k + 1)$, and so n would be divisible by 3, which it is not]*. Thus the number of I's in xUy is not divisible by 3.

In case rule II(d) is applied to s, s has the form $xUUy$, where x and y are strings. The result is the string xUy. This string has the same number of I's as $xUUy$, namely n, and n is not divisible by 3.

By the restriction for the MIU-system, no strings other than those derived from the base and the recursion are in the system. Therefore, for all strings in the MIU-system, the number of I's in the string is not divisible by 3.

5. *b.* (1) ( ) is in P by I.

   (2) (( )) is in P by (1) and II(a).

   (3) (( ))(( )) is in P by (2) and $II(b)$.

6. *b.* Even though the number of its left parentheses equals the number of its right parentheses, this structure is not in P either. Roughly speaking, the reason is that given any parenthesis structure derived from the base structure by repeated application of the rules of the recursion, as you move from left to right along the structure, the total of right parentheses you encounter will never be larger than the number of left parentheses you have already passed by. But if you move along (( )( )))(( ) from left to right, you encounter an extra right parenthesis in the seventh position.

   More formally: Let A be the set of all finite sequences of integers and define a function $g\colon P \to A$ as follows: for each parenthesis structure S in P, let $g[S] = (a_1, a_2, \ldots, a_n)$ where a_i is the number of left parentheses in S minus the number of right parentheses in S counting from left to right through position i. For instance, if $S = (( )( ))$, then $g[S] = (1, 2, 1, 2, 1, 0)$. By the same argument as in part (a), the final component in $g[S]$ will always be 0. We claim that for all parenthesis structures S in P, each component of $g[S]$ is nonnegative. It follows from the claim that if (( )( )))(( ) were in P, then all components of $g[(( )( )))(( )]$ would be nonnegative. But $g[(( )( )))(( )] = (1, 2, 1, 2, 1, 0, -1, 0, 1, 0)$, and one of these components is negative. Consequently, (( )( )))(( ) is not in P.

   Proof of the claim (by structural induction): Let the property be the following sentence: Each component of $g[S]$ is nonnegative, with the final component being 0.

Show that each object in the BASE for P satisfies the property: The only object in the base is ( ), and $g[( )] = (1, 0)$. Both components of $g[( )]$ are nonnegative, and the final component is 0.

Show that for each rule in the RECURSION for P , if the rule is applied to objects in P that satisfy the property, then the objects defined by the rule also satisfy the property: The recursion for P consists of two rules, denoted II(a) and II(b). Let S and T be parenthesis structures in P with the property that all components of $g[S]$ and $g[T]$ are nonnegative, with the final components of both S and T being 0. Consider the effect of applying rules II(a) and II(b).

In case rule II(a) is applied to S, the result is (S). Observe that that the first component in $g[(S)]$ is 1 *[because (S) starts with a left parenthesis]*, every subsequent component of $g[(S)]$ except the last is one more than a corresponding (nonnegative) component of $g[S]$. Thus the next-to-last component of (S) is 1 (because the final component of S is 0), and the final right-parenthesis of (S) reduces the final component of $g[(S)]$ to 0 also. So each component of $g[(S)]$ is nonnegative, and the final component is 0.

In case rule II(b) is applied to S and T, the result is ST. We must show that each component of $g[ST]$ is nonnegative, with the final component being 0. For concreteness, suppose $g[S]$ has m components and $g[T]$ has n components. The first through the mth components of $g[ST]$ are the same as the first through the mth components of S, which are all nonnegative, with the mth component being 0. Thus the $(m+1)$st through the $(m+n)$th components of $g[ST]$ are the same as the first through the nth components of T, which are all nonnegative, with the final component being 0. Because the final component of $g[ST]$ is the same as the final component of T, all components of $g[ST]$ are nonnegative, with the final component being 0.

By the restriction condition, there are no other elements of P besides those obtainable from the base and recursion conditions. Hence, for all S in P, all components of $g[S]$ are nonnegative, with final component 0.

7. b (1) 9, 6.1, 2, 4, 7, and 6 are arithmetic expressions by I.

(2) $(6.1 + 2)$ and $(4\text{-}7)$ are arithmetic expressions by (1), $II(c)$, and $II(d)$

(3) $(9 \cdot (6.1 + 2))$ and $((4 - 7) \cdot 6)$ are arithmetic expressions by (1), (2), and $II(e)$

(4) $\left(\dfrac{(9 \cdot (6.1 + 2))}{((4 - 7) \cdot 6)} \right)$ is an arithmetic expression by (3) and $II(f)$

9. *Proof (by structural induction)*: Let the property be the following sentence: The string begins with an a.

Show that each object in the BASE for S satisfies the property: The only object in the base is a, and the string a begins with an a.

Show that for each rule in the RECURSION for S, if the rule is applied to objects in S that satisfy the property, then the objects defined by the rule also satisfy the property: The recursion for S consists of two rules, denoted II(a) and II(b). In case rule II(a) is applied to a string s in S that begins with a a, the result is the string sa, which begins with the same character as s, namely a. Similarly, in case rule II(b) is applied to a string s that begins with a a, the result is the string sb, which also begins with an a. Thus, when each rule in the RECURSION is applied to strings in S that begin with an a, the results are also strings that begin with an a. Because no objects other than those obtained through the BASE and RECURSION conditions are contained in S, every string in S begins with an a.

11. *Proof (by structural induction)*: Let the property be the following sentence: The string does not have a leading zero.

Show that each object in the BASE for S satisfies the property: The objects in the base are 1, 2, 3, 4, 5, 6, 7, 8, and 9. None of these strings has a leading zero.

Show that for each rule in the RECURSION for S, if the rule is applied to objects in S that satisfy the property, then the objects defined by the rule also satisfy the property:

The recursion for S consists of two rules, denoted II(a) and II(b). In case rule II(a) is applied to a string s in S that does not have a leading zero, the result is the string $s0$, which does not have a leading zero because it begins with the same character as s. In case rule II(b) is applied to string s and t in S that do not have leading zeros, the result is the string st, which also does have a leading zero because it begins with the same character as s. Thus when each rule in the RECURSION is applied to strings in S that do not have a leading zero, the results are also strings that do not have a leading zero. Because no objects other than those obtained through the BASE and RECURSION conditions are contained in S, no string in S has a leading zero.

12. *Proof (by structural induction)*: Let the property be the following sentence: The string represents an odd integer.

Show that each object in the BASE for S satisfies the property: The objects in the base are 1, 3, 5, 7, and 9. All of these strings represent odd integers.

Show that for each rule in the RECURSION for S, if the rule is applied to objects in S that satisfy the property, then the objects defined by the rule also satisfy the property: The recursion for S consists of five rules, denoted II(a)–II(e). Suppose s and t are strings in S that represent odd integers. Then the right-most character for each of s and t is 1, 3, 5, 7, or 9. In case rule II(a) is applied to s and t, the result is the string st, which has the same right-most character as t. So st represents an odd integer. In case rules II(b)–II(e) are applied to s, the results are $2s$, $4s$, $6s$, or $8s$. All of these strings have the same right-most character as s, and, therefore, they all represent odd integers. Thus when each rule in the RECURSION is applied to strings in S that represent odd integers, the result is also a string that represents an odd integer. Because no objects other than those obtained through the BASE and RECURSION conditions are contained in S, all the strings in S represent odd integers.

13. *Proof (by structural induction)*: Let the property be the following sentence: The integer is divisible by 5.

Show that each object in the BASE for S satisfies the property: The objects in the base are 0 and 5. Both of these integers are divisible by 5.

Show that for each rule in the RECURSION for S, if the rule is applied to objects in S that satisfy the property, then the objects defined by the rule also satisfy the property: The recursion for S consists of two rules, denoted II(a) and II(b). Suppose s and t are integers in S that are divisible by 5. By exercises 15 and 16 from Section 3.3, both $s+t$ and $s-t$ are also divisible by 5. Thus when each rule in the RECURSION is applied to integers in S that are divisible by 5 the result is an integer that is also divisible by 5. Because no objects other than those obtained through the BASE and RECURSION conditions are contained in S, all the integers in S are divisible by 5.

14. *Proof (by structural induction)*: Let the property be the following sentence: The integer is divisible by 3.

Show that each object in the BASE for S satisfies the property: The only object in the base is 0, and 0 is divisible by 3.

Show that for each rule in the RECURSION for S, if the rule is applied to objects in S that satisfy the property, then the objects defined by the rule also satisfy the property: The recursion for S consists of two rules denoted II(a) and II(b). Suppose s is an integer in S that is divisible by 3. By exercises 15 and 16 from Section 3.3, both $s+3$ and $s-3$ are also divisible by 3. Thus when each rule in the RECURSION is applied to an integer in S that is divisible by 3, the result is also an integer that is divisible by 3. Because no objects

other than those obtained through the BASE and RECURSION conditions are contained in S, all the integers in S are divisible by 3.

16. Let S be the set of all strings of 0's and 1's in which all the 0's precede all the 1's. The following is a recursive definition of S.

I. BASE: $\epsilon \in S$, where ϵ is the null string

II. RECURSION: If $s \in S$, then

$a. \ 0s \in S$ $b. \ s1 \in S$

III. RESTRICTION: There are no elements of S other than those obtained from I and II.

18. Let S be the set of all strings of a's and $b's$ that contain exactly one a. The following is a recursive definition of S.

I. BASE: $a \in S$

II. RECURSION: If $s \in S$, then

$a. \ bs \in S$ $b. \ sb \in S$

III. RESTRICTION: There are no elements of S other than those obtained from I and II.

20. *Proof (by mathematical induction)*: Let the property be the sentence "If $a_1, a_2, \ldots, a_n$ and $b_1, b_2, \ldots, b_n$ are any real numbers, then $\prod_{i=1}^{n}(a_ib_i) = \left(\prod_{i=1}^{n} a_i\right)\left(\prod_{i=1}^{n} b_i\right).$"

Show that the property is true for $n = 1$: Let a_1 and b_1 be any real numbers. By the recursive definition of product, $\prod_{i=1}^{1}(a_ib_i) = a_1b_1$, $\prod_{i=1}^{1} a_i = a_1$, and $\prod_{i=1}^{1} b_i = b_1$. Therefore, $\prod_{i=1}^{1}(a_ib_i) = \left(\prod_{i=1}^{1} a_i\right)\left(\prod_{i=1}^{1} b_i\right)$, and so the property is true for $n = 1$.

Show that for all integers $k \geq 1$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let k be an integer such that $k \geq 1$. Suppose that if $a_1, a_2, \ldots, a_k$ and $b_1, b_2, \ldots, b_k$ are any real numbers, then $\prod_{i=1}^{k}(a_ib_i) = \left(\prod_{i=1}^{k} a_i\right)\left(\prod_{i=1}^{k} b_i\right)$. *[This is the inductive hypothesis.]* We must show that if $a_1, a_2, \ldots, a_{k+1}$ and $b_1, b_2, \ldots, b_{k+1}$ are any real numbers, then $\prod_{i=1}^{k+1}(a_ib_i) = \left(\prod_{i=1}^{k+1} a_i\right)\left(\prod_{i=1}^{k+1} b_i\right)$. So suppose $a_1, a_2, \ldots, a_{k+1}$ and $b_1, b_2, \ldots, b_{k+1}$ are any real numbers. Then

$\prod_{i=1}^{k+1}(a_ib_i)$

$= \left(\prod_{i=1}^{k}(a_ib_i)\right)(a_{k+1}b_{k+1})$ by the recursive definition of product

$= \left(\left(\prod_{i=1}^{k} a_i\right)\left(\prod_{i=1}^{k} b_i\right)\right)(a_{k+1}b_{k+1})$ by substitution from the inductive hypothesis

$= \left(\left(\prod_{i=1}^{k} a_i\right)a_{k+1}\right)\left(\left(\prod_{i=1}^{k} b_i\right)b_{k+1}\right)$ by the associative and commutative laws of algebra

$= \left(\prod_{i=1}^{k+1} a_i\right)\left(\prod_{i=1}^{k+1} b_i\right)$ by the recursive definition of product.

[This is what was to be shown.]

21. *Proof (by mathematical induction)*: Let the property be the sentence "If $a_1, a_2, \ldots, a_n$ and c are any real numbers, then $\prod_{i=1}^{n}(ca_i) = c^n \left(\prod_{i=1}^{n} a_i\right).$"

Show that the property is true for $n = 1$: Let c and a_1 be any real numbers. By the recursive definition of product, both $\prod_{i=1}^{1}(ca_i)$ and $c^1 \prod_{i=1}^{1} a_i$ equal ca_1, and so the property is true for $n = 1$.

Show that for all integers $k \geq 1$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let k be an integer such that $k \geq 1$. Suppose that if c and $a_1, a_2, \ldots, a_k$ are any real numbers, then $\prod_{i=1}^{k}(ca_i) = c^k \left(\prod_{i=1}^{k} a_i\right)$. *[This is the inductive hypothesis.]* We must show that if c and $a_1, a_2, \ldots, a_{k+1}$ are any real numbers, then $\prod_{i=1}^{k+1}(ca_i) = c^{k+1} \left(\prod_{i=1}^{k+1} a_i\right)$. Let c and $a_1, a_2, \ldots, a_{k+1}$ be any real numbers. Then

$\prod_{i=1}^{k+1}(c \cdot a_i)$

$$
\begin{aligned}
&= \left(\prod_{i=1}^{k}(ca_i)\right)(ca_{k+1}) && \text{by the recursive definition of product} \\
&= \left(c^k\left(\prod_{i=1}^{k}a_i\right)\right)(ca_{k+1}) && \text{by substitution from the inductive hypothesis} \\
&= (c^k c)\left(\left(\prod_{i=1}^{k}a_i\right)a_{k+1}\right) && \text{by the associative and commutative laws of algebra} \\
&= c^{k+1}\left(\prod_{i=1}^{k+1}a_i\right) && \text{by the laws of exponents and the recursive} \\
& && \text{definition of product.}
\end{aligned}
$$

[This is what was to be shown.]

22. *Proof (by mathematical induction)*: Let the property be the sentence "If $a_1, a_2, \ldots, a_n$ are any real numbers, then $|\sum_{i=1}^{n} a_i| \le \sum_{i=1}^{n} |a_i|$."

Show that the property is true for $n = 1$: Let a_1 be any real number. By the recursive definition of summation, both $\left|\sum_{i=1}^{1} a_i\right|$ and $\sum_{i=1}^{1} |a_i|$ equal 1. Hence the property is true for $n = 1$.

Show that for all integers $k \ge 1$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let k be an integer such that $k \ge 1$. Suppose that if $a_1, a_2, \ldots, a_k$ are any real numbers, then $\left|\sum_{i=1}^{k} a_i\right| \le \sum_{i=1}^{k} |a_i|$. *[This is the inductive hypothesis.]* We must show that if $a_1, a_2, \ldots, a_{k+1}$ are any real numbers, then $\left|\sum_{i=1}^{k+1} a_i\right| \le \sum_{i=1}^{k+1} |a_i|$. So suppose $a_1, a_2, \ldots, a_{k+1}$ are any real numbers. Then

$$
\begin{aligned}
\left|\sum_{i=1}^{k+1} a_i\right| &= \left|\left(\sum_{i=1}^{k} a_i\right) + a_{k+1}\right| && \text{by the recursive definition of summation} \\
\Rightarrow \left|\sum_{i=1}^{k+1} a_i\right| &\le \left|\left(\sum_{i=1}^{k} a_i\right)\right| + |a_{k+1}| && \text{by the triangle inequality for absolute value} \\
\Rightarrow \left|\sum_{i=1}^{k+1} a_i\right| &\le \sum_{i=1}^{k} |a_i| + |a_{k+1}| && \text{by substitution from the inductive hypothesis} \\
\Rightarrow \left|\sum_{i=1}^{k+1} a_i\right| &\le \sum_{i=1}^{k+1} |a_i| && \text{by the recursive definition of summation.}
\end{aligned}
$$

[This is what was to be shown.]

24. *Proof (by mathematical induction)*: Let the property be the sentence "If A and $B_1, B_2, \ldots, B_n$ are any sets, then $A \cup \left(\bigcap_{i=1}^{n} B_i\right) = \bigcap_{i=1}^{n}(A \cup B_i)$."

Show that the property is true for $n = 1$: Let A and B_1 be any sets. By the recursive definition of intersection, both $A \cup \left(\bigcap_{i=1}^{1} B_i\right)$ and $\bigcap_{i=1}^{1}(A \cup B_i)$ equal $A \cup B_1$. Hence the property is true for $n = 1$.

Show that for all integers $k \ge 1$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let k be an integer such that $k \ge 1$. Suppose that if A and $B_1, B_2, \ldots, B_k$ are any sets then $A \cup \left(\bigcap_{i=1}^{k} B_i\right) = \bigcap_{i=1}^{k}(A \cup B_i)$. *[This is the inductive hypothesis.]* We must show that if A and $B_1, B_2, \ldots, B_{k+1}$ are any sets then $A \cup \left(\bigcap_{i=1}^{k+1} B_i\right) = \bigcap_{i=1}^{k+1}(A \cup B_i)$. Let A and $B_1, B_2, \ldots, B_{k+1}$ be any sets. Then

$$
\begin{aligned}
A \cup \left(\bigcap_{i=1}^{k+1} B_i\right) &= A \cup \left(\left(\bigcap_{i=1}^{k} B_i\right) \cap B_{k+1}\right) && \text{by the recursive definition of intersection.} \\
&= \left(A \cup \left(\bigcap_{i=1}^{k} B_i\right)\right) \bigcap (A \cup B_{k+1}) && \text{by the distributive laws for sets (Theorem 5.2.2(3))} \\
&= \bigcap_{i=1}^{k}(A \cup B_i) \cap (A \cup B_{k+1}) && \text{by inductive hypothesis} \\
&= \bigcap_{i=1}^{k+1}(A \cup B_i) && \text{by the recursive definition of intersection.}
\end{aligned}
$$

[This is what was to be shown.]

25. *Proof (by mathematical induction):* Let the property be the sentence "If $A_1, A_2, \ldots, A_n$ are any sets, then $(\bigcap_{i=1}^{n} A_i)^c = \bigcup_{i=1}^{n} A_i{}^c$."

    Show that the property is true for $n = 1$: Let A_1 be any set. By the recursive definitions of intersection and union, both $(\bigcap_{i=1}^{1} A_i)^c$ and $\bigcup_{i=1}^{1} A_i{}^c$ equal $A_1{}^c$. Hence the property is true for $n = 1$.

    Show that for all integers $k \geq 1$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let k be an integer with $k \geq 1$. Suppose that if $A_1, A_2, \ldots, A_k$ are any sets then $(\bigcap_{i=1}^{k} A_i)^c = \bigcup_{i=1}^{k} A_i{}^c$. *[This is the inductive hypothesis.]* We must show that if $A_1, A_2, \ldots, A_{k+1}$ are any sets then $(\bigcap_{i=1}^{k+1} A_i)^c = \bigcup_{i=1}^{k+1} A_i^c$. So suppose $A_1, A_2, \ldots, A_{k+1}$ are any sets. Then

    $$
    \begin{aligned}
    (\textstyle\bigcap_{i=1}^{k+1} A_i)^c &= ((\textstyle\bigcap_{i=1}^{k} A_i) \cap A_{k+1})^c && \text{by the recursive definition of intersection} \\
    &= (\textstyle\bigcap_{i=1}^{k} A_i)^c \cup A_{k+1}^c && \text{by De Morgan's law for sets (Theorem 5.2.2(9))} \\
    &= \left(\textstyle\bigcup_{i=1}^{k} A_i{}^c\right) \cup A_{k+1}^c && \text{by inductive hypothesis} \\
    &= \textstyle\bigcup_{i=1}^{k+1} A_i{}^c && \text{by the recursive definition of union.}
    \end{aligned}
    $$

    [This is what was to be shown.]

26. $M(91) = M(M(102)) = M(92) = M(M(103)) = M(93) = M(M(104)) = M(94)$

    $= M(M(105)) = M(95) = M(M(106)) = M(96) = M(M(107)) = M(97) = M(M(108))$

    $= M(98) = M(M(109)) = M(99) = M(M(110)) = M(100) = M(M(111)) = M(101) = 91$

27. *Proof 1 (by a variation of strong mathematical induction):* Consider the property "$M(n) = 91$."

    Show that the property is true for all integers n with $91 \leq n \leq 101$: This statement is proved above in the solution to exercise 26.

    Show that for all integers k, if $1 \leq k < 91$ and the property is true for all i with $k < i \leq 101$, then it is true for k: Let k be an integer such that $1 \leq k < 91$ and suppose $M(i) = 91$ for all i with $k < i \leq 101$. *[This is the inductive hypothesis.]* Then $M(k) = M(M(k + 11))$ by definition of M and $12 \leq k + 11 < 102$. Thus $k < k + 11 \leq 101$, and so by inductive hypothesis $M(k + 11) = 91$. It follows that $M(k) = M(91)$, which equals 91 by the basis step above. Hence $M(k) = 91$ *[as was to be shown]*.

    [Since the basis and inductive steps have been proved, it follows that $M(n) = 91$ for all integers $1 \leq n \leq 101$.]

    Proof 2 (by contradiction): Suppose not. That is, suppose there is at least one positive integer $k \leq 101$ with $M(k) \neq 91$. Let q be the largest such integer. Then $1 \leq q \leq 101$ and $M(q) \neq 91$. Now by the solution to exercise 26, for each integer n with $91 \leq n \leq 101$, $M(n) = 91$. Thus $q \leq 90$ and so $q + 11 \leq 90 + 11 = 101$. Note, therefore, that $q + 11$ is a larger positive integer than q and is also less than 101. Hence, because q is the largest positive integer less than or equal to 101 with $M(q) \neq 91$, we must have that $M(q + 11) = 91$. But, by definition of M, $M(q) = M(M(q + 11))$. So $M(q) = M(M(q + 11)) = M(91) = 91$ (by the solution to exercise 26). Therefore, $M(q) \neq 91$ and $M(q) = 91$, which is a contradiction. We conclude that the supposition is false and $M(n) = 91$ for all positive integers $k \leq 101$.

28. *b.* $A(2, 1) = A(1, A(2, 0)) = A(1, A(1, 1)) = A(1, 3)$ *[by part (a)]* $= A(0, A(1, 2)) = A(0, 4)$ *[by Example 8.4.9]* $= 4 + 1 = 5$

29. *b.* *Proof (by mathematical induction):* Consider the property "$A(2, n) = 3 + 2n$."

    Show that the property is true for $n = 0$: When $n = 0$, $A(2, n) = A(2, 0) = A(1, 1)$ *[by 8.4.2]* $= 3$ *[by exercise 28]*. But also $3 = 3 + 2 \cdot 0 = 3 + 2n$. So the property is true for $n = 0$.

    Show that for all integers $k \geq 0$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let k be an integer with $k \geq 0$ and suppose $A(2, k) = 3 + 2k$. *[This is the inductive hypothesis.]* We must show that $A(2, k + 1) = 3 + 2(k + 1)$. But

$$\begin{aligned}
A(2, k+1) &= A(1, A(2, k)) && \text{by (8.4.3)}\\
&= A(1, 3 + 2k) && \text{by inductive hypothesis}\\
&= (3 + 2k) + 2 && \text{by part (a)}\\
&= 3 + 2(k+1) && \text{by the laws of algebra.}
\end{aligned}$$

[This is what was to be shown.]

c. Proof (by mathematical induction): Consider the property "$A(3, n) = 8 \cdot 2^n - 3$."

Show that the property is true for $n = 0$: When $n = 0$, $A(3, n) = A(3, 0) = A(2, 1)$ *[by 8.4.2]* $= 5$ *[by exercise 28].* But also $5 = 8 \cdot 2^0 - 3 = 8 \cdot 2^n - 3$. So the property is true for $n = 0$.

Show that for all integers $k \geq 0$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let k be an integer with $k \geq 0$ and suppose $A(3, k) = 8 \cdot 2^k - 3$. *[This is the inductive hypothesis.]* We must show that $A(3, k+1) = 8 \cdot 2^{k+1} - 3$. But

$$\begin{aligned}
A(3, k+1) &= A(2, A(3, k)) && \text{by (8.4.3)}\\
&= A(2, 8 \cdot 2^k - 3) && \text{by inductive hypothesis}\\
&= 3 + 2(8 \cdot 2^k - 3) && \text{by part } b\\
&= 3 + 8 \cdot 2^{k+1} - 6 &&\\
&= 8 \cdot 2^{k+1} - 3 && \text{by the laws of algebra.}
\end{aligned}$$

[This is what was to be shown.]

30. (1) $T(2) = T(1) = 1$

    (2) $T(3) = T(10) = T(5) = T(16) = T(8) = T(4) = T(2) = 1$

    (3) $T(4) = 1$ by (2)

    (4) $T(5) = 1$ by (2)

    (5) $T(6) = T(3) = 1$ by (2)

    (6) $T(7) = T(22) = T(11) = T(34) = T(17) = T(52) = T(26) = T(13) = T(40) = T(20) = T(10) = 1$ by (2)

32. G is not well-defined. For each odd integer $n > 1$, $3n - 2$ is odd and $3n - 2 > n$. Thus the values of G for odd integers greater than 1 can never be found because each is defined in terms of values of G for even larger odd integers.

Chapter 9: The Efficiency of Algorithms

The focus of Chapter 9 is the analysis of algorithm efficiency in Sections 9.3 and 9.5. The chapter opens with a brief review of the properties of function graphs that are especially important for understanding O-, Ω-, and Θ-notations, which are introduced in Section 9.2. For simplicity, the examples in Section 9.2 are restricted to polynomial and rational functions. Section 9.3 introduces the analysis of algorithm efficiency with examples that include sequential search, insertion sort, selection sort (in the exercises), and polynomial evaluation (in the exercises). Section 9.4 discusses the properties of logarithms that are particularly important in the analysis of algorithms and other areas of computer science, and Section 9.5 applies the properties to analyze algorithms whose orders involve logarithmic functions. Examples in Section 9.5 include binary search and merge sort.

The exercises in this chapter are designed to give you considerable latitude as to how thoroughly to cover both asymptotic notations and algorithm analysis. The exercise sets for Sections 9.2 and 9.4 contain a particularly wide range of difficulty levels of problems. If you want to move rapidly through the chapter, just avoid those that are especially demanding. Section 9.5 is not particularly difficult and shows how a number of topics studied previously (recursive thinking, solving recurrence relations, strong mathematical induction, logarithms, and asymptotic notations) all combine to give useful information about interesting and practical algorithms.

Comments on Exercises:

Section 9.1: **#20**: This exercise is needed for various of the more theoretical exercises in Sections 9.2 and 9.4. **#26** and **#27** are warm-up exercises for the definitions of asymptotic notations.
Section 9.2: Exercises **#1–9** give practice in interpreting the meanings of the definitions of the asymptotic notations, and exercises **#16–24** and **#28–33** require students to establish orders for functions directly from the definitions. Exercises **#34–47** apply the theorem on polynomial orders.
Section 9.3: Exercises **#6-19** introduce the analysis of algorithms through small algorithm segments. Exercises **#20–27** concern insertion sort, **#28-35** deal with selection sort, and **#36-43** explore the relation between term-by-term polynomial evaluation and Horner's rule.
Section 9.4: Exercises **#3-17** review properties of logarithmic functions, especially in combination with floor and ceiling functions. The emphasis in the rest of the exercise set is on orders that involve logarithmic and exponential functions.
Section 9.5: Exercises **#8-15** take students through the steps for finding logarithmic orders for relatively simple algorithm segments. Exercise **#26** introduces the fast multiplication algorithm.

Section 9.1

3.
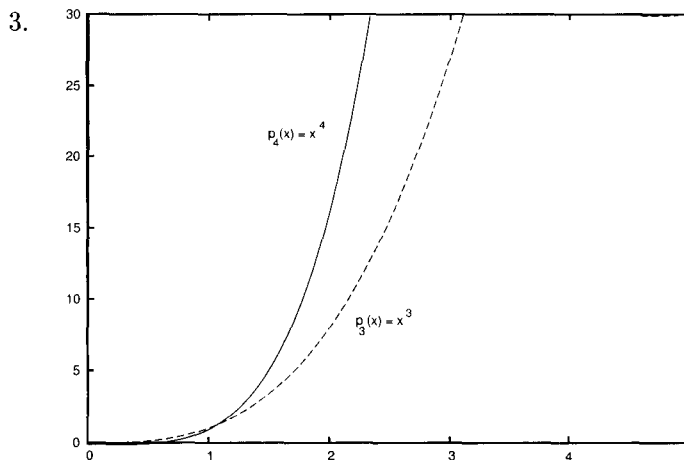
When $0 < x < 1$, $x^3 > x^4$. (For instance, $(1/2)^3 = 1/8 > 1/16 = (1/2)^4$.) When $x > 1$, $x^4 > x^3$.

6.

x	h(x)
0	0
0<x<1	1
1	0
-1	0
-1<x<0	1

graph of h
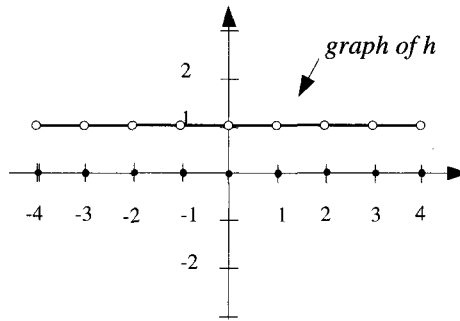
8.

x	G(x)
0	0
1/2	1/2
3/4	3/4
1	0
1 1/2	1/2
1 3/4	3/4
2	0

graph of G
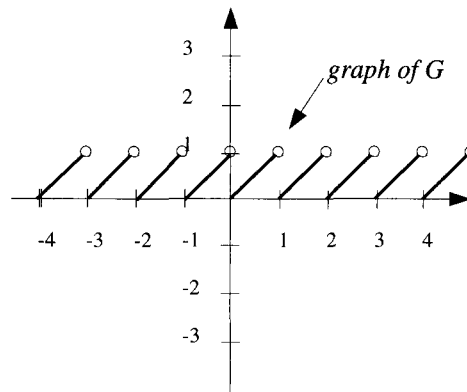
10.

n	g(n) =(n/2) + 1
0	1
1	3/2
2	2
3	5/2
4	3
-1	1/2
-2	0
-3	-1/2

12.

n	$k(n)=\lfloor n^{1/2}\rfloor$
0	0
1	1
2	1
3	1
4	2
5	2
6	2
7	2
8	2
9	3
10	3
15	3
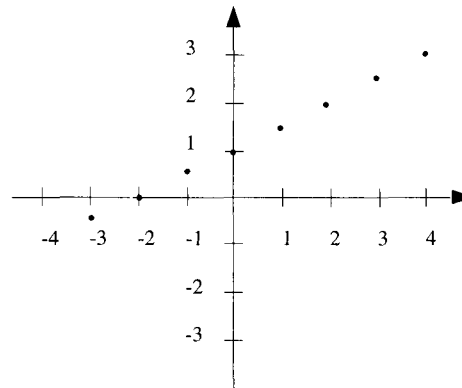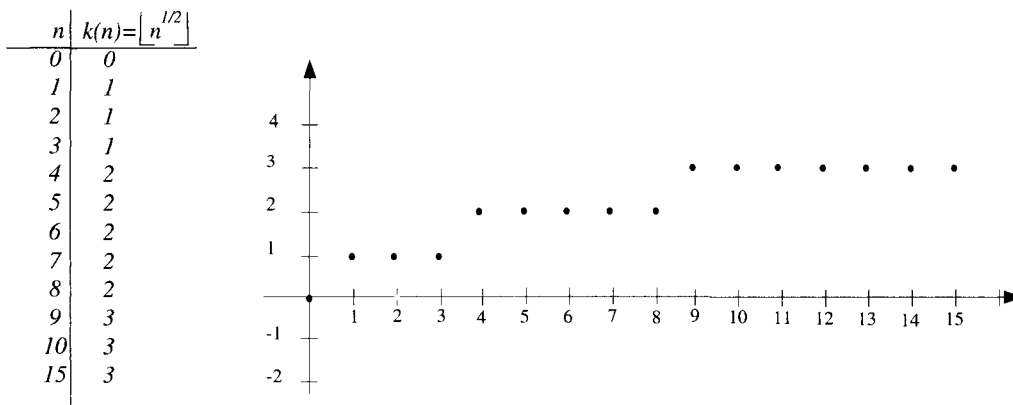
15. *Proof*: Suppose that x_1 and x_2 are particular but arbitrarily chosen real numbers such that $x_1 < x_2$. *[We must show that $g(x_1) > g(x_2)$.]* Multiplying the inequality $x_1 < x_2$ by $-1/3$ gives $(-1/3)x_1 > (-1/3)x_2$. Adding 1 to both sides gives $(-1/3)x_1 + 1 > (-1/3)x_2 + 1$. So by definition of g, $g(x_1) > g(x_2)$ *[as was to be shown]*.

16. *b.* Let $h: \mathbf{R} \to \mathbf{R}$ be the function defined by the formula $h(x) = x^2$. We will show that h is increasing on the set of all real numbers greater than zero. Suppose x_1 and x_2 are real numbers greater than zero and such that $x_1 < x_2$. Multiply both sides of $x_1 < x_2$ by x_1 to obtain $x_1^2 < x_1 x_2$, and multiply both sides of $x_1 < x_2$ by x_2 to obtain $x_1 x_2 < x_2^2$. By transitivity of order *[Appendix A, T17]*, $x_1^2 < x_2^2$, and so by definition of h, $h(x_1) < h(x_2)$.

17. *b.* When $x < 0$, k is increasing.

   Proof: Suppose $x_1 < x_2 < 0$. Multiplying both sides of this inequality by -1 gives $-x_1 > -x_2$, and adding $x_1 x_2$ to both sides gives $x_1 x_2 - x_1 > x_1 x_2 - x_2$. Thus $\dfrac{x_1 x_2 - x_1}{x_1 x_2} > \dfrac{x_1 x_2 - x_2}{x_1 x_2}$ because since x_1 and x_2 are both negative $x_1 x_2$ is positive. Simplifying the two fractions gives $\dfrac{x_2 - 1}{x_2} > \dfrac{x_1 - 1}{x_1}$, and so $k(x_1) < k(x_2)$.

19. *Proof*: Suppose x_1 and x_2 are any real numbers in D and $x_1 < x_2$. *We must show that* $(f+g)(x_1) < (f+g)(x_2)$. Since f and g are both increasing, $f(x_1) < f(x_2)$ and $g(x_1) < g(x_2)$. Adding the two inequalities gives $f(x_1) + g(x_1) < f(x_2) + g(x_2)$, and so by definition of $f+g$, $(f+g)(x_1) < (f+g)(x_2)$. Consequently, $f+g$ is increasing.

20. *b.* *Proof*: Let x_1 and x_2 be real numbers with $0 < x_1 < x_2$. By part (a), $x_1^m < x_2^m$. Now suppose that $g(x_1) \geq g(x_2)$, or, equivalently, $x_1^{\frac{m}{n}} \geq x_2^{\frac{m}{n}}$. Then, since these are nonnegative real numbers, we again use part (a) to obtain $\left(x_1^{\frac{m}{n}}\right)^n \geq \left(x_2^{\frac{m}{n}}\right)^n$. By the laws of exponents, this implies that $x_1^{\frac{m}{n}\cdot n} = x_1^m \geq x_2^m = x_2^{\frac{m}{n}\cdot n}$. But this contradicts the fact that $x_1^m < x_2^m$. Hence the supposition is false, and thus $g(x_1) < g(x_2)$. So g is increasing.

22.
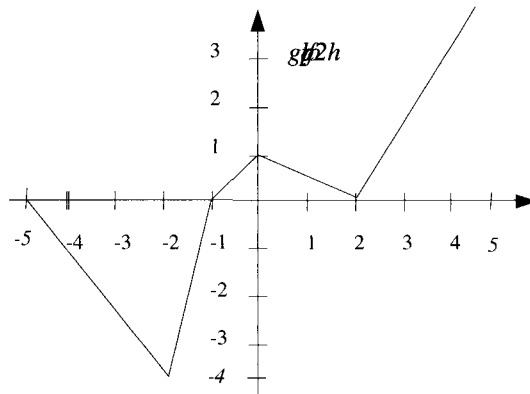
24. *Proof*: Suppose that f is a real-valued function of a real variable, f is increasing on a set S, and M is any negative real number. *[We must show that $M \cdot f$ is decreasing on S. In other words, we must show that for all x_1 and x_2 in the set S, if $x_1 < x_2$ then $(M \cdot f)(x_1) > (M \cdot f)(x_2)$.]* Suppose x_1 and x_2 are in S and $x_1 < x_2$. Since f is increasing on S, $f(x_1) < f(x_2)$. Since M is negative, $Mf(x_1) > Mf(x_2)$ *[because when both sides of an inequality are multiplied by a negative number, the direction of the inequality is reversed]*. It follows by definition of $M \cdot f$ that $(Mf)(x_1) > (Mf)(x_2)$ *[as was to be shown]*.

25. *Proof*: Suppose that f is a real-valued function of a real variable, f is decreasing on a set S, and M is any negative real number. *[We must show that $M \cdot f$ is increasing on S. In other words, we must show that for all x_1 and x_2 in the set S, if $x_1 < x_2$ then $(M \cdot f)(x_1) < (M \cdot f)(x_2)$.]* Suppose x_1 and x_2 are in S and $x_1 < x_2$. Since f is decreasing on S, $f(x_1) > f(x_2)$. Since M is negative, $Mf(x_1) < Mf(x_2)$ *[because when both sides of an inequality are multiplied by a negative number, the direction of the inequality is reversed]*. It follows by definition of Mf that $(Mf)(x_1) < (Mf)(x_2)$ *[as was to be shown]*.

27.
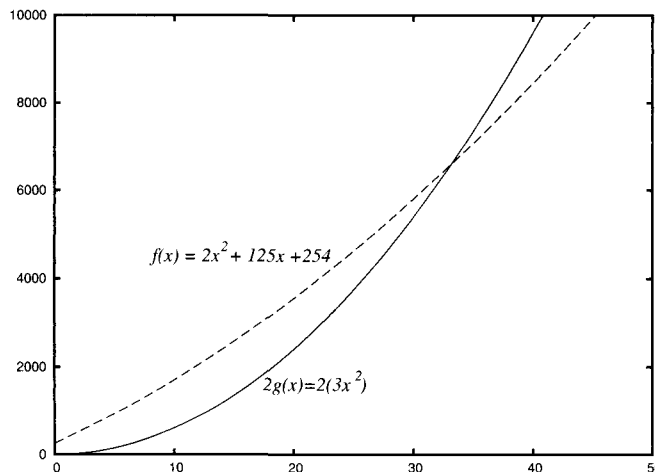
The zoom and trace features of a graphing calculator or computer indicate that when $x \geq 33.2$ (approximately), then $f(x) \leq 2g(x)$.

Alternatively, to find the answer algebraically, solve the equation $2(3x^2) = 2x^2 + 125x + 254$. Subtracting $2x^2 + 125x + 254$ from both sides gives $4x^2 - 125x - 254 = 0$. By the quadratic

formula,

$$x = \frac{125 \pm \sqrt{125^2 + 4064}}{8} = \frac{125 \pm \sqrt{19689}}{8} \cong \frac{125 \pm 140.3175}{8},$$

and so $x \cong 33.165$ or $x \cong -1.915$. Since f and g are defined only for positive values of x, the only place where the two graphs cross is at $x \cong 33.165$. Thus if $x_0 = 33.2$, then for all $x > x_0$, $f(x) \le 2g(x)$.

Section 9.2

2. *a. Formal version of negation*: $f(x)$ is not $O(g(x))$ if, and only if, $\forall$ positive real numbers b and B, $\exists$ a real number $x > b$ such that $|f(x)| > B\,|g(x)|$.

   b. Informal version of negation: $f(x)$ is not $O(g(x))$ if, and only if, no matter what positive real numbers b and B might be chosen, it is possible to find a real number x greater than b with the property that $|f(x)| \ge B\,|g(x)|$.

3. *a. Formal version of negation*: $f(x)$ is not $\Theta(g(x))$ if, and only if, $\forall$ positive real numbers k, A, and B, $\exists$ a real number $x > k$ such that either $|f(x)| < A\,|g(x)|$ or $|f(x)| > B\,|g(x)|$.

   b. Informal version of negation: $f(x)$ is not $O(g(x))$ if, and only if, no matter what positive real numbers k, A, and B might be chosen, it is possible to find a real number x greater than k with the property that either $|f(x)| < A\,|g(x)|$ or $|f(x)| > B\,|g(x)|$.

7. Let $B = 9$ and $b = 1$. Then by substitution, $|3x^6 + 5x^4 - x^3| \le B|x^6|$ for all $x > b$, and hence by definition of O-notation, $3x^6 + 5x^4 - x^3$ is $O(x^6)$.

8. Let $A = 1/2$ and $a = 101$. Then by substitution, $A|x^4| \le |x^4 - 50x^3 + 1|$ for all $x > a$, and hence by definition of Ω-notation, $x^4 - 50x^3 + 1$ is $\Omega(x^4)$.

9. Let $A = 1/2$, $B = 3$, and $k = 25$. Then by substitution, $A|x^2| \le |3x^2 - 80x + 7| \le B|x^2|$ for all $x > k$, and hence by definition of Θ-notation, $3x^2 - 80x + 7$ is $\Theta(x^2)$.

11. *Proof*: Suppose $f\colon \mathbf{R} \to \mathbf{R}$ is a function, $f(x)$ is $O(g(x))$, and c is any nonzero real number. Since $f(x)$ is $O(g(x))$, there exist real numbers B and b such that $|f(x)| \le B|g(x)|$ for all $x > b$. Let $B' = |c|\,B$. Then $B = B'/|c|$, and so

$$|f(x)| \le \frac{B'}{|c|}|g(x)| \qquad \text{for all } x > b.$$

or, equivalently,

$$|c||f(x)| = |cf(x)| \le B'|g(x)| \qquad \text{for all } x > b.$$

Thus $|cf(x)| \le B'|g(x)|$ for all $x > b$, and so, by definition of O-notation, $cf(x)$ is $O(g(x))$.

13. *Proof*: Suppose $f\colon \mathbf{R} \to \mathbf{R}$ is a function. We know that $\frac{1}{2} \le 1 \le 2$ and $|f(x)| \ge 0$ for all real numbers $x \ge 0$. Multiplying all parts of the inequality by $|f(x)|$ gives $\frac{1}{2}|f(x)| \le |f(x)| \le 2|f(x)|$ for all real numbers $x \ge 0$. Let $k = 0$, $A = \frac{1}{2}$, and $B = 2$. Then, by definition of Θ-notation, $f(x)$ is $\Theta(f(x))$.

14. *Note*: For all nonnegative real numbers a, b, c, and d, if $a < b$ and $c < d$ then $ac < bd$. This follows from properties T17 and T19 in Appendix A. To see why, use T19 to multiply both sides of $a < b$ by the nonnegative number c to obtain $ac < bc$, and multiply both sides of $c < d$ by b to obtain $bc < bd$. Then by T17 (the transitive law for order), $ac < bd$.

   Proof: Suppose f, g, h, and k are real-valued functions of a real variable that are defined on the same set D of nonnegative real numbers, and suppose $f(x)$ is $O(h(x))$ and $g(x)$ is $O(k(x))$.

By definition of O-notation, there exist positive real numbers b_1, b_2, B_1, and B_2 such that $|f(x)| \leq B_1 |h(x)|$ for all real numbers $x > b_1$ and $|g(x)| \leq B_2 |k(x)|$ for all real numbers $x > b_2$. Let $B = B_1 B_2$ and let $b = \max(b_1, b_2)$. It follows by the note above that for all real numbers $x > b$,

$$|f(x)g(x)| = |f(x)||g(x)| \leq B_1|h(x)|B_2|k(x)| = B|h(x)k(x)|.$$

Thus, by definition of O-notation, $f(x)g(x)$ is $O(h(x)k(x))$

15. *a. Proof (by mathematical induction):* Let the property $P(n)$ be the sentence "If x is any real number with $x > 1$, then $x^n > 1$.

   Show that the property is true for $n = 1$: We must show that if x is any real number with $x > 1$, then $x^1 > 1$. But $x > 1$ by hypothesis, and $x^1 = x$. So the property is true for $n = 1$.

   Show that for all integers $k \geq 1$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let k be an integer with $k \geq 1$, and suppose that if x is any real number with $x > 1$, then $x^k > 1$. *[This is the inductive hypothesis.]* We must show that if x is any real number with $x > 1$, then $x^{k+1} > 1$. So suppose x is any real number with $x > 1$. By inductive hypothesis, $x^k > 1$, and multiplying both sides by the positive number x gives $x \cdot x^k > x \cdot 1$, or, equivalently, $x^{k+1} > x$. But $x > 1$, and so, by transitivity of order, $x^{k+1} > 1$ *[as was to be shown].*

   b. Proof: Suppose x is any real number with $x > 1$ and m and n are integers with $m < n$. Then $n - m$ is an integer with $n - m \geq 1$, and so, by part (a), $x^{n-m} > 1$. Multiplying both sides by x^m gives $x^m \cdot x^{n-m} > x^m \cdot 1$, and so, by the laws of exponents, $x^n > x^m$ *[as was to be shown].*

17. *a.* For all real numbers $x > 1$, $0 \leq 22x^4 + 8x^2 + 4x$ because all terms are nonnegative. Adding x^4 to both sides gives $x^4 \leq 23x^4 + 8x^2 + 4x$. Because all terms on both sides are nonnegative, we may add absolute value signs to both sides to obtain the result that for all real numbers $x > 1$, $|x^4| \leq |23x^4 + 8x^2 + 4x|$.

   b. For all real numbers $x > 1$,

$$
\begin{array}{rll}
|23x^4 + 8x^3 + 4x| & = & 23x^4 + 8x^3 + 4x \quad \text{because } 23x^4,\ 8x^3,\ \text{and } 4x \text{ are} \\
& & \qquad\qquad\qquad\qquad \text{all positive since } x > 1 \\
\Rightarrow |23x^4 + 8x^3 + 4x| & \leq & 23x^4 + 8x^4 + 4x^4 \quad \text{because } x^3 < x^4 \text{ and } x < x^4 \text{ for } x > 1 \\
\Rightarrow |23x^4 + 8x^3 + 4x| & \leq & 35x^4 \quad\qquad\qquad \text{by combining like terms} \\
\Rightarrow |23x^4 + 8x^3 + 4x| & \leq & 35|x^4| \quad\qquad\quad\ \text{because } x^4 \text{ is positive.}
\end{array}
$$

   c. Let $A = 1$ and $a = 1$. Then by substitution, $A|x^4| \leq |23x^4 + 8x^2 + 4x|$ for all $x > a$, and hence by definition of Ω-notation, $23x^4 + 8x^2 + 4x$ is $\Omega(x^4)$.

   Let $B = 35$ and $b = 1$. Then by substitution, $|23x^4 + 8x^3 + 4x| \leq B|x^4|$ for all $x > b$, and hence by definition of O-notation, $23x^4 + 8x^3 + 4x$ is $O(x^4)$.

   d. Solution 1: Let $A = 1$, $B = 35$, and $k = 1$. By the results of parts (a) and (b), for all real numbers $x > k$, $A|x^4| \leq |23x^4 + 8x^2 + 4x| \leq B|x^4|$, and hence by definition of Θ-notation, $23x^4 + 8x^2 + 4x$ is $\Theta(x^4)$.

   Solution 2: By part (c) and Theorem 9.2.1(1), we can immediately conclude that $23x^4 + 8x^3 + 4x$ is $\Theta(x^4)$.

19. First consider the fact that for all real numbers $x > 1$, $0 \leq 100x + 88$ because all terms are nonnegative. Adding x^2 to both sides gives $x^2 \leq x^2 + 100x + 88$. And because all terms on both sides are nonnegative, we may add absolute value signs to both sides to obtain the result that for all real numbers $x > 1$, $|x^2| \leq |x^2 + 100x + 88|$.

Next consider the following argument: For all real numbers $x > 1$,

$$\begin{array}{rll} |x^2 + 100x + 88| & = & x^2 + 100x + 88 \quad \text{because } x^2, 100x, \text{ and } 88 \text{ are} \\ & & \qquad\qquad\qquad\qquad \text{all positive since } x > 1 \\[4pt] \Rightarrow |x^2 + 100x + 88| & \le & x^2 + 100x^2 + 88x^2 \quad \text{because } x < x^2 \text{ and } 1 < x^2 \text{ for } x > 1 \\[4pt] \Rightarrow |x^2 + 100x + 88| & \le & 189x^2 \qquad\qquad\qquad \text{by combining like terms} \\[4pt] \Rightarrow |x^2 + 100x + 88| & \le & 189|x^2| \qquad\qquad\quad \text{because } x^2 \text{ is positive.} \end{array}$$

Finally, let $A = 1$, $B = 189$, and $k = 1$. Then for all real numbers $x > k$, $A\,|x^2| \le |x^2 + 100x + 88| \le B|x^2|$, and hence by definition of Θ-notation, $x^2 + 100x + 88$ is $\Theta(x^2)$.

21. *a.* For any real number $x > 1$,

$$\begin{array}{rll} |\lfloor\sqrt{x}\rfloor| & = & \lfloor\sqrt{x}\rfloor \quad \text{because since } x > 1 > 0, \text{ then } \lfloor\sqrt{x}\rfloor > 0 \\[4pt] \Rightarrow |\lfloor\sqrt{x}\rfloor| & \le & \sqrt{x} \quad \text{because } \lfloor r \rfloor \le r \text{ for all real numbers } r \\[4pt] \Rightarrow |\lfloor\sqrt{x}\rfloor| & \le & |\sqrt{x}| \quad \text{because } \sqrt{x} \ge 0. \end{array}$$

b. Suppose x is any real number with $x > 1$. By definition of floor, $\lfloor\sqrt{x}\rfloor \le \sqrt{x} < \lfloor\sqrt{x}\rfloor + 1$. Now

$$\begin{array}{rll} \lfloor\sqrt{x}\rfloor + 1 & \le & 2\lfloor\sqrt{x}\rfloor \\[4pt] \Leftrightarrow 1 & \le & \lfloor\sqrt{x}\rfloor \quad \text{by subtracting } \lfloor\sqrt{x}\rfloor \text{ from both sides} \\[4pt] \Leftrightarrow 1 & \le & \sqrt{x} \quad \text{by definition of floor} \\[4pt] \Leftrightarrow 1 & \le & x \quad \text{by squaring both sides (okay because } x \text{ is positive),} \end{array}$$

and the last inequality is true because we are assuming that $x > 1$. Thus, $\sqrt{x} < \lfloor\sqrt{x}\rfloor + 1$ and $\lfloor\sqrt{x}\rfloor + 1 \le 2\lfloor\sqrt{x}\rfloor$, and so, by the transitive law of order (Appendix A, T17), $\sqrt{x} \le 2\lfloor\sqrt{x}\rfloor$. Dividing both sides by 2 gives $\frac{1}{2}\sqrt{x} \le \lfloor\sqrt{x}\rfloor$. Finally, because all quantities are positive, we conclude that $\frac{1}{2}|\sqrt{x}| \le |\lfloor\sqrt{x}\rfloor|$.

c. Let $A = \frac{1}{2}$ and $a = 1$. Then by substitution, $A\,|\sqrt{x}| \le |\lfloor\sqrt{x}\rfloor|$ for all $x > a$, and hence by definition of Ω-notation, $\lfloor\sqrt{x}\rfloor$ is $\Omega(\sqrt{x})$.

Let $B = 1$ and $b = 1$. Then $|\lfloor\sqrt{x}\rfloor| \le B|\sqrt{x}|$ for all real numbers $x > b$, and so by definition of O-notation, $\lfloor\sqrt{x}\rfloor$ is $O(\sqrt{x})$.

d. By part (c) and Theorem 9.2.1(1), we can immediately conclude that $\lfloor\sqrt{x}\rfloor$ is $\Theta(\sqrt{x})$.

23. *a.* For all real numbers $x > 1$,

$$\begin{array}{rll} |\frac{1}{5}x^2 - 42x - 8| & \le & |\frac{1}{5}x^2| + |42x| + |8| \quad \text{by the triangle inequality} \\[4pt] \Rightarrow |\frac{1}{5}x^2 - 42x - 8| & \le & \frac{1}{5}x^2 + 42x + 8 \quad \text{because } \frac{1}{5}x^2, x, \text{ and } 8 \text{ are positive} \\[4pt] \Rightarrow |\frac{1}{5}x^2 - 42x - 8| & \le & \frac{1}{5}x^2 + 42x^2 + 8x^2 \quad \text{because } x < x^2 \text{ and } 1 < x^2 \text{ for } x > 1 \\[4pt] \Rightarrow |\frac{1}{5}x^2 - 42x - 8| & \le & 51x^2 \quad \text{because } \frac{1}{5} + 42 + 8 < 51 \\[4pt] \Rightarrow |\frac{1}{5}x^2 - 42x - 8| & \le & 51|x^2| \quad \text{because } x^2 \text{ is positive.} \end{array}$$

b. Let $B = 51$ and $b = 1$. Then by substitution, $|\frac{1}{5}x^2 - 42x - 8| \le B|x^2|$ for all $x > b$. Hence by definition of O-notation, $\frac{1}{5}x^2 - 42x - 8$ is $O(x^2)$.

24. *a.* For all real numbers $x > 1$,

$$\begin{array}{rll} |\frac{1}{4}x^5 - 50x^3 + 3x + 12| & \le & |\frac{1}{4}x^5| + |50x^3| + |3x| + |12| \quad \text{by the triangle inequality} \\[8pt] \Rightarrow |\frac{1}{4}x^5 - 50x^3 + 3x + 12| & \le & \frac{1}{4}x^5 + 50x^3 + 3x + 12 \quad \text{because } \frac{1}{4}x^5, 50x^3, 3x, \\ & & \qquad\qquad\qquad\qquad\qquad \text{and } 12 \text{ are positive} \\[8pt] \Rightarrow |\frac{1}{4}x^5 - 50x^3 + 3x + 12| & \le & \frac{1}{4}x^5 + 50x^5 + 3x^5 + 12x^5 \quad \text{because } x^3 < x^5, x < x^5, \\ & & \qquad\qquad\qquad\qquad\qquad \text{and } 1 < x^5 \text{ for } x > 1 \\[8pt] \Rightarrow |\frac{1}{4}x^5 - 50x^3 + 3x + 12| & \le & 66x^5 \quad \text{because } \frac{1}{4} + 50 + 3 + 12 < 66 \\[8pt] \Rightarrow |\frac{1}{4}x^5 - 50x^3 + 3x + 12| & \le & 66|x^5| \quad \text{because } x^5 \text{ is positive.} \end{array}$$

b. Let $B = 66$ and $b = 1$. Then by substitution, $|\frac{1}{4}x^5 - 50x^3 + 3x + 12| \leq B|x^2|$ for all $x > b$. Hence by definition of O-notation, $\frac{1}{4}x^5 - 50x^3 + 3x + 12$ is $O(x^2)$.

25. *Proof (by contradiction):* Suppose not. That is, suppose that x^5 is $O(x^2)$. *[We must show that this supposition leads to a contradiction.]* By definition of O-notation, there exist a positive real number B and a nonnegative real number b so that $|x^5| \leq B|x^2|$ (*) for all real numbers $x > b$. Let x be any real number that satisfies both of the following inequalities: $x > b$ and $x > B^{\frac{1}{3}}$. Raising each side of the second inequality to the third power gives $x^3 > B$, and multiplying both sides of this inequality by x^2 yields $x^5 > Bx^2$. Because x and B are positive, we may write $|x^5| > B|x^2|$, which contradicts (*). Hence the supposition is false, and so x^5 is not $O(x^2)$.

27. *Proof:* Suppose $a_0, a_1, a_2, \ldots, a_n$ are real numbers and $a_n \neq 0$; and let

$$d = 2\left(\frac{|a_0| + |a_1| + |a_2| + \cdots + |a_{n-1}|}{|a_n|}\right).$$

Let a be greater than or equal to the maximum of d and 1. Then if $x > a$

$$x \geq 2\left(\frac{|a_0| + |a_1| + |a_2| + \cdots + |a_3| + |a_{n-1}|}{|a_n|}\right)$$

$\Rightarrow \quad \frac{1}{2}|a_n|x \geq |a_0| + |a_1| + |a_2| + \cdots + |a_{n-1}|$

by multiplying both sides by $\frac{1}{2}|a_n|$

$\Rightarrow \quad (1 - \frac{1}{2})|a_n|x \geq |a_0| \cdot \frac{1}{x^{n-1}} + |a_1| \cdot \frac{1}{x^{n-2}} + |a_2| \cdot \frac{1}{x^{n-3}} + \cdots + |a_{n-2}| \cdot \frac{1}{x} + |a_{n-1}| \cdot 1$

because by exercise 15, when $x > 1$ and $m \geq 1$,
then $x^m > 1$, and so $1 > \frac{1}{x^m}$

$\Rightarrow \quad |a_n|x^n - \frac{|a_n|}{2}x^n \geq |a_0| + |a_1|x + |a_2|x^2 + \cdots + |a_{n-2}|x^{n-2} + |a_{n-1}|x^{n-1}$

by multiplying both sides by x^{n-1}.

Subtracting all terms on the right-hand side from both sides and adding the second term on the left-hand side to both sides gives

$$|a_n|x^n - |a_{n-1}|x^{n-1} - |a_{n-2}|x^{n-2} - \cdots - |a_2|x^2 - |a_1|x - |a_0| \geq \frac{|a_n|}{2}x^n.$$

Now $-|r| \leq r \leq |r|$ for all real numbers r. Thus, when $x > 1$, $-|a_i|x^i \leq a_ix^i \leq |a_i|x^i$ for each integer i with $0 \leq i \leq n - 1$, and so

$$|a_n|x^n - |a_{n-1}|x^{n-1} - |a_{n-2}|x^{n-2} - \cdots - |a_2|x^2 - |a_1|x - |a_0|$$
$$\leq a_nx^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_2x^2 + a_1x + a_0$$
$$\leq \left|a_nx^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_2x^2 + a_1x + a_0\right|.$$

Hence

$$\frac{|a_n|}{2}x^n \leq \left|a_nx^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_2x^2 + a_1x + a_0\right|.$$

Let $A = \frac{|a_n|}{2}$ and let a be as defined above. Then

$$Ax^n \leq \left|a_nx^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_2x^2 + a_1x + a_0\right| \qquad \text{for all real numbers } x > a.$$

It follows by definition of Ω-notation that $a_nx^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_2x^2 + a_1x + a_0$ is $\Omega(x^n)$.

29. Let $a = 2\left(\frac{42+8}{1/5}\right) = 500$, and let $A = \left(\frac{1}{2}\right)\left(\frac{1}{5}\right) = \frac{1}{10}$. If $x > 500$, then

$$x \geq 2\left(\frac{42+8}{1/5}\right)$$

$\Rightarrow \qquad \frac{1}{2} \cdot \frac{1}{5}x \geq 42 + 8 \qquad$ by multiplying both sides by $\frac{1}{2} \cdot \frac{1}{5}$

$\Rightarrow \qquad \left(1 - \frac{1}{2}\right) \cdot \frac{1}{5}x \geq 42 + 8 \cdot \frac{1}{x} \qquad$ because $1 - \frac{1}{2} = \frac{1}{2}$, and since $x > 500 > 1$
then $1 > \frac{1}{x}$ and so $8 > 8 \cdot \frac{1}{x}$

$\Rightarrow \qquad \frac{1}{5}x^2 - \frac{1}{2} \cdot \frac{1}{5}x^2 \geq 42x + 8 \qquad$ by multiplying both sides by x

$\Rightarrow \qquad \frac{1}{5}x^2 - 42x - 8 \geq \frac{1}{2} \cdot \frac{1}{5}x^2 \qquad$ by subtracting $42x + 8$ from and
adding $\frac{1}{2} \cdot \frac{1}{5}x^2$ to both sides

$\Rightarrow \qquad \left|\frac{1}{5}x^2 - 42x - 8\right| \geq \frac{1}{10}\left|x^2\right| \qquad$ because both sides are nonnegative.

Thus for all real numbers $x > a$, $\left|\frac{1}{5}x^2 - 42x - 8\right| \geq A\left|x^2\right|$. Hence, by definition of Ω-notation, we conclude that $\frac{1}{5}x^2 - 42x - 8$ is $\Omega(x^2)$.

30. Let $a = 2\left(\frac{50 + 3 + 12}{1/4}\right) = 520$, and let $A = \frac{1}{2} \cdot \frac{1}{4} = \frac{1}{8}$. If $x > 520$, then

$$x \geq 2\left(\frac{50 + 3 + 12}{1/4}\right)$$

$\Rightarrow \qquad \frac{1}{2} \cdot \frac{1}{4}x \geq 50 + 3 + 12$
by multiplying both sides by $\frac{1}{2} \cdot \frac{1}{4}$

$\Rightarrow \qquad \left(1 - \frac{1}{2}\right) \cdot \frac{1}{4}x \geq 50\frac{1}{x} + 3 \cdot \frac{1}{x^3} + 12 \cdot \frac{1}{x^4}$
because $1 - \frac{1}{2} = \frac{1}{2}$, and, since $x > 520 > 1$,
then $1 > \frac{1}{x}, 1 > \frac{1}{x^3}$ and $1 > \frac{1}{x^4}$

$\Rightarrow \qquad \frac{1}{4}x^5 - \frac{1}{2} \cdot \frac{1}{4}x^5 \geq 50x^3 + 3x + 12$
by multiplying both sides by x^4

$\Rightarrow \qquad \frac{1}{4}x^5 - 50x^3 - 3x - 12 \geq \frac{1}{2} \cdot \frac{1}{4}x^5$
by subtracting $50x^3 + 3x + 12$ from and
adding $\frac{1}{2} \cdot \frac{1}{4}x^5$ to both sides

$\Rightarrow \qquad \frac{1}{4}x^5 - 50x^3 + 3x + 12 \geq \frac{1}{2} \cdot \frac{1}{4}x^5$
because $3x + 12 > -3x - 12$ since $x > 0$

$\Rightarrow \qquad \left|\frac{1}{4}x^5 - 50x^3 + 3x + 12\right| \geq \frac{1}{8}\left|x^5\right|$
because both sides are nonnegative.

Thus for all real numbers $x > a$, $\left|\frac{1}{4}x^5 - 50x^3 + 3x + 12\right| \geq A\left|x^5\right|$. Hence, by definition of Ω-notation, we conclude that $\frac{1}{4}x^5 - 50x^3 + 3x + 12$ is $\Omega(x^5)$.

32. By exercise 23, $\frac{1}{5}x^2 - 42x - 8$ is $O(x^2)$ and, by exercise 30, $\frac{1}{5}x^2 - 42x - 8$ is $\Omega(x^2)$. Thus, by Theorem 9.2.1(1), $\frac{1}{5}x^2 - 42x - 8$ is $\Theta(x^2)$.

33. By exercise 24, $\frac{1}{4}x^5 - 50x^3 + 3x + 12$ is $O(x^5)$ and, by exercise 31, $\frac{1}{4}x^5 - 50x^3 + 3x + 12$ is $\Omega(x^5)$. Thus, by Theorem 9.2.1(1), $\frac{1}{4}x^5 - 50x^3 + 3x + 12$ is $\Theta(x^5)$.

35. $\frac{x}{3}(4x^2 - 1) = \frac{4}{3}x^3 - \frac{1}{3}x$ is $\Theta(x^3)$ by the theorem on polynomial orders.

36. $\frac{x(x-1)}{2} + 3x = \frac{x^2 - x}{2} + \frac{6}{2}x = \frac{1}{2}x^2 + \frac{5}{2}x$ is $\Theta(x^2)$ by the theorem on polynomial orders.

38. $\left(\dfrac{n(n+1)}{2}\right)^2 = \dfrac{n^2(n^2+2n+1)}{4} = \dfrac{1}{4}n^4 + \dfrac{1}{2}n^3 + \dfrac{1}{4}n^2$ is $\Theta(n^4)$ by the theorem on polynomial orders.

39. $2(n-1)+\dfrac{n(n+1)}{2} + 4\left(\dfrac{n(n-1)}{2}\right) = 2n-2+\dfrac{n^2}{2}+\dfrac{n}{2}+2(n^2-n) = \dfrac{5}{2}n^2 + \dfrac{1}{2}n - 2$ is $\Theta(n^2)$ by the theorem on polynomial orders.

41. By exercise 11 of Section 4.2, $1^3 + 2^3 + 3^3 + \cdots + n^3 = \left(\dfrac{n(n+1)}{2}\right)^2$, and by exercise 38 above this is $\Theta(n^4)$. Hence $1^3 + 2^3 + 3^3 + \cdots + n^3$ is $O(n^4)$.

43. By factoring out a 5, $5 + 10 + 15 + 20 + 25 + \cdots + 5n = 5(1 + 2 + 3 + \cdots + n) = 5\left(\dfrac{n(n+1)}{2}\right)$ *[by Theorem 4.2.2]* $= \dfrac{5}{2}n^2 + \dfrac{5}{2}n$, which is $\Theta(n^2)$ by the theorem on polynomial orders.

45. $\displaystyle\sum_{k=1}^{n}(k+3) = \sum_{k=1}^{n} k + \sum_{k=1}^{n} 3$ *[by Theorem 4.1.1]* $= \dfrac{n(n+1)}{2} + \underbrace{(3 + 3 + \cdots + 3)}_{n \text{ terms}}$ *[by Theorem 4.2.2]*
$= \dfrac{1}{2}n^2 + \dfrac{1}{2}n + 3n$ *[because multiplication is repeated addition]* $= \dfrac{1}{2}n^2 + \dfrac{7}{2}n$, which is $\Theta(n^2)$ by the theorem on polynomial orders.

46. $\displaystyle\sum_{i=1}^{n} i(i+1) = \dfrac{n(n+1)(n+2)}{3}$ *[by exercise 13, Section 4.2]* $= \dfrac{1}{3}n^3 + n^2 + \dfrac{2}{3}n$, which is $\Theta(n^3)$ by the theorem on polynomial orders.

47. $\displaystyle\sum_{k=1}^{n}(k^2 - 2k) = \sum_{k=1}^{n} k^2 - 2\sum_{k=1}^{n} k$ *[by Theorem 4.1.1]* $= \dfrac{n(n+1)(2n+1)}{6} - 2\left(\dfrac{n(n+1)}{2}\right)$ *[by exercise 10, Section 4.2 and Theorem 4.2.2]* $= \dfrac{2n^3+3n^2+n}{6} + n^2 + n = \dfrac{1}{3}n^3 + \dfrac{3}{2}n^2 + \dfrac{7}{6}n$, which is $\Theta(n^3)$ by the theorem on polynomial orders.

48. *a. Proof:* Suppose $a_0, a_1, a_2, \ldots, a_n$ are real numbers and $a_n \neq 0$. Then

$$\lim_{x\to\infty} \left|\frac{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0}{a_n x^n}\right|$$

$$= \lim_{x\to\infty}\left(1 + \left|\frac{a_{n-1}}{a_n}\right|\frac{1}{x} + \cdots + \left|\frac{a_2}{a_n}\right|\frac{1}{x^{n-2}} + \left|\frac{a_1}{a_n}\right|\frac{1}{x^{n-1}} + \left|\frac{a_0}{a_n}\right|\frac{1}{x^n}\right)$$

$$= \lim_{x\to\infty} 1 + \left|\frac{a_{n-1}}{a_n}\right|\lim_{x\to\infty}\frac{1}{x} + \cdots + \left|\frac{a_2}{a_n}\right|\lim_{x\to\infty}\frac{1}{x^{n-2}} + \left|\frac{a_1}{a_n}\right|\lim_{x\to\infty}\frac{1}{x^{n-1}} + \left|\frac{a_0}{a_n}\right|\lim_{x\to\infty}\frac{1}{x^n}$$

$$= 1$$

because $\displaystyle\lim_{x\to\infty}\frac{1}{x^k} = 0$ for all integers $k \geq 1$.

b. Proof: Suppose $a_0, a_1, a_2, \ldots, a_n$ are real numbers and $a_n \neq 0$. By part (a) and the definition of limit, we can make the following statement: For all positive real numbers ε, there exists a real number M (which we may take to be positive) such that

$$1 - \varepsilon < \left|\frac{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0}{a_n x^n}\right| < 1 + \varepsilon \qquad \text{for all real numbers } x > M.$$

Let $\varepsilon = 1/2$. Then there exists a real number M_0 such that

$$1 - \frac{1}{2} < \left|\frac{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0}{a_n x^n}\right| < 1 + \frac{1}{2} \qquad \text{for all real numbers } x > M_0.$$

Equivalently, for all real numbers $x > M_0$,

$$\frac{1}{2}|a_n||x^n| < |a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0| < \frac{3}{2}|a_n||x^n|.$$

Let $A = \frac{1}{2}|a_n|$, $B = \frac{3}{2}|a_n|$, and $k = M_0$. Then

$$A|x^n| \leq |a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0| \leq B|x^n| \quad \text{for all real numbers } x > k,$$

and so, by definition of Θ-notation, $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$ is $\Theta(x^n)$.

49. *c.* See the solution to exercise 11.

d. It follows from property (9.2.1) that for all real numbers $x > 1$, $x^2 < x^5$ and $1 = x^0 < x^5$. Clearly also $x^5 \leq x^5$. So for all real numbers $x > 1$, $|x^5| \leq 1 \cdot |x^5|$, $|x^2| \leq 1 \cdot |x^5|$, and $|1| \leq 1 \cdot |x^5|$. Hence by definition of O-notation, x^5 is $O(x^5)$, x^2 is $O(x^5)$, and 1 is $O(x^5)$. By part (c), then, $12x^5$ is $O(x^5)$, $-34x^2$ is $O(x^5)$, and $7 = 7 \cdot 1$ is $O(x^5)$. So by part (a), $12x^5 + (-34)x^2 + 7 = 12x^5 - 34x^2 + 7$ is $O(x^5)$.

e. Let a nonnegative integer n be given. It follows from property (9.2.1) that for all real numbers $x > 1$ and for all integers k with $0 \leq k \leq n$, $x^k \leq x^n$. So since all expressions are positive, if $B = 1$ and $b = 1$, then for all real numbers x with $x > b$, $|x^k| \leq B|x^n|$. Thus by definition of O-notation, x^k is $O(x^n)$. Hence, by part (c), $a_k x^k$ is $O(x^n)$ for all real numbers $a_0, a_1, a_2, \ldots, a_n$. So by repeated application of part (a), $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$ is $O(x^n)$.

50. *a. Proof 1 (by mathematical induction)*: Let the property $P(n)$ be the sentence "If $0 < x \leq 1$, then $x^n \leq 1$."

Show that the property is true for $n = 1$: We must show that if $0 < x \leq 1$, then $x^1 \leq 1$. But $x \leq 1$ by assumption and $x^1 = x$. So the property is true for $n = 1$.

Show that for all integers $k \geq 1$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let k be an integer with $k \geq 1$, and suppose that if $0 < x \leq 1$, then $x^k \leq 1$. *[This is the inductive hypothesis.]* We must show that if $0 < x \leq 1$, then $x^{k+1} \leq 1$. So let x be any number with $0 < x \leq 1$. By inductive hypothesis, $x^k \leq 1$, and multiplying both sides of this inequality by the nonnegative number x gives $x \cdot x^k \leq x \cdot 1$. Thus, by the laws of exponents, $x^{k+1} \leq x$. Then $x^{k+1} \leq x$ and $x \leq 1$, and hence, by the transitive property of order (T17 in Appendix B), $x^{k+1} \leq 1$.

Proof 2: By exercise 20(a) of Section 9.1, for any positive integer n, the function f defined by $f(x) = x^n$ is increasing on the set of nonnegative real numbers. Hence if $0 < x \leq 1$, then $x^n \leq 1^n = 1$.

b. Part (a) showed that for any positive real number x and for all integers $n \geq 1$, if $x \leq 1$ then $x^n \leq 1$. The logically equivalent contrapositive for this statement is the following: For any positive real number x and for all integers $n \geq 1$, if $x^n > 1$ then $x > 1$.

c. Substitute $x^{1/n}$ in place of x in the result of part (b) to obtain: For any positive real number x and for all integers $n \geq 1$, if $(x^{1/n})^n > 1$ then $x^{1/n} > 1$. But $(x^{1/n})^n = x$ because x is positive. So for any positive real number x and for all integers $n \geq 1$, if $x > 1$ then $x^{1/n} > 1$.

d. Proof 1: Let p, q, r, and s be integers with q and s nonzero and $\frac{p}{q} > \frac{r}{s}$, and let x be any real number with $x > 1$. Since $\frac{p}{q} > \frac{r}{s}$, then $\frac{p}{q} - \frac{r}{s} > 0$, or, equivalently, $\frac{ps-qr}{qs} > 0$. Thus either both $ps - qr$ and qs are positive, or both are negative.

Case 1 (both $ps - qr$ and qs are positive): By part (c) since $x > 1$, $x^{1/qs} > 1$. Also, because $ps - qr > 0$ and because $ps - qr$ is an integer, then $ps - qr \geq 1$. So by exercise 15b (with $n = ps - qr$ and $m = 1$), $\left(x^{1/qs}\right)^{pq-rs} \geq \left(x^{1/qs}\right)^1 = x^{1/qs} > 1$. But $\left(x^{1/qs}\right)^{pq-rs} = x^{\frac{ps-qr}{qs}} = x^{\frac{p}{q}-\frac{r}{s}} = \frac{x^{\frac{p}{q}}}{x^{\frac{r}{s}}}$. So $\frac{x^{\frac{p}{q}}}{x^{\frac{r}{s}}} > 1$, or, equivalently, $x^{\frac{p}{q}} > x^{\frac{r}{s}}$.

Case 2 (both $ps - qr$ and qs are negative): Let $p' = -p$ and $q' = -q$. Then $\frac{p'}{q'} = \frac{-p}{-q} = \frac{p}{q}$, and so $\frac{p'}{q'} > \frac{r}{s}$. But also $p's - q'r$ and $q's$ are both positive. So by case 1, $x^{\frac{p'}{q'}} > x^{\frac{r}{s}}$, and hence $x^{\frac{p}{q}} > x^{\frac{r}{s}}$.

Proof 2: Let p, q, r, and s be integers with q and s nonzero and $\frac{p}{q} > \frac{r}{s}$, and let x be any real number with $x > 1$. Since $\frac{p}{q} > \frac{r}{s}$, then $\frac{p}{q} - \frac{r}{s} > 0$, or, equivalently, $\frac{ps-qr}{qs} > 0$. Let f be the function defined by the formula $f(x) = x^{\frac{ps-qr}{qs}}$. By the result of exercise 20 in Section 9.1, f is increasing. Hence if $x > 1$, then $x^{\frac{ps-qr}{qs}} > 1^{\frac{ps-qr}{qs}} = 1$. But $\left(x^{1/qs}\right)^{pq-rs} = x^{\frac{ps-qr}{qs}} = x^{\frac{p}{q}-\frac{r}{s}} = \frac{x^{\frac{p}{q}}}{x^{\frac{r}{s}}}$. So $\frac{x^{\frac{p}{q}}}{x^{\frac{r}{s}}} > 1$, or, equivalently, $x^{\frac{p}{q}} > x^{\frac{r}{s}}$.

52. Note that $\sqrt{x}(38x^5 + 9) = 38x^{11/2} + 9x^{1/2}$. By part (d) of exercise 50 (or property (9.2.1)), for all $x > 1$, $x^{1/2} \le x^{11/2}$. Hence, by definition of O-notation (with $B = 1$ and $b = 1$), $x^{1/2}$ is $O(x^{11/2})$. Also by exercise 13, $x^{11/2}$ is $O(x^{11/2})$. Thus, by exercise 49c, $38x^{11/2}$ is $O(x^{11/2})$ and $9x^{1/2}$ is $O(x^{11/2})$, and therefore, by exercise 49a, $38x^{11/2} + 9x^{1/2}$ is $O(x^{11/2})$.

53. *Proof (by contradiction):* Suppose not. That is, suppose there exist rational numbers r and s where $r > s$ and x^r is $O(x^s)$. Then there exist a positive real number B and a nonnegative real number b such that $|x^r| \le B|x^s|$ for all real numbers $x > b$. Let x be any real number that is greater than $B^{1/(r-s)}$, 1, and b.

Case 1($B \ge 1$): In this case, we have that $x > B^{1/(r-s)}$, and so, by exercise 15 (or property (9.2.1)), $x^{r-s} > (B^{1/(r-s)})^{r-s} = B$. But $x^{r-s} = \frac{x^r}{x^s}$, and so $\frac{x^r}{x^s} > B$. Multiplying both sides by x^s gives $x^r > Bx^s$, and because x is positive, we have $|x^r| > B|x^s|$. This contradicts the result that $|x^r| \le B|x^s|$.

Case 2($B < 1$): In this case, we have that $|x^r| \le |x^s|$, or, because x is positive $x^r \le x^s$. But this contradicts the result of exercise 50d (or property (9.2.1)) because $r > s$.

Hence, in either case, we have deduced a contradiction, which implies that the supposition is false and the statement to be proved is true.

55. $f(x) = \frac{(2x^{7/2} + 1)(x - 1)}{(x^{1/2} + 1)(x + 1)} = \frac{2x^{9/2} - 2x^{7/2} + x - 1}{x^{3/2} + x + x^{1/2} + 1}$. The numerator of $f(x)$ is a sum of rational power functions with highest power 9/2, and the denominator is a sum of rational power functions with highest power 3/2. Because $9/2 - 3/2 = 6/2 = 3$, Theorem 9.2.4 implies that $f(x)$ is $\Theta(x^3)$.

56. $f(x) = \frac{(5x^2 + 1)(\sqrt{x} - 1)}{4x^{3/2} - 2x} = \frac{5x^{5/2} - 5x^2 + x^{1/2} - 1}{4x^{3/2} - 2x}$. The numerator of $f(x)$ is a sum of rational power functions with highest power 5/2, and the denominator is a sum of rational power functions with highest power 3/2. Because $5/2 - 3/2 = 2/2 = 1$, Theorem 9.2.4 implies that $f(x)$ is $\Theta(x)$.

57. b. *Proof (by mathematical induction):* Let the property $P(n)$ be the inequality

$$\frac{1}{2}n^{3/2} \le \sqrt{1} + \sqrt{2} + \sqrt{3} + \cdots + \sqrt{n}.$$

Show that the property is true for $n = 1$: We must show that $\frac{1}{2} \cdot 1^{3/2} \le \sqrt{1}$. But the left-hand side of the inequality is 1/2 and the right-hand side is 1, and $1/2 < 1$. So the property is true for $n = 1$.

Show that for all integers $k \ge 1$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let k be an integer with $k \ge 1$, and suppose that

$$\frac{1}{2}k^{3/2} \le \sqrt{1} + \sqrt{2} + \sqrt{3} + \cdots + \sqrt{k}. \qquad \textit{[This is the inductive hypothesis.]}$$

We must show that

$$\frac{1}{2}(k + 1)^{3/2} \le \sqrt{1} + \sqrt{2} + \sqrt{3} + \cdots + \sqrt{k + 1}.$$

By adding $\sqrt{k+1}$ to both sides of the inductive hypothesis, we have

$$\frac{1}{2}k^{3/2} + \sqrt{k+1} \leq \sqrt{1} + \sqrt{2} + \sqrt{3} + \cdots + \sqrt{k} + \sqrt{k+1}.$$

Thus, by the transitivity of order, it suffices to show that

$$\frac{1}{2}(k+1)^{3/2} \leq \frac{1}{2}k^{3/2} + \sqrt{k+1}.$$

Now when $k \geq 1$, $k^2 \geq k^2 - 1 = (k-1)(k+1)$. Divide both sides by $k(k-1)$ to obtain $\frac{k}{k-1} \geq \frac{k+1}{k}$. But $\frac{k+1}{k} \geq 1$, and any number greater than or equal to 1 is greater than or equal to its own square root. Thus $\frac{k}{k-1} \geq \frac{k+1}{k} \geq \sqrt{\frac{k+1}{k}} = \frac{\sqrt{k+1}}{\sqrt{k}}$. Hence $k\sqrt{k} \geq (k-1)\sqrt{k+1} = (k+1-2)\sqrt{k+1} = (k+1)^{3/2} - 2\sqrt{k+1}$. Multiplying both sides by $1/2$ gives $\frac{1}{2}k^{3/2} \geq \frac{1}{2}(k+1)^{3/2} - \sqrt{k+1}$, or, equivalently, $\frac{1}{2}(k+1)^{3/2} \leq \frac{1}{2}k^{3/2} + \sqrt{k+1}$. *[This is what was to be shown].*

58. *a. Proof (by mathematical induction):* Let the property $P(n)$ be the inequality $1^{1/3} + 2^{1/3} + \cdots + n^{1/3} \leq n^{4/3}$.

Show that the property is true for $n = 1$: We must show that $1^{1/3} \leq 1^{4/3}$. But this inequality is true because both sides equal 1.

Show that for all integers $k \geq 1$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let k be an integer with $k \geq 1$, and suppose that

$$1^{1/3} + 2^{1/3} + \cdots + k^{1/3} \leq k^{4/3}. \qquad \text{[This is the inductive hypothesis.]}$$

We must show that
$$1^{1/3} + 2^{1/3} + \cdots + (k+1)^{1/3} \leq (k+1)^{4/3}.$$

But by inductive hypothesis, $1^{1/3} + 2^{1/3} + \cdots + k^{1/3} \leq k^{4/3}$, and so

$$1^{1/3} + 2^{1/3} + \cdots + k^{1/3} + (k+1)^{1/3} \leq k^{4/3} + (k+1)^{1/3}$$

$$\Rightarrow 1^{1/3} + 2^{1/3} + \cdots + k^{1/3} + (k+1)^{1/3} \leq k^{1/3} \cdot k + (k+1)^{1/3} \qquad \text{by factoring out } k$$

$$\Rightarrow 1^{1/3} + 2^{1/3} + \cdots + k^{1/3} + (k+1)^{1/3} \leq (k+1)^{1/3} \cdot k + (k+1)^{1/3} \qquad \text{because } k^{1/3} \leq (k+1)^{1/3}$$

$$\Rightarrow 1^{1/3} + 2^{1/3} + \cdots + k^{1/3} + (k+1)^{1/3} \leq (k+1)^{1/3}(k+1) \qquad \text{by factoring out } (k+1)^{1/3}$$

$$\Rightarrow 1^{1/3} + 2^{1/3} + \cdots + k^{1/3} + (k+1)^{1/3} \leq (k+1)^{4/3} \qquad \text{by the laws of exponents.}$$

b. Proof (by mathematical induction): Let the property $P(n)$ be the inequality $\frac{1}{2}n^{4/3} \leq 1^{1/3} + 2^{1/3} + \cdots + n^{1/3}$.

Show that the property is true for $n = 1$: We must show that $\frac{1}{2} \cdot 1^{4/3} \leq 1^{1/3}$. But this inequality is true because the left-hand side equals $1/2$ and the right-hand side equals 1.

Show that for all integers $k \geq 1$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let k be an integer with $k \geq 1$, and suppose that

$$\frac{1}{2}k^{4/3} \leq 1^{1/3} + 2^{1/3} + \cdots + k^{1/3}. \qquad \text{[This is the inductive hypothesis.]}$$

We must show that
$$\frac{1}{2}(k+1)^{4/3} \leq 1^{1/3} + 2^{1/3} + \cdots + (k+1)^{1/3}.$$

By adding $(k+1)^{1/3}$ to both sides of the inductive hypothesis, we have

$$\frac{1}{2}k^{4/3} + (k+1)^{1/3} \leq 1^{1/3} + 2^{1/3} + \cdots + k^{1/3} + (k+1)^{1/3}.$$

Thus, by the transitivity of order, it suffices to show that

$$\frac{1}{2}(k+1)^{4/3} \leq \frac{1}{2}k^{4/3} + (k+1)^{1/3}.$$

Now when $k \geq 1$, $k^2 \geq k^2 - 1 = (k-1)(k+1)$. Divide both sides by $k(k-1)$ to obtain $\dfrac{k}{k-1} \geq \dfrac{k+1}{k}$. But $\dfrac{k+1}{k} \geq 1$, and any number greater than or equal to 1 is greater than or equal to its own cube root. Thus $\dfrac{k}{k-1} \geq \dfrac{k+1}{k} \geq \sqrt[3]{\dfrac{k+1}{k}} = \dfrac{\sqrt[3]{k+1}}{\sqrt[3]{k}}$. Hence $k \cdot \sqrt[3]{k} \geq (k-1)\sqrt[3]{k+1} = (k+1-2)\sqrt[3]{k+1} = (k+1)^{4/3} - 2\sqrt[3]{k+1}$. Multiplying both sides by $1/2$ gives $\dfrac{1}{2}k^{4/3} \geq \dfrac{1}{2}(k+1)^{4/3} - \sqrt[3]{k+1}$, or, equivalently, $\frac{1}{2}(k+1)^{4/3} \leq \frac{1}{2}k^{4/3} + \sqrt[3]{k+1}$. *[This is what was to be shown]*.

c. Let $A = 1/2$, $B = 1$, and $k = 1$. By parts (a) and (b) and because all quantities are positive,

$$A\left|n^{4/3}\right| \leq \left|1^{1/3} + 2^{1/3} + \cdots + n^{1/3}\right| \leq B\left|n^{4/3}\right| \qquad \text{for all } n > k.$$

Thus by definition of Θ-notation, $1^{1/3} + 2^{1/3} + \cdots + n^{1/3}$ is $\Theta(n^{4/3})$.

60. *Proof*: Suppose $f(x)$ and $g(x)$ are $o(h(x))$ and a and b are any real numbers. Then by properties of limits,

$$\lim_{x\to\infty} \frac{af(x) + bg(x)}{h(x)} = a\lim_{x\to\infty}\frac{f(x)}{h(x)} + b\lim_{x\to\infty}\frac{g(x)}{h(x)} = a\cdot 0 + b\cdot 0 = 0.$$

So $af(x) + bg(x)$ is $o(h(x))$.

61. *Proof*: Suppose a and b are any positive real numbers such that $a < b$. Then $b - a > 0$, and so since $\dfrac{1}{x^c} \to 0$ for any positive number c,

$$\lim_{x\to\infty}\frac{x^a}{x^b} = \lim_{x\to\infty}\frac{1}{x^{b-a}} = 0.$$

So x^a is $o(x^b)$.

Section 9.3

1. *b.* 0.2 microseconds or 0.0000002 seconds   *c.* 1.53 microseconds or 0.00000153 seconds   *f.* 5.09×10^{43} years

3. *a.* When the input size is increased from m to $2m$, the number of operations increases from cm^3 to $c(2m)^3 = 8cm^3$.

   b. By part (a), the number of operations increases by a factor of $\dfrac{8cm^3}{cm^3} = 8$.

   c. When the input size is increased by a factor of 10 (from m to $10m$), the number of operations increases by a factor of $\dfrac{c(10m^3)}{cm^3} = \dfrac{1000cm^3}{cm^3} = 1000$.

5. *a.* By the theorem on polynomial orders, algorithm A has order n^2 and algorithm B has order n^3. So algorithm A has order n^2 and algorithm B has order n^3.

b. Algorithm A is more efficient than algorithm B for values of n with $10^6 n^2 < n^3$. Dividing both sides by n^2 shows that algorithm A is more efficient than algorithm B when $n > 10^6 = 1,000,000$.

c. Algorithm B is 100 times more efficient than algorithm A for values of n with $100(n^3) < 10^6 n^2$. Dividing both sides by $100n^2$ shows that algorithm B is more efficient than algorithm A when $n < 10^4 = 10,000$.

7. *a.* For each iteration of the loop there is one comparison. The number of iterations of the loop is $n - 2 + 1 = n - 1$. Therefore, the total number of elementary operations that must be performed when the algorithm is executed is $n - 1$.

b. By the theorem on polynomial orders, $n - 1$ is $\Theta(n)$, and so the algorithm segment has order n.

10. *a.* For each iteration of the inner loop there is one subtraction. There are $3n$ iterations of the inner loop for each iteration of the outer loop, and there are $n - 2 + 1 = n - 1$ iterations of the outer loop. Therefore, the number of iterations of the inner loop is $3n(n - 1) = 3n^2 - 3n$. It follows that the total number of elementary operations that must be performed when the algorithm is executed is $3n^2 - 3n$.

b. By the theorem on polynomial orders, $3n^2 - 3n$ is $\Theta(n^2)$, and so the algorithm segment has order n^2.

12. *a.* For each iteration of the inner loop there is one comparison. The number of iterations of the inner loop can be deduced from the following table, which shows the values of k and i for which the inner loop is executed.

k	1				2				$\cdots$	$n-2$		$n-1$
i	2	3	$\cdots$	n	3	4	$\cdots$	n	$\cdots$	$n-1$	n	n

$$\underbrace{\qquad}_{n-1} \quad \underbrace{\qquad}_{n-2} \quad \underbrace{\qquad}_{2} \quad \underbrace{\quad}_{1}$$

Therefore, by Theorem 4.2.2, the number of iterations of the inner loop is $(n - 1) + (n - 2) + \cdots + 2 + 1 = \frac{n(n-1)}{2}$. It follows that the total number of elementary operations that must be performed when the algorithm is executed is $1 \cdot \left(\frac{n(n-1)}{2}\right) = \frac{1}{2}n^2 - \frac{1}{2}n$.

By the theorem on polynomial orders, $\frac{1}{2}n^2 - \frac{1}{2}n$ is $\Theta(n^2)$, and so the algorithm segment has order n^2.

13. *a.* For each iteration of the inner loop there is one comparison. The number of iterations of the inner loop can be deduced from the following table, which shows the values of i and j for which the inner loop is executed.

i	1				2				$\cdots$	$n-2$		$n-1$
j	2	3	$\cdots$	n	3	4	$\cdots$	n	$\cdots$	$n-1$	n	n

$$\underbrace{\qquad}_{n-1} \quad \underbrace{\qquad}_{n-2} \quad \underbrace{\qquad}_{2} \quad \underbrace{\quad}_{1}$$

Therefore, by Theorem 4.2.2, the number of iterations of the inner loop is $(n - 1) + (n - 2) + \cdots + 2 + 1 = \frac{n(n-1)}{2}$. It follows that the total number of elementary operations that must be performed when the algorithm is executed is $1 \cdot \left(\frac{n(n-1)}{2}\right) = \frac{1}{2}n^2 - \frac{1}{2}n$.

By the theorem on polynomial orders, $\frac{1}{2}n^2 - \frac{1}{2}n$ is $\Theta(n^2)$, and so the algorithm segment has order n^2.

15. *a.* There are three multiplications for each iteration of the inner loop, and there is one additional addition for each iteration of the outer loop. The number of iterations of the inner loop can be deduced from the following table, which shows the values of i and j for which the inner loop is executed.

i	1				2				$\cdots$	$n-2$		$n-1$	n
j	2	3	$\cdots$	n	3	4	$\cdots$	n	$\cdots$	$n-1$	n	n	

$$\underbrace{\qquad\qquad}_{n-1} \quad \underbrace{\qquad\qquad}_{n-2} \quad \underbrace{\qquad}_{2} \quad \underbrace{\qquad}_{1}$$

Hence, by Theorem 4.2.2, the total number of iterations of the inner loop is $(n-1)+(n-2)+\cdots+2+1 = \dfrac{n(n-1)}{2}$. Because three multiplications are performed for each iteration of the inner loop, the number of operations that are performed when the inner loop is executed is $3\cdot\dfrac{n(n-1)}{2} = \frac{3}{2}(n^2-n) = \frac{3}{2}n^2 - \frac{3}{2}n$. Now an additional operation is performed each time the outer loop is executed, and because the outer loop is executed n times, this gives an additional n operations. Therefore, the total number of operations is $(\frac{3}{2}n^2 - \frac{3}{2}n) + n = \frac{3}{2}n^2 - \frac{1}{2}n$.

b. By the theorem on polynomial orders, $\frac{3}{2}n^2 - \frac{1}{2}n$ is $\Theta(n^2)$, and so the algorithm segment has order n^2.

16. *a.* There are two additions, one subtraction, and one multiplication, for a total of four elementary operations, for each iteration of the inner loop, and there is one additional multiplication for each iteration of the outer loop. The number of iterations of the inner loop can be deduced from the following table, which shows the values of i and j for which the inner loop is executed.

i	1	2		3		4			$\cdots$	n			
j		1		1	2	1	2	3	$\cdots$	1	2	$\cdots$	$n-1$

$$\underbrace{\qquad}_{1} \quad \underbrace{\qquad}_{2} \quad \underbrace{\qquad\qquad}_{3} \quad \underbrace{\qquad\qquad\qquad}_{n-1}$$

Hence, by Theorem 4.2.2, the total number of iterations of the inner loop is $1+2+3+\cdots+(n-1) = \frac{n(n-1)}{2}$. Because four elementary operations are performed for each iteration of the inner loop, the number of operations that are performed when the inner loop is executed is $4\cdot\frac{n(n-1)}{2} = 2n(n-1) = 2n^2 - 2n$. Now an additional operation is performed each time the outer loop is executed, and because the outer loop is executed n times, this gives an additional n operations. Therefore, the total number of operations is $2n^2 - 2n + n = 2n^2 - n$.

b. By the theorem on polynomial orders, $2n^2 - n$ is $\Theta(n^2)$, and so the algorithm segment has order n^2.

18. *a.* There are n iterations of the inner loop for each iteration of the middle loop; there are $2n$ iterations of the middle loop for each iteration of the outer loop; and there are n iterations of the outer loop. Therefore, by the multiplication rule, there are $n\cdot 2n\cdot n = 2n^3$ iterations of the inner loop. Because there are two multiplications for each iteration of the inner loop, the total number of elementary operations that must be performed when the algorithm is executed is $2\cdot(2n^3) = 4n^3$.

b. By the theorem on polynomial orders, $4n^3$ is $\Theta(n^3)$, and so the algorithm segment has order n^3.

19. *a.* By the method of Example 6.5.4, the number of iterations of the inner loop is $\dfrac{n(n+1)(n+2)}{6}$. Because there are two elementary operations (multiplications) for each iteration of the inner loop, the total number of elementary operations that must be performed when the algorithm is executed is $2\left(\dfrac{n(n+1)(n+2)}{6}\right) = \dfrac{n(n+1)(n+2)}{3} = \frac{1}{3}n^3 + n^2 + \frac{2}{3}n$.

b. By the theorem on polynomial orders, $\frac{1}{3}n^3 + n^2 + \frac{2}{3}n$ is $\Theta(n^3)$, and so the algorithm segment has order n^3.

21.

	$a[1]$	$a[2]$	$a[3]$	$a[4]$	$a[5]$
initial order	7	3	6	9	5
result of step 1	3	7	6	9	5
result of step 2	3	6	7	9	5
result of step 3	3	6	7	9	5
result of step 4	3	5	6	7	9

23.

n	5									
$a[1]$	7		3							
$a[2]$	3	7			6					5
$a[3]$	6			7					5	6
$a[4]$	9						5	7		
$a[5]$	5					9				
k		2		3		4	5			
x		3		6		9	5			
j		1	0	2	1	3	4	3	2	1

25. *Solution 1*: The answer is 8, the same as the number of distinct nonzero values of j.

Solution 2: There is one such comparison in step 1, 2 in step 2, 1 in step 3, and 4 in step 4, for a total of 8.

26. One such array is $a[1] = 5$, $a[2] = 4$, $a[3] = 3$, $a[4] = 2$, $a[5] = 1$.

27. *a.*

$$
\begin{aligned}
E_1 &= 0 \\
E_2 &= E_1 + 2 + 1 = 3 \\
E_3 &= E_2 + 3 + 1 = 3 + 4 \\
E_4 &= E_3 + 4 + 1 = 3 + 4 + 5 \\
E_5 &= E_4 + 5 + 1 = 3 + 4 + 5 + 6 \\
&\quad\vdots
\end{aligned}
$$

Guess:
$$
\begin{aligned}
E_n &= 3 + 4 + 5 + \cdots + (n+1) = [1 + 2 + 3 + 4 + 5 + \cdots + (n+1)] - (1+2) \\
&= \frac{(n+1)(n+2)}{2} - 3 = \frac{n^2 + 3n + 2 - 6}{2} = \frac{n^2 + 3n - 4}{2}
\end{aligned}
$$

b. Proof by mathematical induction: Let $E_1, E_2, E_3, \ldots$ be a sequence that satisfies the recurrence relation $E_k = E_{k-1} + k + 1$ for all integers $k \geq 2$, with initial condition $E_1 = 0$, and let the property $P(n)$ be the equation $E_n = \dfrac{n^2 + 3n - 4}{2}$.

Show that the property is true for $n = 1$: For $n = 1$ the equation is $E_1 = \dfrac{1^2 + 3 \cdot 1 - 4}{2} = 0$, which is true.

Show that for all integers $k \geq 1$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let k be an integer with $k \geq 1$, and suppose that $E_k = \dfrac{k^2 + 3k - 4}{2}$. *[This is the inductive hypothesis.]* We must show that $E_{k+1} = \dfrac{(k+1)^2 + 3(k+1) - 4}{2}$. But the left-hand side of this equation equals

$$
\begin{aligned}
E_{k+1} &= E_k + (k+1) + 1 && \text{by definition of } E_1, E_2, E_3, \ldots \\
&= \frac{k^2 + 3k - 4}{2} + (k+1) + 1 && \text{by inductive hypothesis} \\
&= \frac{k^2 + 3k - 4 + 2k + 4}{2} \\
&= \frac{k^2 + 5k}{2}.
\end{aligned}
$$

And the right-hand side of the equation equals

$$
\frac{(k+1)^2 + 3(k+1) - 4}{2} = \frac{k^2 + 2k + 1 + 3k + 3 - 4}{2} = \frac{k^2 + 5k}{2}
$$

also.

[This is what was to be shown.]

29. The top row of the table below shows the initial values of the array, and the bottom row shows the final values. The result of each interchange is shown in a separate row.

$a[1]$	$a[2]$	$a[3]$	$a[4]$	$a[5]$
6	4	5	8	1
4	6	5	8	1
1	6	5	8	4
1	5	6	8	4
1	4	6	8	5
1	4	5	8	6
1	4	5	6	8

31.

n	5												
$a[1]$	6	4			1								
$a[2]$	4	6					5		4				
$a[3]$	5						6				5		
$a[4]$	8												6
$a[5]$	1				4				5		6		8
k	1				2				3		4		
i	2	3	4	5		3	4	5		4	5		5
$temp$	6			4		6		5			6		8

33. There is one comparison for each combination of values of k and i in the trace table for exercise 31. This gives a total of 10.

34. There are 3 comparisons of $a[1]$ with $a[2]$, $a[3]$, and $a[4]$, 2 comparisons of $a[2]$ with $a[3]$, and $a[4]$, and 1 comparison of $a[3]$ with $a[4]$. This gives a total of 6 comparisons.

35. *a.* $n - 1$

c. $n - (k+1) + 1 = n - k$

d. When $a[1]$ is compared to $a[2], a[3], \ldots, a[n]$, there are $n - 1$ comparisons. When $a[2]$ is compared to $a[3], a[4], \ldots, a[n]$, there are $n - 2$ comparisons. And so forth. In the second-to-last step, there are two comparisons: $a[n-2]$ is compared to $a[n-1]$ and $a[n]$. And in the final step, there is just one comparison: $a[n-1]$ is compared to $a[n]$. Therefore, the total number of comparisons is

$$
\begin{aligned}
(n-1) + (n-2) + \cdots + 2 + 1 &= \frac{(n-1)[(n-1)+1]}{2} && \text{by Theorem 4.2.2} \\
&= \frac{n(n-1)}{2} \\
&= \frac{1}{2}n^2 + \frac{1}{2}n.
\end{aligned}
$$

But $\frac{1}{2}n^2 + \frac{1}{2}n$ is $\Theta(n^2)$ by the theorem on polynomial orders. So selection sort has order n^2.

37.

n	2					
$a[0]$	5					
$a[1]$	-1					
$a[2]$	2					
x	3					
$polyval$	5		2			20
i	1		2			
$term$	-1	-3	2	6	18	
j	1		1	2		

39. By the result of exercise 38, $s_n = \frac{1}{2}n^2 + \frac{3}{2}n$, which is $\Theta(n^2)$ by the theorem on polynomial orders.

41.

n	2		
$a[0]$	5		
$a[1]$	-1		
$a[2]$	2		
x	3		
$polyval$	2	5	20
i	1	2	

42. There are two operations (one addition and one multiplication) per iteration of the loop, and there are n iterations of the loop. Therefore, $t_n = 2n$.

43. By the result of exercise 42, $t_n = 2n$. So, by the theorem on polynomial orders, the order of Algorithm 9.3.4 (Horner's rule) is $\Theta(n)$. By the result of exercise 39, the order of Algorithm 9.3.3 (term-by-term polynomial evaluation) is $\Theta(n^2)$. Thus Horner's rule is more efficient than term-by-term polynomial evaluation.

Section 9.4

2.

x	$g(x) = (1/3)^x$
0	1
1	1/3
2	1/9
-1	3
-2	9
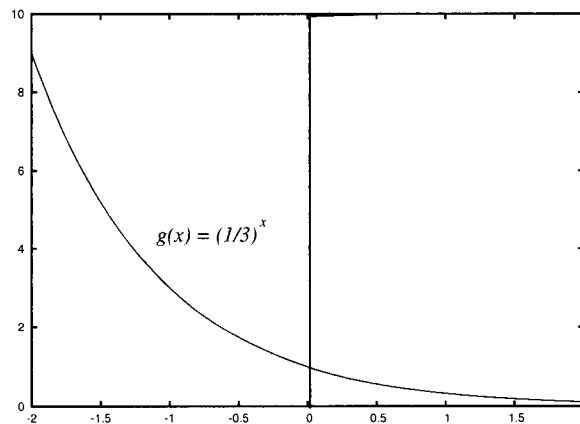
4.

x	$k(x) = \log_2(x)$
1	0
2	1
4	2
8	3
$1/2$	-1
$1/4$	-2
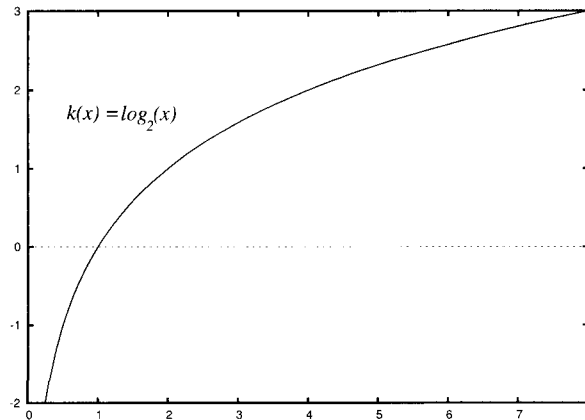
6.

x	$\lceil \log_2 x \rceil$
$1 < x \leq 2$	1
$2 < x \leq 4$	2
$4 < x \leq 8$	3
$1/2 < x \leq 0$	0
$1/4 < x \leq 1/8$	-1
$1/8 < x \leq 1/4$	-2
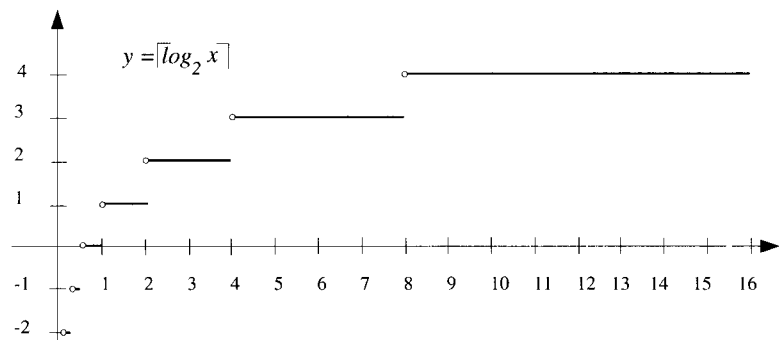
8.

x	$K(x) = x\log_{10}x$
1	0
2	$\sim.6$
3	~1.43
4	~2.4
$1/10$	$-1/10$
$1/100$	$-1/50$
$1/1000$	$-3/1000$
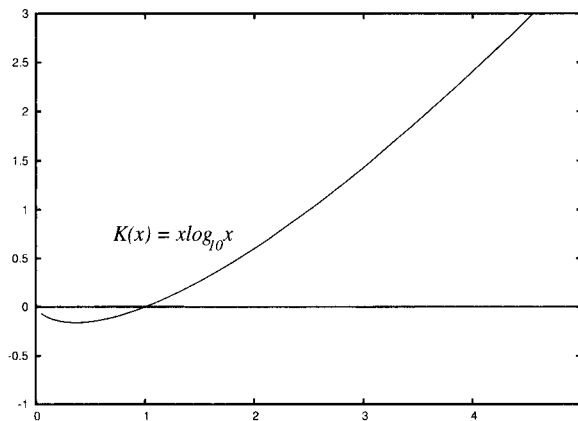
10. *a. Solution 1:* Let b be any positive real number not equal to 1. By definition of logarithm with base b, for any real number x, $\log_b(b^x)$ is the exponent to which b must be raised to obtain b^x. But this exponent is x. So $\log_b(b^x) = x$.

Solution 2: Let $\log_b(b^x) = y$. By definition of logarithm, $b^y = b^x$. It follows from property (7.2.5) that $y = x$. So $\log_b(b^x) = x$.

c. Let $f: \mathbf{R} \to \mathbf{R}^+$ be the exponential function with base b: $f(x) = \exp_b(x) = b^x$ for all real numbers x. Let $g: \mathbf{R}^+ \to \mathbf{R}$ be the logarithmic function with base $b \neq 1$: $g(x) = \log_b(x)$ for all positive real numbers x. Then for all $x \in \mathbf{R}$, $(g \circ f)(x) = g(f(x)) = g(b^x) = \log_b(b^x) = x$

by part (a), and for all $x \in \mathbf{R}^+$, $(f \circ g)(x) = f(g(x)) = f(\log_b(x)) = b^{\log_b x} = x$ by part (b). So $f \circ g = i_{\mathbf{R}^+}$ and $g \circ f = i_{\mathbf{R}}$, and hence $g = \log_b$ and $f = \exp_b$ are inverse functions.

11. *a.* Suppose (u, v) lies on the graph of the logarithmic function with base b. Then by definition, $v = \log_b u$. But by definition of logarithm, this equation is equivalent to $b^v = u$. So (v, u) lies on the graph of the exponential function with base b.

c.
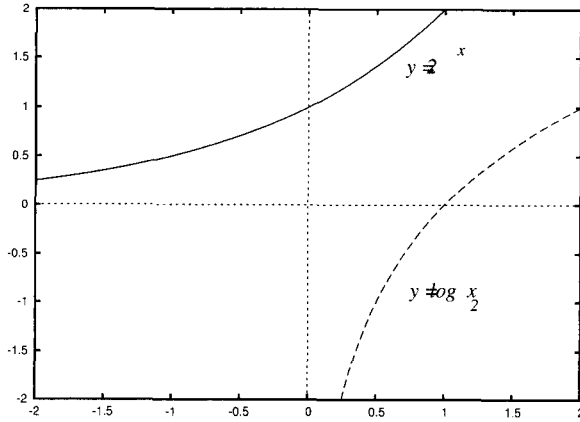
The graphs of $y = 2^x$ and $y = \log_2 x$ are symmetric about the line $y = x$. That is, if the two graphs are drawn on a piece of paper using the same scale on both axes and if the paper is folded along the line $y = x$, then the two graphs will coincide exactly.

12. When $\frac{1}{2} < x < 1$, then $-1 < \log_2 x < 0$.

When $\frac{1}{4} < x < \frac{1}{2}$, then $-2 < \log_2 x < -1$.

When $\frac{1}{8} < x < \frac{1}{4}$, then $-3 < \log_2 x < -2$.

And so forth.
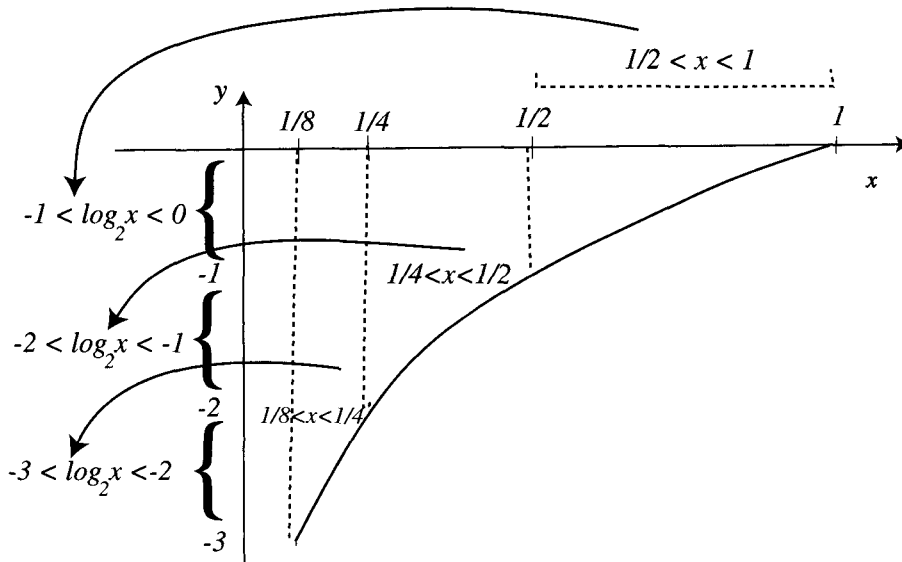
13. If $10^m \leq x < 10^{m+1}$, where m is an integer, then $m = \lfloor \log_{10} x \rfloor$.

Proof: Suppose that m is an integer and x is a real number with $10^m \leq x < 10^{m+1}$. Because the logarithmic function with base 10 is increasing, this inequality implies that

$$\log_{10}(10^m) \leq \log_{10} x < \log_{10}(10^{m+1}).$$

But by definition of logarithm, $\log_{10}(10^m) = m$ and $\log_{10}(10^{m+1}) = m + 1$. Hence

$$m \ \leq \ \log_{10} x \ < \ m + 1.$$

It follows by definition of floor that $m = \lfloor \log_{10} x \rfloor$.

14. *a.* *Proof*: Suppose n is a positive integer, k is a nonnegative integer, and $2^{k-1} < n \leq 2^k$. *[We must show that $\lceil \log_2 n \rceil = k$.]* Since the logarithm with base 2 is an increasing function, taking the logarithm with base 2 of all parts of this inequality preserves the directions of the inequality signs. Thus $\log_2(2^{k-1}) < \log_2(n) \leq \log_2(2^k)$. But by definition of logarithm, $\log_2(2^{k-1}) = k - 1$ and $\log_2(2^k) = k$. Hence $k - 1 < \log_2(n) \leq k$. Since $k - 1$ is an integer, by definition of ceiling, $\lceil \log_2 n \rceil = k$ *[as was to be shown]*.

b. If x is a positive number that lies between two consecutive integer powers of 2, the ceiling of the logarithm with base 2 of x is the exponent of the higher power of 2.

16. If n is an odd integer and $n > 1$, then $\lceil \log_2 n \rceil = \lceil \log_2(n + 1) \rceil$.

Proof: Suppose n is an odd integer and $n > 1$. Since n is odd, n is not an integer power of 2 and so n lies strictly between two successive integer powers of 2. In other words, there is an integer k such that $2^k < n < 2^{k+1}$. Consequently, $2^k < n + 1 \leq 2^{k+1}$. By exercise 14, then, $\lceil \log_2 n \rceil = k + 1$ and $\lceil \log_2(n + 1) \rceil = k + 1$ also. Hence $\lceil \log_2 n \rceil = \lceil \log_2(n + 1) \rceil$.

17. No. *Counterexample*: Let $n = 3$. Then $\lfloor \log_2(n + 1) \rfloor = \lfloor \log_2(4) \rfloor = 2$ whereas $\lfloor \log_2 n \rfloor = \lfloor \log_2 3 \rfloor = 1$.

19. $\lfloor \log_2(5,067,329) \rfloor + 1 = \lfloor 22.272\ldots \rfloor + 1 = 23$

20. No. If $\log_2 n$ is not an integer, then the two formulas give identical answers. But if $\log_2 n$ is an integer, then $\lfloor \log_2 n \rfloor + 1 = \log_2 n + 1 > \log_2 n = \lceil \log_2 n \rceil$. Consider $n = 4$ for instance. Since $4_{10} = 100_2$, three binary digits are needed to represent n. This agrees with the answer obtained from the formula $\lfloor \log_2 n \rfloor + 1 = \lfloor \log_2 4 \rfloor + 1 = 2 + 1 = 3$. On the other hand, $\lceil \log_2 n \rceil = \lceil \log_2 4 \rceil = \lceil 2 \rceil = 2$, which is too small.

22. *a.*

$$
\begin{aligned}
b_1 &= 1 \\
b_2 &= b_{\lceil 2/2 \rceil} + 1 = b_1 + 1 = 1 + 1 = 2 \\
b_3 &= b_{\lceil 3/2 \rceil} + 1 = b_2 + 1 = 2 + 1 = 3 \\
b_4 &= b_{\lceil 4/2 \rceil} + 1 = b_2 + 1 = 2 + 1 = 3 \\
b_5 &= b_{\lceil 5/2 \rceil} + 1 = b_3 + 1 = 3 + 1 = 4 \\
b_6 &= b_{\lceil 6/2 \rceil} + 1 = b_3 + 1 = 3 + 1 = 4 \\
b_7 &= b_{\lceil 7/2 \rceil} + 1 = b_4 + 1 = 3 + 1 = 4 \\
b_8 &= b_{\lceil 8/2 \rceil} + 1 = b_4 + 1 = 3 + 1 = 4 \\
b_9 &= b_{\lceil 9/2 \rceil} + 1 = b_5 + 1 = 4 + 1 = 5 \\
&\ \ \vdots \\
b_{16} &= b_{\lceil 16/2 \rceil} + 1 = b_8 + 1 = 4 + 1 = 5 \\
b_{17} &= b_{\lceil 17/2 \rceil} + 1 = b_9 + 1 = 5 + 1 = 6 \\
&\ \ \vdots \\
b_{32} &= b_{\lceil 32/2 \rceil} + 1 = b_{16} + 1 = 5 + 1 = 6
\end{aligned}
$$

Guess: b_n $=$ $\lceil \log_2 n \rceil + 1$

b. Proof (by strong mathematical induction): Let $b_1, b_2, b_3, \ldots$ be a sequence that satisfies the recurrence relation $b_k = b_{\lceil k/2 \rceil} + 1$ for all integers $k \geq 2$, with initial condition $b_1 = 1$, and let the property $P(n)$ be the equation $b_n = \lceil \log_2 n \rceil + 1$.

Show that the property is true for $n = 1$: For $n = 1$ the right-hand side of the equation is $\lceil \log_2 1 \rceil + 1 = 0 + 1 = 1$, which equals b_1.

Show that for all integers $k > 1$, if the property is true for all i with $1 \leq i < k$ then it is true for k: Let k be an integer with $k > 1$ and suppose $b_i = \lceil \log_2 i \rceil + 1$ for all integers i with $1 \leq i < k$. *[This is the inductive hypothesis.]* We must show that $b_k = \lceil \log_2 k \rceil + 1$. But

$$
\begin{aligned}
b_k &= b_{\lceil k/2 \rceil} + 1 && \text{by definition of } b_1, b_2, b_3, \ldots \\
&= (\lceil \log_2(\lceil k/2 \rceil) \rceil + 1) + 1 && \text{by inductive hypothesis} \\
&= \begin{cases} \lceil \log_2(k/2) \rceil + 2 & \text{if } k \text{ is even} \\ \lceil \log_2((k+1)/2) \rceil + 2 & \text{if } k \text{ is odd} \end{cases} && \begin{array}{l}\text{by definition of ceiling and} \\ \text{exercise 21 in Section 3.5}\end{array} \\
&= \begin{cases} \lceil \log_2 k - \log_2 2 \rceil + 2 & \text{if } k \text{ is even} \\ \lceil \log_2(k+1) - \log_2 2 \rceil + 2 & \text{if } k \text{ is odd} \end{cases} && \text{by exercise 29 in Section 7.2} \\
&= \begin{cases} \lceil \log_2 k - 1 \rceil + 2 & \text{if } k \text{ is even} \\ \lceil \log_2(k+1) - 1 \rceil + 2 & \text{if } k \text{ is odd} \end{cases} && \text{because } \log_2 2 = 1 \\
&= \begin{cases} \lceil \log_2 k \rceil - 1 + 2 & \text{if } k \text{ is even} \\ \lceil \log_2(k+1) \rceil - 1 + 2 & \text{if } k \text{ is odd} \end{cases} && \begin{array}{l}\text{by exercise 19 in Section 3.5} \\ \text{(with } x - 1 \text{ in place of } x)\end{array} \\
&= \begin{cases} \lceil \log_2 k \rceil + 1 & \text{if } k \text{ is even} \\ \lceil \log_2(k+1) \rceil + 1 & \text{if } k \text{ is odd} \end{cases} && \\
&= \lceil \log_2 k \rceil + 1 && \text{by exercise 16.}
\end{aligned}
$$

[This is what was to be shown.]

23. **Proof (by strong mathematical induction)**: Let $c_1, c_2, c_3, \ldots$ be a sequence that satisfies the recurrence relation $c_k = 2c_{\lfloor k/2 \rfloor} + k$ for all integers $k \geq 2$, with initial condition $c_1 = 0$, and let the property $P(n)$ be the inequality $c_n \leq n^2$.

Show that the property is true for $n = 1$: For $n = 1$ the inequality states that $c_1 \leq 1^2$, which is true because $c_1 = 0$.

Show that for all integers $k > 1$, if the property is true for all i with $1 \leq i < k$ then it is true for k: Let k be an integer with $k > 1$ and suppose $c_i \leq i^2$ for all integers i with $1 \leq i < k$. *[This is the inductive hypothesis.]* We must show that $c_k \leq k^2$. First note that because k is an integer with $k > 1$, $2 \leq k$. Thus $1 \leq \dfrac{k}{2} < \dfrac{k}{2} + \dfrac{k}{2} = k$, and so $1 \leq \left\lfloor \dfrac{k}{2} \right\rfloor < k$. Also note that $\lfloor k/2 \rfloor \leq k/2$ by definition of floor. Then

$$
\begin{aligned}
c_k &= 2c_{\lfloor k/2 \rfloor} + k && \text{by definition of } c_1, c_2, c_3, \ldots \\
\Rightarrow c_k &\leq 2(\lfloor k/2 \rfloor^2) + k && \text{by inductive hypothesis} \\
\Rightarrow c_k &\leq 2(k/2)^2 + k && \text{because } \lfloor k/2 \rfloor \leq k/2 \text{ and so } \lfloor k/2 \rfloor^2 \leq (k/2)^2 \\
\Rightarrow c_k &\leq k^2/2 + k^2/2 && \begin{array}{l}\text{because } 2(k/2)^2 = k^2/2, \text{ and since} \\ k \geq 2, \text{ then } k^2 \geq 2k \text{ and so } k^2/2 \geq k\end{array} \\
\Rightarrow c_k &\leq k^2 && \text{by algebra.}
\end{aligned}
$$

[This is what was to be shown.]

24. **Proof (by strong mathematical induction)**: Let $c_1, c_2, c_3, \ldots$ be a sequence that satisfies the recurrence relation $c_k = 2c_{\lfloor k/2 \rfloor} + k$ for all integers $k \geq 2$, with initial condition $c_1 = 0$, and let the property $P(n)$ be the inequality $c_n \leq n \log_2 n$.

Show that the property is true for $n = 1$: For $n = 1$ the inequality states that $c_1 \leq 1 \cdot \log_2 1 = 1 \cdot 0 = 0$, which is true because $c_1 = 0$.

Show that for all integers $k \geq 1$, if the property is true for all i with $1 \leq i < k$ then it is true for k: Let k be an integer with $k > 1$ and suppose $c_i \leq i \log_2 i$ for all integers i with $1 \leq i < k$. *[This is the inductive hypothesis.]* We must show that $c_k \leq k \log_2 k$. First note that because k is an integer with $k > 1$, $2 \leq k$. Thus $1 \leq \dfrac{k}{2} < \dfrac{k}{2} + \dfrac{k}{2} = k$, and so $1 \leq \left\lfloor \dfrac{k}{2} \right\rfloor < k$. Also note that $\lfloor k/2 \rfloor \leq k/2$ by definition of floor. Then

$$
\begin{aligned}
c_k &= 2c_{\lfloor k/2 \rfloor} + k && \text{by definition of } c_1, c_2, c_3, \dots \\[4pt]
\Rightarrow c_k &\leq 2(\lfloor k/2 \rfloor) \log_2 \lfloor k/2 \rfloor) + k && \text{by inductive hypothesis} \\[4pt]
\Rightarrow c_k &\leq 2[k \log_2(k/2)] + k && \text{because (1) } \lfloor k/2 \rfloor < k, \text{ and (2) since } 1 \leq \lfloor k/2 \rfloor \leq k/2, \\
& && \text{we have by property (9.4.1) that } \log_2 \lfloor k/2 \rfloor \leq \log_2(k/2) \\[4pt]
\Rightarrow c_k &\leq k(\log_2 k - \log_2 2) + k && \text{by algebra and exercise 29 in Section 7.2} \\[4pt]
\Rightarrow c_k &\leq k(\log_2 k - 1) + k && \text{because } \log_2 2 = 1 \\[4pt]
\Rightarrow c_k &\leq k \log_2 k && \text{by algebra,}
\end{aligned}
$$

[as was to be shown].

26. With some computer graphing programs (but not most graphing calculators) it is possible to find an approximate value for the point of intersection of $y = 2^x$ and $y = x^{50}$ by making the viewing window include very large values of y. However, because the values of 2^x and of x^{50} are so large in the region where the two are equal, probably the easiest way to solve this problem is to use logarithms. Note that because the logarithmic function with base 2 is increasing, $2^x > x^{50} \Leftrightarrow \log_2(2^x) > \log_2(x^{50}) \Leftrightarrow x > 50 \log_2 x$. By computing values of x and of $50 \log_2 x$ for various values of x or by using a graphing calculator or computer graphing program to graph $y = x$ and $y = 50 \log_2 x$, one finds that the given inequality holds for values of x greater than approximately 438.884. So one answer would be $x = 440$.

   Another approach would involve numerical exploration using properties of exponents. For instance, if $x = 2^9$, then $2^x = 2^{(2^9)} = 2^{512}$ whereas $x^{50} = (2^9)^{50} = 2^{450}$. So $x = 2^9 = 512$ would be another possible answer.

28. The values of x for which $x = 1.0001^x$ are approximately 1.00010001 and 116677.5257. Furthermore, $x > 1.0001^x$ on the approximate interval $1.0001001 < x < 116677.5257$ and $x < 1.0001^x$ on the approximate intervals $1.0001 > x$ and $x > 116677.53$.

31. It is clear from the graphs of $y = \log_2 x$ and $y = x$ that $\log_2 x < x$ for all $x > 0$. Multiply both sides of $\log_2 x < x$ by $5x$ to obtain $5x \log_2 x < 5x \cdot x = 5x^2$. Add x^2 to both sides to obtain $x^2 + 5x \log_2 x < x^2 + 5x^2 = 6x^2$. If $x > 1$, then all quantities are positive, and so $|x^2 + 5x \log_2 x| < 6|x^2|$. Also, when $x > 1$, then $\log_2 x > 0$, and so $5x \log_2 x > 0$. Adding x^2 to both sides gives $x^2 + 5x \log_2 x > x^2$, and, because all quantities are positive, $|x^2 + 5x \log_2 x| > |x^2|$. Let $A = 1$, $B = 6$, and $k = 1$. Then $A|x^2| \leq |x^2 + 5x \log_2 x| \leq B|x^2|$ for all $x > k$, and hence, by definition of Θ-notation, $x^2 + 5x \log_2 x$ is $\Theta(x^2)$.

33. For all integers $n > 0$, $2^n \leq 2^{n+1} \leq 2 \cdot 2^n$. Thus, let $A = 1$, $B = 2$, and $k = 0$. Then $A \cdot 2^n \leq 2^{n+1} \leq B \cdot 2^n$ for all integers $n > k$, and so, by definition of Θ-notation, 2^{n+1} is $\Theta(2^n)$.

34. *Proof (by contradiction):* Suppose 4^n is $O(2^n)$. Then there exist a positive real number B and a nonnegative real number b such that $|4^n| \leq B \cdot |2^n|$ for all integers $n > b$. Because 4^n and 2^n are positive, we have $4^n \leq B \cdot 2^n$ for all integers $n > b$. Divide both sides by 2^n and simplify to obtain $\frac{4^n}{2^n} = \left(\frac{4}{2}\right)^n = 2^n \leq B$. Because the logarithmic function with base 2 is increasing, this inequality implies that $\log_2(2^n) \leq \log_2(B)$, or, equivalently, $n \leq \log_2(B)$ (because $\log_2(2^n)$ is the exponent to which 2 must be raised to obtain 2^n, and this is n). So let n be any integer with $n > \log_2(B)$. Because the exponential function with base 2 is increasing, this inequality

implies that $2^n > 2^{\log_2(B)} = B$ (because $\log_2(B)$ is the exponent to which 2 must be raised to obtain B, and so if 2 is raised to this exponent, the result is B). Thus $2^n \le B$ and $2^n > B$, which is a contradiction. Therefore the supposition is false, and 4^n is not $O(2^n)$.

36. By factoring out a 4 and using the formula for the sum of a geometric sequence (Theorem 4.2.3), we have that for all integers $n > 1$,

$$4 + 4^2 + 4^3 + \cdots + 4^n = 4(1 + 4 + 4^2 + \cdots + 4^{n-1})$$

$$= 4\left(\frac{4^{(n-1)+1} - 1}{4 - 1}\right) = \frac{4}{3}(4^n - 1) = \frac{4}{3} \cdot 4^n - \frac{4}{3} \le \frac{4}{3} \cdot 4^n.$$

Moreover, because $4 + 4^2 + 4^3 + \cdots + 4^{n-1} \ge 0$,

$$4^n \le 4 + 4^2 + 4^3 + \cdots + 4^{n-1} + 4^n.$$

So let $A = 1$, $B = 4/3$, and $k = 1$. Then, because all quantities are positive, $A \cdot |4^n| \le \left|4 + 4^2 + 4^3 + \cdots + 4^n\right| \le B \cdot |4^n|$ for all integers $n > k$, and so, by definition of Θ-notation, $4 + 4^2 + 4^3 + \cdots + 4^n$ is $\Theta(4^n)$.

37. By factoring out a 2, applying a law of exponents, and using the formula for the sum of a geometric sequence (Theorem 4.2.3), we have that for all integers $n > 1$,

$$2 + 2 \cdot 3^2 + 2 \cdot 3^4 + \cdots + 2 \cdot 3^{2n} = 2(1 + 3^2 + 3^{2 \cdot 2} + \cdots + 3^{2n})$$

$$= 2[1 + 3^2 + (3^2)^2 + \cdots + (3^2)^n] = 2(1 + 9 + 9^2 + \cdots + 9^n)$$

$$2\left(\frac{9^{n+1} - 1}{9 - 1}\right) = \frac{2}{8}(9^{n+1} - 1) = \frac{1}{4} \cdot 9 \cdot 9^n - \frac{1}{4} \le \frac{9}{4} \cdot 9^n = \frac{9}{4} \cdot (3^2)^n = \frac{9}{4} \cdot 3^{2n}.$$

Moreover, because $2 + 2 \cdot 3^2 + 2 \cdot 3^4 + \cdots + 2 \cdot 3^{2(n-1)} \ge 0$,

$$2 \cdot 3^{2n} \le 2 + 2 \cdot 3^2 + 2 \cdot 3^4 + \cdots + 2 \cdot 3^{2n}.$$

So let $A = 2$, $B = 9/4$, and $k = 1$. Then, because all quantities are positive, $A \cdot \left|3^{2n}\right| \le \left|2 + 2 \cdot 3^2 + 2 \cdot 3^4 + \cdots + 2 \cdot 3^{2n}\right| \le B \cdot \left|3^{2n}\right|$ for all integers $n > k$, and so, by definition of Θ-notation, $2 + 2 \cdot 3^2 + 2 \cdot 3^4 + \cdots + 2 \cdot 3^{2n}$ is $\Theta(3^{2n})$.

38. By factoring out $1/5$ and using the formula for the sum of a geometric sequence (Theorem 4.2.3), we have that for all integers $n > 1$,

$$\frac{1}{5} + \frac{4}{5^2} + \cdots + \frac{4^n}{5^{n+1}} = \frac{1}{5}\left(1 + \frac{4}{5} + \left(\frac{4}{5}\right)^2 + \cdots + \left(\frac{4}{5}\right)^{n+1}\right)$$

$$= \frac{1}{5}\left(\frac{\left(\frac{4}{5}\right)^{n+1} - 1}{\frac{4}{5} - 1}\right) = \frac{1}{5}\left(\frac{1 - \left(\frac{4}{5}\right)^{n+1}}{\frac{1}{5}}\right)$$

$$= 1 - \frac{4^{n+1}}{5^{n+1}} \le 1$$

Moreover, because $\frac{4}{5^2} + \cdots + \frac{4^n}{5^{n+1}} \ge 0$, then $\frac{1}{5} \le \frac{1}{5} + \frac{4}{5^2} + \cdots + \frac{4^n}{5^{n+1}}$.

So let $A = 1/5$, $B = 1$, and $k = 1$. Then, because all quantities are positive, $A \cdot |1| \le \left|\frac{1}{5} + \frac{4}{5^2} + \cdots + \frac{4^n}{5^{n+1}}\right| \le B \cdot |1|$ for all integers $n > k$, and so, by definition of Θ-notation, $\frac{1}{5} + \frac{4}{5^2} + \cdots + \frac{4^n}{5^{n+1}}$ is $\Theta(1)$.

40. By factoring out an n and using the formula for the sum of a geometric sequence (Theorem 4.2.3), we have that for all integers $n > 1$,

$$\frac{2n}{3} + \frac{2n}{3^2} + \cdots + \frac{2n}{3^n} = \frac{2n}{3}\left(1 + \frac{1}{3} + \left(\frac{1}{3}\right)^2 + \cdots + \left(\frac{1}{3}\right)^{n-1}\right)$$

$$= \frac{2n}{3}\left(\frac{\left(\frac{1}{3}\right)^n - 1}{\frac{1}{3} - 1}\right) = \frac{2n}{3}\left(\frac{1 - \left(\frac{1}{3}\right)^n}{1 - \frac{1}{3}}\right) = \frac{2n}{3}\left(\frac{1 - \frac{1^n}{3^n}}{\frac{2}{3}}\right) = \frac{n}{3}\left(\frac{3^n - 1}{3^{n-1}}\right)$$

$$= n\left(\frac{3^n - 1}{3^n}\right) = n\left(1 - \frac{1}{3^n}\right) \le n$$

Moreover, because $\frac{2n}{3^2} + \cdots + \frac{2n}{3^n} \ge 0$, then $\frac{2}{3}n = \frac{2n}{3} \le \frac{2n}{3} + \frac{2n}{3^2} + \cdots + \frac{2n}{3^n}$.

So let $A = 2/3$, $B = 1$, and $k = 1$. Then, because all quantities are positive, $A|n| \leq \left|\frac{2n}{3} + \frac{2n}{3^2} + \cdots + \frac{2n}{3^n}\right| \leq B|n|$ for all integers $n > k$, and so, by definition of Θ-notation, $\frac{2n}{3} + \frac{2n}{3^2} + \cdots + \frac{2n}{3^n}$ is $\Theta(n)$.

41. Let k_1 and k_2 be any positive integers. If $n > 2$, then $1 < \log_2 n$ because the logarithmic function with base 2 is increasing and $\log_2 2 = 1$. Multiplying both sides of $1 < \log_2 n$ by $k_1 n$ (which is positive) gives $k_1 n < k_1 n \log_2 n$. Adding $k_2 n \log_2 n$ to both sides gives $k_1 n + k_2 n \log_2 n < k_1 n \log_2 n + k_2 n \log_2 n = (k_1 + k_2)n \log_2 n$. When $n > 2$, all quantities are positive and we have $|k_1 n + k_2 n \log_2 n| \leq (k_1 + k_2)|n \log_2 n|$. Then, because k_1 and k_2 are positive and $n > 2$, $k_2 n \log_2 n < k_1 n + k_2 n \log_2 n$. Furthermore, because all quantities are positive, $k_2|n \log_2 n| \leq |k_1 n + k_2 n \log_2 n|$. Let $A = k_2$, $B = k_1 + k_2$ and $k = 2$. Then $A|n \log_2 n| \leq |k_1 n + k_2 n \log_2 n| \leq B|n \log_2 n|$ for all $n > k$, and thus, by definition of Θ-notation, $k_1 n + k_2 n \log_2 n$ is $\Theta(n \log_2 n)$.

42. $1 + \frac{1}{2} = \frac{3}{2}$, $1 + \frac{1}{2} + \frac{1}{3} = \frac{11}{6}$, $1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} = \frac{50}{24} = \frac{25}{12}$, $1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} = \frac{137}{60}$

44. By Example 9.4.7(c), $\ln n \leq 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} \leq 2 \ln n$ for all integers $n \geq 3$. But by property (7.2.7), $\log_2 n = \frac{\log_e n}{\log_e 2} = \frac{\ln n}{\ln 2}$, or, equivalently, $\ln n = (\ln 2)(\log_2 n)$. Substituting for $\ln n$ in the above inequality gives $(\ln 2)(\log_2 n) \leq 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} \leq 2(\ln 2)(\log_2 n)$, and, because all quantities are positive, $\ln 2 |\log_2 n| \leq \left|1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}\right| \leq 2 \ln 2 |\log_2 n|$ Let $A = \ln 2$, $B = 2 \ln 2$, and $k = 3$. Then

$$A|\log_2 n| \leq \left|1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}\right| \leq B|\log_2 n| \quad \text{for all integers } n > k.$$

So by definition of Θ-notation, $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$ is $\Theta(\log_2 n)$.

Note: The result for this exercise could be deduced from part (d) of Example 9.4.7 as follows: By Example 9.4.7(d), $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$ is $\Theta(\ln n)$. So by definition of Θ-notation, there exist positive real numbers A and B and a nonzero constant k such that

$$A|\ln n| \leq \left|1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}\right| \leq B|\ln n| \quad \text{for all integers } n > k.$$

By property (7.2.7), $\log_2 n = \frac{\log_e n}{\log_e 2} = \frac{\ln n}{\ln 2}$, or, equivalently, $\ln n = (\ln 2)(\log_2 n)$. Thus, by substitution,

$$A|(\ln 2)(\log_2 n)| \leq \left|1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}\right| \leq B|(\ln 2)(\log_2 n)| \quad \text{for all integers } n > k,$$

or, equivalently,

$$A \ln 2 |\log_2 n| \leq \left|1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}\right| \leq B \ln 2 |\log_2 n| \quad \text{for all integers } n > k,$$

Let $A' = A \ln 2$ and $B' = B \ln 2$. Then both A' and B' are positive, and

$$A'|\log_2 n| \leq \left|1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}\right| \leq B'|\log_2 n| \quad \text{for all integers } n > k.$$

Hence, by definition of Θ-notation, $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$ is $\Theta(\log_2 n)$.

45. *a. Proof*: If n is any positive integer, then $\log_2 n$ is defined and by definition of floor, $\lfloor \log_2 n \rfloor \leq \log_2 n < \lfloor \log_2 n \rfloor + 1$. If, in addition, n is greater than 2, then since the logarithmic function with base 2 is increasing $\log_2 n > \log_2 2 = 1$. Thus, by definition of floor, $1 \leq \lfloor \log_2 n \rfloor$. Adding $\lfloor \log_2 n \rfloor$ to both sides of this inequality gives $\lfloor \log_2 n \rfloor + 1 \leq 2 \lfloor \log_2 n \rfloor$. Hence, by the transitive

property of order (T17 in Appendix B), $\log_2 n \leq 2 \lfloor \log_2 n \rfloor$, and dividing both sides by 2 gives $\frac{1}{2} \log_2 n \leq \lfloor \log_2 n \rfloor$. Let $A = 1/2$, $B = 1$, and $k = 2$. Then $A \log_2 n \leq \lfloor \log_2 n \rfloor \leq B \log_2 n$ for all integers $n > k$, and, because $\log_2 n$ is positive for $n > 2$, we may write $A |\log_2 n| \leq |\lfloor \log_2 n \rfloor| \leq B |\log_2 n|$ for all integers $n > k$. Therefore, by definition of Θ-notation, $\lfloor \log_2 n \rfloor$ is $\Theta(\log_2 n)$.

b. Proof: If n is any positive real number, then $\log_2 n$ is defined and by definition of floor, $\lfloor \log_2 n \rfloor \leq \log_2 n$. If, in addition, n is greater than 2, then, as in part (a), $\log_2 n < \lfloor \log_2 n \rfloor + 1$ and $\lfloor \log_2 n \rfloor + 1 \leq 2 \log_2 n$. Hence, because $\log_2 n$ is positive for $n > 2$, we may write $|\log_2 n| \leq |\lfloor \log_2 n \rfloor + 1| \leq 2 |\log_2 n|$. Let $A = 1$, $B = 2$ and $k = 2$. Then $A |\log_2 n| \leq |\lfloor \log_2 n \rfloor + 1| \leq B |\log_2 n|$ for all integers $n > k$. Therefore, by definition of Θ-notation, $\lfloor \log_2 n \rfloor + 1$ is $\Theta(\log_2 n)$.

47. *Proof by mathematical induction:* Let the property $P(n)$ be the inequality $\log_2 n \leq n$.

   Show that the property is true for $n = 1$: For $n = 1$ the property is true because the left-hand side of the inequality is $\log_2 1 = 0$ and the right-hand side equals 1.

   Show that for all integers $k \geq 1$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let k be an integer with $k \geq 1$, and suppose that $\log_2 k \leq k$. *[This is the inductive hypothesis.]* We must show that $\log_2(k + 1) \leq k + 1$. But when $1 \leq k$, we can add k to both sides to obtain $k + 1 \leq 2k$. Then, because the logarithmic function with base 2 is increasing, when we apply $\log_2$ to both sides of the inequality, we obtain $\log_2(k + 1) \leq \log_2(2k) = \log_2 2 + \log_2 k$ *[by exercise 30, Section 7.2]* $= 1 + \log_2 k$ *[because $\log_2 2 = 1$].* But, by inductive hypothesis, $\log_2 k \leq k$, and so, $1 + \log_2 k \leq 1 + k = k + 1$. Hence, by the transitive property of order (T17 in Appendix B), $\log_2(k + 1) \leq k + 1$ *[as was to be shown].*

48. *Proof:* Suppose n is a variable that takes positive integer values. Then whenever $n \geq 2$,

$$2^n = \underbrace{2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdots 2}_{n \text{ factors}} \leq \underbrace{2 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdots n}_{n \text{ factors}} \leq 2n!.$$

Let $B = 2$ and $b = 2$. Since 2^n and $n!$ are positive for all n, $|2^n| \leq B|n!|$ for all integers $n > b$. Hence by definition of O-notation 2^n is $O(n!)$.

49. *b.* By part (a), for all integers $n \geq 1$, $n! \leq n^n$. Because the logarithmic function with base 2 is increasing, we have $\log_2(n!) \leq \log_2(n^n) = n \log_2(n)$. Let $B = 1$ and $b = 1$. Then, because all quantities are positive, $|\log_2(n!)| \leq B|n \log_2(n)|$ for all $n > b$, and so by definition of O-notation $\log_2(n!)$ is $O(n \log_2 n)$.

   c. Proof: Suppose n is any nonnegative integer. Then for any integer r with $1 \leq r \leq n$, $n - r$ is positive. So we can multiply both sides of $r \geq 1$ by $n - r$ to obtain $r(n - r) \geq n - r$, or, equivalently, $rn - r^2 \geq n - r$. Adding r to both sides gives $rn - r^2 + r \geq n$, or, equivalently, $r(n - r + 1) \geq n$. It follows that $\prod_{r=1}^{n} r(n - r + 1) \geq \prod_{r=1}^{n} n = n^n$. But $\prod_{r=1}^{n} r(n - r + 1) = \left(\prod_{r=1}^{n} r \right) \left(\prod_{r=1}^{n} (n - r + 1) \right) = (1 \cdot 2 \cdot 3 \cdots (n - 1) \cdot n)(n \cdot (n - 1) \cdots 3 \cdot 2 \cdot 1) = (n!)(n!) = (n!)^2$. Hence, by the transitive property of order (T-17 in Appendix B), $(n!)^2 \geq n^n$.

   d. Proof: By part (c), for any integer $n \geq 1$, $(n!)^2 \geq n^n$. Because the logarithmic function with base 2 is increasing, we have $\log_2((n!)^2) \geq \log_2(n^n)$, and so, by exercise 31 from Section 7.2, $2 \log_2((n!)) \geq n \log_2(n)$. Dividing both sides by 2 gives $\log_2(n!) \geq \frac{1}{2} n \log_2(n)$. Let $A = \frac{1}{2}$ and $a = 1$. Then for all integers $n > a$, $\log_2(n!) \geq A n \log_2(n)$, and thus, because both sides of the inequality are positive, $|\log_2(n!)| \geq A |n \log_2(n)|$. Therefore, by definition of Ω-notation, $\log_2(n!)$ is $\Omega(n \log_2(n))$.

   e. It follows immediately from parts (b) and (d) and Theorem 9.2.1(1) that $\log_2(n!)$ is $\Theta(n \log_2(n))$.

51. *a.* Let n be any positive integer. Then for any real number x *[because $u < 2^u$ for all real numbers u]*,

$$x/n < 2^{x/n} \quad \Rightarrow \quad x < n2^{x/n} \quad \Rightarrow \quad x^n < (n2^{x/n})^n = n^n \cdot 2^x.$$

So $x^n < n^n 2^x$.

b. Let x be any positive real number and let n be any positive integer. Then $x^n = |x^n|$ and $n^n 2^x = 2^x |n^n|$, and thus the result of part (a) may be written as $|x^n| \leq 2^x |n^n|$. Let $B = 2^x$ and $b = 0$. Then $|x^n| \leq B |n^n|$ for all integers $n > b$, and so by definition of O-notation x^n is $O(n^n)$.

53. Let n be any positive integer and x a real number with $x > (2n)^{2n}$. By exercise 52, $\log_2 x < x^{1/n}$ for all positive integers n. But if $n \geq 2$, then $x^{1/n} < x^{1/2}$ (by property (9.2.1)). So, in particular,

$$\log_2 x < x^{1/2}.$$

But since $x > (2n)^{2n}$, then by properties of inequalities and exercise 20 of Section 9.1,

$$x > n^2 \quad \Rightarrow \quad \sqrt{x} > n \quad \Rightarrow \quad \frac{1}{n}\sqrt{x} > 1 \quad \Rightarrow \quad \frac{1}{n}\sqrt{x} \cdot \sqrt{x} > 1 \cdot \sqrt{x} \quad \Rightarrow \quad \frac{1}{n}x > x^{1/2}.$$

Putting the inequalities $\log_2 x < x^{1/2}$ and $x^{1/2} < \frac{1}{n}x$ together gives

$$\log_2 x < \frac{1}{n}x.$$

Applying the exponential function with base 2 to both sides results in

$$2^{\log_2 x} < 2^{\frac{1}{n}x} \quad \Rightarrow \quad x < (2^x)^{1/n} \quad \Rightarrow \quad x^n < 2^x.$$

55. *a.* Let b be a real number with $b > 1$, and let n be any integer with $n \geq 1$. By L'Hôpital's rule,

$$\lim_{x \to \infty} \frac{\log_b x}{x^{1/n}} = \lim_{x \to \infty} \frac{\dfrac{\ln x}{\ln b}}{x^{1/n}} = \lim_{x \to \infty} \frac{\dfrac{1}{x \ln b}}{\dfrac{1}{n} x^{1/n \, - \, 1}}$$

$$= \frac{n}{\ln b} \lim_{x \to \infty} \frac{\dfrac{1}{x}}{(x^{1/n})\dfrac{1}{x}} = \frac{n}{\ln b} \lim_{x \to \infty} \frac{1}{x^{1/n}} = \frac{n}{\ln b} \cdot 0 = 0.$$

b. By the result of part (a) and the definition of limit, given any real number ε, say $\varepsilon = 1$, there exists a real number N so that

$$\left| \frac{\log_b x}{x^{1/n}} - 0 \right| < \varepsilon = 1 \quad \text{for all } x > N.$$

It follows that

$$|\log_b x| < |x^{1/n}| \quad \text{for all } x > N.$$

Let $B = 1$ and $b' = N$. Then

$$|\log_b x| < B|x^{1/n}| \quad \text{for all } x > b',$$

and so by definition of O-notation, $\log_b x$ is $O(x^{1/n})$.

Section 9.5

2. *b.* If $m = 2^k$, where k is a positive integer, then the algorithm requires $c\lfloor \log_2(2^k) \rfloor = c\lfloor k \rfloor = ck$ operations. If the input size is increased to $m^{10} = (2^k)^{10} = 2^{10k}$, then the number of operations required is $c\lfloor \log_2(2^{10k}) \rfloor = c\lfloor 10k \rfloor = c \cdot 10k = 10 \cdot ck$. So the number of operations increases by a factor of 10.

c. When the input size is increased from 2^7 to 2^{28}, the factor by which the number of operations increases is $\dfrac{c\lfloor \log_2(2^{28}) \rfloor}{c\lfloor \log_2(2^7) \rfloor} = \dfrac{28c}{7c} = 4$.

4. To answer this question, we need to find where the graph of $y = \lfloor n^2/10 \rfloor$ crosses the graph of $y = \lfloor n \log_2 n \rfloor$. A little numerical exploration reveals that when $n = 20$, $\lfloor n^2/10 \rfloor = 40$ whereas $\lfloor n \log_2 n \rfloor = 86$, and so for $n = 20$ $\lfloor n^2/10 \rfloor < \lfloor n \log_2 n \rfloor$. However, for $n = 100$, $\lfloor n^2/10 \rfloor = 1000$ whereas $\lfloor n \log_2 n \rfloor = 664$, and so for $n = 100$ $\lfloor n^2/10 \rfloor > \lfloor n \log_2 n \rfloor$. So to find the crossing point of the two graphs, we can use an initial window going from $n = 20$ to $n = 100$ and from $y = 40$ to $y = 1000$. Zooming in shows that the crossing point occurs at approximately $n = 58$. Indeed, for $n = 58$, $\lfloor n^2/10 \rfloor = 336 < 339 = \lfloor n \log_2 n \rfloor$, and for $n = 59$, $\lfloor n^2/10 \rfloor = 348 > 347 = \lfloor n \log_2 n \rfloor$. So if $n \leq 58$, an algorithm that requires $\lfloor n^2/10 \rfloor$ operations is more efficient than an algorithm that requires $\lfloor n \log_2 n \rfloor$ operations.

6. *a.*

index	0			
bot	1	1	1	1
top	10	4	1	0
mid		5	2	1

b.

index	0		8
bot	1	6	
top	10		
mid		5	8

7. *c.* Suppose there is an even number of elements in the array $a[bot], a[bot+1], \ldots, a[top]$. Then $top - bot + 1$ is an even number, and so $top - bot + 1 = 2k$ for some integer k. Solving for top gives $top = 2k + bot - 1$, and hence $bot + top = bot + (2k + bot - 1) = 2 \cdot bot + 2k - 2 + 1 = 2(bot + k - 1) + 1$, which is odd because $bot + k - 1$ is an integer.

12.

n	424	141	47	15	5	1	0

13. For each integer $k \geq 3$, $n \ div \ 3 = \lfloor k/3 \rfloor$. Thus when the algorithm segment is run for a particular k and the **while** loop has iterated one time, the input to the next iteration is $\lfloor k/3 \rfloor$. It follows that the number of iterations of the loop for k is one more than the number of iterations for $\lfloor k/3 \rfloor$. That is, $b_k = 1 + b_{\lfloor k/3 \rfloor}$ for all $k \geq 3$. Also $b_1 = 1$ and $b_2 = 1$ because $\lfloor 1/3 \rfloor = 0$ and $\lfloor 2/3 \rfloor = 0$, and so when k equals 1 or 2, the **while** loop iterates just one time.

14.

$$b_1 = 1$$
$$b_2 = 1$$

$$
\left.
\begin{aligned}
b_3 &= 1 + b_{\lfloor 3/3 \rfloor} = 1 + b_1 = 1 + 1 = 2 \\
b_4 &= 1 + b_{\lfloor 4/3 \rfloor} = 1 + b_1 = 1 + 1 = 2 \\
b_5 &= 1 + b_{\lfloor 5/3 \rfloor} = 1 + b_1 = 1 + 1 = 2 \\
b_6 &= 1 + b_{\lfloor 6/3 \rfloor} = 1 + b_2 = 1 + 1 = 2 \\
&\;\;\vdots \\
b_8 &= 1 + b_{\lfloor 8/3 \rfloor} = 1 + b_2 = 1 + 1 = 2
\end{aligned}
\right\}
$$

$$
\left.
\begin{aligned}
b_9 &= 1 + b_{\lfloor 9/3 \rfloor} = 1 + b_3 = 1 + 2 = 3 \\
&\;\;\vdots \\
b_{26} &= 1 + b_{\lfloor 26/3 \rfloor} = 1 + b_8 = 1 + 2 = 3
\end{aligned}
\right\}
$$

$$b_{27} = 1 + b_{\lfloor 27/3 \rfloor} = 1 + b_9 = 1 + 3 = 4$$

$$\vdots$$

Guess: If n satisfies the inequality $3^r \leq n < 3^{r+1}$ for some integer $r \geq 0$, then $b_n = 1 + r$. In this case $r \leq \log_3 n < r + 1$, and so $r = \lfloor \log_3 n \rfloor$ and the formula is $b_n = 1 + \lfloor \log_3 n \rfloor$ for all integers $n \geq 1$.

b. Proof: Suppose k is an integer and x is any real number with $3^k \leq x < 3^{k+1}$. Because the logarithmic function with base 3 is increasing, it follows that $\log_3(3^k) \leq \log_3(x) < \log_3(3^{k+1})$. But, by definition of logarithm, $\log_3(3^k) = k$ and $\log_3(3^{k+1}) = k + 1$. Thus $k \leq \log_3(x) < k + 1$, and so, by definition of floor, $\lfloor \log_3(x) \rfloor = k$.

c. Proof: Suppose m is an integer with $m \geq 1$. For some integer $a \geq 1$, $3^a \leq 3m < 3^{a+1}$. So since $3^{a+1} = 3 \cdot 3^a > 3^a + 3$ whenever $a \geq 1$,

$$3^a \;\leq\; 3m \;<\; 3m + 1 \;<\; 3m + 2 \;<\; 3^{a+1}.$$

Applying the logarithmic function with base 3 to all parts of these inequalities and using the fact that the logarithmic function with base 3 is increasing gives

$$\log_3(3^a) \;\leq\; \log_3(3m) \;<\; \log_3(3m + 1) \;<\; log_3(3m + 2) \;<\; log_3(3^{a+1}).$$

Since $\log_3(3^a) = a$ and $\log_3(3^{a+1}) = a + 1$,

$$a \;\leq\; \log_3(3m) \;<\; \log_3(3m + 1) \;<\; log_3(3m + 2) \;<\; a + 1.$$

So by definition of floor, $\lfloor \log_3(3m) \rfloor = \lfloor \log_3(3m + 1) \rfloor = \lfloor \log_3(3m + 2) \rfloor$.

d. Proof (by strong mathematical induction): Let $b_1, b_2, b_3, \ldots$ be a sequence that satisfies the recurrence relation $b_k = 1 + b_{\lfloor k/3 \rfloor}$ for all integers $k \geq 2$, with initial conditions $b_1 = 1$ and $b_2 = 1$, and let the property $P(n)$ be the equation $b_n = 1 + \lfloor \log_3 n \rfloor$.

Show that the property is true for $n = 1$ and $n = 2$: For $n = 1$ the equation states that $b_1 = 1 + \lfloor \log_3 1 \rfloor = 1 + 0 = 1$, which is true. For $n = 2$ the equation states that $b_2 = 1 + \lfloor \log_3 2 \rfloor = 1 + 0 = 1$, which is also true because $0 \leq \log_3 2 < 1$.

Show that for all integers $k > 2$, if the property is true for all i with $1 \leq i < k$ then it is true for k: Let k be an integer with $k > 2$ and suppose $b_i = 1 + \lfloor \log_3 i \rfloor$ for all integers i with $1 \leq i < k$. *[This is the inductive hypothesis.]* We must show that

$b_k = 1 + \lfloor \log_3 k \rfloor$. But by the quotient-remainder theorem with $d = 3$, $k = 3q + r$, where q and r are integers and $0 \le r < 3$. Note that $\lfloor k/3 \rfloor = \lfloor (3q+r)/3 \rfloor = \lfloor q + r/3 \rfloor = q$ [since $0 \le r < 3$] and that $q \ge 1$ [since k is positive]. Thus $1 \le q = \lfloor k/3 \rfloor \le k/3 < k$. It follows that

$$
\begin{aligned}
b_k &= 1 + b_{\lfloor k/3 \rfloor} && \text{by part (a)} \\
&= 1 + b_q && \text{because } q = \lfloor k/3 \rfloor \\
&= 1 + (1 + \lfloor \log_3 q \rfloor) && \text{by inductive hypothesis (since } q < k) \\
&= 1 + (\lfloor 1 + \log_3 q \rfloor) && \text{by Theorem 3.5.1.} \\
&= 1 + (\lfloor \log_3 3 + \log_3 q \rfloor) && \text{because } \log_3 3 = 1 \\
&= 1 + (\lfloor \log_3 3q \rfloor) && \text{by the result of exercise 30 in Section 7.2} \\
&= 1 + (\lfloor \log_3 k \rfloor) && \text{by part (c) (because } k = 3q + r \text{ where} \\
& && q \text{ and } r \text{ are integers and } 0 \le r < 3.
\end{aligned}
$$

[This is what was to be shown.]

15. If $n \ge 3$, then, by definition of floor, $\lfloor \log_3 n \rfloor \le \log_3 n < \lfloor \log_3 n \rfloor + 1$. Thus $b_n = 1 + \lfloor \log_3 n \rfloor \le 1 + \log_3 n$ *[by definition of floor]* $\le \log_3 n + \log_3 n$ *[because if $n \ge 3$ then $\log_3 n \ge 1$]* $= 2 \log_3 n$. Furthermore, because $\log_3 n \ge 0$ for $n > 2$, we may write $|\log_3 n| < |\lfloor \log_3 n \rfloor + 1| \le 2 |\log_3 n|$. Let $A = 1$, $B = 2$, and $k = 2$. Then all quantities are positive, and so $A|\log_3 n| < |\lfloor \log_3 n \rfloor + 1| \le B|\log_3 n|$ for all integers $n > k$. Hence by definition of Θ-notation, $b_n = 1 + \lfloor \log_3 n \rfloor$ is $\Theta(\log_3 n)$, and thus the algorithm segment has order $\log_3 n$.

16. Let $w_1, w_2, w_3 \ldots$ be defined as follows: $w_1 = 1$ and $w_k = 1 + w_{\lfloor k/2 \rfloor}$ for all integers $k > 1$. Let k be an even integer, and suppose $w_i = \lfloor \log_2 i \rfloor + 1$ for all integers i with $1 \le i < k$. *[This is the inductive hypothesis.]* *[We will show that $w_k = \lfloor \log_2 k \rfloor + 1$.]* Since k is even, $\lfloor k/2 \rfloor = k/2$. Then $w_k = 1 + w_{\lfloor k/2 \rfloor} = 1 + w_{k/2} = 1 + (\lfloor \log_2 (k/2) \rfloor + 1)$ *[by inductive hypothesis]* $= 1 + \lfloor \log_2 k - \log_2 2 \rfloor + 1)$ *[by exercise 29 of Section 7.2]* $= 1 + \lfloor \log_2 k - 1 \rfloor + 1)$ *[because $\log_2 2 = 1$]* $= 1 + (\lfloor \log_2 k \rfloor - 1 + 1)$ *[by exercise 15 of Section 3.5]* $= \lfloor \log_2 k \rfloor + 1$ *[as was to be shown]*.

17. *a.*

index	0				7
bot	1	7			
top	10		8	7	
mid		6	9	8	7

b.

index	0			
bot	1	7		9
top	10		8	
mid		6	9	8

18. Suppose an array of length k is input to the **while** loop and the loop is iterated one time. The elements of the array can be matched with the integers from 1 to k with $m = \left\lceil \dfrac{k+1}{2} \right\rceil$, as shown below:

	left subarray					right subarray		
$a[bot]$	$a[bot+1]$	$\ldots$	$a[mid-1]$	$a[mid]$	$a[mid+1]$	$\ldots$	$a[top-1]$	$a[top]$
$\updownarrow$	$\updownarrow$		$\updownarrow$	$\updownarrow$	$\updownarrow$		$\updownarrow$	$\updownarrow$
1	2		$m-1$	m	$m+1$		$k-1$	k
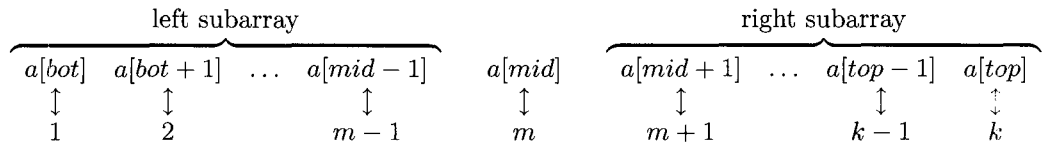
Case 1 (k is even): In this case $m = \left\lceil \dfrac{k+1}{2} \right\rceil = \left\lceil \dfrac{k}{2} + \dfrac{1}{2} \right\rceil = \dfrac{k}{2} + 1$, and so the number of elements in the left subarray equals $m - 1 = (\dfrac{k}{2}+1) - 1 = \dfrac{k}{2} = \left\lfloor \dfrac{k}{2} \right\rfloor$. The number of elements in the right subarray equals $k - (m+1) - 1 = k - m = k - (\dfrac{k}{2}+1) = \dfrac{k}{2} - 1 < \left\lfloor \dfrac{k}{2} \right\rfloor$. Hence both subarrays (and thus the new input array) have length at most $\left\lfloor \dfrac{k}{2} \right\rfloor$.

Case 2 (k is odd): In this case $m = \left\lceil \dfrac{k+1}{2} \right\rceil = \dfrac{k+1}{2}$, and so the number of elements in the left subarray equals $m - 1 = \dfrac{k+1}{2} - 1 = \dfrac{k-1}{2} = \left\lfloor \dfrac{k}{2} \right\rfloor$. The number of elements in the right subarray equals $k - m = k - \dfrac{k+1}{2} = \dfrac{k-1}{2} = \left\lfloor \dfrac{k}{2} \right\rfloor$ also. Hence both subarrays (and thus the new input array) have length $\left\lfloor \dfrac{k}{2} \right\rfloor$.

The arguments in cases 1 and 2 show that the length of the new input array to the next iteration of the **while** loop has length at most $\lfloor k/2 \rfloor$.

19. By exercise 18, given an input array of length k to the **while** loop of the modified binary search algorithm, the worst that can happen is that the next iteration of the loop will have to search an array of length $\lfloor k/2 \rfloor$. Hence the maximum number of iterations of the loop is one more than the maximum number necessary to execute it for an input array of length $\lfloor k/2 \rfloor$. Thus $w_k = 1 + w_{\lfloor k/2 \rfloor}$ for $k \geq 2$.

21.

23.

Initial Array `5 2 3 9 7 4 3 2`
split
`5 2 3 9`   `7 4 3 2`
split
`5 2` `3 9`   `7 4` `3 2`
split
`5` `2` `3` `9`   `7` `4` `3` `2`
merge
`2 5` `3 9`   `4 7` `2 3`
merge
`2 3 5 9`   `2 3 4 7`
merge
Final Array `2 2 3 3 4 5 7 9`
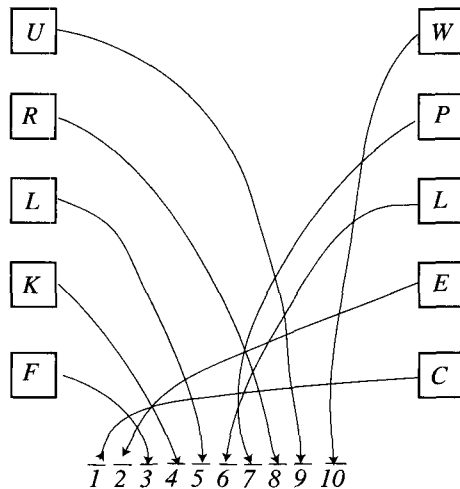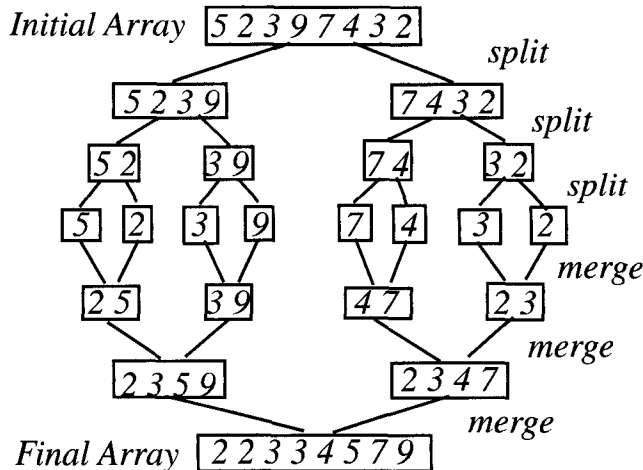
24. *a.* Refer to Figure 9.5.3. Observe that when k is odd, the subarray $a[mid+1], a[mid+2], \ldots a[top]$ has length $k - \left(\dfrac{k+1}{2} + 1\right) + 1 = \dfrac{k-1}{2} = \lfloor k/2 \rfloor$. And when k is even, the subarray $a[mid+1], a[mid+2], \ldots a[top]$ has length $k - \left(\dfrac{k}{2} + 1\right) + 1 = \dfrac{k}{2} = \lfloor k/2 \rfloor$. So in either case the subarray has length $\lfloor k/2 \rfloor$.

25. *a. Proof (by strong mathematical induction)*: Let $m_1, m_2, m_3, \ldots$ be a sequence that satisfies the recurrence relation $m_k = m_{\lfloor k/2 \rfloor} + m_{\lceil k/2 \rceil} + k - 1$ for all integers $k \geq 1$, with initial condition $m_1 = 0$, and let the property $P(n)$ be the inequality $\frac{1}{2} n \log_2 n \leq m_n$.

Show that the property is true for $n = 1$: For $n = 1$, the left-hand side of the inequality is $\frac{1}{2} \cdot 1 \cdot \log_2 1 = \frac{1}{2} \cdot 1 \cdot 0 = 0$ and the right-hand side is m_1, which also equals 0. So the inequality is true for $n = 1$.

Show that for all integers $k > 1$, if the property is true for all i with $1 \leq i < k$ then it is true for k: Let k be an integer with $k > 1$ and suppose that $m_i \leq 2i \log_2 i$ for all integers i with $1 \leq i < k$. *[This is the inductive hypothesis.]* We must show that $m_k \leq 2k \log_2 k$.

Case 1 (k is even): In this case,

$$
\begin{array}{rrll}
& m_k & = & m_{\lfloor k/2 \rfloor} + m_{\lceil k/2 \rceil} + k - 1 \quad \text{by definition of } m_1, m_2, m_3, \ldots \\
\Rightarrow & m_k & = & m_{k/2} + m_{k/2} + k - 1 \quad \text{because } k \text{ is even} \\
\Rightarrow & m_k & = & 2m_{k/2} + k - 1. \\
\Rightarrow & m_k & \geq & 2 \cdot \frac{1}{2} \cdot \frac{k}{2} \log_2 \left(\frac{k}{2}\right) + k - 1 \quad \text{by inductive hypothesis} \\
\Rightarrow & m_k & \geq & \frac{k}{2}(\log_2 k - \log_2 2) + k - 1 \quad \text{by exercise 29 of Section 7.2} \\
\Rightarrow & m_k & \geq & \frac{1}{2}k(\log_2 k - 1) + k - 1 \quad \text{because } \log_2 2 = 1 \\
\Rightarrow & m_k & \geq & \frac{1}{2}k \log_2 k - \frac{k}{2} + k - 1 \\
\Rightarrow & m_k & \geq & \frac{1}{2}k \log_2 k + \frac{k}{2} - 1 \\
\Rightarrow & m_k & \geq & \frac{1}{2}k \log_2 k + \frac{k-2}{2} \\
\Rightarrow & m_k & \geq & \frac{1}{2}k \log_2 k \quad \text{because when } k \geq 2 \text{ then } \frac{k-2}{2} \geq 0.
\end{array}
$$

Case 2 (k is odd): In this case, $k = 2q + 1$ for some integer q and $1 \le q$ (since $k \ge 2$). Then $k/2 = q + 1/2$, and so $\lfloor k/2 \rfloor = q$ and $\lceil k/2 \rceil = q + 1$, where $1 \le q < q + 1 < 2q + 1 = k$. It follows that

$$m_k = m_{\lfloor k/2 \rfloor} + m_{\lceil k/2 \rceil} + k - 1$$
by definition of $m_1, m_2, m_3, \ldots$

$$\Rightarrow \quad m_k = m_q + m_{q+1} + 2q$$
by substitution and by subtracting 1 from both sides of $k = 2q + 1$

$$\Rightarrow \quad m_k \ge \tfrac{1}{2}q\log_2(q) + \tfrac{1}{2}(q+1)\log_2(q+1) + 2q$$
by inductive hypothesis

$$\Rightarrow \quad m_k \ge \tfrac{1}{2}[q\log_2(q) + (q+1)\log_2(q+1) + 4q]$$
by factoring out 1/2

$$\Rightarrow \quad m_k \ge \tfrac{1}{2}[q\log_2(q) + 2q + (q+1)\log_2(q+1) + 2q]$$
because $4q = 2q + 2q$

$$\Rightarrow \quad m_k \ge \tfrac{1}{2}[q(\log_2(q) + 2) + (q+1)\log_2(q+1) + (q+1)]$$
by factoring out q and because $q \ge 1$ implies that $2q \ge q + 1$

$$\Rightarrow \quad m_k \ge \tfrac{1}{2}[q(\log_2(q) + 2) + (q+1)(\log_2(q+1) + 1)]$$
by factoring out $q + 1$

$$\Rightarrow \quad m_k \ge \tfrac{1}{2}[q(\log_2(q) + \log_2(4)) + (q+1)(\log_2(q+1) + \log_2(2))]$$
because $\log_2 4 = 2$ and $\log_2 2 = 1$

$$\Rightarrow \quad m_k \ge \tfrac{1}{2}[q\log_2(4q) + (q+1)\log_2(2q+2)]$$
by exercise 30 of Section 7.2

$$\Rightarrow \quad m_k \ge \tfrac{1}{2}[q\log_2(2q+1) + (q+1)\log_2(2q+1)]$$
by property (9.4.1) and because $q \ge 1$
implies that $2q + 1 < 2q + 2 \le 2q + 2q = 4q$

$$\Rightarrow \quad m_k \ge \tfrac{1}{2}[(2q+1)\log_2(2q+1)]$$
by factoring out $\log_2(2q+1)$

$$\Rightarrow \quad m_k \ge \tfrac{1}{2}k\log_2 k$$
because $k = 2q + 1$.

Cases 1 and 2 show that regardless of whether k is even or odd, $m_k \ge \tfrac{1}{2}k\log_2 k$ *[as was to be shown]*.

b. Proof (by strong mathematical induction): Let $m_1, m_2, m_3, \ldots$ be a sequence that satisfies the recurrence relation $m_k = m_{\lfloor k/2 \rfloor} + m_{\lceil k/2 \rceil} + k - 1$ for all integers $k \ge 1$, with initial condition $m_1 = 0$, and let the property $P(n)$ be the inequality $m_n \le 2n\log_2 n$.

Show that the property is true for $n = 1$: For $n = 1$ the left-hand side of the inequality is m_1, which equals 0, and the right-hand side is $2 \cdot 1 \cdot \log_2 1 = 2 \cdot 1 \cdot 0 = 0$ also. So the inequality is true for $n = 1$.

Show that for all integers $k > 1$, if the property is true for all i with $1 \le i < k$ then it is true for k: Let k be an integer with $k > 1$ and suppose that $m_i \le 2i\log_2 i$ for all integers i with $1 \le i < k$. *[This is the inductive hypothesis.]* We must show that $m_k \le 2k\log_2 k$.

Case 1 (k is even): In this case,

$$m_k = m_{\lfloor k/2 \rfloor} + m_{\lceil k/2 \rceil} + k - 1 \qquad \text{by definition of } m_1, m_2, m_3, \ldots$$
$$\Rightarrow \quad m_k = m_{k/2} + m_{k/2} + k - 1 \qquad \text{because } k \text{ is even}$$
$$\Rightarrow \quad m_k = 2m_{k/2} + k - 1.$$
$$\Rightarrow \quad m_k \le 2 \cdot 2 \cdot \frac{k}{2}\log_2\left(\frac{k}{2}\right) + k - 1 \qquad \text{by inductive hypothesis}$$
$$\Rightarrow \quad m_k \le 2k(\log_2 k - \log_2 2) + k - 1 \qquad \text{by exercise 29 of Section 7.2}$$
$$\Rightarrow \quad m_k \le 2k(\log_2 k - 1) + k - 1 \qquad \text{because } \log_2 2 = 1$$
$$\Rightarrow \quad m_k \le 2k\log_2 k - 1$$
$$\Rightarrow \quad m_k \le 2k\log_2 k.$$

Case 2 (k is odd): In this case, as in part (a), $k = 2q + 1$ for some integer q and $1 \leq q$ (since $k \geq 2$). Then $k/2 = q + 1/2$, and so $\lfloor k/2 \rfloor = q$ and $\lceil k/2 \rceil = q + 1$, where $1 \leq q < q + 1 < 2q + 1 = k$. It follows that

$$
\begin{aligned}
m_k &= m_{\lfloor k/2 \rfloor} + m_{\lceil k/2 \rceil} + k - 1 \\
&\qquad \text{by definition of } m_1, m_2, m_3, \ldots \\
\Rightarrow \quad m_k &= m_q + m_{q+1} + 2q \\
&\qquad \text{by substitution and by subtracting 1 from both sides of } k = 2q + 1 \\
\Rightarrow \quad m_k &\leq 2q \log_2(q) + 2(q+1) \log_2(q+1) + 2q \\
&\qquad \text{by inductive hypothesis} \\
\Rightarrow \quad m_k &\leq 2[q \log_2(q) + (q+1) \log_2(q+1) + q] \\
&\qquad \text{by factoring out 2} \\
\Rightarrow \quad m_k &\leq 2[q(\log_2(q) + 1) + (q+1) \log_2(q+1)] \\
&\qquad \text{by factoring out } q \\
\Rightarrow \quad m_k &\leq 2[q(\log_2(q) + \log_2(2)) + (q+1) \log_2(q+1)] \\
&\qquad \text{because } \log_2(2) = 1 \\
\Rightarrow \quad m_k &\leq 2[q(\log_2(2q)) + (q+1) \log_2(q+1)] \\
&\qquad \text{by exercise 30 of Section 7.2} \\
\Rightarrow \quad m_k &\leq 2[q(\log_2(k)) + (q+1) \log_2(k)] \\
&\qquad \text{because } q + 1 \leq q + q = 2q < k \text{ and because} \\
&\qquad \text{the logarithm function with base 2 is increasing} \\
\Rightarrow \quad m_k &\leq 2[(q + (q+1))(\log_2(k))] \\
&\qquad \text{by factoring out } \log_2(k) \\
\Rightarrow \quad m_k &\leq 2k \log_2 k \qquad \text{because } k = 2q + 1.
\end{aligned}
$$

Cases 1 and 2 show that regardless of whether k is even or odd, $m_k \leq 2k \log_2 k$ *[as was to be shown].*

26. Algorithm   Fast Computation of Integral Powers

[Given a real number x and a positive integer n, this algorithm computes x^n. It first calls Algorithm 4.1.1 to find the binary representation of n: $(r[k]r[k-1]\ldots r[1]r[0])_2$. Then it computes x^n using the fact that $x^n = x^{r[k]2^k} \cdot x^{r[k-1]2^{k-1}} \cdots x^{r[1]2^1} \cdot x^{r[0]2^0}$. Initially, factor is set equal to x and answer is either set equal to x if $r[0] = 1$ (which means that $x^{r[0]2^0} = x$) or it is set equal to 1 if $r[0] = 0$ (which means that $x^{r[0]2^0} = 1$). For each $i = 1$ to k, the value of factor is squared to obtain the numbers x^{2^i}, and each such number is made a factor of the answer provided $r[i] = 1$ (which means that $x^{r[i]2^i} = x^{2^i}$.)]

Input: x *[a real number]*, n *[a positive integer]*

Algorithm Body:

    Call Algorithm 4.1.1 with input n to obtain the output $r[0], r[1], \ldots, r[k]$.

    factor $:= x$

    if $r[0] = 1$ **then** *answer* $:= x$ **else** *answer* $= 1$

    for $i := 1$ **to** k

        factor $:= factor \cdot factor$

        if $r[i] = 1$ **then** *answer* $:= answer \cdot factor$

    next i

Output: *answer [a real number]*

b. There are at most two multiplications per iteration of the **for-next** loop and there are k iterations of this loop. Hence the total number of multiplications is at most $2k$. Now $n = 2^k + $ *lower powers of 2*. Consequently, $2^k \leq n < 2^{k+1}$, and so $k = \lfloor \log_2 n \rfloor$ by property (9.4.2). Thus the number of multiplications is at most $2 \lfloor \log_2 n \rfloor$.

Chapter 10: Relations

The first section of this chapter is an introduction to concepts and notation with emphasis on understanding equivalent ways to specify and represent relations, both finite and infinite. In Section 10.2 the reflexivity, symmetry, and transitivity properties of binary relations are introduced and explored, and in Section 10.3 equivalence relations are discussed. At this point in the course, students are generally able to handle the level of abstraction fairly well. Some still need to be reminded of the logic discussed in the first two chapters and the proof methods covered in Chapter 3. For instance, even at this late stage of the course, I find that a few students rephrase the definition of symmetric as "$x \ R \ y$ and $y \ R \ x$". But even these students are responsive to correction and are generally able to succeed with some assistance. In fact, it is often only at this point in the course that one can count on virtually all students understanding that the same proof outline is used to prove universal conditional statements no matter what the mathematical context.

Class participation in the discussion of these sections is very helpful. For instance, each time you write a definition of a property on the board, you can ask what it means for something not to have that property. And instead of just working examples to prove or disprove the properties in various instances, you can pose questions on the board and get the class to solve them for you, preferably by having several students each contribute a part of the solution. After all, once the definitions have been written down, it is just a question of thinking things through to apply them in any given instance, and students are supposed to have learned how to think things through or at least to be making significant progress in doing so. If time allows, it is desirable to have students present solutions to homework problems for the rest of the class to critique or to work on solving problems together in groups.

Section 10.4 deepens and extends the discussion of congruence relations in Sections 10.2 and 10.3 through applications to modular arithmetic and cryptography. The section is designed to make it possible to give students meaningful practice with RSA cryptography without having to spend several weeks to do so. After a brief introduction to the idea of cryptography, the first part of the section is devoted to helping students develop facility with modular arithmetic, especially finding least positive residues of integers raised to large positive powers and using the Euclidean algorithm to compute positive inverses modulo a number. Proofs of the underlying mathematical theory are left to the end of the section.

Partial order relations are not discussed until the last section of this chapter so as not to confuse students by presenting the definitions of symmetry and antisymmetry side-by-side. Another reason for placing the discussion of partial order relations in Section 10.5 is that the flavor of partial order relations is rather different from that of equivalence relations.

Comments on Exercises:

Section 10.2: **#6-8** and **#50-51**: It would seem as if finite sets would provide the simplest examples of relations, and by and large they do. But in these problems, a few properties are vacuously true (or "true by default"), which is a mode of reasoning that some students still find hard to grasp. Actually, the idea of vacuous truth has occurred frequently enough throughout the book that there frequently are students who relish encountering it in new situations. And usually even the students who still find the idea mind-boggling are amused by it.

Section 10.3: **#31-36**: These exercises are designed to give students practice doing the kind of reasoning that is used to prove the main theorem of the section. These are good exercises to go over with the class as a whole, having a different student supply each step of the solution. **#43**: This

exercise is somewhat whimsical, and students often ask what is its point. It is intended to provide an occasion to discuss the fact that a given equivalence class may have many different names, at least as many as there are representatives in the class, and that one needs to distinguish between what such a mathematical object *is* and what it is *called.*

Section 10.1

2. *a.* No, $2 \not\geq 4$. Yes, $4 \geq 3$. Yes, $4 \geq 4$. No, $2 \notin D$.

   b. $S = \{(3,3), (4,3), (5,3), (4,4), (5,4)\}$

3. *b.* *Proof*: Let n be any even integer. Then $n - 0 = n$ is also even, and so $n \, E \, 0$ by definition of E.

4. The following is a rather complete proof. Shorter versions that have a correct flow and feel should certainly be acceptable.

   Proof: We first observe that for all integers m and n, if $m - n$ is even then both m and n are even or both m and n are odd. To do this, we prove the logically equivalent statement: for all integers m and n, if $m - n$ is even and at least one of m or n is odd, then both m and n are odd. *[See exercise 14 in Section 1.2.]* So suppose m and n are any integers so that $m - n$ is even and at least one of m or n is odd. Since $m - n$ is even, $m - n = 2r$ for some integer r. In case m is odd, then $m = 2s + 1$ for some integer s, and so $n = m - (m - n) = (2s + 1) - 2r = 2(s - r) + 1$, which is odd *[because $s - r$ is an integer]*. In case n is odd, then $n = 2s + 1$ for some integer s, and so $m = (m - n) + n = 2r + (2s + 1) = 2(r + s) + 1$, which is odd *[because $r + s$ is an integer]*. Hence in either case, both m and n are odd *[as was to be shown]*.   To finish the proof, we need to show that for all integers m and n, if both m and n are even or both m and n are odd, then $m - n$ is even. So suppose m and n are any integers such that both m and n are even or both m and n are odd. Then $m = 2a + r$ and $n = 2b + r$ where a and b are integers and $r = 0$ or $r = 1$. It follows that $m - n = (2a + r) - (2b + r) = 2a - 2b = 2(a - b)$. But $a - b$ is an integer (because it is a difference of integers), and thus $m - n$ is even by definition of even.

5. *c.* *One possible answer*: 4, 7, 10, −2, −5

   d. *One possible answer*: 5, 8, 11, −1, −4

   e. *Theorem:*   1. All integers of the form $3k$ are related by T to 0.

   2. All integers of the form $3k + 1$ are related by T to 1.

   3. All integers of the form $3k + 2$ are related by T to 2.

   Proof of (2): Let n be any integer of the form $n = 3k + 1$ for some integer k. By substitution, $n - 1 = (3k + 1) - 1 = 3k$, and so by definition of divisibility, $3 \mid (n - 1)$. Hence by definition of T, $n \, T \, 1$.

   The proofs of (1) and (3) are identical to the proof of (2) with 0 and 2 respectively substituted in place of 1.

6. *a.* Yes, $2 \geq 1$. Yes, $2 \geq 2$. No, $2 \not\geq 3$. Yes, $-1 \geq -2$.

7. *b.*
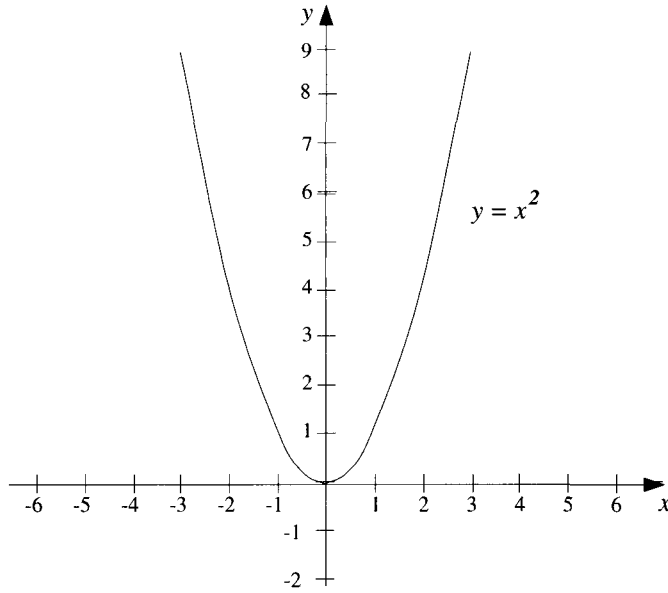
8. *c.* Yes, both have the prime factor 5.   *d.* Yes, both have the prime factor 2.

9. *b.* No, $\{a\}$ has one element and $\{a, b\}$ has two.   *c.* Yes, both have one element.

10. *b.* Yes, because $\{a, b\} \cap \{b, c\} = \{b\} \neq \emptyset$.   *c.* Yes, because $\{a, b\} \cap \{a, b, c\} = \{a, b\} \neq \emptyset$.

11. *b.* No, because $aa \neq bb$.   *c.* Yes, because $aa = aa$.

12. *a.*
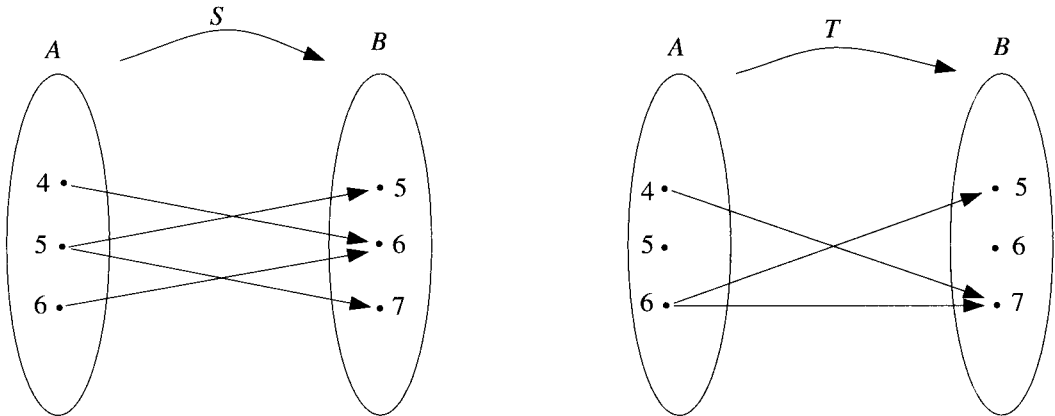
b. S is not a function because $(5, 5) \in S$ and $(5, 7) \in S$ and $5 \neq 7$. So S does not satisfy property (2) of the definition of function. T is not a function both because $(5, x) \notin T$ for any x in B and because $(6, 5) \in T$ and $(6, 7) \in T$ and $5 \neq 7$. So T does not satisfy either property (1) or property (2) of the definition of function.

14. The following 12 sets are all the binary relations from $\{a, b\}$ to $\{x, y\}$ that are not functions:

$\emptyset$, $\{(a, x)\}$, $\{(a, y)\}$, $\{(b, x)\}$, $\{(b, y)\}$, $\{(a, x), (a, y)\}$, $\{(b, x), (b, y)\}$, $\{(a, x), (a, y), (b, x)\}$,
$\{(a, x), (a, y), (b, y)\}$, $\{(b, x), (b, y), (a, x)\}$, $\{(b, x), (b, y), (a, y)\}$, $\{(a, x), (a, y), (b, x), (b, y)\}$.

15. *a.* There are 2^{mn} binary relations from A to B because a binary relation from A to B is any subset of $A \times B$, $A \times B$ is a set with mn elements (since A has m elements and B has n elements), and the number of subsets of a set with mn elements is 2^{mn} (by Theorem 5.3.1).

b. In order to define a function from A to B we must specify exactly one image in B for each of the m elements in A. So we can think of constructing a function from A to B as an m-step process, where step i is to choose an image for the ith element of A (for $i = 1, 2, \ldots, m$). Because there are n choices of image for each of the m elements, by the multiplication rule, the total number of functions is $\underbrace{n \cdot n \cdot n \cdots n}_{m \text{ factors}} = n^m$.

c. $\dfrac{n^m}{2^{nm}} = \left(\dfrac{n}{2^n}\right)^m$

18. $S = \{(3,6), (4,4), (5,5)\}$ $S^{-1} = \{(6,3), (4,4), (5,5)\}$

19. *c.* Yes, *aba* is the concatenation of *a* with *ba*.

d. No, $abb\ T^{-1}\ bba \Leftrightarrow bba\ T\ abb$, but $bba\ \not{T}\ abb$ because *abb* is not the concatenation of *a* with *bba*.

f. Yes, $abba\ T^{-1}\ bba \Leftrightarrow bba\ T\ abba$, and $bba\ T\ abba$ because *abba* is the concatenation of *a* with *bba*.

20.
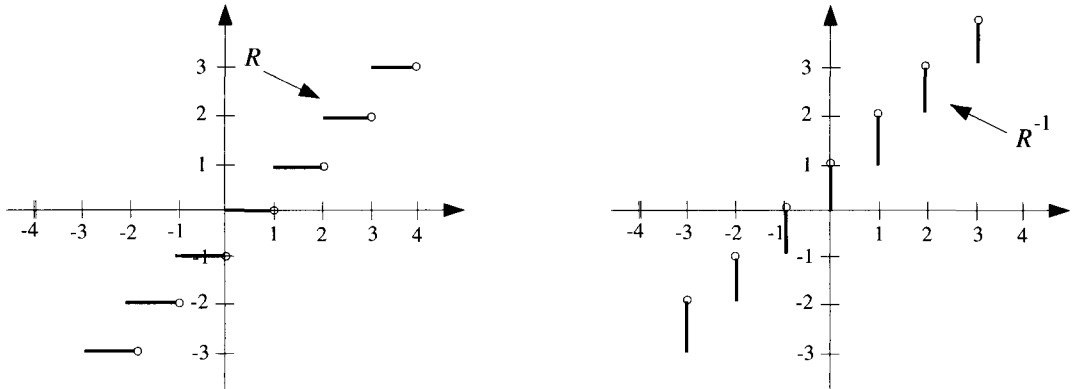
21. *b.* A function $F: X \to Y$ is onto if, and only if, for all $y \in Y$, $\exists x \in X$ such that $(x,y) \in F$.

22. *b.* No. If $F: X \to Y$ is not one-to-one, then there exist x_1 and x_2 in X and y in Y such that $(x_1, y) \in F$ and $(x_2, y) \in F$ and $x_1 \neq x_2$. But this implies that there exist x_1 and x_2 in X and y in Y such that $(y, x_1) \in F^{-1}$ and $(y, x_2) \in F^{-1}$ and $x_1 \neq x_2$. Consequently, F^{-1} does not satisfy property (2) of the definition of function.

24.
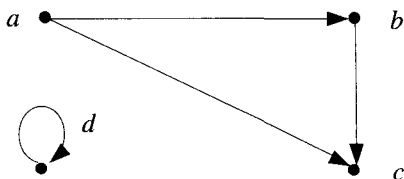
26.
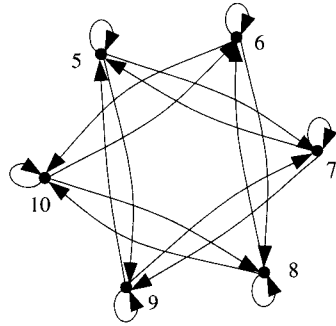
27.
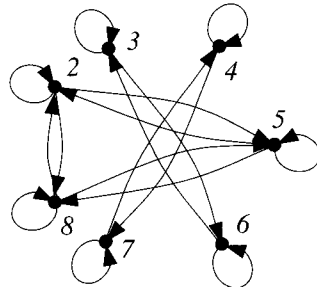
28. *b.*

466581	Mary Lazars
778400	Jamal Baskers

30. $A \times B = \{(-1, 1), (1, 1), (2, 1), (4, 1), (-1, 2), (1, 2), (2, 2), (4, 2)\}$

$R = \{(-1, 1), (1, 1), (2, 2)\}$

$S = \{(-1, 1), (1, 1), (2, 2), (4, 2)\}$

$R \cup S = S \qquad R \cap S = R$

32.
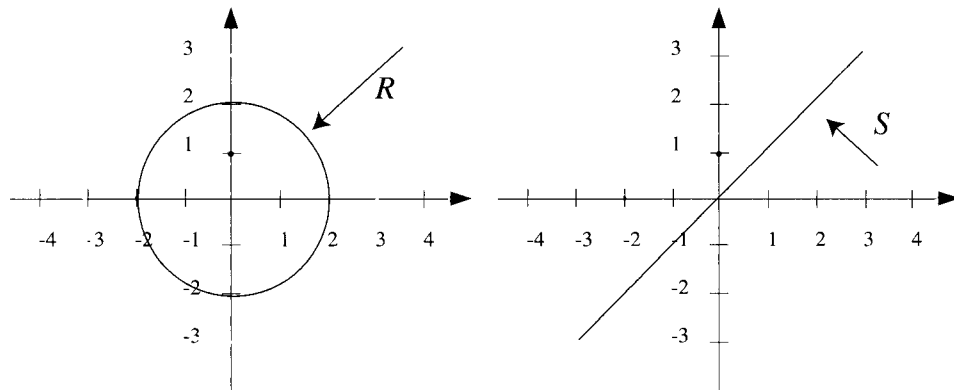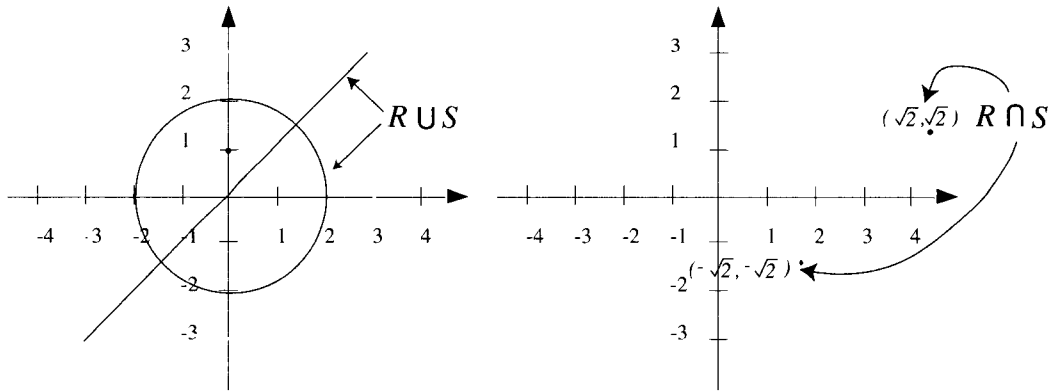
To obtain $R \cap S$, solve the system of equations:
$$x^2 + y^2 = 4$$
$$x = y$$

Substituting the second equation into the first gives $x^2 + y^2 = 4 \Rightarrow 2x^2 = 4 \Rightarrow x^2 = 2 \Rightarrow x = \pm\sqrt{2}$. Hence $x = y = \sqrt{2}$ or $x = y = -\sqrt{2}$.

33.
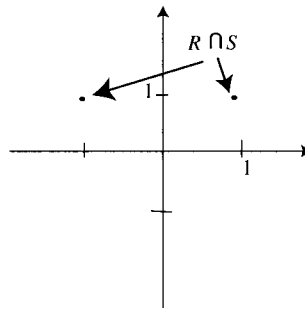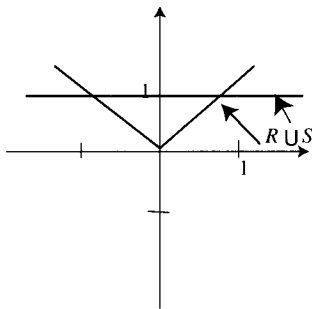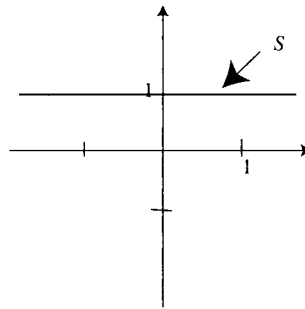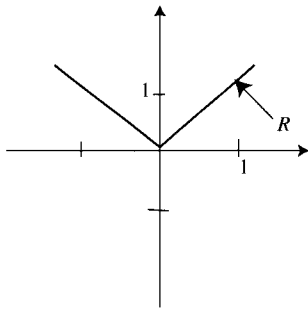
Section 10.2

2. *a.*
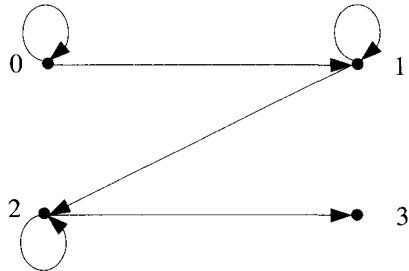
b. R_2 is not reflexive because $(3,3) \notin R_2$.

c. R_2 is not symmetric because, for example, $(0,1) \in R_2$ but $(1,0) \notin R_2$.

d. R_2 is not transitive because, for example, $(0,1) \in R_2$ and $(1,2) \in R_2$ but $(0,2) \notin R_2$.

4. *a.*
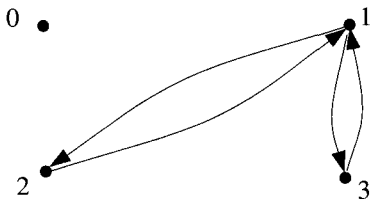
b. R_4 is not reflexive because, for instance, $(0,0) \notin R_4$. (In fact, $(x,x) \notin R_4$ for any x in A.)

c. R_4 is symmetric.

d. R_4 is not transitive because, for example, $(3,1) \in R_4$ and $(1,2) \in R_4$ but $(3,2) \notin R_4$.

5. *a.*
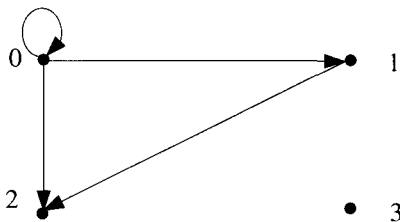
b. R_5 is not reflexive because, for example, $(1,1) \notin R_2$.

c. R_5 is not symmetric because, for example, $(0,1) \in R_5$ but $(1,0) \notin R_5$.

d. R_5 is transitive.

7. *a.*
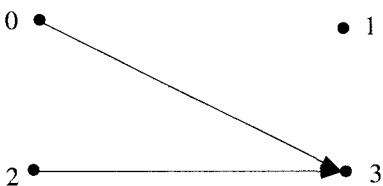
b. R_7 is not reflexive because, for example, $(0,0) \notin R_7$.

c. R_7 is not symmetric because, for example, $(0,3) \in R_7$ but $(3,0) \notin R_7$.

d. R_7 is transitive.

8. *a.*

b. R_8 is not reflexive because, for example, $(2,2) \notin R_8$.

c. R_8 is symmetric.

d. R_8 is transitive.

10. $S^t = \{(0,0), (0,3), (1,0), (1,2), (2,0), (3,2), (0,2), (1,3), (2,2), (2,3), (3,3), (3,0)\}$

11. $T^t = \{(0,2), (1,0), (2,3), (3,1), (0,3), (1,2), (2,1), (3,2), (3,0), (0,0), (0,1), (1,1), (1,3), (3,3),$
$(2,2), (2,0)\}$

13. *C is not reflexive*: C is reflexive $\Leftrightarrow$ for all real numbers x, $x \, C \, x$. By definition of C this means that for all real numbers x, $x^2 + x^2 = 1$. But this is false. As a counterexample, take $x = 0$. Then $x^2 + x^2 = 0^2 + 0^2 = 0 \neq 1$.

C is symmetric: C is symmetric $\Leftrightarrow$ for all real numbers x and y, if $x \, C \, y$ then $y \, C \, x$. By definition of C this means that for all real numbers x and y, if $x^2 + y^2 = 1$ then $y^2 + x^2 = 1$. But this is true because by commutativity of addition, $x^2 + y^2 = y^2 + x^2$ for all real numbers x and y.

C is not transitive: C is transitive $\Leftrightarrow$ for all real numbers x, y, and z, if $x \, C \, y$ and $y \, C \, z$ then $x \, C \, z$. By definition of C this means that for all real numbers x, y and z, if $x^2 + y^2 = 1$ and $y^2 + z^2 = 1$ then $x^2 + z^2 = 1$. But this is false. As a counterexample, take $x = 0$, $y = 1$, and $z = 0$. Then $x^2 + y^2 = 1$ because $0^2 + 1^2 = 1$ and $y^2 + z^2 = 1$ because $1^2 + 0^2 = 1$, but $x^2 + z^2 \neq 1$ because $0^2 + 0^2 = 0 \neq 1$.

16. *F is reflexive*: Suppose m is any integer. Since $m - m = 0$ and $5 \mid 0$, we have that $5 \mid (m - m)$. Consequently, $m \, F \, m$ by definition of F.

F is symmetric: Suppose m and n are any integers such that $m \, F \, n$. By definition of F this means that $5 \mid (m - n)$, and so, by definition of divisibility, $m - n = 5k$ for some integer k. Now $n - m = -(m - n)$. Hence by substitution, $n - m = -(5k) = 5 \cdot (-k)$. It follows that $5 \mid (n - m)$ by definition of divisibility (since $-k$ is an integer), and thus $n \, F \, m$ by definition of F.

F is transitive: Suppose m, n and p are any integers such that $m \, F \, n$ and $n \, F \, p$. By definition of F, this means that $5 \mid (m - n)$ and $5 \mid (n - p)$, and so, by definition of divisibility, $m - n = 5k$ for some integer k, and $n - p = 5l$ for some integer l. Now $m - p = (m - n) + (n - p)$. Hence by substitution, $m - p = 5k + 5l = 5(k + l)$. It follows that $5 \mid (m - p)$ by definition of divisibility (since $k + l$ is an integer), and thus $m \, F \, p$ by definition of F.

17. *O is not reflexive*: O is reflexive $\Leftrightarrow$ for all integers m, $m \, O \, m$. By definition of O this means that for all integers m, $m - m$ is odd. But this is false. As a counterexample, take any integer m. Then $m - m = 0$, which is even, not odd.

O is symmetric: Suppose m and n are any integers such that $m \ O \ n$. By definition of O this means that $m - n$ is odd, and so by definition of odd $m - n = 2k + 1$ for some integer k. Now $n - m = -(m - n)$. Hence by substitution, $n - m = -(2k + 1) = 2(-k - 1) + 1$. It follows that $n - m$ is odd by definition of odd (since $-k - 1$ is an integer), and thus $n \ O \ m$ by definition of O.

O is not transitive: O is transitive $\Leftrightarrow$ for all integers m, n, and p, if $m \ O \ n$ and $n \ O \ p$ then $m \ O \ p$. By definition of O this means that for all integers m, n, and p, if $m - n$ is odd and $n - p$ is odd then $m - p$ is odd. But this is false. As a counterexample, take $m = 1$, $n = 0$, and $p = 1$. Then $m - n = 1 - 0 = 1$ is odd and $n - p = 0 - 1 = -1$ is also odd, but $m - p = 1 - 1 = 0$ is not odd. Hence $m \ O \ n$ and $n \ O \ p$ but $m \ \cancel{O} \ p$.

19. *A is reflexive*: A is reflexive $\Leftrightarrow$ for all real numbers x, $\mid x \mid = \mid x \mid$. But this is true by the reflexive property of equality.

    A is symmetric: [*We must show that for all real numbers x and y, if $\mid x \mid = \mid y \mid$ then $\mid y \mid = \mid x \mid$.*] But this is true by the symmetric property of equality.

    A is transitive: A is transitive $\Leftrightarrow$ for all real numbers x, y, and z, if $\mid x \mid = \mid y \mid$ and $\mid y \mid = \mid z \mid$, then $\mid x \mid = \mid z \mid$. But this is true by the transitive property of equality.

20. *P is not reflexive*: P is reflexive $\Leftrightarrow$ for all integers n, $n \ P \ n$. By definition of P this means that for all integers n, $\exists$ a prime number p such that $p \mid n$ and $p \mid n$. But this is false. As a counterexample, take $n = 1$. There is no prime number that divides 1.

    P is symmetric: [*We must show that for all integers m and n, if $m \ P \ n$ then $n \ P \ m$.*] Suppose m and n are integers such that $m \ P \ n$. By definition of P this means that there exists a prime number p such that $p \mid m$ and $p \mid n$. But to say that "$p \mid m$ and $p \mid n$" is logically equivalent to saying that "$p \mid n$ and $p \mid m$." Hence there exists a prime number p such that $p \mid n$ and $p \mid m$, and so by definition of P, $n \ P \ m$.

    P is not transitive: P is transitive $\Leftrightarrow$ for all integers m, n, and p, if $m \ P \ n$ and $n \ P \ p$ then $m \ P \ p$. But this is false. As a counterexample, take $m = 2$, $n = 6$, and $p = 9$. Then $m \ P \ n$ because the prime number 2 divides both 2 and 6 and $n \ P \ p$ because the prime number 3 divides both 6 and 9, but $m \ \cancel{P} \ n$ because the numbers 2 and 9 have no common prime factor.

22. *G is not reflexive*: G is reflexive $\Leftrightarrow$ for all strings s of 0's and 1's, $s \ G \ s$. By definition of G this means that for all strings s of 0's and 1's, the number of 0's in s is greater than the number of 0's in s. But this is false for every string of 0's and 1's. For instance, let $s = 00$. Then the number of 0's in s is 2 which is not greater than 2.

    G is not symmetric: For G to be symmetric would mean that for all strings s and t of 0's and 1's, if $s \ G \ t$ then $t \ R \ s$. By definition of G, this would mean that for all strings s and t of 0's and 1's, if the number of 0's in s is greater than the number of 0's in t, then the number of 0's in t is greater than the number of 0's in s. But this is false for all strings s and t of 0's and 1's. For instance, take $s = 100$ and $t = 10$. Then the number of 0's in s is 2 and the number of 0's in t is 1. It follows that $s \ G \ t$ (since $2 > 1$), but $t \ \cancel{G} \ s$ (since $1 \not> 2$).

    G is transitive: To prove transitivity of G, we must show that for all strings s, t, and u of 0's and 1's, if $s \ G \ t$ and $t \ G \ u$ then $s \ G \ u$. By definition of G this means that for all strings s, t, and u of 0's and 1's, if the number of 0's in s is greater than the number of 0's in t and the number of 0's in t is greater than the number of 0's in u, then the number of 0's in s is greater than the number of 0's in u. But this is true by the transitivity property of order (Appendix A, T17).

24. *$\mathscr{P}$ is not reflexive*: $\mathscr{P}$ is reflexive $\Leftrightarrow$ for all sets $A \in \mathscr{P}(X)$, $A \ \mathscr{P} \ A$. By definition of $\mathscr{P}$ this means that for all sets A in $\mathscr{P}(X)$, $N(A) < N(A)$. But this is false for every set in $\mathscr{P}(X)$. For instance, let $A = \emptyset$. Then $N(A) = 0$, and 0 is not less than 0.

$\mathscr{R}$ *is not symmetric*: For R to be symmetric would mean that for all sets A and B in $\mathscr{P}(X)$, if A $\mathscr{R}$ B then B $\mathscr{R}$ A. By definition of $\mathscr{R}$, this would mean that for all sets A and B in $\mathscr{P}(X)$, if $N(A) < N(B)$, then $N(B) < N(A)$. But this is false for all sets A and B in $\mathscr{P}(X)$. For instance, take $A = \emptyset$ and $B = \{a\}$. Then $N(A) = 0$ and $N(B) = 1$. It follows that A is related to B by $\mathscr{R}$ (since $0 < 1$), but B is not related to A by $\mathscr{R}$ (since $1 \not< 0$).

$\mathscr{R}$ *is transitive*: To prove transitivity of $\mathscr{R}$, we must show that for all sets A, B, and C in $\mathscr{P}(X)$, if A $\mathscr{R}$ B and B $\mathscr{R}$ C then A $\mathscr{R}$ C. By definition of $\mathscr{R}$ this means that for all sets A, B, and C in $\mathscr{P}(X)$, if $N(A) < N(B)$ and $N(B) < N(C)$, then $N(A) < N(C)$. But this is true by the transitivity property of order (Appendix A, T17).

25. $\mathscr{N}$ *is not reflexive*: $\mathscr{N}$ is reflexive $\Leftrightarrow$ for all sets $A \in \mathscr{P}(X)$, A $\mathscr{N}$ A. By definition of $\mathscr{N}$ this means that for all sets A in $\mathscr{P}(X)$, $N(A) \neq N(A)$ (where for each set X, $N(S)$ denotes the number of elements in S). But this is false for every set in $\mathscr{P}(X)$. For instance, let $A = \emptyset$. Then $N(A) = 0$. And it is not true that $0 \neq 0$.

$\mathscr{N}$ *is symmetric*: $\mathscr{N}$ is symmetric $\Leftrightarrow$ for all sets A and B in $\mathscr{P}(X)$, if A $\mathscr{N}$ B then B $\mathscr{N}$ A. By definition of $\mathscr{N}$, this means that for all sets A and B in $\mathscr{P}(X)$, if $N(A) \neq N(B)$, then $N(B) \neq N(A)$. But this is true.

$\mathscr{N}$ *is not transitive*: $\mathscr{N}$ is transitive $\Leftrightarrow$ for all sets A, B, and C in $\mathscr{P}(X)$, if A $\mathscr{N}$ B and B $\mathscr{N}$ C then A $\mathscr{N}$ C. By definition of $\mathscr{N}$ this means that for all sets A, B, and C in $\mathscr{P}(X)$, if $N(A) \neq N(B)$ and $N(B) \neq N(C)$, then $N(A) \neq N(C)$. But this is false. As a counterexample, let $A = \{a\}$, $B = \{a,b\}$, and $C = \{b\}$. Then $N(A) = 1$, $N(B) = 2$, and $N(C) = 1$. So $N(A) \neq N(B)$ and $N(B) \neq N(C)$, but $N(A) = N(C)$.

27. $\mathscr{R}$ *is not reflexive*: $\mathscr{R}$ is reflexive $\Leftrightarrow$ for all sets $X \in \mathscr{P}(A)$, X $\mathscr{R}$ X. By definition of $\mathscr{R}$ this means that for all sets X in $\mathscr{P}(A)$, $X \neq X$. But this is false for every set in $\mathscr{P}(A)$. For instance, let $X = \emptyset$. It is not true that $\emptyset \neq \emptyset$.

$\mathscr{R}$ *is symmetric*: $\mathscr{R}$ is symmetric $\Leftrightarrow$ for all sets X and Y in $\mathscr{P}(A)$, if X $\mathscr{R}$ Y then Y $\mathscr{R}$ X. By definition of $\mathscr{R}$, this means that for all sets X and Y in $\mathscr{P}(A)$, if $X \neq Y$, then $Y \neq X$. But this is true.

$\mathscr{R}$ *is not transitive*: $\mathscr{R}$ is transitive $\Leftrightarrow$ for all sets X, Y, and Z in $\mathscr{P}(A)$, if X $\mathscr{R}$ Y and Y $\mathscr{R}$ Z then X $\mathscr{R}$ Z. By definition of $\mathscr{R}$ this means that for all sets X, Y, and Z in $\mathscr{P}(A)$, if $X \neq Y$ and $Y \neq Z$, then $X \neq Z$. But this is false as the following counterexample shows. Since $A \neq \emptyset$, there exists an element x in A. Let $X = \{x\}$, $Y = \emptyset$, and $Z = \{x\}$. Then $X \neq Y$ and $Y \neq Z$, but $X = Z$.

28. $\mathscr{C}$ *is not reflexive*: $\mathscr{C}$ is reflexive $\Leftrightarrow$ for all sets $X \in \mathscr{P}(A)$, X $\mathscr{C}$ X. By definition of $\mathscr{C}$ this means that for all sets X in $\mathscr{P}(A)$, $X = A - X$. But this is false for every set in $\mathscr{P}(A)$ because $A \neq \emptyset$. For instance, let $X = \emptyset$. It is not true that $\emptyset = A - \emptyset$ because $A - \emptyset = A$ and $A \neq \emptyset$.

$\mathscr{C}$ *is symmetric*: *[We must show that for all sets X and Y in $\mathscr{P}(A)$, if X $\mathscr{C}$ Y then Y $\mathscr{C}$ X.]* Suppose X and Y are sets in $\mathscr{P}(A)$ and "$X \mathscr{C} Y$. By definition of $\mathscr{C}$, this means that $Y = A - X$. By the properties of sets given in Sections 5.2, $A - Y = A - (A - X) = A \cap (A \cap X^c)^c = A \cap (A^c \cup X) = (A \cap A^c) \cup (A \cap X) = \emptyset \cup (A \cap X) = (A \cap X) \cup \emptyset = A \cap X = X$ (because $X \subseteq A$). Hence Y $\mathscr{C}$ X.

$\mathscr{C}$ *is not transitive*: $\mathscr{C}$ is transitive $\Leftrightarrow$ for all sets X, Y, and Z in $\mathscr{P}(A)$, if X $\mathscr{R}$ Y and Y $\mathscr{C}$ Z then X $\mathscr{C}$ Z. By definition of $\mathscr{C}$ this means that for all sets X, Y, and Z in $\mathscr{P}(A)$, if $Y = A - X$ and $Z = A - Y$, then $Z = A - X$. However this is false, as the following counterexample shows. Since $A \neq \emptyset$, there exists an element x in A. Let $X = \{x\}$, $Y = A - X$, and $Z = A - Y$. Then by substitution, $Z = A - (A - X) = X$ *[by the same argument as in the proof of symmetry above]* . Suppose $Z = A - X$. Then we would have $A - X = X$. But this is impossible because $x \in \{x\} = X$ and $x \notin A - \{x\} = A - X$. Therefore it cannot be the case that $Z = A - X$. Consequently X $\mathscr{C}$ Y and Y $\mathscr{C}$ Z but X is not related to Z by $\mathscr{C}$.

29. $\mathscr{R}$ *is reflexive: [We must show that for all sets* X *in* $\mathscr{P}(A)$, $X \mathscr{R} X$.*]* Suppose X is a set in $\mathscr{P}(A)$. By definition of subset, we know that $X \subseteq X$. By definition of $\mathscr{R}$, then, $X \mathscr{R} X$.

$\mathscr{R}$ *is symmetric: [We must show that for all sets* X *and* Y *in* $\mathscr{P}(A)$, *if* $X \mathscr{R} Y$ *then* $Y \mathscr{R} X$.*]* Suppose X and Y are sets in $\mathscr{P}(A)$ and $X \mathscr{R} Y$. By definition of $\mathscr{R}$, this means that $X \subseteq Y$ or $Y \subseteq X$. In case $X \subseteq Y$, then the statement "$Y \subseteq X$ or $X \subseteq Y$" is true, and so by definition of $\mathscr{R}$, $Y \mathscr{R} X$. In case $Y \subseteq X$ then the statement "$Y \subseteq X$ or $X \subseteq Y$" is also true, and so by definition of $\mathscr{R}$, $Y \mathscr{R} X$. Therefore in either case $Y \mathscr{R} X$.

If A *has at least two elements, then* $\mathscr{R}$ *is not transitive:* $\mathscr{R}$ is transitive $\Leftrightarrow$ for all sets X, Y, and Z in $\mathscr{P}(A)$, if $X \mathscr{R} Y$ and $Y \mathscr{R} Z$ then $X \mathscr{R} Z$. By definition of $\mathscr{R}$ this means that for all sets X, Y, and Z in $\mathscr{P}(A)$, if either $X \subseteq Y$ or $Y \subseteq X$ and either $Y \subseteq Z$ or $Z \subseteq Y$, then either $X \subseteq Z$ or $Z \subseteq X$. However this is false, as the following counterexample shows. Since A has at least two elements, there exist elements x and y in A with $x \neq y$. Let $X = \{x\}$, $Y = A$, and $Z = \{y\}$. Then $X \subseteq Y$ and so $X \mathscr{R} Y$ and $Z \subseteq Y$ and so $Y \mathscr{R} Z$. But $X \not\subseteq Z$ and $Z \not\subseteq X$ because $x \neq y$. Hence X is not related to Z by $\mathscr{R}$.

If A *has a single element, then* $\mathscr{R}$ *is transitive:* In this case, given any two subsets of A, either one is a subset of the other or the other is a subset of the one. Hence regardless of the choice of X, Y, and Z, it must be the case that $X \subseteq Z$ or $Z \subseteq X$ and so $X \mathscr{R} Z$.

32. $\mathscr{R}$ *is reflexive:* $\mathscr{R}$ is reflexive $\Leftrightarrow$ for all elements (x, y) in $\mathbf{R} \times \mathbf{R}$, $(x, y)\mathscr{R}(x, y)$. By definition of $\mathscr{R}$ this means that for all elements (x, y) in $\mathbf{R} \times \mathbf{R}$, $y = y$. But this is true.

$\mathscr{R}$ *is symmetric: [We must show that for all elements* (x_1, y_1) *and* (x_2, y_2) *in* $\mathbf{R} \times \mathbf{R}$, *if* $(x_1, y_1)\mathscr{R}(x_2, y_2)$ *then* $(x_2, y_2)\mathscr{R}(x_1, y_1)$.*]* Suppose (x_1, y_1) and (x_2, y_2) are elements of $\mathbf{R} \times \mathbf{R}$ such that $(x_1, y_1)\mathscr{R}(x_2, y_2)$. By definition of $\mathscr{R}$ this means that $y_1 = y_2$. By symmetry of equality, $y_2 = y_1$. So by definition of $\mathscr{R}$, $(x_2, y_2)\mathscr{R}(x_1, y_1)$.

$\mathscr{R}$ *is transitive: [We must show that for all elements* (x_1, y_1), (x_2, y_2) *and* (x_3, y_3) *in* $\mathbf{R} \times \mathbf{R}$, *if* $(x_1, y_1)\mathscr{R}(x_2, y_2)$ *and* $(x_2, y_2)\mathscr{R}(x_3, y_3)$ *then* $(x_1, y_1)\mathscr{R}(x_3, y_3)$.*]* Suppose (x_1, y_1), (x_2, y_2), and (x_3, y_3) are elements of $\mathbf{R} \times \mathbf{R}$ such that $(x_1, y_1)\mathscr{R}(x_2, y_2)$ and $(x_2, y_2)\mathscr{R}(x_3, y_3)$. By definition of $\mathscr{R}$ this means that $y_1 = y_2$ and $y_2 = y_3$. By transitivity of equality, $y_1 = y_3$. Hence by definition of $\mathscr{R}$, $(x_1, y_1)\mathscr{R}(x_3, y_3)$.

33. R *is reflexive:* R is reflexive $\Leftrightarrow$ for all points p in A, $p \, R \, p$. By definition of R this means that for all elements p in A, p and p both lie on the same half line emanating from the origin. But this is true.

R *is symmetric: [We must show that for all points* p_1 *and* p_2 *in* A, *if* $p_1 R \, p_2$ *then* $p_2 R \, p_1$.*]* Suppose p_1 and p_2 are points in A such that $p_1 R \, p_2$. By definition of R this means that p_1 and p_2 lie on the same half line emanating from the origin. But this implies that p_2 and p_1 lie on the same half line emanating from the origin. So by definition of R, $p_2 R \, p_1$.

R *is transitive: [We must show that for all points* p_1, p_2 *and* p_3 *in* A, *if* $p_1 R \, p_2$ *and* $p_2 R \, p_3$ *then* $p_1 R \, p_3$.*]* Suppose p_1, p_2, and p_3 are points in A such that $p_1 R \, p_2$ and $p_2 R \, p_3$. By definition of R, this means that p_1 and p_2 lie on the same half line emanating from the origin and p_2 and p_3 lie on the same half line emanating from the origin. Since two points determine a line, it follows that both p_1 and p_3 lie on the same half line determined by the origin and p_2. Thus p_1 and p_3 lie on the same half line emanating from the origin, and so by definition of R, $p_1 R \, p_3$.

35. R *is reflexive:* R is reflexive $\Leftrightarrow$ for all lines l in A, $l \, R \, l$. By definition of R this means that for all lines l in the plane, l is parallel to itself. But this is true.

R *is symmetric: [We must show that for all lines* l_1 *and* l_2 *in* A, *if* $l_1 R \, l_2$ *then* $l_2 R \, l_1$.*]* Suppose l_1 and l_2 are lines in A such that $l_1 R \, l_2$. By definition of R this means that l_1 is parallel to l_2. But this implies that l_2 is parallel to l_1. So by definition of R, $l_2 R \, l_1$.

R *is transitive: [We must show that for all lines* l_1, l_2 *and* l_3 *in* A, *if* $l_1 R \, l_2$ *and* $l_2 R \, l_3$ *then* $l_1 R \, l_3$.*]* Suppose l_1, l_2, and l_3 are lines of A such that $l_1 R \, l_2$ and $l_2 R \, l_3$. By definition of R

this means that l_1 is parallel to l_2 and l_2 is parallel to l_3. Since two lines each parallel to a third line are parallel to each other, it follows that l_1 is parallel to l_3 because both are parallel to l_2. Hence by definition of R, $l_1 R\ l_3$.

36. *R is not reflexive:* R is reflexive $\Leftrightarrow$ for all lines l in A, $l\ R\ l$. By definition of R this means that for all lines l in the plane, l is perpendicular to itself. But this is false for every line in the plane.

R is symmetric: [We must show that for all lines l_1 and l_2 in A, if $l_1 R\ l_2$ then $l_2 R\ l_1$.] Suppose l_1 and l_2 are lines in A such that $l_1 R\ l_2$. By definition of R this means that l_1 is perpendicular to l_2. But this implies that l_2 is perpendicular to l_1. So by definition of R, $l_2 R\ l_1$.

R is not transitive: R is transitive $\Leftrightarrow$ for all lines l_1, l_2, and l_3 in A, if $l_1 R\ l_2$ and $l_2 R\ l_3$ then $l_1 R\ l_3$. But this is false. As a counterexample, take l_1 and l_3 to be the horizontal axis and l_2 to be the vertical axis. Then $l_1 R\ l_2$ and $l_2 R\ l_3$ because the horizontal axis is perpendicular to the vertical axis and the vertical axis is perpendicular to the horizontal axis. But $l_1 \not{R}\ l_3$ because the horizontal axis is not perpendicular to itself.

37. *b.* A reflexive relation must contain (a,a) for all eight elements a in A. Any subset of the remaining 56 elements of $A \times A$ (which has a total of 64 elements) can be combined with these eight to produce a reflexive relation. Therefore, there are as many reflexive binary relations as there are subsets of a set of 56 elements, namely 2^{56}.

d. Form a relation that is both reflexive and symmetric by a two-step process: (1) pick all eight elements of the form (x,x) where $x \in A$, (2) pick a set of (distinct) pairs of elements of the form (a,b) and (b,a). There is just one way to perform step 1, and, as explained in the answer to part (c), there are 2^{28} ways to perform step 2. Therefore, there are 2^{28} binary relations on A that are reflexive and symmetric.

39. **Algorithm   Test for Symmetry**

[The input for this algorithm consists of a binary relation R defined on a set A which is represented as the one-dimensional array $a[1], a[2], \ldots, a[n]$. To test whether R is symmetric, the variable "answer" is initially set equal to "yes" and then each pair of elements $a[i]$ and $a[j]$ of A is examined in turn to see whether the condition "if $(a[i], a[j]) \in R$ then $(a[j], a[i]) \in R$" is satisfied. If not, then "answer" is set equal to "no", the while loop is not repeated, and processing terminates.]

Input: *n [a positive integer], $a[1], a[2], \ldots, a[n]$ [a one-dimensional array representing a set A], R [a subset of $A \times A$]*

Algorithm Body:

> $i := 1$, *answer* := "yes"
>
> **while** (*answer* = "yes" and $i \leq n$)
>
>> $j := 1$
>>
>> **while** (*answer* = "yes" and $j \leq n$)
>>
>>> **if** $(a[i], a[j]) \in R$ and $(a[j], a[i]) \notin R$ **then** *answer* := "no"
>>>
>>> $j := j + 1$
>>
>> **end while**
>>
>> $i := i + 1$
>
> **end while**

Output: *answer [a string]*

40. **Algorithm   Test for Transitivity**

[The input for this algorithm consists of a binary relation R defined on a set A which is represented as the one-dimensional array $a[1], a[2], \ldots, a[n]$. To test whether R is transitive,

the variable "answer" is initially set equal to "yes" and then each triple of elements $a[i]$, $a[j]$, and $a[k]$ of A is examined in turn to see whether the condition "if $(a[i], a[j]) \in R$ and $(a[j], a[k]) \in R$ then $(a[i], a[k]) \in R$" is satisfied. If not, then "answer" is set equal to "no", the while loop is not repeated, and processing terminates.]

Input: n *[a positive integer]*, $a[1], a[2], \ldots, a[n]$ *[a one-dimensional array representing a set A]*, R *[a subset of $A \times A$]*

Algorithm Body:

> $i := 1$, *answer* := "yes"
>
> **while** (*answer* = "yes" and $i \leq n$)
>
> > $j := 1$
> >
> > **while** (*answer* = "yes" and $j \leq n$)
> >
> > > $k := 1$
> > >
> > > **while** (*answer* = "yes" and $k \leq n$)
> > >
> > > > **if** $(a[i], a[j]) \in R$ and $(a[j], a[k]) \in R$ and $(a[i], a[k]) \notin R$ **then** *answer* := "no"
> > > >
> > > > $k := k + 1$
> > >
> > > **end while**
> > >
> > > $j := j + 1$
> >
> > **end while**
> >
> > $i := i + 1$
>
> **end while**

Output: *answer [a string]*

41. *Proof*: Define an **R-sequence on A from x to y** to be any finite sequence of elements of A, say $(x_0, x_1, x_2, \ldots, x_n)$, with $n > 0$, $x = x_0$, and $y = x_n$, such that $x_i \, R \, x_{i+1}$ for all integers i with $0 \leq i < n$. Let T be the binary relation on A defined as follows: $x \; \boldsymbol{T} \; \boldsymbol{y} \; \Leftrightarrow \; \exists$ **an R-sequence on A from x to y**. We will show that $T = R^t$.

Part 1 (T is transitive): Suppose $a \, T \, b$ and $b \, T \, c$ for some a, b, and c in A. Then there is an R-sequence $(x_0, x_1, x_2, \ldots, x_m)$ on A from a to b and an R-sequence $(y_0, y_1, y_2, \ldots, y_n)$ on A from b to c. But because $x_m = y_0 = b$, it follows that $(x_0, x_1, x_2, \ldots, x_m, y_1, y_2, \ldots, y_n)$ is an R-sequence on A from a to c. Thus $a \, T \, c$.

Part 2 ($R \subseteq T$): Suppose $(a, b) \in R$. Then $a \, R \, b$, and, by definition of R-sequence, (a, b) is an R-sequence from a to b. Thus, by definition of T, $a \, T \, b$, or, equivalently, $(a, b) \in T$.

Part 3 (If S is any transitive relation on A such that $R \subseteq S$, then $T \subseteq S$): Suppose S is any transitive relation on A such that $R \subseteq S$, and suppose $(a, b) \in T$. Then $a \, T \, b$ and there exists an R-sequence $(x_0, x_1, x_2, \ldots, x_n)$ from a to b. We must show that $(a, b) \in S$. We do this by mathematical induction.

Let the property $P(n)$ be the sentence "If $\sigma = (x_0, x_1, x_2, \ldots, x_n)$ is any R-sequence on A from a to b, then $(a, b) \in S$."

Show that the property is true for $n = 1$: If $\sigma = (x_0, x_1)$ is any R-sequence on A from a to b, then $x_0 = a$ and $x_1 = b$, and so $a \, R \, b$, or, equivalently, $(a, b) \in R$. Thus, $(a, b) \in S$ because $R \subseteq S$.

Show that for all integers $k \geq 1$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let k be any integer with $k \geq 1$, and suppose that if $\tau = (y_0, y_1, y_2, \ldots, y_k)$ is any R-sequence on A from a to b then $(a, b) \in S$. *[This is the inductive hypothesis.]* We must show that if $\sigma = (x_0, x_1, x_2, \ldots, x_{k+1})$ is any R-sequence on A from a to b, then $(a, b) \in S$. So suppose $\sigma = (x_0, x_1, x_2, \ldots, x_{k+1})$ is an R-sequence on A from a to b. Then $(x_0, x_1, x_2, \ldots, x_k)$

is an R-sequence on A from a to x_k, and so, by inductive hypothesis, $(a, x_k) \in S$. Moreover, by definition of R-sequence, $x_k \ R \ x_{k+1}$, or, equivalently, $(x_k, x_{k+1}) \in R$. But $R \subseteq S$, and thus $(x_k, x_{k+1}) \in S$. Therefore, $(a, b) \in S$ because S is transitive and because $x_{k+1} = b$. *[This is what was to be shown.]*

Part 4 (Conclusion of the proof): Parts (1)-(3) show that T satisfies the three conditions necessary for it to be the transitive closure of R.

42. The following is an easily understood algorithm to construct the transitive closure of a relation. A somewhat more efficient algorithm, known as Warshall's algorithm, is discussed in most books on the design and analysis of algorithms. See, for example, *Computer Algorithms* (Second Edition) by Sara Baase, Reading, Massachusetts: Addison-Wesley Publishing Company, 1988, pp.287-90.

Algorithm   Constructing a Transitive Closure

[The input for this algorithm consists of a binary relation R defined on a set A which is represented as the one-dimensional array $a[1], a[2], \ldots, a[n]$. The transitive closure is constructed by modifying the procedure used to test for transitivity described in the answer to exercise 40. Initially, the transitive closure, R^t, is set equal to R. Then a check is made through all triples of elements of A. In all cases for which $(a[i], a[j]) \in R^t$, $(a[j], a[k]) \in R^t$, and $(a[i], a[k]) \notin R^t$, the pair $(a[i], a[k])$ is added to R^t. After R^t has been enlarged in this way, it still may not equal the actual transitive closure of R because some of the added pairs may combine with pairs already present to necessitate the presence of additional pairs. So if any pairs have been added, an additional pass through all triples of elements of A is made. If after all triples of elements of A have been examined no pair has been added, the current relation R^t is transitive and equals the transitive closure of R.]

Input: *n [a positive integer], $a[1], a[2], \ldots, a[n]$ [a one-dimensional array representing a set A], R [a subset of $A \times A$]*

Algorithm Body:

$R^t := R$

repeat := *"yes"*

while (*repeat* = *"yes"*)

  repeat := *"no"*

  $i := 1$

  while ($i \leq n$)

    $j := 1$

    while ($j \leq n$)

      $k := 1$

      while ($k \leq n$)

        if $(a[i], a[j]) \in R^t$ and $(a[j], a[k]) \in R^t$ and $(a[i], a[k]) \notin R^t$ **then do**

          $R^t := R^t \cup \{(a[i], a[k])\}$

          repeat := *"yes"* **end do**

        $k := k + 1$

      end while

      $j := j + 1$

    end while

    $i := i + 1$

  end while

end while

Output: R^t *[a subset of $A \times A$]*

43. *b. $R \cap S$ is symmetric*: Suppose R and S are symmetric. *[To show that $R \cap S$ is symmetric, we must show that $\forall x, y \in A$, if $(x, y) \in R \cap S$ then $(y, x) \in R \cap S$.]* So suppose x and y are elements of A such that $(x, y) \in R \cap S$. By definition of intersection, $(x, y) \in R$ and $(x, y) \in S$. It follows that $(y, x) \in R$ because R is symmetric and $(x, y) \in R$, and also $(y, x) \in S$ because S is symmetric and $(x, y) \in S$. Thus by definition of intersection $(y, x) \in R \cap S$.

c. $R \cap S$ is transitive: Suppose R and S are transitive. *[To show that $R \cap S$ is transitive, we must show that $\forall x, y, z \in A$, if $(x, y) \in R \cap S$ and $(y, z) \in R \cap S$ then $(x, z) \in R \cap S$.]* So suppose x, y, and z are elements of A such that $(x, y) \in R \cap S$ and $(y, z) \in R \cap S$. By definition of intersection, $(x, y) \in R$, $(x, y) \in S$, $(y, z) \in R$, and $(y, z) \in S$. It follows that $(x, z) \in R$ because R is transitive and $(x, y) \in R$ and $(y, z) \in R$. Also $(x, z) \in S$ because S is transitive and $(x, y) \in S$ and $(y, z) \in S$. Thus by definition of intersection $(x, z) \in R \cap S$.

44. *a. $R \cup S$ is reflexive*: Suppose R and S are reflexive. *[To show that $R \cup S$ is reflexive, we must show that $\forall x \in A$, $(x, x) \in R \cup S$.]* So suppose $x \in A$. Since R is reflexive, $(x, x) \in R$, and since S is reflexive, $(x, x) \in S$. Thus by definition of union $(x, x) \in R \cup S$ *[as was to be shown]*.

c. $R \cup S$ is not necessarily transitive: As a counterexample, let $R = \{(0, 1)\}$ and $S = \{(1, 2)\}$. Then both R and S are transitive (by default), but $R \cup S = \{(0, 1), (1, 2)\}$ is not transitive because $(0, 1) \in R \cup S$ and $(1, 2) \in R \cup S$ but $(0, 2) \notin R \cup S$. As another counterexample, let $R = \{(x, y) \in \mathbf{R} \times \mathbf{R} \mid x < y\}$ and let $S = \{(x, y) \in \mathbf{R} \times \mathbf{R} \mid x > y\}$. Then both R and S are transitive because of the transitivity of order for the real numbers. But $R \cup S = \{(x, y) \in \mathbf{R} \times \mathbf{R} \mid x \neq y\}$ is not transitive because, for instance, $(1, 2) \in R \cup S$ and $(2, 1) \in R \cup S$ but $(1, 1) \notin R \cup S$.

46. R_2 is not irreflexive because $(0, 0) \in R_2$. R_2 is not asymmetric because $(0, 0) \in R_2$ and $(0, 0) \in R_2$. R_2 is not intransitive because $(0, 0) \in R_2$ and $(0, 1) \in R_2$ and $(0, 1) \in R_2$.

48. R_4 is irreflexive. R_4 is not asymmetric because $(1, 2) \in R_4$ and $(2, 1) \in R_4$. R_4 is intransitive.

49. R_5 is not irreflexive because $(0, 0) \in R_5$. R_5 is not asymmetric because $(0, 0) \in R_5$ and $(0, 0) \in R_5$. R_5 is not intransitive because $(0, 1) \in R_5$ and $(1, 2) \in R_5$ and $(0, 2) \in R_5$.

51. R_7 is irreflexive. R_7 is asymmetric. R_7 is intransitive (by default).

52. R_8 is not irreflexive because $(0, 0) \in R_8$. R_8 is not asymmetric because $(0, 0) \in R_8$ and $(0, 0) \in R_8$. R_8 is not intransitive because $(0, 0) \in R_8$ (so a counterexample is $x = y = z = 0$).

Section 10.3

2. *b.* $R = \{(0, 0), (1, 1), (1, 3), (1, 4), (3, 1), (3, 3), (3, 4), (4, 1)(4, 3), (4, 4), (2, 2)\}$

   c. $R =$
   $\{(0,0),(1,1),(1,2),(1,3),(1,4), (2,1),(2,2),(2,3),(2,4), (3,1),(3,2),(3,3),(3,4), (4,1),(4,2),(4,3),(4,4)\}$

4. distinct equivalence classes: $\{a\}$, $\{b, d\}$, $\{c\}$

6. distinct equivalence classes: $\{0, 3, -3\}$, $\{1, 4, -2\}$, $\{2, 5, -1, -4\}$

9. distinct equivalence classes: $\{\emptyset, \{0\}, \{1, -1\}, \{-1, 0, 1\}\}$, $\{\{1\}, \{0, 1\}\}$, $\{\{-1\}, \{0, -1\}\}$

11. distinct equivalence classes: $\{00\}$, $\{01, 10\}$, $\{02, 11, 20\}$, $\{12, 21\}$, $\{22\}$

12. distinct equivalence classes: $\{0, 3, -3\}$, $\{1, 4, -2, 2, -5, 5, -1, -4\}$

13. *b.* false   *c.* true   *d.* true

14. *b.* $[35] = [-7] = [0]$, $[3] = [17]$, $[12] = [-2]$

15. *b. Proof*: Suppose that m and n are integers such that $m \equiv n \pmod{d}$. *[We must show that m mod d = n mod d.]* By definition of congruence, $d \mid (m - n)$, and so by definition of divisibility $m - n = dk$ for some integer k. Let $m \bmod d = r$. Then $m = dl + r$ for some integer l. Since $m - n = dk$, then by substitution, $(dl + r) - n = dk$, or, equivalently, $n = d(l - k) + r$. Since $l - k$ is an integer, it follows by definition of *mod*, that $n \bmod d = r$ also, and so $m \bmod d = n \bmod d$ *[as was to be shown].*

Suppose that m and n are integers such that $m \bmod d = n \bmod d$. *[We must show that $m \equiv n \pmod{d}$.]* Let $r = m \bmod d = n \bmod d$. Then by definition of *mod*, $m = dp + r$ and $n = dq + r$ for some integers p and q. By substitution, $m - n = (dp + r) - (dq + r) = d(p - q)$. Since $p - q$ is an integer, it follows that $d \mid (m - n)$, and so by definition of congruence, $m \equiv n \pmod{d}$.

16. *b.* Let $A_1 = \{1, 2\}$, $A_2 = \{2, 3\}$, $x = 1$, $y = 2$, and $z = 3$. Then both x and y are in A_1 and both y and z are in A_2, but x and z are not both in either A_1 or A_2.

17. *b.* (1) *Proof:*

S is reflexive because for each student x at a college, x has the same age as x.

S is symmetric because for all students x and y at a college, if x is the same age as y then y is the same age as x.

S is transitive because for all students x, y, and z at a college, if x is the same age as y and y is the same age as z then x is the same age as z.

S is an equivalence relation because it is reflexive, symmetric, and transitive.

(2) There is one equivalence class for each age that is represented in the student body of your college. Each equivalence class consists of all the students of a given age.

18. (1) The solution given in Appendix B for exercise 15 in Section 10.2 showed that E is reflexive, symmetric, and transitive. Thus E is an equivalence relation.

19. (1) *Proof:*

F *is reflexive*: Suppose m is any integer. Since $m - m = 0$ and $4 \mid 0$, we have that $4 \mid (m - m)$. Consequently, $m \, F \, m$ by definition of F.

F *is symmetric*: Suppose m and n are any integers such that $m \, F \, n$. By definition of F this means that $4 \mid (m - n)$, and so, by definition of divisibility, $m - n = 4k$ for some integer k. Now $n - m = -(m - n)$. Hence by substitution, $n - m = -(4k) = 4 \cdot (-k)$. It follows that $4 \mid n - m$ by definition of divisibility (since $-k$ is an integer), and thus $n \, F \, m$ by definition of F.

F *is transitive*: Suppose m, n and p are any integers such that $m \, F \, n$ and $n \, F \, p$. By definition of F, this means that $4 \mid (m - n)$ and $4 \mid (n - p)$, and so, by definition of divisibility, $m - n = 4k$ for some integer k, and $n - p = 4l$ for some integer l. Now $m - p = (m - n) + (n - p)$. Hence by substitution, $m - p = 4k + 4l = 4(k + l)$. It follows that $4 \mid (m - p)$ by definition of divisibility (since $k + l$ is an integer), and thus $m \, F \, p$ by definition of F.

F is an equivalence relation because it is reflexive, symmetric, and transitive.

(2) Four distinct classes: $\{x \in \mathbf{Z} \mid x = 4k \text{ for some integer } k\}$, $\{x \in \mathbf{Z} \mid x = 4k + 1 \text{ for some integer } k\}$, $\{x \in \mathbf{Z} \mid x = 4k + 2 \text{ for some integer } k\}$, $\{x \in \mathbf{Z} \mid x = 4k + 3 \text{ for some integer } k\}$

20. (1) *Proof:*

$\mathscr{R}$ is reflexive because any statement form in three variables has the same truth table as itself.

$\mathscr{R}$ is symmetric because for all statement forms S and T in three variables, if S has the same truth table as T, then T has the same truth table as S.

$\mathscr{R}$ is transitive because for all statement forms S, T, and U in three variables, if S has the same truth table as T and T has the same truth table as U, then S has the same truth table as U.

$\mathscr{R}$ is an equivalence relation because it is reflexive, symmetric, and transitive.

(2) There are $2^8 = 256$ distinct equivalence classes, one for each distinct truth table for a statement form in three variables. Each equivalence class consists of all statement forms in three variables with a given truth table.

21. (1) *Proof:*

S is reflexive because for each part x in P, x has the same part number and is shipped from the same supplier as x.

S is symmetric because for all parts x and y in P, if x has the same part number and is shipped from the same supplier as y then y has the same part number and is shipped from the same supplier as x.

S is transitive because for all parts x, y, and z in P, if x has the same part number and is shipped from the same supplier as y and y has the same part number and is shipped from the same supplier as z then x has the same part number and is shipped from the same supplier as z.

S is an equivalence relation because it is reflexive, symmetric, and transitive.

(2) There are as many distinct equivalence classes as there are distinct ordered pairs of the form (n, s) where n is a part number and s is a supplier name and s supplies a part with the number n. Each equivalence class consists of all parts that have the same part number and are shipped from the same supplier.

24. (1) *Proof:*

D is reflexive: Suppose m is any integer. Since $m^2 - m^2 = 0$ and $3 \mid 0$, we have that $3 \mid (m^2 - m^2)$. Consequently, $m \, D \, m$ by definition of D.

D is symmetric: Suppose m and n are any integers such that $m \, D \, n$. By definition of D this means that $3 \mid (m^2 - n^2)$, and so, by definition of divisibility, $m^2 - n^2 = 3k$ for some integer k. Now $n^2 - m^2 = -(m^2 - n^2)$. Hence by substitution, $n^2 - m^2 = -(3k) = 3 \cdot (-k)$. It follows that $3 \mid (n^2 - m^2)$ by definition of divisibility (since $-k$ is an integer), and thus $n \, D \, m$ by definition of D.

D is transitive: Suppose m, n and p are any integers such that $m \, D \, n$ and $n \, D \, p$. By definition of D, this means that $3 \mid (m^2 - n^2)$ and $3 \mid (n^2 - p^2)$, and so, by definition of divisibility, $m^2 - n^2 = 3k$ for some integer k, and $n^2 - p^2 = 3l$ for some integer l. Now $m^2 - p^2 = (m^2 - n^2) + (n^2 - p^2)$. Hence by substitution, $m^2 - p^2 = 3k + 3l = 3(k + l)$. It follows that $3 \mid (m^2 - p^2)$ by definition of divisibility (since $k + l$ is an integer), and thus $m \, D \, p$ by definition of D.

D is an equivalence relation because it is reflexive, symmetric, and transitive.

(2) Since $m^2 - n^2 = (m - n)(m + n)$ for all integers m and n, $m \, D \, n \Leftrightarrow 3 \mid (m - n)$ or $3 \mid (m + n)$. Then by examining cases, one sees that $m \, D \, n \Leftrightarrow$ for some integers k and l either ($m = 3k$ and $n = 3l$) or ($m = 3k + 1$ and $n = 3l + 1$) or ($m = 3k + 1$ and $n = 3l + 2$) or ($m = 3k + 2$ and $n = 3l + 1$) or ($m = 3k + 2$ and $n = 3l + 2$). Therefore, there are two distinct equivalence classes $\{m \in \mathbf{Z} \mid m = 3k$ for some integer $k\}$ and $\{m \in \mathbf{Z} \mid m = 3k + 1$ or $m = 3k + 2$ for some integer $k\}$.

26. (1) *Proof:*

R is reflexive because for each identifier x in A, x has the same memory location as x.

R is symmetric because for all identifiers x and y in A, if x has the same memory location as y then y has the same memory location as x.

R is transitive because for all identifiers x, y, and z in A, if x has the same memory location as y and y has the same memory location as z then x has the same memory location as z.

R is an equivalence relation because it is reflexive, symmetric, and transitive.

(2) There are as many distinct equivalence classes as there are distinct memory locations that are used to store variables during execution of the program. Each equivalence class consists of all variables that are stored in the same location.

27. (1) *Proof:*

$\parallel$ is reflexive because for each point l in A, l is parallel to l.

$\parallel$ is symmetric because for all points l_1 and l_2 in A, if l_1 is parallel to l_2 then l_2 is parallel to l_1.

$\parallel$ is transitive because for all points l_1, l_2, and l_3 in A, if l_1 is parallel to l_2 and l_2 is parallel to l_3 then l_1 is parallel to l_3.

$\parallel$ is an equivalence relation because it is reflexive, symmetric, and transitive.

28. (1) *Proof:*

R is reflexive because for each point p in P, p lies on the same half-line emanating from the origin as p.

R is symmetric because for all points p_1 and p_2 in P, if p_1 lies on the same half-line emanating from the origin as p_2 then p_2 lies on the same half-line emanating from the origin as p_1.

R is transitive because for all points p_1, p_2, and p_3 in P, if p_1 lies on the same half-line emanating from the origin as p_2 and p_2 lies on the same half-line emanating from the origin as p_3 then p_1 lies on the same half-line emanating from the origin as p_3.

R is an equivalence relation because it is reflexive, symmetric, and transitive.

(2) There are as many distinct equivalence classes as there are points on a circle centered at the origin. Each equivalence class consists of all points that lie on the same half-line emanating from the origin.

29. The distinct equivalence classes can be identified with the points on a geometric figure, called a *torus*, that has the shape of the surface of a doughnut. Each point in the interior of the rectangle $\{(x, y) \mid 0 < x < 1 \text{ and } 0 < y < 1\}$ is only equivalent to itself. Each point on the top edge of the rectangle is in the same equivalence class as the point vertically below it on the bottom edge of the rectangle (so we can imagine identifying these points by gluing them together — this gives us a cylinder), and each point on the left edge of the rectangle is in the same equivalence class as the point horizontally across from it on the right edge of the rectangle (so we can also imagine identifying these points by gluing them together — this brings the two ends of the cylinder together to produce a torus).

32. *Proof:* Suppose R is an equivalence relation on a set A, a and b are in A, and $b \in [a]$. By definition of equivalence class, $b \ R \ a$. But since R is an equivalence relation, R is symmetric; hence $a \ R \ b$.

34. *Proof:* Suppose R is an equivalence relation on a set A, a and b are in A, and $[a] = [b]$. Since R is reflexive, $a \ R \ a$, and so by definition of class, $a \in [a]$. *[Alternatively, one could reference exercise 31 here.]* Since $[a] = [b]$, by definition of set equality, $a \in [b]$. But then by definition of equivalence class, $a \ R \ b$.

36. *Proof:* Suppose R is an equivalence relation on a set A, a and b are in A, and $a \in [b]$. By definition of class, $a \ R \ b$. We must show that $[a] = [b]$. To show that $[a] \subseteq [b]$, suppose $x \in [a]$. *[We must show that $x \in [b]$.]* By definition of class, $x \ R \ a$. By transitivity of R, since $x \ R \ a$ and $a \ R \ b$ then $x \ R \ b$. Thus by definition of class, $x \in [b]$ *[as was to be shown]* . To show that $[b] \subseteq [a]$, suppose $x \in [b]$. *[We must show that $x \in [a]$.]* By definition of class, $x \ R \ b$. But also

$a\ R\ b$, and so by symmetry, $b\ R\ a$. Thus since R is transitive and since $x\ R\ b$ and $b\ R\ a$, then $x\ R\ a$. Therefore, by definition of class, $x \in [a]$ *[as was to be shown]*. Since we have proved both subset relations $[a] \subseteq [b]$ and $[b] \subseteq [a]$, we conclude that $[a] = [b]$.

37. There are, of course, an infinite number of answers to this exercise. One simple approach is to use one of the circuits given in the exercise, adding two NOT-gates that cancel each other out, or adding an AND-gate and a circuit for, say, $Q \lor \sim Q$, or an OR-gate and a circuit for, say, $Q\land \sim Q$. Another approach is to play with the input-output table directly, looking at it as, for instance, the table for $\sim ((P \land Q) \lor (P \land \sim Q) \lor (\sim P \land Q))$. Some possible answers are shown below.
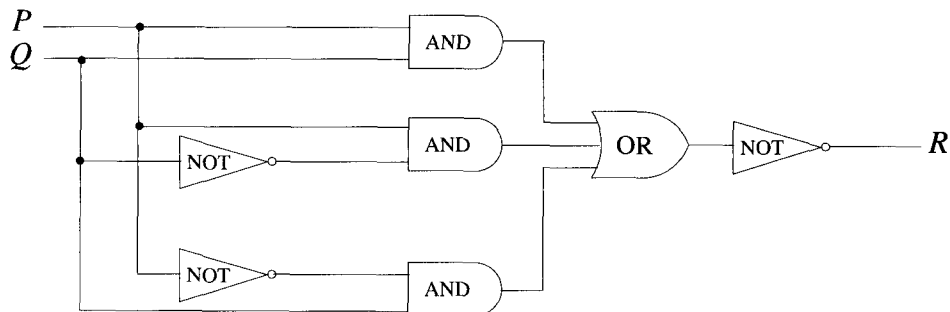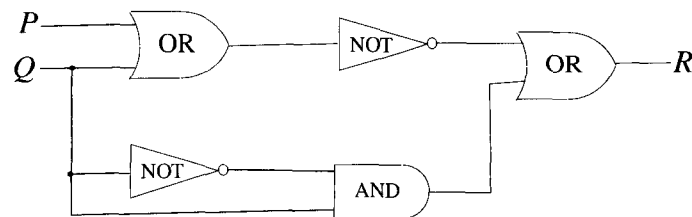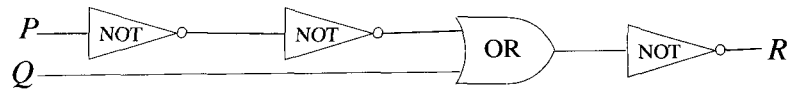
38. *a.* Suppose $(a, b) \in A$. By commutativity of multiplication for the real numbers, $ab = ba$. But then by definition of R, $(a, b)R(a, b)$.

   b. Suppose $(a, b), (c, d) \in A$ and $(a, b)R(c, d)$. By definition of R, $ad = bc$, and so by commutativity of multiplication for the real numbers and symmetry of equality, $cb = da$. But then by definition of R, $(c, d)R(a, b)$.

   d. For example, (2,5), (4,10), (-2,-5), and (6,15) are all in $[(2,5)]$.

39. *b. Proof:* Suppose (a, b), (a', b'), (c, d), and (c', d') are any elements of A such that $[(a, b)] = [(a', b')]$ and $[(c, d)] = [(c', d')]$. By definition of the relation, a, a', c, and c' are integers and b, b', d, and d' are nonzero integers, and $ab' = a'b$ (*) and $cd' = c'd$ (**). We must show that $[(a, b)] \cdot [(c, d)] = [(a', b')] \cdot [(c', d')]$. By definition of the multiplication, this equation holds if, and only if, $[(ac, bd)] = [(a'c', b'd')]$. And by definition of the relation, this equation holds if, and only if, $ac \cdot b'd' = bd \cdot a'c'$. (***) But multiplying equations (*) and (**) gives $ab' \cdot cd' = a'b \cdot c'd$. And by the associative and commutative laws for real numbers, this equation is equivalent to (***). Hence $[(a, b)] \cdot [(c, d)] = [(a', b')] \cdot [(c', d')]$.

   d. The identity element for multiplication is $[(1, 1)]$. To prove this, suppose (a, b) is any element of A. We must show that $[(a, b)] \cdot [(1, 1)] = [(a, b)]$. But by definition of the multiplication this

equation holds if, and only if, $[(a \cdot 1, b \cdot 1)] = [(a, b)]$. By definition of the relation, this equation holds if, and only if, $a \cdot 1 \cdot b = b \cdot 1 \cdot a$, and this equation holds for all integers a and b. Thus $[(a, b)] \cdot [(1, 1)] = [(a, b)]$ *[as was to be shown]*.

f. Given any $(a, b) \in A$ with $a \neq 0$, $[(b, a)]$ is an inverse for multiplication for $[(a, b)]$. To prove this, we must show that $[(a, b)] \cdot [(b, a)] = [(1, 1)]$, which (by part (d)) is the identity element for multiplication. But by definition of the multiplication, $[(a, b)] \cdot [(b, a)] = [(ab, ba)]$. And by definition of the relation, $[(ab, ba)] = [(1, 1)]$ if, and only if, $ab \cdot 1 = ba \cdot 1$, which is true for all integers a and b. Thus $[(a, b)] \cdot [(b, a)] = [(1, 1)]$ *[as was to be shown]*.

40. *b.* Let (a, b) and (c, d) be any elements of $A = \mathbf{Z}^+ \times \mathbf{Z}^+$, and suppose (a, b) R (c, d). *[We must show that (c, d) R (a, b)]*. By definition of R, $a + d = c + b$, and so by the symmetry property of equality, $c + b = a + d$. But then by definition of R, (c, d) R (a, b) *[as was to be shown]*.

    c. *Proof:* Let (a, b), (c, d), and (e, f) be any elements of $A = \mathbf{Z}^+ \times \mathbf{Z}^+$, and suppose (a, b) R (c, d) and (c, d) R (e, f). *[We must show that (a, b) R (e, f)]*. By definition of R, $a + d = c + b$ (*) and $c + f = e + d$ (**). Adding (*) and (**) together gives $a + d + c + f = c + b + e + d$, and subtracting $c + d$ from both sides gives $a + f = b + e$. Then by definition of R, (a, b) R (e, f) *[as was to be shown]*.

    e. *One possible answer:* $(4, 2), (5, 3), (6, 4), (7, 5), (8, 6)$

    f. *One possible answer:* $(2, 3), (3, 4), (4, 5), (5, 6), (6, 7)$

41. The given argument assumes that from the fact that the statement "$\forall x$ in A, if x R y then y R x" is true, it follows that given any element x in R, there must exist an element y in R such that x R y and y R x. This is false. For instance, consider the following binary relation R defined on $A = \{1, 2\}$: $R = \{(1, 1)\}$. This relation is symmetric and transitive, but it is not reflexive. Given $2 \in A$, there is no element y in A such that $(2, y) \in R$. Thus we cannot go on to use symmetry to say that $(y, 2) \in R$ and transitivity to conclude that $(2, 2) \in R$.

42. *Proof:* Suppose R is a binary relation on a set A, R is symmetric and transitive, and for every x in A there is a y in A such that x R y. Suppose x is any particular but arbitrarily chosen element of A. By hypothesis, there is a y in A such that x R y. By symmetry, y R x, and so by transitivity x R x. Therefore, R is reflexive. Since we already know that R is symmetric and transitive, we conclude that R is an equivalence relation.

43. *a.* Haddock's Eyes   *b.* The Aged Aged Man   *d.* A-sittin on a Gate

    This exercise follows up on the comment at the bottom of page 605. We may call an equivalence class by many different names depending on which of its elements we use to describe it when we use the equivalence class notation, but what the equivalence class *is* is the set of all its elements.

Section 10.4

2. *a.* DQ DSSOH D GDB

    b. KEEPS THE DOCTOR AWAY

4. *a.* The relation $7 \mid (68 - 33)$ is true because $68 - 33 = 35$ and $7 \mid 35$ (since $35 = 7 \cdot 5$).

    b. By definition of congruence modulo n, to show that $68 \equiv 33 \pmod 7$, one must show that $7 \mid (68 - 33)$, which was verified in part (a).

    c. To show that $68 = 33 + 7k$ for some integer k, one solves the equation for k and checks that the result is an integer. In this case, $k = (68 - 33)/7 = 5$, which is an integer. So $68 = 33 + 7 \cdot 5$.

d. When 68 is divided by 7, the remainder is 5 because $68 = 7 \cdot 9 + 5$. When 33 is divided by 7, the remainder is also 5 because $33 = 7 \cdot 4 + 5$. Thus 68 and 33 have the same remainder when divided by 7.

e. By definition, 68 *mod* 7 is the remainder obtained when 68 is divided by 7, and 33 *mod* 7 is the remainder obtained when 33 is divided by 7. In part (d) these two numbers were shown to be equal.

5. *Proof*: Suppose a, b and c and n are any integers with $n > 1$ and $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. By definition of congruence modulo n this means that $n \mid (a-b)$ and $n \mid (b-c)$, and so, by definition of divisibility, $a - b = nk$ for some integer k, and $b - c = nl$ for some integer l. Now $a - c = (a-b) + (b-c)$. Hence by substitution, $a - c = nk + nl = n(k+l)$. It follows that $n \mid (a-c)$ by definition of divisibility (since $k + l$ is an integer), and thus $a \equiv c \pmod{n}$ by definition of congruence modulo n.

6. *Proof*: Given any integer $n > 1$ and any integer a with $0 \leq a < n$, the notation $[a]$ denotes the equivalence class of a for the relation of congruence modulo n (Theorem 10.4.2). We first show that given any integer m, m is in one of the classes $[0], [1], [2], \ldots, [n-1]$. The reason is that, by the quotient-remainder theorem, $m = nk + a$, where k and a are integers and $0 \leq a < n$, and so, by Theorem 10.4.1, $m \equiv a \pmod{n}$. It follows by Lemma 10.3.2 that $[m] = [a]$. Next we use an argument by contradiction to show that all the equivalence classes $[0], [1], [2], \ldots, [n-1]$ are distinct. For suppose not. That is, suppose a and b are integers with $0 \leq a < n$ and $0 \leq b < n$, $a \neq b$, and $[a] = [b]$. Without loss of generality, we may assume that $a > b \geq 0$, which implies that $-a < -b \leq 0$. Adding a to all parts of the inequality gives $0 < a - b \leq a$. By Theorem 10.3.4, $[a] = [b]$ implies that $a \equiv b \pmod{n}$. Hence, by Theorem 10.4.1, $n \mid (a-b)$, and so, by Example 3.3.3, $n \leq a - b.$. But $a < n$. Thus $n \leq a - b \leq a < n$, which is contradictory. Therefore the supposition is false, and we conclude that all the equivalence classes $[0], [1], [2], \ldots, [n-1]$ are distinct.

8. *a.* $45 \equiv 3 \pmod{6}$ because $45 - 3 = 42 = 6 \cdot 7$, and $104 \equiv 2 \pmod{6}$ because $104 - 2 = 102 = 6 \cdot 17$

   b. $45 + 104 \equiv (3+2) \pmod{6}$ because $45 + 104 = 149$ and $3 + 2 = 5$ and $149 - 5 = 144 = 6 \cdot 24$

   c. $45 - 104 \equiv (3-2) \pmod{6}$ because $45 - 104 = -59$ and $3 - 2 = 1$ and $-59 - 1 = -60 = 6 \cdot (-10)$

   d. $45 \cdot 104 \equiv (3 \cdot 2) \pmod{6}$ because $45 \cdot 104 = 4680$ and $3 \cdot 2 = 6$ and $4680 - 6 = 4674 = 6 \cdot 779$

   e. $45^2 \equiv 3^2 \pmod{6}$ because $45^2 = 2025$ and $3^2 = 9$ and $2025 - 9 = 2016 = 6 \cdot 336$

10. *Proof*: Suppose a, b, c, d, and n are integers with $n > 1$, $a \equiv c \pmod{n}$, and $b \equiv d \pmod{n}$. By definition, $a - c = nr$ and $b - d = ns$ for some integers r and s. Then

$$(a-b) - (c-d) = (a-c) - (b-d) = nr - ns = n(r-s).$$

But $r - s$ is an integer, and so, by definition, $a - b \equiv (c-d) \pmod{n}$.

11. *Proof (by mathematical induction on m)*: Let a, c, and n be integers with $n > 1$ and $a \equiv c \pmod{n}$, and let the property $P(m)$ be the congruence $a^m \equiv c^m \pmod{n}$.

    Show that the property is true for $m = 1$ When $m = 1$, the congruence is $a^1 \equiv c^1 \pmod{n}$, which is true by assumption.

    Show that for all integers $k \geq 1$, if the property is true for $m = k$ then it is true for $m = k + 1$: Let k be an integer with $k \geq 1$, and suppose that $a^k \equiv c^k \pmod{n}$. *[This is the inductive hypothesis.]* We must show that $a^{k+1} \equiv c^{k+1} \pmod{n}$. But by assumption $a \equiv c \pmod{n}$, and by inductive hypothesis $a^k \equiv c^k \pmod{n}$. By 10.4.3(3), we can multiply the left- and right-hand sides of these two congruences together to obtain $a \cdot a^k \equiv c \cdot c^k \pmod{n}$, or, equivalently, $a^{k+1} \equiv c^{k+1} \pmod{n}$ *[as was to be shown]*.

12. *b.* *Proof*: Suppose a is a positive integer. Then $a = \sum_{k=0}^{n} d_k 10^k$, for some nonnegative integer n and integers d_k where $0 \le d_k < 10$ for all $k = 1, 2, \ldots, n$. By Theorem 10.4.3,

$$a = \sum_{k=0}^{n} d_k 10^k \equiv \sum_{k=0}^{n} d_k \cdot 1 \equiv \sum_{k=0}^{n} d_k (\bmod\, 9)$$

because, by part (a), each $10^k \equiv 1 \,(\bmod\, 9)$. Hence, by Theorem 10.4.1, both a and $\sum_{k=0}^{n} d_k$ have the same remainder upon division by 9, and thus if either one is divisible by 9, so is the other.

13. *a.* *Proof*: Let n be any positive integer. By definition of congruence modulo n, $10 \equiv -1 \,(\bmod\, 11)$ because $10 - (-1) = 11$ and $11 \mid 11$. Thus, by Theorem 10.4.3(4), $10^n \equiv (-1)^n (\bmod\, 11)$.

b. *Proof*: Suppose a is a positive integer. Then $a = \sum_{k=0}^{n} d_k 10^k$, for some nonnegative integer n and integers d_k where $0 \le d_k < 10$ for all $k = 1, 2, \ldots, n$. By Theorem 10.4.3,

$$a = \sum_{k=0}^{n} d_k 10^k \equiv \left(\sum_{k=0}^{n} d_k \cdot (-1)^k \right) (\bmod\, 11)$$

because, by part (a), each $10^k \equiv (-1)^k (\bmod\, 11)$. Hence, by Theorem 10.4.1, both a and $\sum_{k=0}^{n} d_k \cdot (-1)^k$ have the same remainder upon division by 11, and thus if either one is divisible by 11, so is the other.

17. $89^1 \bmod 713 = 89$

$89^2 \bmod 713 = 78$

$89^4 \bmod 713 = 78^2 \bmod 713 = 380$

$89^8 \bmod 713 = 380^2 \bmod 713 = 374$

$89^{16} \bmod 713 = 374^2 \bmod 713 = 128$

$89^{32} \bmod 713 = 128^2 \bmod 713 = 698$

$89^{64} \bmod 713 = 698^2 \bmod 713 = 225$

$89^{128} \bmod 713 = 225^2 \bmod 713 = 2$

$89^{256} \bmod 713 = 2^2 \bmod 713 = 4$

Hence, by Theorem 10.4.3, $89^{307} = 89^{256+32+16+2+1} = 89^{256} 89^{32} 89^{16} 89^2 89^1 \equiv 4 \cdot 698 \cdot 128 \cdot 78 \cdot 89 \equiv 15 \,(\bmod\, 713)$, and thus $89^{307} \bmod 713 = 15$.

18. $48^1 \bmod 713 = 48$

$48^2 \bmod 713 = 165$

$48^4 \bmod 713 = 165^2 \bmod 713 = 131$

$48^8 \bmod 713 = 131^2 \bmod 713 = 49$

$48^{16} \bmod 713 = 49^2 \bmod 713 = 262$

$48^{32} \bmod 713 = 262^2 \bmod 713 = 196$

$48^{64} \bmod 713 = 196^2 \bmod 713 = 627$

$48^{128} \bmod 713 = 627^2 \bmod 713 = 266$

$48^{256} \bmod 713 = 266^2 \bmod 713 = 169$

Hence, by Theorem 10.4.3, $48^{307} = 48^{256+32+16+2+1} = 48^{256} 48^{32} 48^{16} 48^2 48^1 \equiv 169 \cdot 196 \cdot 262 \cdot 165 \cdot 48 \equiv 12 \,(\bmod\, 713)$, and thus $48^{307} \bmod 713 = 12$.

20. The letters in WELCOME translate numerically into 23, 05, 12, 03, 15, 13, and 05. The solution for exercise 19 in Appendix B shows that E, L, and O are encrypted as 15, 23, and 20, respectively. To encrypt W, we compute $23^3 \bmod 55 = 12$, to encrypt C, we compute $3^3 \bmod 55 = 27$, and to encrypt M, we compute $13^3 \bmod 55 = 52$. So the ciphertext is 12 15 23 27 20 52 15. As noted in the answer to exercise 19, individual symbols in messages are normally grouped together in blocks during encryption so that deciphering cannot be accomplished through knowledge of frequency patterns of letters or words.

21. The letters in EXCELLENT translate numerically into 05, 24, 03, 05, 12, 12, 05, 14, 20. The solutions for exercises 19 and 20 in Appendix B and above show that E, L, and C are encrypted as 15, 23, and 27, respectively. To encrypt X, we compute $24^3 \bmod 55 = 19$, to encrypt N, we compute $14^3 \bmod 55 = 49$, and to encrypt T, we compute $20^3 \bmod 55 = 25$. So the ciphertext is 15 19 27 15 23 23 15 49 25.

23. By Example 10.4.10, the decryption key is 27. Thus the residues modulo 55 for 8^{27}, 5^{27}, and 15^{27} must be found and then translated into letters of the alphabet. Because $27 = 16+8+2+1$, we first perform the following computations:

$$
\begin{array}{lll}
8^1 \equiv 8 \ (\mathrm{mod}\,55) & 5^1 \equiv 5 \ (\mathrm{mod}\,55) & 15^1 \equiv 15 \ (\mathrm{mod}\,55) \\
8^2 \equiv 9 \ (\mathrm{mod}\,55) & 5^2 \equiv 25 \ (\mathrm{mod}\,55) & 15^2 \equiv 5 \ (\mathrm{mod}\,55) \\
8^4 \equiv 9^2 \equiv 26 \ (\mathrm{mod}\,55) & 5^4 \equiv 25^2 \equiv 20 \ (\mathrm{mod}\,55) & 15^4 \equiv 5^2 \equiv 25 \ (\mathrm{mod}\,55) \\
8^8 \equiv 26^2 \equiv 16 \ (\mathrm{mod}\,55) & 5^8 \equiv 20^2 \equiv 15 \ (\mathrm{mod}\,55) & 15^8 \equiv 25^2 \equiv 20 \ (\mathrm{mod}\,55) \\
8^{16} \equiv 16^2 \equiv 36 \ (\mathrm{mod}\,55) & 5^{16} \equiv 15^2 \equiv 5 \ (\mathrm{mod}\,55) & 15^{16} \equiv 20^2 \equiv 15 \ (\mathrm{mod}\,55)
\end{array}
$$

Then

$8^{27} \bmod 55 = (36 \cdot 16 \cdot 9 \cdot 8) \bmod 55 = 2,$

$5^{27} \bmod 55 = (5 \cdot 15 \cdot 25 \cdot 5) \bmod 55 = 25,$

$15^{27} \bmod 55 = (15 \cdot 20 \cdot 5 \cdot 15) \bmod 55 = 5.$

But 2, 25, and 5 translate into letters as B, Y, and E. So the message is BYE.

24. By Example 10.4.10, the decryption key is 27. Thus the residues modulo 55 for 51^{27}, 14^{27}, 49^{27}, and 15^{27} must be found and then translated into letters of the alphabet. Because $27 = 16 + 8 + 2 + 1$, we first perform the following computations:

$$
\begin{array}{lll}
51^1 \equiv 51 \ (\mathrm{mod}\,55) & 14^1 \equiv 14 \ (\mathrm{mod}\,55) & 49^1 \equiv 49 \ (\mathrm{mod}\,55) \\
51^2 \equiv 16 \ (\mathrm{mod}\,55) & 14^2 \equiv 31 \ (\mathrm{mod}\,55) & 49^2 \equiv 36 \ (\mathrm{mod}\,55) \\
51^4 \equiv 16^2 \equiv 36 \ (\mathrm{mod}\,55) & 14^4 \equiv 31^2 \equiv 26 \ (\mathrm{mod}\,55) & 49^4 \equiv 36^2 \equiv 31 \ (\mathrm{mod}\,55) \\
51^8 \equiv 36^2 \equiv 31 \ (\mathrm{mod}\,55) & 14^8 \equiv 26^2 \equiv 16 \ (\mathrm{mod}\,55) & 49^8 \equiv 31^2 \equiv 26 \ (\mathrm{mod}\,55) \\
51^{16} \equiv 31^2 \equiv 26 \ (\mathrm{mod}\,55) & 14^{16} \equiv 16^2 \equiv 36 \ (\mathrm{mod}\,55) & 49^{16} \equiv 26^2 \equiv 16 \ (\mathrm{mod}\,55)
\end{array}
$$

Then

$51^{27} \bmod 55 = (26 \cdot 31 \cdot 16 \cdot 51) \bmod 55 = 6,$

$14^{27} \bmod 55 = (36 \cdot 16 \cdot 31 \cdot 14) \bmod 55 = 9,$

$49^{27} \bmod 55 = (16 \cdot 26 \cdot 36 \cdot 49) \bmod 55 = 14.$

In addition, we know from the solution to exercise 23 above that $15^{27} \bmod 55 = 5$. But 6, 9, 14, and 5 translate into letters as F, I, N, and E. So the message is FINE.

25. *Proof*: Let a and n be positive integers such that $a^n - 1$ is prime. We will show that n is prime. Note that $a > 1$ because otherwise $a^n - 1$ would equal 0, which is not a prime number. By Theorem 4.2.3, using a in place of r and $n-1$ in place of n, we have that $1 + a + a^2 + \cdots + a^{n-1} = \dfrac{a^n - 1}{a - 1}$. Multiplying both sides by $a - 1$ gives $a^n - 1 = (a-1)(1 + a + a^2 + \cdots + a^{n-1})$. Because $a^n - 1$ is prime, one of these factors equals 1. The second factor is greater than 1 because a is

positive. Thus the first factor $a - 1 = 1$, and so $a = 2$. Next we prove by contradiction that n is prime. For suppose n is not prime, then $n = st$ where s and t are integers with $1 < s < n$ and $1 < t < n$. Then $a^n - 1 = a^{st} - 1 = (a^s)^t - 1$, and so, by Theorem 4.2.3 with a^s in place of r and $t - 1$ in place of n, $1 + a^s + a^{2s} + \cdots + a^{(t-1)s} = \dfrac{a^{ts} - 1}{a^s - 1}$. Multiplying both sides by $a^s - 1$ gives $a^n - 1 = (a^s - 1)(1 + a^s + a^{2s} + \cdots + a^{(t-1)s})$. But since $s > 1$ and $a > 1$, this equation implies that $a^n - 1$ is a product of two positive integer factors, neither of which is 1. Hence $a^n - 1$ is not prime, which contradicts the hypothesis that it is prime. Therefore we conclude that n is prime *[as was to be shown]*.

27. *Step 1:* $4158 = 1568 \cdot 2 + 1022$, and so $1022 = 4158 - 1568 \cdot 2$

Step 2: $1568 = 1022 \cdot 1 + 546$, and so $546 = 1568 - 1022$

Step 3: $1022 = 546 \cdot 1 + 476$, and so $476 = 1022 - 546$

Step 4: $546 = 476 \cdot 1 + 70$, and so $70 = 546 - 476$

Step 5: $476 = 70 \cdot 6 + 56$, and so $56 = 476 - 70 \cdot 6$

Step 6: $70 = 56 \cdot 1 + 14$, and so $14 = 70 - 56$

Step 7: $56 = 14 \cdot 4 + 0$, and so $\gcd(4158, 1568) = 14$,

which is the remainder obtained just before the final division.

Substitute back through steps 6–1:

$$14 = 70 - 56 = 70 - (476 - 70 \cdot 6) = 70 \cdot 7 - 476$$
$$= (546 - 476) \cdot 7 - 476 = 7 \cdot 546 - 8 \cdot 476$$
$$= 7 \cdot 546 - 8 \cdot (1022 - 546) = 15 \cdot 546 - 8 \cdot 1022$$
$$= 15 \cdot (1568 - 1022) - 8 \cdot 1022 = 15 \cdot 1568 - 23 \cdot 1022$$
$$= 15 \cdot 1568 - 23 \cdot (4158 - 1568 \cdot 2) = 61 \cdot 1568 - 23 \cdot 4158$$

(It is always a good idea to verify that no mistake has been made by verifying that the final expression really does equal the greatest common divisor. In this case, a computation shows that the answer is correct.)

29.

a	284	168	116	52	12	4
b	168	116	52	12	4	0
r		116	52	12	4	0
q		1	1	2	4	3
s	1	0	1	-1	3	-13
t	0	1	-1	2	-5	22
u	0	1	-1	3	-13	42
v	1	-1	2	-5	22	-71
$newu$		1	-1	3	-13	42
$newv$		-1	2	-5	22	-71
$sA + tB$	284	168	116	52	12	4

30. *Proof:* Suppose a and b are positive integers, $S = \{x \mid x \text{ is a positive integer and } x = as + bt$ for some integers s and $t\}$, and c is the least element of S. We will show that $c \mid b$. By the quotient-remainder theorem, $b = cq + r$ (*) for some integers q and r with $0 \le r < c$. Now because c is in S, $c = as + bt$ for some integers s and t. Thus, by substitution into equation (*), $r = b - cq = b - (as + bt)q = a(-sq) + b(1 - tq)$. Hence, by definition of S, either $r = 0$ or $r \in S$. But if $r \in S$, then $r \ge c$ because c is the least element of S, and thus both $r < c$ and $r \ge c$ would be true, which would be a contradiction. Therefore, $r \notin S$, and thus by elimination, we conclude that $r = 0$. It follows that $b - cq = 0$, or, equivalently, $b = cq$, and so $c \mid b$ *[as was to be shown]*.

32. *a. Step 1*: $660 = 41 \cdot 16 + 4$, and so $4 = 660 - 41 \cdot 16$.

   Step 2: $41 = 4 \cdot 10 + 1$, and so $1 = 41 - 4 \cdot 10$.

   Step 3: $4 = 1 \cdot 4 + 0$, and so $\gcd(660, 41) = 1$.

   Substitute back through steps 2–1:

   $$1 = 41 - (660 - 41 \cdot 16) \cdot 10 = 660 \cdot (-10) + 41 \cdot 161.$$

   Thus $41 \cdot 161 \equiv 1 \pmod{660}$, and so 161 is an inverse for 41 modulo 660.

   b. By part (a), $41 \cdot 161 \equiv 1 \pmod{660}$. Multiply both sides by 125 and apply Theorem 10.4.3 to obtain $41 \cdot 161 \cdot 125 \equiv 1 \cdot 125 \pmod{660}$, or, equivalently, $41 \cdot 20125 \equiv 125 \pmod{660}$. Thus a solution for $41x \equiv 125 \pmod{660}$ is $x = 20,125$. Now the the remainder obtained when $20,125$ is divided by 660 is 325, and so, by Theorem 10.4.1, $20125 \equiv 325 \pmod{660}$. But then, by Theorem 10.4.3, $41 \cdot 20125 \equiv 41 \cdot 325 \pmod{660}$. This shows that 325 is also a solution for the congruence, and because $0 \le 325 < 660$, 325 is the least positive solution for the congruence.

33. *Proof*: Suppose a, b, and c are integers such that $\gcd(a, b) = 1$, $a \mid c$, and $b \mid c$. We will show that $ab \mid c$. By Corollary 10.4.6 (or by Theorem 10.4.5), there exist integers s and t such that $as + bt = 1$. Also, by definition of divisibility, $c = au = bv$, for some integers u and v. Hence, by substitution, $c = asc + btc = as(bv) + bt(au) = ab(sv + tu)$. But $sv + tu$ is an integer, and so, by definition of divisibility, $ab \mid c$ *[as was to be shown]*.

34. *One counterexample among many*: Let $a = 2$, $b = 6$, and $c = 24$. Then $ab \mid c$ because $12 \mid 24$, but $\gcd(2, 6) \ne 1$, and so the following statement is false: $\gcd(a, b) = 1$ and $a \mid c$ and $b \mid c$.

37. The numeric equivalents of C, O, M, and E are 03, 15, 13, and 05. To encrypt these letters, the following quantities must be computed: $3^{43} \bmod 713$, $15^{43} \bmod 713$, $13^{43} \bmod 713$, and $5^{43} \bmod 713$. Note that $43 = 32 + 8 + 2 + 1$.

   C: $\quad 3 \equiv 3 \pmod{713}$
   $3^2 \equiv 9 \pmod{713}$
   $3^4 \equiv 9^2 \equiv 81 \pmod{713}$
   $3^8 \equiv 81^2 \equiv 144 \pmod{713}$
   $3^{16} \equiv 144^2 \equiv 59 \pmod{713}$
   $3^{32} \equiv 59^2 \equiv 629 \pmod{713}$
   Thus the ciphertext is
   $3^{43} \bmod 713$
   $\quad = (629 \cdot 144 \cdot 9 \cdot 3) \bmod 713 = 675.$

   O: $\quad 15 \equiv 15 \pmod{713}$
   $15^2 \equiv 225 \pmod{713}$
   $15^4 \equiv 225^2 \equiv 2 \pmod{713}$
   $15^8 \equiv 2^2 \equiv 4 \pmod{713}$
   $15^{16} \equiv 4^2 \equiv 16 \pmod{713}$
   $15^{32} \equiv 16^2 \equiv 256 \pmod{713}$
   Thus the ciphertext is
   $15^{43} \bmod 713$
   $\quad = (256 \cdot 4 \cdot 225 \cdot 15) \bmod 713 = 89.$

   M: $\quad 13 \equiv 13 \pmod{713}$
   $13^2 \equiv 169 \pmod{713}$
   $13^4 \equiv 169^2 \equiv 41 \pmod{713}$
   $13^8 \equiv 41^2 \equiv 255 \pmod{713}$
   $13^{16} \equiv 255^2 \equiv 142 \pmod{713}$
   $13^{32} \equiv 142^2 \equiv 200 \pmod{713}$
   Thus the ciphertext is
   $13^{43} \bmod 713$
   $\quad = (200 \cdot 255 \cdot 169 \cdot 13) \bmod 713 = 476.$

   E: $\quad 5 \equiv 5 \pmod{713}$
   $5^2 \equiv 25 \pmod{713}$
   $5^4 \equiv 625 \pmod{713}$
   $5^8 \equiv 625^2 \equiv 614 \pmod{713}$
   $5^{16} \equiv 614^2 \equiv 532 \pmod{713}$
   $5^{32} \equiv 532^2 \equiv 676 \pmod{713}$
   Thus the ciphertext is
   $5^{43} \bmod 713$
   $\quad = (676 \cdot 614 \cdot 25 \cdot 5) \bmod 713 = 129.$

   Therefore, the encrypted message is 675 089 476 129. (Again, note that, in practice, individual symbols are grouped together in blocks during encryption so that deciphering cannot be accomplished through knowledge of frequency patterns of letters or words. We kept them separate so that the numbers in the computations would be smaller and easier to work with.)

38. To check that 307 is an inverse for 43 modulo 660, we compute $307 \cdot 43 - 1 = 13200 = 660 \cdot 20$. Hence, by definition of the congruence relation, $307 \cdot 43 \equiv 1 \pmod{660}$.

40. By exercise 38, the decryption key, d, is 307. So to decrypt the message, the following quantities must be computed: $28^{307} \bmod 713$, $18^{307} \bmod 713$, $675^{307} \bmod 713$, and $129^{307} \bmod 713$. Note

that $307 = 256 + 32 + 16 + 2 + 1$. To obtain the other letters in the message we perform the following computations:

$28 \equiv 28 \pmod{713}$	$18 \equiv 18 \pmod{713}$	$129 \equiv 129 \pmod{713}$
$28^2 \equiv 71 \pmod{713}$	$18^2 \equiv 324 \pmod{713}$	$129^2 \equiv 242 \pmod{713}$
$28^4 \equiv 71^2 \equiv 50 \pmod{713}$	$18^4 \equiv 324^2 \equiv 165 \pmod{713}$	$129^4 \equiv 78^2 \equiv 98 \pmod{713}$
$28^8 \equiv 50^2 \equiv 361 \pmod{713}$	$18^8 \equiv 165^2 \equiv 131 \pmod{713}$	$129^8 \equiv 78^2 \equiv 335 \pmod{713}$
$28^{16} \equiv 361^2 \equiv 555 \pmod{713}$	$18^{16} \equiv 131^2 \equiv 49 \pmod{713}$	$129^{16} \equiv 78^2 \equiv 284 \pmod{713}$
$28^{32} \equiv 555^2 \equiv 9 \pmod{713}$	$18^{32} \equiv 49^2 \equiv 262 \pmod{713}$	$129^{32} \equiv 78^2 \equiv 87 \pmod{713}$
$28^{64} \equiv 9^2 \equiv 81 \pmod{713}$	$18^{64} \equiv 262^2 \equiv 196 \pmod{713}$	$129^{64} \equiv 78^2 \equiv 439 \pmod{713}$
$28^{128} \equiv 81^2 \equiv 144 \pmod{713}$	$18^{128} \equiv 196^2 \equiv 627 \pmod{713}$	$129^{128} \equiv 627^2 \equiv 211 \pmod{713}$
$28^{256} \equiv 144^2 \equiv 59 \pmod{713}$	$18^{256} \equiv 627^2 \equiv 266 \pmod{713}$	$129^{256} \equiv 266^2 \equiv 315 \pmod{713}$

Thus the decryption for 028 is

$28^{307} \bmod 713 = (28^{256+32+16+2+1}) \bmod 713$

$= (59 \cdot 9 \cdot 555 \cdot 71 \cdot 28) \bmod 713 = 14$, which corresponds to the letter N.

The decryption for 018 is

$18^{307} \bmod 713 = (18^{256+32+16+2+1}) \bmod 713$

$= (266 \cdot 262 \cdot 49 \cdot 324 \cdot 18) \bmod 713 = 9$, which corresponds to the letter I.

The answer to exercise 39 in Appendix B showed that the decryption for 675 is 3, which corresponds to the letter C.

The decryption for 129 is

$129^{307} \bmod 713 = (129^{256+32+16+2+1}) \bmod 713$

$= (315 \cdot 87 \cdot 284 \cdot 242 \cdot 129) \bmod 713 = 5$, which corresponds to the letter E.

Therefore, the decrypted message is NICE.

41. *a. Proof (by mathematical induction)*: Suppose p is a prime number. Let the property $P(s)$ be the sentence "If $q_1, q_2, \ldots, q_s$ are prime numbers and $p \mid q_1 q_2 \cdots q_s$, then $p = q_i$ for some integer i with $1 \leq i \leq s$.

Show that the property is true for $s = 1$ When $s = 1$, the sentence becomes "If q_1 is a prime number and $p \mid q_1$, then $p = q_1$." This is true because the only positive divisors of a prime number are 1 and itself and p cannot equal 1 because 1 is not prime."

Show that for all integers $k \geq 1$, if the property is true for $s = k$ then it is true for $s = k + 1$: Let k be an integer with $k \geq 1$, and suppose that if $q_1, q_2, \ldots, q_k$ are prime numbers and $p \mid q_1 q_2 \cdots q_k$, then $p = q_i$ for some i with $1 \leq i \leq k$. *[This is the inductive hypothesis.]* We must show that if $q_1, q_2, \ldots, q_{k+1}$ are prime numbers and $p \mid q_1 q_2 \cdots q_{k+1}$, then $p = q_i$ for some integer i with $1 \leq i \leq k + 1$. So suppose $q_1, q_2, \ldots, q_{k+1}$ are prime numbers and $p \mid q_1 q_2 \cdots q_{k+1}$. Let $a = q_1 q_2 \cdots q_k$. Then $p \mid a q_{k+1}$. In case $p = q_{k+1}$, we are done because we may take $i = k + 1$. In case $p \neq q_{k+1}$, $\gcd(p, q_{k+1}) = 1$ *[because both p and q_{k+1} are prime]*, and so, by Euclid's lemma, $p \mid a$, or, equivalently, $p \mid q_1 q_2 \cdots q_k$. Thus, by inductive hypothesis, $p = q_i$ for some integer i with $1 \leq i \leq k$. Hence, in either case, $p = q_i$ for some i with $1 \leq i \leq k + 1$. *[This is what was to be shown.]*

b. Proof by contradiction: Suppose not. That is, suppose n is an integer with $n > 1$, and suppose n has two different factorizations: $n = p_1 p_2 \cdots p_t = q_1 q_2 \cdots q_u$, where t and u are positive integers and $p_1, p_2, \cdots, p_t$, and $q_1, q_2, \cdots, q_u$ are prime numbers. Cancel out all factors that appear on both sides of the equation as many times as they appear on both sides. Then none of the factors on one side equal any of the factors on the other side. Either one side of the resulting equation equals 1 or at least one prime factor remains on each side. In the first case, we would have a prime number or a product of prime numbers equalling 1, which is impossible because all prime numbers are greater than 1. Thus we may eliminate this case and conclude that the resulting equation has the form $p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$, where r and s are positive integers and $p_j \neq q_i$ for any integers j and i. But this equation implies that

$p_1 \mid q_1 q_2 \cdots q_s$ because $p_1 \cdot (p_2 \cdots p_r) = q_1 q_2 \cdots q_s$ and $p_2 \cdots p_r$ is an integer. Hence, by part (a), $p_1 = q_i$ for some integer i with $1 \le i \le s$. We conclude that $p_1 = q_i$ and $p_1 \ne q_i$, which is a contradiction. Therefore, the supposition is false and so the prime factorization of n is unique except, possibly, for the order in which the prime factors are written.

42. *b.* When $a = 8$ and $p = 11$, $a^{p-1} = 8^{10} = 1 \equiv 1073741824 \pmod{11}$ because $1073741824 - 1 = 11 \cdot 97612893$.

43. *Two possible answers out of many*: (1) Let $a = 5$ and $p = 4$. Then $5^3 \equiv 1 \pmod 4$ because $5^3 - 1 = 4 \cdot 31$. (2) Let $a = 7$ and $p = 6$. Then $7^5 \equiv 1 \pmod 6$ because $7^5 - 1 = 6 \cdot 2801$.

45. To solve this problem, we need to find a positive integer x such that $x \equiv 2 \pmod{15}$, $x \equiv 1 \pmod{14}$, and $x \equiv 0 \pmod{13}$. We apply the technique in the proof of the Chinese remainder theorem with $n_1 = 15$, $n_2 = 14$, $n_3 = 13$, $a_1 = 2$, $a_2 = 1$, and $a_3 = 0$. Then $N = 15 \cdot 14 \cdot 13 = 2730$, $N_1 = 14 \cdot 13 = 182$, $N_2 = 15 \cdot 13 = 195$, and $N_3 = 15 \cdot 14 = 210$.

To find x_1, we solve $N_1 x_1 = 182 x_1 \equiv 1 \pmod{15}$. Now $182 = 15 \cdot 12 + 2$, and so $2 = 182 - 15 \cdot 12$. Also $15 = 2 \cdot 7 + 1$, and so $1 = 15 - 2 \cdot 7$. Hence, by substitution, $1 = 15 - (182 - 15 \cdot 12) \cdot 7 = 182 \cdot (-7) + 85 \cdot 15$, and so $182 \cdot (-7) \equiv 1 \pmod{15}$. Thus $x_1 \equiv -7 \pmod{15} \equiv 8 \pmod{15}$ because $15 \mid ((-7) - 8)$. So we may take $x_1 = 8$.

To find x_2, we solve $N_2 x_2 = 195 x_2 \equiv 1 \pmod{14}$. Now $195 = 14 \cdot 13 + 13$, and so $13 = 195 - 14 \cdot 13$. Also $14 = 1 \cdot 13 + 1$, and so $1 = 14 - 13$. Hence, by substitution, $1 = 14 - (195 - 14 \cdot 13) = 195 \cdot (-1) + 14 \cdot 14$, and so $195 \cdot (-1) \equiv 1 \pmod{14}$. Thus $x_2 \equiv -1 \pmod{14} \equiv 13 \pmod{14}$ because $14 \mid (-1 - 13)$. So we may take $x_2 = 13$.

To find x_3, we solve $N_3 x_3 = 210 x_3 \equiv 0 \pmod{13}$. Now $210 = 13 \cdot 16 + 2$, and so $2 = 210 - 13 \cdot 16$. Also $13 = 2 \cdot 6 + 1$, and so $1 = 13 - 2 \cdot 6$. Hence, by substitution, $1 = 13 - (210 - 13 \cdot 16) \cdot 6 = 210 \cdot (-6) + 97 \cdot 13$, and so $210 \cdot (-6) \equiv 1 \pmod{13}$. Thus $x_3 \equiv -6 \pmod{13} \equiv 7 \pmod{13}$ because $13 \mid (-6 - 7)$. So we may take $x_2 = 7$. (Strictly speaking, as you will see below, we did not need to calculate x_3 because $a_3 = 0$.)

By the proof of the Chinese remainder theorem, a solution x for the congruences is $x = a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 = 2 \cdot 182 \cdot 8 + 1 \cdot 195 \cdot 13 + 0 \cdot 210 \cdot 7 = 5447$. But $5447 \bmod 2730 = 2717$. Thus the least positive solution to the system of congruences is 2717. To check this answer, observe that $2717 = 15 \cdot 181 + 2$, $2717 = 14 \cdot 194 + 1$, and $2717 = 13 \cdot 209$.

46. To solve this problem, we need to find a positive integer x such that $x \equiv 1 \pmod 2$, $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 4$, $x \equiv 4 \pmod 5$, $x \equiv 5 \pmod 6$, and $x \equiv 0 \pmod 7$. Note first that if $x \equiv 1 \pmod 2$ and $x \equiv 2 \pmod 3$, then $x \equiv 5 \pmod 6$. We could obtain this result by formal application of the Chinese remainder theorem, but it is simpler to observe that because $x \equiv 2 \pmod 3$, $x = 3k + 2$ for some integer k, and because $x \equiv 1 \pmod 2$, x is odd. Now if k is even, then $x = 3k + 2$ is a sum of even integers and hence even, which it is not. Thus k is odd, and so $k = 2m + 1$ for some integer m. By substitution, $x = 3(2m + 1) + 2 = 6m + 5$. Hence $x \equiv 5 \pmod 6$. Secondly, observe that the congruence $x \equiv 3 \pmod 4$ implies that for some integer l, $x = 4l + 3 = 2(2l + 1) + 1$, which implies that $x \equiv 1 \pmod 2$. Thus it suffices to solve the system of congruences modulo 3, 4, 5, and 7. In other words, it suffices to find a positive integer x such that $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 4$, $x \equiv 4 \pmod 5$, and $x \equiv 0 \pmod 7$. Because 3, 4, 5, and 7 are relatively prime, we may apply the technique in the proof of the Chinese remainder theorem.

Let $n_1 = 3$, $n_2 = 4$, $n_3 = 5$, $n_4 = 7$, $a_1 = 2$, $a_2 = 3$, $a_3 = 4$, and $a_4 = 0$. Then $N = 3 \cdot 4 \cdot 5 \cdot 7 = 420$, $N_1 = 4 \cdot 5 \cdot 7 = 140$, $N_2 = 3 \cdot 5 \cdot 7 = 105$, $N_3 = 3 \cdot 4 \cdot 7 = 84$, $N_4 = 3 \cdot 4 \cdot 5 = 60$.

To find x_1, we solve $N_1 x_1 = 140 x_1 \equiv 1 \pmod 3$. Now $140 = 3 \cdot 46 + 2$, and so $2 = 140 - 3 \cdot 46$. Also $3 = 2 \cdot 1 + 1$, and so $1 = 3 - 2$. Hence, by substitution, $1 = 3 - (140 - 3 \cdot 46) = 140 \cdot (-1) + 3 \cdot 47$, and so $140 \cdot (-1) \equiv 1 \pmod 3$. Thus $x_1 \equiv -1 \pmod 3 \equiv 2 \pmod 3$ because $3 \mid ((-1) - 2)$. So we may take $x_1 = 2$.

To find x_2, we solve $N_2 x_2 = 105 x_2 \equiv 1 \pmod 4$. Now $105 = 4 \cdot 26 + 1$, and so $1 = 105 - 4 \cdot 26$. Hence, $105 \cdot 1 \equiv 1 \pmod 4$. Thus we may take $x_2 = 1$.

To find x_3, we solve $N_3 x_3 = 84 x_3 \equiv 1 \pmod 5$. Now $84 = 5 \cdot 16 + 4$, and so $4 = 84 - 5 \cdot 16$. Also $5 = 4 \cdot 1 + 1$, and so $1 = 5 - 4$. Hence, by substitution, $1 = 5 - (84 - 5 \cdot 16) = 84 \cdot (-1) + 5 \cdot 17$, and so $84 \cdot (-1) \equiv 1 \pmod 5$. Thus $x_3 \equiv -1 \pmod 5 \equiv 4 \pmod 5$ because $5 \mid ((-1) - 4)$. So we may take $x_3 = 4$.

Because $a_4 = 0$, we do not need to compute x_4. By the Chinese remainder theorem, a solution x for the congruences is $x = a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 + a_4 N_4 x_4 = 2 \cdot 140 \cdot 2 + 3 \cdot 105 \cdot 1 + 4 \cdot 84 \cdot 4 + 0 \cdot 60 \cdot x_4 = 2219$. But $2219 \bmod 420 = 119$. Thus the least positive solution to the system of congruences is 119. To check this answer, observe that $119 = 2 \cdot 59 + 1$, $119 = 3 \cdot 39 + 2$, $119 = 4 \cdot 29 + 3$, $119 = 5 \cdot 23 + 4$, $119 = 6 \cdot 19 + 5$, and $119 = 7 \cdot 17$.

47. *Lemma*: For all integers a, b, and c, if $a \mid c$, $b \mid c$, and $\gcd(a, b) = 1$, then $ab \mid c$.

Proof: Suppose a, b, and c are any integers such that $a \mid c$, $b \mid c$, and $\gcd(a, b) = 1$. By definition of divisibility, there exist integers x and y such that $c = ax = by$ (*), and by Theorem 10.4.5, there exist integers s and t such that $as + bt = 1$ (**). Multiplying both sides of equation (**) by c gives $(as + bt)c = 1 \cdot c = c$, and so $acs + cbt = c$ (***) Substituting from (*) into (***) gives $c = a(by)s + (ax)bt = ab(ys + xt)$, and this equation implies that $ab \mid c$ *[because $ys + xt$ is an integer]*.

Proof of exercise statement: Suppose n_1, n_2, n_3, are pairwise relatively prime positive integers and a_1, a_2, and a_3 are any integers, and suppose that x and x' are such that

$$x \equiv a_1 \pmod{n_1} \qquad x \equiv a_2 \pmod{n_2} \qquad x \equiv a_3 \pmod{n_3},$$
$$x' \equiv a_1 \pmod{n_1} \qquad x' \equiv a_2 \pmod{n_2} \qquad x' \equiv a_3 \pmod{n_3}.$$

We will show that $x \equiv x' \pmod n$, where $n = n_1 n_2 n_3$. First observe that by the symmetric and transitive properties of the congruence relation,

$$x \equiv x' \pmod{n_1} \qquad x \equiv x' \pmod{n_2} \qquad x \equiv x' \pmod{n_3}.$$

Thus $n_1 \mid (x - x')$, $n_2 \mid (x - x')$, and $n_3 \mid (x - x')$. Now because n_1 and n_2 are relatively prime, by the lemma, $n_1 n_2 \mid (x - x')$. Moreover, $n_1 n_2$ and n_3 are relatively prime and $n_1 n_2 \mid (x - x')$ and $n_3 \mid (x - x')$, and so, again by the lemma, $n_1 n_2 n_3 \mid (x - x')$. Letting $n = n_1 n_2 n_3$, by definition of divisibility we have that $n \mid (x - x')$, and so, by definition of congruence, $x \equiv x' \pmod n$. *[as was to be shown]*.

Section 10.5

1. *c.*
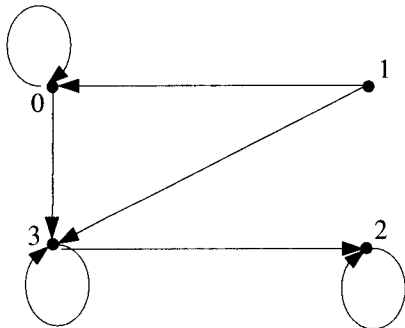
R_3 is antisymmetric: there are no cases where $a\ R\ b$ and $b\ R\ a$ and $a \neq b$.

d.
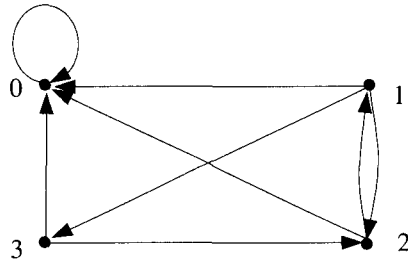
R_4 is not antisymmetric: $1\ R_4\ 2$ and $2\ R_4\ 1$ and $1 \neq 2$.

3. R is not antisymmetric. *Counterexample*: Let $s = 0$ and $t = 1$. Then $s\ R\ t$ and $t\ R\ s$ because $l(s) \leq l(t)$ and $l(t) \leq l(s)$, since both $l(s)$ and $l(t)$ equal 1, but $s \neq t$.

4. R is antisymmetric.

   Proof 1: The statement "For all real numbers x and y, if $x < y$ and $y < x$, then $x = y$" is vacuously true because, by the trichotomy law (Appendix A, T16), there are no real numbers x and y such that $x < y$ and $y < x$.

   Proof 2 (by contradiction): Suppose R is not antisymmetric. Then there exist distinct real numbers x and y such that $x < y$ and $y < x$. But this contradicts the trichotomy law (Appendix A, T16) which says that both $x < y$ and $y < x$ are not simultaneously true. *[Hence the supposition is false and so R is antisymmetric.]*

6. R is a partial order relation.

   Proof:

   R is reflexive: Suppose $r \in P$. Then $r = r$, and so by definition of R, $r\ R\ r$.

   R is antisymmetric: Suppose $r, s \in P$ and $r\ R\ s$ and $s\ R\ r$. *[We must show that $r = s$.]* By definition of R, either r is an ancestor of s or $r = s$ and either s is an ancestor of r or $s = r$. Now it is impossible for both r to be an ancestor of s and s to be an ancestor of r. Hence one of these conditions must be false, and so $r = s$ *[as was to be shown]*.

   R is transitive: Suppose $r, s, t \in P$ and $r\ R\ s$ and $s\ R\ t$. *[We must show that $r\ R\ t$.]* By definition of R, either r is an ancestor of s or $r = s$ and either s is an ancestor of t or $s = t$. In case r is an ancestor of s and s is an ancestor of t, then r is an ancestor of t, and so $r\ R\ t$. In case r is an ancestor of s and $s = t$, then r is an ancestor of t, and so $r\ R\ t$. In case $r = s$ and s is an ancestor of t, then r is an ancestor of t, and so $r\ R\ t$. In case $r = s$ and $s = t$, then $r = t$, and so $r\ R\ t$. Thus in all four possible cases, $r\ R\ t$ *[as was to be shown]*.

   Since R is reflexive, antisymmetric, and transitive, R is a partial order relation.

7. R is not a partial order relation because R is not antisymmetric. *Counterexample*: Let $m = 2$ and $n = 4$. Then $m\ R\ n$ because every prime factor of 2 is a prime factor of 4, and $n\ R\ m$ because every prime factor of 4 is a prime factor of 2. But $m \neq n$ because $2 \neq 4$.

9. R is not a partial order relation because R is not antisymmetric. *Counterexample*: Let $x = 2$ and $y = -2$. Then $x\ R\ y$ because $(-2)^2 \leq 2^2$, and $y\ R\ x$ because $2^2 \leq (-2)^2$. But $x \neq y$ because $2 \neq -2$.

11. *c*. True, by (3).   *d*. True, by (2).   *e*. False. By (2), $bbaa \preceq bbab$.
    f. True, by (1).   *g*. True, by (2).

12. *Proof*:

$\preceq$ *is reflexive*: Suppose s is in S. If $s = \epsilon$, then $s \preceq s$ by (3). If $s \neq \epsilon$, then $s \preceq s$ by (1). Hence in either case, $s \preceq s$.

$\preceq$ *is antisymmetric*: Suppose s and t are in S and $s \preceq t$ and $t \preceq s$. *[We must show that* $s = t$.] By definition of S, either $s = \epsilon$ or $s = a_1 a_2 \ldots a_m$ and either $t = \epsilon$ or $t = b_1 b_2 \ldots b_n$ for some positive integers m and n and elements $a_1, a_2, \ldots, a_m$ and $b_1, b_2, \ldots, b_n$ in A. It is impossible to have $s \preceq t$ by virtue of condition (2) because in that case there is no condition that would give $t \preceq s$. *[For suppose $s \preceq t$ by virtue of condition (2). Then for some integer k with $k \leq m$, $k \leq n$, and $k \geq 1$, $a_i = b_i$ for all $i = 1, 2, \ldots, k-1$, and $a_k R b_k$ and $a_k \neq b_k$. In this situation, it is clearly impossible for $t \preceq s$ by virtue either of condition (1) or (3), and so if $t \preceq s$, then it must be by virtue of condition (2). But in that case, since $a_k \neq b_k$, it must follow that $b_k R a_k$, and so since R is a partial order relation, $a_k = b_k$. However, this contradicts the fact that $a_k \neq b_k$. Hence it cannot be the case that $s \preceq t$ by virtue of condition (2).]* Similarly, it is impossible for $t \preceq s$ by virtue of condition (2). Hence $s \preceq t$ and $t \preceq s$ by virtue either of condition (1) or of condition (3). In case $s \preceq t$ by virtue of condition (1), then neither s nor t is the null string and so $t \preceq s$ by virtue of condition (1) also. Then by (1) $m \leq n$ and $a_i = b_i$ for all $i = 1, 2, \ldots, m$ and $n \leq m$ and $b_i = a_i$ for all $i = 1, 2, \ldots, m$, and so in this case $s = t$. In case $s \preceq t$ by virtue of condition (3), then $s = \epsilon$, and so since $t \preceq s$, $t \preceq \epsilon$. But the only condition that can give this result is (3) with $t = \epsilon$. Hence in this case, $s = t = \epsilon$. Thus in all possible cases, if $s \preceq t$ and $t \preceq s$, then $s = t$ *[as was to be shown]*.

$\preceq$ *is transitive*: Suppose s and t are in S and $s \preceq t$ and $t \preceq u$. *[We must show that $s \preceq u$.]* By definition of S, either $s = \epsilon$ or $s = a_1 a_2 \ldots a_m$, either $t = \epsilon$ or $t = b_1 b_2 \ldots b_n$, and either $u = \epsilon$ or $u = c_1 c_2 \ldots c_p$ for some positive integers m, n, and p and elements $a_1, a_2, \ldots, a_m$, $b_1, b_2, \ldots, b_n$, and $c_1, c_2, \ldots, c_p$ in A.

Case 1 ($s = \epsilon$): In this case, $s R u$ by (3).

Case 2 ($s \neq \epsilon$): In this case, since $s R t$, $t \neq \epsilon$ either, and since $t R u$, $u \neq \epsilon$ either.

Subcase a ($s R t$ and $t R u$ by condition (1)): Then $m \leq n$ and $n \leq p$ and $a_i = b_i$ for all $i = 1, 2, \ldots, m$ and $b_j = c_j$ for all $j = 1, 2, \ldots, n$. It follows that $a_i = c_i$ for all $i = i, 2, \ldots, m$, and so by (1), $s R u$.

Subcase b ($s R t$ by condition (1) and $t R u$ by condition (2)): Then $m \leq n$ and $a_i = b_i$ for all $i = 1, 2, \ldots, m$, and for some integer k with $k \leq n$, $k \leq p$, and $k \geq 1$, $b_j = c_j$ for all $j = 1, 2, \ldots, k-1$, $b_k R c_k$, and $b_k \neq c_k$. If $k \leq m$, then s and u satisfy condition (2) *[because $a_i = b_i$ for all $i = 1, 2, \ldots, m$ and so $k \leq m$, $k \leq p$, $k \geq 1$, $a_i = b_i = c_i$ for all $i = 1, 2, \ldots, k-1$, $a_k R c_k$, and $a_k \neq c_k$]*. If $k > m$, then s and u satisfy condition (1) *[because $a_i = b_i = c_i$ for all $i = 1, 2, \ldots, m$]*. Thus in either case $s R u$.

Subcase c ($s R t$ by condition (2) and $t R u$ by condition (1)): Then for some integer k with $k \leq m$, $k \leq n$, $k \geq 1$, $a_i = b_i$ for all $i = 1, 2, \ldots, k-1$, $a_k R b_k$, and $a_k \neq b_k$, and $n \leq p$ and $b_j = c_j$ for all $j = i, 2, \ldots, n$. Then s and u satisfy condition (2) *[because $k \leq n$, $k \leq p$ (since $k \leq n$ and $n \leq p$), $k \geq 1$, $a_i = b_i = c_i$ for all $i = 1, 2, \ldots, k-1$ (since $k-1 < n$), $a_k R c_k$ (since $b_k = c_k$ because $k \leq n$), and $a_k \neq c_k$ (since $b_k = c_k$ and $a_k \neq b_k$)]*. Thus $s R u$.

Subcase d ($s R t$ by condition (2) and $t R u$ by condition (2)): Then for some integer k with $k \leq m$, $k \leq n$, $k \geq 1$, $a_i = b_i$ for all $i = 1, 2, \ldots, k-1$, $a_k R b_k$, and $a_k \neq b_k$, and for some integer l with $l \leq n$, $l \leq p$, and $l \geq 1$, $b_j = c_j$ for all $j = 1, 2, \ldots, l-1$, $b_l R c_l$, and $b_l \neq c_l$. If $k < l$, then $a_i = b_i = c_i$ for all $i = 1, 2, \ldots, k-1$, $a_k R b_k$, $b_k = c_k$ (in which case $a_k R c_k$), and $a_k \neq c_k$ (since $a_k \neq b_k$). Thus if, $k < l$, then $s \preceq u$ by condition (2). If $k = l$, then $b_k R c_k$ (in which case $a_k R c_k$ by transitivity of R) and $b_k \neq c_k$. It follows that $a_k \neq c_k$ *[for if $a_k = c_k$, then $a_k R b_k$ and $b_k R a_k$, which implies that $a_k = b_k$ (since R is a partial order) and contradicts the fact that $a_k \neq b_k$]*. Thus if $k = l$, then $s \preceq u$ by condition (2). If $k > l$, then $a_i = b_i = c_i$ for all $i = 1, 2, \ldots, l-1$, $a_l R c_l$ (because $b_l R c_l$ and $a_l = b_l$), $a_l \neq c_l$ (because $b_l \neq c_l$ and $a_l = b_l$). Thus if $k > l$, then $s \preceq u$ by condition (2). Hence in all cases $s \preceq u$.

The above arguments show that in all possible cases, $s \preceq u$ *[as was to be shown]*. Hence $\preceq$ *is* transitive.

Since $\preceq$ *is* reflexive, antisymmetric, and transitive, $\preceq$ *is* a partial order relation.

14. *b.* $\{(a,a),(b,b),(c,c)\}$, $\{(a,a),(b,b),(c,c),(a,b)\}$,
$\{(a,a),(b,b),(c,c),(a,c)\}$, $\{(a,a),(b,b),(c,c),(a,b),(a,c)\}$,
$\{(a,a),(b,b),(c,c),(a,b),(b,c),(a,c)\}$, $\{(a,a),(b,b),(c,c),(a,c),(c,b),(a,b)\}$,
$\{(a,a),(b,b),(c,c),(b,c)\}$, $\{(a,a),(b,b),(c,c),(c,b)\}$,
$\{(a,a),(b,b),(c,c),(a,b),(c,b)\}$, $\{(a,a),(b,b),(c,c),(a,c),(b,c)\}$

15. *Proof*: Suppose R is a relation on a set A and R is reflexive, symmetric, transitive, and antisymmetric. We will show that R is the identity relation on A. First note that for all x and y in A, if $x \, R \, y$ then, because R is symmetric, $y \, R \, x$. But then, because R is also anti-symmetric $x = y$. Thus for all x and y in A, if $x \, R \, y$ then $x = y$. This argument, however, does not prove that R is the identity relation on A because the conclusion would also follow from the hypothesis (by default) in the case where $A \neq \emptyset$ and $R = \emptyset$. But when $A \neq \emptyset$, it is impossible for R to equal $\emptyset$ because R is reflexive, which means that $x \, R \, x$ for every x in A. Thus every element in A is related by R to itself, and no element in A is related to anything other than itself. It follows that R is the identity relation on A.

16. *b.*
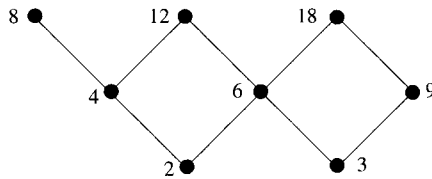
17. *b.*
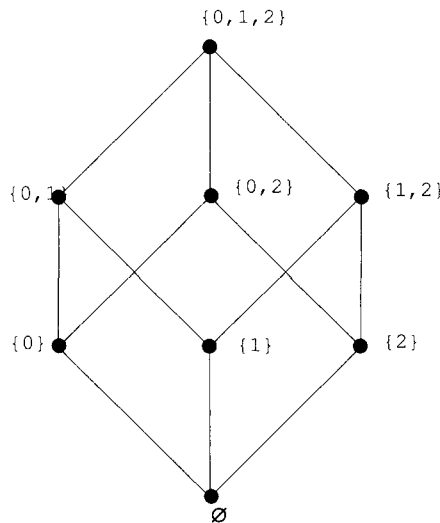
19.
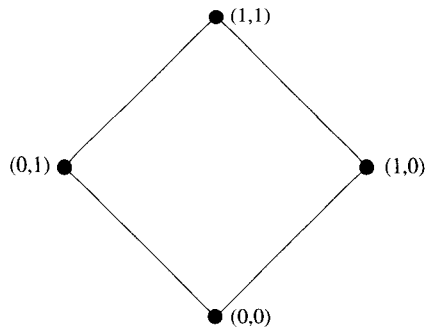
20.
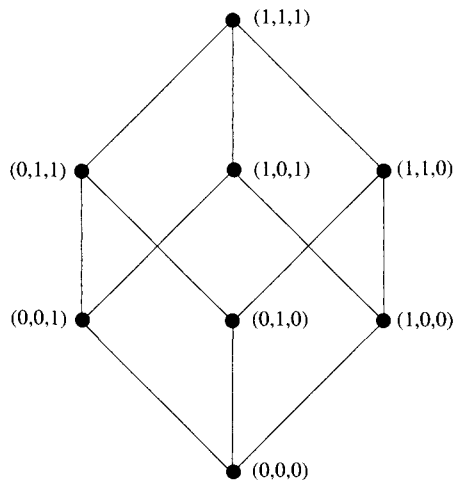
23. greatest element: none   least element: none
    maximal elements: 8, 12, 18   minimal elements: 2, 3

25. greatest element: $\{0, 1, 2\}$ least element: $\emptyset$
    maximal elements: $\{0, 1, 2\}$ minimal elements: $\emptyset$

27. greatest element: (1,1)   least element: (0,0)
    maximal elements: (1,1)   minimal elements: (0,0)

28. greatest element: (1,1,1)   least element: (0,0,0)
    maximal elements: (1,1,1)   minimal elements: (0,0,0)

29. greatest element: 2^n least element: 1
    maximal elements: 2^n minimal elements: 1

30. *c.* no greatest element and no least element
    d. greatest element: 9   least element: 1

32. R is a total order on A because it is reflexive, antisymmetric, and transitive (so it is a partial order) and because $[c, b, a, d]$ is a chain that contains every element of A.

33. A is not totally ordered by the given relation because $9 \nmid 12$ and $12 \nmid 9$.

34. There are $n!$ total orderings on a set with n elements because $n!$ is the number of ways to write n elements in a row or as a chain.

35. *Proof*: Let R' be the restriction of R to B. Then R' is reflexive because given any x in B, $(x,x) \in R$ since R is reflexive and $B \subseteq A$, and so $(x,x) \in R'$ by definition of R'. Furthermore, R' is antisymmetric because given any x and y in B such that $(x,y) \in R'$ and $(y,x) \in R'$, then $(x,y) \in R$ and $(y,x) \in R$ by definition of R' and since R is antisymmetric, $x = y$. Finally, R' is transitive because given any x, y, and z in B such that $(x,y) \in R'$ and $(y,z) \in R'$, then by definition of R', $(x,y) \in R$ and $(y,z) \in R$. Since R is transitive, $(x,z) \in R$, and so by definition of R', $(x,z) \in R'$. Since R' is reflexive, antisymmetric, and transitive, R' is a partial order relation on B.

37. $\{2, 4, 12, 24\}$ or $\{3, 6, 12, 24\}$

38. $\{(0,0), (0,1), (1,1)\}$ or $\{(0,0), (1,0), (1,1)\}$

41. *b*. This proof is identical to that given in part (a) provided the following changes are made: (1) Change "minimal" to "maximal" throughout the entire proof; (2) Change " $\preceq$ " to " $\succeq$ " and " $\succeq$ " to " $\preceq$ " throughout step 2 of the proof.

42. *a. Proof*: Suppose A is any partially ordered set, ordered with respect to a relation $\preceq$, and a and b are greatest elements of A. By definition of greatest element, $x \preceq a$ for all x in A; in particular, $b \preceq a$. Similarly, $x \preceq b$ for all x in A, and so $a \preceq b$. Since $\preceq$ *is* a partial order, it is antisymmetric, and thus $a = b$. Hence A has at most one greatest element.

   b. Proof: Suppose A is any partially ordered set, ordered with respect to a relation $\preceq$, and a and b are least elements of A. By definition of least element, $a \preceq x$ for all x in A; in particular, $a \preceq b$. Similarly, $b \preceq x$ for all x in A, and so $b \preceq a$. Since $\preceq$ *is* a partial order, it is antisymmetric, and thus $a = b$. Hence A has at most one least element.

44.
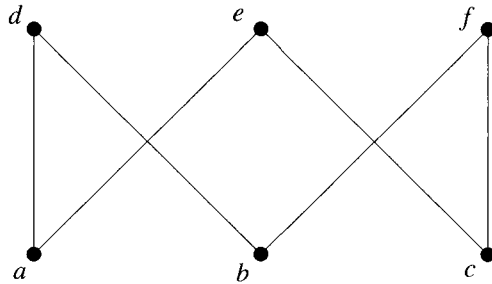
46. One such total order is 3,9,2,6,18,4,12,8.

48. One such total order is $(0,0,0),(0,0,1),(0,1,0),(0,1,1),(1,0,0),(1,0,1),(1,1,0),(1,1,1)$.

49. One such total order is $\emptyset, \{a\}, \{b\}, \{c\}, \{d\}, \{a,b\}, \{a,c\}, \{a,d\}, \{b,c\}, \{b,d\}, \{c,d\},$
    $\{a,b,c\}, \{a,b,d\}, \{a,c,d\}, \{b,c,d\}, \{a,b,c,d\}.$

50. *a*. 350, 390, 345, 301, 230, 200

   b. (1) 140, 150, 155, 141, 200, 225, 250, 230, 300, 340, 345, 301, 360, 390, 350

   (2) 150, 155, 200, 140, 141, 225, 300, 340, 345, 250, 360, 301, 230, 390, 350

51. *b.* (i) Annotate the given Hasse diagram by indicating in boxes the least number of days needed to accomplish each job, taking into account the time needed to perform prerequisite jobs.

$$
\begin{array}{c}
\boxed{5} \\
3 \bullet \\
\boxed{4}\ 7\bullet \qquad \boxed{2}\ \bullet 8 \\
\boxed{2}\ 10\bullet \qquad \boxed{4}\ \bullet 4 \\
\boxed{3}\ \bullet 5 \qquad 2\ \bullet\ \boxed{1} \\
\boxed{1}\ \bullet 9 \quad \bullet 6\ \boxed{2} \\
1\ \bullet \\
\boxed{1}
\end{array}
$$
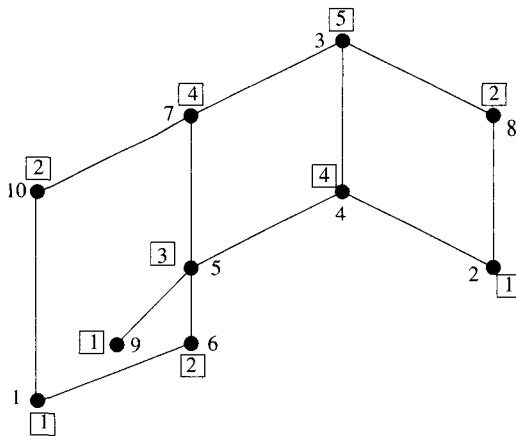
Therefore, at least five days are needed to perform all ten jobs.

(ii) At most four jobs can be performed at the same time. For instance, 10, 9, 6 and 2 could be performed simultaneously. One way to see why the maximum cannot be greater than four is to observe that S can be written as a union of four chains: $1 \preceq 10 \preceq 7 \preceq 3$, $1 \preceq 6 \preceq 5 \preceq 7 \preceq 3$, $9 \preceq 5 \preceq 4 \preceq 3$, and $2 \preceq 8 \preceq 3$, and at most one job from each chain can be performed at any one time.

52. *a.* 33 hours

Chapter 11: Graphs and Trees

The first section of this chapter introduces the terminology of graph theory, illustrating it in a variety of different instances. Several exercises are designed to clarify the distinction between a graph and a drawing of a graph. You might point out to students the advantage of the formal definition over the informal drawing for computer representation of graphs. Other exercises explore the use of graphs to solve problems of various sorts. In some cases, students may be able to solve the given problems, such as the wolf, the goat, the cabbage and the ferryman, more easily without using graphs than using them. The point to make is that such problems *can* be solved using graphs and that for more complex problems involving, say, hundreds of possible states, a graphical representation coupled with a computer path-finding algorithm makes it possible find a solution that could not be discovered by trial-and-error alone. Exercise 33, on the number of edges of a complete graph, is good to assign because discussing the variety of solutions provides a way to illustrate the relations among different branches of discrete mathematics. The rest of the exercises in this section give students practice in applying the theorem that relates the total degree of a graph to the number of its edges, especially for exploring properties of simple graphs, complete graphs, and bipartite graphs.

In Section 11.2 the general topic of paths and circuits is discussed, including the notion of connectedness and Euler and Hamiltonian circuits. As throughout the chapter, an attempt is made to balance the presentation of theory and application so that you can create whatever mix seems most appropriate for your students. Thus while many exercises are designed to develop facility with terminology and the use of theorems, quite a few others provide opportunities for students to engage in the kind of reasoning that lies behind the theorems.

Section 11.3 introduces the concept of the adjacency matrix of a graph. The main theorem of the section states that the ijth entry of the kth power of the adjacency matrix equals the number of walks of length k from the ith to the jth vertices in the graph. Matrix multiplication is defined and explored in this section in a way that is intended to be adequate for students who have never seen the definition before but also provide some challenge to students who were exposed to the topic in high school.

The concept of graph isomorphism is discussed in Section 11.4. In this section the main theorem gives a list of isomorphic invariants that can be used to determine the non-isomorphism of two graphs. The theoretical exercises at the end of this section give students an opportunity to fill in the parts of the proof of this theorem that are not included in the text.

The last two sections of the chapter deal with the subject of trees. Section 11.5 is rather long. In addition to definitions, examples, and theorems giving necessary and sufficient conditions for graphs to be trees, the section also contains the definition of rooted tree, binary tree, and the theorems that relate the number of internal to the number of terminal vertices of a full binary tree and the maximum height of a binary tree to the number of its terminal vertices. Section 11.6 on spanning trees contains Kruskal's and Prim's algorithms and proofs of their correctness, as well as applications of minimum spanning trees.

Section 11.1

2. $V(G) = \{v_1, v_2, v_3, v_4\}$, $E(G) = \{e_1, e_2, e_3, e_4, e_5\}$

   edge-endpoint function:

edge	endpoints
e_1	$\{v_1, v_2\}$
e_2	$\{v_2, v_3\}$
e_3	$\{v_2, v_3\}$
e_4	$\{v_2, v_4\}$
e_5	$\{v_4\}$

4.

6.

7.   *or*
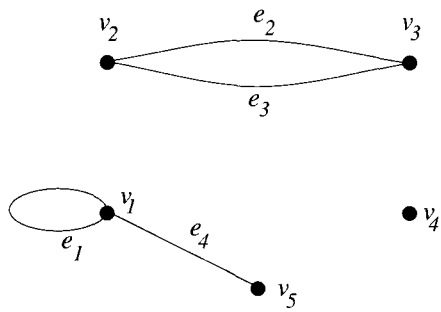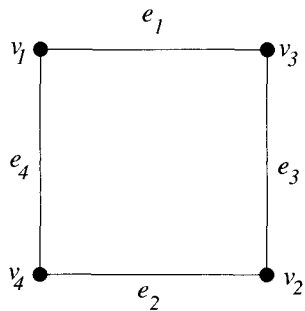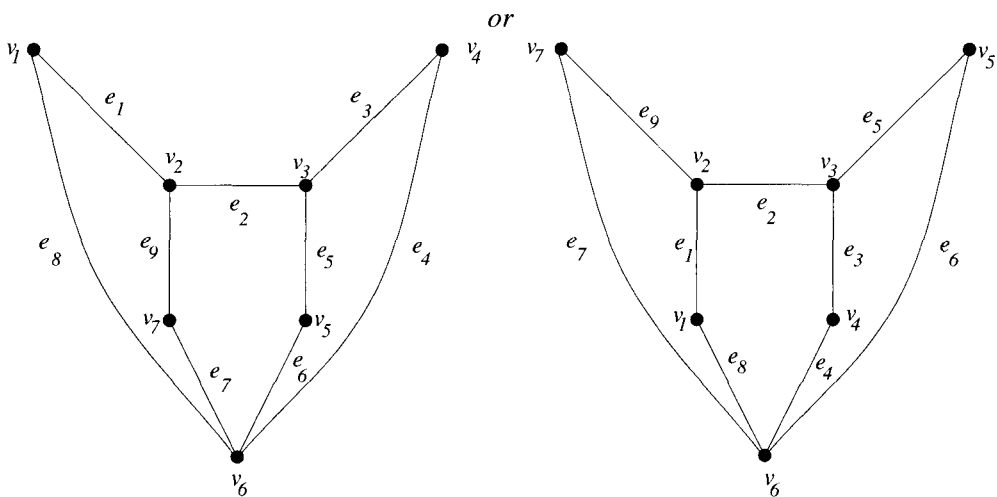
9. (i) e_1, e_2, e_7 are incident on e_1.

(ii) v_1 and v_2 are adjacent to v_3.

(iii) e_2 and e_7 are adjacent to e_1.

(iv) e_1 and e_3 are loops.

(v) e_4 and e_5 are parallel.

(vi) v_4 is an isolated vertex.

(vii) degree of $v_3 = 2$

(viii) total degree of the graph $= 14$

10. *b.* Yes. According to the graph, *Poetry Magazine* is an instance of a Literary journal which is a Scholarly journal and, therefore, contains Long words.

11.

$$(vvccB/) \rightarrow (vc/Bvc) \rightarrow (vvcB/c) \rightarrow (c/Bvvc) \rightarrow (vcB/vc) \rightarrow (/Bvvcc)$$
$$(vvccB/) \rightarrow (vv/Bcc) \rightarrow (vvcB/c) \rightarrow (c/Bvvc) \rightarrow (vcB/vc) \rightarrow (/Bvvcc)$$
$$(vvccB/) \rightarrow (vv/Bcc) \rightarrow (vvcB/c) \rightarrow (c/Bvvc) \rightarrow (ccB/vv) \rightarrow (/Bvvcc)$$

13.
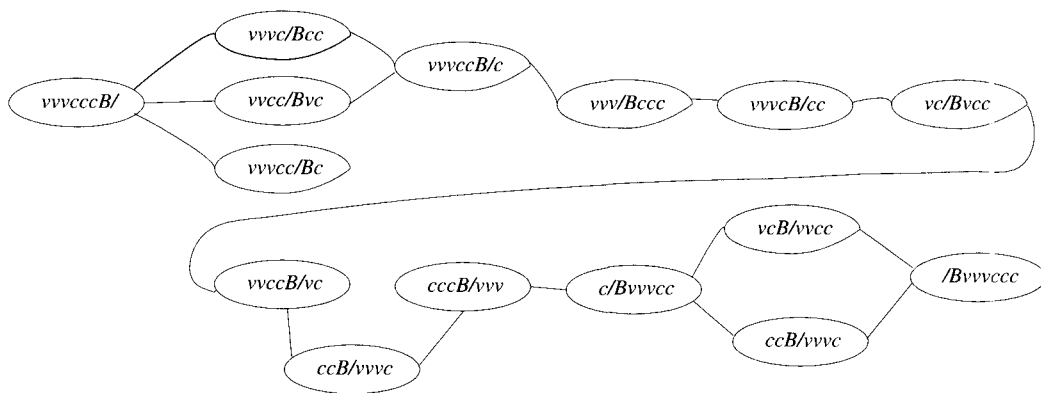
The diagram shows several solutions. Among them is $(vvvcccB/) \rightarrow (vvcc/Bvc) \rightarrow (vvvccB/c)$ $\rightarrow (vvv/Bccc) \rightarrow (vvvcB/cc) \rightarrow (vc/Bvvcc) \rightarrow (vvcB/vc) \rightarrow (cc/Bvvvc) \rightarrow (cccB/vvv)$ $\rightarrow (c/Bvvvcc) \rightarrow (vcB/vvcc) \rightarrow (/Bvvvccc)$, or one can end with $(c/Bvvvcc) \rightarrow (ccB/vvvc)$ $\rightarrow (/Bvvvccc)$, or one can start with $(vvvcccB/) \rightarrow (vvvc/Bcc) \rightarrow (vvvccB/c)$.

14. Represent possible amounts of water in jugs A and B by ordered pairs with, say, the ordered pair (1,3) indicating that there is one quart of water in jug A and three quarts in jug B. Starting with (0,0), draw an edge from one ordered pair to another if it is possible to go from the situation represented by the one pair to that represented by the other and back by either filling a jug from the tap, emptying a jug into the drain, or transferring water from one jug to another. Except for (0,0), only draw edges from states that have edges incident on them (since these are the only states that can be reached). The resulting graph is shown as follows:
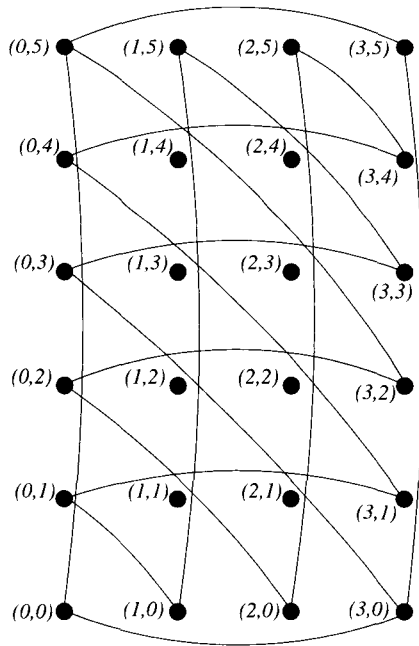
It is clear from the graph that one solution is $(0,0) \to (3,0) \to (0,3) \to (3,3) \to (1,5) \to (1,0)$ and another solution is $(0,0) \to (0,5) \to (3,2) \to (0,2) \to (2,0) \to (2,5) \to (3,4) \to (0,4) \to (3,1) \to (0,1)$.

Note that it would be possible to add arrows to the above graph from each reachable state to each other state that could be obtained from it either by filling one of the jugs to the top or by emptying the entire contents of one of the jugs. For instance, one could draw an arrow from (0,3) to (0,5) or from (0,3) to (0,0). Because the graph is connected, all such arrows would point to states already reachable by other means, so that it is not necessary to add such additional arrows to find solutions to the problem (and it makes the diagram look more complicated). However, if the problem were to find all possible solutions, the arrows would have to be added.

17. *Solution 1*: If there were a graph with four vertices of degrees 1, 1, 1 and 4, then its total degree would be 7, which is odd, which would contradict Corollary 11.1.2. Thus there is no such graph.

    Solution 2: If there were a graph with four vertices of degrees 1, 1, 1 and 4, then it would have three vertices of odd degree, which would contradict Corollary 11.1.3. Thus there is no such graph.

18.
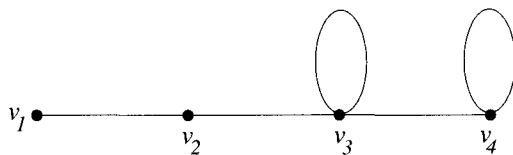
20. Since a simple graph has no loops or parallel edges, the maximum number of edges incident on a vertex equals the number of other vertices in the graph (because the vertex can only be connected to these and only once each). In a simple graph with five vertices, therefore, the maximum degree of any vertex is four, and so there can be no vertex of degree 5. Thus there is no simple graph with five vertices of degrees 2, 3, 3, 3, and 5.

21.
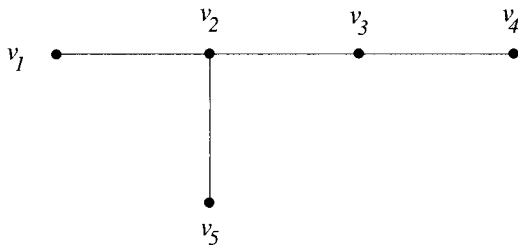
23. Let us first deduce what we can about such a graph. Its total degree would be two times the number of edges, or 18, and since each vertex would have degree 3, the number of vertices would be 18/3, or 6. Two graphs that satisfy the given properties are shown below.
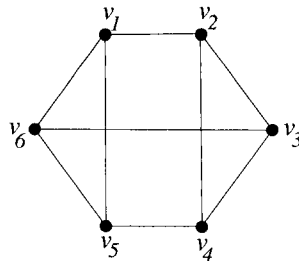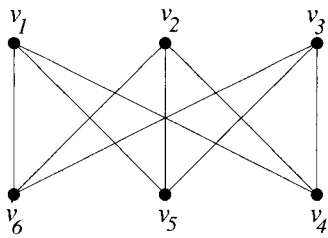
24. *b.* There are 7 nonempty subgraphs.
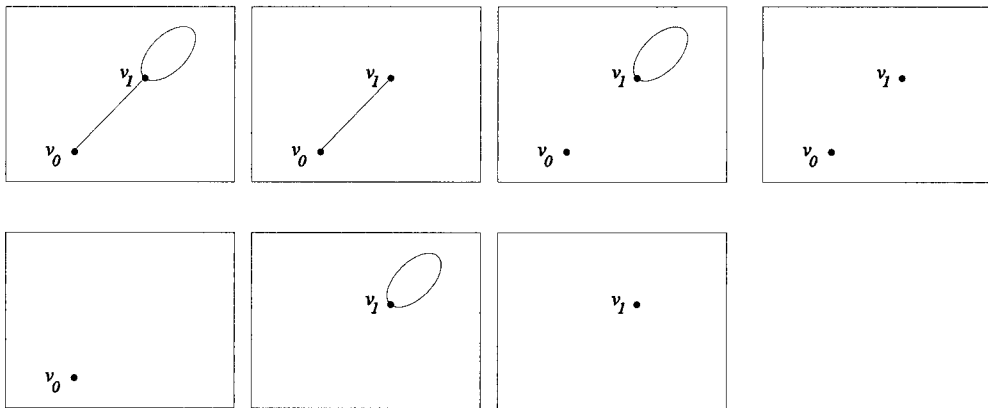
c. There are 17 nonempty subgraphs.
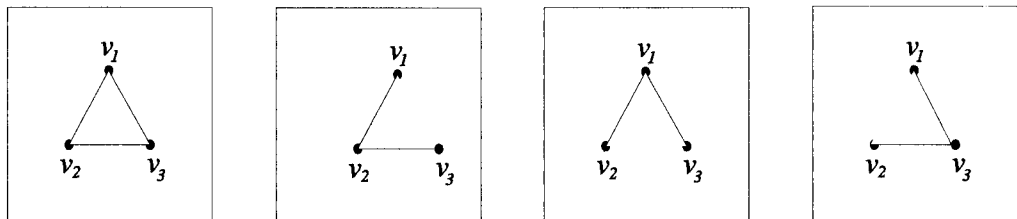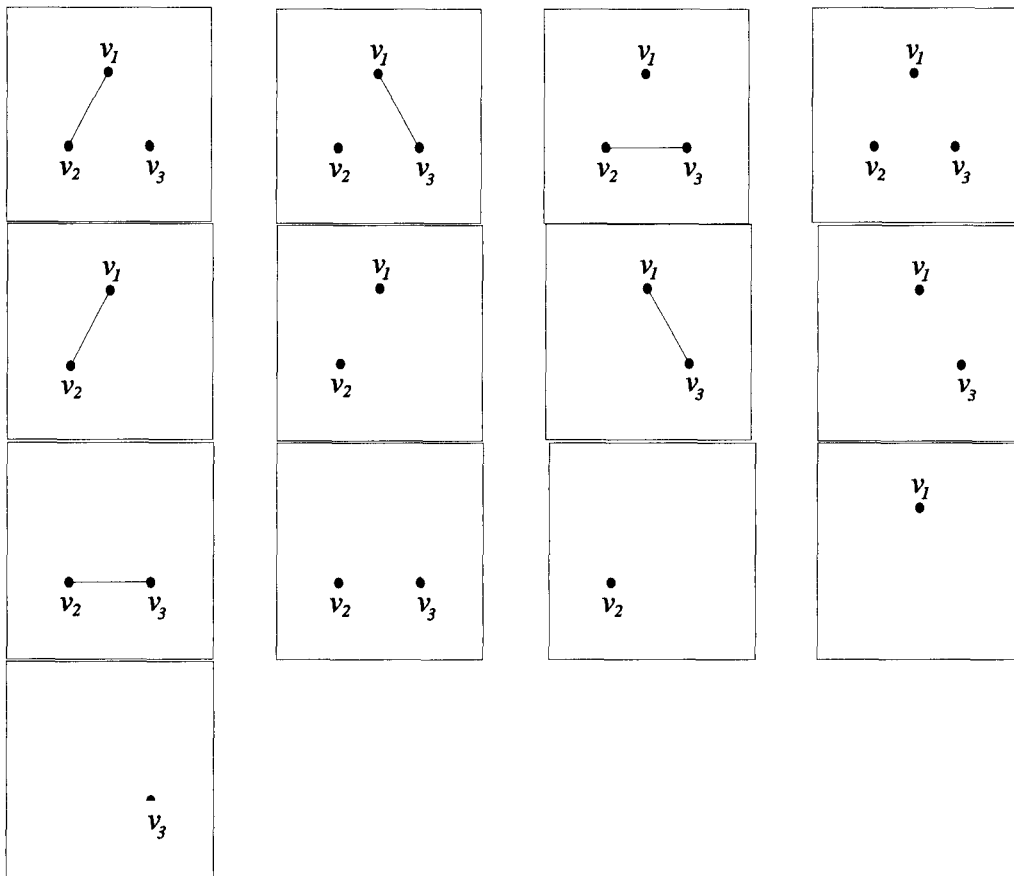
25. *b.* Yes. Each could be friends with all three others.

26. No. If the people were represented by vertices of a graph and each handshake were represented by an edge joining two vertices, the result would be a graph with a total degree of 75, which is odd. But this is impossible because the total degree of a graph must be even.

27. Yes. For example, the graph shown below satisfies this condition.
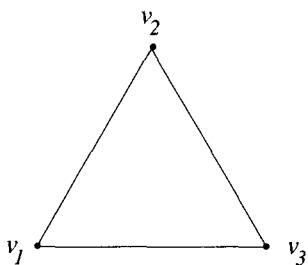
29. The total degree of the graph is $1 + 1 + 4 + 4 + 6 = 16$. So by Theorem 11.1.1, the number of edges is $16/2$, or 8.

30. Let t be the total degree of the graph. Since the degree of each vertex is at least $d_{\min}$ and at most $d_{\max}$, $d_{\min} \cdot v \le t \le d_{\max} \cdot v$. But by Theorem 11.1.1, t equals twice the number of edges. So by substitution, $d_{\min} \cdot v \le 2e \le d_{\max} \cdot v$.

32. *Proof:* Suppose not. That is, suppose there exists a positive integer n such that there is a sum of n odd integers that is even and n is not even. By Theorem 3.6.2, n is odd. Thus, by exercise 31, any sum of n odd integers is odd, which contradicts the supposition that there is

a sum of n odd integers that is even. *[Hence the supposition is false, and the given statement is true.]*

33. *b. Proof 1:* Suppose n is an integer with $n \geq 1$ and K_n is a complete graph on n vertices. If $n = 1$, then K_n has one vertex and 0 edges and $\frac{n(n-1)}{2} = \frac{1(1-1)}{2} = 0$, and so K_n has $\frac{n(n-1)}{2}$ edges. If $n \geq 2$, then since each pair of distinct vertices of K_n is connected by exactly one edge, there are as many edges in K_n as there are subsets of size two of the set of n vertices. By Theorem 6.4.1, there are $\binom{n}{2}$ such sets. But $\binom{n}{2} = \frac{n!}{2!(n-2)!} = \frac{n(n-1)}{2}$. Hence there are $\frac{n(n-1)}{2}$ edges in K_n.

Proof 2 (by mathematical induction): Let the property $P(n)$ be the sentence "the complete graph on n vertices, K_n, has $\frac{n(n-1)}{2}$ edges."

Show that the property is true for $n = 1$: For $n = 1$ the property is true because the complete graph on one vertex, K_1, has 0 edges and $\frac{n(n-1)}{2} = \frac{1(1-1)}{2} = 0$.

Show that for all integers $m \geq 1$, if the property is true for $n = m$ then it is true for $n = m + 1$: Let m be an integer with $m \geq 1$, and suppose that K_m has $\frac{m(m-1)}{2}$ edges. *[This is the inductive hypothesis.]* We must show that K_{m+1} has

$$\frac{(m+1)((m+1)-1)}{2} = \frac{(m+1)m}{2}$$

edges. Note that K_{m+1} vertices can be obtained from K_m vertices by adding one vertex, say v, and connecting v to each of the k other vertices. But by inductive hypothesis, K_m has $\frac{m(m-1)}{2}$ edges. Connecting v to each of the m other vertices adds another m edges. Hence the total number of edges of K_{m+1} is $\frac{m(m-1)}{2} + m = \frac{m(m-1)}{2} + \frac{2m}{2} = \frac{m^2 - m + 2m}{2} = \frac{m(m+1)}{2}$ *[as was to be shown]*.

Proof 3: Suppose n is an integer with $n \geq 1$ and K_n is a complete graph on n vertices. Because each vertex of K_n is connected by an edge to each of the other $n - 1$ vertices of K_n by exactly one edge, the degree of each vertex of K_n is $n - 1$. Thus the total degree of K_n equals the number of vertices times the degree of each vertex, or $n(n - 1)$. But by Theorem 11.1.1, the total degree of K_n equals twice the number e of edges of K_n, and so $n(n-1) = 2e$. Equivalently, $e = n(n - 1)/2$, *[as was to be shown]*.

34. *Proof:* Let n be a positive integer and let G be any simple graph with n vertices. Add edges to G to connect any pairs of vertices not already connected by an edge of G. The result is a complete graph on n vertices which has $n(n - 1)/2$ edges by exercise 33. Hence the number of edges of G is at most $n(n - 1)/2$.

36. *b.* $K_{1,3}$
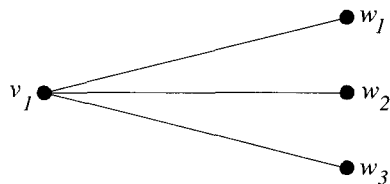
c. $K_{3,4}$
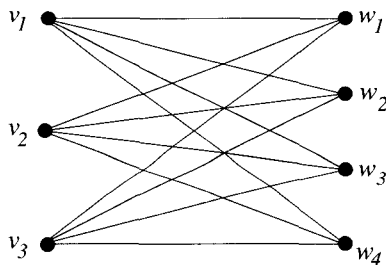
d. If $n \neq m$, the vertices of $K_{m,n}$ are divided into two groups: one of size m and the other of size n. Every vertex in the group of size m has degree n because each is connected to every vertex in the group of size n. So $K_{m,n}$ has n vertices of degree m. Similarly, every vertex in the group of size n has degree m because each is connected to every vertex in the group of size m. So $K_{m,n}$ has n vertices of degree m. Note that if $n = m$, then all $n + m = 2n$ vertices have the same degree, namely n.

e. The total degree of $K_{m,n}$ is $2mn$ because $K_{m,n}$ has m vertices of degree n (which contribute mn to its total degree) and n vertices of degree m (which contribute another mn to its total degree)

f. The number of edges of $K_{m,n} = mn$. The reason is that the total degree of $K_{m,n}$ is $2mn$, and so, by Theorem 11.1.1, $K_{m,n}$ has $2mn/2 = mn$ edges. Another way to reach this conclusion is to say that $K_{m,n}$ has n edges coming out of each of the group of m vertices (each leading to a vertex in the group of n vertices) for a total of mn edges. Equivalently, $K_{m,n}$ has m edges coming out of each of the group of n vertices (each leading to a vertex in the group of m vertices) for a total of mn edges.

37. *c.*
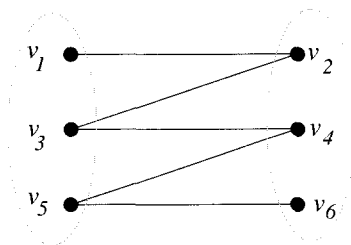
d. Suppose the graph were bipartite with disjoint vertex sets V_1 and V_2, where no vertices within either V_1 or V_2 are connected by edges. Then v_1 would be in one of the sets, say V_1, and so v_2 and v_6 would be in V_2 (because each is connected by an edge to v_1). Furthermore, v_3, v_4, and v_5 would be in V_1 (because all are connected by edges to v_2). But v_4 is connected by an edge to v_5, and so both cannot be in V_1. This contradiction shows that the supposition is false, and so the graph is not bipartite.

e.
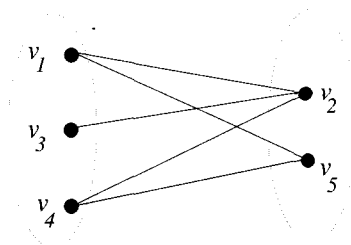
f. Suppose the graph were bipartite with disjoint vertex sets V_1 and V_2, where no vertices within either V_1 or V_2 are connected by edges. Then v_1 would be in one of the sets, say V_1, and so v_2 and v_5 would be in V_2 (because each is connected by an edge to v_1). Furthermore, v_3 and v_4 would be in V_1 (because v_3 is connected by an edge to v_2 and v_4 is connected by an edge to v_5). But v_3 is connected by an edge to v_4, and so both cannot be in V_1. This contradiction shows that the supposition is false, and so the graph is not bipartite.

38. Yes. Given positive integers r and s, let G be the complete bipartite graph $K_{r,s}$. If $r \neq s$, then G has r vertices of degree s, s vertices of degree r, and no vertices of any other degree. If $r = s$, then G has $2r$ vertices, all of degree r, and no vertices of any other degree.

39. *b.*
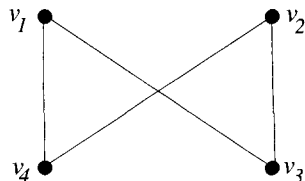
40. *a.*

b.

41. *a.*
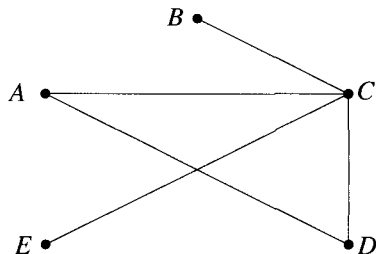
42. The graph obtained by taking all the vertices and edges of G together with all the edges of G' is K_n. Therefore, by exercise 33b, the number of edges of G plus the number of edges of G' equals $n(n-1)/2$.

43. Represent each person at the party by a vertex of an acquaintance graph and draw an edge connecting each pair of acquaintances. By assumption, the graph has at least two vertices. If

the acquaintance graph has at least one edge, then the people represented by the endpoints of that edge are acquaintances. If the acquaintance graph has no edges, then its complement has at least one edge (because the graph has at least two vertices), and we may choose such an edge. Then the people represented by the endpoints of that edge are mutual strangers.

44. *a.* Yes. Let G be a simple graph with n vertices and let v be a vertex of G. Since G has no parallel edges, v can be joined by at most a single edge to each of the $n-1$ other vertices of G, and since G has no loops, v cannot be joined to itself. Therefore, the maximum degree of v is $n-1$.

b. No. Suppose there is a simple graph with four vertices each of which has a different degree. By part (a), no vertex can have degree greater than three, and, of course, no vertex can have degree less than 0. Therefore, the only possible degrees of the vertices are 0, 1, 2, and 3. Since all four vertices have different degrees, there is one vertex with each degree. But then the vertex of degree 3 is connected to all the other vertices, which contradicts the fact that one of the vertices has degree 0. Hence the supposition is false, and there is no simple graph with four vertices each of which has a different degree.

c. No. Suppose there is a simple graph with n vertices (where $n \geq 2$) each of which has a different degree. By part (a), no vertex can have degree greater than $n-1$, and, of course, no vertex can have degree less than 0. Therefore, the only possible degrees of the vertices are 0, 1, 2,..., $n-1$. Since the vertices all have different degrees, there are n vertices, and there are n integers from 0 to $n-1$ inclusive, there is one vertex with each degree. But then the vertex of degree $n-1$ is connected to all the other vertices, which contradicts the fact that one of the vertices has degree 0. Hence the supposition is false, and there is no simple graph with n vertices each of which has a different degree.

45. Yes. Suppose that in a group of two or more people, each person is acquainted with a different number of people. Then the acquaintance graph representing the situation is a simple graph in which all the vertices have different degrees. But by exercise 44(c) such a graph does not exist. Hence the supposition is false, and so in a group of two or more people there must be at least two people who are acquainted with the same number of people within the group.

46. In the graph below each committee name is represented as a vertex and labeled with the first letter of the name of the committee. Vertices are joined if, and only if, the corresponding committees have a member in common.
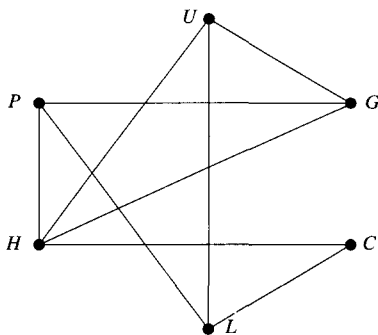
To the first time slot, assign a committee whose vertex has maximal degree. There is only one choice, the hiring committee. Since the library committee has no members in common with the hiring committee, assign it to meet in the first time slot also. Every other committee shares a member with the hiring committee and so cannot meet during the first time slot. To the second time slot, assign a committee that has not already been scheduled and whose vertex has next highest degree. This will be either the personnel, undergraduate education, or graduate education committee. Say the personnel committee is selected. The committees that have not already been scheduled and that do not share a member with the personnel committee are the

undergraduate education and the colloquium committees. So assign these to the second time slot also. To the third time slot, assign a committee that has not already been scheduled and whose vertex has next highest degree. Only the graduate education committee satisfies this condition. The time slots of all the committee meetings are as follows.

> Time 1: hiring, library
>
> Time 2: personnel, undergraduate education, colloquium
>
> Time 3: graduate education

Note that if the graduate education committee is chose in step 2, the result is as follows.

> Time 1: hiring, library
>
> Time 2: graduate education, colloquium
>
> Time 3: personnel, undergraduate education

Section 11.2

2. *a.* just a walk, not a path or a circuit

   b. simple circuit

   c. just a closed walk, not a path or a circuit (has a repeated edge)

   d. circuit, not a simple circuit

   e. path, not a simple path, not a circuit

   f. simple path

3. *b.* No, because $e_1 e_2$ could refer either to $v_1 e_1 v_2 e_2 v_1$ or to $v_2 e_1 v_1 e_2 v_2$.

5. *a.* The number of simple paths from a to c is 4 *[the number of ways to choose an edge to travel from a to b].*

   b. The number of paths from a to c is $4 + 4 \cdot 3 \cdot 2 = 28$. (In addition to the 4 simple paths from a to c, there are $4 \cdot 3 \cdot 2$ paths with vertices $ababc$. The reason is that there are 4 edges to choose from to go from a to b, then 3 edges to choose from to return from b to a, and finally 2 edges to choose from to go from a to b before traveling along the edge that joins b to c.)

   c. There are infinitely many walks from a to c because it is possible to travel back and forth from a to b or from b to c an arbitrarily large number of times before ending up at c.

6. *b.* $\{v_7, v_8\}, \{v_1, v_2\}, \{v_3, v_4\}$

   c. $\{v_2, v_3\}, \{v_6, v_7\}, \{v_7, v_8\}, \{v_9, v_{10}\}$

7. *a.* For any positive integer n, consider the graph with distinct vertices $v_0, v_1, v_2, \ldots, v_n$ and edges $\{v_0, v_1\}, \{v_0, v_2\}, \ldots, \{v_0, v_i\}, \ldots, \{v_0, v_n\}$. Removal of any of these edges disconnects the graph.

   b. For any positive integer n, consider the graph with distinct vertices $v_1, v_2, \ldots, v_n$ and edges $\{v_1, v_2\}, \{v_2, v_3\}, \ldots, \{v_{i-1}, v_i\}, \ldots, \{v_{n-1}, v_n\}, \{v_n, v_0\}$. Any one of these edges can be removed without disconnecting the graph.

8. *b.* Two connected components:
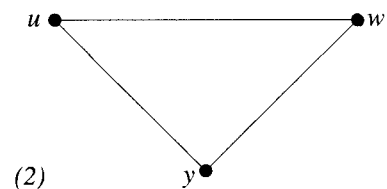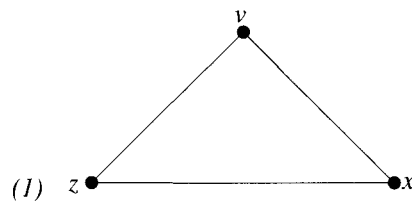
c. Three connected components:

(1)   *(2)*   *(3)*
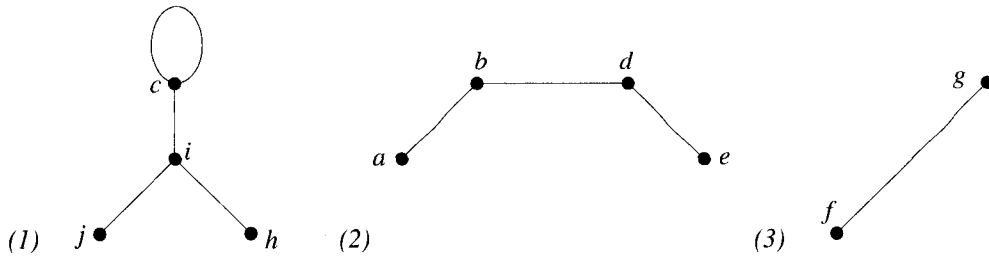
d. Two connected components:

(1)   *(2)*
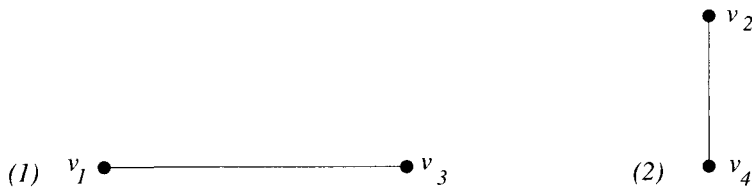
9. *b.* Yes, by Theorem 11.2.3 since G is connected and every vertex has even degree.

c. Not necessarily. It is not specified that G is connected. For instance, the following graph satisfies the given conditions but does not have an Euler circuit:
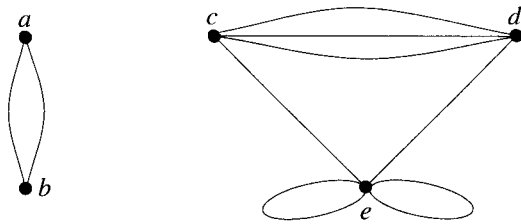
10. One such example is given in the answer to exercise 9c above. A simpler example is the graph shown below. Its vertices have degrees 2, 2, 2, and 0 which are all even numbers, but the graph does not have an Euler circuit.
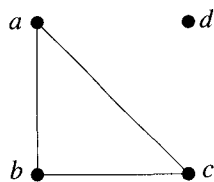
11. Yes. The graph that models the situation in which each bridge is crossed twice is the following.
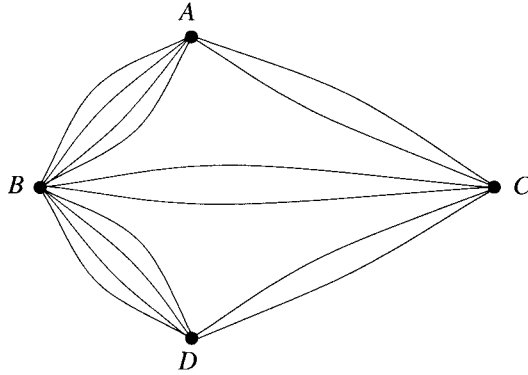
This graph is connected and its vertices have degrees 6, 6, 6, and 10, all of which are even numbers. Therefore, by Theorem 11.2.3, the graph has an Euler circuit, and so it is possible for a citizen of Königsberg to make a tour of the city and cross each bridge exactly twice.

13. This graph does not have an Euler circuit because vertices v_1, v_8, v_9, and v_7 have odd degree.

15. One Euler circuit is the following: *stuvwxyzrsuwyuzs*.

16. This graph does not have an Euler circuit because it is not connected.

17. This graph does not have an Euler circuit because vertices C and D have odd degree.

18. Yes. One Euler circuit is *ABDEACDA*.

20. There is not an Euler path from u to w because e, f, and h also have odd degree.

21. One Euler path from u to w is $uv_1v_2v_3uv_0v_7v_6v_3v_4v_6wv_5v_4w$.

22. Yes. One such path is *AHGBCDGFE*.

24. One Hamiltonian circuit is *balkjedcfihgb*.

25. Call the given graph G and suppose G has a Hamiltonian circuit. Then G has a subgraph H that satisfies conditions (1) – (4) of Proposition 11.2.6. Since the degree of c in G is five and every vertex in H has degree two, three edges incident on c must be removed from G to create H. Edge $\{c, d\}$ cannot be removed because doing so would result in vertex d having degree less than two in H. Similar reasoning shows that edges $\{c, f\}$, $\{c, b\}$, and $\{c, g\}$ cannot be removed either. It follows that the degree of c in H must be at least four, which contradicts the condition that every vertex in H has degree two in H. Hence no such subgraph H can exist, and so G does not have a Hamiltonian circuit.

27. Call the given graph G and suppose G has a Hamiltonian circuit. Then G has a subgraph H that satisfies conditions (1) – (4) of Proposition 11.2.6. Since the degree of B in G is five and every vertex in H has degree two, three edges incident on B must be removed from G to create H. Edge $\{B, C\}$ cannot be removed because doing so would result in vertex C having degree less than two in H. Similar reasoning shows that edges $\{B, E\}$, $\{B, F\}$, and $\{B, A\}$ cannot be removed either. It follows that the degree of B in H must be at least four, which contradicts the condition that every vertex in H has degree two in H. Hence no such subgraph H can exist, and so G does not have a Hamiltonian circuit.

28. Call the given graph G and suppose G has a Hamiltonian circuit. Then G has a subgraph H that satisfies conditions (1) – (4) of Proposition 11.2.6. Since the degree of b in G is three and every vertex in H has degree two, one edge incident on b must be removed from G to create H.

Edge $\{b, a\}$ cannot be removed because doing so would result in vertex a having degree less than two in H. Similar reasoning shows that edges $\{b, d\}$ and $\{b, c\}$ cannot be removed either. It follows that the degree of b in H must be at least three, which contradicts the condition that every vertex in H has degree two in H. Hence no such subgraph H can exist, and so G does not have a Hamiltonian circuit.

29. One Hamiltonian circuit is *abcdefga*.

30. One Hamiltonian circuit is $v_0 v_1 v_5 v_4 v_7 v_6 v_2 v_3 v_0$.

31. Call the given graph G and suppose G has a Hamiltonian circuit. Then G has a subgraph H that satisfies conditions (1) – (4) of Proposition 11.2.6. Edges $\{a, b\}$ and $\{a, d\}$ must be part of H because otherwise vertices b and d would have degree less than two in H. Similarly, edges $\{c, b\}$ and $\{c, d\}$ must be in H. Therefore, edges $\{a, e\}$ and $\{f, c\}$ are not in H because otherwise vertices a and c would have degrees greater than two in H. But removal of $\{a, e\}$ and $\{f, c\}$ disconnects G, which implies that H is not connected. This contradicts the condition that H is connected. Hence no such subgraph H can exist, and so G does not have a Hamiltonian circuit.

32. Other such graphs are those shown in exercise 12 and Example 11.2.6.

33. Other such graphs are those shown in exercises 17, 21, 23, 24, 29 and 30.

34. In the graph below, *abcda* is both an Euler and a Hamiltonian circuit.
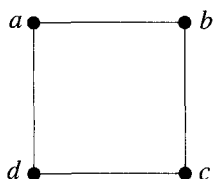
35. In the graph below, $ve_1 we_2 v$ is a Hamiltonian circuit that is not an Euler circuit, and $ve_1 we_2 ve_3 we_4 v$ is an Euler circuit that is not a Hamiltonian circuit.
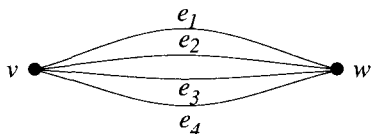
36. It is clear from the map that only a few routes have a chance of minimizing the distance. For instance, one must go to either Düsseldorf or Luxembourg just after leaving Brussels or just before returning to Brussels, and one must either travel from Berlin directly to Munich or the reverse. The possible minimizing routes are those shown below plus the same routes traveled in the reverse direction.

Route	Total Distance (in km)
Bru-Lux-Düss-Ber-Mun-Par-Bru	$219 + 224 + 564 + 585 + 832 + 308 = 2732$
Bru-Düss-Ber-Mun-Par-Lux-Bru	$223 + 564 + 585 + 832 + 375 + 219 = 2798$
Bru-Düss-Lux-Ber-Mun-Par-Bru	$223 + 224 + 764 + 585 + 832 + 308 = 2936$
Bru-Düss-Ber-Mun-Lux-Par-Bru	$223 + 564 + 585 + 517 + 375 + 308 = 2572$

The routes that minimize distance, therefore, are the bottom route shown in the table and that same route traveled in the reverse direction.

37. *b.* This statement is the contrapositive of the statement proved in part (a). So since a statement is logically equivalent to its contrapositive, this statement is true.

39. *Proof*: Suppose vertices v and w are part of a circuit in a graph G and one edge e is removed from the circuit. Without loss of generality, we may assume the v occurs before the w in the circuit, and we may denote the circuit by $v_0 e_1 v_1 e_2 \ldots e_{n-1} v_{n-1} e_n v_0$ with $v_i = v$, $v_j = w$, $i < j$, and $e_k = e$. If either $k \le i$ or $k > j$, then $v = v_i e_{i+1} v_{i+1} \ldots v_{j-1} e_j v_j = w$ is a path in G from v to w that does not include e. If $i < k \le j$, then $v = v_i e_i v_{i-1} e_{i-1} \ldots v_1 e_1 v_0 e_n v_{n-1} \ldots e_{j+1} v_j = w$ is a path in G from v to w that does not include e. These possibilities are illustrated by examples (1) and (2) in the diagram below. In either case there is a path in G from v to w that does not include e.

(1)
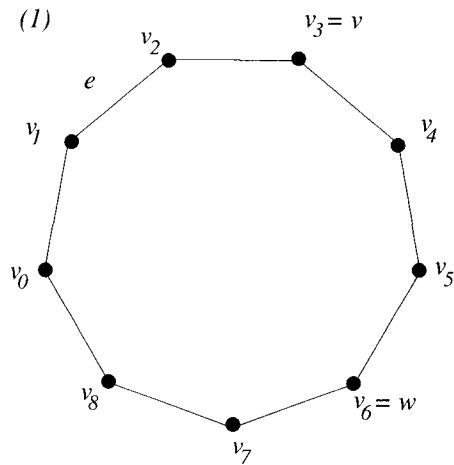
$i = 3, j=6$, e is deleted

path from v to w :

$v = v_3\, v_4\, v_5\, v_6\ = w$

(2)
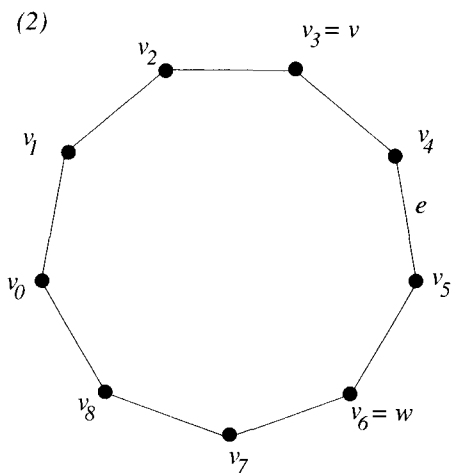
$i = 3, j=6$, e is deleted

path from v to w :

$v = v_3\, v_2\, v_1\, v_0\, v_8\, v_7\, v_6\ = w$

41. *Proof*: Suppose there is a path P in a graph G from a vertex v to a vertex w. By definition of path from v to w, P has the form $v = v_0 e_1 v_1 e_2 v_2 \ldots e_{n-1} v_{n-1} e_n v_n = w$ for some vertices $v_0, v_1, \ldots, v_n$ and distinct edges $e_1, e_2, \ldots, e_n$. Then $w = v_n e_n v_{n-1} e_{n-1} \ldots v_2 e_2 v_1 e_1 v_0 = v$ is a path from w to v.

43. *Proof*: Suppose C is a circuit in a graph G that starts and ends at a vertex v, and suppose w is another vertex in the circuit. By definition the circuit has the form $v e_1 v_1 e_2 v_2 \ldots e_{n-1} v_{n-1} e_n v$ where $v_1, v_2, \ldots, v_{n-1}$ are vertices of G, $e_1, e_2, \ldots, e_n$ are distinct edges of G, and $v_i = w$ for some i with $1 \le i \le n-1$. Then $w = v_i e_{i+1} v_{i+1} \ldots e_n v e_1 v_1 e_2 v_2 \ldots v_i = w$ is a circuit that starts and ends at w.

46. *Proof*: Let G be a graph and let v and w be two distinct vertices of G.

($\Rightarrow$) Suppose there is an Euler path in G from v to w. Form a new graph G' from G by adding an edge e from v to w. To the end of the Euler path in G from v to w, add edge e and vertex

v. The result is an Euler circuit in G' from v to v. It follows from Theorem 11.1.1 that every vertex in G' has even degree. Now the degrees of all vertices in G' except v and w are the same as their degrees in G. So all such vertices have even degree in G. Also the degrees of v and w in G are one less than their degrees in G'; so since one less than an even number is odd, both v and w have odd degree in G. Furthermore, G' is connected because it has an Euler circuit, and since removing an edge from a circuit does not disconnect a graph. (by Lemma 11.2.1c, which is proved as Lemma 11.5.2) and since G is obtained from G' by removing edge e (which is an edge of a circuit), G is also connected.

($\Leftarrow$) Suppose G is connected, v and w have odd degree, and all other vertices of G have even degree. Form a new graph G' from G by adding an edge e from v to w. This increases the degrees of v and w by one each, so that every vertex of G' has even degree and G' remains connected. Therefore, by Theorem 11.2.3, G' has an Euler circuit. Construct a (possibly different) Euler circuit for G' by starting at w, following e to v, and continuing from v using the method outlined in the proof of Theorem 11.2.3, eventually to return to w having traversed every edge of G'. Removing the initial vertex w and edge e from this circuit gives an Euler path in G from v to w.

47. *a.* For each integer $n \geq 1$, the complete graph on n vertices, K_n, has an Euler circuit if, and only if, n is odd. The reason is that by Theorem 11.2.4 K_n has an Euler circuit if, and only if, every vertex has even degree. But the degree of each vertex of K_n is $n-1$, and $n-1$ is even exactly when n is odd. (Note that the Euler circuit for K_1 is the trivial circuit.)

b. For each integer $n \geq 1$, K_n has an Hamiltonian circuit if, and only if, $n = 1$ or $n > 2$. When $n = 1$, the Hamiltonian circuit for K_n is the trivial circuit. For any integer $n > 2$, we can construct a Hamiltonian circuit for K_n as follows: Arrange the vertices of K_n in any order, and construct a circuit by starting at any vertex, visiting every other vertex in the order listed, and returning to the starting vertex. This is possible because each pair of vertices is connected by an edge. Hence K_n has a Hamiltonian circuit. K_2 does not have a Hamiltonian circuit because K_2 does not have any circuits, other than trivial ones, that start and end at the same vertex.

48. *a.* Let m and n be positive integers and let $K_{m,n}$ be a complete bipartite graph on (m, n) vertices. Since $K_{m,n}$ is connected, by Theorem 11.2.4 it has an Euler circuit if, and only if, every vertex has even degree. But $K_{m,n}$ has m vertices of degree n and n vertices of degree m. So $K_{m,n}$ has an Euler circuit if, and only if, both m and n are even.

b. Let m and n be positive integers, let $K_{m,n}$ be a complete bipartite graph on (m, n) vertices, and suppose $V_1 = \{v_1, v_2, \ldots, v_m\}$ and $V_2 = \{w_1, w_2, \ldots, w_n\}$ are the disjoint sets of vertices such that each vertex in V_1 is joined by an edge to each vertex in V_2 and no vertex within V_1 or V_2 is joined by an edge to any other vertex within the same set. If $m = n \geq 2$, then $K_{m,n}$ has the following Hamiltonian circuit: $v_1 w_1 v_2 w_2 \ldots v_m w_m v_1$. If $K_{m,n}$ has a Hamiltonian circuit, then $m = n$ because the vertices in any Hamiltonian circuit must alternate between V_1 and V_2 (since no edges connect vertices within either set) and because no vertex, except the first and last, appears twice in a Hamiltonian circuit. If $m = n = 1$, then $K_{m,n}$ does not have a Hamiltonian circuit because $K_{1,1}$ contains just one edge joining two vertices. Therefore, $K_{m,n}$ has a Hamiltonian circuit if, and only if, $m = n \geq 2$.

49. *Proposition*: If n is an integer with $n \geq 2$, then a simple disconnected graph with n vertices has a maximum of $(n-1)(n-2)/2$ edges.

Proof: Let n be an integer with $n \geq 2$, and let G be a simple disconnected graph with n vertices and a maximum number of edges. Then G consists of just two connected components because if G had more than two components, an edge could be added between two vertices in two separate components, giving a graph that would still be disconnected but would have more edges than G. Suppose one connected component contains k vertices ($1 \leq k \leq n-1$). Then the other connected component contains $n - k$ vertices. By exercise 34 of Section 11.1,

the maximum number of edges in the two components are $k(k-1)/2$ and $(n-k)(n-k-1)/2$ respectively. Therefore, the total maximum number of edges is $k(k-1)/2+(n-k)(n-k-1)/2$. We may complete the proof in several ways.

Version 1: Observe that

$$\frac{k(k-1)}{2}+\frac{(n-k)(n-k-1)}{2}=\frac{k^2-k+n^2-nk-n-nk+k^2+k}{2}=k^2-nk+\frac{n^2-n}{2}.$$

We wish to find an integer k, with $1 \le k \le n-1$, that maximizes $k^2-nk+\dfrac{n^2-n}{2}$. Let f be the function defined by specifying that $f(x)=x^2-nx+\dfrac{n^2-n}{2}$ on the interval $1 \le x \le n-1$. We may use either calculus or the technique of completing the square to find k.

Version 1a (using calculus): Because $f'(x)=2x-n$, (1) $f'(x)>0 \Leftrightarrow 2x-n>0 \Leftrightarrow x>n/2$, (2) $f'(x)=0 \Leftrightarrow 2x-n=0 \Leftrightarrow x=n/2$, and (3) $f'(x)<0 \Leftrightarrow 2x-n<0 \Leftrightarrow x<n/2$. Therefore, f is decreasing on $x \le n/2$, attains a minimum at $x=n/2$, and is increasing for $x \ge n/2$ and decreasing for $x < n/2$. It follows that f achieves its maximum values at the endpoints of the interval: $x=1$ and $x=n-1$. These both correspond to the situation in which one component of G has one vertex and no edges and the other component is a complete graph on $n-1$ vertices. Consequently, the total number of edges for the graph is the same as the total number of edges of a complete graph on $n-1$ vertices, namely $(n-1)(n-2)/2$ (by exercise 33b of Section 11.1).

Version 1b (using completing the square): Note that $f(x)=x^2-nx+\frac{n^2-n}{2}=(x-\frac{n}{2})^2-\frac{n}{4}+\frac{n^2-n}{4}=(x-\frac{n}{2})^2+(\frac{n^2-2n}{4})$ for all real x. It follows that the graph of f is a parabola that opens out upward with minimum value at $x=n/2$. Thus, as above, f achieves its maximum values at the endpoints of the interval: $x=1$ and $x=n-1$, and, therefore, the total number of edges for the graph is $(n-1)(n-2)/2$.

Version 2 (an alternative way to complete the proof that does not use calculus): In this version, we show that the total number of edges, which we know to be $k(k-1)/2+(n-k)(n-k-1)/2$, is less than or equal to $\dfrac{(n-1)(n-2)}{2}$. Observe that

$$\frac{k(k-1)}{2}+\frac{(n-k)(n-k-1)}{2} \le \frac{(n-1)(n-2)}{2} \Leftrightarrow k^2-k+n^2-2nk+k^2-n+k \le n^2-3n+2$$
$$\Leftrightarrow 2k^2-2 \le -2n+2nk \Leftrightarrow k^2-1 \le -n+nk \Leftrightarrow (k-1)(k+1) \le n(k-1).$$

Call the final inequality (*). When $k=1$, inequality (*) is true because both sides are 0. When $k>1$, we may divide both sides of (*) by $k-1$, which is positive, to deduce that

$$(k-1)(k+1) \le n(k-1) \Leftrightarrow k+1 \le n \Leftrightarrow k \le n-1.$$

But this last inequality is true because $k \le n-1$. So, because the original inequality is equivalent to one that is known to be true, the original inequality must also be true.

50. *Proof 1*: Suppose a graph G is bipartite. We will show that every circuit in G has an even number of edges. Let V_1 and V_2 be disjoint subsets of vertices such that vertices in V_1 are joined by edges to vertices in V_2 but no edges join vertices within either V_1 or V_2, and suppose that $v \in V_1$. Let C be any circuit in G. Since no edges join vertices within either V_1 or V_2, the only way that C can start from a vertex and return to the same vertex is for it to go back and forth from V_1 to V_2. Thus adjacent edges of C can be divided into pairs, one leading from V_1 to V_2 and the other leading back. It follows that the total number of edges in C is even.

Proof 2: Let G be a bipartite graph with disjoint subsets of vertices V_1 and V_2 such that vertices in V_1 are joined by edges to vertices in V_2 but no edges join vertices within either V_1 or V_2, and suppose C is a circuit in G. In case C is a trivial circuit, C has an even number of edges because 0 is even. In case C is a nontrivial circuit, C must have a vertex in one

set of vertices, have an edge leading from that vertex to a vertex in the other set of vertices (because G is simple and therefore has no loops). C must also have an edge going back to the first set of vertices, and this edge cannot be the same as the first edge because G is simple and therefore has no parallel edges. Thus C has at least 3 edges and may be displayed as $a_0b_0a_1b_1a_2\ldots b_ka_k = a_0$, where $a_0, a_1, a_2, \ldots$ are vertices in V_1 and $b_0, b_1, b_2, \ldots$ are vertices in V_2. The edges of C may, therefore, be grouped in pairs as follows:

$\{a_0, b_0)\{b_0, a_1\}$ $\{a_1, b_1)\{b_1, a_2\}$ $\{a_2, b_2)\{b_2, a_3\}$ $\ldots$ $\{a_{k-1}, b_{k-1})\{b_{k-1}, a_k\}$ $\{a_k, b_k)\{b_k, a_0\}$.

Hence the number of edges of C is clearly $2(k + 1)$, an even number

Section 11.3

1. *b.* By equating corresponding entries, we see that $2a = 4$, $b + c = 3$, $c - a = 1$, and $2b - a = -2$. Now $2a = 4 \Rightarrow a = 2$, $c - a = c - 2 = 1 \Rightarrow c = 3$, and $b + c = b + 3 = 3 \Rightarrow b = 0$. Substituting these solutions into the last equation to check for consistency gives $2b - a = 2 \cdot 0 - 2 = -2$, which agrees. Therefore, $a = 2$, $b = 0$, and $c = 3$.

2. *b.*
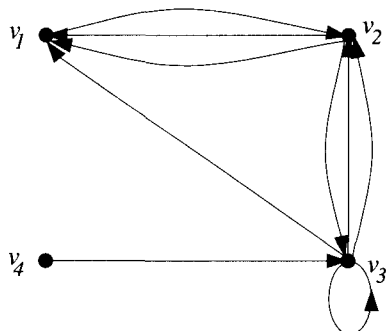
	v_1	v_2	v_3	v_4
v_1	1	0	1	0
v_2	0	0	1	0
v_3	1	0	0	1
v_4	0	0	1	0

3. *b.*

Any labels may be applied to the edges because the adjacency matrix does not determine edge labels.

4. *b.*

	v_1	v_2	v_3	v_4
v_1	0	0	0	0
v_2	0	1	1	2
v_3	0	1	1	0
v_4	0	2	0	0

d.

	a_1	a_2	b_1	b_2	b_3
a_1	0	0	1	1	1
a_2	0	0	1	1	1
b_1	1	1	0	0	0
b_2	1	1	0	0	0
b_3	1	1	0	0	0

5. *b.*

Any labels may be applied to the edges because the adjacency matrix does not determine edge labels.

6. *b.* The graph is not connected; the matrix shows that there are no edges joining the vertices from the set $\{v_1, v_2\}$ to those in the set $\{v_3, v_4\}$.

7. If, for all integers $i \geq 1$, all entries in the ith row and ith column of the adjacency matrix of a graph are zero, then the graph has no loops.

8. *b.* 2

9. *b.*

$$\begin{bmatrix} 0 & 8 \\ -5 & 4 \end{bmatrix}$$

c.

$$\begin{bmatrix} -2 & -3 \\ 4 & 6 \end{bmatrix}$$

10. *c.* no product (**A** does not have the same number of columns as rows)

d. no product (**B** has two columns and **C** has three rows)

e.

$$\begin{bmatrix} -2 & -6 \\ -5 & 3 \\ -2 & 0 \end{bmatrix}$$

g.

$$\begin{bmatrix} -8 & 0 \\ 7 & 27 \end{bmatrix}$$

h. no product (**C** does not have the same number of columns as rows)

j.

$$\begin{bmatrix} 0 & 4 & -2 \\ 3 & 1 & -2 \\ 1 & 1 & -1 \end{bmatrix}$$

11. The following is one example among many.

Let $\mathbf{A} = \begin{bmatrix} 1 & 2 \\ 0 & 0 \end{bmatrix}$ and $\mathbf{B} = \begin{bmatrix} 1 & 0 \\ 2 & 0 \end{bmatrix}$. Then $\mathbf{AB} = \begin{bmatrix} 5 & 0 \\ 0 & 0 \end{bmatrix}$ whereas $\mathbf{BA} = \begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix}$.

13. The following is one example among many.

Let $\mathbf{A} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$ and $\mathbf{B} = \begin{bmatrix} 0 & 0 \\ 1 & -1 \end{bmatrix}$. Then $\mathbf{A} \neq \mathbf{B}$, $\mathbf{B} \neq \mathbf{O}$, and $\mathbf{AB} = \begin{bmatrix} 1 & -1 \\ 1 & -1 \end{bmatrix} \neq \mathbf{O}$ whereas $\mathbf{BA} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \mathbf{O}$.

14. *Proof*: Let **I** be the $m \times m$ identity matrix and let $\mathbf{A} = (a_{ij})$ be any $m \times n$ matrix. Then for all $i, j = 1, 2, \ldots, m$, the ijth entry of **IA** is $\Sigma_{k=1}^{m} \delta_{ik} a_{kj} = \delta_{ii} a_{ij} = a_{ij}$ because by definition of **I**, $\delta_{ik} = 0$ for all k with $i \neq k$ and $\delta_{ii} = 1$. But a_{ij} is the ijth entry of **A**. So $\mathbf{IA} = \mathbf{A}$.

16. *Proof*: Let $\mathbf{A} = (a_{ij})$, $\mathbf{B} = (b_{ij})$, and $\mathbf{C} = (c_{ij})$ be any $m \times k$, $k \times r$, and $r \times n$ matrices, respectively. The numbers of rows and columns are such that $\mathbf{AB}$, $\mathbf{BC}$, $(\mathbf{AB})\mathbf{C}$, and $\mathbf{A}(\mathbf{BC})$ are all defined. Let $\mathbf{AB} = (d_{ij})$ and $\mathbf{BC} = (e_{ij})$. Then for all integers i and j with $1 \le i \le m$ and $1 \le j \le n$,

$$
\begin{aligned}
\text{the } ij\text{th entry of } (\mathbf{AB})\mathbf{C} &= \Sigma_{p=1}^{r} d_{ip} c_{pj} \\
&= \Sigma_{p=1}^{r} \left(\Sigma_{q=1}^{k} a_{iq} b_{qp} \right) c_{pj} \\
&= \Sigma_{p=1}^{r} \Sigma_{q=1}^{k} a_{iq} b_{qp} c_{pj} \qquad \text{by Theorem 4.1.1} \\
&= \Sigma_{q=1}^{k} \Sigma_{p=1}^{r} a_{iq} b_{qp} c_{pj} \qquad \text{by a generalized commutative law} \\
&= \Sigma_{q=1}^{k} a_{iq} \left(\Sigma_{p=1}^{r} b_{qp} c_{pj} \right) \qquad \text{by Theorem 4.1.1} \\
&= \Sigma_{q=1}^{k} a_{iq} e_{qj} \\
&= \text{the } ij \text{ th entry of } \mathbf{A}(\mathbf{BC}).
\end{aligned}
$$

Since all corresponding entries are equal, $(\mathbf{AB})\mathbf{C} = \mathbf{A}(\mathbf{BC})$.

18. *Proof (by mathematical induction)*: Let the property $P(n)$ be the sentence "$\mathbf{A}^n$ is symmetric."

Show that the property is true for $n = 1$: For $n = 1$ the property is true because by assumption $\mathbf{A}$ is a symmetric matrix.

Show that for all integers $k \ge 1$, if the property is true for $n = k$ then it is true for $n = k + 1$: Let k be an integer with $k \ge 1$, and suppose that $\mathbf{A}^k$ is symmetric. *[This is the inductive hypothesis.]* We must show that $\mathbf{A}^{k+1}$ is symmetric. Let $\mathbf{A}^k = (b_{ij})$. Then for all $i, j = 1, 2, \ldots, m$, the ijth entry of $\mathbf{A}^{k+1}$ = the ijth entry of $\mathbf{A}\mathbf{A}^k$ *[by definition of matrix power]* $= \Sigma_{r=1}^{m} a_{ir} b_{rj}$ *[by definition of matrix multiplication]* $= \Sigma_{r=1}^{m} a_{ri} b_{jr}$ *[because $\mathbf{A}$ is symmetric by hypothesis and $\mathbf{A}^k$ is symmetric by inductive hypothesis]* $= \Sigma_{r=1}^{m} b_{jr} a_{ri}$ *[because multiplication of real numbers is commutative]* = the jith entry of $\mathbf{A}^k \mathbf{A}$ *[by definition of matrix multiplication]* = the jith entry of $\mathbf{A}\mathbf{A}^k$ *[by exercise 17]* = the jith entry of $\mathbf{A}^{k+1}$ *[by definition of matrix power]*. Therefore, $\mathbf{A}^{k+1}$ is symmetric *[as was to be shown]*.

19. *b.* There are three walks of length two from v_1 to v_3 because the entry in row 1 column 3 (and row 3 column 1) of $\mathbf{A}^2$ is 3. There are 15 walks of length three from v_1 to v_3 because the entry in row 1 column 3 (and row 3 column 1) of $\mathbf{A}^3$ is 15.

c. The calculations are $\begin{bmatrix} 2 & 1 & 0 \end{bmatrix} \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix} = 2 \cdot 2 + 1 \cdot 1 + 0 \cdot 0 = 5$. In this sum

$$
2 \cdot 2 = \begin{bmatrix} \text{number of edges} \\ \text{from } v_3 \text{ to } v_1 \end{bmatrix} \cdot \begin{bmatrix} \text{number of edges} \\ \text{from } v_1 \text{ to } v_3 \end{bmatrix} = \begin{bmatrix} \text{number of walks of length 2} \\ \text{from } v_3 \text{ to } v_3 \text{ that go via } v_1 \end{bmatrix}
$$

$$
1 \cdot 1 = \begin{bmatrix} \text{number of edges} \\ \text{from } v_3 \text{ to } v_2 \end{bmatrix} \cdot \begin{bmatrix} \text{number of edges} \\ \text{from } v_2 \text{ to } v_3 \end{bmatrix} = \begin{bmatrix} \text{number of walks of length 2} \\ \text{from } v_3 \text{ to } v_3 \text{ that go via } v_2 \end{bmatrix}
$$

$$
0 \cdot 0 = \begin{bmatrix} \text{number of edges} \\ \text{from } v_3 \text{ to } v_3 \end{bmatrix} \cdot \begin{bmatrix} \text{number of edges} \\ \text{from } v_3 \text{ to } v_3 \end{bmatrix} = \begin{bmatrix} \text{number of walks of length 2} \\ \text{from } v_3 \text{ to } v_3 \text{ that go via } v_3 \end{bmatrix}
$$

Since any walk of length two from v_3 to v_3 must go via either v_1, v_2, or v_3, $2 \cdot 2 + 1 \cdot 1 + 0 \cdot 0 = 5$ is the total number of walks of length two from v_3 to v_3.

In the diagram below, the five walks of length two from v_3 to v_3 can be seen to be $v_3 e_1 v_1 e_1 v_3$, $v_3 e_1 v_1 e_2 v_3$, $v_3 e_2 v_1 e_1 v_3$, $v_3 e_2 v_1 e_2 v_3$, and $v_3 e_5 v_2 e_5 v_3$.
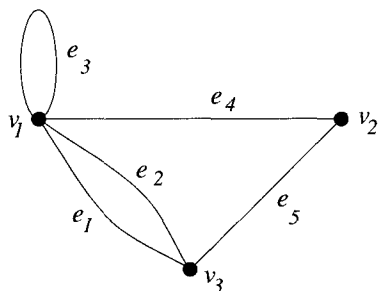
21. *Proof (by mathematical induction)*: Let the property $P(n)$ be the sentence "all the entries along the main diagonal of $\mathbf{A}^n$ are equal to each other and all the entries off the main diagonal are also equal to each other."

Show that the property is true for $n = 1$: For $n = 1$ the property is true because $\mathbf{A}^1 = \mathbf{A}$, which is the adjacency matrix for K_3, and all the entries along the main diagonal of $\mathbf{A}$ are 0 *[because K_3 has no loops]* and all the entries off the main diagonal are 1 *[because each pair of vertices is connected by exactly one edge]*.

Show that for all integers $m \geq 1$, if the property is true for $n = m$ then it is true for $n = m + 1$: Let m be an integer with $m \geq 1$, and suppose that all the entries along the main diagonal of $\mathbf{A}^m$ are equal to each other and all the entries off the main diagonal are also equal to each other. *[This is the inductive hypothesis.]* Then

$$\mathbf{A}^m = \begin{bmatrix} b & c & c \\ c & b & c \\ c & c & b \end{bmatrix} \quad \text{for some integers } b \text{ and } c.$$

It follows that

$$\mathbf{A}^{m+1} = \mathbf{A}\mathbf{A}^m = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} b & c & c \\ c & b & c \\ c & c & b \end{bmatrix} = \begin{bmatrix} 2c & b+c & b+c \\ b+c & 2c & b+c \\ b+c & b+c & 2c \end{bmatrix}$$

As can be seen, all the entries of $\mathbf{A}^{m+1}$ along the main diagonal are equal to each other and all the entries off the main diagonal are equal to each other. So the property is true for $n = m+1$.

22. *a.*
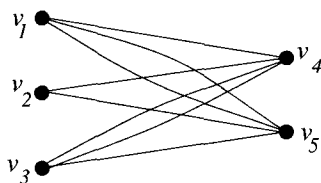
Any labels may be applied to the edges because the adjacency matrix does not determine edge labels. Regardless of edge labels, this graph is bipartite.

b. Proof:

($\Rightarrow$) Suppose that a graph G with n vertices is bipartite. Then its vertices can be partitioned into two disjoint sets V_1 and V_2 so that no two vertices within V_1 are connected to each other by an edge and no two vertices within V_2 are connected to each other by an edge. Label the vertices in V_1 as $v_1, v_2, \ldots, v_k$ and label the vertices in V_2 as $v_{k+1}, v_{k+2}, \ldots, v_n$. Then the adjacency matrix of G relative to this vertex labeling is

$$\begin{array}{c} \\ v_1 \\ v_2 \\ \vdots \\ v_k \\ v_{k+1} \\ \vdots \\ v_n \end{array} \begin{array}{cccccccc} v_1 & v_2 & \dots & v_k & v_{k+1} & \dots & v_n \\ \begin{bmatrix} 0 & 0 & \dots & 0 & a_{1,k+1} & \dots & a_{1,n} \\ 0 & 0 & \dots & 0 & a_{2,k+1} & \dots & a_{2,n} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 0 & a_{k,k+1} & \dots & a_{k,n} \\ a_{k+1,1} & a_{k+1,2} & \dots & a_{k+1,k} & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ a_{n,1} & a_{n,2} & \dots & a_{n,k} & 0 & \dots & 0 \end{bmatrix} \end{array}$$

Let $\mathbf{A}$ be the $k \times (n-k)$ matrix whose ijth entry is $a_{i,k+j}$ for all $i = 1, 2, \ldots, k$ and $j = 1, 2, \ldots, n - k$, and let $\mathbf{B}$ be the $(n - k) \times k$ matrix whose jith entry is $a_{k+j,i}$ for all $i = 1, 2, \ldots, k$ and $j = 1, 2, \ldots, n - k$. For all i and j, the ijth entry of $\mathbf{A} = a_{i,k+j} =$ the number of edges from v_i to $v_{k+j} =$ the number of edges from v_{k+j} to $v_i = a_{k+j,i} =$ the jith entry of $\mathbf{B}$, and so $\mathbf{B} = \mathbf{A}^t$ and the adjacency matrix of G has the required form.

($\Leftarrow$) Suppose that for some labeling of the vertices of a graph G, its adjacency matrix has the given form. Denote the labeling of the vertices of G that gives rise to this adjacency matrix by $v_1, v_2, \ldots, v_n$. Let $V_1 = \{v_1, v_2, \ldots, v_k\}$ and $V_2 = \{v_{k+1}, v_{k+2}, \ldots, v_n\}$. For all i and j with $1 \le i, j \le k$, the ijth entry of the adjacency matrix is zero. This implies that there is no edge that connects two vertices in V_1. Similarly, for all i and j with $k + 1 \le i, j \le n$, the ijth entry in the adjacency matrix is zero, and so there is no edge that connects two vertices in V_2. Therefore, G is bipartite.

23. *a. Proof:* Suppose G is a graph with n vertices, v and w are distinct vertices of G, and there is a walk in G from v to w. If this walk has length k greater than or equal to n, then it contains a repeated vertex, say u, because there are only n vertices in G and there are $k + 1$ vertices in a walk of length k. Replace the section of the walk from u to u by the vertex u alone; the result is still a walk from v to w but it has shorter length than the given walk *[because a walk consists of an alternating sequence of vertices and edges so that the section of a walk between two vertices contains at least one edge].* If this walk has length greater than or equal to n, then repeat the replacement process described above. Continue repeating the replacement process until a walk from v to w with no more than $n - 1$ edges is found. This must happen eventually because the total number of edges and vertices in the initial walk is finite and each repetition of the process results in the removal of at least one edge.

b. Proof: Let G be a graph with n vertices (where $n > 1$) and let $\mathbf{A}$ be the adjacency matrix of G relative to the vertex labeling $v_1, v_2, \ldots, v_n$.

($\Rightarrow$) Suppose G is connected. Let integers i and j with $1 \le i < j \le n$ be given. We will show that the ijth entry in the matrix sum $\mathbf{A} + \mathbf{A}^2 + \ldots + \mathbf{A}^{n-1}$ is positive. Since G is connected, there is a walk from v_i to v_j, and so by part (a), there is a walk of length at most $n - 1$ from v_i to v_j. Let the length of such a walk be k. Then the ijth entry of $\mathbf{A}^k$, which equals the number of walks of length k from v_i to v_j (by Theorem 11.3.2), is at least one. Now all entries in all powers of $\mathbf{A}$ are nonnegative *[because each equals the number of walks from one vertex to another]*, and if one term of a sum of nonnegative numbers is positive then the entire sum is positive. Hence the ijth entry in $\mathbf{A} + \mathbf{A}^2 + \ldots + \mathbf{A}^{n-1}$ *[which is the sum of the ijth entries in all powers of $\mathbf{A}$ from 1 to $n - 1$]* is positive.

($\Leftarrow$) Suppose every entry in $\mathbf{A} + \mathbf{A}^2 + \ldots + \mathbf{A}^{n-1}$ is positive. Let v_i and v_j be any two vertices of G. We must show that there is a walk from v_i to v_j. For each $k = 1, 2, \ldots, n - 1$, the ijth entry of $\mathbf{A}^k$ equals the number of walks of length k from v_i to v_j (by Theorem 11.3.2) and is therefore nonnegative. By supposition, when these nonnegative numbers are added together, the sum is positive. Now the only way that a sum of real numbers can be positive is for at least one of the numbers to be positive. Hence for some k, the ijth entry of $\mathbf{A}^k$ is positive. It

follows that the number of walks of length k from v_i to v_j is positive, and so there is at least one walk joining v_i to v_j.
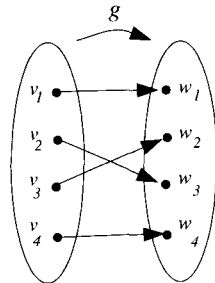
Section 11.4

3. The graphs are isomorphic. One way to define to isomorphism is as follows.
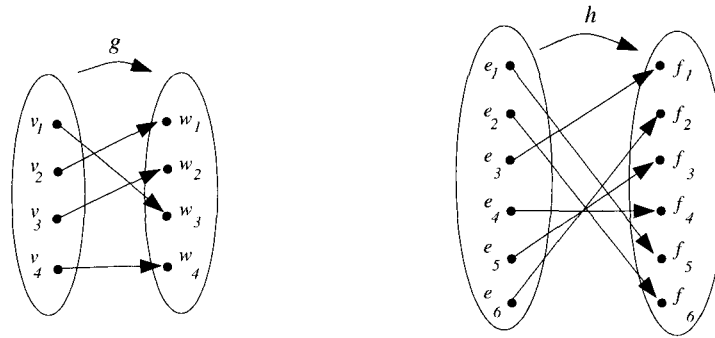
4. The graphs are not isomorphic: G has a circuit of length 4, a circuit of length 5, and a vertex of degree 4, whereas G' has none of these.

5. The graphs are not isomorphic: G has a vertex of degree five whereas G' does not.

7. The graphs are isomorphic. One way to define to isomorphism is as follows.

9. The graphs are isomorphic. One way to define to isomorphism is as follows.
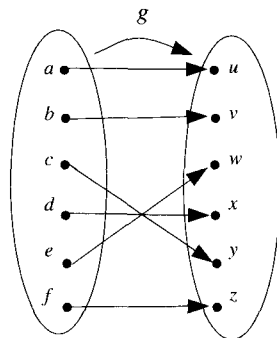
11. The graphs are not isomorphic: G' has a circuit of length six whereas G does not. Also G' is connected whereas G is not.

13. The graphs are not isomorphic: G has a simple circuit of length five ($abcfea$) whereas G' does not.

15. There is one such graph with 0 edges, one with 1 edge, and there are two with 2 edges, three with 3 edges, two with 4 edges, one with 5 edges, and one with 6 edges. These eleven graphs are shown below.
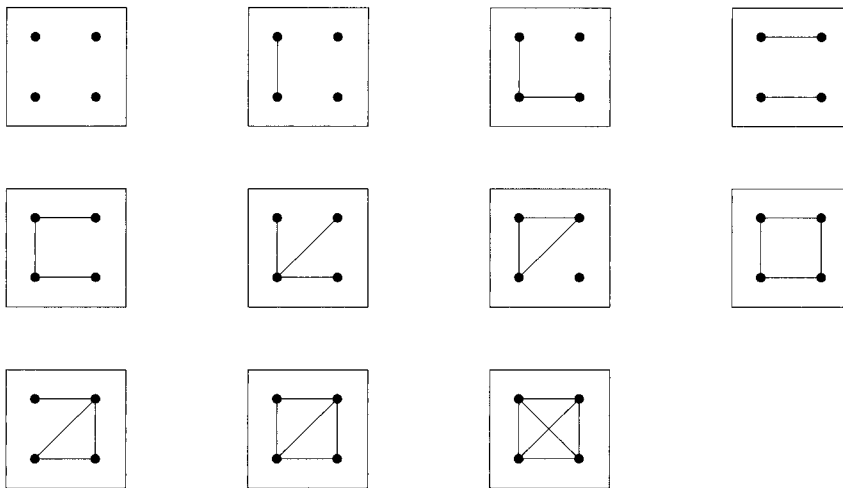
17. There is one such graph with 0 edges, and there are two with 1 edge (one in which the edge is a loop and one in which it is not), and six with 2 edges (two simple graphs, one with two parallel edges, two in which one of the edges is a loop and the other is not a loop, and two in which both edges are loops). These are shown below.
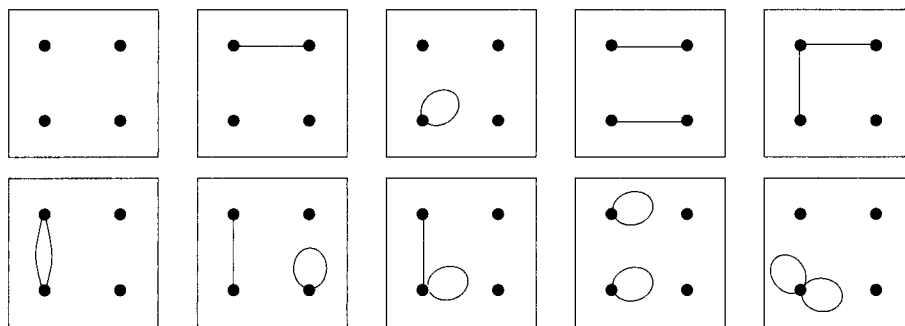
18. There are three such graphs in which all 3 edges are loops, five in which 2 edges are loops and 1 is not a loop, six in which 1 edge is a loop and 2 edges are not loops, and six in which none of the 3 edges is a loop. These 20 graphs are shown below.
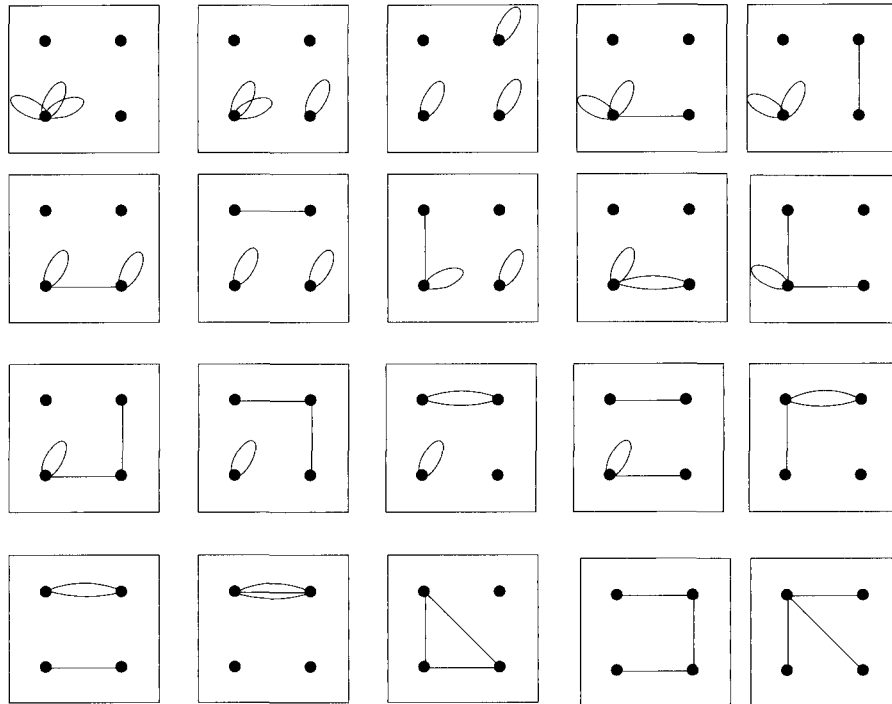
20. Four (of many) such graphs are shown below.
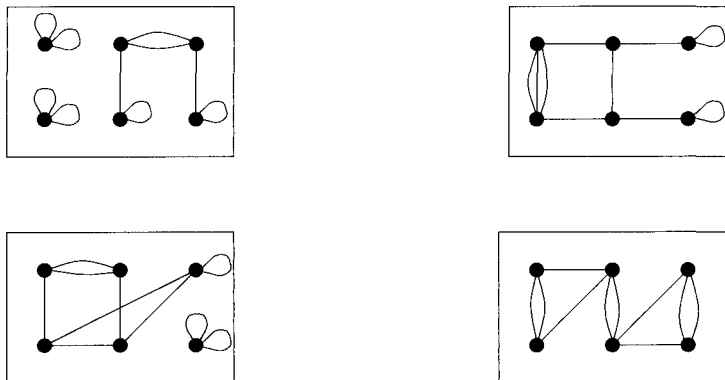
22. *Proof:* Suppose G and G' are isomorphic graphs and G has m edges where m is a nonnegative integer. By definition of graph isomorphism, there is a one-to-one correspondence $h: E(G) \rightarrow E(G')$. But $E(G)$ is a finite set and two finite sets in one-to-one correspondence have the same number of elements. Therefore, there are as many edges in $E(G')$ as there are in $E(G)$, and so G and G' have the same number of edges.

24. *Proof:* Suppose G and G' are isomorphic graphs and suppose G has a simple circuit C of length k, where k is a nonnegative integer. By definition of graph isomorphism, there are one-to-one correspondences $g: V(G) \rightarrow V(G')$ and $h: E(G) \rightarrow E(G')$ that preserve the edge-endpoint functions in the sense that for all v in $V(G)$ and e in $E(G)$, v is an endpoint of $e \Leftrightarrow g(v)$ is an endpoint of $h(e)$. Let C be $v_0 e_1 v_1 e_2 \ldots e_k v_k (= v_0)$, and let C' be $g(v_0)h(e_1)g(v_1)h(e_2)\ldots h(e_k)g(v_k)(= g(v_0))$. By the same reasoning as in the solution to exercise 23, C' is a circuit of length k in G'. Suppose C' is not a simple circuit. Then C' has a repeated vertex, say $g(v_i) = g(v_j)$ for some $i, j = 0, 1, 2, \ldots, k-1$ with $i \neq j$. But since g is a

one-to-one correspondence this implies that $v_i = v_j$, which is impossible because C is a simple circuit. Hence the supposition is false, C' is a simple circuit, and therefore G' has a simple circuit of length k.

25. *Proof*: Suppose G and G' are isomorphic graphs and suppose G has m vertices of degree k, v_1, $v_2, \ldots, v_m$, where m and k are nonnegative integers. By definition of graph isomorphism, there are one-to-one correspondences $g \colon V(G) \to V(G')$ and $h \colon E(G) \to E(G')$ that preserve the edge-endpoint functions in the sense that for all v in $V(G)$ and e in $E(G)$, v is an endpoint of $e \Leftrightarrow g(v)$ is an endpoint of $h(e)$. Consider the vertices $g(v_1)$, $g(v_2), \ldots, g(v_m)$ in G'. Because g is a one-to-one correspondence, these vertices are all distinct. And applying the same argument as that used in Example 11.4.4 to each vertex $g(v_i)$ enables us to conclude that each has degree k. Hence G' has at least m vertices of degree k. If G' had an additional vertex w of degree k, then, by similar reasoning as in Example 11.4.4, $g^{-1}(w)$ would also have degree k and, because g is a one-to-one correspondence, $g^{-1}(w) \neq v_i$ for any $i = 1, 2, \ldots, m$, which would contradict the assumption that G has exactly m vertices of degree k. Thus G' does not have more than m vertices of degree k, and so G' has exactly m vertices of degree k.

26. *Proof*: Suppose G and G' are isomorphic graphs and suppose G has m distinct simple circuits of length k, where m and k are nonnegative integers. By definition of graph isomorphism, there are one-to-one correspondences $g \colon V(G) \to V(G')$ and $h \colon E(G) \to E(G')$ that preserve the edge-endpoint functions in the sense that for all v in $V(G)$ and e in $E(G)$, v is an endpoint of $e \Leftrightarrow g(v)$ is an endpoint of $h(e)$. Define a function K from the set of all simple circuits of length k in G to the set of all simple circuits of length k in G' as follows: Given a simple circuit C in G of length k, denote C by $x_0 c_0 x_1 c_1 \ldots x_{k-1} c_{k-1} x_0$ where x_0, $x_1, \ldots$, and x_{k-1} are distinct vertices and c_0, $c_1, \ldots$, and c_{k-1} are distinct edges. Define $K(C) = g(x_0)h(c_0)g(x_1)h(c_1)\ldots g(x_{k-1})h(c_{k-1})g(x_0)$. *[We will show that K is one-to-one.]* Suppose $C_1 = v_0 e_1 v_1 e_2 \ldots e_k v_0$ and $C_2 = w_0 f_1 w_1 f_2 \ldots f_k w_0$ are simple circuits of length k in G with $K(C_1) = K(C_2)$. By definition of K, $g(v_0)h(e_0)g(v_1)h(e_1)\ldots g(v_{k-1})h(e_{k-1})g(v_0) = g(w_0)h(f_0)g(w_1)h(f_1)\ldots g(w_{k-1})h(f_{k-1})g(w_0)$, and, by definition of sequence, this implies that $g(v_i) = g(w_i)$ and $h(e_i) = h(f_i)$ for all $i = 0, 1, 2, \ldots, k-1$. Since both g and h are one-to-one, we have that $v_i = w_i$ and $e_i = f_i$ for all $i = 0, 1, 2, \ldots, k-1$, and, thus, $C_1 = C_2$. Hence K is one-to-one. But because the graphs are finite, K is a function from one finite set to another, and so, by Theorem 7.3.2, since K is also onto. Therefore K is a one-to-one correspondence, and thus there are the same number of distinct simple circuits of length k in G as there are in G'. So since G has m simple circuits of length k, G' also has m simple circuits of length k.

27. *Proof*: Suppose G and G' are isomorphic graphs and suppose G is connected. By definition of graph isomorphism, there are one-to-one correspondences $g \colon V(G) \to V(G')$ and $h \colon E(G) \to E(G')$ that preserve the edge-endpoint functions in the sense that for all v in $V(G)$ and e in $E(G)$, v is an endpoint of $e \Leftrightarrow g(v)$ is an endpoint of $h(e)$. Suppose w and x are any two vertices of G'. Then $u = g^{-1}(w)$ and $v = g^{-1}(x)$ are distinct vertices in G (because g is a one-to-one correspondence). Since G is connected, there is a walk in G connecting u and v. Say this walk is $u e_1 v_1 e_2 v_2 \ldots e_n v$. Because g and h preserve the edge-endpoint functions, $w = g(u)h(e_1)g(v_1)h(e_2)g(v_2)\ldots h(e_n)g(v) = x$ is a walk in G' connecting w and x.

28. *Proof*: Suppose G and G' are isomorphic graphs and suppose G has an Euler circuit C. Let m be the number of edges in G. Then C has length m because it includes every edge of G. By the same argument as in the answer to exercise 23, G' has a corresponding circuit C' of length m, and by exercise 22, G' also has m edges. Since all the edges of a circuit are distinct, C' includes all of the m edges of G'. Hence C' is an Euler circuit for G'.

29. *Proof*: Suppose G and G' are isomorphic graphs and suppose G has an Hamiltonian circuit C. Let the number of vertices of G be n. Since C is a Hamiltonian circuit, it is a simple circuit that has length n (because it includes every vertex of G exactly once, except for the

first and last which are repeated). By the same argument as in the answer to exercise 23, G' has a corresponding circuit C' of length n, and by exercise 21, G' also has n vertices. Now all the edges and vertices of a simple circuit are distinct except for the repetition of the first and last vertex, the vertices of C' are by construction the images under g of the vertices of C, and since g is a one-to-one correspondence, g sends the n distinct vertices of C onto the n distinct vertices of G'. Hence C' is a simple circuit of length n in G', and so C' includes all of the n vertices of G'. Therefore, C' is a Hamiltonian circuit for G'.

30. Suppose that G and G' are isomorphic via one-to-one correspondences $g\colon V(G) \to V(G')$ and $h\colon E(G) \to E(G')$, where g and h preserve the edge-endpoint functions. Now w_6 has degree one in G', and so by the argument given in Example 11.4.4, w_6 must correspond to one of the vertices of degree one in G : either $g(v_1) = w_6$ or $g(v_6) = w_6$. Similarly, since w_5 has degree three in G', w_5 must correspond to one of the vertices of degree three in G : either $g(v_3) = w_5$ or $g(v_4) = w_5$. Because g and h preserve the edge-endpoint functions, edge f_6 with endpoints w_5 and w_6 must correspond to an edge in G with endpoints v_1 and v_3, or v_1 and v_4, or v_6 and v_3, or v_6 and v_4. But this contradicts the fact that none of these pairs of vertices are connected by edges in G. Hence the supposition is false, and G and G' are not isomorphic.

Section 11.5

1. *b.* Math 110

2. *b.*
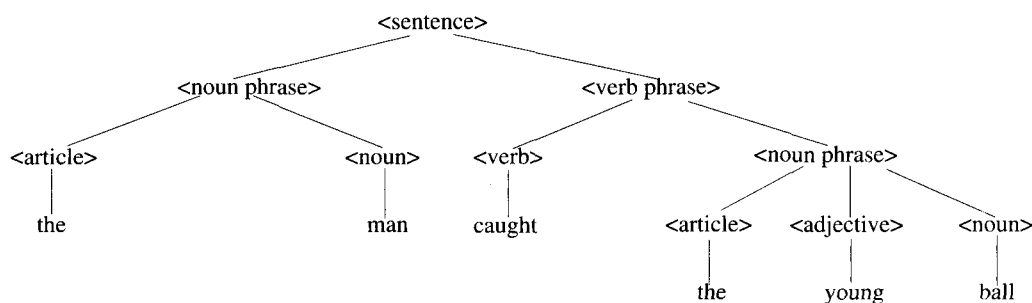
3. By Theorem 11.5.2, a tree with n vertices (where $n \geq 1$) has $n - 1$ edges, and so by Theorem 11.1.1, its total degree is twice the number of edges, or $2(n - 1) = 2n - 2$.

4. *b.*
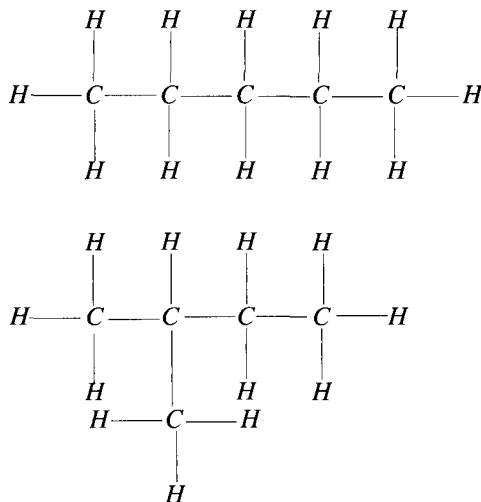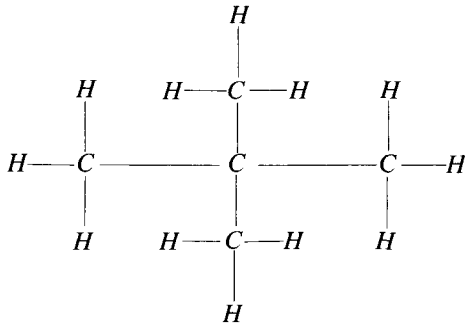
c. *Proof*: Let G be the graph of a hydrocarbon molecule with the maximum number of atoms for the number of its carbon atoms, and suppose G has k carbon atoms and m hydrogen atoms. By Example 11.5.4, G is a tree with $k + m$ vertices. By exercise 3, the total degree of this tree is $2(k + m) - 2 = 2k + 2m - 2 = 2(k + m - 1)$.

d. *Proof*: Let G be the graph of a hydrocarbon molecule with the maximum number of atoms for the number of its carbon atoms, and suppose G has k carbon atoms and m hydrogen atoms. Each carbon atom is bonded to four other atoms because otherwise an additional hydrogen atom could be bonded to it, which would contradict the assumption that the number of hydrogen atoms is maximal for the given number of carbon atoms. Hence each of the k carbon atom vertices has degree four in the graph. Also each hydrogen atom is bonded to exactly one carbon atom because otherwise the molecule would not be connected. Hence each of the m hydrogen atom vertices has degree one in the graph. It follows that the total degree of the graph is $4 \cdot k + 1 \cdot m = 4k + m$.

e. Equating the results of parts (c) and (d) above gives $2k + 2m - 2 = 4k + m$. Solving for m gives $m = 2k + 2$. In other words, a hydrocarbon molecule with k carbon atoms and a maximal number of hydrogen atoms has $2k + 2$ hydrogen atoms.

5. *Proof*: Let T be a particular but arbitrarily chosen tree that has more than one vertex, and consider the following algorithm. For justification of the various steps, see the proof of Lemma 11.5.1.

Step 1: Pick a vertex v_0 of T and let e_0 be an edge incident on v_0.

[The starting vertex and edge are given the names v_0 and e_0 that will not be changed during execution of the algorithm.]

Step 2: **if** $\deg(v_0) > 1$

    then choose e_1 to be an edge incident on v_0 such that $e_1 \neq e_0$

    else let $v_1 := v_0$ and let $e_1 := e_0$

[The name v_1 is given to the first vertex of degree 1 that is found. The second vertex of degree 1 will be named v_2. The name e_1 is given to the edge adjacent to the starting vertex along which the search for a vertex of degree 1 begins.]

Step 3: Let v' be the vertex at the other end of e_1 from v_0, and let $e := e_1$ and $v := v'$.

[The values of v and e may change many times during the search outward from v_0 toward a vertex of degree 1.]

Step 4: **while** $(\deg(v) > 1)$

    Choose e' to be an edge incident on v such that $e' \neq e$.

    Let v' be the vertex at the other end of e' from v.

    Let $e := e'$ and $v := v'$.

   end while

Step 5: **if** v_1 does not have a value

**then** let $v_1 := v$ and $e_1 := e_0$, and go to step 3

[If $\deg(v_0) \neq 1$, a vertex v_1 of degree 1 was first sought by moving away from v_0 along an edge other than e_0. Now a return is made to v_0, and the search for a second vertex of degree 1 is made by moving away from v_0 starting along e_0.]

else let $v_2 := v$

[If $\deg(v_0) = 1$, Step 5 is executed just once; otherwise it is executed twice, once to give v_1 a value and again to give v_2 a value.]

After execution of this algorithm, v_1 and v_2 are distinct vertices of degree 1.

6. Define an infinite graph G as follows: $V(G) = \{v_i \mid i \in \mathbf{Z}\} = \{\ldots, v_{-2}, v_{-1}, v_0, v_1, v_2, \ldots\}$, $E(G) = \{e_i \mid i \in \mathbf{Z}\} = \{\ldots, e_{-2}, e_{-1}, e_0, e_1, e_2, \ldots\}$, and the edge-endpoint function is defined by the rule $f(e_i) = \{v_{i-1}, v_i\}$ for all $i \in \mathbf{Z}$. Then G is circuit-free, but each vertex has degree two. G is illustrated below.
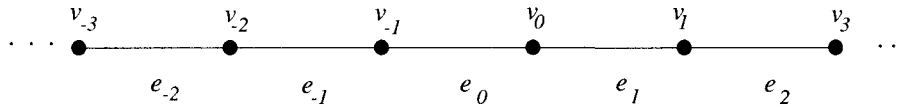
7. *b.* terminal vertices: v_1, v_2, v_5, v_6, v_8 internal vertices: v_3, v_4, v_7

15. One such graph is shown below.
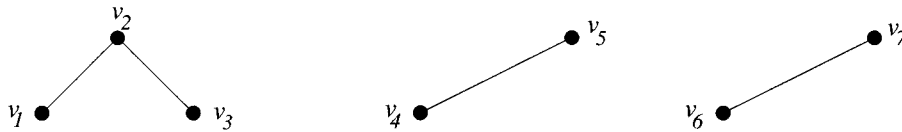
16. Any tree with twelve vertices has eleven edges, not fifteen. Thus there is no such graph.

17. One such graph is shown below.
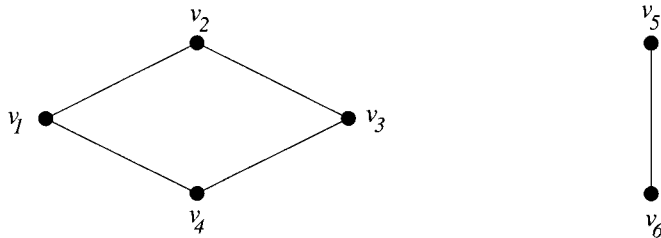
18. Any tree with five vertices has four edges. By Theorem 11.1.1, the total degree of such a graph is eight, not ten. Hence there is no such graph.

19. By Theorem 11.5.4, a connected graph with ten vertices and nine edges is a tree. By definition of tree, a tree cannot have a nontrivial circuit. Hence there is no such graph.

20. One such graph is shown below.
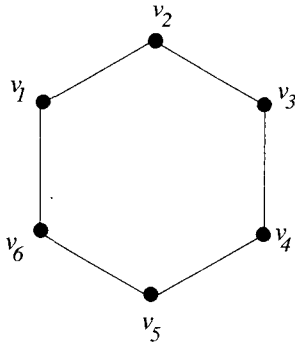
21. Any tree with ten vertices has nine edges. By Theorem 11.1.1, the total degree of such a tree is 18, not 24. Hence there is no such graph.

23. Yes, because a connected graph with no nontrivial circuits is a tree, and a tree with nine vertices has eight edges, not twelve.

24. Yes. Given any two vertices u and w of G', then u and w are vertices of G neither equal to v. Since G is connected, there is a walk in G from u to w, and so by Lemma 11.2.1, there is a path in G from u to w. This path does not include edge e or vertex v because a path does not have a repeated edge, and e is the unique edge incident on v. *[If a path from u to w leads into v, then it must do so via e. But then it cannot emerge from v to continue on to w because no edge other than e is incident on v.]* Thus this path is a path in G'. It follows that any two vertices of G' are connected by a walk in G', and so G' is connected.

26. No. Suppose there were a connected graph with n vertices and $n-2$ or fewer edges. Either the graph itself would be a tree or edges could be eliminated from its circuits to obtain a tree. In either case, there would be a tree with n vertices and $n-2$ or fewer edges. This would contradict the result of Theorem 11.5.2, which says that a tree with n vertices has $n-1$ edges. So there is no connected graph with n vertices and $n-2$ or fewer edges.

28. Yes. Suppose G is a circuit-free graph with n vertices and at least $n-1$ edges. Let $G_1, G_2, \ldots, G_k$ be the connected components of G where $k \geq 1$. Each G_i is a tree because each is connected and circuit-free. For each $i = 1, 2, \ldots, k$, let n_i be the number of vertices in G_i. Since G has n vertices in all, $n_1 + n_2 + \ldots + n_k = n$. By Theorem 11.5.2, G_i has $n_i - 1$ edges for all $i = 1, 2, \ldots, k$. So the number of edges in G is $(n_1 - 1) + (n_2 - 1) + \ldots + (n_k - 1) = (n_1 + n_2 + \ldots + n_k) - k = n - k$. But by hypothesis, G has at least $n - 1$ edges. So $n - k \geq n - 1$. It follows that $k \leq 1$, and so G has exactly one connected component. Therefore, G is connected.

29. *Proof*: Let T be a nonempty, nontrivial tree and let S be the set of all paths from one vertex to another of T. Among all the paths in S, choose a path P with the most edges. *[This is possible because since the number of vertices and edges of a graph is finite, there are only finitely many paths in T.]* The initial and final vertices of P both have degree one. For suppose that one of these vertices, say v, does not have degree one. Let e be the edge of the path that leads into v. Since $\deg(v) > 1$, there is an edge e' of T with $e \neq e'$. Add e' and the vertex at the other end of e' from v to the path. The result is a path that is longer than P (the path of maximal length), which is a contradiction. Hence the supposition is false, and so both the initial and final vertices of P have degree one.

30. Such a tree must have 4 edges and, therefore, a total degree of 8. Since at least two vertices have degree 1 and no vertex has degree greater than 4, the possible degrees of the five vertices are as follows: 1,1,1,1,4; 1,1,1,2,3; and 1,1,2,2,2. The corresponding trees are shown below.
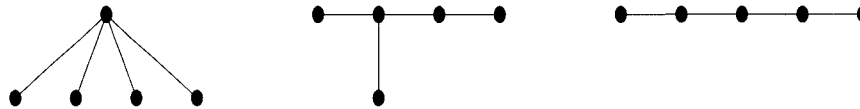
31. *a. Proof:* Suppose G and G' are isomorphic graphs and G has a vertex v of degree i that is adjacent to a vertex w of degree j (where i and j are positive integers). Since G and G' are isomorphic, there are one-to-one correspondences $g\colon V(G) \to V(G')$ and $h\colon E(G) \to E(G')$ that preserve the edge-endpoint functions in the sense that for all vertices v and edges e in G, e is an endpoint of $v \Leftrightarrow h(e)$ is an endpoint of $g(v)$. It follows that since v and w are adjacent vertices of G, $g(v)$ and $g(w)$ are adjacent vertices of G'. Let $e_1, e_2, \ldots, e_i$ be the i edges incident on v and let $f_1, f_2, \ldots, f_j$ be the j edges incident on w. Then since g and h preserve the edge-endpoint functions and h is one-to-one, $h(e_1), h(e_2), \ldots, h(e_i)$ are i distinct edges incident on $g(v)$, and $h(f_1), h(f_2), \ldots, h(f_j)$ are j distinct edges incident on $g(w)$. There are no more than i edges incident on $g(w)$ because any such edge would have to be the image under h of an edge incident on v *[because h is onto]*. Similarly, there are no more than j edges incident on $g(w)$. Hence $g(v)$ has degree i and $g(w)$ has degree j, and so G' has a vertex of degree i that is adjacent to a vertex of degree j.

b. The six nonisomorphic trees with six vertices are shown below. Note that a tree with six vertices has five edges and hence a total degree of ten. Also any such tree has at least two vertices of degree one, and it has no vertex of degree greater than five. Thus the possible degrees of the vertices of such a tree are the following: 2, 2, 2, 2, 1, 1; 3, 2, 2, 1, 1, 1; 3, 3, 1, 1, 1, 1; 4, 2, 1, 1, 1, 1; or 5, 1, 1, 1, 1, 1. Furthermore, by part (a) the two trees whose vertices have degrees 1, 1, 1, 2, 2, and 3 are not isomorphic: in one, the vertex of degree 3 is adjacent to vertices of degrees 1, 1, and 2, whereas in the other, the vertex of degree 3 is adjacent to vertices of degrees 2, 2, and 1.
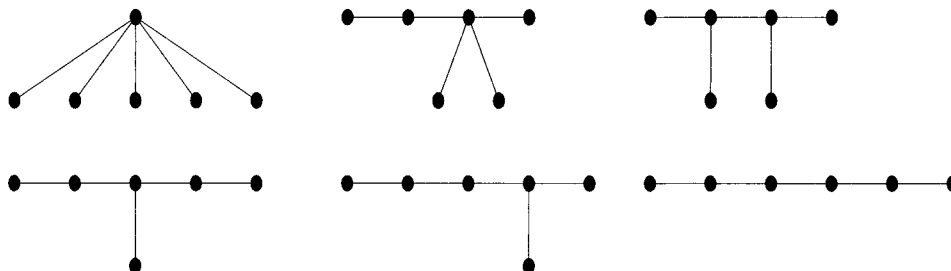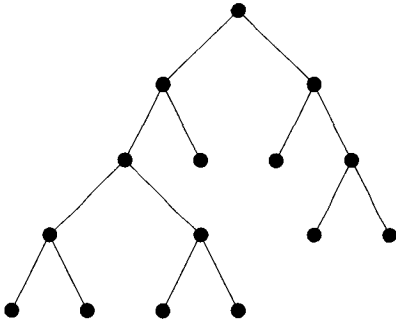

33. *a.* 3 *b.* 0 *c.* 5 *d.* v_{14}, v_{15}, v_{16} *e.* v_1 *f.* v_2 (only) *g.* v_{17}, v_{18}, v_{19}
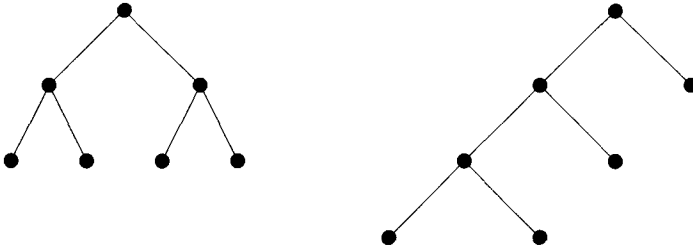
34. *b.*
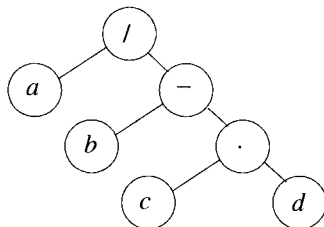
43. There is no tree with the given properties because any full binary tree with eight internal vertices has nine terminal vertices, not seven.
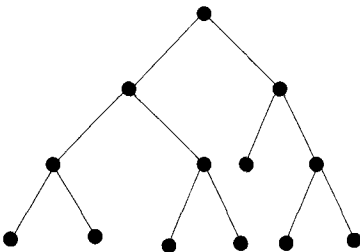
44. One such tree is the following.

45. A full binary tree with k internal vertices has $2k + 1$ vertices in all. If $2k + 1 = 7$, then $k = 3$. Thus such a tree would have three internal and four terminal vertices. Two such trees are shown below.

46. There is no tree with the given properties because a full binary tree with five internal vertices has $2 \cdot 5 + 1$ or eleven vertices in all, not nine.

47. A full binary tree with four internal vertices has five terminal vertices. One such tree is shown below.
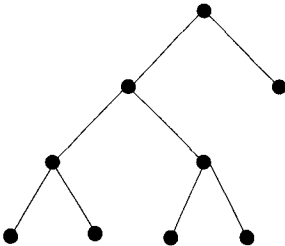

48. There is no tree with the given properties because a binary tree of height four has at most $2^4 = 16$ terminal vertices.

49. There is no tree with the given properties because a full binary tree has $2k + 1$ vertices, where k is the number of internal vertices, and $16 \neq 2k + 1$ for any integer k.

50. A full binary tree with seven terminal vertices has six internal vertices. One such tree of height three is shown below.
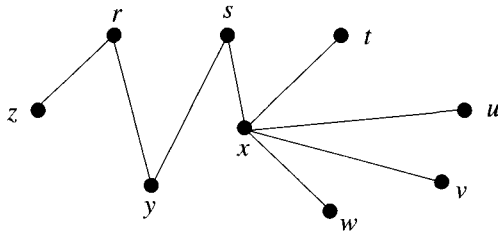
51. *b.* height $\geq \log_2 40 \cong 5.322$. Since the height of a tree is an integer, the height must be at least 6.

c. height $\geq \log_2 60 \cong 5.907$. Since the height of a tree is an integer, the height must be at least 6.
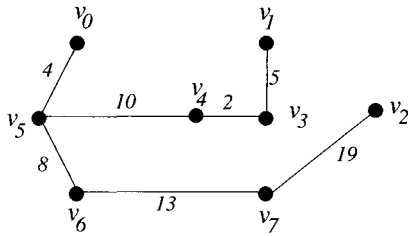
Section 11.6

2.
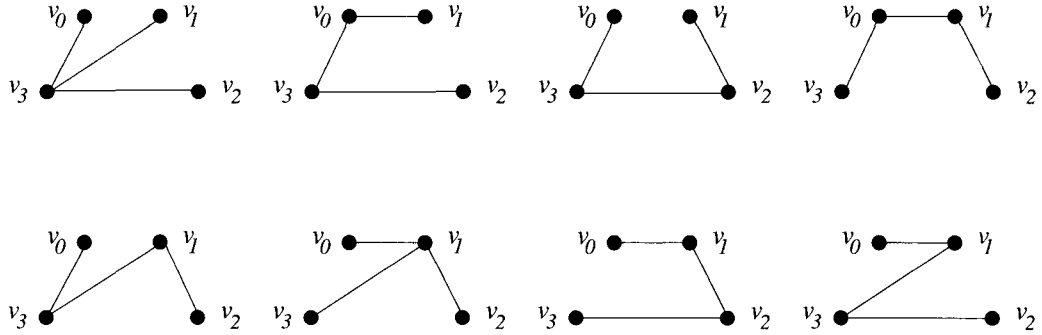
4. One of many spanning trees is the following.

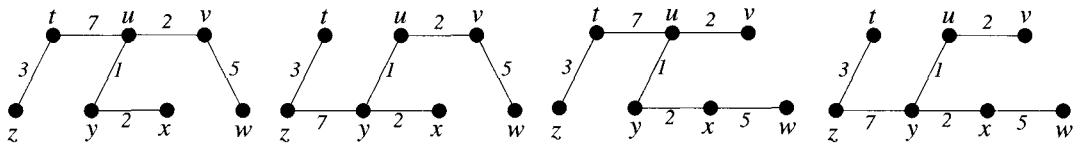6. Minimum spanning tree:

Order of adding the edges: $\{v_3, v_4\}$, $\{v_0, v_5\}$, $\{v_1, v_3\}$, $\{v_5, v_6\}$, $\{v_4, v_5\}$, $\{v_6, v_7\}$, $\{v_2, v_7\}$
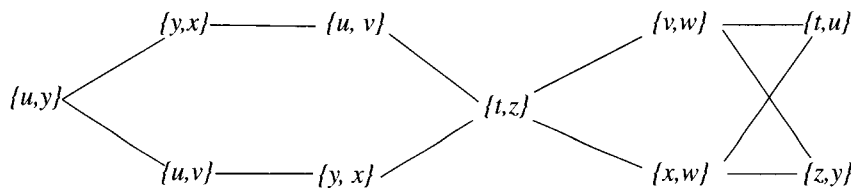
8. Minimum spanning tree: same as in exercise 6.

Order of adding the edges: $\{v_0, v_5\}$, $\{v_5, v_6\}$, $\{v_5, v_4\}$, $\{v_4, v_3\}$, $\{v_3, v_1\}$, $\{v_6, v_7\}$, $\{v_7, v_2\}$
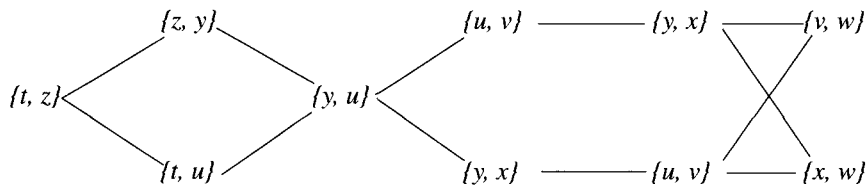
10. There are four minimum spanning trees:

When Kruskal's algorithm is used, edges are added in any of the orders obtained by following one of the eight paths from left to right across the diagram below.

$\{y,x\}$———$\{u, v\}$ $\{v,w\}$———$\{t,u\}$

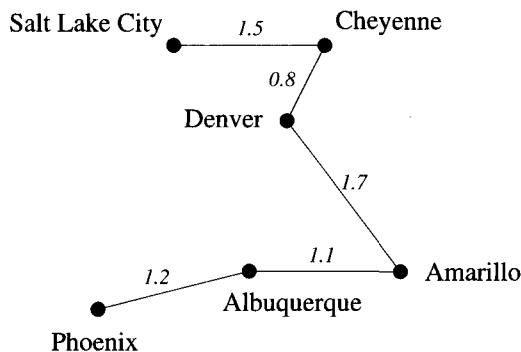$\{u,y\}$ $\{t,z\}$

$\{u,v\}$———$\{y, x\}$ $\{x,w\}$———$\{z,y\}$

When Prim's algorithm is used, edges are added in any of the orders obtained by following one of the eight paths from left to right across the diagram below.

$\{z, y\}$ $\{u, v\}$———$\{y, x\}$———$\{v, w\}$

$\{t, z\}$ $\{y, u\}$

$\{t, u\}$ $\{y, x\}$———$\{u, v\}$———$\{x, w\}$

11.

Salt Lake City 1.5 Cheyenne

0.8

Denver

1.7

1.2 1.1 Amarillo

Phoenix Albuquerque

12. *Proof*: Suppose T_1 and T_2 are spanning trees for a graph G with n vertices. By definition of spanning tree, both T_1 and T_2 contain all n vertices of G, and so by Theorem 11.5.2, both T_1 and T_2 have $n - 1$ edges.

13. *a.* If there were two distinct paths from one vertex of a tree to another, they (or pieces of them) could be patched together to obtain a nontrivial circuit. But a tree cannot have a nontrivial circuit.

14. *Proof*: Suppose that G is a graph with n vertices and with spanning tree T, and suppose e is an edge of G that is not in T.

(1) Let H be the graph obtained by adding e to T. Then H has n vertices and n edges and is connected, and so H contains a nontrivial circuit *[because if H were both connected and circuit-free, then H would be a tree and would therefore have $n - 1$ edges which it does not]*.

(2) Suppose H contains two distinct sets of edges that form nontrivial circuits C_1 and C_2. Then one of the circuits, say C_1, would contain an edge, say e_1, not contained in C_2. Remove e_1 from H to obtain a graph H'. By Lemma 11.5.3, H' is connected. Since e_1 is not in C_2, and e_1 was the only edge removed from H to obtain H', C_2 is a circuit in H'. Remove an edge from C_2 to obtain a graph H''. Again, by Lemma 11.5.3, H'' is connected. Then H'' is a connected graph with $n - 2$ edges that contains all n vertices of G. By Proposition 11.6.1 (or by exercise 26 of Section 11.5), this is impossible. Hence the supposition is false, and so the graph obtained by adding e to T contains at most one circuit.

By (1) and (2) above, T contains one and only one nontrivial circuit.

16. *b. Counterexample*: Let G be the following simple graph.
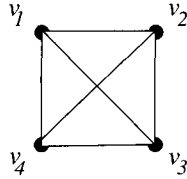
Then G has the spanning trees shown below.
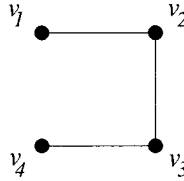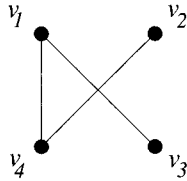
These trees have no edge in common.

17. *Proof*:

($\Rightarrow$) Let G be a graph and e an edge that is contained in every spanning tree for G. Suppose that removal of e does not disconnect G. Let G' be the graph obtained by removing e from G. Then G' is connected, and so it has a spanning tree T' (by Proposition 11.6.1). But T' contains every vertex of G (because no vertices were removed from G to create G'), and every edge in T' is also an edge in G (by construction). Hence T' is a spanning tree for G that does not contain e. This contradicts the fact that e is contained in every spanning tree for G. Hence the supposition is false, and so removal of e disconnects G .

($\Leftarrow$) Let G be a graph and e an edge of G such that removal of e disconnects G. Suppose there is a spanning tree T of G that does not contain e. Then T is a connected subgraph of G that does not contain e. Hence removal of e plus (possibly) other edges from G does not disconnect G, which implies that removal of e alone from G does not disconnect G, a contradiction. Hence the supposition is false, and so e is contained in every spanning tree T of G.

18. *Proof*: Since T_2 is obtained from T_1 by removing e' and adding e, $w(T_2) = w(T_1) - w(e') + w(e)$. Now according to the proof of Theorem 11.6.3, $w(e') \geq w(e)$. Hence $w(e') - w(e) \geq 0$, and so $w(T_2) = w(T_1) - (w(e') - w(e)) \leq w(T_1)$.

20. *Proof*: Let G be a connected, weighted graph, and let e be an edge of G (not a loop) that has smaller weight than any other edge of G. Suppose there is a minimum spanning tree T that does not contain e. Since T is a spanning tree, T contains the endpoints v and w of e. By exercise 13, there is a unique path in T from v to w. Let e' be any edge along this path. By exercise 19, $w(e') \leq w(e)$. This contradicts the fact that $w(e)$ has smaller weight than any other edge of G. Hence the supposition is false: every minimum spanning tree contains e.

22. *Proof*: Suppose not. Suppose G is a connected, weighted graph, e is an edge of G that (1) has larger weight than any other edge of G and (2) is in a circuit of G, and suppose that there is a minimum spanning tree T for G that contains e. Construct another tree T' as follows: Let v and w be the endpoints of e. Because e is part of a circuit in G, there is a path in G that joins v and w. Also there is an edge e' of this path such that e' is not an edge of T (for otherwise T would contain a circuit). Form T' by removing e from T and adding e'. Then T' contains all n vertices of G, has $n - 1$ edges, and is connected *[because T is connected and contains all the vertices of G, and so some edges of T must be incident on the endpoints of e']*.

By Theorem 11.5.4, therefore, T' is a tree. But T' also contains all the vertices of G [because T' is formed from T by adding and deleting only edges], and so T' is a spanning tree for G. Now $w(T') = w(T) - w(e) + w(e') = w(T) - (w(e) - w(e')) < w(T)$ because $w(e) > w(e')$. Thus T' is a spanning tree of smaller weight than a minimum spanning tree for G, which is a contradiction. Hence the supposition is false, and the given statement is true.

24. The output will be a minimum spanning tree for the connected component of the graph that contains the starting vertex input to Prim's algorithm.

25. *Proof*: Suppose that G is a connected, weighted graph with n vertices and that T is the output graph produced when G is input to Algorithm 11.6.3. Clearly T is a subgraph of G and T is connected because no edge is removed from T as T is being constructed if its removal would disconnect T. Also T is circuit-free because if T had a circuit then the circuit would contain edges $e_1, e_2, \ldots, e_k$ of maximal weight. At some point during execution of the algorithm, each of these edges would be examined (since all edges are examined eventually). Let e_i be the first such edge to be examined. When examined, e_i must be removed because deletion of an edge from a circuit does not disconnect a graph and at the time e_i is examined no other edge of the circuit would have been removed. But this contradicts the supposition that e_i was one of the edges in the output graph T. Thus T is circuit-free. Furthermore, T contains every vertex of G since only edges, not vertices, are removed from G in the construction of T. Hence T is a spanning tree for G.

Next we show that T has minimum weight. Let T_1 be any minimum spanning tree for G. If $T = T_1$, we are done. If $T \neq T_1$, then there is an edge e of T that is not in T_1. Now adding e to T_1 produces a graph with a unique set of edges that forms a circuit C (by exercise 14). Let e' be an edge of C that is not in T, and let T_2 be the graph obtained from T_1 by removing e' and adding e. Note that T_2 has $n - 1$ edges and n vertices and that T_2 is connected. Consequently, T_2 is a spanning tree for G. Now $w(e') \leq w(e)$ because at the stage in Algorithm 11.6.3 when e' was deleted from T, e was also available to be deleted from T [since it was in T, and at that stage its deletion would not have disconnected T because e' was also in T and so were all the other edges in C which stayed in T throughout execution of the algorithm], and e would have been deleted from T if its weight had been greater than that of e'. Therefore, $w(T_2) = w(T_1) - w(e') + w(e) = w(T_1) - (w(e') - w(e)) \leq w(T_1)$. Since T_1 is a minimum spanning tree and T_2 is a spanning tree with weight less than or equal to T_1, T_2 is also a minimum spanning tree for G. In addition, T_2 has one more edge in common with T than does T_1. [The remainder of the proof is identical to the last few lines of the proofs of Theorems 11.6.2 and 11.6.3.] If T now equals T_2, then we are done. If not, then, as above, we can find another minimum spanning tree T_3 having one more edge in common with T than T_2. Continuing in this way produces a sequence of minimum spanning trees $T_1, T_2, T_3, \ldots$ each of which has one more edge in common with T than the preceding tree. Since T has only a finite number of edges, this sequence if finite, and so for some k, T_k is identical to T. This shows that T is itself a minimum spanning tree.

Chapter 12: Regular Expressions and Finite-State Automata

This chapter opens with some historical background about the connections between computers and formal languages. Section 12.1 focuses on regular expressions and emphasizes their utility for pattern matching, whether for compilers or for general text processing.

Section 12.2 introduces the concept of finite-state automaton. In one sense, it is a natural sequel to the discussions of digital logic circuits in Section 1.4 and Boolean functions in Section 7.1, with the next-state function of an automaton governing the operation of sequential circuit in much the same way that a Boolean function governs the operation of a combinatorial circuit. Students seem genuinely to enjoy working with automata. When you present the section in class, it is helpful to nice lead in to the concept of the language accepted by an automaton by including the following kind of example: for a particular finite-state automaton under discussion, give a list of strings and ask students to determine whether or not these strings are accepted by the automaton. The section also gives students significant practice in finding a finite-state automaton that corresponds to a regular expression and shows how to write a program to implement a finite-state automaton. Both abilities are useful for computer programming. The section ends with a statement and partial proof of Kleene's theorem, which describes the exact nature of the relationship between finite-state automata and regular languages.

The equivalence and simplification of finite-state automata, discussed in Section 12.3, provides an additional application for the concept of equivalence relation, introduced in Section 10.3. Because equivalence of digital logic circuits is defined in Section 10.3, when covering Section 12.3, you can draw parallels between the simplification of digital logic circuits discussed in Section 1.4 and the simplification of finite-state automata developed in this section. Both kinds of simplification have obvious practical use.

Section 12.1

2. a. $L_3 = \{\epsilon, y, y, yy, yy, yyy, x, xy, xyy, xx, xxy, xxx\}$

   b. $\sum^4 = \{xxxx, xxxy, xxyx, xxyy, xyxx, xyxy, xyyx, xyyy, yxxx, yxxy, yxyx, yxyy,$
   $yyxx, yyxy, yyyx, yyyy\}$

   c. A is the set of all strings of length 1 or 2, B is the set of all strings of length 3 or 4 and $A \cup B$ is the set of all non-empty strings of length ≤ 4.

3. $L = \{11*, 11/, 12*, 12/, 21*, 21/, 22*, 22/\}$

   $11* = 1*1 = 1$, $11/ = 1/1 = 1$, $12* = 1*2 = 2$, $12/ = 1/2 = 0.5$, $21* = 2*1 = 2$, $21/ = 2/1 = 2$, $22* = 2*2 = 4$, $22/ = 2/2 = 1$

5. $L_1 L_2$ is the set of all strings of a's, b's and c's with an equal number of a's and b's and with all the c's at the end of the string. Note that $\epsilon \in L_1 L_2$.

   $L_1 \cup L_2$ is the set of all strings of a's and b's that consist of only c's or that have no c's but have an equal number of a's and b's. Note that $\epsilon \in L_1 \cup L_2$.

   $(L_1 \cup L_2)^*$ is the set of all strings of a's and b's and c's such that every substring containing no c's and having maximal length has an equal number of a's and b's.

6. $L_1 L_2$ is the set of strings of 0's and 1's that both start and end with a 0.

   $L_1 \cup L_2$ is the set of strings of 0's and 1's that start with a 0 or end with a 0 (or both).

   $(L_1 \cup L_2)^*$ is the set of strings of 0's and 1's that start with a 0 or end with a 0 (or both) or that contain 00.

8. $(((0^*)1) \mid (0((0^*)1)^*))$

9. $(((x \mid (y(z^*)))^*)((yx) \mid (((yz)^*)z)))$

11. $11^* \mid 10^* \mid 1^*1$ (Note that by definition of the $\mid$ symbol, this expression can be written more simply as $1^*1 \mid 10^*$. If the $^+$ notation is used, it can be further simplified to $1^+ \mid 10^*$.)

12. $xy(x^*y)^* \mid (yx \mid y)y^*$

14. $L(\emptyset \mid \epsilon) = L(\emptyset) \cup L(\epsilon) = \emptyset \cup \{\epsilon\} = \{\epsilon\}$

15. $L((a \mid b)c) = L(a \mid b)L(c) = (L(a) \cup L(b))L(c) = (\{a\} \cup \{b\})\{c\} = \{a, b\}\{c\} = \{ac, bc\}$

17. $\epsilon, b, bb, bab, ab, ba, a, \ldots$

18. $x, yxxy, xx, xyxxy, xyxxyyxxy, \ldots$

20. The language consists of the set of all strings of 0's and 1's that start with a 1 and end with 00 (and contain any number of 0's and 1's in between).

21. The language consists of the set of all strings of x's and y's that start with xy or yy followed by any string of x's and y's.

23. The string $zyyxz$ does not belong to the language defined by $(x^*y \mid zy^*)^*$ because any x in the language must be followed by possibly more x's and then a y (which could be followed by other symbols). On the other hand $zyyzy$ belongs to the language because both zyy and zy belong to zy^* and the language is closed under concatenation.

24. The string 120 does not belong to the language defined by $(01^*2)^*$ because it does not start with 0. However, 01202 does belong to the language because 012 and 02 are both defined by 01^*2 and the language is closed under concatenation.

26. $(a \mid b)^*b(a \mid b)(a \mid b)$

27. $x \mid y^* \mid y^*(xyy^*)(\epsilon \mid x)$

29. These languages are not the same because $rsrs$ is in the language defined by $(rs)^*$, but it is not in the language r^*s^*.

30. Note that for any regular expression x, $(x^*)^*$ defines the set of all strings obtained by concatenating a finite number of a finite number of concatenations of copies of x. But any such string can equally well be obtained simply by concatenating a finite number of copies of x, and thus $(x^*)^* = x^*$. Hence the given languages are the same: $L((rs)^*) = L(((rs)^*)^*)$.

32. $[A - Z]^*BIO[A - Z]^*)\mid([A - Z]^*INFO[A - Z]^*$

33. $[a - z]\{3\}[a - z]^*ly$

35. $[\hat{}\,aeiou]^*(a|e|i|o|u)[\hat{}\,aeiou]^*$

36. $[\hat{}\,AEIOU][A - Z]^*[A|E|I|O|U]\{2\}[A - Z]^*$

38. $(800|888) - [0 - 9]\{3\} - 2[0 - 9]\{2\}2$

40. The following string is broken up into four sections corresponding to (1) months with 30 days (those numbered 4, 6, 9, and 11), (2) months with 31 days (those numbered 1,3, 5, 7, 8, 10, and 12), (3) months with 29 days (month 2, in leap years), and (4) months with 28 days (month 2, in non-leap years).

$(((([4\ 6\ 9\ 11] \mid 0[4\ 6\ 9])[- /]([1 - 30] \mid 0[1 - 9])[- /][0 - 9]\{2\})$

$\mid ((([1\ 3\ 5\ 7\ 8\ 10\ 12] \mid 0[1\ 3\ 5\ 7\ 8])[- /]([1 - 31] \mid 0[1 - 9])[- /][0 - 9]\{2\})$

$\mid (2 \mid 02)[- /]([1 - 29] \mid 0[1 - 9])[- /]([0\ 2\ 4\ 6\ 8][0\ 4\ 8] \mid [1\ 3\ 5\ 7\ 9][2\ 6]))$

$\mid (2 \mid 02)[- /]([1 - 28] \mid 0[1 - 9])[- /]([0\ 2\ 4\ 6\ 8][1\ 2\ 3\ 5\ 6\ 7\ 9] \mid [1\ 3\ 5\ 7\ 9][0\ 1\ 3\ 4\ 5\ 7\ 8\ 9]))$

41. $(00 \mid 11 \mid (01 \mid 10)(00 \mid 11)^*(01 \mid 10))^*$

Section 12.2

1. *b.* \$1 or more deposited. *c.* 75 ¢ deposited

3. *a.* U_0, U_1, U_2, U_3 *b.* a, b *c.* U_0 *d.* U_3

    e.

state	input a	b
$\rightarrow$ U_0	U_2	U_1
U_1	U_2	U_3
U_2	U_2	U_2
◎ U_3	U_3	U_3

4. *a.* s_0, s_1, s_2 *b.* $0, 1$ *c.* s_0 *d.* s_2

    e.

state	input 0	1
$\rightarrow$ s_0	s_1	s_0
s_1	s_2	s_0
◎ s_2	s_2	s_0

6. *a.* s_0, s_1, s_2, s_3 *b.* $0, 1$ *c.* s_0 *d.* s_0

    e.

state	input 0	1
$\rightarrow$ ◎ s_0	s_0	s_1
s_1	s_1	s_2
s_2	s_2	s_3
s_3	s_3	s_0

9. *a.* s_0, s_1, s_2, s_3 *b.* $0, 1$ *c.* s_0 *d.* s_1

    e.
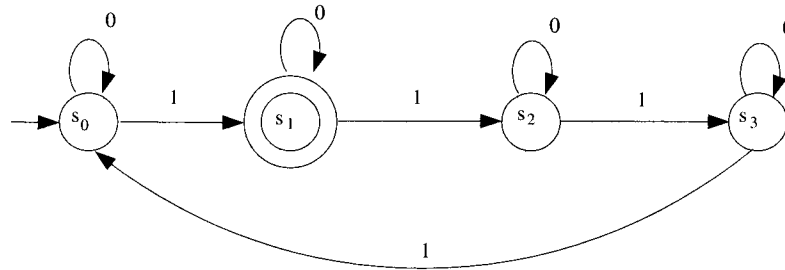
10. *b.* $N(s_2, 0) = s_3$, $N(s_1, 0) = s_3$ *d.* $N^*(s_2, 11010) = s_3$, $N^*(s_0, 01000) = s_3$

11. *b.* $N(s_0, 0) = s_1$, $N(s_4, 1) = s_3$ *d.* $N^*(s_0, 1111) = s_3$, $N^*(s_2, 00111) = s_2$

13. *a.* (i) U_3 (ii) U_2 (iii) U_2 (iv) U_3

    b. *bb* and *bbaaaabaa*

    c. The language accepted by this automaton is the set of all strings of a's and b's that begin *bb*.

    d. $bb(a \mid b)^*$

16. *a.* The language accepted by this automaton is the set of all strings of 0's and 1's in which the number of 1's is divisible by 4.

 b. $(0^*10^*10^*10^*10^*)^*$

19. *a.* The language accepted by this automaton is the set of all strings in which the number of 1's has the form $4k + 1$ for some integer k.

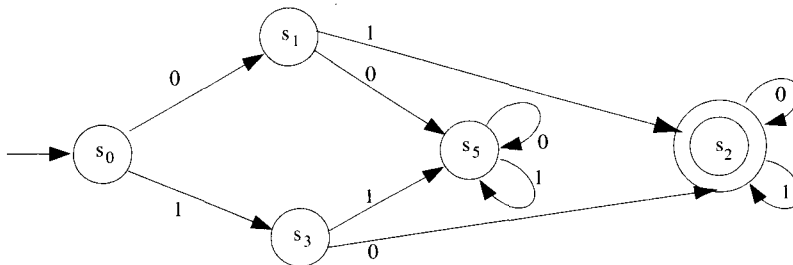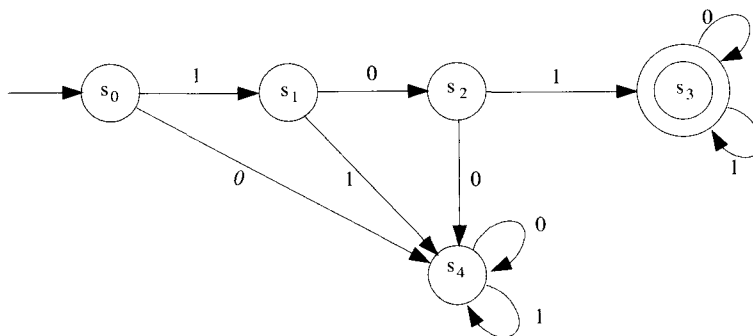 *b.* $(0 \mid 10^*10^*10^*1)^*10^*$

21. *a.*
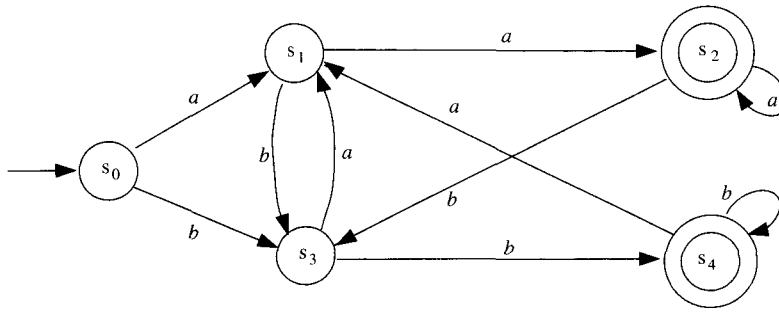
 b. $(a|b)^*(aa|bb)$

22. *a.*

 b. $(01|10)(0|1)^*$

24. *a.*

 b. $101(0|1)^*$

27. *a.*
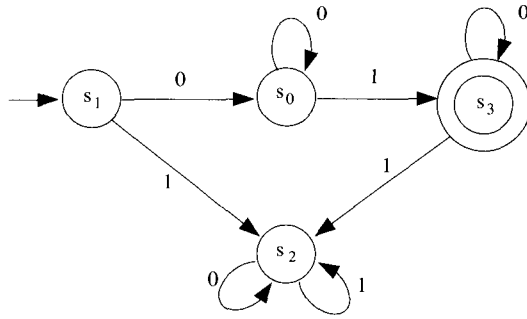
b. 00*10* (or using the $^+$ notation: 0^+10^*)

30.
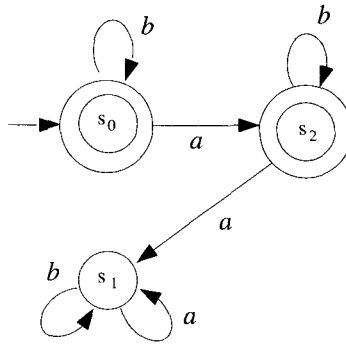
32.
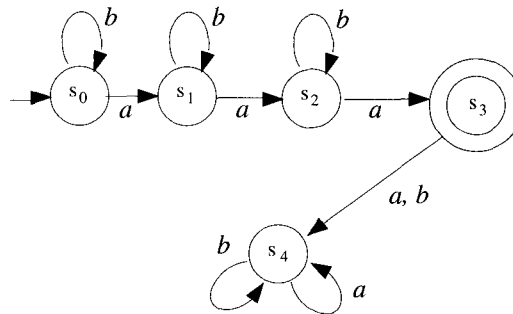
34.
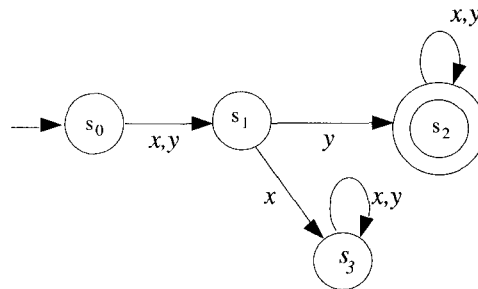
35.
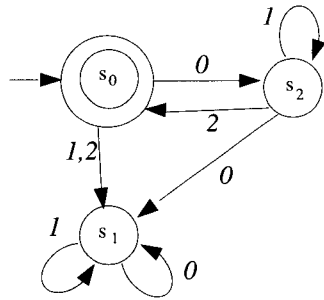
37.
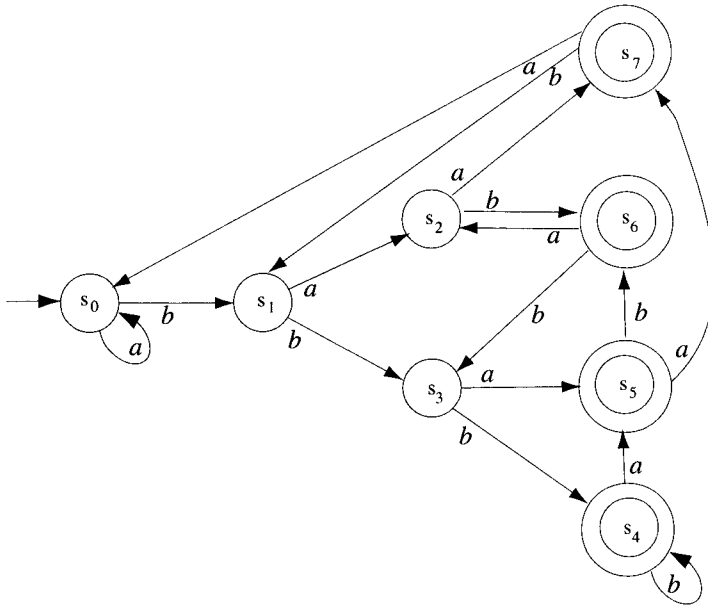
38.
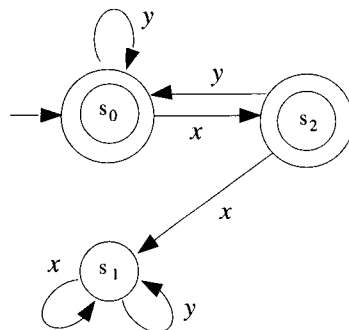
40.
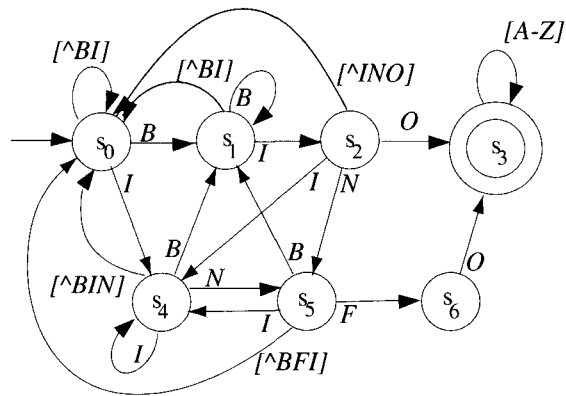
41.
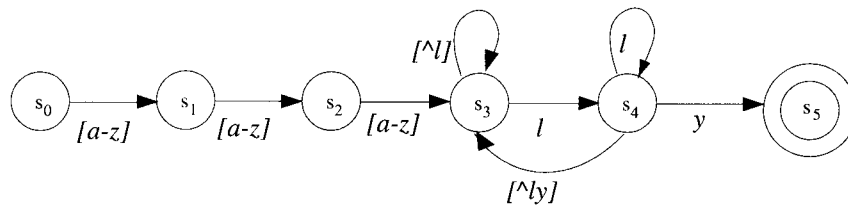
43.
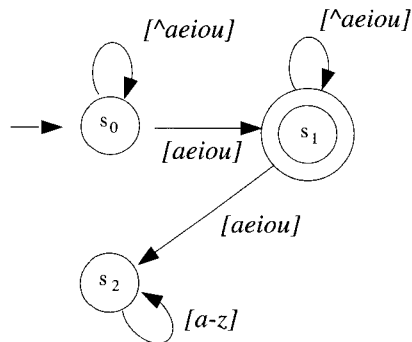
44.
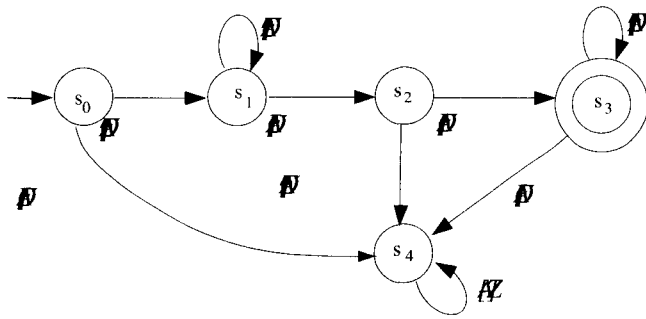
46. Let d represent the character class $[0-9]$. Also any input symbol that is not labeled as an explicit transition from one state to another should be understood to lead to an error state. For simplicity, this error state is not shown.
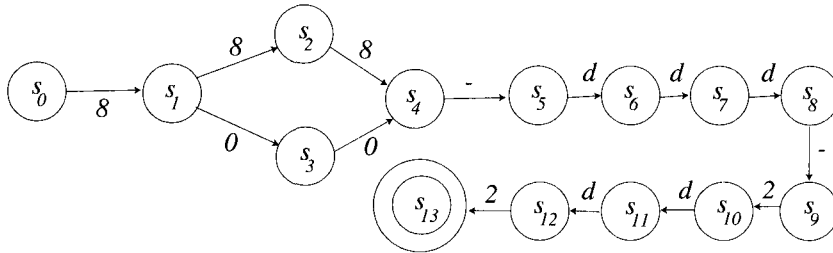
47. To simplify the appearance of this regular expression, we let d denote the character class $[0-9]$. Then the regular expression for signed or unsigned numbers is denoted $((+\mid-\mid\epsilon)(d^+\mid d^+\backslash.d^+\mid.d^+\mid\backslash.d^+)$. (Following standard usage, we exclude numbers of the form 2. or 147., which contain a decimal point but no decimal expansion.)
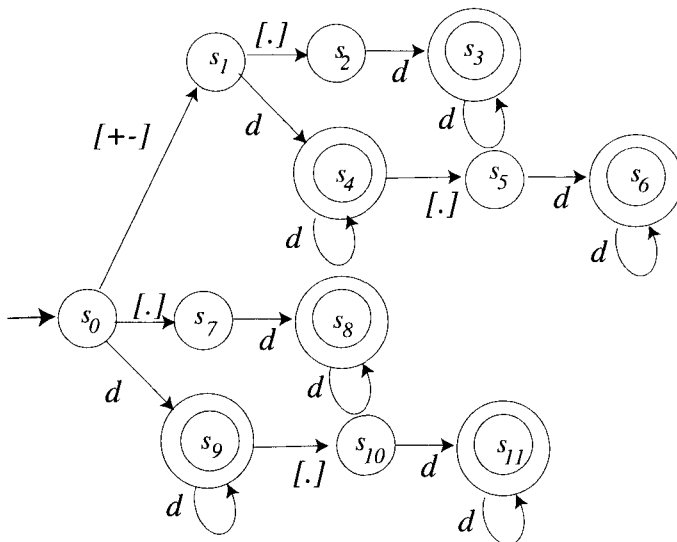
48. Let d represent the character class $[0-9]$.
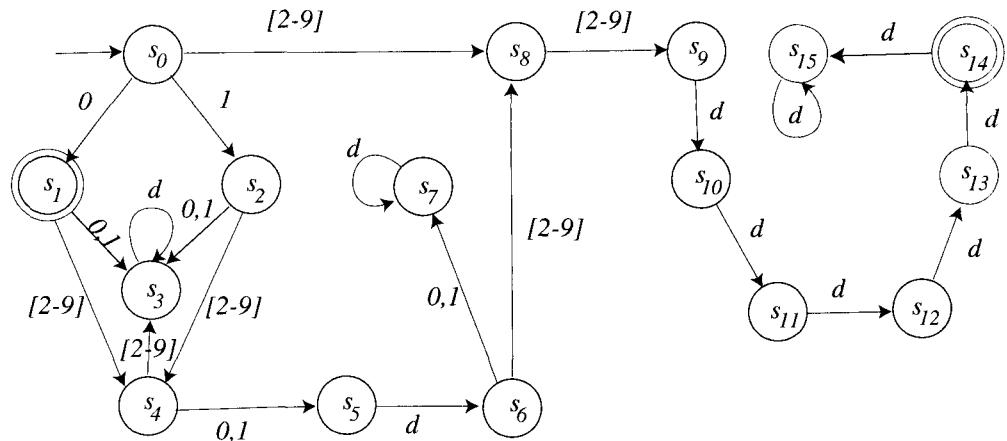
49.

Algorithm 12.2.3 Finite-State Automaton of Exercise 2

[This algorithm simulates the action of the finite-state automaton of exercise 2 by mimicking the functioning of the transition diagram. The states are denoted 0, 1, and 2.]

Input: *string [a string of 0's and 1's plus an end marker e]*

Algorithm Body:

$state := 0$

$symbol :=$ first symbol in the input string

while $(symbol \neq e)$

if $state = 0$ **then if** $symbol = 0$

$\qquad\qquad\qquad$ **then** $state := 1$

$\qquad\qquad\qquad$ **else** $state := 0$

else if $state = 1$ **then if** $symbol = 0$

$\qquad\qquad\qquad$ **then** $state := 1$

$\qquad\qquad\qquad$ **else** $state := 2$

else if $state = 2$ **then if** $symbol = 0$

$\qquad\qquad\qquad$ **then** $state := 2$

$\qquad\qquad\qquad$ **else** $state := 2$

$symbol :=$ next symbol in the input string

end while

Output: *state*

50.

Algorithm 12.2.4 Finite-State Automaton of Exercise 8

[This algorithm simulates the action of the finite-state automaton of exercise 8 by repeated application of the next-state function. The states are denoted 0, 1, and 2.]

Input: *string [a string of 0's and 1's plus an end marker e]*

Algorithm Body:

$N(0,0) := 1, N(0,1) := 2, N(1,0) := 1, N(1,1) := 2, N(2,0) := 1, N(2,1) := 2,$

$state := 0$

$symbol :=$ first symbol in the input string

while ($symbol \neq e$)

    $state := N(state, symbol)$

    $symbol :=$ next symbol in the input string

end while

Output: $state$

51. *Proof (by contradiction)*: Suppose there were a finite-state automaton A that accepts L. Consider all strings of the form a^i for some integer $i \geq 0$. Since the set of all such strings is infinite and the number of states of A is finite, by the pigeonhole principle at least two of these strings, say a^p and a^q with $p < q$, must send A to the same state, say s, when input to A starting in its initial state. (The strings of the given form are the pigeons, the states are the pigeonholes, and each string is associated with the state to which A goes when the string is input to A starting in its initial state.) Because A accepts L, A accepts $a^q b^q$ but not $a^p b^q$. But since $a^q b^q$ is accepted by A, inputting b^q to A when it is in state s (after input of a^q) sends A to an accepting state. Because A also goes to state s after input of a^p, inputting b^q to A after inputting a^p also sends A to an accepting state. Thus $a^p b^q$ is accepted by A and yet it is not accepted by A, which is a contradiction. Hence the supposition is false: there is no finite-state automaton that accepts L.

52. *Proof (by contradiction)*: Suppose there were a finite-state automaton A that accepts L. Consider all strings of the form a^i for some integer $i \geq 0$. Since the set of all such strings is infinite and the number of states of A is finite, by the pigeonhole principle at least two of these strings, say a^p and a^q with $p < q$, must send A to the same state, say s, when input to A starting in its initial state. Because A accepts L, A accepts $a^p b^p$ but not $a^q b^p$. But since $a^p b^p$ is accepted by A, inputting b^p to A when it is in state s (after input of a^p) sends A to an accepting state. Because A also goes to state s after input of a^q, inputting b^p to A after inputting a^q also sends A to an accepting state. Thus $a^q b^p$ is accepted by A and yet it is not accepted by A, which is a contradiction. Hence the supposition is false: there is no finite-state automaton that accepts L.

53. *Proof 1 (by contradiction)*: Suppose there were a finite-state automaton A that accepts L. Let N be the number of states in A. Choose an integer m with $(m+1)^2 - m^2 > N$. *[Such an integer exists because $(m+1)^2 - m^2 = 2m+1$, and $2m+1 > N$ if, and only if, $m > (N-1)/2$. So any integer m with $m > (N-1)/2$ will work.]* Consider the set of all strings a^i with $m^2 < i \leq (m+1)^2$. Since $(m+1)^2 - m^2 > N$ and A has N states, there exist integers p and q so that $m^2 < p < q \leq (m+1)^2$ and both a^p and a^q send A to the same state s. *[This follows from the pigeonhole principle: the $2m+1$ strings a^i with $m^2 < i \leq (m+1)^2$ are the pigeons and the N states are the pigeonholes.]* Now $a^{(m+1)^2}$ is in L and hence sends A to an accepting state. But $(m+1)^2 = q + ((m+1)^2 - q)$, and so $a^{(m+1)^2} = a^q a^{(m+1)^2 - q}$. This implies that when A is in state s, input of $a^{(m+1)^2 - q}$ sends A to an accepting state. Since a^p also sends A to state s, it follows that $a^p a^{(m+1)^2 - q} = a^{p + (m+1)^2 - q} = a^{(m+1)^2 - (q-p)}$ sends A to an accepting state also. Let $k = (m+1)^2 - (q-p)$. Then a^k is accepted by A. However, a^k is not in L because $(m+1)^2 - (q-p)$ is not a perfect square. (The reason is that since $m^2 < p < q \leq (m+1)^2$, then $q - p < (m+1)^2 - m^2$, and so $m^2 < (m+1)^2 - (q-p)$. Furthermore $(m+1)^2 - (q-p) < (m+1)^2$ because $q - p > 0$. Hence $k = (m+1)^2 - (q-p)$ is in between two successive perfect squares and so is not a perfect square.) This result contradicts the supposition that A is an automaton that accepts L. Hence the supposition that A exists is false.

Proof 2 (by contradiction): Suppose there were a finite-state automaton A that accepts all strings of the form a^n where $n = m^2$ for some positive integer m. Since there are infinitely many strings of the form a^i for some integer $i \geq 1$ and A has only finitely many states, at least two strings a^p and a^q with $0 < p < q$ must go to the same state s. Consider the strings $a^p a^{(q-1)q}$ and $a^q a^{(q-1)q} = a^{q^2}$. Since A accepts strings of the form a^{m^2}, it will accept $a^q a^{(q-1)q}$. But since A will be in the same state after processing a^p as it is after processing a^q, it will also accept $a^p a^{(q-1)q} = a^{q^2-(q-p)}$. Now $q^2 - (q-p) \neq m^2$ for any integer m. The reason is that since p and q are integers with $0 < p < q$, then $q + p > 1$. It follows that $q^2 - 2q + 1 < q^2 - (q-p)$, and so $(q-1)^2 < q^2 - (q-p)$. Furthermore, since $q - p > 0$, $q^2 - (q-p) < q^2$. Hence $(q-1)^2 < q^2 - (q-p) < q^2$. Thus on the one hand A accepts $a^{q^2-(q-p)}$ but on the other hand A does not accept $a^{q^2-(q-p)}$ because $q^2 - (q-p)$ is not a perfect square. This is a contradiction. It follows that the supposition that A exists is false.

54. *a. Proof*: Suppose A is a finite-state automaton with input alphabet $\sum$, and suppose $L(A)$ is the language accepted by A. Define a new automaton A' as follows: Both the states and the input symbols of A' are the same as the states and input symbols of A. The only difference between A and A' is that each accepting state of A is a non-accepting state of A', and each non-accepting state of A is an accepting state of A'. It follows that each string in $\sum^*$ that is accepted by A is not accepted by A', and each string in $\sum^*$ that is not accepted by A is accepted by A'. Thus $L(A') = (L(A))^c$.

b. Proof: Let A_1 and A_2 be finite-state automata, and let $L(A_1)$ and $L(A_2)$ be the languages accepted by A_1 and A_2, respectively. By part (a), there exist automata A_1' and A_2' such that $L(A_1') = (L(A_1))^c$ and $L(A_2') = (L(A_2))^c$. Hence, by Kleene's theorem (part 1), there are regular expressions r_1 and r_2 that define $(L(A_1))^c$ and $(L(A_2))^c$, respectively. So we may write $(L(A_1))^c = L(r_1)$ and $(L(A_2))^c = L(r_2)$. Now by definition of regular expression, $r_1 \mid r_2$ is a regular expression, and, by definition of the language defined by a regular expression, $L(r_1 \mid r_2) = L(r_1) \cup L(r_2)$. Thus, by substitution and De Morgan's law, $L(r_1 \mid r_2) = (L(A_1))^c \cup (L(A_2))^c = (L(A_1) \cap L(A_2))^c$, and so, by Kleene's theorem (part(2)), there is a finite-state automaton, say A, that accepts $(L(A_1) \cap L(A_2))^c$. It follows from part (a) that there is a finite-state automaton, A', that accepts $((L(A_1) \cap L(A_2))^c)^c$. But, by the double complement law for sets, $((L(A_1) \cap L(A_2))^c)^c = L(A_1) \cap L(A_2)$. So there is a finite-state automaton, A', that accepts $L(A_1) \cap L(A_2)$, and hence, by Kleene's theorem and the definition of regular language, $L(A_1) \cap L(A_2)$ is a regular language.

Section 12.3

2. *a.* 0-equivalence classes: $\{s_0, s_1, s_3, s_4\}$, $\{s_2, s_5, s_6\}$

   1-equivalence classes: $\{s_0, s_1\}$, $\{s_3\}$, $\{s_4\}$, $\{s_2, s_5\}$, $\{s_6\}$

   2-equivalence classes: $\{s_0, s_1\}$, $\{s_3\}$, $\{s_4\}$, $\{s_2, s_5\}$, $\{s_6\}$

   b. transition diagram for $\bar{A}$:
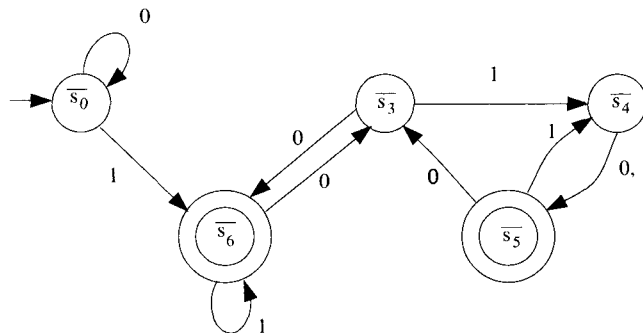
3. *a.* 0-equivalence classes: $\{s_1, s_3\}, \{s_0, s_2\}$

   1-equivalence classes: $\{s_1, s_3\}, \{s_0, s_2\}$

   b. transition diagram for $\bar{A}$:
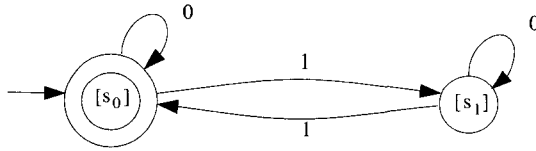
5. *a.* 0-equivalence classes: $\{s_0, s_1, s_3, s_4\}, \{s_2, s_5\}$

   1-equivalence classes: $\{s_0, s_3, s_4\}, \{s_1\}, \{s_2, s_5\}$

   2-equivalence classes: $\{s_0, s_3\}, \{s_4\}, \{s_1\}, \{s_2, s_5\}$

   3-equivalence classes: $\{s_0, s_3\}, \{s_4\}, \{s_1\}, \{s_2, s_5\}$

   b. transition diagram for $\bar{A}$:
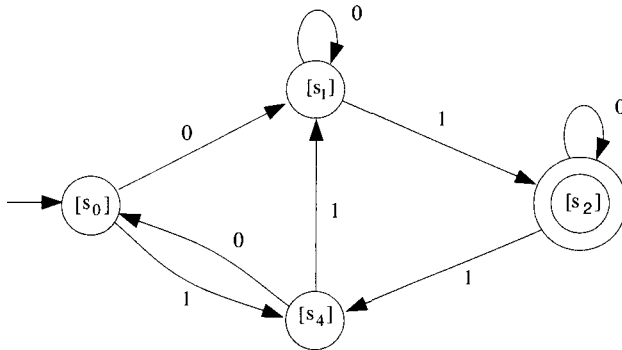
6. *a.* 0-equivalence classes: $\{s_0, s_1, s_3, s_4, s_5\}, \{s_2, s_6\}$

   1-equivalence classes: $\{s_0, s_4, s_5\}, \{s_1, s_3\}, \{s_2\}, \{s_6\}$

   2-equivalence classes: $\{s_0, s_4\}, \{s_5\}, \{s_1\}, \{s_3\}, \{s_2\}, \{s_6\}$

   3-equivalence classes: $\{s_0\}, \{s_4\}, \{s_5\}, \{s_1\}, \{s_3\}, \{s_2\}, \{s_6\}$

   b. The transition diagram for $\overline{A}$ is the same as the one given for A except that the states are denoted $[s_0], [s_1], [s_2], [s_3], [s_4], [s_5], [s_6]$.

8. For A:

   0-equivalence classes: $\{s_2, s_4\}, \{s_0, s_1, s_3\}$

   1-equivalence classes: $\{s_2, s_4\}, \{s_0, s_1\}, \{s_3\}$

   2-equivalence classes: $\{s_2, s_4\}, \{s_0, s_1\}, \{s_3\}$

   Therefore, the states of $\overline{A}$ are the 2-equivalence classes of A.

   For A':

   0-equivalence classes: $\{s_4'\}, \{s_0', s_1', s_2', s_3'\}$

   1-equivalence classes: $\{s_4'\}, \{s_1', s_3'\}, \{s_0', s_2'\}$

   2-equivalence classes: $\{s_4'\}, \{s_1', s_3'\}, \{s_0', s_2'\}$

   Therefore, the states of $\overline{A'}$ are the 2-equivalence classes of A'.

   According to the text, two automata are equivalent if, and only if, their quotient automata are isomorphic, provided inaccessible states have first been removed. Now A and A' have

no inaccessible states, and $\overline{A}$ has one accepting state and two nonaccepting states as does $\overline{A'}$. But the labels on the arrows connecting the states are different. For instance, in both quotient automata, there is one nonaccepting state which has an arrow going out from it to the accepting state and an arrow going back from the accepting state to it. But for $\overline{A}$, the label on the arrow going to the accepting state is labeled 0 whereas for $\overline{A'}$ it is labeled 1.
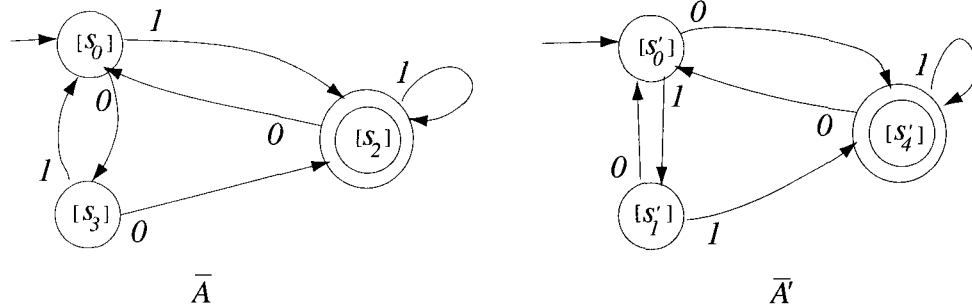
The nonequivalence of A and A' can also be seen by noting, for example, that the string 00 is accepted by A but not by A'.

10. For A:

0-equivalence classes: $\{s_0, s_1, s_2, s_3\}$, $\{s_4\}$

1-equivalence classes: $\{s_0, s_1, s_2\}$, $\{s_3\}$, $\{s_4\}$

2-equivalence classes: $\{s_0\}$, $\{s_1, s_2\}$, $\{s_3\}$, $\{s_4\}$

3-equivalence classes: $\{s_0\}$, $\{s_1, s_2\}$, $\{s_3\}$, $\{s_4\}$

Therefore, the states of $\overline{A}$ are the 3-equivalence classes of A.

For A':

0-equivalence classes: $\{s_0', s_1', s_3'\}$, $\{s_2', s_4'\}$

1-equivalence classes: $\{s_0'\}$, $\{s_1'\}$, $\{s_3'\}$, $\{s_2', s_4'\}$

2-equivalence classes: $\{s_0'\}$, $\{s_1'\}$, $\{s_3'\}$, $\{s_2'\}$, $\{s_4'\}$

Therefore, the states of $\overline{A}'$ are the 2-equivalence classes of A'.

According to the text, two automata are equivalent if, and only if, their quotient automata are isomorphic, provided inaccessible states have first been removed. Now A and A' have no inaccessible states, and $\overline{A}$ has four states whereas $\overline{A'}$ has five states. Therefore A and A' are not equivalent. This result can also be obtained by noting, for example, that the string 10 is accepted by A' but not by A.

11. *Proof*: Suppose A is a finite-state automaton with set of states S and relation R_* of $*$-equivalence of states. We will show that R_* is reflexive, symmetric, and transitive.

R_* *is reflexive*: Suppose that s is a state of A. It is certainly true that for all input strings w, $N^*(s, w)$ is an accepting state $\Leftrightarrow N^*(s, w)$ is an accepting state. So by definition of R_*, $s\ R_* s$.

R_* *is symmetric*: This is proved in Appendix B of the text.

R_* *is transitive*: Suppose that s, t, and u are states of A such that $s\ R_* t$ and $t\ R_* u$. By definition of R_*, for all input strings w, $N^*(s, w)$ is an accepting state $\Leftrightarrow N^*(t, w)$ is an accepting state and $N^*(t, w)$ is an accepting state $\Leftrightarrow N^*(u, w)$ is an accepting state. It follows by transitivity of the $\Leftrightarrow$ relation that $N^*(s, w)$ is an accepting state $\Leftrightarrow N^*(u, w)$ is an accepting state. Hence by definition of R_*, $s\ R_* u$.

Since R_* is reflexive, symmetric, and transitive, R_* is an equivalence relation.

14. *Proof*: Suppose k is an integer such that $k \geq 1$ and states s and t are k-equivalent. Then for all input strings w of length less than or equal to k, $N^*(s, w)$ is an accepting state $\Leftrightarrow N^*(t, w)$ is an accepting state. Since $k - 1 < k$, it follows that for all input strings w of length less than or equal to $k - 1$, $N^*(s, w)$ is an accepting state $\Leftrightarrow N^*(t, w)$ is an accepting state. Hence s and t are $(k - 1)$-equivalent.

15. *Proof*: Suppose k is an integer such that $k \geq 1$ and C_k is a k-equivalence class. We must show that there is a $k - 1$ equivalence class, C_{k-1}, such that $C_k \subseteq C_{k-1}$. By property (12.3.3), the $(k - 1)$-equivalence classes partition the set of all states of A in to a union of mutually disjoint subsets. Let s be any state in C_k. Then s is in *some* $(k - 1)$-equivalence class; call it C_{k-1}. Let t be any other state in C_k. *[We will show that $t \in C_{k-1}$ also.]* Then $t\ R_k\ s$, and so for all input strings of length k, $N^*(t, w)$ is an accepting state $\Leftrightarrow N^*(s, w)$ is an accepting state. Since $k - 1 < k$, it follows that for all input strings of length $k - 1$, $N^*(t, w)$ is an accepting state $\Leftrightarrow N^*(s, w)$ is an accepting state. Consequently, $t\ R_{k-1}\ s$, and so t and s are in the same $(k - 1)$-equivalence class. But $s \in C_{k-1}$. Hence $t \in C_{k-1}$ also. We, therefore, conclude that $C_k \subseteq C_{k-1}$.

16. *Proof*: Suppose s and t are states that are k-equivalent for all integers $k \geq 0$. Let w be any *[particular but arbitrarily chosen]* input string and let the length of w be l. Then $l \geq 0$ and so by hypothesis, s and t are R_l-equivalent. By definition of R_l, $N^*(s, w)$ is an accepting state $\Leftrightarrow N^*(t, w)$ is an accepting state. Since the choice of w was arbitrary, we conclude that for all input strings w, $N^*(s, w)$ is an accepting state $\Leftrightarrow N^*(t, w)$ is an accepting state. Thus by definition of $*$-equivalence, s and t are $*$-equivalent.

17. *Proof*: Suppose k is an integer such that states s and t are k-equivalent and suppose that m is a nonnegative integer less than k. Then for all input strings w of length less than or equal to k, $N^*(s, w)$ is an accepting state $\Leftrightarrow N^*(t, w)$ is an accepting state. Now since m is a nonnegative integer and $m < k$, then any string of length less than or equal to m has length less than or equal to k. Consequently, for all input strings w of length less than or equal to m, $N^*(s, w)$ is an accepting state $\Leftrightarrow N^*(t, w)$ is an accepting state. Hence s and t are m-equivalent.

18. *Proof*: Suppose A is an automaton and C is a $*$-equivalence class of states of A. By Theorem 12.3.2, for some integer $K \geq 0$, C is a K-equivalence class of A. Suppose C contains both an accepting state s and a nonaccepting state t of A. Since both s and t are in the same K-equivalence class, s is K-equivalent to t (by exercise 34 of Section 10.3), and so by exercise 17, s is 0-equivalent to t. But this is impossible because there are only two 0-equivalence classes, the set of all accepting states and the set of all nonaccepting states, and these two sets are disjoint. Hence the supposition that C contains both an accepting and a nonaccepting state is false: C consists entirely of accepting states or entirely of nonaccepting states.

19. *Proof*: Suppose A is an automaton and states s and t of A are $*$-equivalent. Let m be any input symbol and let w be any input string. By definition of the next-state and eventual-state functions, $N^*(N(s, m), w) = N^*(s, mw)$ and $N^*(N(t, m), w) = N^*(t, mw)$, where mw is the concatenation of m and w. But since s and t are $*$-equivalent, $N^*(s, mw)$ is an accepting state $\Leftrightarrow N^*(t, mw)$ is an accepting state. Hence $N^*(N(s, m), w)$ is an accepting state $\Leftrightarrow N^*(N(t, m), w)$ is an accepting state. So by definition of $*$-equivalence, $N(s, m)$ is $*$-equivalent to $N(t, m)$.

General Review Guide: Chapter 1

Compound Statements

- What is a statement? *(p. 2)*
- If p and q are statements, how do you symbolize "p but q" and "neither p nor q"? *(p. 3)*
- What does the notation $a \leq x < b$ mean? *(p. 4)*
- What is the conjunction of statements p and q? *(p. 5)*
- What is the disjunction of statements p and q? *(p. 6)*
- What are the truth table definitions for $\sim p$, $p \wedge q$, $p \vee q$, $p \to q$, and $p \leftrightarrow q$? *(pp. 5, 6, 18, 24)*
- How do you construct a truth table for a general compound statement? *(p. 7)*
- What is exclusive or? *(p. 7)*
- What is a tautology, and what is a contradiction? *(p. 13)*
- What is a conditional statement? *(p. 18)*
- Given a conditional statement, what is its hypothesis (antecedent)? conclusion (consequent)? *(p. 18)*
- What is a biconditional statement? *(p. 24)*
- What is the order of operations for the logical operators? *(p. 24)*

Logical Equivalence

- What does it mean for two statement forms to be logically equivalent? *(p. 8)*
- How do you test to see whether two statement forms are logically equivalent? *(p. 9)*
- How do you annotate a truth table to explain how it shows that two statement forms are or are not logically equivalent? *(p. 9)*
- What is the double negative property? *(p. 9)*
- What are De Morgan's laws? *(p. 10)*
- How is Theorem 1.1.1 used to show that two statement forms are logically equivalent? *(p. 14)*
- What are negations for the following forms of statements? *(pp. 10, 11, 20)*
    - $p \wedge q$
    - $p \vee q$
    - $p \to q$ (if p then q)

Converse, Inverse, Contrapositive

- What is the contrapositive of a statement of the form "If p then q"? *(p. 21)*
- What are the converse and inverse of a statement of the form "If p then q"? *(p. 22)*
- Can you express converses, inverses, and contrapositives of conditional statements in ordinary English? *(p. 21-22)*
- If a conditional statement is true, can its converse also be true? *(p. 22)*
- Given a conditional statement and its contrapositive, converse, and inverse, which of these are logically equivalent and which are not? *(p. 23)*

Necessary and Sufficient Conditions, Only If

- What does it mean to say that something is true only if something else is true? *(p. 23)*
- How are statements about only-if statements translated into if-then form.? *(p. 23)*
- What does it mean to say that something is a necessary condition for something else? *(p. 25)*
- What does it mean to say that something is a sufficient condition for something else? *(p. 25)*

- How are statements about necessary and sufficient conditions translated into if-then form.? *(pp. 25-26)*

Validity and Invalidity

- How do you identify the logical form of an argument? *(p. 2)*
- What does it mean for a form of argument to be valid? *(p. 29)*
- How do you test to see whether a given form of argument is valid? *(p. 30)*
- How do you annotate a truth table to explain how it shows that an argument is or is not valid? *(pp. 30-31)*
- What are modus ponens and modus tollens? *(pp. 31-32)*
- Can you give examples for and prove the validity of the following forms of argument? *(pp. 33-35)*

$$\begin{array}{lll} & p & \\ \therefore & p \vee q & \end{array} \quad \text{and} \quad \begin{array}{ll} & q \\ \therefore & p \vee q \end{array}$$

$$\begin{array}{lll} & p \wedge q & \\ \therefore & p & \end{array} \quad \text{and} \quad \begin{array}{ll} & p \wedge q \\ \therefore & q \end{array}$$

$$\begin{array}{lll} & p \vee q & \\ & \sim q & \\ \therefore & p & \end{array} \quad \text{and} \quad \begin{array}{ll} & p \vee q \\ & \sim p \\ \therefore & q \end{array}$$

$$\begin{array}{ll} & p \rightarrow q \\ & q \rightarrow r \\ \therefore & p \rightarrow r \end{array}$$

$$\begin{array}{ll} & p \vee q \\ & p \rightarrow r \\ & q \rightarrow r \\ \therefore & r \end{array}$$

- What are converse error and inverse error? *(p. 37)*
- Can a valid argument have a false conclusion? *(p. 38)*
- Can an invalid argument have a true conclusion? *(p. 38)*
- Which of modus ponens, modus tollens, converse error, and inverse error are valid and which are invalid? *(pp. 31, 32, 37, 38)*
- What is the contradiction rule? *(p. 39)*
- How do you use valid forms of argument to solve puzzles such as those of Raymond Smullyan about knights and knaves? *(p. 40)*

Digital Logic Circuits and Boolean Expressions

- Given a digital logic circuit, how do you
  - find the output for a given set of input signals *(p. 47)*
  - construct an input/output table *(p. 47)*
  - find the corresponding Boolean expression? *(p. 48)*
- What is a recognizer? *(p. 49)*
- Given a Boolean expression, how do you draw the corresponding digital logic circuit? *(p. 49)*
- Given an input/output table, how do you draw the corresponding digital logic circuit? *(p. 51)*
- What is disjunctive normal form? *(p. 52)*
- What does it mean for two circuits to be equivalent? *(p. 53)*
- What are NAND and NOR gates? *(p. 54)*
- What are Sheffer strokes and Peirce arrows? *(p. 54)*

Binary and Hexadecimal Notation

- How do you transform positive integers from decimal to binary notation and the reverse? *(p. 59)*
- How do you add and subtract integers using binary notation? *(p. 60)*
- What is a half-adder? *(p. 61)*
- What is a full-adder? *(p. 62)*
- What is the 8-bit two's complement of an integer in binary notation? *(p. 63)*
- How do you find the 8-bit two's complement of a positive integer *a* that is at most 255? *(p. 64)*
- How do you find the decimal representation of the integer with a given 8-bit two's complement? *(p. 65)*
- How are negative integers represented using two's complements? *(p. 66)*
- How is computer addition with negative integers performed? *(pp. 66-70)*
- How do you transform positive integers from hexadecimal to decimal notation? *(p. 71)*
- How do you transform positive integers from binary to hexadecimal notation and the reverse? *(p. 72)*

- What is octal notation? *(p. 74)*

Test Your Understanding: Chapter 1

Test yourself by filling in the blanks.

1. A statement is ____.

2. If p and q are statements, the statement "p but q" is symbolized ____.

3. If p and q are statements, the statement "neither p nor q" is symbolized ____.

4. An *and* statement is true if, and only if, both components are ____.

5. An *or* statement is false if, and only if, both components are ____.

6. An *if-then* statement is false if, and only if, its hypothesis is ____ and its conclusion is ____.

7. A statement of the form $p \leftrightarrow q$ is true if, and only if, ____.

8. If a logical expression includes the symbols $\sim$, $\wedge$ or $\vee$, and $\rightarrow$ or $\leftrightarrow$ and the expression does not include parentheses, then the first operation to be performed is ____, the second is ____, and the third is ____. To indicate the order of operations for an expression that includes both $\wedge$ and $\vee$ or both $\rightarrow$ and $\leftrightarrow$, it is frequently necessary to add ____.

9. A tautology is ____ for every substitution of statements for the statement variables.

10. A contradiction is ____ for every substitution of statements for the statement variables.

11. Two statement forms are logically equivalent if, and only if, their truth values are ____ for every substitution of statements for the statement variables.

12. *Less formal version*: Two statement forms are logically equivalent if, and only if, they always have ____.

13. Two statement forms are not logically equivalent if, and only if, ____.

14. De Morgan's laws say that ____ and ____.

15. The negation of $p \rightarrow q$ is ____.

16. The contrapositive of "if p then q" is ____.

17. The converse of "if p then q" is ____.

18. The inverse of "if p then q" is ____.

19. A conditional statement and its contrapositive are ____.

20. A conditional statement and its converse are not ____.

21. If r and s are statements, r only if s can be expressed in if-then form as ____ or as ____.

22. If t and u are statements, t is a sufficient condition for u can be expressed in if-then form as ____.

23. If v and w are statements, v is a necessary condition for w can be expressed in if-then form as ____ or as ____.

24. A form of argument is valid if, and only if, for every substitution of statements for the statement variables, if ____ of the premises are ____, then the conclusion is ____.

25. *Less formal version*: A form of argument is valid if, and only if, in all cases where the premises are ____, the conclusion is also ____.

26. A form of argument is invalid if, and only if, there is a substitution of statements for the statement variables that makes the premises ____ and the conclusion ____.

27. *Less formal version*: A form of argument is invalid if, and only if, it is possible for all the premises to be ____ and the conclusion ____.

28. Modus ponens is an argument of the form ____, and modus tollens is an argument of the form ____.

29. Converse error is an argument of the form ____, and inverse error is an argument of the form ____.

30. Insert the words "valid " or "invalid" as appropriate: modus ponens is ____; modus tollens is ____; converse error is ____; inverse error is ____.

31. The contradiction rule is an argument of the form ____.

32. The input/output table for a digital logic circuit is a table that shows ____.

33. The Boolean expression that corresponds to a digital logic circuit is ____.

34. A recognizer is a digital logic circuit that ____.

35. Two digital logic circuits are equivalent if, and only if, ____.

36. A NAND-gate is constructed by placing a ____ gate immediately following an ____ gate.

37. A NOR-gate is constructed by placing a ____ gate immediately following an ____ gate.

38. To represent a nonnegative integer in binary notation means to write it as a sum of products of the form ____, where ____.

39. To add integers in binary notation, you use the facts that $1_2 + 1_2 =$ ____ and $1_2 + 1_2 + 1_2 =$ ____.

40. To subtract integers in binary notation, you use the facts that $10_2 - 1_2 =$ ____ and $11_2 - 1_2 =$ ____.

41. A half-adder is a digital logic circuit that ____, and a full-adder is a digital logic circuit that ____.

42. The 8-bit two's complement of a positive integer a is ____.

43. To find the 8-bit two's complement of a positive integer a that is at most 255, you ____, ____, and ____.

44. If a is an integer with $-128 \leq a \leq 127$, the 8-bit representation of a is ____ if $a \geq 0$ and is ____ if $a < 0$.

45. To add two integers in the range -128 through 127 whose sum is also in the range -128 through 127, you ____, ____, ____, and ____.

46. To represent a nonnegative integer in hexadecimal notation means to write it as a sum of products of the form ____, where ____.

47. To convert a nonnegative integer from hexadecimal to binary notation, you ____ and ____.

Answers

1. a sentence that is true or false but not both
2. $p \land q$
3. $\sim p \land \sim q$
4. true
5. false
6. true, false
7. both p and q are true or both p and q are false
8. $\sim$; $\land$ or $\lor$; $\rightarrow$ or $\leftrightarrow$; parentheses
9. true
10. false
11. identical
12. the same truth values
13. there exist statements with the property that when the statements are substituted for the statement variables, one of the resulting statements is true and the other is false
14. $\sim (p \land q) \equiv \sim p \lor \sim q$; $\sim (p \lor q) \equiv \sim p \land \sim q$
15. $p \lor \sim q$
16. if $\sim q$ then $\sim p$
17. if q then p
18. if $\sim p$ then $\sim q$
19. logically equivalent
20. logically equivalent
21. if $\sim s$ then $\sim r$; if r then s
22. if t then u
23. if $\sim v$ then $\sim w$; if w then v
24. all; true; true
25. true; true
26. true; false
27. true; false

28.
$$\begin{array}{ll} p \to q & p \to q \\ p & \sim q \\ \therefore \; q & \therefore \; \sim p \end{array}$$

29.
$$\begin{array}{ll} p \to q & p \to q \\ q & \sim p \\ \therefore \; p & \therefore \; \sim q \end{array}$$

30. valid; valid; invalid; invalid

31.
$$p \to \mathbf{c}, \text{ where } \mathbf{c} \text{ is a contradiction}$$
$$\therefore \; \sim p$$

32. shows the output signal(s) that correspond to all possible combinations of input signals to the circuit

33. a logical expression that represents the input signals symbolically and indicates the successive actions of the logic gates on the input signals

34. outputs a 1 for exactly one particular combination of input signals and outputs 0's for all other combinations

35. they have the same input/output table

36. NOT; AND

37. NOT; OR

38. $d \cdot 2^n; d = 0$ or $d = 1$, and n is a nonnegative integer

39. $10_2; 11_2$

40. $1_2; 10_2$

41. outputs the sum of any two binary digits;
    outputs the sum of any three binary digits

42. $2^8 - a$

43. write the 8-bit binary representation of a;
    flip the bits
    add 1 in binary notation

44. the 8-bit binary representation of a
    the 8-bit binary representation of $2^8 - a$

45. convert both integers to their 8-bit binary representations
    add the results using binary notation
    truncate any leading 1
    convert back to decimal form

46. $d \cdot 16^n; d = 0, 1, 2, \ldots 9, A, B, C, D, E, F$, and n is a nonnegative integer

47. write each hexadecimal digit in fixed 4-bit binary notation
    juxtapose the results

General Review Guide: Chapter 2

Quantified Statements

- What is a predicate? *(p. 76)*
- What is the truth set of a predicate? *(p. 77)*
- What is a universal statement, and what is required for such a statement to be true? *(p. 78)*
- What is the method of exhaustion? *(p. 79)*
- What is required for a universal statement to be false? *(p. 78)*
- What is an existential statement, and what is required for such a statement to be true? *(p. 80)*
- What is required for a existential statement to be false? *(p. 80)*
- What are some ways to translate quantified statements from formal to informal language? *(p. 80)*
- What are some ways to translate quantified statements from informal to formal language? *(pp. 81-82)*
- What is a universal conditional statement? *(p. 81)*
- What is an equivalent way to write a universal conditional statement? *(pp. 83)*
- What are equivalent ways to write existential statements? *(p. 83)*
- What does it mean for a statement to be quantified implicitly? *(p. 83)*
- What do the notations $\Rightarrow$ and $\Leftrightarrow$ mean? *(p. 84)*
- What is the relation among $\forall$, $\exists$, $\wedge$, and $\vee$? *(p. 91)*
- What does it mean for a universal statement to be vacuously true? *(p. 92)*
- What is the rule for interpreting a statement that contains both a universal and an existential quantifier? *(p. 99)*
- How are statements expressed in the computer programming language Prolog? *(p. 107)*

Negations: What are negations for the following forms of statements?

- $\forall x, Q(x)$ *(p. 88)*
- $\exists x$ such that $Q(x)$ *(p. 89)*
- $\forall x,$ if $P(x)$ then $Q(x)$ *(p. 91)*
- $\forall x, \exists y$ such that $P(x,y)$ *(p. 103)*
- $\exists x$ such that $\forall y, P(x,y)$ *(p. 103)*

Variants of Conditional Statements

- What are the converse, inverse, and contrapositive of a statement of the form "$\forall x,$ if $P(x)$ then $Q(x)$"? *(p. 93)*
- How are quantified statements involving necessary and sufficient conditions and the phrase *only-if* translated into if-then form? *(p. 95)*

Validity and Invalidity

- What is universal instantiation? *(p. 111)*
- What are the universal versions of modus ponens, modus tollens, converse error, and inverse error, and which of these forms of argument are valid and which are invalid? *(pp. 112, 114, 118)*
- How is universal modus ponens used in a proof? *(p. 113)*

- How can diagrams be used to test the validity of an argument with quantified statements? *(p. 115)*

Test Your Understanding: Chapter 2

Test yourself by filling in the blanks.

1. A predicate is _____.

2. The truth set of a predicate $P(x)$ with domain D is _____.

3. A statement of the form "$\forall x \in D$, $Q(x)$" is true if, and only if, _____.

4. A statement of the form "$\exists x \in D$, $Q(x)$" is true if, and only if, _____.

5. A universal conditional statement is a statement of the form _____.

6. A negation of a universal statement is an _____ statement.

7. A negation of an existential statement is a _____ statement.

8. A statement of the form "All A are B" can be written with a quantifier and a variable as _____.

9. A statement of the form "Some A are B" can be written with a quantifier and a variable as .

10. A statement of the form "No A are B" can be written with a quantifier and a variable as .

11. A negation for a statement of the form "$\forall x \in D$, $Q(x)$" is _____.

12. A negation for a statement of the form "$\exists x \in D$ such that $Q(x)$" is _____.

13. A negation for a statement of the form "$\forall x \in D$, if $P(x)$ then $Q(x)$" is _____.

14. For a statement of the form "$\forall x \in D$, $Q(x)$" to be vacuously true means that _____.

15. Given a statement of the form "$\forall x$, if $P(x)$ then $Q(x)$," the contrapositive is _____, the converse is _____, and the inverse is _____.

16. If you want to establish the truth of a statement of the form "$\forall x \in D$, $\exists y \in E$ such that $P(x,y)$," your challenge is to allow someone else to pick _____, and then you must find _____ for which $P(x,y)$ _____.

17. If you want to establish the truth of a statement of the form "$\exists x \in D$ such that $\forall y \in E$, $P(x,y)$," your job is to find _____ with the property that no matter what _____, $P(x,y)$ will be _____.

18. A negation for a statement of the form "$\forall x \in D$, $\exists y \in E$ such that $P(x,y)$" is _____.

19. A negation for a statement of the form "$\exists x \in D$ such that $\forall y \in E$, $P(x,y)$" is _____.

20. The rule of universal instantiation says that _____.

21. Universal modus ponens is an argument of the form _____, and universal modus tollens is an argument of the form _____.

22. To use a diagram to represent a statement of the form "All A are B," you _____.

23. To use a diagram to represent a statement of the form "Some A are B," you _____.

24. To use a diagram to represent a statement of the form "No A are B," you _____.

Answers

1. a sentence that contains a finite number of variables and becomes a statement when specific values are substituted for the variables

2. the set of all x in D such that $P(x)$ is true

3. $Q(x)$ is true for each individual x in D

4. there is at least one x in D for which $Q(x)$ is true

5. $\forall x$, if $P(x)$ then $Q(x)$, where $P(x)$ and $Q(x)$ are predicates

6. existential

7. universal

8. $\forall x$, if x is an A then x is a B

9. $\exists x$ such that x is an A and x is a B

10. $\forall x$, if x is an A then x is not a B (Or: $\forall x$, if x is an B then x is not a A)

11. $\exists x \in D$ such that $\sim Q(x)$

12. $\forall x \in D, \sim Q(x)$

13. $\exists x \in D$ such that $P(x)$ and $\sim Q(x)$

14. there are no elements in D

15. $\forall x$, if $\sim Q(x)$ then $\sim P(x)$;
    $\forall x$, if $Q(x)$ then $P(x)$
    $\forall x$, if $\sim P(x)$ then $\sim Q(x)$

16. whatever element x in D they wish; an element y in E; is true

17. an element x in D; element y in E anyone might choose; true

18. $\exists x \in D$ such that $\forall y \in E, \sim P(x,y)$

19. $\forall x \in D, \exists y \in E$ such that $\sim P(x,y)$

20. if a property is true of everything in a domain, then it is true of any particular thing in the domain

21.
$\forall x$, if $P(x)$ then $Q(x)$	$\forall x$, if $P(x)$ then $Q(x)$
$P(a)$, for a particular a	$\sim Q(a)$, for a particular a
$\therefore \quad Q(a)$	$\therefore \quad \sim P(a)$

22. place a disk labeled A inside a disk labeled B

23. draw overlapping disks labeled A and B, respectively, and place a dot inside the part that overlaps

24. draw non-overlapping disks labeled A and B

General Review Guide: Chapter 3

Definitions

- Why is the phrase "if, and only if" used in a definition? *(p. 127)*
- How are the following terms defined?
    - even integer *(p. 127)*
    - odd integer *(p. 127)*
    - prime number *(p. 128)*
    - composite number *(p. 128)*
    - rational number *(p. 141)*
    - divisibility of one integer by another *(p. 148)*
    - the floor of a real number *(p. 165)*
    - the ceiling of a real number *(p. 165)*
    - greatest common divisor of two integers *(p. 192)*

Proving an Existential Statement/Disproving a Universal Statement

- How do you determine the truth of an existential statement? *(p. 128)*
- What does it mean to "disprove" a statement? *(p. 129)*
- What is disproof by counterexample? *(p. 129)*
- How do you establish the falsity of a universal statement? *(p. 129)*

Proving a Universal Statement/Disproving an Existential Statement

- If a universal statement is defined over a small, finite domain, how do you use the method of exhaustion to prove that it is true? *(p. 130)*
- What is the method of generalizing from the generic particular? *(p. 130)*
- If you use the method of direct proof to prove a statement of the form "$\forall x$, if $P(x)$ then $Q(x)$", what do you suppose and what do you have to show? *(p. 131)*
- What are the guidelines for writing proofs of universal statements? *(p. 134)*
- What are some common mistakes people make when writing mathematical proofs? *(p. 135)*
- How do you disprove an existential statement? *(p. 138)*
- What is the method of proof by division into cases? *(p. 138)*
- If you use the method of proof by contradiction to prove a statement, what do you suppose and what do you have to show? *(p. 171)*
- If you use the method of proof by contraposition to prove a statement of the form "$\forall x$, if $P(x)$ then $Q(x)$", what do you suppose and what do you have to show? *(p. 175)*
- Are you able to use the various methods of proof and disproof to establish the truth or falsity of statements about odd and even integers *(p. 133)*, prime numbers *(p. 138)*, rational numbers *(pp. 143, 145, 146)*, divisibility of integers *(pp. 151-152)*, and the floor and ceiling of a real number *(pp. 166-168)*?

Some Important Theorems and Algorithms

- What is the theorem about divisibility by a prime number? *(p. 151)*
- What is the unique factorization theorem for the integers? (This theorem is also called the fundamental theorem of arithmetic.) *(p. 153)*
- What is the quotient-remainder theorem? Can you apply it to specific situations? *(p. 157)*
- What is the theorem about the irrationality of the square root of 2? Can you prove this theorem? *(p. 181)*

- What is the theorem about the infinitude of the prime numbers? Can you prove this theorem? *(p. 183)*
- What is the division algorithm ? *(p. 191)*
- What is the Euclidean algorithm? *(p. 192)*
- How do you use the Euclidean algorithm to compute the greatest common divisor of two positive integers? *(p. 195)*

Notation for Algorithms

- How is an assignment statement executed? *(p. 186)*
- How is an **if-then** statement executed? *(p. 187)*
- How is an **if-then-else** statement executed? *(p. 187)*
- How are the statements **do** and **end do** used in an algorithm? *(p. 187)*
- How is a **while** loop executed? *(p. 188)*
- How is a **for-next** loop executed? *(p. 189)*
- How do you construct a trace table for a segment of an algorithm? *(pp. 188-89, 191)*

Test Your Understanding: Chapter 3

Test yourself by filling in the blanks.

1. An integer is even if, and only if, it ____.

2. An integer is odd if, and only if, it ____.

3. An integer is prime if, and only if, ____.

4. An integer is composite if, and only if, ____.

5. If $n = 2k + 1$ for some integer k, then ____.

6. Given integers a and b, if there exists an integer k such that $b = ak$, then ____.

7. To find a counterexample for a statement of the form "$\forall x \in D$, if $P(x)$ then $Q(x)$" you find ____.

8. According to the method of generalizing from the generic particular, to prove that every element of a domain satisfies a certain property, you suppose that ____ and you show that ____.

9. According to the method of direct proof, to prove that a statement of the form "$\forall x$ in D, if $P(x)$ then $Q(x)$" is true, you suppose that ____ and you show that ____.

10. Proofs should always be written in ____ sentences, and each assertion made in a proof should be accompanied by a ____.

11. The fact that a universal statement is true in some instances does not imply that it is ____.

12. When writing a proof, it is a mistake to use the same letter to represent ____.

13. A real number is rational if, and only if, ____.

14. An integer a divides an integer b if, and only if, ____.

15. If a and b are integers, the notation $a \mid b$ stands for _____, and the notation a/b stands for _____.

16. According to the theorem about divisibility by a prime number, given any integer $n > 1$, there is a _____.

17. The unique factorization theorem (fundamental theorem of arithmetic) says that given any integer $n > 1$, n can be written as a _____ in a way that is unique, except possibly for the _____ in which the numbers are written.

18. The quotient-remainder theorem says that given any integer n and any positive integer d, there exist unique integers q and r such that _____.

19. If n is a nonnegative integer and d is a positive integer, then $n \ div \ d =$ _____ and $n \ mod \ d =$ _____ where _____.

20. The parity property says that any integer is either _____.

21. Suppose that at some point in a proof you know that one of the statements A_1 or A_2 or A_3 is true and you want to show that regardless of which statement happens to be true a certain conclusion C will follow. Then you need to show that _____ and _____ and _____.

22. Given any real number x, the floor of x is the unique integer n such that _____.

23. Given any real number x, the ceiling of x is the unique integer n such that _____.

24. To prove a statement by contradiction, you suppose that _____ and you show that _____.

25. To prove a statement of the form "$\forall x \in D$, if $P(x)$ then $Q(x)$" by contraposition, you suppose that _____ and you show that _____.

26. One way to prove that $\sqrt{2}$ is an irrational number is to assume that $\sqrt{2} = a/b$ for some integers a and b with no common factors greater than 1, use the lemma that says that if the square of an integer is even then _____, and eventually show that a and b _____.

27. One way to prove that there are infinitely many prime numbers is to assume that there are only finitely many prime numbers $p_1, p_2, \ldots, p_n$, construct the number _____, and then show that this number has to be divisible by a prime number that is greater than _____.

28. When an algorithm statement of the form $x := e$ is executed, _____.

29. Consider an algorithm statement of the following form.

> **if** (*condition*)
>   **then** s_1
>   **else** s_2

When such a statement is executed, the truth or falsity of the *condition* is evaluated. If *condition* is true, _____. If *condition* is false, _____.

30. Consider an algorithm statement of the following form.

> **while** (*condition*)
>   [*statements that make up the body of the loop*]
> **end while**

When such a statement is executed, the truth or falsity of the *condition* is evaluated. If *condition* is true, _____. If *condition* is false, _____.

31. Consider an algorithm statement of the following form.

> **for** *variable* := *initial expression* **to** *final expression*
>   *[statements that make up the body of the loop]*
> **next** *(same) variable*

When such a statement is executed, *variable* is set equal to the value of the *initial expression*, and a check is made to determine whether the value of *variable* is less than or equal to the value of *final expression*. If so,_____. If not,_____.

32. Given a nonnegative integer a and a positive integer d, the division algorithm computes _____.

33. Given integers a and b, not both zero, $\gcd(a, b)$ is the integer d that satisfies the following two conditions: _____ and _____.

34. If r is a positive integer, then $\gcd(r, 0) =$ _____.

35. If a and b are integers with $b \neq 0$ and if q and r are nonnegative integers such that $a = bq + r$, then $\gcd(a, b) =$ _____.

36. Given positive integers A and B with $A > B$, the Euclidean algorithm computes _____.

Answers

1. equals twice some integer

2. equals twice some integer plus 1

3. it is greater than 1, and if it is written as a product of positive integers, then one of the integers is 1

4. it is greater than 1, and it can be written as a product of positive integers neither of which is 1

5. n is an odd integer

6. a divides b (or $a \mid b$, or a is a factor of b; or a is a divisor of b; or b is divisible by a; or b is a multiple of a)

7. an element of D for which $P(x)$ is true and $Q(x)$ is false

8. you have a particular but arbitrarily chosen element of the domain
   that element satisfies the property

9. x is any *[particular but arbitrarily chosen]* element of D for which $P(x)$ is true
   $Q(x)$ is true

10. complete; reason that justifies the assertion

11. true in all instances

12. two different quantities

13. it can be written as a ratio of integers with a nonzero denominator

14. there is an integer, say k, such that $b = ak$

15. the sentence "a divides b"; the real number a divided by b (if $b \neq 0$)

16. prime number that divides n

17. product of prime numbers, order

18. $n = dq + r$ and $0 \leq r < d$

19. q; r; $n = dq + r$ and $0 \leq r < d$

20. even or odd

21. if A_1 is true then C is true; if A_2 is true then C is true; if A_3 is true then C is true

22. $n \leq x < n + 1$

23. $n - 1 < x \leq n$

24. the statement is false; this supposition leads to a contradiction

25. x is any *[particular but arbitrarily chosen]* element of D for which $Q(x)$ is false
$P(x)$ is false

26. the integer is even; have a common factor greater than 1

27. $p_1 \cdot p_2 \cdots p_n + 1$; all the numbers $p_1, p_2, \ldots, p_n$

28. the expression e is evaluated (using the current values of all the variables in the expression), and this value is placed in the memory location corresponding to x (replacing any previous contents of the location)

29. statement s_1 is executed; statement s_2 is executed

30. all statements in the body of the loop are executed in order and then execution moves back to the beginning of the loop and the process repeats;
execution passes to the next algorithm statement following the loop

31. the statements in the body of the loop are executed in order, *variable* is increased by 1, and execution returns to the top of the loop;
execution passes to the next algorithm statement following the loop

32. integers q and r with the property that $n = dq + r$ and $0 \le r < d$

33. d divides a and d divides b; if c is a common divisor of both a and b, then $c \le d$

34. r

35. $\gcd(b, r)$

36. the greatest common divisor of A and B

General Review Guide: Chapter 4

Sequences and Summations

- What is a method to help find an explicit formula for a sequence whose first few terms are given (provided a nice explicit formula exists!)? *(p. 201)*
- What is the summation notation for a sum that is given in expanded form? *(p. 202)*
- What is the expanded form for a sum that is given in summation notation? *(p. 203)*
- What is the product notation? *(p. 205)*
- What is factorial notation? *(p. 206)*
- What are some properties of summations and products? *(p. 207)*
- How do you transform a summation by making a change of variable? *(p. 209)*
- What is an algorithm for converting from base 10 to base 2? *(p. 211)*

Mathematical Induction

- What do you show in the basis step and what do you show in the inductive step when you use (ordinary) mathematical induction to prove that a property involving an integer n is true for all integers greater than or equal to some initial integer? *(p. 218)*
- What is the inductive hypothesis in a proof by (ordinary) mathematical induction? *(p. 218)*
- Are you able to use (ordinary) mathematical induction to construct proofs involving various kinds of statements such as formulas, divisibility properties, and inequalities? *(pp. 218, 220, 223, 229, 231, 232)*
- Are you able to apply the formula for the sum of the first n positive integers? *(p. 222)*
- Are you able to apply the formula for the sum of the successive powers of a number, starting with the zeroth power? *(p. 225)*

Strong Mathematical Induction and The Well-Ordering Principle

- What do you show in the basis step and what do you show in the inductive step when you use strong mathematical induction to prove that a property involving an integer n is true for all integers greater than or equal to some initial integer? *(p. 235)*
- What is the inductive hypothesis in a proof by strong mathematical induction? *(p. 235)*
- Are you able to use strong mathematical induction to construct proofs of various statements? *(pp. 236-240)*
- What is the well-ordering principle for the integers? *(p. 240)*
- Are you able to use the well-ordering principle for the integers to prove statements, such as the existence part of the quotient-remainder theorem? *(p. 241)*
- How are ordinary mathematical induction, strong mathematical induction, and the well-ordering principle related? *(p. 240)*

Algorithm Correctness

- What are the pre-condition and the post-condition for an algorithm? *(p. 245)*
- What does it mean for a loop to be correct with respect to its pre- and post-conditions? *(p. 246)*
- What is a loop invariant? *(p. 247)*
- How do you use the loop invariant theorem to prove that a loop is correct with respect to its pre- and post-conditions? *(pp. 248-253)*

Test Your Understanding: Chapter 4

Test yourself by filling in the blanks.

1. The expanded form of the summation $\displaystyle\sum_{k=1}^{n} a_k$ is _____.

2. When $n = 1$, the value of $1^2 + 2^2 + 3^2 + \cdots + n^2$ is _____.

3. The expanded form of the product $\displaystyle\prod_{i=0}^{m} c_i$ is _____.

4. The notation $n! =$ _____.

5. When $\displaystyle c\sum_{k=1}^{n} a_k + \sum_{k=1}^{n} b_k$ is written as a single summation, the result is _____.

6. If you start with $\displaystyle\sum_{k=1}^{n} a_k$ and make the change of variable $j = k - 1$, the result is _____.

7. Repeated division by 2 is used to convert a positive integer to _____ notation.

8. To prove by (ordinary) mathematical induction that a property is true for all integers $n \geq a$, the first step is to show that _____ and the second step is to show that _____.

9. To prove by (ordinary) mathematical induction that $P(n)$ is true for all integers n greater than or equal to some integer a, the inductive hypothesis in the inductive step is _____.

10. To prove by strong mathematical induction that a property is true for all integers $n \geq a$, the first step is to show that _____ and the second step is to show that _____.

11. If the claim that $P(n)$ is true for all integers n greater than or equal to some integer a is proved by strong mathematical induction and if the basis step shows that $P(n)$ is true for all integers n with $a \leq n \leq b$, then the inductive hypothesis in the inductive step is _____.

12. The well-ordering principle for the integers says that _____.

13. A pre-condition for an algorithm is _____ and a post-condition for an algorithm is _____.

14. A loop is defined as correct with respect to its pre- and post-conditions if, and only if, whenever the algorithm variables satisfy the pre-condition for the loop and the loop terminates after a finite number of steps, then _____.

15. For each iteration of a loop, if a loop invariant is true before iteration of the loop, then _____.

16. Given a **while** loop with guard G and a predicate $I(n)$ if the following four properties are true, then the loop is correct with respect to its pre- and post-conditions:
    (1) The pre-condition for the loop implies that _____ is true before the first iteration of the loop;
    (2) For all integers $k \geq 0$, if the guard G and the predicate $I(k)$ are both true before an iteration of the loop, then _____;
    (3) After a finite number of iterations of the loop, _____;
    (4) If N is the least number of iterations after which G is false and $I(N)$ is true, then the values of the algorithm variables will be as specified _____.

Answers

1. $a_1 + a_2 + \cdots + a_n$

2. 1

3. $c_1 c_2 \cdots c_m$

4. $n(n-1)(n-2) \cdots 3 \cdot 2 \cdot 1$

5. $\displaystyle\sum_{k=1}^{n}(ca_k + b_k)$

6. $\displaystyle\sum_{j=0}^{n-1} a_{j+1}$

7. binary

8. the property is true for $n = a$
   for all integers $k \geq a$, if the property is true for $n = k$ then it is true for $n = k + 1$

9. the supposition that for any *[particular but arbitrarily chosen]* integer k with $k \geq a$, $P(k)$ is true

10. the property is true for an initial integer or set of initial integers
    for any integer k that is greater than the largest of the initial integers, if the property is true for all integers from the smallest of the initial integers through $k - 1$, then it is true for k

11. the supposition that for any *[particular but arbitrarily chosen]* integer with $k \geq b$, $P(i)$ is true for all integers i with $a \leq i < k$

12. any set of integers, all of which are greater than or equal to some fixed integer, has a least element

13. a predicate that describes the initial state of the input variables for the algorithm;
    a predicate that describes the final state of the output variables for the algorithm

14. the algorithm variables satisfy the post-condition for the loop

15. it is true after iteration of the loop

16. $I(0)$ is true
    $I(k + 1)$ is true after the iteration of the loop
    the guard G becomes false
    in the post-condition of the loop

General Review Guide: Chapter 5

Definitions: Can you define the following terms, use them correctly in sentences, and work with concrete examples involving them?

- subset *(p. 256)*
- proper subset *(p. 257)*
- equality of sets *(p. 258)*
- union, intersection, and difference of sets *(p. 260)*
- complement of a set *(p. 260)*
- empty set *(p. 262)*
- disjoint sets *(p. 262)*
- mutually disjoint sets *(p. 262)*
- partition of a set *(p. 263)*
- power set of a set *(p. 264)*
- Cartesian product of sets *(p. 265)*

Set Theory

- What is the difference between $\in$ and $\subseteq$? *(p. 258)*
- How do you use an element argument to prove that one set is a subset of another set? *(p. 269)*
- How are the procedural versions of set definitions used to prove properties of sets? *(p. 270)*
- What is the basic (two-step) method for showing that two sets are equal? *(p. 273)*
- Are you familiar with the set properties in Theorems 5.2.1 and 5.2.2? *(pp. 269, 272)*
- Why is the empty set a subset of every set? *(p. 278)*
- What is the special method used to show that a set equals the empty set? *(p. 279)*
- How do you find a counterexample for a proposed set identity? *(p. 283)*
- How do you find the number of subsets of a set with a finite number of elements? *(p. 285)*
- What is an "algebraic method" for proving that one set equals another set? *(p. 286)*
- What is a Boolean algebra? *(p. 288)*
- How do you deduce additional properties of a Boolean algebra from the properties that define it? *(p. 289)*
- What is Russell's paradox? *(p. 293)*
- What is the Halting Problem? *(p. 295)*

Test Your Understanding: Chapter 5

Test yourself by filling in the blanks.

1. The notation $x \in A$ is read ____.

2. The notation $A \subseteq B$ is read ____ and means that ____.

3. A set A equals a set B if, and only if, A and B have ____.

4. An element x is in $A \cup B$ if, and only if, ____.

5. An element x is in $A \cap B$ if, and only if, ____.

6. An element x is in $A - B$ if, and only if, ____.

7. An element x is in A^c if, and only if, _____.

8. The empty set is a set with _____.

9. The power set of a set A is _____.

10. Sets A and B are disjoint if, and only if, _____.

11. A collection of nonempty sets $A_1, A_2, \ldots, A_n$ is a partition of a set A if, and only if, _____.

12. Given sets A and B, the Cartesian product of A and B, $A \times B$, is _____.

13. Given sets $A_1, A_2, \ldots, A_n$, the Cartesian product $A_1 \times A_2 \times \cdots \times A_n$ is _____.

14. To use an element argument for proving that a set X is a subset of a set Y, you suppose that _____ and show that _____.

15. To use the basic method for proving that two sets X and Y are equal, you prove that _____ and that _____.

16. To prove a proposed set identity involving set variables A, B, and C, you suppose that _____ and show that _____.

17. If $\emptyset$ is a set with no elements and A is any set, the relation of $\emptyset$ and A is that _____.

18. To use the element method for proving that a set X equals the empty set, you prove that X has _____. To do this, you suppose that _____ and you show that this supposition leads to _____.

19. To show that a set X is not a subset of a set Y, _____.

20. Given a proposed set identity involving set variables A, B, and C, the most common way to show that the proposed identity is false is to find _____.

21. When using the "algebraic" method for proving a set identity, it is important to _____.

22. The operations of $+$ and $\cdot$ in a Boolean algebra are generalizations of the operations of _____ and _____ in the set of all statements forms in a given finite number of variables and the operations of _____ and _____ in the set of all subsets of a given set.

23. Russell showed that the following proposed "set definition" could not actually define a set: _____.

24. Turing's solution to the halting problem showed that there is no computer algorithm that will accept any algorithm X and data set D as input and then will indicate whether or not _____.

Answers

1. x is an element of the set A
2. the set A is a subset of the set B;
   for all x, if $x \in A$ then $x \in B$ (in other words, every element of A is also an element of B)
3. exactly the same elements
4. x is in A or x is in B
5. x is in A and x is in B
6. x is in A and x is not in B
7. x is not in A
8. no elements
9. the set of all subsets of A

10. $A \cap B = \emptyset$ (in other words, A and B have no elements in common)

11. $A = A_1 \cup A_2 \cup \cdots \cup A_n$ and $A_i \cap A_j = \emptyset$ for all $i, j = 1, 2, \ldots, n$ (in other words, A is the union of all the sets $A_1, A_2, \ldots, A_n$ and no two of these sets have any elements in common)

12. the set of all ordered pairs (a, b), where a is in A and b is in B

13. the set of all ordered n-tuples $(a_1, a_2, \ldots, a_n)$, where a_i is in A_i for all $i = 1, 2, \ldots, n$

14. x is any *[particular but arbitrarily chosen]* element of X

    x is an element of Y

15. $X \subseteq Y$; $Y \subseteq X$

16. A, B, and C are any *[particular but arbitrarily chosen]* sets; the left-hand and right-hand sides of the equation are equal for those sets

17. $\emptyset \subseteq A$

18. no elements; there is at least one element in X; a contradiction

19. show that there is an element of X that is not an element of Y

20. concrete sets A, B, and C for which the left-hand and right-hand sides of the equation are not equal

21. use the set properties from Theorem 5.2.2 exactly as they are stated

22. $\vee$; $\wedge$; $\cup$; $\cap$

23. the set of all sets that are not elements of themselves

24. execution of the algorithm terminates in a finite number of steps

General Review Guide: Chapter 6

Probability

- What is the sample space of an experiment? *(p. 299)*
- What is an event in the sample space? *(p. 299)*
- What is the probability of an event when all the outcomes are equally likely? *(p. 299)*

Counting

- If m and n are integers with $m \leq n$, how many integers are there from m to n inclusive? *(p. 302)*
- How do you construct a possibility tree? *(p. 306)*
- What are the multiplication rule, the addition rule, and the difference rule? *(pp. 308, 321, 322)*
- When should you use the multiplication rule and when should you use the addition rule? *(p. 345)*
- What is the inclusion/exclusion formula? *(p. 327)*
- What is a permutation? an r-permutation? *(p. 313, 315)*
- What is $P(n,r)$? *(p. 315)*
- How does the multiplication rule give rise to $P(n,r)$? *(p. 315)*
- What is $\binom{n}{r}$? *(p. 334)*
- What is an r-combination? *(p. 334)*
- What formulas are used to compute $\binom{n}{r}$ by hand? *(p. 337)*
- What is an r-combination with repetition allowed (or a multiset of size r)? *(p. 349)*
- How many r-combinations with repetition allowed can be selected from a set of n elements? *(p. 351)*

Pascal's Formula and the Binomial Theorem

- What is Pascal's formula? Can you apply it in various situations? *(p. 358)*
- How is Pascal's formula proved? *(p. 360)*
- What is the binomial theorem? *(p. 364)*
- How is the binomial theorem proved? *(p. 364-367)*

Probability Axioms and Expected Value

- What is the range of values for the probability of an event? *(p. 370)*
- What is the probability of an entire sample space? *(p. 370)*
- What is the probability of the empty set? *(p. 370)*
- If A and B are disjoint events in a sample space S, what is $P(A \cup B)$? *(p. 370)*
- If A is an event in a sample space S, what is $P(A^c)$? *(p. 371)*
- If A and B are any events in a sample space S, what is $P(A \cup B)$? *(p. 371)*
- How do you compute the expected value of a random experiment or process, if the possible outcomes are all real numbers and you know the probability of each outcome? *(p. 373)*
- What is the conditional probability of one event given another event? *(p. 376)*
- What is Bayes' theorem? *(p. 379)*
- What does it mean for two events to be independent? *(p. 381)*

- What is the probability of an intersection of two independent events? *(p. 385)*
- What does it mean for events to be mutually independent? *(p. 384)*
- What is the probability of an intersection of mutually independent events? *(p. 385)*

Test Your Understanding: Chapter 6

Test yourself by filling in the blanks.

1. A sample space of a random process or experiment is _____.

2. An event in a sample space is _____.

3. To compute the probability of an event using the equally likely probability formula, you take the ratio of the _____ to the _____.

4. If $m \leq n$, the number of integers from m to n inclusive is _____.

5. The multiplication rule says that if an operation can be performed in k steps and, for each i with $1 \leq i \leq k$, the ith step can be performed in n_i ways (regardless of how previous steps were performed), then _____.

6. A permutation of a set of elements is _____.

7. The number of permutations of a set of n elements equals _____.

8. An r-permutation of a set of n elements is _____.

9. The number of r-permutations of a set of n elements is denoted _____.

10. One formula for the number of r-permutations of a set of n elements is _____ and another formula is _____.

11. The addition rule says that if a finite set A equals the union of k distinct mutually disjoint subsets $A_1, A_2, \ldots, A_k$, then _____.

12. The difference rule says that if A is a finite set and B is a subset of A, then _____.

13. If S is a finite sample space and A is an event in S, then the probability of A^c equals _____.

14. The inclusion/exclusion rule for two sets says that if A and B are any finite sets, then _____.

15. The inclusion/exclusion rule for three sets says that if A, B, and C are any finite sets, then _____.

16. The number of subsets of size r that can be formed from a set with n elements is denoted _____, which is read as _____.

17. Alternative phrases used to describe a subset of size r that is formed from a set with n elements are _____ and _____.

18. Two ordered selections are said to be the same if _____ and also if _____.

19. Two unordered selections are said to be the same if _____, regardless of _____.

20. The formula relating $\binom{n}{r}$ and $P(n, r)$ is _____.

21. Additional formulas for $\binom{n}{r}$ are _____ and _____.

22. The phrase "at least n" means _____, and the phrase "at most n" means _____.

23. Suppose a collection consists of n objects of which, for each i with $1 \leq i \leq k$, n_i are of type i and are indistinguishable from each other. Also suppose that $n = n_1 + n_2 + \cdots + n_k$. Then the number of distinct permutations of the n objects is _____.

24. Given a set $X = \{x_1, x_2, \ldots x_n\}$, an r-combination with repetition allowed, or a multiset of size r, chosen from X is _____, which is denoted _____.

25. If $X = \{x_1, x_2, \ldots x_n\}$, the number of r-combinations with repetition allowed (or multisets of size r) chosen from X is _____.

26. When choosing k elements from a set of n elements, order may or may not matter and repetition may or may not be allowed.

    - The number of ways to choose the k elements when repetition is allowed and order matters is _____.

    - The number of ways to choose the k elements when repetition is not allowed and order matters is _____.

    - The number of ways to choose the k elements when repetition is not allowed and order does not matter is _____.

    - The number of ways to choose the k elements when repetition is allowed and order does not matter is _____.

27. If n is a nonnegative integer, then $\dbinom{n}{n} = $ _____ and $\dbinom{n}{1} = $ _____.

28. If n and r are nonnegative integers with $r \leq n$, then the relation between $\dbinom{n}{r}$ and $\dbinom{n}{n-r}$ is _____.

29. Pascal's formula says that if n and r are positive integers with $r \leq n$, then _____.

30. The crux of the algebraic proof of Pascal's formula is that to add two fractions you need to express both of them with a _____.

31. The crux of the combinatorial proof of Pascal's formula is that the set of subsets of size r of a set $\{x_1, x_2, \ldots, x_n\}$ can be partitioned into the set of subsets of size r that contain _____ and those that _____.

32. The binomial theorem says that given any real numbers a and b and any nonnegative integer n, _____.

33. The crux of the algebraic proof of the binomial theorem is that, after making a change of variable so that two summations have the same lower and upper limits, you use the fact that $\dbinom{m}{k} + \dbinom{m}{k-1} = $ _____.

34. The crux of the combinatorial proof of the binomial theorem is that the number of ways to arrange k b's and $(n-k)$ a's in order is _____.

35. If A is an event in a sample space S, $P(A)$ can take values between _____ and _____. Moreover, $P(S) = $ _____, and $P(\emptyset) = $ _____.

36. If A and B are disjoint events in a sample space S, $P(A \cup B) = $ _____.

37. If A is an event in a sample space S, $P(A^c) = $ _____.

38. If A and B are any events in a sample space S, $P(A \cup B) =$ ____.

39. If the possible outcomes of a random process or experiment are real numbers $a_1, a_2, \ldots, a_n$, which occur with probabilities $p_1, p_2, \ldots, p_n$, then the expected value of the process is ____.

40. If A and B are any events in a sample space S and $P(A) \neq 0$, then the conditional probability of B given A is $P(B|A) =$ ____.

41. Bayes' theorem says that if a sample space S is a union of mutually disjoint events $B_1, B_2, \ldots, B_n$ with nonzero probabilities, if A is an event in S with $P(A) \neq 0$, and if k is an integer with $1 \leq k \leq n$, then ____.

42. Events A and B in a sample space S are independent if, and only if, ____.

43. Events A, B, and C in a sample space S are mutually independent if, and only if, ____, ____, ____, and ____.

Answers

1. the set of all outcomes of the random process or experiment

2. a subset of the sample space

3. number of outcomes in the event; total number of outcomes

4. $n - m + 1$

5. the operation as a whole can be performed in $n_1 n_2 \cdots n_k$ ways

6. an ordering of the elements of the set in a row

7. $n!$

8. an ordered selection of r of the elements of the set

9. $P(n, r)$

10. $n(n-1)(n-2) \cdots (n-r+1)$; $\dfrac{n!}{(n-r)!}$

11. the number of elements in A equals $N(A_1) + N(A_2) + \cdots + N(A_k)$

12. the number of elements in $A - B$ is the difference between the number of elements in A minus the number of elements in B

13. $1 - P(A)$

14. $N(A \cup B) = N(A) + N(B) - N(A \cap B)$

15. $N(A \cup B \cup C) = N(A) + N(B) + N(C) - N(A \cap B) - N(A \cap C) - N(B \cap C) + N(A \cap B \cap C)$

16. $\dbinom{n}{r}$; n choose r

17. an r-combination of the set of n elements; an unordered selection of r elements chosen from the set of n elements

18. the elements chosen are the same; the elements are chosen in the same order

19. the elements chosen are the same; the order in which the elements are chosen

20. $\dbinom{n}{r} = \dfrac{P(n,r)}{r!}$

21. $\dbinom{n}{r} = \dfrac{n(n-1)(n-2) \cdots (n-r+1)}{r!}$; $\dbinom{n}{r} = \dfrac{n!}{r!(n-r)!}$

22. n or more; n or fewer

23. $\dbinom{n}{n_1}\dbinom{n-n_1}{n_2}\dbinom{n-n_1-n_2}{n_3} \cdots \dbinom{n-n_1-n_2-\cdots-n_{k-1}}{n_k} = \dfrac{n!}{n_1! n_2! n_3! \cdots n_k!}$

24. an unordered selection of elements taken from X with repetition allowed $[x_1, x_2, \ldots x_{i_r}]$ where each x_{i_j} is in X and some of the x_{i_j} may equal each other

25. $\binom{k+n-1}{k}$

26. n^k; $n(n-1)(n-2)\cdots(n-k+1)$; $\binom{n}{k}$; $\binom{k+n-1}{k}$

27. 1; n

28. $\binom{n}{r} = \binom{n}{n-r}$

29. $\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$

30. common denominator

31. x_n; do not contain x_n

32. $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$

33. $\binom{m+1}{k}$

34. $\binom{n}{k}$

35. 0; 1; 1; 0

36. $P(A) + P(B)$

37. $1 - P(A)$

38. $P(A) + P(B) - P(A \cap B)$

39. $a_1 p_1 + a_2 p_2 + \cdots + a_n p_n$

40. $\dfrac{P(A \cap B)}{P(A)}$

41. $P(B_k | A) = \dfrac{P(A|B_k)P(B_k)}{P(A|B_1)P(B_1) + P(A|B_2)P(B_2) + \cdots + P(A|B_n)P(B_n)}$

42. $P(A \cap B) = P(A) \cdot P(B)$

43. $P(A \cap B) = P(A) \cdot P(B)$; $P(A \cap C) = P(A) \cdot P(C)$; $P(B \cap C) = P(B) \cdot P(C)$; $P(A \cap B \cap C) = P(A) \cdot P(B) \cdot P(C)$

General Review Guide: Chapter 7

Definitions: How are the following terms defined?

- function f from a set X to a set Y *(p. 390)*
- If f is a function from a set X to a set Y, what are

    – the domain, co-domain, and range of f *(p. 390)*

    – the image of X under f *(p. 390)*

    – the value of f at x, where x is in X *(p. 390)*

    – the image of x under f, where x is in X *(p. 390)*

    – the output of f for the input x, where x is in X *(p. 390)*

    – an inverse image of y, where y is in Y *(p. 390)*

- logarithm with base b of a positive number x *(p. 395)*
- one-to-one function *(p. 402)*
- onto function *(p. 407)*
- exponential function with base b *(p. 411)*
- one-to-one correspondence *(p. 413)*
- inverse function *(p. 415)*
- composition of functions *(p. 432)*
- cardinality *(p. 443)*
- countable set and uncountable set. *(p. 445)*

General Function Facts

- How do you draw an arrow diagram for a function defined on a finite set? *(p. 390)*
- Given a function defined by an arrow diagram or by a formula, how do you find values of the function, the range of the function, and the inverse image of an element in its co-domain? *(p. 391, pp. 394-8)*
- How do you show that two functions are equal? *(p. 393)*
- If the claim is made that a given formula defines a function from a set X to a set Y, how do you determine that the "function" is not well-defined? *(p. 398)*

One-to-one and Onto

- How do you show that a function is not one-to-one? *(p. 403, 404)*
- How do you show that a function defined on an infinite set is one-to-one? *(p. 404)*
- How do you show that a function is not onto? *(p. 407, 409)*
- How do you show that a function defined on an infinite set is onto? *(p. 409)*
- How do you determine if a given function has an inverse function? *(p. 415)*
- How do you find an inverse function if it exists? *(p. 415-6)*

Exponents and Logarithms

- What are the four laws of exponents? *(p. 411)*
- What are the corresponding properties of logarithms? *(p. 412 and 419-exercises 29-31)*

- How are the logarithmic function with base b and the exponential function with base b related? *(p. 415)*

Composition of Functions

- How do you compute the composition of two functions? *(p. 432)*
- What kind of function do you obtain when you compose two one-to-one functions? *(p. 437)*
- What kind of function do you obtain when you compose two onto functions? *(p. 438)*
- What kind of function do you obtain when you compose a one-to-one function with a function that is not one-to-one? *(p. 442-exercise 18)*
- What kind of function do you obtain when you compose an onto function with a function that is not onto? *(p. 442-exercise 19)*
- What is the composition of a function with its inverse? *(p. 436)*

Applications of Functions

- What is the pigeonhole principle? *(p. 420)*
- What is the generalized pigeonhole principle? *(p. 425)*
- How do you show that one set has the same cardinality as another? *(p. 443)*
- How do you show that a given set is countably infinite? countable? *(p. 446)*
- How do you show that the set of all positive rational numbers is countable? *(p. 448)*
- How is the Cantor diagonalization process used to show that the set of real numbers between 0 and 1 is uncountable? *(p. 450)*

Test Your Understanding: Chapter 7

Test yourself by filling in the blanks.

1. A function f from a set X to a set Y is a relation between elements of X (called inputs) and elements of Y (called outputs) such that _____ input element of X is related to _____ output element of Y.

2. Given a function f from a set X to a set Y, $f(x)$ is _____.

3. Given a function f from a set X to a set Y, if $f(x) = y$, then y is called _____ or _____ or _____ or _____.

4. Given a function f from a set X to a set Y, the range of f (or the image of X under f) is _____.

5. Given a function f from a set X to a set Y, if $f(x) = y$, then x is called _____ or _____.

6. Given a function f from a set X to a set Y, if $y \in Y$, then $f^{-1}(y) =$ _____ and is called _____.

7. Given functions f and g from a set X to a set Y, $f = g$ if, and only if, _____.

8. Given positive real numbers x and b with $b \neq 1$, $\log_b x =$ _____.

9. If F is a function from a set X to a set Y, then F is one-to-one if, and only if, _____.

10. If F is a function from a set X to a set Y, then F is not one-to-one if, and only if, _____.

11. If F is a function from a set X to a set Y, then F is onto if, and only if, _____.

12. If F is a function from a set X to a set Y, then F is not onto if, and only if, ____.

13. The following two statements are ____:

    $\forall \ u,v \in U$, if $H(u) = H(v)$ then $u = v$.

    $\forall \ u,v \in U$, if $u \neq v$ then $H(u) \neq H(v)$.

14. Given a function $F: X \to Y$ (where X is an infinite set or a large finite set), to prove that F is one-to-one, you suppose that ____ and then you show that ____.

15. Given a function $F: X \to Y)$ (where X is an infinite set or a large finite set), to prove that F is onto, you suppose that ____ and then you show that ____.

16. Given a function $F: X \to Y$, to prove that F is not one-to-one, you ____.

17. Given a function $F: X \to Y$, to prove that F is not onto, you ____.

18. A one-to-one correspondence from a set X to a set Y is a ____ that is ____.

19. If F is a one-to-one correspondence from a set X to a set Y and y is in Y, then $F^{-1}(y)$ is ____.

20. The pigeonhole principle states that ____.

21. The generalized pigeonhole principle states that ____.

22. If X and Y are finite sets and f is a function from X to Y then f is one-to-one if, and only if, ____.

23. If f is a function from X to Y and g is a function from Y to Z, then $g \circ f$ is a function from ____ to ____, and $(g \circ f)(x)$ ____ for all x in X.

24. If f is a function from X to Y and i_X and i_Y are the identity functions from X to X and Y to Y, respectively, then $f \circ i_X = $ ____ and $i_Y \circ f = $ ____.

25. If f is a one-to-one correspondence from X to Y, then $f^{-1} \circ f = $ ____ and $f \circ f^{-1} = $ ____.

26. If f is a one-to-one function from X to Y and g is a one-to-one function from Y to Z, you prove that $g \circ f$ is one-to-one by supposing that ____ and then showing that ____.

27. If f is an onto function from X to Y and g is an onto function from Y to Z, you prove that $g \circ f$ is onto by supposing that ____ and then showing that ____.

28. A set is finite if, and only if, ____.

29. To prove that a set A has the same cardinality as a set B you must ____.

30. Given a set A, the reflexive property of cardinality says that ____.

31. Given sets A and B, the symmetric property of cardinality says that ____.

32. Given sets A, B, and C, the transitive property of cardinality says that ____.

33. A set is called countably infinite if, and only if, ____.

34. A set is called countable if, and only if, ____.

35. In each of the following, fill in the blank with the word countable or the word uncountable.

    (a) The set of all integers is ____.
    (b) The set of all rational numbers is ____.

(c) The set of all real numbers between 0 and 1 is _____.

(d) The set of all real numbers is _____.

(e) The set of all computer programs in a given computer language is _____.

(f) The set of all functions from the set of all positive integers, $\mathbf{Z}^+$, to $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ is _____.

36. The Cantor diagonalization process is used to prove that _____.

Answers

1. each, one and only one
2. the unique output element y in Y that is related to x by f
3. the value of f at x; the image of x under f; the output of f for the input x
4. the set of all y in Y such that $f(x) = y$
5. an inverse image of y under f; a preimage of y
6. $\{x \in X \mid f(x) = y\}$; the inverse image of y
7. $f(x) = g(x)$ for all $x \in X$
8. the exponent to which b must be raised to obtain x
   Or: $\log_b y = x \Leftrightarrow b^y = x$
9. for all x_1 and x_2 in X, if $F(x_1) = F(x_2)$ then $x_1 = x_2$
10. there exist elements x_1 and x_2 in X such that $F(x_1) = F(x_2)$ and $x_1 \neq x_2$
11. for all y in Y, there exists at least one element x in X such that $f(x) = y$
12. there exists an element y in Y such that for all elements x in X, $f(x) \neq y$
13. logically equivalent ways of expression what it means for H to be a one-to-one function (The second way is the contrapositive of the first.)
14. x_1 and x_2 are any *[particular but arbitrarily chosen]* elements in X with the property that $F(x_1) = F(x_2)$; $x_1 = x_2$
15. y is any *[particular but arbitrarily chosen]* element in Y; there exists at least one element x in X such that $F(x) = y$
16. show that there are concrete elements x_1 and x_2 in X with the property that $F(x_1) = F(x_2)$ and $x_1 \neq x_2$
17. show that there is a concrete element y in Y with the property that $F(x) \neq y$ for any element x in X
18. function from X to Y; one-to-one and onto
19. the unique element x in X such that $F(x) = y$ (in other words, $F^{-1}(y)$ is the unique preimage of y in X)
20. if n pigeons fly into m pigeonholes and $n > m$, then at least two pigeons fly into the same pigeonhole
    Or: given any function from a finite set to a smaller finite set, there must be at least two elements in the function's domain that have the same image in the function's co-domain
    Or: a function from one finite set to a smaller finite set cannot be one-to-one
21. if n pigeons fly into m pigeonholes and, for some positive integer k, $n > mk$, the at least one pigeonhole contains $k + 1$ or more pigeons
    Or: for any function f from a finite set X to a finite set Y and for any positive integer k, if $N(X) > k \cdot N(Y)$, then there is some $y \in Y$ such that y is the image of at least $k + 1$ distinct elements of Y
22. f is onto
23. X; Z; $g(f(x))$
24. f; f

25. i_X; i_Y

26. x_1 and x_2 are any *[particular but arbitrarily chosen]* elements in X with the property that $(g \circ f)(x_1) = (g \circ f)(x_2)$; $x_1 = x_2$

27. z is any *[particular but arbitrarily chosen]* element in Z; there exists at least one element x in X such that $(g \circ f)(x) = z$

28. it is the empty set or there is a one-to-one correspondence from $\{1, 2, \ldots, n\}$ to it, where n is a positive integer

29. show that there exists a function from A to B that is one-to-one and onto;
    Or: show that there exists a one-to-one correspondence from A to B

30. A has the same cardinality as A

31. if A has the same cardinality as B, then B has the same cardinality as A

32. if A has the same cardinality as B and B has the same cardinality as C, then A has the same cardinality as C

33. it has the same cardinality as the set of all positive integers

34. it is finite or countably infinite

35. countable; countable; uncountable; uncountable; countable; uncountable

36. the set of all real numbers between 0 and 1 is uncountable

General Review Guide: Chapter 8

Recursion

- What is an explicit formula for a sequence? *(p. 457)*
- What does it mean to define a sequence recursively? *(p. 457-8)*
- What is a recurrence relation with initial conditions? *(p. 458)*
- How do you compute terms of a recursively defined sequence? *(p. 458)*
- Can different sequences satisfy the same recurrence relation? *(p. 459)*
- What is the "recursive paradigm"? *(p. 460)*
- How do you develop recurrence relations for sequences that are variations of the towers of Hanoi sequence? *(p. 460)*
- How do you develop recurrence relations for sequences that are variations of the Fibonacci sequence? *(p. 464)*
- How do you develop recurrence relations for sequences that involve compound interest? *(p. 466-7)*
- How do you develop recurrence relations for sequences that involve the number of bit strings with a certain property? *(p. 467)*
- How do you find a recurrence relation for the number of ways a set of size n can be partitioned into r subsets? *(p. 469)*

Solving Recurrence Relations

- What is the method of iteration for solving a recurrence relation? *(p. 475)*
- How do you use the formula for the sum of the first n integers and the formula for the sum of the first n powers of a real number r to simplify the answers you obtain when you solve recurrence relations? *(p. 480)*
- How is mathematical induction used to check that the solution to a recurrence relation is correct? *(p. 483)*
- What is a second-order linear homogeneous recurrence relation with constant coefficients? *(p. 487)*
- What is the characteristic equation for a second-order linear homogeneous recurrence relation with constant coefficients? *(p. 489)*
- What is the distinct-roots theorem? If the characteristic equation of a relation has two distinct roots, how do you solve the relation? *(p. 491)*
- What is the single-root theorem? If the characteristic equation of a relation has a single root, how do you solve the relation? *(p. 497)*

General Recursive Definitions

- When a set is defined recursively, what are the three parts of the definition? *(p. 500)*
- Given a recursive definition for a set, how can you tell that a given element is in the set? *(p. 500-1)*
- What is structural induction? *(p. 502)*
- Given a recursive definition for a set, is there a way to tell that a given element is not in the set? *(p. 508, exercises 4, 6a, 8-14)*
- What are the recursive definitions for sum, product, union, and intersection? *(p. 503-5)*
- What is a recursive function? *(p. 505)*

Test Your Understanding: Chapter 8

Test yourself by filling in the blanks

1. The reason we can't always specify a sequence by giving its initial terms is that _____.

2. For a sequence $a_0, a_1, a_2, \ldots$ to be defined by an explicit formula means that _____.

3. A recurrence relation for a sequence $a_0, a_1, a_2, \ldots$ is _____. The initial conditions for such a recurrence relation specify _____.

4. To solve the Tower of Hanoi puzzle, we imagine the first step as consisting of all the moves needed to _____, the second step as moving _____, and the third step as _____.

5. The crucial observation used to solve the Fibonacci numbers problem is that the number of rabbits born at the end of month k is the same as _____. Also because no rabbits die, all the rabbits that are alive at the end of month $k - 1$ are still alive at _____. So the total number of rabbits alive at the end of month k equals _____.

6. When interest is compounded periodically, the amount in the account at the end of period k equals _____ plus _____.

7. A bit string of length k that does not contain the pattern 11 either starts with a _____, which is followed by a _____, or it starts with _____, which is followed by a _____.

8. The Stirling number of the second kind, $S_{n,r}$, can be interpreted as _____.

9. Because any partition of a set $X = \{x_1, x_2, \ldots, x_n\}$ either contains x_n or does not, the number of partitions of X into r subsets equals _____ plus _____.

10. To find an explicit formula for a recurrence relation by the method of iteration, you start by writing down _____ and then you use the recurrence relation to _____.

11. A sequence $a_1, a_2, a_3, \ldots$ is called an arithmetic sequence if, and only if, there is a constant d such that _____, or, equivalently, _____.

12. A sequence $a_1, a_2, a_3, \ldots$ is called an geometric sequence if, and only if, there is a constant r such that _____ or, equivalently, _____.

13. Two useful formulas for simplifying explicit formulas for recurrence relations that have been obtained by iteration are _____ and _____.

14. When an explicit formula for a recurrence relation has been obtained by iteration, the correctness of the formula can be checked by _____.

15. A second-order linear homogeneous recurrence relation with constant coefficients is a recurrence relation of the form _____ for all integers $k \geq$ _____, where _____.

16. Given a recurrence relation of the form $a_k = Aa_{k-1} + Ba_{k-2}$ for all integers $k \geq 2$, the characteristic equation of the relation is _____.

17. If a sequence $a_1, a_2, a_3, \ldots$ is defined by a second-order linear homogeneous recurrence relation with constant coefficients and the characteristic equation for the relation has two distinct roots r and s (which could be complex numbers), then the sequence satisfies an explicit formula of the form _____.

18. If a sequence $a_1, a_2, a_3, \ldots$ is defined by a second-order linear homogeneous recurrence relation with constant coefficients and the characteristic equation for the relation has only a single root r, then the sequence satisfies an explicit formula of the form _____.

19. The BASE for a recursive definition of a set is _____.

20. The RECURSION for a recursive definition of a set is _____.

21. The RESTRICTION for a recursive definition of a set is _____.

22. One way to show that a given element is in a recursively defined set is to start with an element or elements in the _____ and apply the rules from the _____ until you obtain the given element.

23. Another way to show that a given element is in a recursively defined set is to use _____ to characterize all the elements of the set and then observe that the given element satisfies the characterization.

24. To prove that every element in a recursively defined set S satisfies a certain property, you show that _____ and that, for each rule in the RECURSION, if_____ then_____.

25. A function is said to be defined recursively if, and only if, _____.

Answers

1. two sequences may have the same initial terms and yet have different terms later on

2. a_n equals an algebraic expression in the variable n

3. a formula that relates each term a_k of the sequence to certain of its predecessors; enough initial values of the sequence to enable subsequent values to be computed using the recurrence relation

4. transfer the top $k-1$ disks from the initial pole to the pole that is not the ultimate target pole;
   the bottom disk from the initial pole to the target pole;
   consisting of all the moves needed to transfer the top $k-1$ disks from the pole that is not the ultimate target pole to the target pole

5. the number of rabbits alive at the end of month $k-2$;
   the end of month k;
   the sum of the number of rabbits alive at the end of month $k-1$ plus the number alive at the end of month $k-2$

6. the amount in the account at the end of period $k-1$;
   the interest earned during period k

7. 0; bit string of length $k-1$ that does not contain the pattern 11;
   01; bit string of length $k-2$ that does not contain the pattern 11

8. the number of ways a set of size n can be partitioned into r subsets

9. the number of partitions of X into r subsets of which $\{x_n\}$ is one; the number of partitions of X into r subsets, none of which is $\{x_n\}$

10. as many terms of the sequence as are specified in the initial conditions; compute subsequent terms of the sequence by successive substitution

11. $a_k = a_{k-1} + d$, for all integers $k \geq 1$;
    $a_n = a_0 + dn$, for all integers $n \geq 0$

12. $a_k = ra_{k-1}$, for all integers $k \geq 1$;
    $a_n = a_0 r^n$, for all integers $n \geq 0$

13. the formula for the sum of the terms of a geometric sequence;
    the formula for the sum of the first n positive integers

14. mathematical induction

15. $a_k = Aa_{k-1} + Ba_{k-2}$; 2; A and B are fixed real numbers with $B \neq 0$

16. $t^2 - At - B = 0$

17. $a_n = Cr^n + Ds^n$, where C and D are real or complex numbers

18. $a_n = Cr^n + Dnr^n$, where C and D are real numbers

19. a statement that certain objects belong to the set

20. a collection of rules indicating how to form new set objects from those already known to be in the set

21. a statement that no objects belong to the set other than those coming from either the BASE or the RECURSION

22. BASE; RECURSION

23. structural induction

24. each object in the BASE satisfies the property
    the rule is applied to an object or objects in the BASE
    the object defined by the rule also satisfies the property

25. its rule of definition refers to itself

General Review Guide: Chapter 9

Definitions: How are the following terms defined?

- real-valued function of a real variable *(p. 510)*
- graph of a real-valued function of a real variable *(p. 511)*
- power function with exponent *a* *(p. 511)*
- floor function *(p. 512)*
- multiple of a real-valued function of a real variable *(p. 514)*
- increasing function *(pp. 515-6)*
- decreasing function *(pp. 515-6)*
- $f(x)$ is $\Omega(g(x)$, where f and g are real-valued functions of a real variable defined on the same set of nonnegative real numbers *(p. 519)*
- $f(x)$ is $O(g(x))$, where f and g are real-valued functions of a real variable defined on the same set of nonnegative real numbers *(p. 519)*
- $f(x)$ is $\Theta(g(x))$, where f and g are real-valued functions of a real variable defined on the same set of nonnegative real numbers *(p. 519)*
- algorithm A is $\Theta(g(n)$ (or A has order $g(n)$) *(p. 533)*
- algorithm A is $\Omega(g(n)$ (or A has a best case order $g(n)$) *(p. 533)*
- algorithm A is $O(g(n)$ (or A has a worst case order $g(n)$) *(p. 533)*

Polynomial and Rational Functions and Their Orders

- What is the difference between the graph of a function defined on an interval of real numbers and the graph of a function defined on a set of integers? *(p. 513)*
- How do you graph a multiple of a real-valued function of a real variable? *(p. 514)*
- How do you prove that a function is increasing (decreasing)? *(p. 516)*
- What are some properties of O-, Ω-, and Θ-notation? Can you prove them? *(p. 521)*
- If $x > 1$, what is the relationship between x^r and x^s, where r and s are rational numbers and $r < s$? *(p. 522)*
- Given a polynomial, how do you use the definition of Θ-notation to show that the polynomial has order x^n, where n is the degree of the polynomial? *(pp. 523-5)*
- What is the theorem on polynomial orders? *(p. 526)*
- What is an order for the sum of the first n integers? *(p. 527)*

Efficiency of Algorithms

- How do you compute the order of an algorithm segment that contains a loop? a nested loop? *(pp. 533-35)*
- How do you find the number of times a loop will iterate when an algorithm segment is executed? *(p. 534)*
- How do you use the theorem on polynomial orders to help find the order of an algorithm segment? *(p. 535)*
- What is the sequential search algorithm? How do you compute its worst case order? its average case order? *(p. 536)*
- What is the insertion sort algorithm? How do you compute its best and worst case orders? *(p. 536)*

Logarithmic and Exponential Orders

- What do the graphs of logarithmic and exponential functions look like? *(pp. 544-5)*

- What can you say about the base 2 logarithm of a number that is between two consecutive powers of 2? *(p. 546)*
- How do you compute the number of bits needed to represent a positive integer in binary notation? *(p. 547)*
- How are logarithms used to solve recurrence relations? *(p. 548)*
- If $b > 1$, what can you say about the relation among $\log_b x$, x^r, and $x \log_b x$? *(p. 550)*
- If $b > 1$ and $c > 1$, how are orders of $\log_b x$ and $\log_c x$ related? *(p. 552)*
- What is an order for a harmonic sum? *(p. 553)*
- What is a divide-and-conquer algorithm? *(p. 557)*
- What is the binary search algorithm? *(p. 557)*
- What is the worst case order for the binary search algorithm, and how do you find it? *(p. 560)*
- What is the merge sort algorithm? *(p. 564)*
- What is the worst case order for the merge sort algorithm, and how do you find it? *(p. 567)*

Test Your Understanding: Chapter 9

Test yourself by filling in the blanks.

1. If f is a real-valued function of a real variable, then the domain and co-domain of f are both _____.

2. A point (x, y) lies on the graph of a real-valued function of a real variable f if, and only if, _____.

3. If a is any nonnegative real number, then the power function with exponent a, p_a, is defined by _____.

4. Given a function $f \colon \mathbf{R} \to \mathbf{R}$ and a real number M, the function Mf is defined by _____.

5. Given a function $f \colon \mathbf{R} \to \mathbf{R}$, to prove that f is increasing, you suppose that _____ and then you show that _____.

6. Given a function $f \colon \mathbf{R} \to \mathbf{R}$, to prove that f is decreasing, you suppose that _____ and then you show that _____.

7. A sentence of the form "$A|g(x)| \le |f(x)|$ for all $x > a$," translates into Ω-notation as _____.

8. A sentence of the form "$|f(x)| \le B|g(x)|$ for all $x > b$," translates into O-notation as _____.

9. A sentence of the form "$A|g(x)| \le |f(x)| \le B|g(x)|$ for all $x > k$," translates into Θ-notation as _____.

10. When $x > 1$, x^2 _____ x and x^5 _____ x^2.

11. According to the theorem on polynomial orders, if $p(x)$ is a polynomial in x, then $p(x)$ is $\Theta(x^n)$, where n is _____.

12. If n is a positive integer, then $1 + 2 + 3 + \cdots + n$ has order _____.

13. When an algorithm segment contains a nested **for-next** loop, you can find the number of times the loop will iterate by constructing a table in which each column represents _____.

14. In the worst case, the sequential search algorithm has to look through _____ elements of the input array before it terminates

15. The worst case order of the insertion sort algorithm is ____, and its average case order is ____.

16. The domain of the exponential function is ____, and its range is ____.

17. The domain of the logarithmic function is ____, and its range is ____.

18. If k is an integer and $2^k \leq x < 2^{k+1}$, then $\lfloor \log_2 x \rfloor = $ ____.

19. If b is a real number with $b > 1$ and if x is a sufficiently large real number, then when the quantities x, x^2, $\log_b x$, and $x \log_b x$ are arranged in order of increasing size, the result is ____.

20. If n is a positive integer, then $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$ has order ____.

21. To solve a problem using a divide-and-conquer algorithm, you reduce it to ____, which ____ and so forth until ____.

22. To search an array using the binary search algorithm in each step, you compare a middle element of the array to ____. If the middle element is less than ____, you ____, and if the middle element is greater than ____, you ____.

23. The worst case order of the binary search algorithm is ____.

24. To sort an array using the merge sort algorithm, in each step until the last one you split the array into approximately two equal sections and sort each section using ____. Then you ____ the two sorted sections.

25. The worst case order of the merge sort algorithm is ____.

Answers

1. sets of real numbers
2. $y = f(x)$
3. $p_a(x) = x^a$ for all real numbers x
4. $(Mf)(x) = M \cdot f(x)$ for $x \in \mathbf{R}$
5. x_1 and x_2 are any real numbers such that $x_1 < x_2$
   $f(x_1) < f(x_2)$
6. x_1 and x_2 are any real numbers such that $x_1 < x_2$
   $f(x_1) > f(x_2)$
7. $f(x)$ is $\Omega(g(x))$
8. $f(x)$ is $O(g(x))$
9. $f(x)$ is $\Theta(g(x))$
10. $>, >$
11. the degree of $p(x)$
12. n^2
13. one iteration of the innermost loop
14. n
15. n^2, n^2
16. the set of all real numbers, the set of all positive real numbers
17. the set of all positive real numbers, the set of all real numbers
18. k
19. $\log_b x \leq x \leq x \log_b x \leq x^2$
20. $\ln x$ (or, equivalently, $\log_2 x$)
21. a fixed number of smaller problems of the same kind
    can themselves be reduced to the same finite number of smaller problems of the same kind
    easily resolved problems are obtained

22. the element you are looking for
    the element you are looking for
    apply the binary search algorithm to the lower half of the array
    the element you are looking for
    apply the binary search algorithm to the upper half of the array

23. $\log_2 n$, where n is the length of the array

24. merge sort; merge

25. $n \log_2 n$

General Review Guide: Chapter 10

Definitions: How are the following terms defined?

- binary relation from a set A to a set B *(p. 572)*
- inverse of a binary relation from a set A to a set B *(p. 578)*
- n-ary relation R on $A_1 \times A_2 \times \cdots \times A_n$ *(p. 581)*
- reflexive, symmetric, and transitive properties of a binary relation *(p. 584)*
- transitive closure of a relation *(p. 588)*
- equivalence relation on a set *(p. 597)*
- equivalence class *(p. 599)*
- a is congruent to b modulo d *(p. 597)*
- plaintext and cyphertext *(p. 611)*
- residue of a modulo n *(p. 614)*
- d is a linear combination of a and b *(p. 619)*
- a and b are relatively prime *(p. 621)*
- an inverse of a modulo n *(p. 622)*
- antisymmetric binary relation *(p. 632)*
- partial order relation *(p. 634)*
- a and b are comparable *(p. 639)*
- total order relation *(p. 639)*
- chain, length of a chain *(p. 640)*
- maximal element, greatest element, minimal element, least element *(p. 641)*
- topological sorting *(p. 642)*

General Binary Relations

- Given the definition of a binary relation as a subset of a Cartesian product, what does it mean for one element to be related to another? *(p. 572)*
- How do you draw an arrow diagram for a binary relation? *(p. 574)*
- A function f from A to B is a binary relation from A to B that satisfies what special properties? *(p. 575)*
- Given a binary relation on a set, how do you draw a directed graph for the relation? *(p. 580)*

Properties of Binary Relations and Equivalence Relations

- How do you show that a binary relation on a finite set is reflexive? symmetric? transitive? *(p. 585)*
- How do you show that a binary relation on an infinite set is reflexive? symmetric? transitive? *(p. 589-92)*
- How do you show that a binary relation on a set is not reflexive? not symmetric? not transitive? *(p. 585, p. 590)*
- How do you find the transitive closure of a relation? *(p. 588)*
- What is the binary relation induced by a partition of a set? *(p. 595)*
- How do you prove basic properties of equivalence classes? *(p. 602)*
- Given an equivalence relation on a set A, what is the relationship between the distinct equivalence classes of the relation and the set A? *(p. 603)*
- In what way are rational numbers equivalence classes? *(p. 607)*

Cryptography

- How does the Caesar cipher work? *(p. 611)*
- If a, b, and n are integers with $n > 1$, what are some different ways of expressing the fact that $n \mid (a - b)$? *(p. 613)*
- If n is an integer with $n > 1$, is congruence modulo n an equivalence relation on the set of all integers? *(p. 614)*
- How do you add, subtract, and multiply integers modulo an integer $n > 1$? *(p. 615)*
- What is an efficient way to compute a^k where a is an integer with $a > 1$ and k is a large integer? *(p. 618)*
- How do you express the greatest common divisor of two integers as a linear combination of the integers? *(p. 620)*
- When can you find an inverse modulo n for a positive integer a, and how do you find it? *(p. 621)*
- How do you encrypt and decrypt messages using RSA cryptography? *(p. 624)*
- What is Euclid's lemma? How is it proved? *(p. 625)*
- What is Fermat's little theorem? How is it proved? *(p. 626)*
- What is the Chinese remainder theorem? How is it proved? *(p. 627)*
- Why does the RSA cipher work? *(p. 628)*

Partial Order Relations

- How do you show that a relation on a set is or is not antisymmetric? *(pp. 632-4)*
- If A is a set with a partial order relation R, S is a set of strings over A, and a and b are in S, how do you show that $a \preceq b$, where $\preceq$ denotes the lexicographic ordering of S? *(p. 636)*
- How do you construct the Hasse diagram for a partial order relation? *(p. 637)*
- How do you find a chain in a partially ordered set? *(p. 640)*
- Given a set with a partial order, how do you construct a topological sorting for the elements of the set? *(p. 642)*
- Given a job scheduling problem consisting of a number of tasks, some of which must be completed before others can be begun, how can you use a partial order relation to determine the minimum time needed to complete the job? *(p. 644)*

Test Your Understanding: Chapter 10

Test yourself by filling in the blanks.

1. A binary relation R from A to B is _____.

2. If R is a binary relation, the notation xRy means that _____.

3. If R is a binary relation, the notation $x \not{R} y$ means that _____.

4. For a binary relation R on a set A to be reflexive means that _____.

5. For a binary relation R on a set A to be symmetric means that _____.

6. For a binary relation R on a set A to be transitive means that _____.

7. To show that a binary relation R on an infinite set A is reflexive, you suppose that _____ and you show that _____.

8. To show that a binary relation R on an infinite set A is symmetric, you suppose that _____ and you show that _____.

9. To show that a binary relation R on an infinite set A is transitive, you suppose that _____ and you show that _____.

10. To show that a binary relation R on a set A is not reflexive, you _____.

11. To show that a binary relation R on a set A is not symmetric, you _____.

12. To show that a binary relation R on a set A is not transitive, you _____

13. Given a binary relation R on a set A, the transitive closure of R is the binary relation R^t on A that satisfies the following three properties: _____, _____, and _____.

14. For a binary relation on a set to be an equivalence relation, it must be _____.

15. The notation $m \equiv n \pmod{d}$ is read _____ and means that _____.

16. Given an equivalence relation R on a set A and given an element a in A, the equivalence class of a is denoted _____ and is defined to be _____.

17. If A is a set, R is an equivalence relation on A, and a and b are elements of A, then either $[a] = [b]$ or _____.

18. If A is a set and R is an equivalence relation on A, then the distinct equivalence classes of R form _____.

19. Let $A = \mathbf{Z} \times (\mathbf{Z} - \{0\})$, and define a binary relation R on A by specifying that for all (a, b) and (c, d) in A, $(a, b)R(c, d)$ if, and only if, $ad = bc$. Then there is exactly one equivalence class of R for each _____.

20. When letters of the alphabet are encrypted using the Caesar cipher, the encrypted version of a letter is _____.

21. If a, b, and n are integers with $n > 1$, the following are all different ways of expressing the fact that $n \mid (a - b)$: _____, _____, _____, _____.

22. If a, b, c, d, m and n are integers with $n > 1$ and if $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$, then $a + b \equiv$_____, $a - b \equiv$_____, $ab \equiv$_____, and $a^m \equiv$_____.

23. If a, n, and k are positive integers with $n > 1$, an efficient way to compute $a^k \pmod{n}$ is to write k as a _____ and use the facts about computing products and powers modulo n.

24. To express a greatest common divisor of two integers as a linear combination of the integers, you use the extended _____ algorithm.

25. To find an inverse for a positive integer a modulo an integer n with $n > 1$, you express the number 1 as _____.

26. To encrypt a message M using RSA cryptography with public key pq and e, you use the formula _____, and to decrypt a message C, you use the formula _____, where _____.

27. Euclid's lemma says that for all integers a, b, and c if $\gcd(a, c) = 1$ and $a \mid bc$, then _____.

28. Fermat's little theorem says that if p is any prime number and a is any integer such that $p \nmid a$ then _____.

29. The Chinese remainder theorem says that if $n_1, n_2, \ldots, n_k$ are pairwise relatively prime positive integers and $a_1, a_2, \ldots, a_k$ are any integers, then the congruences $x \equiv a_i \pmod{n_i}$ for $i = 1, 2, \ldots, k$, have a _____.

30. The crux of the proof that the RSA cipher works is that if (1) p and q are large prime numbers, (2) $M < pq$, (3) M is relatively prime to pq, (4) e is relatively prime to $(p-1)(q-1)$, and (5) d is a positive inverse for e modulo $(p-1)(q-1)$, then $M \equiv$ _____.

31. For a binary relation R on a set A to be antisymmetric means that _____.

32. To show that a binary relation R on an infinite set A is antisymmetric, you suppose that _____ and you show that _____.

33. To show that a binary relation R on a set A is not antisymmetric, you _____.

34. To construct a Hasse diagram for a partial order relation, you start with a directed graph of the relation in which all arrows point upward and you eliminate _____, _____, and _____.

35. If A is a set that is partially ordered with respect to a relation $\preceq$ and if a and b are elements of A, we say that a and b are comparable if, and only if, _____ or _____.

36. A relation $\preceq$ on a set A is a total order if, and only if, _____.

37. If A is a set that is partially ordered with respect to a relation $\preceq$, and if B is a subset of A, then B is a chain if, and only if, for all a and b in B, _____.

38. Let A be a set that is partially ordered with respect to a relation $\preceq$, and let a be an element of A.

   (a) a is maximal if, and only if, _____.

   (b) a is a greatest element of A if, and only if, _____.

   (c) a is called minimal if, and only if, _____.

   (d) a is called a least element of A if, and only if, _____.

39. Given a set A that is partially ordered with respect to a relation $\preceq$, the relation $\preceq'$ is a topological sorting for $\preceq$, if, and only if, $\preceq'$ is a _____ and for all a and b in A if $a \preceq b$ then _____.

40. PERT and CPM are used to produce efficient _____.

Answers

1. a subset of $A \times B$
2. x is related to y by R
3. x is not related to y by R
4. for all x in A; $x\,R\,x$
5. for all x and y in A, if $x\,R\,y$ then $y\,R\,x$
6. for all x, y, and z in A, if $x\,R\,y$ and $y\,R\,z$ then $x\,R\,z$
7. x is any element of A; $x\,R\,x$
8. x and y are any elements of A such that $x\,R\,y$; $y\,R\,x$
9. x, y, and z are any elements of A such that $x\,R\,y$ and $y\,R\,z$; $x\,R\,z$
10. show the existence of an element x in A such that $x\,\not\!R\,x$
11. show the existence of elements x and y in A such that $x\,R\,y$ but $y\,\not\!R\,x$
12. show the existence of elements x, y, and z in A such that $x\,R\,y$ and $y\,R\,z$ but $x\,\not\!R\,z$
13. R^t is transitive; $R \subseteq R^t$; If S is any other transitive relation that contains R, then $R^t \subseteq S$
14. reflexive, symmetric, and transitive
15. m is congruent to n modulo d; d divides $m - n$
16. $[a]$; the set of all x in A such that $x\,R\,a$

17. $[a] \cap [b] = \emptyset$

18. a partition of A

19. rational number

20. three places in the alphabet to the right of the letter, with X wrapped around to A, Y to B, and Z to C

21. $a \equiv b \pmod{n}$
    $a = b + kn$ for some integer k
    a and b have the same nonnegative remainder when divided by n
    $a \bmod n = b \bmod n$

22. $(c + d) \pmod{n}$; $(c - d) \pmod{n}$; $(cd) \pmod{n}$; $c^m \pmod{n}$

23. sum of powers of 2

24. version of the Euclidean

25. a linear combination of a and n

26. $C = M^e \bmod pq$; $M = C^d \bmod pq$; d is a positive inverse for e modulo $(p-1)(q-1)$

27. $a \mid b$

28. $a^{p-1} \equiv 1 \pmod{p}$

29. simultaneous solution x that is unique modulo n, where $n = n_1 n_2 \cdots n_k$

30. $M^{ed} \pmod{pq}$

31. for all a and b in A, if $a \, R \, b$ and $b \, R \, a$ then $a = b$

32. a and b are any elements of A with $a \, R \, b$ and $b \, R \, a$; $a = b$

33. show the existence of elements a and b in A such that $a \, R \, b$ and $b \, R \, a$ and $a \neq b$

34. all loops; all arrows whose existence is implied by the transitive property; the direction indicators on the arrows

35. $a \preceq b$; $b \preceq a$

36. for any two elements a and b in A; either $a \preceq b$ or $b \preceq a$

37. a and b are comparable

38.
    (a) for all b in A either $b \preceq a$ or b and a are not comparable
    (b) for all b in A, $b \preceq a$
    (c) for all b in A either $a \preceq b$ or b and a are not comparable
    (d) for all b in A, $a \preceq b$

39. total order; $a \preceq b$

40. scheduling of tasks

General Review Guide: Chapter 11

Definitions: How are the following terms defined?

- graph *(p. 650)*
- directed graph *(p. 653)*
- simple graph *(p. 656)*
- complete graph on n vertices *(p. 656)*
- complete bipartite graph on (m, n) vertices *(p. 657)*
- subgraph *(p. 657)*
- degree of a vertex in a graph, total degree of a graph *(p. 658)*
- walk, path, simple path, closed walk, circuit, simple circuit *(p. 667)*
- trivial circuit, nontrivial circuit *(p. 669)*
- connected vertices, connected graph *(p. 669)*
- connected component of a graph *(p. 670)*
- Euler circuit in a graph *(p. 671)*
- Euler path in a graph *(p. 675)*
- Hamiltonian circuit in a graph *(p. 677)*
- adjacency matrix of a directed (or undirected) graph *(pp. 685-6)*
- symmetric matrix *(p. 687)*
- isomorphic graphs *(p. 698)*
- isomorphic invariant for graphs *(p. 701)*
- circuit-free graph *(p. 705)*
- tree *(p. 705)*
- terminal vertex (or leaf), internal vertex (or branch vertex) *(p. 710)*
- rooted tree, level of a vertex in a rooted tree, height of a rooted tree *(p. 715)*
- parents, children, siblings, descendants, and ancestors in a rooted tree *(p. 715)*
- binary tree, full binary tree *(p. 716)*
- spanning tree *(p. 724)*
- weighted graph, minimum spanning tree *(p. 725)*

Graphs

- What does the handshake theorem say? In other words, how is the total degree of a graph related to the number of edges of the graph? *(p. 659)*
- How can you use the handshake theorem to determine whether graphs with specified properties exist? *(pp. 660, 662)*
- If an edge is removed from a nontrivial circuit in a graph, does the graph remain connected? *(p. 670)*
- A graph has an Euler circuit if, and only if, it satisfies what two conditions? *(p. 675)*
- A graph has a Hamiltonian circuit if, and only if, it satisfies what four conditions? *(p. 678)*
- What is the traveling salesman problem? *(p. 679)*
- How do you find the adjacency matrix of a directed (or undirected) graph? How do you find the graph that corresponds to a given adjacency matrix? *(pp. 685-6)*
- How can you determine the connected components of a graph by examining the adjacency matrix of the graph? *(p. 688)*
- How do you multiply two matrices? *(p. 689)*
- How do you use matrix multiplication to compute the number of walks from one vertex to another in a graph? *(p. 694)*

- How do you show that two graphs are isomorphic? *(p. 698)*
- What are some invariants for graph isomorphisms? *(p. 701)*

Trees

- If a tree has at least two vertices, how many vertices of degree 1 does it have? *(p. 709)*
- If a tree has n vertices, how many edges does it have? *(p. 710)*
- If a connected graph has n vertices, what additional property guarantees that it will be a tree? *(p. 714)*
- Given a full binary tree, what is the relation among the number of its internal vertices, terminal vertices, and total number of vertices? *(p. 717)*
- Given a binary tree, what is the relation between the number of its terminal vertices and its height? *(p. 718)*
- How does Kruskal's algorithm work? *(p. 726)*
- How do you know that Kruskal's algorithm produces a minimum spanning tree? *(p. 727)*
- How does Prim's algorithm work? *(p. 729)*
- How do you know that Prim's algorithm produces a minimum spanning tree? *(p. 730)*

Test Your Understanding: Chapter 11

Test yourself by filling in the blanks.

1. A graph consists of two finite sets: _____ and _____, where each edge is associated with a set consisting of _____.

2. A loop in a graph is _____.

3. Two distinct edges in a graph are parallel if, and only if, _____.

4. An edge is said to _____ its endpoints.

5. Two vertices are called adjacent if, and only if, _____.

6. An edge is incident on _____.

7. Two edges incident on the same endpoint are _____.

8. A vertex on which no edges are incident is _____.

9. A graph with no vertices is _____.

10. In a directed graph, each edge is associated with _____.

11. A simple graph is _____.

12. A complete graph on n vertices is a _____.

13. A complete bipartite graph on (m, n) vertices is a simple graph whose vertices can be divided into two distinct sets V_1 and V_2 in such a way that (1) each of the m vertices in V_1 is _____ to each of the n vertices in V_2, no vertex in V_1 is connected to _____, and no vertex in V_2 is connected to _____.

14. A graph H is a subgraph of a graph G if, and only if, (1) _____, (2) _____, and (3) _____.

15. The degree of a vertex in a graph is _____.

16. The total degree of a graph is ____.

17. The handshake theorem says that the total degree of a graph is ____.

18. In any graph the number of vertices of odd degree is ____.

19. Let G be a graph and let v and w be vertices in G.

    (a) A walk from v to w is ____.

    (b) A path from v to w is ____.

    (c) A simple path from v to w is ____.

    (d) A closed walk is ____.

    (e) A circuit is ____.

    (f) A simple circuit is ____.

    (g) A trivial circuit is ____.

    (h) Vertices v and w are connected if, and only if, ____.

20. A graph is connected if, and only if, ____.

21. Removing an edge from a nontrivial circuit in a graph does not ____.

22. An Euler circuit in a graph is ____.

23. A graph has an Euler circuit if, and only if, ____.

24. Given vertices v and w in a graph, there is an Euler path from v to w if, and only if, ____.

25. A Hamiltonian circuit in a graph is ____.

26. If a graph G has a nontrivial Hamiltonian circuit, then G has a subgraph H with the following properties: ____, ____, ____, and ____.

27. A traveling salesman problem involves finding a ____ that minimizes the total distance traveled for a graph in which each edge is marked with a distance.

28. In an adjacency matrix for a directed graph, the entry in the ith row and jth column is ____.

29. In an adjacency matrix for a (undirected) graph, the entry in the ith row and jth column is ____.

30. An $n \times n$ square matrix is called symmetric if, and only if, for all integers i and j from 1 to n, the entry in row ____ and column ____ equals the entry in row ____ and column ____.

31. The ijth entry in the product of two matrices $\mathbf{A}$ and $\mathbf{B}$ is obtained by multiplying row ____ of $\mathbf{A}$ by row ____ of $\mathbf{B}$.

32. In an $n \times n$ identity matrix the entries along the diagonal are all ____ and the off-diagonal entries are all ____.

33. If G is a graph with vertices $v_1, v_2, \ldots, v_m$ and $\mathbf{A}$ is the adjacency matrix of G, for each positive integer n and for all integers i and j with $i, j = 1, 2, \ldots, m$, the ijth entry of $\mathbf{A}^n =$ ____.

34. If G and G' are graphs, then G is isomorphic to G' if, and only if, there exist a one-to-one correspondence g from the vertex set of G to the vertex set of G' and a one-to-one correspondence h from the edge set of G to the edge set of G' such that for all vertices v and edges e in G, v is an endpoint of e if, and only if, ____.

35. A property P is an isomorphic invariant for graphs if, and only if, given any graphs G and G', if G has property P and G' is isomorphic to G then ____.

36. Some invariant properties for graph isomorphisms are ____, ____, ____, ____, ____, ____, ____, ____, ____, and ____.

37. A circuit-free graph is a graph with ____.

38. A forest is a graph that is ____, and a tree is a graph that is ____.

39. A trivial tree is a graph that consists ____, and an empty tree is a tree that ____.

40. Any tree with at least two vertices has at least one vertex of degree ____.

41. If a tree T has at least two vertices, then a terminal vertex (or leaf) in T is a vertex of degree ____ and an internal vertex (or branch vertex) in T is a vertex of degree ____.

42. For any positive integer n, any tree with n vertices has ____.

43. For any positive integer n, if G is a connected graph with n vertices and $n-1$ edges then ____.

44. A rooted tree is a tree in which ____. The level of a vertex in a rooted tree is ____. The height of a rooted tree is ____.

45. A binary tree is a rooted tree in which ____.

46. A full binary tree is a rooted tree in which ____.

47. If k is a positive integer and T is a full binary tree with k internal vertices, then T has a total of ____ vertices and has ____ terminal vertices.

48. If T is a binary tree that has t terminal vertices and height h, then t and h are related by the inequality ____.

49. A spanning tree for a graph G is ____.

50. A weighted graph is a graph for which ____, and the total weight of the graph is ____.

51. A minimum spanning tree for a connected weighted graph is ____.

52. In Kruskal's algorithm, the edges of a connected, weighted graph are examined one by one in order of ____.

53. In Prim's algorithm, a minimum spanning tree is built by expanding outward ____.

Answers

1. a finite set of vertices, a finite set of edges, either one or two vertices called its endpoints
2. an edge with a single endpoint
3. they have the same set of endpoints
4. connect
5. they are connected by an edge
6. each of its endpoints
7. adjacent
8. isolated
9. empty
10. an ordered pair of vertices called its endpoints
11. a graph with no loops or parallel edges
12. simple graph with n vertices whose set of edges contains exactly one edge for each pair of vertices

13. connected by an edge, any other vertex in V_1, any other vertex in V_2

14. every vertex in H is also a vertex in G, every edge in H is also a vertex in G, every edge in H has the same endpoints as it has in G

15. the number of edges that are incident on the vertex, with an edge that is a loop counted twice

16. the sum of the degrees of all the vertices of the graph

17. equal to twice the number of edges of the graph

18. an even number

19.
    (a) a finite alternating sequence of adjacent vertices and edges of G
    (b) a walk that does not contain a repeated edge
    (c) a path that does not contain a repeated vertex
    (d) a walk that starts and ends at the same vertex
    (e) a closed walk that does not contain a repeated edge
    (f) a circuit that does not have any repeated vertex other than the first and the last
    (g) a walk consisting of a single vertex and no edge
    (h) there is a walk from v to w

20. given any two vertices in the graph there is a walk from one to the other

21. disconnect the graph

22. a circuit that contains every vertex and every edge of the graph

23. the graph is connected and every vertex has even degree

24. the graph is connected, v and w have odd degree, and all other vertices have even degree

25. a simple circuit that includes every vertex of the graph

26. H contains every vertex of G; H is connected; H has the same number of edges as vertices; every vertex of H has degree 2

27. Hamiltonian circuit

28. the number of arrows from v_i (the ith vertex) to v_j (the jth vertex)

29. the number of edges connecting v_i (the ith vertex) and v_j (the jth vertex)

30. i; j; j; i

31. i; j

32. 1; 0

33. the number of walks of length n from v_i to v_j

34. $g(v)$ is an endpoint of $h(e)$

35. G' has property P

36. has n vertices; has m edges; has a vertex of degree k; has m vertices of degree k; has a circuit of length k; has a simple circuit of length k; has m simple circuits of length k; is connected; has an Euler circuit; has a Hamiltonian circuit

37. no nontrivial circuits

38. circuit-free; connected and circuit-free

39. of a single vertex and no edges; has no vertices or edges

40. 1

41. 1; at least 2

42. $n - 1$ edges

43. G is a tree

44. one vertex is distinguished from the others and is called the root
the number of edges along the unique path between it and the root
the maximum level of any vertex of the tree

45. every parent has at most two children

46. every parent has exactly two children

47. $2k + 1$; $k + 1$

48. $t \le 2^h$, or, equivalently, $\log_2 t \le h$
49. a subgraph of G that contains every vertex of G and is a tree
50. each edge has an associated real number weight
    the sum of the weights of all the edges of the graph
51. a spanning tree that has the least possible total weight compared to all other spanning trees for the graph
52. weight, starting with an edge of least weight
53. in a sequence of adjacent edges starting from some vertex

General Review Guide: Chapter 12

Definitions: How are the following terms defined?

- alphabet, string over an alphabet, formal language over an alphabet *(p. 736)*
- Σ^n, Σ^* (the Kleene closure of Σ), and Σ^+ (the positive closure of Σ), where Σ is an alphabet *(p. 736)*
- concatenation of x and y, where x and y are strings *(p. 738)*
- concatenation of L and L', where L and L' are languages *(p. 738)*
- union of L and L', where L and L' are languages *(p. 738)*
- Kleene closure of L , where L is a language *(p. 738)*
- regular expression over an alphabet *(p. 738)*
- language defined by a regular expression *(p. 739)*
- finite-state automaton *(p. 748)*
- language accepted by a finite-state automaton *(p. 750)*
- eventual-state function for a finite-state automaton *(p. 751)*
- regular language *(p. 759)*
- $*$-equivalence of states in a finite-state automaton *(p. 764)*
- k-equivalence of states in a finite-state automaton *(p. 765)*
- quotient automaton *(p. 769)*
- equivalent automata *(p. 771)*

Regular Expressions

- What is the order of precedence for the operations in a regular expression? *(p. 737)*
- How do you find the language defined by a regular expression? *(p. 740)*
- Given a language, how do you find a regular expression that defines the language? *(p. 741)*
- What are some practical uses of regular expressions? *(p. 742)*

Finite-State Automata

- How do you construct an annotated next-state table for a finite-state automaton given the transition diagram for the automaton? *(p. 748)*
- How do you construct a transition diagram for a finite-state automaton given its next-state table? *(p. 749)*
- How do you find the state to which a finite-state automaton goes if the characters of a string are input to it? *(p. 750)*
- How do you find the language accepted by a finite-state automaton? *(p. 750)*
- Given a simple formal language, how do you construct a finite-state automaton to accept the language? *(p. 752)*
- How can you use software to simulate the action of a finite-state automaton? *(p. 754)*
- What do the two parts of Kleene's theorem say about the relation between the language accepted by a finite-state automaton and the language defined by a regular expression? *(pp. 756, 758)*
- How can the pigeonhole principle be used to show that a language is not regular? *(p. 759)*
- How do you find the k-equivalence classes for a finite-state automaton? *(p. 766)*
- How do you find the $*$-equivalence classes for a finite-state automaton? *(p. 767)*
- How do you construct the quotient automaton for a finite-state automaton? *(p. 769)*
- What is the relation between the language accepted by a finite-state automaton and the language accepted by the corresponding quotient automaton? *(p. 769)*

Test Your Understanding: Chapter 12

Test yourself by filling in the blanks.

1. If x and y are strings, the concatenation of x and y is _____.

2. If L and L' are languages, the concatenation of L and L' is _____.

3. If L and L' are languages, the union of L and L' is _____.

4. If L is a language, the Kleene closure of L is _____.

5. The set of regular expressions over a finite alphabet Σ is defined recursively. The BASE for the definition is the statement that _____. The RECURSION for the definition specifies that if r and s are any regular expressions in the set, then the following are also regular expressions in the set: _____, _____, and _____.

6. The function that associates a language to each regular expression over an alphabet Σ is defined recursively. The BASE for the definition is the statement that $L(\emptyset) =$ _____, $L(\epsilon) =$ _____, and $L(a) =$ _____ for every $a \in \Sigma$. The RECURSION for the definition specifies that if $L(r)$ and $L(r\prime)$ are the languages defined by the regular expressions r and r' over Σ, then $L(rr') =$ _____, $L(r \mid r') =$ _____, and $L(r^*) =$ _____.

7. The notation $[A - C\ x - z]$ is an example of a _____ and denotes the regular expression _____.

8. Use of a single dot in a regular expression stands for _____.

9. The symbol $^\wedge$, placed at the beginning of a character class, indicates _____.

10. The symbol $+$ following a regular expression r means that _____.

11. If r is a regular expression, the notation $r?$ denotes _____.

12. If r is a regular expression, the notation $r\{n\}$ means that _____ and the notation $r\{m,n\}$ means that _____.

13. The five objects that make up a finite-state automaton are _____, _____, _____, _____, and _____.

14. The next-state table for an automaton shows the values of _____.

15. In the annotated next-state table, the initial state is indicated with an _____ and the accepting states are marked by _____.

16. A string w consisting of input symbols is accepted by a finite-state automaton A if, and only if, _____.

17. The language accepted by a finite-state automaton A is _____.

18. If N is the next-state function for a finite-state automaton A, the eventual-state function N^* is defined as follows: for each state s of A and for each string w that consists of input symbols of A, $N^*(s, w) =$ _____.

19. One part of Kleene's theorem says that given any language that is accepted by a finite-state automaton, there is _____.

20. The second part of Kleene's theorem says that given any language defined by a regular expression, there is _____.

21. A regular language is _____.

22. Given the language consisting of all strings of the form $a^k b^k$, where k is a positive integer, the pigeonhole principle can be used to show that the language is _____.

23. Given a finite-state automaton A with eventual-state function N^* and given any states s and t in A, we say that s and t are $*$-equivalent if, and only if, _____.

24. Given a finite-state automaton A with eventual-state function N^* and given any states s and t in A, we say that s and t are k-equivalent if, and only if, _____.

25. Given states s and t in a finite-state automaton A, s is 0-equivalent to t if, and only if, either both s and t are _____ or both are _____. Moreover, for every integer $k \geq 1$, s is k-equivalent to t if, and only if, (1) s and t are $(k-1)$-equivalent and (2) _____.

26. If A is a finite-state automaton, then for some integer $K \geq 0$, the set of K-equivalence classes of states of A equals the set of _____-equivalence classes of A, and for all such K these are both equal to the set of _____.

27. Given a finite-state automaton A, the set of states of the quotient automaton $\bar{A}$ is _____.

Answers

1. the string obtained by juxtaposing the characters of x and y
2. $\{xy \mid x \in L \text{ and } y \in L'\}$
3. $\{s \mid s \in L \text{ or } s \in L'\}$
4. $\{t \mid t \text{ is a concatenation of any finite number of strings in } L\}$
5. $\emptyset$, ϵ, and each individual symbol in Σ are regular expressions over Σ; (rs); $(r \mid s)$; (r^*)
6. $\emptyset$; $\{\epsilon\}$; $\{a\}$; $L(r)L(r')$; $L(r) \cup L(r')$; $(L(r))^*$
7. character class; $(A \mid B \mid C \mid x \mid y \mid z)$
8. an arbitrary character
9. a character of the same type as those in the range of the class, but not any of the characters following the $^\wedge$, is to occur at that point in the string
10. the string contains at least one occurrence of r
11. $(\epsilon \mid r)$
12. r can be concatenated with itself n times; r can be concatenated with itself from m through n times
13. a finite set of states; a finite set of input symbols; a designated initial state; a designated set of accepting states; a next-state function that associates a "next-state" with each state and input symbol of the automaton
14. the next-state function for each state and input symbol of the automaton
15. arrow; double circles
16. when the symbols in the string are input to the automaton in sequence from left to right, starting from the initial state, the automaton ends up in an accepting state
17. the set of strings that are accepted by A
18. the state to which A goes if it is in state s and the characters of w are input to it in sequence
19. a regular expression that defines the same language
20. a finite-state automaton that accepts the same language
21. a language defined by a regular expression
22. not regular
23. for all input strings w, either $N^*(s, w)$ and $N^*(t, w)$ are both accepting states or both are nonaccepting states
24. for all input strings w of length less than or equal to k, either $N^*(s, w)$ and $N^*(t, w)$ are both accepting states or both are nonaccepting states
25. accepting states, nonaccepting states; for any input symbol m, $N(s, m)$ and $N(t, m)$ are also $(k-1)$-equivalent
26. $(K+1)$; $*$-equivalence classes of states of A
27. the set of $*$-equivalence classes of states of A

Tips for Success with Proofs and Disproofs

Make sure your proofs are genuinely convincing. Express yourself carefully and completely – but concisely! Write in complete sentences, but don't use an unnecessary number of words.

Disproof by Counterexample

- To disprove a universal statement, give a counterexample.
- Write the word "Counterexample" at the beginning of a counterexample.
- Write counterexamples in complete sentences.
- Give values of the variables that you believe show the property is false.
- Include the computations that prove beyond any doubt that these values really do make the property false.

All Proofs

- Write the word "Proof" at the beginning of a proof.
- Write proofs in complete sentences.
- Start each sentence with a capital letter and finish with a period.

Direct Proof

- Begin each direct proof with the word "Suppose."
- In the "Suppose" sentence:
    - Introduce a variable or variables (indicating the general set they belong to - e.g., integers, real numbers etc.), and
    - Include the hypothesis that the variables satisfy.
- Identify the conclusion that you will need to show in order to complete the proof.
- Reason carefully from the "suppose" to the "conclusion to be shown."
- Include the little words (like "Then," "Thus," "So," "It follows that") that make your reasoning clear.
- Give a reason to support each assertion you make in your proof.

Proof by Contradiction

- Begin each proof by contradiction by writing "Suppose not. That is, suppose...," and continue this sentence by carefully writing the negation of the statement to be proved.
- After you have written the "suppose," you need to show that this supposition leads logically to a contradiction.
- Once you have derived a contradiction, you can conclude that the think you supposed is false. Since you supposed that the given statement was false, you now know that the given statement is true.

Proof by Contraposition

- Look to see if the statement to be proved is a universal conditional statement.
- If so, you can prove it by writing a direct proof of its contrapositive.

Formats for Proving Formulas by Mathematical Induction

When using mathematical induction to prove a formula, students are sometimes tempted to present their proofs in a way that assumes what is to be proved. There are several formats you can use, besides the one shown most frequently in the textbook, to avoid this fallacy. A crucial point is this:

> If you are hoping to prove that an equation is true but you haven't yet done so, either preface it with the words "We must show that" or put a question mark above the equal sign.

Format 1 (the format used most often in the textbook for the inductive step): Start with the left-hand side (LHS) of the equation to be proved and successively transform it using definitions, known facts from basic algebra, and (for the inductive step) the inductive hypothesis until you obtain the right-hand side (RHS) of the equation.

Format 2 (the format used most often in the textbook for the basis step): Transform the LHS and the RHS of the equation to be proved *independently*, one after the other, until both sides are shown to equal the same expression. Because two quantities equal to the same quantity are equal to each other, you can conclude that the two sides of the equation are equal to each other.

Format 3: This format is just like Format 2 except that the computations are done in parallel. But in order to avoid the fallacy of assuming what is to be proved, do NOT put an equal sign between the two sides of the equation until the very last step. Separate the two sides of the equation with a vertical line.

Format 4: This format is just like Format 3 except that the two sides of the equation are separated by an equal sign with a question mark on top: $\stackrel{?}{=}$

Format 5: Start by writing something like "We must show that" and the equation you want to prove true. In successive steps, indicate that this equation is true if, and only if, ($\Leftrightarrow$) various other equations are true. But be sure that both the directions of your "if and only if" claims are correct. In other words, be sure that the $\Leftarrow$ direction is just as true as the $\Rightarrow$ direction. If you finally get down to an equation that is known to be true, then because each subsequent equation is true *if, and only if*, the previous equation is true, you will have shown that the original equation is true.

Example: Prove that for each integer $n \geq 1$,

$$\boxed{1 + 3 + 5 + \cdots + (2n - 1) = n^2} \leftarrow \text{This is the equation.}$$

Proof that the equation is true for $n = 1$:

Solution (Format 2):
When $n = 1$, the LHS of the equation equals 1, and the RHS equals 1^2 which also equals 1. So the equation is true for $n = 1$.

Solution (Format 5):
When $n = 2$, we must show that $1 = 1^2$. Because this is true, the equation is true for $n = 1$.

Proof that if the equation is true for $n = k$ then it is true for $n = k + 1$:

Solution (Format 2):
Suppose that for some integer $k \geq 1$, $1 + 3 + 5 + \cdots + (2k - 1) = k^2$. *[This is the inductive hypothesis.]*
We must show that $1 + 3 + 5 + \cdots + (2k + 1) = (k + 1)^2$.
But the LHS of the equation to be shown is

$$1 + 3 + 5 + \cdots + (2k + 1) = 1 + 3 + 5 + \cdots + (2k - 1) + (2k + 1)$$
$$\text{by making the next-to-last term explicit}$$
$$= k^2 + (2k + 1) \qquad \text{by inductive hypothesis.}$$

And the RHS of the equation to be shown is

$$(k + 1)^2 = k^2 + 2k + 1 \qquad \text{by basic algebra.}$$

So the LHS and the RHS are equal to the same quantity, and thus they are equal to each other *[as was to be shown]*.

Solution (Format 3):
Suppose that for some integer $k \geq 1$, $1 + 3 + 5 + \cdots + (2k - 1) = k^2$. *[This is the inductive hypothesis.]*
We must show that $1 + 3 + 5 + \cdots + (2k + 1) = (k + 1)^2$.
But

$$
\begin{array}{ll}
1 + 3 + 5 + \cdots + (2k + 1) & \Big| \quad (k + 1)^2 \\
= 1 + 3 + 5 + \cdots + (2k - 1) + (2k + 1) & \Big| \\
\quad \text{by making the next-to-last term explicit} & \Big| \\
= k^2 + (2k + 1) & \Big| \\
\quad \text{by inductive hypothesis} & \Big| \\
= k^2 + 2k + 1 & \Big| \quad = k^2 + 2k + 1 \\
\quad \text{by basic algebra} & \Big| \qquad \text{by basic algebra}
\end{array}
$$

So the LHS and the RHS are equal to the same quantity, and thus they are equal to each other *[as was to be shown]*.

Solution (Format 4):
Suppose that for some integer $k \geq 1$, $1 + 3 + 5 + \cdots + (2k - 1) = k^2$. *[This is the inductive hypothesis.]*
We must show that $1 + 3 + 5 + \cdots + (2k + 1) = (k + 1)^2$.
But

$$
\begin{array}{lcl}
1 + 3 + 5 + \cdots + (2k + 1) & \overset{?}{=} & (k + 1)^2 \\
1 + 3 + 5 + \cdots + (2k - 1) + (2k + 1) & \overset{?}{=} & k^2 + 2k + 1 \\
\quad \text{by making the next-to-last term explicit} & & \quad \text{by basic algebra} \\
k^2 + (2k + 1) & \overset{?}{=} & k^2 + 2k + 1 \\
\quad \text{by inductive hypothesis} & & \\
k^2 + 2k + 1 & = & k^2 + 2k + 1 \\
\quad \text{by basic algebra} & &
\end{array}
$$

So the LHS and the RHS are equal to the same quantity, and thus they are equal to each other *[as was to be shown]*.

Solution (Format 5):
Suppose that for some integer $k \geq 1$, $1 + 3 + 5 + \cdots + (2k - 1) = k^2$. *[This is the inductive hypothesis.]*
We must show that $1 + 3 + 5 + \cdots + (2k + 1) = (k + 1)^2$.
But this equation is true if, and only if, ($\Leftrightarrow$)

$$
\begin{array}{rcll}
1 + 3 + 5 + \cdots + (2k - 1) + (2k + 1) & = & (k + 1)^2 & \text{by making the next-to-last term explicit} \\
\Leftrightarrow \qquad k^2 + (2k + 1) & = & (k + 1)^2 & \text{by inductive hypothesis} \\
\Leftrightarrow \qquad k^2 + 2k + 1 & = & (k + 1)^2 &
\end{array}
$$

which is true by basic algebra. Thus the equation to be shown is also true.

Supplementary Exercises and Exam Questions

Chapter 1

1. Which of the following is a negation for "Jim is inside and Jan is at the pool."

   (a) Jim is inside or Jan is not at the pool.
   (b) Jim is inside or Jan is at the pool.
   (c) Jim is not inside or Jan is at the pool.
   (d) Jim is not inside and Jan is not at the pool.
   (e) Jim is not inside or Jan is not at the pool.

2. Which of the following is a negation for "Jim has grown or Joan has shrunk."

   (a) Jim has grown or Joan has shrunk.
   (b) Jim has grown or Joan has not shrunk.
   (c) Jim has not grown or Joan has not shrunk.
   (d) Jim has grown and Joan has shrunk.
   (e) Jim has not grown and Joan has not shrunk.
   (f) Jim has grown and Joan has not shrunk.

3. Write a negation for each of the following statements:

   (a) The variable S is undeclared and the data are out of order.
   (b) The variable S is undeclared or the data are out of order.
   (c) If Al was with Bob on the first, then Al is innocent.
   (d) $-5 \leq x < 2$ (where x is a particular real number)

4. Are the following statement forms logically equivalent: $p \vee q \rightarrow p$ and $p \vee (\sim p \wedge q)$? Include a truth table and a few words explaining how the truth table supports your answer.

5. State precisely (but concisely) what it means for two statement forms to be logically equivalent.

6. Write the following two statements in symbolic form and determine whether they are logically equivalent. Include a truth table and a few words explaining how the truth table supports your answer.

   If Sam bought it at Crown Books, then Sam didn't pay full price.

   Sam bought it at Crown Books or Sam paid full price.

7. Write the following two statements in symbolic form and determine whether they are logically equivalent. Include a truth table and a few words explaining how the truth table supports your answer.

   If Sam is out of Schlitz, then Sam is out of beer.

   Sam is not out of beer or Sam is not out of Schlitz.

8. Write the converse, inverse, and contrapositive of "If Ann is Jan's mother, then Jose is Jan's cousin."

9. Write the converse, inverse, and contrapositive of " If Ed is Sue's father, then Liu is Sue's cousin."

10. Write the converse, inverse, and contrapositive of "If Al is Tom's cousin, then Jim is Tom's grandfather."

11. Rewrite the following statement in if-then form without using the word "necessary": Getting an answer of 10 for problem 16 is a necessary condition for solving problem 16 correctly.

12. State precisely (but concisely) what it means for a form of argument to be valid.

13. Consider the argument form:

$$p \rightarrow \sim q$$
$$q \rightarrow \sim p$$
$$\therefore \quad p \vee q$$

Use the truth table below to determine whether this form of argument is valid or invalid. Include a truth table and a few words explaining how the truth table supports your answer.

p	q	$\sim p$	$\sim q$	$p \rightarrow \sim q$	$q \rightarrow \sim p$	$p \vee q$
T	T	F	F	F	F	T
T	F	F	T	T	T	T
F	T	T	F	T	T	T
F	F	T	T	T	T	F

14. Consider the argument form:

$$p \wedge \sim q \rightarrow r$$
$$p \vee q$$
$$q \rightarrow p$$
Therefore r.

Use the truth table below to determine whether this argument form is valid or invalid. Annotate the table (as appropriate) and include a few words explaining how the truth table supports your answer.

p	q	r	$\sim q$	$p \wedge \sim q$	$p \wedge \sim q \rightarrow r$	$p \vee q$	$q \rightarrow p$	r
T	T	T	F	F	T	T	T	T
T	T	F	F	F	T	T	T	F
T	F	T	T	T	T	T	T	T
T	F	F	T	T	F	T	T	F
F	T	T	F	F	T	T	F	T
F	T	F	F	F	T	T	F	F
F	F	T	T	F	T	F	T	T
F	F	F	T	F	T	F	T	F

15. Determine whether the following argument is valid or invalid. Include a truth table and a few words explaining why the truth table shows validity or invalidity.

If Hugo is a physics major or if Hugo is a math major, then he needs to take calculus.

Hugo needs to take calculus or Hugo is a math major.

Therefore, Hugo is a physics major or Hugo is a math major.

16. Determine whether the following argument is valid or invalid. Include a truth table and a few words explaining why the truth table shows validity or invalidity.

> If 12 divides 709,438 then 3 divides 709,438.
> If the sum of the digits of 709,438 is divisible by 9 then 3 divides 709,438.
> The sum of the digits of 709,438 is not divisible by 9.
>
> Therefore,   12 does not divide 709,438.

17. Write the form of the following argument. Is the argument valid or invalid? Justify your answer.

> If 54,587 is a prime number, then 17 is not a divisor of 54,587.
> 17 is a divisor of 54,587.
>
> Therefore,   54,587 is not a prime number.

18. Write the form of the following argument. Is the argument valid or invalid? Justify your answer.

> If Ann has the flu, then Ann has a fever.
> Ann has a fever.
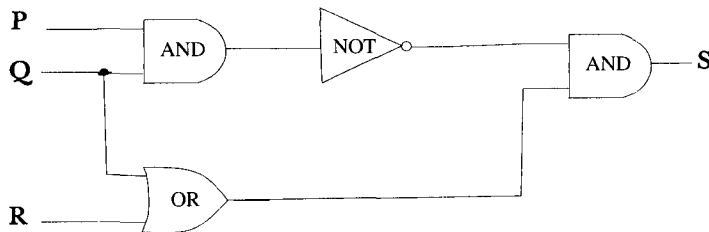>
> Therefore,   Ann has the flu.

19. On the island of knights and knaves, you meet three natives, A, B, and C, who address you as follows:

A: At least one of us is a knave.

B: At most two of us are knaves.

What are A, B, and C?

20. Consider the following circuit.

(a) Find the output of the circuit corresponding to the input $P = 1$, $Q = 0$, and $R = 1$.

(b) Write the Boolean expression corresponding to the circuit.

21. Write 110101_2 in decimal form.

22. Write 75 in binary notation.

23. Draw the circuit that corresponds to the following Boolean expression: $(P \wedge Q) \vee (\sim P \wedge \sim Q)$.(*Note for students who have studied some circuit design*: Do not simplify the circuit; just draw the one that exactly corresponds to the expression.)

24. Find a circuit with the following input/output table.

P	Q	R	S
1	1	1	0
1	1	0	0
1	0	1	1
1	0	0	0
0	1	1	1
0	1	0	0
0	0	1	0
0	0	0	0

25. Find $10111_2 + 1011_2$.

26. Write 100110_2 in decimal form.

27. Write the 8-bit two's complement for 49.

Chapter 2

1. Rewrite the following statement in the form $\forall$ _____ x, if _____ then _____ (where each of the second two blanks are sentences involving the variable x)

    Every valid argument with true premises has a true conclusion.

2. Consider the statement "The square of any odd integer is odd."

    (a) Rewrite the statement in the form $\forall$_____ n, _____. (Do not use the words "if" or "then.")

    (b) Rewrite the statement in the form $\forall$_____ n, if _____ then _____. (Make sure you use the variable n when you fill in each of the second two blanks.)

    (c) Write a negation for the statement.

3. Rewrite the following statement formally. Use variables and include both quantifiers $\forall$ and $\exists$ in your answer.

    Every rational number can be written as a ratio of some two integers.

4. Rewrite the following statement formally. Use variables and include both quantifiers $\forall$ and $\exists$ in your answer.

    Every even integer greater than 2 can be written as a sum of two prime numbers.

5. Write a negation for each of the following statements:

    (a) For all integers n, if n is prime then n is odd.

    (b) $\forall$ real numbers x, if $x < 1$ then $\dfrac{1}{x} > 1$.

    (c) For all integers a and b, if a^2 divides b^2 then a divides b.

    (d) For all real numbers x and y with $x < y$, there exists an integer n such that $x \leq n \leq y$.

    (e) $\forall$ real numbers x, if $x(x - 2) > 0$ then $x > 2$ or $x < 0$.

    (f) $\forall$ real numbers x, if $x(x - 2) \leq 0$ then $0 \leq x \leq 2$.

6. Which of the following is a negation for "Given any real numbers a and b, if a and b are rational then a/b is rational."

    (a) There exist real numbers a and b such that a and b are not rational and a/b is not rational.

    (b) Given any real numbers a and b, if a and b are not rational then a/b is not rational.

    (c) There exist real numbers a and b such that a and b are not rational and a/b is rational.

    (d) Given any real numbers a and b, if a and b are rational then a/b is not rational.

    (e) There exist real numbers a and b such that a and b are rational and a/b is not rational.

    (f) Given any real numbers a and b, if a and b are not rational then a/b is rational.

7. Which of the following is a negation for "For all real numbers r, there exists a number s such that $rs > 10$."

    (a) There exists a real number r such that for all real numbers s, $rs \not> 10$.

    (b) For all real numbers r, there does not exist a number s such that $rs > 10$.

    (c) There exists real numbers r and s such that $rs \not> 10$.

    (d) For all real numbers r and s, $rs \not> 10$.

    (e) There exists a real number r and there does not exist a real number s such that $rs \not> 10$.

    (f) For all real numbers r, there exists a number s such that $rs \not> 10$.

    (g) There exists a real number r such that there does not exist a real number s with $rs \neq 1$.

8. Which of the following is a negation for "There exists a real number x such that for all real numbers y, $xy > y$."

    (a) There exists a real number x such that for all real numbers y, $xy \leq y$.

    (b) There exists a real number y such that for all real numbers x, $xy \leq y$.

    (c) There exist real numbers x and y such that $xy \leq y$.

    (d) For all real numbers x there exists a real number y such that $xy \leq y$.

    (e) For all real numbers y there exists a real number x such that $xy \leq y$.

    (f) For all real numbers x and y, $xy \leq y$.

9. Which of the following is a negation for "For any integer n, if n is composite, then n is even or $n > 2$."

    (a) For any integer n, if n is composite, then n is not even or $n \leq 2$.

    (b) For any integer n, if n is not composite, then n is not even or $n \leq 2$.

    (c) For any integer n, if n is not composite, then n is not even and $n \leq 2$.

    (d) For any integer n, if n is not composite, then n is even and $n \leq 2$.

    (e) For any integer n, if n is not composite, then n is not even and $n \leq 2$.

    (f) There exists an integer n such that if n is composite, then n is not even and $n \leq 2$.

    (g) There exists an integer n such that n is composite and n is not even and $n \leq 2$.

    (h) There exists an integer n such that if n is not composite, then n is not even and $n \leq 2$.

    (i) There exists an integer n such that n is composite and n is even and $n \leq 2$.

    (j) There exists an integer n such that if n is not composite, then n is not even or $n \leq 2$.

10. Let T be the statement

$$\forall \text{ real numbers } x, \text{ if } -1 < x \leq 0 \text{ then } x + 1 > 0.$$

    (a) Write the converse of T.

(b) Write the contrapositive of T.

11. Rewrite the following statement in if-then form without using the word "only": A graph with n vertices is a tree only if it has $n - 1$ edges.

12. Are the following two statements logically equivalent? Justify your answer.

   (a) A real number is less than 1 only if its reciprocal is greater than 1.

   (b) Having a reciprocal greater than 1 is a sufficient condition for a real number to be less than 1.

13. For each of the following statements, (1) write the statement informally without using variables or the symbols $\forall$ or $\exists$, and (2) indicate whether the statement is true or false and briefly justify your answer.

   (a) $\forall$ integers a, $\exists$ an integer b such that $a + b = 0$.

   (b) $\exists$ an integer a such that $\forall$ integers b, $a + b = 0$.

14. For each of the following statements, (1) write the statement informally without using variables or the symbols $\forall$ or $\exists$, and (2) indicate whether the statement is true or false and briefly justify your answer.

   (a) $\forall$ real numbers x, $\exists$ a real number y such that $x < y$.

   (b) $\exists$ a real number y such that $\forall$ real numbers x, $x < y$.

15. Is the following argument valid or invalid? Justify your answer.

> All real numbers have nonnegative squares.
> The number i has a negative square.
> Therefore, the number i is not a real number.

16. Is the following argument valid or invalid? Justify your answer.

> All prime numbers greater than 2 are odd.
> The number a is not prime.
> Therefore, the number a is not odd.

Chapter 3

1. State precisely (but concisely) what it means for an integer n to be odd.

2. Find a counterexample to show that the following statement is false:

$$\text{For all nonzero real numbers } a, \ b, \ c \text{ and } d, \ \frac{a}{b} + \frac{c}{d} = \frac{a + c}{b + d}.$$

3. Consider the following statement:

> Statement A: $\forall$ integers m and n, if $2m + n$ is odd then m and n are both odd.

   (a) Write a negation for Statement A.

(b) Disprove Statement A. That is, show that Statement A is false.

4. If m and n are integers, is $6m^2 + 34n - 18$ an even integer? Justify your answer.

5. Show that the following statement is false: The product of any two irrational numbers is irrational.

6. State precisely (but concisely) what it means for a number r to be rational.

7. Is 605.83 a rational number? Justify your answer.

8. Is 56.745 a rational number? Justify your answer.

9. State precisely (but concisely) what it means for an integer n to be divisible by an integer d.

10. Is 0 divisible by 3? Justify your answer.

11. Does 12 divide 72? Justify your answer.

12. Outline a proof of the following statement by writing the "starting point" and the "conclusion to be shown" in a proof of the statement.

$$\forall \text{ real numbers } r \text{ and } s, \text{ if } r \text{ and } s \text{ are rational then } r - s \text{ is rational.}$$

That is, complete the sentences below.

Proof: Suppose _____.

We must show that _____.

13. Prove the following statement directly from the definitions of the terms. Do not use any other facts previously proved in class or in the text or in the exercises.

$$\text{For all rational numbers } r, \text{ and } s, \text{ if } s \neq 0, \text{ then } \frac{2r}{5s} \text{ is a rational number.}$$

14. Prove the following statement directly from the definitions of the terms. Do not use any other facts previously proved in class or in the text or in the exercises.

$$\text{For all integers } a, b, \text{ and } c, \text{ if } a \mid b \text{ and } a \mid c, \text{ then } a \mid (5b + 3c).$$

15. Use the definition of divisibility to prove: For all integers a, and b, if a divides b then a^3 divides b^3.

16. Prove the statement below directly from the definitions of the terms. Do not use any other facts previously proved in class or in the text or in the exercises.

$$\text{For all integers } n, \ n^2 + n + 1 \text{ is odd.}$$

17. Prove the following statement: The sum of any two consecutive integers can be written in the form $4n + 1$ for some integer n.

18. Prove the following statement: For all real numbers x, $\lfloor x - 2 \rfloor = \lfloor x \rfloor - 2$.

19. Prove the following statement: There is no smallest positive rational number.

20. Prove the following statement by contradiction: For all real numbers r and s, if r is rational and s is irrational, then $r + 2s$ is irrational.

21. Consider the following statement: For all integers n, if n^3 is even then n is even.

   (a) Prove the statement either by contradiction or by contraposition. Clearly indicate which method you are using.

   (b) If you used proof by contradiction in part (a), write what you would "suppose" and what you would "show" to prove the statement by contraposition. If you used proof by contraposition. in part (a), write what you would "suppose" and what you would "show" to prove the statement by contradiction.

22. Consider the following statement: For all real numbers r, if r^3 is irrational then r is irrational.

   (a) Prove the statement either by contradiction or by contraposition. Clearly indicate which method you are using.

   (b) If you used proof by contradiction in part (a), write what you would "suppose" and what you would "show" to prove the statement by contraposition. If you used proof by contraposition in part (a), write what you would "suppose" and what you would "show" to prove the statement by contradiction.

23. Consider the following statement: For all integers n, if n^3 is odd then n is odd.

   (a) Prove the statement either by contradiction or by contraposition. Clearly indicate which method you are using.

   (b) If you used proof by contradiction in part (a), write what you would "suppose" and what you would "show" to prove the statement by contraposition. If you used proof by contraposition in part (a), write what you would "suppose" and what you would "show" to prove the statement by contradiction.

24. True or false? For any irrational number r, r^2 is irrational. Justify your answer.

25. Fill in the blanks of the following proof by contradiction that $7 + 4\sqrt{2}$ is an irrational number. (You may use the fact that $\sqrt{2}$ is irrational.)

    Proof: Suppose not. Suppose that $7 + 4\sqrt{2}$ is _____. By definition of rational, $7 + 4\sqrt{2} = \dfrac{a}{b}$, where_____. Multiplying both sides by b gives

    $$7b + 4b\sqrt{2} = a,$$

    so if we subtract $7b$ from both sides we have

    $$4b\sqrt{2} = \underline{\hspace{1cm}}.$$

    Dividing both sides by $4b$ gives
    $$\sqrt{2} = \underline{\hspace{1cm}}.$$

    But then $\sqrt{2}$ would be a rational number because _____. This contradicts our knowledge that $\sqrt{2}$ is irrational. Hence _____.

26. Prove by contradiction that $4 + 3\sqrt{2}$ is an irrational number. (You may use the fact that $\sqrt{2}$ is irrational.)

27. Use the Euclidean algorithm to find the greatest common divisor of 284 and 168. Show your work.

28. Use the Euclidean algorithm to calculate the greatest common divisor of 10,673 and 11,284. Show your work.

Chapter 4

1. Compute $\sum_{k=0}^{3} \frac{1}{2^k}$.

2. Compute $\sum_{k=1}^{4} k^2$.

3. Use summation notation to rewrite the following: $1^3 - 2^3 + 3^3 - 4^3 + 5^3$.

4. Use a summation symbol to rewrite the following: $1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \frac{1}{5} - \frac{1}{6}$

5. Transform the following summation by making the change of variable $j = k + 1$:

$$\sum_{k=1}^{n} \frac{k^2}{n}.$$

6. Transform the following summation by making the change of variable $i = k + 1$:

$$\sum_{k=0}^{n} \frac{k^2}{k + n}.$$

7. Use repeated division by 2 to find the binary representation of the number 103_2. Show your work.

8. Use the formula
$$1 + r + r^2 + \cdots + r^n = \frac{r^{n+1} - 1}{r - 1}$$

(for all real numbers $r \neq 1$ and for all integers $n \geq 0$) to find

$$2 + 2^2 + 2^3 + \cdots + 2^m$$

where m is an integer that is at least 1.

9. For each integer $n \geq 3$, let $P(n)$ be the equation

$$3 + 4 + 5 + \cdots + n = \frac{(n - 2)(n + 3)}{2}.$$

(Recall that by definition $3 + 4 + 5 + \cdots + n = \sum_{i=3}^{n} i$.)

   (a) Is the equation true for $n = 3$? Justify your answer.

   (b) In the inductive step of a proof that this formula is true for all integers $n \geq 3$, we suppose the formula is true when k is substituted in place of n (this is the inductive hypothesis), and then we show that the equation is true when $k + 1$ is substituted in place of n. Fill in the blanks below to write what we suppose and what we must show for this particular formula.

   Proof that for all integers $k \geq 3$,   if the equation is true for $n = k$ then it is true for $n = k + 1$:

   Let k be any integer that is greater than or equal to 3, and suppose that _____.
   We must show that _____.

   (c) Finish the proof started in (b) above.

10. For each integer $n \geq 3$, let $P(n)$ be the equation

$$2 \cdot 3 + 3 \cdot 4 + \cdots + (n-1) \cdot n = \frac{(n-2)(n^2 + 2n + 3)}{3}.$$

(Recall that by definition $2 \cdot 3 + 3 \cdot 4 + \cdots + (n-1) \cdot n = \sum_{i=3}^{n} (i-1) \cdot i.$)

(a) Is the equation true for $n = 3$? Justify your answer.

(b) In the inductive step of a proof that this formula is true for all integers $n \geq 3$, we suppose the formula is true for when k is substituted in place of n (this is the inductive hypothesis), and then we show that the formula is true when $k + 1$ is substituted in place of n. Fill in the blanks below to write what we suppose and what we must show for this particular formula.

Proof that for all integers $k \geq 3$, if the equation is true for $n = k$ then it is true for $n = k + 1$:

Let k be any integer that is greater than or equal to 3, and suppose that _____.
We must show that _____.

(c) Finish the proof started in (b) above.

11. For each integer $n \geq 0$, let $P(n)$ be the equation

$$1 + 3 + 3^2 + \cdots + 3^n = \frac{3^{n+1} - 1}{2}.$$

(Recall that by definition $1 + 3 + 3^2 + \cdots + 3^n = \sum_{i=0}^{n} 3^i.$)

(a) Is the equation true for $n = 0$? Justify your answer.

(b) In the inductive step of a proof that this formula is true for all integers $n \geq 0$, we suppose the formula is true for when k is substituted in place of n (this is the inductive hypothesis), and then we show that the formula is true when $k + 1$ is substituted in place of n. Fill in the blanks below to write what we suppose and what we must show for this particular formula.

Proof that for all integers $k \geq 0$, if the equation is true for $n = k$ then it is true for $n = k + 1$:

Let k be any integer that is greater than or equal to 0, and suppose that _____.
We must show that _____.

(c) Finish the proof started in (b) above.

12. Use mathematical induction to prove that for all integers $n \geq 1$,

$$4 + 8 + 12 + \cdots + 4n = 2n^2 + 2n.$$

13. Use mathematical induction to prove that for all integers $n \geq 3$, $3 + 4 + 5 + \cdots + n = \frac{(n-2)(n+3)}{2}.$

14. Use mathematical induction to prove that for all integers $n \geq 3$, $2 \cdot 3 + 3 \cdot 4 + \cdots + (n-1) \cdot n = \frac{(n-2)(n^2 + 2n + 3)}{3}.$

15. Use mathematical induction to prove that for all integers $n \geq 0$, $1+3+3^2+\cdots+3^n = \dfrac{3^{n+1}-1}{2}$.

16. Use mathematical induction to prove that for all integers $n \geq 0$, $8^n - 1$ is divisible by 7.

17. Use mathematical induction to prove that for all integers $n \geq 5$, $1 + 4n < 2^n$.

18. Use strong mathematical induction to prove that for all integers $n \geq 2$, either n is prime or n is a product of prime numbers.

19. A sequence $a_0, a_1, a_2, \ldots$ is defined recursively as follows:

$$a_0 = 2, \quad a_1 = 9$$
$$a_k = 5a_{k-1} - 6a_{k-2} \quad \text{for all integers } k \geq 2.$$

    Use strong mathematical induction to prove that for all integers $n \geq 0$, $a_n = 5 \cdot 3^n - 3 \cdot 2^n$.

20. A sequence $s_1, s_2, s_3, \ldots$ is defined recursively as follows:

$$
\begin{aligned}
s_k &= 5s_{k-1} + (s_{k-2})^2 \quad \text{for all integers } k \geq 3 \\
s_1 &= 4 \\
s_2 &= 8
\end{aligned}
$$

    Use (strong) mathematical induction to prove that s_n is divisible by 4 for all integers $n \geq 1$.

21. The following **while** loop is annotated with a pre- and post-condition and also a loop invariant. Use the loop invariant theorem to prove the correctness of the loop with respect to the pre- and post-conditions.

    [*Pre-condition: product = A[1] and i = 1*]

    > **while** $(i \neq m)$
    >> 1. $i := i + 1$
    >> 2. $product := product A \cdot [i]$
    >
    > **end while**

    [*Post-condition: product = $A[1] \cdot A[2] \cdots A[m]$*]

    loop invariant: $I(n)$ is "$i = n + 1$ and $product := A[1] \cdot A[2] \cdots A[n+1]$"

Chapter 5

1. Let A and B be sets. Define precisely (but concisely) what it means for A to be a subset of B.

2. Write a negation for the following statement:

    $$\text{For all } x, \text{ if } x \in A \cap B \text{ then } x \in B.$$

3. Fill in the blanks in the following sentence: If A, B and C are any sets, then by definition of set difference $x \in A - (B \cap C)$ if, and only if, x _____ and x _____.

4.

    (a) Is $2 \subseteq \{2, 4, 6\}$?

    (b) Is $\{3\} \in \{1, 3, 5\}$?

5. If $X = \{u, v\}$, what is the power set of X?

6. Fill in the blanks:

    (a) Given sets A and B, to prove that $(A - B) \cup (A \cap B) \subseteq A$, we suppose that $x \in$ _____ and we must show that $x \in$ _____.

    (b) By definition of union, to say that $x \in (A - B) \cup (A \cap B)$ means that _____.

7. Define sets A and B as follows: $A = \{n \in \mathbf{Z} \mid n = 8r - 3 \text{ for some integer } r\}$ and $B = \{m \in \mathbf{Z} \mid m = 4s + 1 \text{ for some integer } s\}$.

    (a) Is $A \subseteq B$?

    (b) Is $B \subseteq A$?

Justify your answers carefully. (In other words, provide a proof if the statement is true or a disproof if the statement is false.)

8. Let $X = \{l \in Z \mid l = 5a + 2 \text{ for some integer } a\}$, $Y = \{m \in Z \mid m = 4b + 3 \text{ for some integer } b\}$, and $Z = \{n \in Z \mid n = 4c - 1 \text{ for some integer } c\}$.

    (a) Is $X \subseteq Y$?

    (b) Is $Y \subseteq Z$?

Justify your answers carefully. (In other words, provide a proof if the statement is true or a disproof if the statement is false.)

9. The following is an outline of a proof that $(A \cup B)^c \subseteq A^c \cap B^c$. Fill in the blanks.

Proof: Given sets A and B, to prove that $(A \cup B)^c \subseteq A^c \cap B^c$, we suppose $x \in$ __(a)__ and then we show that $x \in$ __(b)__. So suppose that __(c)__. Then by definition of complement, __(d)__. So by definition of union, it is not the case that (x is in A or x is in B). Consequently, x is not in A __(e)__ x is not in B because of De Morgan's law of logic. In symbols, this says that $x \notin A$ and $x \notin B$. So by definition of complement, $x \in$ __(f)__ and $x \in$ __(g)__. Thus, by definition of intersection, $x \in$ __(h)__. *[as was to be shown]*.

10. Prove the following statement using an element argument and reasoning directly from the definitions of union, intersection, set difference.

$$\text{For all sets } A, B, \text{ and } C, (A \cup B) \cap C \subseteq A \cup (B \cap C).$$

11. Disprove the following statement by finding a counterexample.

$$\text{For all sets } A, B, \text{ and } C, A \cup (B \cap C) \subseteq (A \cup B) \cap C.$$

12. Consider the statement

$$\text{For all sets } A \text{ and } B, (A - B) \cap B = \emptyset.$$

The proof below is the beginning of a proof using the element method for prove that a set equals the empty set. Complete the proof without using any of the set properties from Theorem 5.2.2.

Proof: Suppose the given statement is false. Then there exist sets A and B such that $(A - B) \cap B \neq \emptyset$. Thus there is an element x in $(A - B) \cap B$. By definition of intersection,....

13. Consider the statement

$$\text{For all sets } A \text{ and } B, (A - B) \cap B = \emptyset.$$

Complete the proof begun below in which the given statement is derived algebraically from the properties on the attached sheet. Be sure to give a reason for every step that exactly justifies what was done in the step:

Proof:

Let A and B be any sets. Then the left-hand side of the equation to be shown is

$$(A - B) \cap B \quad = \quad (A \cap B^c) \cap B \quad \text{by the _____ law}$$

$$= \quad \text{_____} \qquad \qquad \text{by the _____ law}$$

$$= \quad \text{_____} \qquad \qquad \text{by the _____ law}$$

$$= \quad \text{_____} \qquad \qquad \text{by the _____ law}$$

$$= \quad \text{\_\_\_\_\_} \qquad \qquad \text{by the _____ law}$$

which is the right-hand side of the equation to be shown. *[Hence the given statement is true.]*

(The number of lines in the outline shown above are just meant to be suggestive. To complete the proof you may need more lines or you may be able to do it with fewer lines. Use however many lines as you need.)

14.

   (a) Prove the following statement using the element method for prove that a set equals the empty set: For all sets A and B, $A \cap (B - A) = \emptyset$.

   (b) Use the properties in Theorem 5.2.2 to prove the statement in part (a). Be sure to give a reason for every step.

15. Derive the following result "algebraically" using the properties listed in Theorem 5.2.2 (and reproduced on the attached sheet). Give a reason for every step.

   For all sets A, B, and C, $(A \cup C) - B = (A - B) \cup (C - B)$.

16. Derive the following result. You may do so either "algebraically" using the properties listed in Theorem 5.2.2, being sure to give a reason for every step, or you may use the element method for proving a set equals the empty set.

   For all sets B and C, $(B - C) - B = \emptyset$.

17. Use the element method for proving a set equals the empty set to prove that

   For all sets A and C, $(A - C) \cap (C - A) = \emptyset$.

18. Is the following sentence a statement: This sentence is false or $-2^2 = 4$. Justify your answer.

Chapter 6

1. On each of three consecutive days the National Weather Service announces that there is a 50-50 chance of rain. Assuming that the National Weather Service is correct, what is the probability that it rains on at most one of the three days? Justify your answer. (*Hint*: Represent the outcome that it rains on day 1 and doesn't rain on days 2 and 3 as RNN.)

2. How many elements are in the one-dimensional array shown below?

$$A[7], \ A[8], \ \dots \ , \ A\left[\left\lfloor \frac{145}{2} \right\rfloor\right]$$

3. In a certain state, license plates each consist of 2 letters followed by 3 digits.

   (a) How many different license plates are there?

   (b) How many different license plates are there that have no repeated letters or digits?

4. In a certain state, license plates each consist of 2 letters followed by either 3 or 4 digits. How many different license plates are there that have no repeated letters or digits?

5. Suppose there are three routes from Byrne Hall to McGaw Hall and five routes from McGaw Hall to Monroe Hall. How many ways is it possible to travel from Byrne Hall to Monroe Hall by way of McGaw Hall?

6. In a certain discrete math class, three quizzes were given. Out of the 30 students in the class:

   > 15 scored 12 or above on quiz #1,
   > 12 scored 12 or above on quiz #2,
   > 18 scored 12 or above on quiz #3,
   > 7 scored 12 or above on quizzes #1 and #2,
   > 11 scored 12 or above on quizzes #1 and #3,
   > 8 scored 12 or above on quizzes #2 and #3,
   > 4 scored 12 or above on quizzes #1, #2, and #3.

   (a) How many scored 12 or above on at least one quiz?

   (b) How many scored 12 or above on quizzes 1 and 2 but not 3?

7. A club has seven members. Three are to be chosen to go as a group to a national meeting.

   (a) How many distinct groups of three can be chosen?

   (b) If the club contains four men and three women, how many distinct groups of three contain two men and one woman?

   (c) If the club contains four men and three women, how many distinct groups of three contain at most two men?

   (d) If the club contains four men and three women, how many distinct groups of three contain at least one woman?

   (e) If the club contains four men and three women, what is the probability that a distinct group of three will contain at least one woman?

   (f) If two members of the club refuse to travel together as part of the group (but each is willing to go if the other does not), how many distinct groups of three can be chosen?

   (g) If two members of the club insists on either traveling together or not going at all, How many distinct groups of three can be chosen?

8. Suppose that a fair coin is tossed ten times.

   (a) How many ways can at least eight heads be obtained?

   (b) What is the probability of obtaining at least eight heads?

9. A large pile of coins consists of pennies, nickels, dimes, and quarters (at least 20 of each).

   (a) How many different collections of 20 coins can be chosen?

   (b) How many different collections of 20 coins chosen at random will contain at least 3 coins of each type?

   (c) What is the probability that a collection of 20 coins chosen at random will contain at least 3 coins of each type?

10. Prove for all integers n, k, and r with $n \geq k \geq r$ that $\binom{n}{k}\binom{k}{r} = \binom{n}{r}\binom{n-r}{k-r}$.

11. The binomial theorem states that for any real numbers a and b,

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k \quad \text{for any integer } n \geq 0.$$

Use this theorem to compute $(2x-1)^5$.

12. The binomial theorem states that for any real numbers a and b,

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k \quad \text{for any integer } n \geq 0.$$

Use this theorem to show that for any integer $n \geq 0$, $\sum_{k=0}^{n}(-1)^k \binom{n}{k} 3^{n-k} 2^k = 1$.

13. Express the following sum in closed form (without using a summation symbol and without using an ellipsis ...): $\sum_{k=0}^{n} \binom{n}{k} 7^k$.

14. Let A, B, and C be events in a sample space S such that $S = A \cup B \cup C$. Suppose that $P(A) = 0.3$, $P(B) = 0.6$, and $P(A \cap B) = 0.2$. Find each of the following.

   (a) $P(A \cup B)$

   (b) $P(C)$

   (c) $P(A^c \cup B^c)$

15. An urn contains four balls numbered 1, 3, 4, and 6. If a person selects a set of two balls at random, what is the expected value of the product of the numbers on the balls?

16. Suppose A and B are events in a sample space S, and $P(A|B) = 1/2$ and $P(B) = 1/3$. What is $P(A \cap B)$?

17. A teacher offers ten possible assignments for extra credit in a course but requires students to choose them, without looking, from a hat. Six assignments involve library research and four are computer programming exercises. Suppose that a student chooses two assignments, one after the other, at random without replacement.

   (a) What is the probability that both assignments are computer programming exercises?

   (b) What is the probability that at least one of the assignments is a computer programming exercise?

18. A screening test for a certain disease is used in a large population of people of whom 1 in 1000 actually have the disease. Suppose that the false positive rate is 1% and the false negative rate is 0.5%. Thus a person who has the disease tests positive for it 99.5% of the time, and a person who does not have the disease tests negative for it 99% of the time.

   (a) What is the probability that a randomly chosen person who tests positive for the disease actually has the disease?

   (b) What is the probability that a randomly chosen person who tests negative for the disease actually has the disease?

19. A coin is loaded so that the probability of heads is 0.55 and the probability of tails is 0.45. Suppose the coin is tossed twice and the results of the tosses are independent.

   (a) What is the probability of obtaining exactly two heads?

(b) What is the probability of obtaining exactly one head?

(c) What is the probability of obtaining no heads?

(d) What is the probability of obtaining at least one head?

Chapter 7

1. Let $X = \{a, b, c\}$ and $Y = \{u, v\}$. Which of the following arrow diagrams define functions from X to Y?
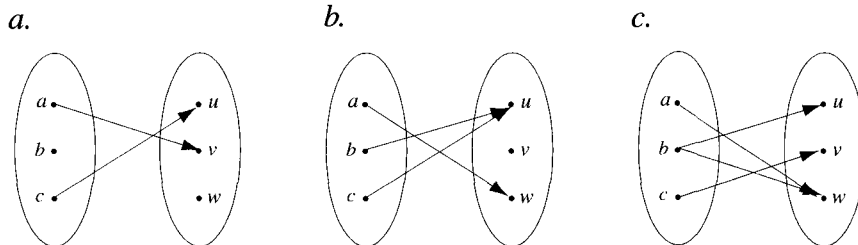
2. $\log_3(\frac{1}{9}) = $ ____ because _____.

3. Is $\log_2 5 = \log_{16} 625$? Why or why not?

4. Define precisely (but concisely) what it means for a function f to be one-to-one.

5. Let f be a function from a set X to a set Y. Define precisely (but concisely) what it means for f to be onto.

6. Let $A = B = \{1, 2, 3\}$, and consider the function $f\colon A \to B$ defined as follows: $f(1) = 3$, $f(2) = 1$, $f(3) = 3$. Is f onto? Why or why not?

7.

(a) Draw an arrow diagram for a function that is onto but not one-to-one.

(b) Define a function $f\colon \mathbf{R}-\{0\} \longrightarrow \mathbf{R}$ by the formula $f(x) = \dfrac{x + 3}{x}$ for all nonzero real numbers x. Prove that f is one-to-one.

8. Let S be the set of all strings in 0's and 1's, and define a function $g\colon S \longrightarrow \mathbf{Z}$ as follows: for each string s in S,

$$g(s) = \text{the number of 1's in } s \text{ minus the number of 0's in } s.$$

(a) What is $g(101011)$? $g(00100)$?

(b) Is g one-to-one? Prove or give a counterexample.

(c) Is g onto? Prove or give a counterexample.

9. Let S be the set of all strings in 0's and 1's, and define a function $g\colon S \longrightarrow \mathbf{Z}$ as follows: for each string s in S,

$$g(s) = \text{the number of 0's in } s.$$

(a) What is $g(101011)$? $g(00100)$?

(b) Is g one-to-one? Prove or give a counterexample.

(c) Is g onto? Prove or give a counterexample.

10. Let S be the set of all strings in 0's and 1's, and define a function
$F : S \rightarrow \mathbf{Z}^{nonneg}$ as follows: for all strings s in S,

$$F(s) = \text{the number of 1's in } s.$$

(a) What is $F(001000)$? $F(111001)$? $F(10101)$? $F(0100)$?

(b) Is F one-to-one? Prove or give a counterexample.

(c) Is F onto? Prove or give a counterexample.

(d) Is F a one-to-one correspondence? If so, find F^{-1}.

11. Let S be the set of all nonzero real numbers. Define a function g from S to S by the formula
$g(x) = \dfrac{1}{x}$, for all nonzero real numbers x.

(a) Show that g is a one-to-one correspondence from S to S.

(b) Find g^{-1}.

12. Let S be the set of all even integers, and define a function $f\colon \mathbf{Z} \longrightarrow \mathbf{S}$ as follows:

$$f(n) = 2n \qquad \text{for all integers } n.$$

(a) Prove that f is one-to-one and onto

(b) Find a formula for the inverse function f^{-1}.

(c) Does the set of all even integers have the same cardinality as the set of all integers? Why or why not?

13. Define a function $f\colon \mathbf{R} \longrightarrow \mathbf{R}$ as follows: for all real numbers x,

$$f(x) = 16x - 5.$$

Then f is both one-to-one and onto. Find the inverse function f^{-1}.

14. If five integers are chosen from the set $\{1, 2, 3, 4, 5, 6, 7, 8\}$, must there be at least two integers with the property that the larger minus the smaller is 2? Explain your answer clearly.

15. Given any set of 30 integers, must there be two that have the same remainder when they are divided by 25? Explain your answer clearly.

16. Given any set of 15 integers, must there be two that have the same remainder when divided by 12? Explain your answer clearly.

17. Let T be the set $\{3, 4, 5, 6, 7, 8, 9, 10\}$ and suppose five integers are chosen from T. Must two of these integers have the property that the difference of the larger minus the smaller equals 2? Why or why not? Explain clearly. (You will not receive credit for this problem unless you explain your reasoning clearly. Try to write an answer that would convince a good but skeptical student who missed the last few weeks of this class.)

18. If six integers are chosen from the set $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, must there be at least two integers with the property that the sum of the smaller plus the larger is 11? Why or why not? Explain clearly. (You will not receive credit for this problem unless you explain your reasoning clearly. Try to write an answer that would convince a good but skeptical student who missed the last few weeks of this class.)

19. Prove that if $f\colon X \to Y$ and $g\colon Y \to Z$ are one-to-one, then $g \circ f\colon X \to Z$ is also one-to-one.

20. Prove that if $f\colon X \to Y$ and $g\colon Y \to Z$ are onto, then $g \circ f\colon X \to Z$ is also onto.

21. Is the set of all squares of positive integers countable? That is, is the set $S = \{m \in \mathbf{Z} \mid m = k^2$ for some positive integer $k\}$ a countable set. Justify your answer.

22. Prove that the set of all integers and the set of all odd integers have the same cardinality.

Chapter 8

1. In a *Double Tower of Hanoi with Adjacency Requirement* there are three poles in a row and $2n$ disks, two of each of n different sizes, where n is any positive integer. Initially pole A (at one end of the row) contains all the disks, placed on top of each other in *pairs* of decreasing size. Disks may only be transferred one-by-one from one pole to an *adjacent* pole and at no time may a larger disk be placed on top of a smaller one. However a disk may be placed on top of another one of the same size. Let C be the pole at the other end of the row and let

$$s_n = \left[\begin{array}{l} \text{the minimum number of moves} \\ \text{needed to transfer a tower of } 2n \\ \text{disks from pole } A \text{ to pole } C \end{array} \right].$$

(a) Find s_1 and s_2.

(b) Find a recurrence relation expressing s_k in terms of s_{k-1} for all integers $k \geq 2$. Justify your answer carefully.

2. In a *Triple Tower of Hanoi*, there are three poles in a row and $3n$ disks, *three* of each of n different sizes, where n is any positive integer. Initially, one of the poles contains all the disks placed on top of each other in triples of decreasing size. Disks are transferred one by one from one pole to another, but at no time may a larger disk be placed on top of a smaller disk. However, a disk may be placed on top of one of the same size. Let t_n be the minimum number of moves needed to transfer a tower of $3n$ disks from one pole to another. Find a recurrence relation for $t_1, t_2, t_3, \ldots$. Justify your answer carefully.

3. A single pair of rabbits (male and female) is born at the beginning of a year. Assume the following conditions: (a) Rabbit pairs are not fertile during their first *two* months of life, but thereafter they give birth to *four* new male/female pairs at the end of every month; (b) No deaths occur. Let s_n = the number of pairs of rabbits alive at the end of month n, for each integer $n \geq 1$, and let $s_0 = 1$. Find a recurrence relation for $s_0, s_1, s_2, \ldots$. Justify your answer carefully.

4. Suppose a certain amount of money is deposited into an account paying 4% annual interest, compounded quarterly. For each positive integer n, let S_n = the amount on deposit at the end of the nth quarter, and let S_0 be the initial amount deposited.

(a) Find a recurrence relation for $S_0, S_1, S_2, \ldots$, assuming no additional deposits or withdrawals for a 4-year period.

(b) If $S_0 = \$5000$, find the amount of money on deposit at the end of 4 years.

(c) Find the APR for the account.

5. Consider the set S of all strings of a's and b's. For each integer $n \geq 0$, let

$$\boxed{a_n = \text{the number of strings of length n that do not contain the pattern } bb.}$$

Find a recurrence relation for $a_1, a_2, a_3, \ldots$. Explain your answer carefully.

6. A sequence $a_1, a_2, a_3, \ldots$ is defined as follows:

$$a_1 = 3, \qquad \text{and} \qquad a_k = 4a_{k-1} + 2 \quad \text{for all integers } k \geq 2.$$

(a) Find $a_1, a_2,$ and a_3.

(b) Supposing that $a_5 = 4^4 \cdot 3 + 4^3 \cdot 2 + 4^2 \cdot 2 + 4 \cdot 2 + 2$, find a similar numerical expression for a_6 by substituting the right-hand side of this equation in place of a_5 in the equation

$$a_6 = 4 \cdot a_5 + 2.$$

(c) Guess an explicit formula for a_n.

7. A sequence $c_0, c_1, c_2, \ldots$ is defined as follows:

$$c_0 = 1 \qquad \text{and} \qquad c_k = 7c_{k-1} + 2 \quad \text{for each integer } k \geq 1.$$

(a) Find c_1 and c_2.

(b) Use one of the reference formulas given at the end of this exam to simplify the expression

$$7^n + 2 \cdot 7^{n-1} + \cdots + 2 \cdot 7^2 + 2 \cdot 7 + 2.$$

(c) Use iteration to guess an explicit formula for the sequence $c_0, c_1, c_2, \ldots$.

8. Use iteration to find an explicit formula for the sequence $b_0, b_1, b_2, \ldots$ defined recursively as follows:
$$\begin{aligned} b_k &= 2b_{k-1} + 3 \quad \text{for all integers } k \geq 1 \\ b_0 &= 1. \end{aligned}$$

If appropriate, simplify your answer using one of the following reference formulas:

(a) $1 + 2 + 3 + \cdots + n = \dfrac{n(n+1)}{2}$ for all integers $n \geq 1$.

(b) $1 + r + r^2 + \cdots + r^m = \dfrac{r^{m+1} - 1}{r - 1}$ for all integers $m \geq 0$ and all real numbers $r \neq 1$.

9. A sequence is defined recursively as follows:

$$a_0 = 2 \qquad \text{and} \qquad a_k = 4a_{k-1} + 1 \quad \text{for all } k \geq 1.$$

It is proposed that an explicit formula for this sequence is

$$a_n = \frac{7 \cdot 4^n - 1}{3}.$$

Use mathematical induction to check whether this proposed formula is correct.

10. A sequence is defined recursively as follows:

$$\begin{aligned} s_k &= 5s_{k-1} + 1 \quad \text{for all integers } k \geq 1 \\ s_0 &= 1. \end{aligned}$$

Use mathematical induction to verify that this sequence satisfies the explicit formula

$$s_n = \frac{5^{n+1} - 1}{4} \qquad \text{for all integers } n \geq 0.$$

11. A sequence $a_0, a_1, a_2, \ldots$ satisfies the recurrence relation $a_k = 4a_{k-1} - 3a_{k-2}$ with initial conditions $a_0 = 1$ and $a_1 = 2$. Find an explicit formula for the sequence.

12. A sequence $b_1, b_2, b_3, \ldots$ satisfies the recurrence relation $b_k = 2b_{k-1} + 8b_{k-2}$ with initial conditions $b_1 = 1$ and $b_2 = 0$. Find an explicit formula for the sequence.

13. A sequence $c_0, c_1, c_2, \ldots$ satisfies the recurrence relation $c_k = 6c_{k-1} - 9c_{k-2}$ with initial conditions $c_0 = 1$ and $c_1 = 6$. Find an explicit formula for the sequence.

14. A sequence $d_1, d_2, d_3, \ldots$ satisfies the recurrence relation $d_k = 8d_{k-1} - 16d_{k-2}$ with initial conditions $d_1 = 0$ and $d_2 = 1$. Find an explicit formula for the sequence.

15. Define a set S recursively as follows:

    I. BASIS: $11 \in S$

    II. RECURSION:

    a. If $s \in S$, then $0s \in S$ and $s0 \in S$

    b. If x is any string (including the null string) such that $1x1 \in S$, then $10x1 \in S$ and $1x01 \in S$

    III. RESTRICTION: No strings other than those derived from I and II are in S.

    a. Is $00100010 \in S$?   b. Is $011011 \in S$?

16. Define a set S recursively as follows:

    I. BASIS: $\epsilon \in S$

    II. RECURSION: If s and t are in S, then

    a. $0s \in S$ b. $s0 \in S$ c. $1s1t \in S$ d. $s1t1 \in S$

    III. RESTRICTION: No strings other than those derived from I and II are in S.

    Use structural induction to prove that every string in S contains an even number of 1's.

17. Use the recursive definition of summation together with mathematical induction to prove that for all positive integers n, if $a_1, a_2, \ldots, a_n$ and $b_1, b_2, \ldots, b_n$ are real numbers, then

$$\sum_{k=1}^{n}(2a_k - 3b_k) = 2\sum_{k=1}^{n} a_k - 3\sum_{k=1}^{n} b_k.$$

Chapter 9

1. Draw a careful graph of the function f defined by the formula $f(n) = \left\lfloor \dfrac{n}{3} \right\rfloor$ for all integers n.

2. Let h be the function whose graph is shown below. Carefully sketch the graph of $2h$.
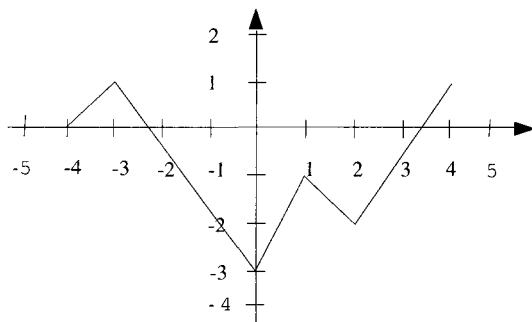
3. If x is a real number and $x > 1$, is $x^2 > x$? Why? Is $5x^3 > 5$? Why?

4. Consider the statement:

$$3\left|x^2\right| \le \left|3x^2 + 17x + 5\right| \qquad \text{for all } x > 1.$$

Express this statement using Ω-notation.

5. Consider the statement:

$$\left|3x^2 + 17x + 5\right| \le 25\left|x^2\right| \qquad \text{for all } x > 1.$$

Express this statement using O-notation.

6. Consider the statement:

$$3\left|x^2\right| \le \left|3x^2 + 17x + 5\right| \le 25\left|x^2\right| \qquad \text{for all } x > 1.$$

Express this statement using Θ-notation.

7. Express the following statement using Ω-notation.:

$$\left|x^5\right| \le \left|\frac{12x^5(3x+4)}{x+2}\right| \qquad \text{for all real numbers } x > 2.$$

8. Express the following statement using O-notation:

$$\left|\frac{12x^5(3x+4)}{x+2}\right| \le 36\left|x^5\right| \qquad \text{for all real numbers } x > 2.$$

9. Express the following statement using Θ-notation:

$$\left|x^5\right| \le \left|\frac{12x^5(3x+4)}{x+2}\right| \le 36\left|x^5\right| \qquad \text{for all real numbers } x > 2.$$

10. Use the definition of O-notation to prove that $2x^2 + 3x + 4$ is $O(x^2)$. (Do not use the theorem on polynomial orders.)

11. Use the definition of O-notation to prove that $15x^3 + 8x + 4$ is $O(x^3)$.(Do not use the theorem on polynomial orders.)

12. Explain why the following statement is true. (You may use the theorem on polynomial orders.)

$$3 + 6 + 9 + \cdots + 3n \text{ is } O(n^2).$$

13. Use the *definition* of O-notation to show that $5x^3 + 3x^2 + 4$ is $O(x^3)$. Be sure to justify each step of your answer.

   (a) Find the total number of additions and multiplications that must be performed when the following algorithm is executed. Show your work carefully.

   for $i := 1$ **to** n
       for $j = i$ **to** n
           $a := 2 \cdot (5 \cdot i + j + 1)$
       next j
   next i

   (b) Find an order for the algorithm segment of part (a) from among the following: $\log_2 n$, n, $n \cdot \log_2 n$, n^2, n^3, and n^4. Give a reason for your answer.

14.

(a) Consider the following algorithm segment:

  for $i := 1$ **to** n
    for $j := 1$ **to** i
      $x := 5 \cdot i + 8 \cdot j$
    next j
  next i

(b) How many additions and multiplications are performed when the inner loop of this algorithm segment is executed? How many additions and multiplications are performed when the entire algorithm segment is executed?

(c) Find an order for this algorithm segment from among the following: $\log_2 n$, n, $n \cdot \log_2 n$, n^2, n^3, and n^4. Give a reason for your answer.

15. Describe the operation of the sequential search algorithm.

16. Describe the operation of the insertion sort algorithm.

17. Sketch the graph of $y = \log_3 x$.

18. Define a function $F\colon \mathbf{R}^+ \longrightarrow \mathbf{R}$ by the formula $F(x) = \log_2(x)$ for all positive real numbers x.

(a) Graph F, marking units carefully on your axes.

(b) What is $F(\frac{1}{8})$? Why?

(c) Write the equation $2^{20} = 1,048,576$ in logarithmic form.

19. If n and k are positive integers and $2^k \le n < 2^{k+1}$, what is $\lfloor \log_2(n) \rfloor$? Be sure to justify each step of your answer.

20. Use O-notation to express the following statement:

$$\mid 5x + x \log_2 x \mid \le 6 \mid x \log_2 x \mid \ \text{ for all } x > 2.$$

21. Describe the operation of the binary search algorithm.

22. Describe the operation of the merge sort algorithm.

Chapter 10

1. Define a binary relation R from $\{a, b, c\}$ to $\{u, v\}$ as follows: $R = \{(a, v), (b, u), (b, v), (c, u)\}$.

(a) Draw an arrow diagram for R.

(b) Is R a function? Why or why not?

2. Define a binary relation R from $\{a, b, c\}$ to $\{u, v\}$ as follows: $R = \{(a, u), (b, u), (c, v)\}$.

(a) Draw an arrow diagram for R.

(b) Is R a function? Why or why not?

3. Define a binary relation R from $\{a, b, c\}$ to $\{u, v\}$ as follows: $R = \{(a, v), (b, u)\}$.

(a) Draw an arrow diagram for R.

(b) Is R a function? Why or why not?

4. Define a binary relation T from $\mathbf{R}$ to $\mathbf{R}$ as follows: for all $(x, y) \in \mathbf{R} \times \mathbf{R}$, $x \, T \, y \Leftrightarrow y > x + 1$.

   (a) Is $(1, 0) \in T$? Is $(0, 1) \in T$? Is $(-2, 5) \in T$? Is $(-3, -4) \in T$?

   (b) Sketch the graph of T in the Cartesian plane.

5. Let $A = \{0, 1, 2, 3\}$ and define a binary relation R on A as follows:
   $R = \{(0, 2), (0, 3), (2, 0), (2, 1)\}$.

   (a) Draw the directed graph of R.

   (b) Is R reflexive? Explain.

   (c) Is R transitive? Explain.

6. Let $A = \{2, 3, 4, 5, 6, 7, 8\}$ and define a binary relation R on A as follows: for all $x, y \in A$,

   $$x \, R \, y \Leftrightarrow 3 \mid (x - y).$$

   (a) Is $7 \, R \, 2$? Is $7 \, R \, 4$? Is $2 \, R \, 5$? Is $8 \, R \, 8$?

   (b) Draw the directed graph of R.

7. Let $A = \{3, 4, 5, 6, 7\}$ and define a binary relation R on A as follows: for all $x, y \in A$,

   $$x \, R \, y \Leftrightarrow 2 \mid (x - y).$$

   (a) Is $6 \, R \, 3$? Is $4 \, R \, 6$?

   (b) Draw the directed graph of R.

8. Let $B = \{0, 1, 2, 3\}$ and define a binary relation U on B by

   $$U = \{(0, 2), (0, 3), (2, 0), (2, 1)\}.$$

   Is U transitive? Justify your answer.

9. Define a binary relation R on the set $\{1, 2, 3, 4\}$ as follows:

   $$T = \{(1, 4), (2, 3), (2, 4), (4, 1), (2, 1), (1, 2), (3, 2)\}$$

   (a) Is R symmetric? Justify your answer.

   (b) Is R transitive? Justify your answer.

10. Define a binary relation S on the set of all positive integers as follows: for all positive integers m and n,
    $$m \, S \, n \Leftrightarrow m \mid n.$$
    Is S reflexive? Justify your answer.

11. Let $B = \{0, 1, 2, 3\}$ and define a binary relation U on B by

    $$U = \{(0, 2), (0, 3), (1, 2)\}.$$

    Is U transitive? Justify your answer.

12. Let R be the binary relation defined on the set of all integers $\mathbf{Z}$ as follows: for all integers m and n,
    $$m \, R \, n \Longleftrightarrow m - n \text{ is divisible by } 5.$$

    (a) Is R reflexive? Prove or give a counterexample.

    (b) Is R symmetric? Prove or give a counterexample.

(c) Is R transitive? Prove or give a counterexample.

13. Let $A = \{1, 2, 3, 4\}$. The following relation R is an equivalence relation on A:

$$R = \{(1,1),(1,3),(1,4),(2,2),(3,1),(3,3),(3,4),(4,1),(4,3),(4,4)\}.$$

(a) Draw the directed graph of R.

(b) Find the distinct equivalence classes of R.

14. Let S be the set of all strings of 0's and 1's of length 3. Define a binary relation R on S as follows: for all strings s and t in S,

$$s \; R \; t \iff \begin{array}{l} \text{the two left-most characters} \\ \text{of } s \text{ are the same as the two} \\ \text{left-most characters of } t. \end{array}$$

(a) Prove that R is an equivalence relation on S.

(b) Find the distinct equivalence classes of R.

15. Define a binary relation T on $\mathbf{R}$ as follows: for all x and y in , $x \; T \; y$ if and only if $x^2 = y^2$. Then T is an equivalence relation on $\mathbf{R}$.

(a) Prove that T is an equivalence relation on $\mathbf{R}$.

(b) Find the distinct equivalence classes of T.

16. Prove that if a, b, c, d and n are integers, $n > 1$, $a \equiv c \pmod{n}$, and $b \equiv d \pmod{n}$, then $ab \equiv cd \pmod{n}$.

17. Use the fact that $29 = 16 + 8 + 4 + 1$ to compute $18^{29} \bmod 65$.

18. Find a positive inverse for 7 modulo 48. (That is, find a positive integer n such that $7n \equiv 1 \pmod{48}$.)

19. An RSA cipher has public key $pq = 65$ and $e = 7$.

(a) Translate the message YES into its numeric equivalent, and use the formula $C = M^e \pmod{pq}$ to encrypt the message.

(b) Decrypt the ciphertext 50 41 and translate the result into letters of the alphabet to discover the message.

Chapter 11

1. If a graph has vertices of degrees 1, 1, 2, 3, and 3, how many edges does it have? Why?

2. For each of (a)–(c) below, either draw a graph with the specified properties or else explain why no such graph exists.

(a) Graph with six vertices of degrees 1, 1, 2, 2, 2, and 3.

(b) Graph with four vertices of degrees 1, 2, 2, and 5.

(c) Simple graph with five vertices of degrees 1, 1, 1, 1, and 5.

3. Determine whether each of the following graphs has an Euler circuit. If it does have an Euler circuit, find such a circuit. If it does not have an Euler circuit, explain why you can be 100% sure that it does not.
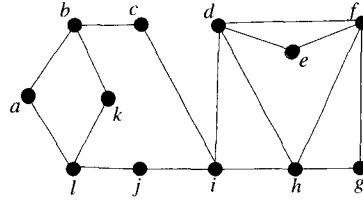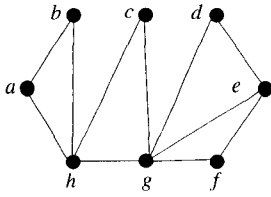
4. Determine whether each of the following graphs has a Hamiltonian circuit. If it does have an Hamiltonian circuit, find such a circuit. If it does not have an Hamiltonian circuit, explain why you can be 100% sure that it does not.
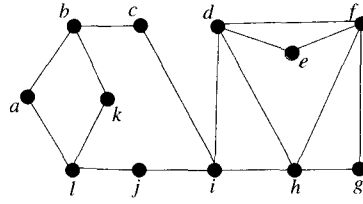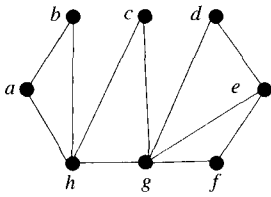
5. Draw a directed graph with the following adjacency matrix:

$$
\begin{array}{c|cccc}
 & v_1 & v_2 & v_3 & v_4 \\
\hline
v_1 & 1 & 2 & 0 & 0 \\
v_2 & 0 & 0 & 0 & 1 \\
v_3 & 2 & 20 & 1 & 0 \\
v_4 & 0 & 1 & 0 & 0
\end{array}
$$

6. Find the following matrix product:

$$
\begin{bmatrix} 2 & 0 \\ 0 & 1 \\ 3 & 2 \end{bmatrix}
\begin{bmatrix} 1 & 3 & 0 \\ 2 & 4 & 2 \end{bmatrix}
$$

7. Consider the adjacency matrix for a graph that is shown below. Answer the following questions by examining the matrix and its powers only, not by drawing the graph. Show your work in a way that makes your reasoning clear.

$$
\begin{array}{c|cccc}
 & v_1 & v_2 & v_3 & v_4 \\
\hline
v_1 & 0 & 1 & 0 & 1 \\
v_2 & 1 & 0 & 2 & 0 \\
v_3 & 0 & 2 & 0 & 0 \\
v_4 & 1 & 0 & 0 & 0
\end{array}
$$

(a) How many walks of length 2 are there from v_1 to v_2?

(b) How many walks of length 2 are there from v_1 to v_3?

(c) How many walks of length 2 are there from v_2 to v_2?

8. Determine whether any two of G_1, G_2, and G_3 are isomorphic. If they are, give vertex and edge functions that define the isomorphism. If they are not, give an isomorphic invariant that they do not share.
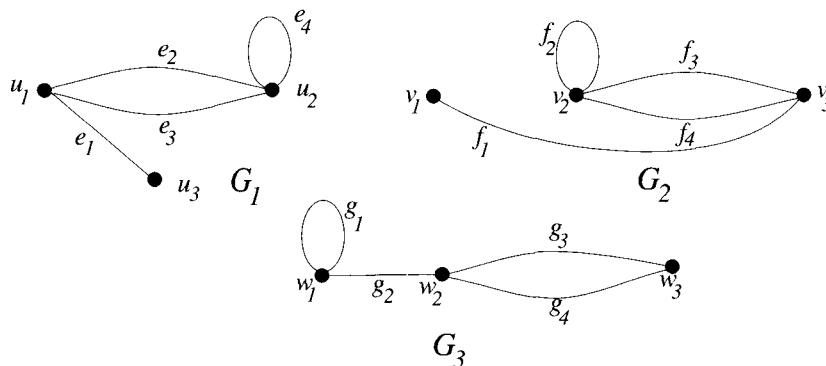
9. Determine whether any two of the simple graphs G_1, G_2, and G_3 are isomorphic. If they are, give a vertex function that defines the isomorphism. If they are not, give an isomorphic invariant that they do not share.
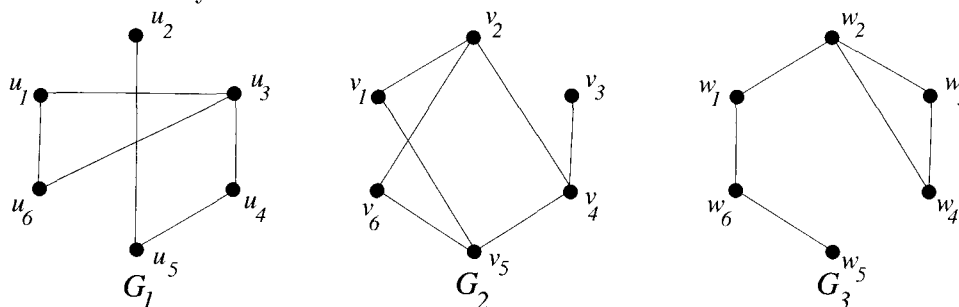
10. Prove that having a vertex of degree 3 is an invariant for graph isomorphism.

11. A certain graph is 19 vertices, 19 edges, and no nontrivial circuits. Is it connected? Explain.

12. A certain connected graph has 68 vertices and 72 edges. Does it have a nontrivial circuit? Explain.

13. Either draw a graph with the given specification or explain why no such graph exists.

   (a) full binary tree with 16 vertices of which 6 are internal vertices
   (b) binary tree, height 3, 9 vertices
   (c) binary tree, height 4, 18 terminal vertices

14. Consider the following weighted graph:
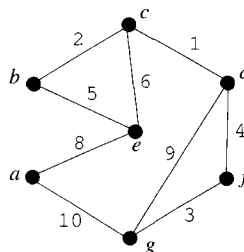
(a) Use Kruskal's algorithm to find a minimum spanning tree for the graph, and indicate the order in which edges are added to form the tree.

(b) Use Prim's algorithm starting with vertex a to find a minimum spanning tree for the graph, and indicate the order in which edges are added to form the tree.

Chapter 12

1. Let $\Sigma = \{0, 1\}$, and let L be the language over Σ consisting of all strings of 0's and 1's of length 4 with an equal number of 0's and 1's. List the elements of L.

2. Let L be the language defined by the regular expression $0(0 \mid 1)^*1(0 \mid 1)^*$.

   (a) Write 3 strings that belong to L

   (b) Use words to describe L.

3. Let L be the language defined by the regular expression $(x \mid y)^*x(x \mid y)$.

   (a) Write 3 strings that belong to L

   (b) Use words to describe L.

4. Consider the language that consists of all strings of a's and b's in which the second character from the beginning is a b. Find a regular expression that defines this language.

5. Consider the language that consists of all strings of 0's and 1's in which the number of 1's is evenly divisible by 4. Find a regular expression that defines this language.

6. Consider the finite-state automaton given by the following transition diagram:
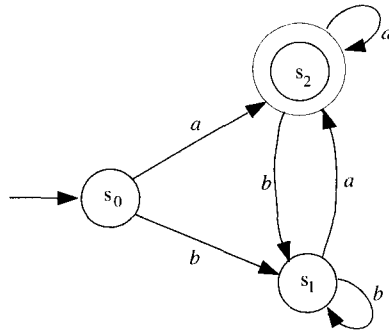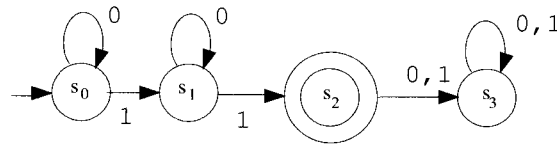

   (a) What is $N(s_2, a)$?

   (b) To what state does the automaton go if the string $babaa$ is input to it?

   (c) Indicate which of the following strings are accepted by the automaton:

$$abab \qquad bbab \qquad abbbaa \qquad a$$

   (d) Describe the language accepted by this automaton.

   (e) Find a regular expression that defines the same language.

7. Consider the finite-state automaton given by the following transition diagram:

(a) To what state does the automaton go if the string 10010010 is input to it? Is this string accepted by the automaton?

(b) Indicate which of the following strings are accepted by the automaton:

$$000101 \qquad 0100010 \qquad 000100 \qquad 110001$$

(c) Describe the language accepted by the automaton.

(d) Find a regular expression that defines the same language.

8. Consider the finite-state automaton given by the following next-state table:

	input a	b
$\rightarrow U_0$	U_2	U_1
U_1	U_3	U_2
U_2	U_2	U_2
$\odot U_3$	U_3	U_3

states

(a) Draw the transition diagram for this automaton.

(b) Indicate which of the following strings are accepted by the automaton:

$$abba \qquad babb \qquad ba \qquad bbababa$$

(c) Describe the language accepted by the automaton.

(d) Find a regular expression that defines the same language.

9. Consider the finite-state automaton given by the following next-state table:

	input symbols 0	1
$\rightarrow s_0$	s_0	s_1
s_1	s_2	s_1
$\odot s_2$	s_0	s_1

states

(a) Draw the transition diagram for this automaton.

(b) Indicate which of the following strings are accepted by the automaton:

$$0100 \qquad 1001 \qquad 0110 \qquad 101010$$

(c) Describe the language accepted by the automaton.

(d) Find a regular expression that defines the same language.

10. Consider the finite-state automaton given by the following next-state table:

input

states		0	1
$\rightarrow s_0$		s_2	s_1
s_1		s_2	s_3
s_2		s_2	s_2
$\circledcirc s_3$		s_3	s_3

(a) Draw the transition diagram for the automaton.

(b) Indicate which of the following strings are accepted by the automaton:

$$0100 \qquad 101 \qquad 1110 \qquad 00101$$

(c) Describe the language accepted by this automaton.

(d) Find a regular expression that defines the same language.

11. Consider the regular expression $0^*10^* \mid 0^*10^*10^*$.

(a) Describe the language defined by this expression.

(b) Design a finite-state automaton to accept the language defined by the expression.

12. Consider the regular expression $a(a \mid b)^*b$.

(a) Describe the language defined by this expression.

(b) Design a finite-state automaton to accept the language defined by the expression.

13. Prove that there is no finite-state automaton that accepts the language L consisting of all strings of x's and y's of the form $x^n y^n$ where n is a positive integer.

14. Finite-state automata A and A' are defined by the transition diagrams shown below.

(a) Find the quotient automaton for A.

(b) Find the quotient automaton for A'.

(c) Are A and A' equivalent? Explain.

Ideas for Projects

1. Look up some of the arguments in Lewis Carroll's *Symbolic Logic*, and analyze them using the techniques discussed in the textbook.

2. Find out about "fuzzy logic." What is its relation to the logic discussed in the textbook? What is fuzzy logic used for?

3. Jerry Loder from the University of New Mexico has created a number of discrete mathematical projects based on historical sources, which are described at www.math.nmsu.edu/hist_projects/. Visit the website and choose one of the projects to explore and write up. (Additional projects by others are being planned.)

4. To help prepare for doing your taxes, your tax advisor asks you to answer the following yes-or-no questions:

   (i) If you report business expenses, are all meals and entertainment expresses properly documented?

   (ii) If you report automobile expenses, do you have written documentation of the business miles claimed?

   Suppose you do report business expenses but you neither have business expenses for meals or entertainment nor do you use an automobile in your business.

   (a) How should you answer the questions?

   (b) Analyze your response to part (a) in light of the discussion about conditional statements in Section 1.2 and universally quantified statements in Section 2.2.

5. In logic the words "valid" and "true" have different meanings. Explain the difference between these words as they are used in logic.

6. Valid forms of argument are closely related to certain kinds of tautologies. Let A be the argument form

$$
\begin{array}{c}
p_1 \\
p_2 \\
\vdots \\
p_n \\
\therefore q
\end{array}
$$

   and let S be the statement form $p_1 \wedge p_1 \wedge \cdots \wedge p_n \to q$. Explain why if A is valid, then S is a tautology, and, conversely, if S is a tautology, then A is valid.

7. Once a Boolean expression has been written in disjunctive normal form, a Karnaugh map can be used to simplify it. Find out how Karnaugh maps work, and write a summary of the method. Include a few examples.

8. The Quine-McCluskey algorithm is another method that can be used to simplify Boolean expressions. Find out how this method works, and compare it to the method that uses Karnaugh maps.

9. Here is a description of the game "Use It Or Lose It": A person is told that they can spend $100, but only on items costing exactly $64, $32, $16, $8, $4, $2, and $1 and they may purchase at most one item at any given price. Any money that is unspent is lost. How should the person allocate the money if they want to spend all of the $100? Suppose instead of $100, the person was allowed to spend $99, $98, $97, and so forth. How should the person allocate the money? Explain the connection between this game and binary notation. Explore whether it is possible to find two different ways for allocating any particular amount of money if the aim is to spend it all.

10. Find out about the game WFF 'N PROOF: The Game of Modern Logic. Work a few of the problems and compare and contrast the approach of the game to the presentation about logic in the textbook.

11. A solution to exercise 59 of Section 3.1 shows that the expression $2^{2^n} + 1$ is not prime when $n = 5$. Write a computer program to test the primality of the number when $n = 6$. Discuss the question of using a computer to determine whether the number is prime for $n > 6$.

12. The winning strategy for the game of Nim involves knowing properties of odd and even integers. Find out about this game, and explain why the winning strategy works.

13. Explore the following questions, and write up your findings: Which integers can be written as a sum of 2 or more consecutive integers? Are there any integers that cannot be expressed in this way?

14. Find out about the Beal conjecture. What is its relation to Fermat's last theorem? How did it come to be conjectured? What is the current status of the conjecture? Report on your findings.

15. Find out about Lagrange's four-square theorem. How is it proved?

16. What is the largest prime number now known? What is a Mersenne prime, and what role do these numbers play in the search for large prime numbers?

17. What is the *Encyclopedia of Integer Sequences*? What are some ways it is used?

18. Exercise 11 in Section 4.5 introduces a kind of multiplication used by the ancient Egyptians. This algorithm is also known as Russian peasant multiplication. Report on the history of both techniques, and explain how and why they work.

19. Find out about the issues involved in drawing Venn diagrams when the number of sets is greater than 3, and report on your findings. (Two helpful websites are www.combinatorics.org/Surveys/ds5/VennSymmEJC.html and www.siam.org/siamnews/01-04/venn.pdf.)

20. What are Gray codes? How are they related to Venn diagrams?

21. Find out about Markov chains, and give some examples of how they are used.

22. What are the binomial and hypergeometric probability distributions and how are they used?

23. What are generating functions, and how are they used to solve problems?

24. Find statistics about the prevalence of false positives and false negatives for various medical tests, and report on your findings.

25. Find out about Pick's theorem. How is it proved?

26. Find out about the Catalan conjecture. How did it come to be conjectured? What is the current status of the conjecture? Report on your findings.

27. Find out about Ramsey numbers, and report on your findings.

28. Report on the computer algorithms that are used to generate all the partitions of a set.

29. Find out about the evolution in the mathematical meaning of the word "function."

30. Write a computer program to calculate the number of one-to-one functions from a set with m elements to a set with n elements, where m and n are positive integers and $m \leq n$.

31. Write a computer program to calculate the number of onto functions from a set with m elements to a set with n elements, where m and n are positive integers and $m \geq n$.

32. What are the transfinite cardinal numbers: $\aleph_0$, $\aleph_1$, $\aleph_2$, and so forth? How is arithmetic performed with these numbers?

33. Report on some of the occurrences of Fibonacci numbers in nature and some of the applications of Fibonacci numbers.

34. Report on the current status of knowledge about the 4-pole tower of Hanoi problem.

35. Find out about the bubble sort and the quick sort algorithms, and describe their operation. Discuss the efficiency of these algorithms compared to the efficiency of the insertion sort, the selection sort, and the merge sort algorithms.

36. Describe the construction and uses of a relational database.

37. Describe Warshall's algorithm for computing the transitive closure of a relation. What are some practical uses of Warshall's algorithm?

38. Report on the way the set of all rational numbers can be constructed using logic and set theory (including the definitions of ordered pair, Cartesian product, and equivalence relation) alone. What techniques are used to extend the construction to the set of all real numbers?

39. How is multiplication actually performed in modern computers? Are the same algorithms used for large integers as for small ones? Research this topic and describe your findings.

40. What other cryptographic systems are currently used for the electronic transmission of data? What kinds of mathematics are they based on?

41. What is a knight's tour? What is the history of the knight's tour problems, and how are some of them solved?

42. Describe the Instant Insanity puzzle, and discuss the way that graph theory can be used to solve it.

43. Report on the current state of knowledge about the traveling salesman problem.

44. Describe Dijkstra's shortest path algorithm, and discuss its efficiency and the proof of its correctness.

45. What is Euler's formula for the relationship among the number of edges, faces, and vertices of a convex polygon? How is it proved? What are planar graphs, and what is the relation between Euler's formula and planar graphs?

46. What is Kuratowski's theorem, how is it proved, and what are some of its practical applications?

47. In what way is graph coloring related to graph theory? State the 4-color theorem, and discuss the history of its proof.

48. Describe the n-queens problem, and discuss its solution.

49. What is a Huffman code, and what are some of its practical applications?

50. Report on some of the applications of graph theory to fields like economics, chemistry, psychology, sociology, management, and biology.

51. Find out about Turing machines, and describe their operation. Include a few examples.

52. What is a nondeterministic finite-state automaton? What kind of language is accepted by such an automaton? Include a few examples.

53. Discuss the way that the Backus-Naur form is used to describe grammars of computer programming languages, command sets, and communication protocols.
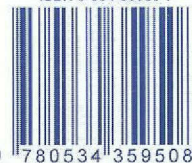
http://mathematics.brookscole.com