جامعة بيرزيت
BIRZEIT UNIVERSITY

Discrete Mathematic and Application Comp233

CHAPTER 4

ELEMENTARY NUMBER THEORY AND METHODS OF PROOF

Instructor :Murad Njoum

Example 1 – *Even and Odd Integers*

Use the definitions of *even* and *odd* to justify your answers to the following questions.

a. Is 0 even?

b. Is −301 odd?

c. If *a* and *b* are integers, is $6a^2b$ even?

d. If *a* and *b* are integers, is $10a + 8b + 1$ odd?

e. Is every integer either even or odd?

Solution:

a. Yes, $0 = 2 \cdot 0$.

b. Yes, $-301 = 2(-151) + 1$.

• Definitions

An integer n is **even** if, and only if, n equals twice some integer. An integer n is **odd** if, and only if, n equals twice some integer plus 1.

Symbolically, if n is an integer, then

$$n \text{ is even} \Leftrightarrow \exists \text{ an integer } k \text{ such that } n = 2k.$$
$$n \text{ is odd} \Leftrightarrow \exists \text{ an integer } k \text{ such that } n = 2k + 1.$$

Example 1 – *Solution*

cont'd

c. **Yes**, $6a^2b = 2(3a^2b)$, and since *a* and *b* are integers, so is $3a^2b$ (being a product of integers).

d. **Yes**, $10a + 8b + 1 = 2(5a + 4b) + 1$, and since *a* and *b* are integers, so is $5a + 4b$ (being a sum of products of integers).

e. The answer is yes, although the proof is not obvious.

Definitions

The integer 6, which equals $2 \cdot 3$, is a product of two smaller positive integers.

On the other hand, 7 cannot be written as a product of two smaller positive integers; its only positive factors are 1 and 7. A positive integer, such as 7, that cannot be written as a product of two smaller positive integers is called *prime*.

• Definition

An integer n is **prime** if, and only if, $n > 1$ and for all positive integers r and s, if $n = rs$, then either r or s equals n. An integer n is **composite** if, and only if, $n > 1$ and $n = rs$ for some integers r and s with $1 < r < n$ and $1 < s < n$.

In symbols:

n is prime $\Leftrightarrow$ $\forall$ positive integers r and s, if $n = rs$ then either $r = 1$ and $s = n$ or $r = n$ and $s = 1$.

n is composite $\Leftrightarrow$ $\exists$ positive integers r and s such that $n = rs$ and $1 < r < n$ and $1 < s < n$.

Example 2 – *Prime and Composite Numbers*

a. Is 1 prime?

b. Is every integer greater than 1 either prime or composite?

c. Write the first six prime numbers.

d. Write the first six composite numbers.

Solution:

a. No. A prime number is required to be greater than 1.

b. Yes. Let n be any integer that is greater than 1. Consider all pairs of positive integers r and s such that $n = rs$. There exist at least two such pairs, namely $r = n$ and $s = 1$ and $r = 1$ and $s = n$.

Example 2 – *Solution*

cont'd

Moreover, since $n = rs$, all such pairs satisfy the inequalities $1 \leq r \leq n$ and $1 \leq s \leq n$. If n is prime, then the two displayed pairs are the only ways to write n as rs.

Otherwise, there exists a pair of positive integers r and s such that $n = rs$ and neither r nor s equals either 1 or n. Therefore, in this case $1 < r < n$ and $1 < s < n$, and hence n is composite.

c. ***2, 3, 5, 7, 11, 13***

d. ***4, 6, 8, 9, 10, 12***

Proving Existential Statements

We have known that a statement in the form

$x \in D$ such that $Q(x)$

is true if, and only if,

$Q(x)$ is true for at least one x in D.

One way to prove this is to find an x in D that makes Q(x) true.

Another way is to give a set of directions for finding such an *x*. Both of these methods are called **constructive استنتاجي proofs of existence**.

Example 3 – *Constructive Proofs of Existence*

a. Prove the following: an even integer n that can be written in two ways as a sum of two prime numbers.

b. Suppose that r and s are integers. Prove the following: an integer k such that $22r + 18s = 2k$.

Solution:

a. Let $n = 10$. Then $10 = 5 + 5 = 3 + 7$ and 3, 5, and 7 are all prime numbers.

b. Let $k = 11r + 9s$.

Then k is an integer because it is a sum of products of integers; and by substitution, $2k = 2(11r + 9s)$, which equals $22r + 18s$ by the distributive law of algebra.

Proving Existential Statements

A **nonconstructive proof of existence** involves showing either

(a) that the existence of a value of *x* that makes *Q*(*x*) true is guaranteed by an axiom or a **previously proved theorem or**

(b) that the assumption that there is no such *x* leads to a contradiction.

The **disadvantage** of a nonconstructive proof is that it may give virtually **no clue** about where or how *x* may be found.

Disproving Universal Statements by Counterexample

To **disprove a statement** means to show that it is false. Consider the question of disproving a statement of the form

∀ *x* in *D*, if *P*(*x*) then *Q*(*x*).

Showing that this statement is false is equivalent to showing that its negation is true. The negation of the statement is existential:

***x* in *D* such that *P*(*x*) and not *Q*(*x*).**

Disproof by Counterexample

To disprove a statement of the form "$\forall x \in D$, if $P(x)$ then $Q(x)$," find a value of x in D for which the hypothesis $P(x)$ is true and the conclusion $Q(x)$ is false. Such an x is called a **counterexample.**

Example 4 – *Disproof by Counterexample*

Disprove the following statement by finding a counterexample:

∀ real numbers *a* and *b*, if $a^2 = b^2$ then $a = b$.

Solution:

To disprove this statement, you need to find real numbers *a* and *b* such that the hypothesis $a^2 = b^2$ is true and the conclusion $a = b$ is false.

The fact that both positive and negative integers have positive squares helps in the search.

Statement: ∀ real numbers a and b, if $a^2 = b^2$, then $a = b$.
Counterexample: Let $a = 1$ and $b = -1$. Then $a^2 = 1^2 = 1$ and $b^2 = (-1)^2 = 1$, and so $a^2 = b^2$. But $a \neq b$ since $1 \neq -1$.

Proving Universal Statements

The vast majority of mathematical statements to be proved are universal. In discussing how to prove such statements, it is helpful to imagine them in a standard form:

$$\forall x \in D, \text{ if } P(x) \text{ then } Q(x).$$

When D is finite or when only a finite number of elements satisfy *P*(*x*), such a statement can be proved by the method of exhaustion استنزاف.

Example 5 – *The Method of Exhaustion*

Use the method of **exhaustion** to prove the following statement:

∀ n ***Z***, if n is **even** and $4 \le n \le 26$, then n can be written as a sum of two prime numbers.

Solution:

$4 = 2 + 2$	$6 = 3 + 3$	$8 = 3 + 5$	$10 = 5 + 5$
$12 = 5 + 7$	$14 = 11 + 3$	$16 = 5 + 11$	$18 = 7 + 11$
$20 = 7 + 13$	$22 = 5 + 17$	$24 = 5 + 19$	$26 = 7 + 19$

Proving Universal Statements

The most powerful technique for proving a universal statement is one that works regardless of the size of the domain over which the statement is quantified.

It is called the *method of generalizing from the generic particular*. Here is the idea underlying the method:

طريقة التعميم من العام الخاص

Method of Generalizing from the Generic Particular

To show that every element of a set satisfies a certain property, suppose x is a *particular* but *arbitrarily chosen* element of the set, and show that x satisfies the property.

Example 6 – *Generalizing from the Generic Particular*

At some time you may have been shown a "mathematical trick" like the following.

You ask a person to pick any number, add 5, multiply by 4, subtract 6, divide by 2, and subtract twice the original number.

Then you astound the person by announcing that their final result was 7. How does this "trick" work?

Example 6 – *Generalizing from the Generic Particular* cont'd

Let an empty box • or the symbol *x* stand for the number the person picks. Here is what happens when the person follows your directions:

Step	Visual Result	Algebraic Result
Pick a number.	•	x
Add 5.	• |||||	$x + 5$
Multiply by 4.	• ||||| • ||||| • ||||| • |||||	$(x + 5) \cdot 4 = 4x + 20$
Subtract 6.	• || • || • ||||| • |||||	$(4x + 20) - 6 = 4x + 14$
Divide by 2.	• || • |||||	$\frac{4x + 14}{2} = 2x + 7$
Subtract twice the original number.	|| |||||	$(2x + 7) - 2x = 7$

Example 6 – *Generalizing from the Generic Particular*

cont'd

Thus no matter what number the person starts with, the result will always be 7.

Note that the ***x*** in the analysis above is ***particular*** **محدد** (because it represents a single quantity), but it is also ***arbitrarily*** *اعتباطيا* *chosen* or *generic* (because any number whatsoever can be put in its place).

This illustrates the process of drawing a general conclusion from a particular but generic object.

Proving Universal Statements

When the method of ***generalizing*** from the ***generic particular*** is applied to a property of the form "If *P*(*x*) then *Q*(*x*)," the result is the method of ***direct proof.***

We have known that the only way an if-then statement can be false is for the hypothesis to be ***true and the conclusion to be false***.

Thus, given the statement "If *P*(*x*) then *Q*(*x*)," if you can show that the truth of *P*(*x*) compels the truth of *Q*(*x*), then you will have proved the statement.

Proving Universal Statements

It follows by the method of generalizing from the generic particular that to show that "∀ *x*, if *P*(*x*) then *Q*(*x*)," is true for *all* elements *x* in a set *D*, **you suppose *x* is a particular but arbitrarily chosen element of *D* that makes *P*(*x*) true, and then you show that *x* makes *Q*(*x*) true.**

Method of Direct Proof

1. Express the statement to be proved in the form "$\forall x \in D$, if $P(x)$ then $Q(x)$." (This step is often done mentally.) ذهنيا
2. Start the proof by supposing x is a particular but arbitrarily chosen element of D for which the hypothesis $P(x)$ is true. (This step is often abbreviated "Suppose $x \in D$ and $P(x)$.") اختصار
3. Show that the conclusion $Q(x)$ is true by using definitions, previously established results, and the rules for logical inference.

Example 7 – *A Direct Proof of a Theorem*

Prove that the sum of any two even integers is even.

Solution:

Whenever you are presented with a statement to be proved, it is a good idea to ask yourself whether you believe it to be true.

In this case you might imagine some pairs of even integers, say 2 + 4, 6 + 10, 12 + 12, 28 + 54, and **mentally check** that their sums are even.

Example 7 – *Solution* cont'd

However, since you cannot possibly check all pairs of even numbers, you cannot know for sure that the statement is true in general by checking its truth in these particular instances.

Many properties hold for a large number of examples and yet fail to be true in general.

To prove this statement in general, you need to show that no matter what even integers are given, their sum is even. But given any two even integers, it is possible to represent them as **2*r*** and **2s** for some integers *r* and *s*.

Example 7 – *Solution* cont'd

And by the distributive law of algebra, $2r + 2s = 2(r + s)$, which is even. Thus the statement is true in general.

Suppose the statement to be proved were much more complicated than this. What is the method you could use to derive a proof?

Formal Restatement: $\forall$ integers *m* and *n*, if *m* and *n* are even then $m + n$ is even.

This statement is universally quantified over an infinite domain. Thus to prove it in general, you need to show that no matter what two integers you might be given, if both of them are even then their sum will also be even.

Example 7 – *Solution*

cont'd

Next ask yourself, "**Where am I starting from?**" or "**What am I supposing?**" The answer to such a question gives you the starting point, or first sentence, of the proof.

Starting Point: *Suppose m and n are particular but arbitrarily chosen integers that are even.*

Or, in abbreviated form:

Suppose *m* and *n* are any even integers.

Then ask yourself, "**What conclusion do I need to show in order to complete the proof?**"

To Show: ***m* + *n* is even**.

Example 7 – *Solution*

cont'd

One of the basic laws of logic, called *existential instantiation*, says, in effect, that if you know something exists, you can give it a name.

However, you cannot use the same name to refer to two different things, both of which are currently under discussion.

Existential Instantiation

If the existence of a certain kind of object is assumed or has been deduced then it can be given a name, as long as that name is not currently being used to denote something else.

Example 7 – *Solution*

cont'd

Thus since m equals twice some integer, you can give that integer a name, and since n equals twice some integer, you can also give that integer a name:

$$m = 2r, \text{ for some integer } r \qquad \text{and} \qquad n = 2s, \text{ for some integer } s.$$

Now what you want to show is that $m + n$ is even.

In other words, you want to show that $m + n$ equals

2 • (some integer). Having just found alternative representations for m (as $2r$) and n (as $2s$), it seems reasonable to substitute these representations in place of m and n:

$$m + n = 2r + 2s.$$

Example 7 – *Solution*

cont'd

Your goal is to show that $m + n$ is even. By definition of even, this means that $m + n$ can be written in the form

$$2 \cdot (\text{some integer}).$$

This analysis narrows the gap between the starting point and what is to be shown to showing that

$$2r + 2s = 2 \cdot (\text{some integer}).$$

Why is this true? First, because of the distributive law from algebra, which says that

$$2r + 2s = 2(r + s),$$

and, second, because the sum of any two integers is an integer, which implies that $r + s$ is an integer.

Example 7 – *Solution*

cont'd

In keeping with this analogy, the bracketed comments can be thought of as similar to the explanatory documentation provided by a good programmer. Documentation is not necessary for a program to run, but it helps a human reader understand what is going on.

Theorem 4.1.1

The sum of any two even integers is even.

Proof:

Suppose m and n are *[particular but arbitrarily chosen]* even integers. *[We must show that m + n is even.]*

Example 7 – *Solution*

cont'd

By definition of even, $m = 2r$ and $n = 2s$ for some integers r and s. Then

$$m + n = 2r + 2s \quad \text{by substitution}$$

$$= 2(r + s) \quad \text{by factoring out a 2.}$$

Let $t = r + s$. Note that t is an integer because it is a sum of integers. Hence

$$m + n = 2t \quad \text{where } t \text{ is an integer.}$$

It follows by definition of even that $m + n$ is even.
[This is what we needed to show.]

Directions for Writing Proofs of Universal Statements

Think of a proof as a way to communicate a convincing argument for the truth of a mathematical statement.

Over the years, the following rules of style have become fairly standard for writing the final versions of proofs:

1. **Copy the statement of the theorem to be proved on your paper.**

2. **Clearly mark the beginning of your proof with the word Proof.**

3. **Make your proof self-contained.**

Directions for Writing Proofs of Universal Statements

This means that you should explain the meaning of each variable used in your proof in the body of the proof. Thus you will begin proofs by introducing the initial variables and stating what kind of objects they are.

At a later point in your proof, you may introduce a new variable to represent a quantity that is known at that point to exist.

4. **Write your proof in complete, gramatically correct sentences.**

This does not mean that you should avoid using symbols and shorthand abbreviations, just that you should incorporate them into sentences.

Directions for Writing Proofs of Universal Statements

5. **Keep your reader informed about the status of each statement in your proof.**

Your reader should never be in doubt about whether something in your proof has been assumed or established or is still to be deduced. If something is assumed, preface it with a word like *Suppose* or *Assume*.

If it is still to be shown, preface it with words like, *We must show that* or *In other words*, *we must show that*.
This is especially important if you introduce a variable in rephrasing what you need to show.

Directions for Writing Proofs of Universal Statements

6. **Give a reason for each assertion in your proof.**

Each assertion in a proof should come directly from the hypothesis of the theorem, or follow from the definition of one of the terms in the theorem, or be a result obtained earlier in the proof, or be a mathematical result that has previously been established or is agreed to be assumed.

Indicate the reason for each step of your proof using phrases such as *by hypothesis*, *by definition of* . . . , and *by theorem* . . . .

Directions for Writing Proofs of Universal Statements

7. **Include the "little words and phrases" that make the logic of your arguments clear.**

When writing a mathematical argument, especially a proof, indicate how each sentence is related to the previous one.

Does it follow from the previous sentence or from a combination of the previous sentence and earlier ones? If so, start the sentence by stating the reason why it follows or by writing *Then*, or *Thus*, or *So*, or *Hence*, or *Therefore*, or *Consequently*, or *It follows that*, and include the reason at the end of the sentence.

Directions for Writing Proofs of Universal Statements

If a sentence expresses a new thought or fact that does not follow as an immediate consequence of the preceding statement but is needed for a later part of a proof, introduce it by writing *Observe that*, or *Note that*, or *But*, or *Now*.

Sometimes in a proof it is desirable to define a new variable in terms of previous variables. In such a case, introduce the new variable with the word *Let*.

8. **Display equations and inequalities.**

The convention is to display equations and inequalities on separate lines to increase readability, both for other people and for ourselves so that we can more easily check our work for accuracy.

Common Mistakes

The following are some of the most common mistakes people make when writing mathematical proofs.

1. **Arguing from examples.**

Looking at examples is one of the most helpful practices a problem solver can engage in and is encouraged by all good mathematics teachers.

However, it is a mistake to think that a general statement can be proved by showing it to be true for some special cases. A property referred to in a universal statement may be true in many instances without being true in general.

Common Mistakes

2. **Using the same letter to mean two different things.**
   Some beginning theorem provers give a new variable quantity the same letter name as a previously introduced variable.

3. **Jumping to a conclusion.**
   To jump to a conclusion means to allege the truth of something without giving an adequate reason.

4. **Circular reasoning.**
   To engage in circular reasoning means to assume what is to be proved; it is a variation of jumping to a conclusion.

Common Mistakes

5. **Confusion between what is known and what is still to be shown.**

   A more subtle way to engage in circular reasoning occurs when the conclusion to be shown is restated using a variable.

6. **Use of *any* rather than *some*.**

   There are a few situations in which the words *any* and *some* can be used interchangeably.

Example – *Disproving an Existential Statement*

Show that the following statement is false:

There is a positive integer n such that $n^2 + 3n + 2$ is prime.

Solution:

Proving that the given statement is false is equivalent to proving its negation is true.

The negation is

For all positive integers n, $n^2 + 3n + 2$ is not prime.

Because the negation is universal, it is proved by generalizing from the generic particular.

Example 9 – *Solution*

cont'd

Claim: The statement "There is a positive integer *n* such that $n^2 + 3n + 2$ is prime" is false.

Proof:

Suppose *n* is any *[particular but arbitrarily chosen]* positive integer. *[We will show that $n^2 + 3n + 2$ is not prime.]*

We can factor $n^2 + 3n + 2$ to obtain

$$n^2 + 3n + 2 = (n + 1)(n + 2).$$

We also note that $n + 1$ and $n + 2$ are integers (because they are sums of integers) and that both $n + 1 > 1$ and $n + 2 > 1$ (because $n \geq 1$). Thus $n^2 + 3n + 2$ is a product of two integers each greater than 1, and so $n^2 + 3n + 2$ is not prime.

Conjecture تخمين, Proof, and Disproof

More than 350 years ago, the French mathematician Pierre de Fermat claimed that it is impossible to find positive integers *x*, *y*, and *z* with $x^n + y^n = z^n$ if *n* is an integer that is at least 3. (For $n = 2$, the equation has many integer solutions, such as $3^2 + 4^2 = 5^2$ and $5^2 + 12^2 = 13^2$.)

Fermat wrote his claim in the margin of a book, along with the comment "I have discovered a truly remarkable PROOF of this theorem which this margin is too small to contain."

Conjecture, Proof, and Disproof

In other words, no three perfect fourth powers add up to another perfect fourth power. For small numbers, Euler's conjecture looked good.

But in 1987 a Harvard mathematician, Noam Elkies, proved it wrong. One counterexample, found by Roger Frye of Thinking Machines Corporation in a long computer search, is $95{,}800^4 + 217{,}519^4 + 414{,}560^4 = 422{,}481^4$.

Direct Proof and Counterexample II: Rational Numbers

Sums, differences, and products of integers are integers. But most quotients of integers are not integers. Quotients القواسم of integers are, however, important; they are known as *rational numbers*.

• Definition

A real number r is **rational** if, and only if, it can be expressed as a quotient of two integers with a nonzero denominator. A real number that is not rational is **irrational.** More formally, if r is a real number, then

$$r \text{ is rational} \Leftrightarrow \exists \text{ integers } a \text{ and } b \text{ such that } r = \frac{a}{b} \text{ and } b \neq 0.$$

The word *rational* contains the word *ratio*, which is another word for quotient القسمة حاصل. A rational number can be written as a ratio of integers.

Example 1 – *Determining Whether Numbers Are Rational or Irrational*

a. Is 10/3 a rational number?

b. Is $-\frac{5}{39}$ a rational number?

c. Is 0.281 a rational number?

d. Is 7 a rational number?

e. Is 0 a rational number?

Example 1 – *Determining Whether Numbers Are Rational or Irrational* cont'd

f. Is 2/0 a rational number?

g. Is 2/0 an irrational number?

h. Is 0.12121212 . . . a rational number (where the digits 12 are assumed to repeat forever)?

i. If m and n are integers and neither m nor n is zero, is $(m + n)/mn$ a rational number?

Example 1 – *Solution*

a. Yes, 10/3 is a quotient of the integers 10 and 3 and hence is rational.

b. Yes, $-\frac{5}{39} = \frac{-5}{39}$, which is a quotient of the integers −5 and 39 and hence is rational.

c. Yes, 0.281 = 281/1000. Note that the real numbers represented on a typical calculator display are all finite decimals.

An explanation similar to the one in this example shows that any such number is rational. It follows that a calculator with such a display can represent only rational numbers.

Example 1 – *Solution*

cont'd

d. Yes, 7 = 7/1.

e. Yes, 0 = 0/1.

f. No, 2/0 is not a number (division by 0 is not allowed).

g. No, because every irrational number is a number, and 2/0 is not a number.

Example 1 – *Solution*

cont'd

h. Yes. Let $x = 0.12121212....$ $100x = 12.12121212....$

Thus $100x - x = 12.12121212... - 0.12121212... = 12.$

But also $100x - x = 99x$ by basic algebra

Hence $99x = 12,$

And so $x = \frac{12}{99}.$

Therefore, 0.12121212…. = 12/99, which is a ratio of two nonzero integers and thus is a rational number.

Example 1 – *Solution*

cont'd

Note that you can use an argument similar to this one to show that any repeating decimal is a rational number.

i. Yes, since *m* and *n* are integers, so are *m* + *n* and *mn* (because sums and products of integers are integers).
Also $mn \neq 0$ by the *zero product property*.

One version of this property says the following:

Zero Product Property

If neither of two real numbers is zero, then their product is also not zero.

It follows that (*m* + *n*)/*mn* is a quotient of two integers with a nonzero denominator and hence is a rational number.

More on Generalizing from the Generic Particular

Some people like to think of the method of generalizing from the generic particular as a challenge process.

If you claim a property holds for all elements in a domain, then someone can challenge your claim by picking any element in the domain whatsoever and asking you to prove that that element satisfies the property.

To prove your claim, you must be able to meet all such challenges. That is, you must have a way to convince the challenger that the property is true for an *arbitrarily chosen* element in the domain.

More on Generalizing from the Generic Particular

For example, suppose "A" claims that every integer is a rational number. "B" challenges this claim by asking "A" to prove it for $n = 7$.

"A" observes that

$$7 = \frac{7}{1}$$ which is a quotient of integers and hence rational.

"B" accepts this explanation but challenges again with $n = -12$. "A" responds that

$$-12 = \frac{-12}{1}$$ which is a quotient of integers and hence rational.

More on Generalizing from the Generic Particular

Next "B" tries to trip up "A" by challenging with $n = 0$, but "A" answers that

$$0 = \frac{0}{1}$$ which is a quotient of integers and hence rational.

As you can see, "A" is able to respond effectively to all "B"s challenges because "A" has a general procedure for putting integers into the form of rational numbers: "A" just divides whatever integer "B" gives by 1.

That is, no matter what integer *n* "B" gives "A", "A" writes

$$n = \frac{n}{1}$$ which is a quotient of integers and hence rational.

This discussion proves the following theorem.

Theorem 4.2.1

Every integer is a rational number.

51

Example 2 – *A Sum of Rationals Is Rational*

Prove that the sum of any two rational numbers is rational.

Solution:

Begin by mentally or explicitly rewriting the statement to be proved in the form "∀ _______, if _______ then _______."

Formal Restatement: ∀ real numbers *r* and *s*, if *r* and *s* are rational then *r* + *s* is rational.

Next ask yourself, "**Where am I starting from?**" or "**What am I supposing?**" The answer gives you the starting point, or first sentence, of the proof.

Instructor: Murad Njoum

52

Example 2 – *Solution*

cont'd

Starting Point: Suppose *r* and *s* are particular but arbitrarily chosen real numbers such that *r* and *s* are rational; or, more simply, Suppose *r* and *s* are rational numbers.

Then ask yourself, "What must I show to complete the proof?"

To Show: *r* + *s* is rational.

Finally ask, "How do I get from the starting point to the conclusion?" or "Why must *r* + *s* be rational if both *r* and *s* are rational?" The answer depends in an essential way on the definition of rational.

Example 2 – *Solution*

cont'd

Rational numbers are quotients of integers, so to say that *r* and *s* are rational means that

$$r = \frac{a}{b} \quad \text{and} \quad s = \frac{c}{d} \quad \text{for some integers } a, b, c, \text{ and } d \text{ where } b \neq 0 \text{ and } d \neq 0.$$

It follows by substitution that

$$r + s = \frac{a}{b} + \frac{c}{d}.$$

Example 2 – *Solution*

cont'd

You need to show that $r + s$ is rational, which means that $r + s$ can be written as a single fraction or ratio of two integers with a nonzero denominator.

But the right-hand side of equation (4.2.1) in

$$\frac{a}{b} + \frac{c}{d} = \frac{ad}{bd} + \frac{bc}{bd}$$ rewriting the fraction with a common denominator

$$= \frac{ad + bc}{bd}$$ adding fractions with a common denominator.

Example 2 – *Solution*

cont'd

Is this fraction a ratio of integers? Yes. Because products and sums of integers are integers, $ad + bc$ and bd are both integers.

Is the denominator $bd \neq 0$? Yes, by the zero product property (since $b \neq 0$ and $d \neq 0$). Thus $r + s$ is a rational number.

This discussion is summarized as follows:

Theorem 4.2.2

The sum of any two rational numbers is rational.

Example 2 – *Solution*

cont'd

Proof:

Suppose r and s are rational numbers. *[We must show that $r + s$ is rational.]*

Then, by definition of rational, $r = a/b$ and $s = c/d$ for some integers a, b, c, and d with $b \neq 0$ and $d \neq 0$.

Thus

$$r + s = \frac{a}{b} + \frac{c}{d} \quad \text{by substitution}$$

$$= \frac{ad + bc}{bd} \quad \text{by basic algebra.}$$

Example 2 – *Solution*

cont'd

Let $p = ad + bc$ and $q = bd$. Then p and q are integers because products and sums of integers are integers and because a, b, c, and d are all integers.

Also $q \neq 0$ by the zero product property.

Thus

$$r + s = \frac{p}{q} \text{ where } p \text{ and } q \text{ are integers and } q \neq 0.$$

Therefore, $r + s$ is rational by definition of a rational number. *[This is what was to be shown.]*

Deriving New Mathematics from Old

In the future, when we ask you to **prove something directly from the definitions,** we will mean that you should restrict yourself to this approach.

However, once a collection of statements has been proved directly from the definitions, another method of proof becomes possible.

The statements in the collection can be used to derive additional results.

Example 3 – *Deriving Additional Results about Even and Odd Integers*

Suppose that you have already proved the following properties of even and odd integers:

1. The sum, product, and difference of any two even integers are even.
2. The sum and difference of any two odd integers are even.
3. The product of any two odd integers is odd.
4. The product of any even integer and any odd integer is even.

Example 3 – *Deriving Additional Results about Even and Odd Integers*

cont'd

5. The sum of any odd integer and any even integer is odd.

6. The difference of any odd integer minus any even integer is odd.

7. The difference of any even integer minus any odd integer is odd.

Use the properties listed above to prove that if ***a* is any even** integer and ***b* is *any odd integer***, then $\frac{a^2+b^2+1}{2}$ is an integer.

Example 3 – *Solution*

Suppose *a* is **any even** integer and *b* is **any odd integer**. By property 3, b^2 is odd, and by property 1, a^2 is even.

Then by property 5, $a^2 + b^2$ is odd, and because 1 is also odd, the sum is even $(a^2 + b^2) + 1 = a^2 + b^2 + 1$

Hence, **by definition of even,** there exists an integer *k* such that

$a^2 + b^2 + 1 = 2k.$

Dividing both sides by 2 gives $\frac{a^2+b^2+1}{2}$ = *k*, which is an integer.

Thus $\frac{a^2+b^2+1}{2}$ is an integer *[***as was to be shown***]*.

Example 4 – *The Double of a Rational Number*

A **corollary** نتيجة is a statement whose truth can be immediately deduced from a theorem that has already been proved.

Corollary 4.2.3

The double of a rational number is rational.

Solution:

The double of a number is just its sum with itself.

But since the sum of any two rational numbers is rational (Theorem 4.2.2), the sum of a rational number with itself is rational. Hence the double of a rational number is rational.

Example 4 – *Solution* cont'd

Here is a formal version of this argument:

Proof:

Suppose r is any rational number. Then $2r = r + r$ is a sum of two rational numbers.

So, by Theorem 4.2.2, $2r$ is rational.

Direct Proof and Counterexample III: Divisibility

The notion of divisibility is the central concept of one of the most beautiful subjects in advanced mathematics: **number theory**, the study of properties of integers.

• Definition

If n and d are integers and $d \neq 0$ then

n is **divisible by** d if, and only if, n equals d times some integer.

Instead of "n is divisible by d," we can say that

n **is a multiple of** d, or
d **is a factor of** n, or
d **is a divisor of** n, or
d **divides** n.

The notation **d | n** is read "d divides n." Symbolically, if n and d are integers and $d \neq 0$:

$$d \mid n \quad \Leftrightarrow \quad \exists \text{ an integer } k \text{ such that } n = dk.$$

Example 1 – *Divisibility*

a. Is 21 divisible by 3?

b. Does 5 divide 40?

c. Does 7|42?

d. Is 32 a multiple of −16?

e. Is 6 a factor of 54?

f. Is 7 a factor of −7?

a. Yes, 21 = 3 • 7.

b. Yes, 40 = 5 • 8.

c. Yes, 42 = 7 • 6.

d. Yes, 32 = (−16) • (−2).

e. Yes, 54 = 6 • 9.

f. Yes, −7 = 7 • (−1).

Direct Proof and Counterexample III: Divisibility

Two useful properties of divisibility are (1) that if one positive integer divides a second positive integer, then the first is less than or equal to the second, and (2) that the only divisors of 1 are 1 and −1.

Theorem 4.3.1 A Positive Divisor of a Positive Integer

For all integers a and b, if a and b are positive and a divides b, then $a \leq b$.

Theorem 4.3.2 Divisors of 1

The only divisors of 1 are 1 and -1.

Example 1 – *Divisibility of Algebraic Expressions*

a. If a and b are integers, is $3a + 3b$ divisible by 3?

b. If k and m are integers, is $10km$ divisible by 5?

Solution:

a. Yes. By the distributive law of algebra, $3a + 3b = 3(a + b)$ and $a + b$ is an integer because it is a sum of two integers.

b. Yes. By the associative law of algebra, $10km = 5 \cdot (2km)$ and $2km$ is an integer because it is a product of three integers.

Direct Proof and Counterexample III: Divisibility

When the definition of divides is rewritten formally using the existential quantifier, the result is

$$d \mid n \quad \Leftrightarrow \quad \exists \text{ an integer } k \text{ such that } n = dk.$$

Since the negation of an existential statement is universal, it follows that *d* does not divide *n* (denoted $d \nmid n$) if, and only if, ∀ integers *k*, *n* ≠ *dk*, or, in other words, the quotient *n*/*d* is not an integer.

$$\text{For all integers } n \text{ and } d, \quad d \nmid n \quad \Leftrightarrow \quad \frac{n}{d} \text{ is not an integer.}$$

Does 4 | 15?

Solution:

No, $\frac{15}{4} = 3.75$, which is not an integer.

Example 6 – *Solution*

cont'd

Prove that for all integers *a*, *b*, and *c*, if *a* | *b* and *b* | *c*, then *a* | *c*. (transitive).

Proof:

Suppose *a*, *b*, and *c* are *[particular but arbitrarily chosen]* integers such that *a* divides *b* and *b* divides *c*. *[We must show that a divides c.]* By definition of divisibility,

$$b = ar \quad \text{and} \quad c = bs \quad \text{for some integers } r \text{ and } s.$$

By substitution

$$\begin{aligned} c &= bs \\ &= (ar)s \\ &= a(rs) \quad \text{by basic algebra.} \end{aligned}$$

Example 6 – *Solution*

cont'd

Let $k = rs$. Then k is an integer since it is a product of integers, and therefore

$$c = ak \quad \text{where } k \text{ is an integer.}$$

Thus a divides c by definition of divisibility. *[This is what was to be shown.]*

Theorem 4.3.3 Transitivity of Divisibility

For all integers a, b, and c, if a divides b and b divides c, then a divides c.

Proving Properties of Divisibility

Counterexamples and Divisibility

Theorem 4.3.4 Divisibility by a Prime

Any integer $n > 1$ is divisible by a prime number.

To show that a proposed divisibility property is not universally true, you need only find one pair of integers for which it is false.

Example 7 – *Checking a Proposed Divisibility Property*

Is the following statement true or false? For all integers a and b, if $a \mid b$ and $b \mid a$ then $a = b$.

Solution:

This statement is false. Can you think of a counterexample just by concentrating for a minute or so?

The following discussion describes a mental process that may take just a few seconds. It is helpful to be able to use it consciously, however, to solve more difficult problems.

Example 7 – *Solution*

cont'd

To discover the truth or falsity of the given statement, start off much as you would if you were trying to prove it.

Starting Point: Suppose a and b are integers such that $a \mid b$ and $b \mid a$.

Ask yourself, "Must it follow that $a = b$, or could it happen that $a \neq b$ for some a and b?" Focus on the supposition. What does it mean? By definition of divisibility, the conditions $a \mid b$ and $b \mid a$ mean that

$$b = ka \quad \text{and} \quad a = lb \quad \text{for some integers } k \text{ and } l.$$

Example 7 – *Solution*

cont'd

Must it follow that $a = b$, or can you find integers a and b that satisfy these equations for which $a \neq b$? The equations imply that

$$b = ka = k(lb) = (kl)b.$$

Since $b \mid a$, $b \neq 0$, and so you can cancel b from the extreme left and right sides to obtain

$$1 = kl.$$

In other words, k and l are divisors of 1. But, by Theorem 4.3.2, the only divisors of 1 are 1 and –1. Thus k and l are both 1 or are both –1. If $k = l = 1$, then $b = a$.

Example 7 – *Solution*

cont'd

But if $k = l = -1$, then $b = -a$ and so $a \neq b$.

This analysis suggests that you can find a counterexample by taking $b = -a$.

Here is a formal answer:

Proposed Divisibility Property: For all integers a and b, if $a \mid b$ and $b \mid a$ then $a = b$.

Counterexample: Let $a = 2$ and $b = -2$. Then

$$a \mid b \text{ since } 2 \mid (-2) \text{ and } b \mid a \text{ since } (-2) \mid 2, \text{ but } a \neq b \text{ since } 2 \neq -2.$$

Therefore, the statement is false.

The Unique Factorization of Integers Theorem

Theorem 4.3.5 Unique Factorization of Integers Theorem (Fundamental Theorem of Arithmetic)

Given any integer $n > 1$, there exist a positive integer k, distinct prime numbers $p_1, p_2, \ldots, p_k$, and positive integers $e_1, e_2, \ldots, e_k$ such that

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \ldots p_k^{e_k},$$

and any other expression for n as a product of prime numbers is identical to this except, perhaps, for the order in which the factors are written.

The unique factorization of integers theorem says that any integer greater than 1 either is prime or can be written as a product of prime numbers in a way that is unique except, perhaps, for the order in which the primes are written.

The Unique Factorization of Integers Theorem

Because of the unique factorization theorem, any integer $n > 1$ can be put into a *standard factored form* in which the prime factors are written in ascending order from left to right.

• Definition

Given any integer $n > 1$, the **standard factored form** of n is an expression of the form

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_k^{e_k},$$

where k is a positive integer; $p_1, p_2, \ldots, p_k$ are prime numbers; $e_1, e_2, \ldots, e_k$ are positive integers; and $p_1 < p_2 < \cdots < p_k$.

Example 9 – *Using Unique Factorization to Solve a Problem*

Suppose *m* is an integer such that

$$8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot m = 17 \cdot 16 \cdot 15 \cdot 14 \cdot 13 \cdot 12 \cdot 11 \cdot 10.$$

Does 17 | *m*?

Solution:

Since 17 is one of the prime factors of the right-hand side of the equation, it is also a prime factor of the left-hand side (by the unique factorization of integers theorem).

But 17 does not equal any prime factor of 8, 7, 6, 5, 4, 3, or 2 (because it is too large). Hence 17 must occur as one of the prime factors of *m*, and so **17 | *m***.

Direct Proof and Counterexample IV: **Division into Cases and the Quotient-Remainder Theorem**

The quotient-remainder theorem says that when any integer *n* is divided by any positive integer *d*, the result is a quotient *q* and a nonnegative remainder *r* that is smaller than *d*.

Theorem 4.4.1 The Quotient-Remainder Theorem

Given any integer n and positive integer d, there exist unique integers q and r such that

$$n = dq + r \quad \text{and} \quad 0 \le r < d.$$

Example 1 – *The Quotient-Remainder Theorem*

For each of the following values of *n* and *d*, find integers *q* and *r* such that and $n = dq + r \qquad 0 \le r < d.$

a. $n = 54$, $d = 4$ **b.** $n = -54$, $d = 4$ **c.** $n = 54$, $d = 70$

Solution:

a. $54 = 4 \cdot 13 + 2$; hence $q = 13$ and $r = 2$.

b. $-54 = 4 \cdot (-14) + 2$; hence $q = -14$ and $r = 2$.

c. $54 = 70 \cdot 0 + 54$; hence $q = 0$ and $r = 54$.

div and mod

However, they do not give the values that satisfy the quotient-remainder theorem when a negative integer *n* is divided by a positive integer *d*.

• **Definition**

Given an integer n and a positive integer d,

n div d = the integer quotient obtained when n is divided by d, and

n mod d = the nonnegative integer remainder obtained when n is divided by d.

Symbolically, if n and d are integers and $d > 0$, then

$$n \text{ div } d = q \quad \text{and} \quad n \text{ mod } d = r \quad \Leftrightarrow \quad n = dq + r$$

where q and r are integers and $0 \le r < d$.

div and mod

For instance, to compute *n div d* for a nonnegative integer *n* and a positive integer *d*, you just divide *n* by *d* and ignore the part of the answer to the right of the decimal point.

To find *n mod d*, you can use the fact that if $n = dq + r$, then $r = n - dq$. Thus $n = d \cdot (n \; div \; d) + n \; mod \; d$, and so

$$n \; mod \; d = n - d \cdot (n \; div \; d).$$

Hence, to find *n mod d* compute *n div d*, multiply by *d*, and subtract the result from *n*.

Example 2 – *Solution*

cont'd

Discarding the fractional part gives 32 *div* 9 = 3, and so

$$32 \; mod \; 9 = 32 - 9 \cdot (32 \; div \; 9) = 32 - 27 = 5.$$

A calculator with a built-in integer-part function iPart allows you to input a single expression for each computation:

$$32 \; div \; 9 = \text{iPart}(32/9)$$

$$\text{and} \quad 32 \; mod \; 9 = 32 - 9 \cdot \text{iPart}\,(32/9) = 5.$$

Representations of Integers

We have defined, an even integer to have the form twice some integer. At that time we could have defined an odd integer to be one that was not even.

Instead, because it was more useful for proving theorems, we specified that an odd integer has the form twice some integer plus one.

The quotient-remainder theorem brings these two ways of describing odd integers together by guaranteeing that any integer is either even or odd.

Representations of Integers

To see why, let *n* be any integer, and consider what happens when *n* is divided by 2.

By the quotient-remainder theorem (with *d* = 2), there exist unique integers *q* and *r* such that

$$n = 2q + r \quad \text{and} \quad 0 \leq r < 2.$$

But the only integers that satisfy are *r* = 0 and *r* = 1. $0 \leq r < 2$

It follows that given any integer *n*, there exists an integer *q* with

$$n = 2q + 0 \quad \text{or} \quad n = 2q + 1.$$

Representations of Integers

In the case that $n = 2q + 0 = 2q$, *n* is even. In the case that $n = 2q + 1$, *n* is odd. Hence *n* is either even or odd, and, because of the uniqueness of *q* and *r*, *n* cannot be both even and odd.

The *parity* of an integer refers to whether the integer is even or odd. For instance, 5 has odd parity and 28 has even parity.

We call the fact that any integer is either even or odd the **parity property خاصية التكافؤ.**

Example 5 – *Consecutive Integers Have Opposite Parity*

Prove that given any two consecutive integers, one is even and the other is odd.

Solution:
Two integers are called *consecutive* if, and only if, one is one more than the other. So if one integer is *m*, the next consecutive integer is *m* + 1.

To prove the given statement, start by supposing that you have two particular but arbitrarily chosen consecutive integers. If the smaller is *m*, then the larger will be *m* + 1.

Example 5 – *Solution*

cont'd

How do you know for sure that one of these is even and the other is odd? You might imagine some examples: 4, 5; 12, 13; 1,073, 1,074.

In the first two examples, the smaller of the two integers is even and the larger is odd; in the last example, it is the reverse. These observations suggest dividing the analysis into two cases.

Case 1: The smaller of the two integers is even.

Case 2*:* The smaller of the two integers is odd.

Example 5 – *Solution*

cont'd

This discussion is summarized as follows.

Theorem 4.4.2 The Parity Property

Any two consecutive integers have opposite parity.

Proof:
Suppose that two *[particular but arbitrarily chosen]* consecutive integers are given; call them m and $m + 1$.
[We must show that one of m and m + 1 is even and that the other is odd.]

Example 5 – *Solution*

cont'd

By the parity property, either *m* is even or *m* is odd. *[We break the proof into two cases depending on whether m is even or odd.]*

Case 1 (m is even): In this case, $m = 2k$ for some integer *k*, and so $m + 1 = 2k + 1$, which is odd *[by definition of odd]*.

Hence in this case, one of *m* and $m + 1$ is even and the other is odd.

Example 5 – *Solution*

cont'd

Case 2 (m is odd): In this case, $m = 2k + 1$ for some integer *k*, and so

.

$$m + 1 = (2k + 1) + 1 = 2k + 2 = 2(k + 1)$$

But $k + 1$ is an integer because it is a sum of two integers. Therefore, $m + 1$ equals twice some integer, and thus
$m + 1$ is even.

Hence in this case also, one of *m* and $m + 1$ is even and the other is odd.

It follows that regardless of which case actually occurs for the particular *m* and $m + 1$ that are chosen, one of *m* and
$m + 1$ is even and the other is odd. *[This is what was to be shown.]*

Representations of Integers

There are times when division into more than two cases is called for. Suppose that at some stage of developing a proof, you know that a statement of the form

$$A_1 \text{ or } A_2 \text{ or } A_3 \text{ or} \ldots \text{or } A_n$$

is true, and suppose you want to deduce a conclusion *C*.

By definition of *or*, you know that at least one of the statements A_i is true (although you may not know which).

In this situation, you should use the **method of division into cases**.

Representations of Integers

First assume *A_1 is true* and *deduce C*; next assume *A2 is true* and *deduce C*; and so forth until you have assumed *An is true and deduced C*.

At that point, you can conclude that regardless of which statement A_i happens to be true, the truth of *C* follows.

Method of Proof by Division into Cases

To prove a statement of the form "If A_1 or A_2 or ... or A_n, then C," prove all of the following:

$$\begin{aligned} &\text{If } A_1, \text{ then } C, \\ &\text{If } A_2, \text{ then } C, \\ &\vdots \\ &\text{If } A_n, \text{ then } C. \end{aligned}$$

This process shows that C is true regardless of which of $A_1, A_2, \ldots, A_n$ happens to be the case.

Example 6 – *Representations of Integers Modulo 4*

Show that any integer can be written in one of the four forms

$$n = 4q \quad \text{or} \quad n = 4q + 1 \quad \text{or} \quad n = 4q + 2 \quad \text{or} \quad n = 4q + 3$$

for some integer *q*.

Solution:

Given any integer *n*, apply the quotient-remainder theorem to *n* with $d = 4$.

This implies that there exist an integer quotient *q* and a remainder *r* such that

$$n = 4q + r \quad \text{and} \quad 0 \le r < 4.$$

Example 6 – *Solution* cont'd

But the only nonnegative remainders *r* that are less than 4 are 0, 1, 2, and 3.

Hence

$$n = 4q \quad \text{or} \quad n = 4q + 1 \quad \text{or} \quad n = 4q + 2 \quad \text{or} \quad n = 4q + 3$$

for some integer *q*.

Example 7 – *The Square of an Odd Integer*

Prove: The square of any odd integer has the form 8*m* + 1 for some integer *m*.

Solution:
Begin by asking yourself, "**Where am I starting from?**" and "What do I need to show?" To help answer these questions, introduce variables to represent the quantities in the statement to be proved.

Formal Restatement: ∀ odd integers *n*, an integer *m* such that $n^2 = 8m + 1.$

From this, you can immediately identify the starting point and what is to be shown.

Example 7 – *Solution* cont'd

Starting Point: Suppose *n* is a particular but arbitrarily chosen odd integer.

To Show: an integer *m* such that $n^2 = 8m + 1.$

This looks tough. Why should there be an integer *m* with the property that $n^2 = 8m + 1$?

That would say that $(n^2 – 1)/8$ is an integer, or that 8 divides $n^2 – 1$.

Example 7 – *Solution*

cont'd

That means that their product is divisible by 4. **But that's not enough**. You need to show that the product is divisible by 8. This seems to be a blind alley طرق مغلق.

You could try another track. Since *n* is odd, you could represent *n* as $2q + 1$ for some integer *q*.

Then $n^2 = (2q + 1)^2 = 4q^2 + 4q + 1 = 4(q^2 + q) + 1.$

Example 7 – *Solution*

cont'd

It is clear from this analysis that n^2 can be written in the form $4m + 1$, but it may not be clear that it can be written as $8m + 1$. This also seems to be a **blind alley.**

You could try breaking into cases based on these two different forms.

It turns out that this last possibility works! In each of the two cases, the conclusion follows readily by direct calculation.

Example 7 – *Solution*

cont'd

The details are shown in the following formal proof:

Theorem 4.4.3

The square of any odd integer has the form $8m + 1$ for some integer m.

Proof:

Suppose *n* is a *[particular but arbitrarily chosen]* odd integer. By the quotient-remainder theorem, *n* can be written in one of the forms

$$4q \quad \text{or} \quad 4q+1 \quad \text{or} \quad 4q+2 \quad \text{or} \quad 4q+3$$

for some integer *q*.

In fact, since *n* is odd and 4*q* and 4*q* + 2 are even, *n* must have one of the forms

$$4q+1 \quad \text{or} \quad 4q+3.$$

Instructor: Murad Njoum

Example 7 – *Solution*

cont'd

Case 1 (*n* = 4*q* + 1 for some integer *q*): *[We must find an integer m such that*
] $n^2 = 8m + 1.$

Since $n = 4q + 1$,

$$n^2 = (4q+1)^2 \quad \text{by substitution}$$

$$= (4q+1)(4q+1) \quad \text{by definition of square}$$

$$= 16q^2 + 8q + 1$$

$$= 8(2q^2 + q) + 1 \quad \text{by the laws of algebra.}$$

Instructor: Murad Njoum

Example 7 – *Solution*

cont'd

Let $m = 2q^2 + q$. Then *m* is an integer since 2 and *q* are integers and sums and products of integers are integers.

Thus, substituting,

$n^2 = 8m + 1$ is an integer.

Example 7 – *Solution*

cont'd

Case 2 (*n* = 4*q* + 3 for some integer *q*): *[We must find an integer m such that $n^2 = 8m + 1$.]*

Since $n = 4q + 3$,

$$n^2 = (4q + 3)^2 \quad \text{by substitution}$$

$$= (4q + 3)(4q + 3) \quad \text{by definition of square}$$

$$= 16q^2 + 24q + 9$$

$$= 16q^2 + 24q + (8 + 1)$$

$$= 8(2q^2 + 3q + 1) + 1 \quad \text{by the laws of algebra.}$$

Example 7 – *Solution*

cont'd

[The motivation for the choice of algebra steps was the desire to write the expression in the form
8 • *(some integer)* + 1.*]*

Let $m = 2q^2 + 3q + 1$. Then *m* is an integer since 1, 2, 3, and *q* are integers and sums and products of integers are integers.

Thus, substituting, $n^2 = 8m + 1$ where *m* is an integer.

Cases 1 and 2 show that given any odd integer, whether of the form
for some integer m. *[This is what we needed to show.]*

$4q + 1$ or $4q + 3$, $n^2 = 8m + 1$

Representations of Integers

Note that the result of Theorem 4.4.3 can also be written, "For any odd integer *n*, n^2 *mod* 8 = 1."

In general, according to the quotient-remainder theorem, if an integer *n* is divided by an integer *d*, the possible remainders are 0, 1, 2, . . ., (*d* – 1).

This implies that *n* can be written in one of the forms for some integer *q*.

$$dq,\ dq + 1,\ dq + 2, ,\ \ldots,\ dq + (d - 1)$$