FACULTY OF ENGINEERING AND TECHNOLOGY

COMPUTER SCIENCE DEPARTMENT

COMP233
Discrete Mathematics

CHAPTER 4

Elementary Number Theory and Methods of Proof

Motivation

- Mathematics, as a science, commenced when first someone, probably a Greek, proved propositions about “any” things or about “some” things without specification of definite particular things.

  — Alfred North Whitehead, 1861–1947

- In this chapter, we will learn how to properly prove and disprove certain theory.

Motivation – cont.

- Our area of application for this chapter will be number theory. As such, the theories we will prove might seem obvious.

- Be especially critical of any statement following the word “obviously.”

— Anna Pell Wheeler 1883–1966

Number Theory

- Direct Proof and Counterexamples
- Rational Numbers
- Divisibility
- Division into Cases and the Quotient-Remainder Theorem

Number Theory

- Direct Proof and Counterexamples
- Rational Numbers
- Divisibility
- Division into Cases and the Quotient-Remainder Theorem

Assumptions

- In this text we assume a familiarity with the laws of basic algebra, which are listed in Appendix A – go to the book to refer to them.
- We also use the three properties of equality: For all objects A, B, and C,
  1) *A = A*
  2) *if A = B then B = A*
  3) *if A = B and B = C, then A = C.*
- In addition, we assume that there is no integer between 0 and 1 and that the set of all integers is closed under addition, subtraction, and multiplication. This means that sums, differences, and products of integers are integers.
- Most quotients of integers are not integers. For example, 3÷ 2, which equals 3/2, is not an integer, and 3 ÷ 0 is not even a number.

Outline

- Even and Odd Integers
- Prime and Composite Numbers
- Methods of Proof
- Direct Proof

Outline

- Even and Odd Integers
- Prime and Composite Numbers
- Methods of Proof
- Direct Proof

Even and Odd Integers

- 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
  - $n \; is \; even \leftrightarrow \exists$ an integer k such that $n = 2k.$
  - $n \; is \; odd \leftrightarrow \exists$ an integer k such that $n = 2k + 1.$

Even and Odd Integers – cont.

- It follows from the definition that if you are doing a problem in which you happen to know that a certain integer is even, you can deduce that it has the form 2·(some integer).
- Conversely, if you know in some situation that an integer equals 2·(some integer), then you can deduce that the integer is even.

- Similarly, knowing a certain integer is odd, you can deduce it has the form of 2·(some integer) + 1.
- And knowing that an integers equals 2·(some integer) + 1, you can deduce that it is odd.

Examples

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

a) Is 0 even?

Yes, $0 = 2 \cdot 0$.

b) Is −301 odd?

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

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

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

Examples – cont.

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

d) If a and b are integers, is 10a + 8b + 1 odd?

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) Is every integer either even or odd?

The answer is yes, although the proof is not obvious. We will show in Section 4.4 that this fact results from another fact known as the quotient-remainder theorem.

Outline

- Even and Odd Integers
- Prime and Composite Numbers
- Methods of Proof
- Direct Proof

Prime and Composite Numbers

- 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 $1 < s < n$.

Examples

- Use the definitions of prime and composite to justify your answers to the following questions.

a) Is 1 prime?

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

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

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.

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.

Examples

- Use the definitions of prime and composite to justify your answers to the following questions.

c) Write the first six prime numbers.

2, 3, 5, 7, 11, 13

d) Write the first six composite numbers.

4, 6, 8, 9, 10, 12

Outline

- Even and Odd Integers
- Prime and Composite Numbers
- Methods of Proof
- Direct Proof

Methods of Proof

	Method of Proof	Method of Disproof
Universal Statements $\forall x \in D, P(x)$	Direct Proof	Counterexample
Existential Statements $\exists x \in D \; such \; that \; P(x)$	One Example	Direct Proof of Negation

Disproving Universal Statements

- Disprove the following statement:

$$\forall a, b \in \mathbb{R}, \qquad a^2 = b^2 \rightarrow a = b$$

- Since it's a universal statement, the method for disproving it is through giving one counterexample.

  Suppose $a = 1$ and $b = -1$

  $1^2 = 1$ and $-1^2 = 1$, therefore $a^2 = b^2$

  However, $1 \neq -1$, therefore $a \neq b$

  Hence, the statement is false.

Disproving Universal Statements

- Disprove the following statement:

$$\forall a, b \in \mathbb{R}, \qquad a^2 = b^2 \rightarrow a = b$$

- Since it's a universal statement, the method for disproving it is through giving one counterexample.

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

Disproving Universal Statements

- Disprove the following statement:

$$\forall a, b \in \mathbb{R}, \qquad a^2 = b^2 \rightarrow a = b$$

- Since it's a universal statement, the method for disproving it is through giving one counterexample.

  We can produce an infinite number of examples, where $a = -b$ that would disprove this statement.

  However, we only need one example to disprove the statement.

  But, our example needs to be clear and concise.

Proving Universal Statement

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

  $\forall n \in Z$, if n is even and $4 \leq n \leq 26$, then n can be written as a sum of two prime numbers.

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

Method of Exhaustion

- We have shown that the method of exhaustion can be used to prove universal statement.
- However, sometimes it is very difficult to use this method when the domain we have is large.
- And when the domain is infinite, it is impossible to use this method.

- Universal statements with infinite domains make up the majority of mathematical statements. That's why we need a smarter way of proof.

Outline

- Even and Odd Integers
- Prime and Composite Numbers
- Methods of Proof
- Direct Proof

Method of Generalizing from the Generic Particular

- Let's play a game!
  - *Think of any positive integer.*
  - *Add 5 to it.*
  - *Multiply the result by 4.*
  - *Subtract 6.*
  - *Divide by 2.*
  - *Subtract twice the original number.*
- The number you have now is 7!

Method of Generalizing from the Generic Particular – cont.

- How does this trick work even when each of you picked a different number?

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.	|| |||||	$(2x + 7) - 2x = 7$

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.
  - *Particular: because it represents a single quantity*
  - *Arbitrarily chosen (or generic): (because any number whatsoever can be put in its place*

- 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*.

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.)

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 $x \in D\ and\ P(x)$.")

3. Show that the conclusion $Q(x)$ is true by using definitions, previously established results, and the rules for logical inference.

Example

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

Formal Restatement: ∀ integers m and n, if m and n are even then m + n is even.

Or $\forall m, n \in \mathbb{Z}, Even(m) \wedge Even(n) \rightarrow Even(m + n)$

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

We need to show that $m + n$ is even.

Example

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

Since m is even, we can say $m = 2i$ for some integer i.

Since n is even, we can say $n = 2j$ for some integer j.
$m + n = 2i + 2j = 2(i + j)$

$i + j = k$ is an integer because it is the summation of two integers.

Therefore, by definition of even integers, $m + n = 2k$, is an even integer.

And this is what we needed to show.

Disproving Existential Statement

- Disproving existential statements is done by proving that the negation of the existential statement is true.

- The negation of an existential statement is a universal statement.

$$\sim(\exists x \in D, such\ that\ P(x)) \equiv \forall x \in D, \sim P(x)$$

$\Longrightarrow$ we use direct proof methods to disprove existential statements.

Example

- Disprove that there is a positive integer n such that $n^2 + 3n + 2$ is prime.

- The negation of the statement is

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

Proof: Suppose n is any particular but arbitrarily chosen positive integer.

We will show that $n^2 + 3n + 2$ is not prime.

Example

- Disprove that there is a positive integer n such that $n^2 + 3n + 2$ is 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.

We also note 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.

And this is what we needed to show.

Directions for Writing Proofs of Universal Statements

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: you should explain the meaning of each variable used in your proof
4) Write your proof in complete, grammatically-correct sentences.
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.
6) Give a reason for each assertion in your proof.
7) Include the “little words and phrases” that make the logic of your arguments clear.
8) 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 to Avoid

- Arguing from examples.
- Using the same letter to mean two different things.
- Jumping to a conclusion without giving adequate reasoning.
- Circular reasoning, meaning to assume what is to be proved.
- Confusion between what is known and what is still to be shown.
- Use of any rather than some

Suppose m is a particular but arbitrarily chosen odd integer.
By definition of odd, m = 2a + 1 for ~~any~~ some integer a.

- Misuse of the word if.

Suppose p is a prime number.
~~If~~ Because p is prime, then p cannot be written as a product of two smaller positive integers.