CHAPTER 4
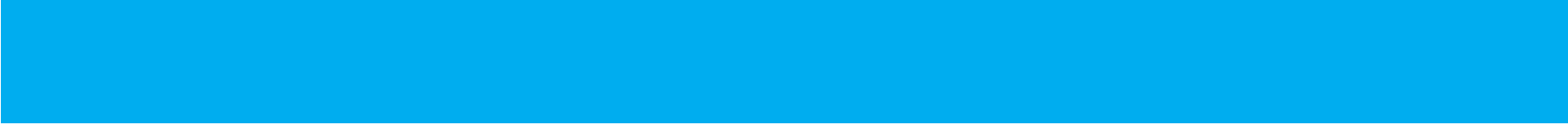
ELEMENTARY NUMBER THEORY AND METHODS OF PROOF

4.1 Direct Proof and Counterexample Ⅰ : Introduction

Even, Odd, Prime, and Composite Integers

Even, Odd, Prime, and Composite Integers

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, for any integer, n

$$n \text{ is even} \iff n = 2k \text{ for some integer } k$$

$$n \text{ is odd} \iff n = 2k + 1 \text{ for some integer } k$$

Example 4.1.1 – *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 10*a* + 8*b* + 1 odd?

e. Is every integer either even or odd?

Example 4.1.1 – *Solution*

a. Yes, 0 is even because 0 = 2 · 0.

b. Yes, −301 is odd because −301 = 2(−151) + 1 and −151 is an integer.

c. Yes, $6a^2b$ is even because $6a^2b = 2(3a^2b)$ and $3a^2b$ is an integer since it is a product of integers.

d. Yes, 10a + 8b + 1 is odd because

10a + 8b + 1 = 2(5a + 4b) + 1 and 5a + 4b is an integer since it is a sum of products of integers.

Example 4.1.1 – *Solution*

continued

e. Yes, every integer is either even or odd. However, the reason for this fact is not immediately apparent. It can be deduced using the method of proof by contradiction. It is also a consequence of the quotient-remainder theorem.

Even, Odd, Prime, and Composite Integers

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: For each integer n with $n > 1$,

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

$$n \text{ is composite} \iff \exists \text{ positive integers } r \text{ and } s \text{ such that } n = rs$$
$$\text{and } 1 < r < n \text{ and } 1 < s < n.$$

Proving Existential Statements

Proving Existential Statements

According to the definition, a statement in the form

$$\exists x \in D \text{ such that } Q(x)$$

is true if, and only if,

$$Q(x) \text{ is true for at least one } x \text{ in } D.$$

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 proofs of existence**. The logical principle underlying such a proof is called **existential generalization**.

Proving Existential Statements

It says that if you know a certain property is true for a particular object, then you may conclude that "there exists an object for which the property is true."

Example 4.1.3 – *Constructive Proofs of Existence*

a. Prove: ∃ 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: ∃ an integer k such that $22r + 18s = 2k$.

Example 4.1.3 – *Solution*

a. Let $n = 10$. Then $10 = 5 + 5 = 3 + 7$ and 3, 5, and 7 are all prime numbers. Thus $\exists$ an even integer—namely, 10—that can be written in two ways as a sum of two prime numbers.

b. Let $k = 11r + 9s$. Then k is an integer because it is a sum of products of integers, and by substitution, and the distributive law of algebra,

$$2k = 2(11r + 9s) = 22r + 18s.$$

Thus $\exists$ an integer, namely k, such that $22r + 18s = 2k$.

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

Disproving Universal Statements by Counterexample

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 4.1.4 – *Disproof by Counterexample*

Disprove the following statement by finding a counterexample:

$\forall$ real numbers a and b, if $a^2 = b^2$ then $a = b$.

Disproving Universal Statements by Counterexample

Statement: $\forall$ 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

Example 4.1.5 – *The Method of Exhaustion*

Use the method of exhaustion to prove the following statement:

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

Example 4.1.5 – *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 based on a logical principle sometimes called *universal generalization*. A more descriptive name is *generalizing from the generic particular*.

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.

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*.

Method of Direct Proof

1. Express the statement to be proved in the form "For every $x \in D$, 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 4.1.7 – *A Direct Proof of a Theorem*

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

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

Starting Point: Suppose m and n are any 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.

24

Example 4.1.7 – *Solution*

continued

Theorem 4.1.1

The sum of any two even integers is even.

Getting Proofs Started

Write the first sentence of a proof (the "starting point") and the last sentence of a proof (the "conclusion to be shown") for the following statement:

Every complete bipartite graph is connected.

27

Example 4.1.8 – *Solution*

It is helpful to rewrite the statement formally using a quantifier and a variable:

Formal Restatement: For every graph G, if G is complete bipartite, then G is connected.

(domain: graph G; hypothesis: G is complete bipartite; conclusion: G is connected)

The first sentence, or starting point, of a proof supposes the existence of an object (in this case G) in the domain (in this case the set of all graphs) that satisfies the hypothesis of the if-then part of the statement (in this case that G is complete bipartite). The conclusion to be shown is just the conclusion of the if-then part of the statement (in this case that G is connected).

Example 4.1.8 – *Solution*

Starting Point: Suppose G is a *[particular but arbitrarily chosen]* graph such that G is complete bipartite.

Conclusion to Be Shown: G is connected.

Thus,

the proof has the following shape:

Proof:

Suppose G is a *[particular but arbitrarily chosen]* graph such that G is complete bipartite.

⋮

Therefore, G is connected.

Example 4.1.9 – *Fill in the Blanks for a Proof*

Fill in the blanks in the proof of the following theorem.

Theorem: For all integers r and s, if r is even and s is odd then $3r + 2s$ is even.

Proof: Suppose r and s are any *[particular but arbitrarily chosen]* integers such that r is even, and s is odd.

[We must show that $3r + 2s$ is even.]

By $\underline{\quad(a)\quad}, r = 2m$ and $s = 2n + 1$ for some integers m and n.

Example 4.1.9 – *Fill in the Blanks for a Proof*

continued

Then

$$3r + 2s = 3(2m) + 2(2n + 1) \qquad \text{by } \underline{\quad(b)\quad}$$

$$= 6m + 4n + 2 \qquad \text{by multiplying out}$$

$$= 2(3m + 2n + 1) \qquad \text{by factoring out 2}$$

Let $t = 3m + 2n + 1$.

Then t is an integer because m, n, 3, 2, and 1 are integers and because $\underline{\quad(c)\quad}$.

Example 4.1.9 – *Solution*

Hence 3*r* + 2*s* = 2*t*, where *t* is an integer, and so by ___(d)___, 3*r* + 2*s* is even *[as was to be shown].*

(a) definition of even and odd, (b) substitution, (c) products and sums of integers are integers, (d) definition of even.