Chapter 1

Elementary Number Theory and Methods of Proof

1.1 Direct Proof and Counterexample I: Introduction

Definition 1: Even and Odd

An integer n in **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.

Definition 2: Prime and Composite

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 $1 < s < n$.

1.1.1 Proving Existential Statements

There are two ways to prove an existential statement: find one condition that satisfies the predicate, or give a set of directions for finding that condition. These methods are called **constructive proofs of existence**. A **nonconstructive proof of existence** shows that the condition satisfying the predicate is guaranteed from some axiom/theorem, or showing that the lack of such a condition would lead to a contradiction.

1.1.2 Disproving Universal Statements

Definition 3: Disproof by Counterexample

To disprove a universal statement of the form $\forall x \in D, P(x) \rightarrow Q(x)$, simply find an x for which $P(x)$ is true and $Q(x)$ is false.

1.1.3 Proving Universal Statements

The **Method of Exhaustion**, although impractical, can work for small domains. For more general cases, we use

Definition 4: Method of Generalizing from the Generic Particular

To show that every element of a set satisfies a certain property, show that a particular but arbitrary chosen x satisfies the property. When using this method on a universal conditional, this is known as the **method of direct proof**.

Definition 5: 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.

1.1.4 Proof Guidelines

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.
4. Write your proof in complete, grammatically correct sentences.
5. Keep your reader informed about the status of each statement in your proof.
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.
9. Note: be careful with using the word if. Use because instead if the premise is not in doubt.

1.1.5 Disproving Existential Statements

In order to prove that an existential statement is false, you simply have to prove that its negation is true.

1.2 Direct Proof and Counterexample II: Rational Numbers

Definition 6: Rational Number

A real number 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**.

Theorem 1: Rational Number Properties

- Every integer is a rational number.
- The sum of any two rational numbers is rational.

Definition 7: Corollary

A statement whose truth can be immediately deduced from a theorem that has already been proven.

1.3 Direct Proof and Counterexample III: Divisibility

Definition 8: Divisibility

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. The notation $d \mid n$ is read "d divides n". Symbolically,

$$d \mid n \leftrightarrow \exists k \in \mathbb{Z} \mid n = dk.$$

It then follows that

$$d \nmid n \leftrightarrow \forall k \in Z | n \neq dk.$$

1.3.1 The Unique Factorization of Integers Theorem

Because of its importance, this theorem is also called the *fundamental theorem of arithmetic*. It states 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. Formally,

Theorem 2: Unique Factorization of Integers

Given any integer $n > 1$ there exists 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

$$n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}.$$

When the values of p are ordered in non decreasing order, the above is known as the **standard factored form** of n.

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

Theorem 3: The Quotient-Remainder Theorem

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

$$n = dq + r, 0 \leq r < d.$$

Note that if n is negative, the remainder is still positive.

1.4.1 div and mod

From the quotient remainder theorem, div is the value q, and mod is the value r. Note that

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

1.4.2 Method of Proof by Division into Cases

To prove a statement of the form "If A_1 or A_2 or A_3 or $\ldots$ or A_n, then C prove that A_i for all $1 \leq i \leq n$ implies C. This is useful when a statement can be easily split into multiple statements that fully encompass the original statement.

Example 1

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

Proof (Brief). Suppose n is an odd integer. By the quotient remainder theorem and using the fact that the integer is odd, we can split the possible forms of n into two cases: $4q + 1$ or $4q + 3$ for some integer q. It can be proven through substitution that these two cases simplify to the form $n^2 = 8m + 1$.

1.4.3 Absolute Value and the Triangle Inequality

Definition 9: Absolute Value

For any real number x, the **absolute value of x** is defined as follows:

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases} \tag{1.1}$$