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 $\forall x \in D, P(x) \to Q(x)$, 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 $p_1, p_2, \dots p_k$, and positive integers $e_1, e_2, \dots e_k$ such that

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

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 $\dots$ 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:

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

Theorem 4: Triangle Inequality

For all real numbers x and y, $|x + y| \leq |x| + |y|$.

1.5 Indirect Argument: Contradiction and Contraposition

Proof by contradiction is extremely intuitive and exactly what it sounds like. Assume that the negation is true, and show that this assumption leads to a contradiction. Argument by contrapositive is equally intuitive given the fact that a statement is logically equivalent to its contrapositive. Note that proof by contraposition can only be used on universal conditionals.

Chapter 2

Sequences, Mathematical Induction, and Recursion

The proof chapter is finally over! I did not like that chapter D:

2.1 Sequences

Definition 10: Sequence

A **sequence** is a function whose domain is either all the integers between two given integers or all the integers greater than or equal to a given integer.

The first term of a sequence is known as the **initial term**, and the last term is known as the **final term**. An **explicit formula** or **general formula** is a rule that shows how the values of a_k depend on k.

2.1.1 Summation Notation

Definition 11: Summation Notation

For integers m and n where $m \leq n$,

$$\sum_{k=m}^{n} a_k = a_m + a_{m+1} + \ldots + a_n.$$

We call k the **index** of the summation, m the **lower limit** of the summation, and n the **upper limit** of the summation.
A recursive definition of summation notation:

$$\sum_{k=m}^{m} a_k = a_m \text{ and } \sum_{k=m}^{n} a_k = \sum_{k=m}^{n-1} a_k + a_n.$$

2.1.2 Product Notation

Definition 12: Product Notation

For integers m and n where $m \leq n$,

$$\prod_{k=m}^{n} a_k = a_m \cdot a_{m+1} \cdot \ldots \cdot a_n.$$

The recursive definition of product notation is in essence the same idea as the one in summation notation.

2.1.3 Properties of Summations and Products

Theorem 5: Properties

1. $\sum_{k=m}^{n} a_k + \sum_{k=m}^{n} b_k = \sum_{k=m}^{n}(a_k + b_k)$
2. $c \cdot \sum_{k=m}^{n} a_k = \sum_{k=m}^{n} c \cdot a_k$
3. $(\prod_{k=m}^{n} a_k) * (\prod_{k=m}^{n} b_k) = (\prod_{k=m}^{n}(a_k \cdot b_k))$

Substituting a new variable for k is simple. Change the limits by setting k equal to each of the limits and noting the new value, then change the expression itself by substituting k.

2.2 Mathematical Induction

The general structure of mathematical induction mirrors a line of thinking somewhat like a domino effect: If we can show that some property $P(n)$ is true for some integer a, and for all integers $k \geq a$, if $P(k)$ is true then $P(k+1)$ is true, then the statement "for all integers $n \geq a, P(n)$ is true. This is known as the **Principle of Mathematical Induction**. Showing that $P(n)$ is true for some integer a is known as the **basis step**, and proving that the truth of $P(k+1)$ follows from the truth of $P(k)$ is known as the **inductive step**.

Example 2: Sum of the First n Integers

For all integers $n \geq 1$,

$$1 + 2 + \ldots + n = \frac{n * (n+1)}{2}.$$

Proof (Brief). Let the property $P(n)$ be the given equation. It can be shown that $P(1)$ is true. We assume that $P(k)$ is true ($P(k)$ is known as the **inductive hypothesis**) and use the fact that $P(k) + k = P(k+1)$. Using algebraic manipulation, we find that $P(k+1)$ is true.

In general, use the inductive hypothesis to prove the inductive step.

2.3 Strong Mathematical Induction

Definition 13: Principle of Strong Mathematical Induction

Let $P(n)$ be a property that is defined for integers n, and let a and b be fixed integers with $a \leq b$. Suppose the following two statements are true:

1. $P(a), P(a+1), \ldots, P(b)$ are all true. (**basis step**)

2. For any integer $k \geq b$, if $P(i)$ is true for all integers i from a through k, then $P(k+1)$ is true. (**inductive step**)

Then the statement

$$\text{for all integers } n \geq a, P(n).$$

is true.

Example 3: Number of Multiplications Needed to Multiply n Numbers

Prove that for any integer $n \geq 1$, if $x_1, x_2, \ldots x_n$ are n numbers, then no matter how the parentheses are inserted into their product, the number of multiplications used to compute the product is $n-1$.

Proof (Brief). $P(1)$ is evidently true, as it takes 0 multiplications to multiply one number. Using the inductive hypothesis that $P(i)$ is true for all integers i from 1 to k, we now attempt to prove that $P(k+1)$ is also true. We do this by splitting the $k+1$ integers into two sides with l $(1 \leq l \leq k)$ factors on the left and r $(1 \leq r \leq k)$ factors on the right.

By inductive hypothesis, we note that we end up with $(l-1)+(r-1)+1 = l+r-1$ multiplications, which, when considering that $l+r = k+1$, proves the statement.

Definition 14: Well-Ordering Principle for the Integers

Let S be a set of integers containing one or more integers all of which are greater than some fixed integer. Then S has a least element.

A consequence of the well-ordering principle is the fact that any strictly decreasing sequence of nonnegative integers is finite. (This is because from the well-ordering principle, there must be some least element r_k, which is the final element, because if there were some term r_{k+1}, then $r_{k+1} < r_k$, which contradicts the well-ordering principle.

2.4 Recursion

Solving a problem recursively means to find a way to break it down into smaller subproblems each having the same form as the original problem.

Example 4: Tower of Hanoi

What is the least number of steps to move 64 golden disks from pole A to pole C (given the information that there are three poles, all the disks are different sizes, and at any point, discs on every pole must be in increasing order of size)?

The key observation here is to note that if we know the solution for $k-1$ discs, we can use this information to get the solution for k discs:

1. Move $k-1$ discs to pole B.
2. Move the bottom disc of pole A to pole C.
3. Move all the discs from pole B to pole C.

It then follows that we get the recurrence $m_k = 2m_{k-1} + 1$ where m_k is the number of moves to move k discs from one pole to another.

An explicit formula for this recurrence can be found through iteration and using the formula for the sum of a geometric sequence. From this, we get the formula $m_n = 2^n - 1$.

2.4.1 Checking the Correctness of Explicit Formulas

We can use mathematical induction to check the correctness of explicit formulas. For example, we can verify the formula for Tower of Hanoi by showing that it is true for 1 ring, and then showing that it is true for all $k+1$ assuming that k is true. Check your induction proof carefully to make sure that no mistakes were made, and that the recursive form as well as the explicit form were both used.