

1.7 Proofs

A *proof* is a valid argument that establishes the truth of a mathematical statement. It makes use of the hypothesis of the statement (if there are any), axioms assumed to be true, definitions of terms, and previously proven statements. Using these ingredients and rules of inference, the final step of the proof establishes the truth of the statement.

- A *theorem* is a statement that can be shown to be true. It is usually reserved for statements that are considered to be important. Less important statements are sometimes called *propositions*, *results*, *facts*, etc.
- A less important statement that is helpful in proving a theorem is called a *lemma*.
- A *corollary* is a result that can be established directly from a theorem that has just been proved.
- An *axiom* or *postulate* is a statement that is assumed to be true. For example, Euclidean geometry is based on five axioms one of which is “Any two points can be joined by a straight line.”

Some useful definitions

1. An integer n is *even* if there is an integer k so that $n = 2k$, and n is *odd* if there is an integer k so that $n = 2k + 1$. (Hence, an integer is either even or odd but not both.)
2. A real number r is *rational* if there are integers p and q with $q \neq 0$ such that $r = \frac{p}{q}$. A real number that is not rational is called *irrational*.
3. Let a and b be integers. We say that a is *divisible* by b provided there is an integer c so that $a = bc$. In this case, we also say that b *divides* a , and b is a *divisor* of a . The notation is $b|a$.
4. Let p be an integer such that $p > 1$. We say that p is *prime* if the only divisors of p are 1 and p . Otherwise, p is *composite*. (Note: 1 is neither prime nor composite!)

Understanding how theorems are stated

Many theorems are implications – e.g., if some hypothesis is satisfied then some conclusion must follow. However, they are often not stated in the “if-then” format. One must then be able to identify what the hypothesis and conclusions are.

The square of an odd integer is odd.

Every even integer greater than 2 is the sum of two primes.

Strategies for proving theorems

1. Direct proof for “ $P \rightarrow Q$ ”.
Assume P is true. Show that Q is true.

Example: Prove that the square of an odd integer is odd.

Example: Let a, b and c be integers. Prove that if a divides b and a divides c then a divides $b + c$.

2. Indirect Proof for “ $P \rightarrow Q$ ”.

Assume $\neg Q$ is true. Show that $\neg P$ is true.

Example. Prove that if n is an integer and $n^3 + 5$ is odd, then n is even.

Example: Suppose a_1, a_2, \dots, a_n are integers between 0 and 50. If their average is 30, then some $a_i \geq 30$.

3. Proof by contradiction.

Main idea: If the statement is false, we will arrive at a contradiction; hence, the statement must be true.

Example: Prove that $\sqrt{2}$ is irrational.

The Pigeonhole Principle. (*Sec. 6.2*) If $n + 1$ objects are placed in n boxes, then there is one box that contains at least two objects.

Example: Suppose five points are placed in a unit square. Show that there are two points whose distance from each other is at most $\sqrt{2}/2$.

Example: Show that among $n + 1$ positive integers not exceeding $2n$, there must be an integer that divides one of the other integers.

4. Proof by cases.

Consider the different possibilities. This is based on the fact that

$$(p_1 \vee p_2 \vee \dots \vee p_n) \rightarrow q \equiv (p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \dots \wedge (p_n \rightarrow q).$$

Example: For any real numbers x and y , show that $|x||y| = |xy|$.

Example: Prove that if n is an integer not divisible by 3 then $n^2 = 3q + 1$ for some integer q .

Last example: Show that in a group of six people, there is always three people who know each other mutually or three people who don't know each other at all.