Mathematical Proofs

adapted from http://zimmer.csufresno.edu

Direct Proofs

Let's start with an example.

Example: Let's prove this theorem: $a \mid b \wedge b \mid c \Rightarrow a \mid c$

Proof. By our assumptions, and the definition of divisibility, there are natural numbers k_1 and k_2 such that $b = a \cdot k_1$ and $c = b \cdot k_2$. Thus, $c = b \cdot k_2 = = a \cdot k_1 \cdot k_2$. Let $k = k_1 \cdot k_2$. Now $k \in \mathbb{N}$ and $c = a \cdot k$, so by the definition of divisibility, $a \mid c$.

If P, Then Q

Most theorems (homework or test problems) that you want to prove are either explicitly or implicity in the form "If P, Then Q". In the previous example, $P = a \mid b \wedge b \mid c$ and $Q = a \mid c$ This is the standard form of a theorem (though it can be disguised). A direct proof should be thought of as a flow of implications beginning with P and ending with Q.

$$P \rightarrow ... \rightarrow Q$$

Most proofs are (and should be) direct proofs. Always try direct proof first, unless you have a good reason not to.

It Seems Too Easy

If you find a simple proof, and you are convinced of its correctness, then don't be shy about it. Many times proofs are simple and short.

In the theorem below, *n* perfect square is meant to be an integer in the form n^2 where n itself is an integer and an odd integer is any integer in the form $2a+1$ where $a \in \mathbb{Z}$.

Theorem. Every odd integer is the difference of two perfect squares.

Proof. Suppose $2a+1$ is an odd integer, then $2a+1 = (a+1)^2 - a^2$.

Where's the proof? It's there. It's just very short.

Proof by Contrapositive

Proof by contrapositive takes advantage of the logical equivalence between "P implies Q" and "Not Q implies Not P". So, to $P \rightarrow Q$ prove by the method of contrapositive means to prove $\sim P \rightarrow \sim Q$.

Example: Here is a simple example that illustrates the method. The proof will use the following definitions.

Definitions.

1. $n \in \mathbb{Z}$ is **even** (respectively **odd**) if $\exists k \in \mathbb{Z} : n = 2k \ \ (resp. n = 2k+1)$.
2. Two integers are said to have the same **parity** if they are both odd or both even.

For the purpose of this example we will assume as proved that each integer is either even or odd.

Theorem. If n and m are two integers for which $n+m$ is even, then n and m have the same parity.

Proof. The contrapositive version of this theorem is "If n and m are two integers with opposite parity, then their sum must be odd." So we assume n and m have opposite parity. Since one of these integers is even and the other odd, there is no loss of generality to suppose n is even and m is odd. Thus, there are integers k and m for which $n = 2k$ and $m = 2l+1$. Now then, we compute the sum $m+n = 2k+2l+1 = 2(k+l)+1$, which is an odd integer by definition.

Proof by Contradiction

To prove a statement by contradiction, start by assuming the opposite of what you would like to prove. Then show that the consequences of this premise are impossible. This means that your original statement must be true.

Example: Prove the by contradiction that there is no greatest integer.

Proof: Suppose not. [We take the negation of the theorem and suppose it to be true.] Suppose there is greatest integer N. [We must deduce a contradiction.] Then $\forall n \in \mathbb{N}, \ N \geq n$ Now suppose $M = N + 1$. Then, M is an integer. Also, $M > N$. Therefore, M is an integer that is greater than the greatest integer. This contradicts the supposition that $N \geq n$ for every integer n. [Hence, the supposition is false and the statement is true.] And this completes the proof.

One of the first proofs by contradiction is attributed to Euclid.

Theorem. There are infinitely many prime numbers.

Proof. Assume to the contrary that there are only finitely many prime numbers, and all of them are listed as follows: $p_1, p_2, \ldots, p_n$. Consider the number $q = p_1 \cdot p_2 \ldots p_n + 1$. The number q is either prime or composite. If we divided any of the listed primes p_i into q, there would result a remainder of 1 for each $i = 1, 2, \ldots, n$. Thus, q cannot be composite. We conclude that q is a prime number, not among the primes listed above, contradicting our assumption that all primes are in the list $p_1, p_2, \ldots, p_n$.

Exercises

Use direct proof to show that the following statements hold for all natural numbers:

1. $2 \mid (t^2 - t)$
2. $2 \mid (n^2 - 3n)$
3. $3 \mid (t^3 - t)$
4. $3 \mid (n^3 + 2n)$
5. $5 \mid (t^5 - t)$
6. $6 \mid (n^3 - n)$
7. $4 \mid (n^4 - n^2)$
8. $4 \mid (n^4 + 3n^2)$

Prove directly using statements from previous exercises:

9. $12 \mid (n^4 - n^2)$
10. $30 \mid (n^5 - n)$
11. $6 \mid (n^3 + 11n)$
12. $12 \mid (n^5 - n^3)$
13. $15 \mid (n^5 - n)$
14. $15 \mid (n^6 - n^2)$

Use proof by contrapositive to show that the following implications hold $\forall n \in \mathbb{N}$:

15. $3 \nmid n \rightarrow 9 \nmid n$
16. $10 \nmid n \rightarrow 20 \nmid n$
17. $5 \mid (n^2 + 6) \rightarrow 5 \nmid n^2$
18. $3 \mid (n^2 + 2) \rightarrow 3 \nmid n$
19. $3 \mid (n^2 + 1) \rightarrow 6 \nmid n$
20. $10 \mid (n^2 + 6) \rightarrow 5 \nmid n$
21. $5 \mid (n^2 + 1) \rightarrow 10 \nmid n$
22. n^2 is even $\rightarrow n$ is even
23. n^2 is odd $\rightarrow n$ is odd
24. $6 \mid n \rightarrow 3 \mid n$
25. $4 \mid n^2 \rightarrow 2 \mid n$
26. $3 \nmid (n^4 + 2) \rightarrow 3 \mid n$
27. $3 \nmid (n^4 - 1) \rightarrow 3 \mid n$

★ *Prove by contradiction:*

28. The set $\mathbb{N}$ is infinite.
29. There is no least positive rational number.
30. $\sqrt{2} \notin \mathbb{Q}$
31. $\sqrt{3} \notin \mathbb{Q}$