ON PROOFS

Proofs are deductive arguments for mathematical statements. We can usually trace them back to a set of axioms, and they use formal logic.

Axioms (or postulates) are starting points – they are statements that we take to be true.

Example. In Euclidean geometry, we use Euclids postulates (e.g., *A straight line segment can be drawn joining any two points* or *Any straight line segment can be extended indefinitely in a straight line*).

Some Types of Proofs

- **Direct:** Direct proofs take the hypothesis of the statement to directly establish the conclusion.

  Example. The sum of two even integers is even.
  Proof. Let a and b be two even integers. By definition of even, we can write $a = 2m$ and $b = 2n$ for the integers m and n. Consider $a + b = 2m + 2n = 2(m + n)$, which is an even integer. □

- **Contrapositive:** If we want to show: "If p, then q", we instead show: "If not q, then not p."

  Example. If x^2 is an even integer, then x is even.
  Proof. We show the contrapositive: if x is not even, then x^2 is not even. Suppose x is not an even integer. Then it must be odd. We can write it as $2m + 1$ for some integer m. Consider $x^2 = (2m + 1)^2 = 4m^2 + 4m + 1 = 2(2m^2 + 2m) + 1$, which is an odd number. Thus, x^2 is not even. □

- **Contradiction (reductio ad absurdum):** If we assume a statement is true, then a logical contradiction occurs and so the original statement must actually be false.

  Example. For a real number x, if $x^2 = 0$, then $x = 0$.
  Proof. For a real number x, suppose that $x^2 = 0$ and that $x \neq 0$. Consider the equation $x^2 = 0$ and multiply both sides by $1/x$.
  Then we have $x^2(1/x) = 0(1/x)$ or that $x = 0$, which is a contradiction with our original assumption. Thus, $x = 0$ must actually be true. □

- **Construction:** These proofs are used to show the existence of a mathematical object by giving a method for creating it.

  Example. There exists an even integer that can be written in two ways as the sum of two prime numbers.
  Proof. We only need to provide an example that this object exists. Take the number 10. $10 = 5 + 5$ and $10 = 3 + 7$. Thus, there exists an even integer that can be written in two ways as the sum of two primes. □

- **Exhaustion (brute force):** We split our statement into a set of finite cases and check each case.

Example. The Four Color Theorem (motivated by map-coloring) was proven by exhaustion. See: `http://en.wikipedia.org/wiki/Four_color_theorem`.

- **Induction:** A proof by induction is just like an ordinary proof in which every step must be justified. However it employs a neat trick which allows you to prove a statement about an arbitrary number n by first proving it is true when $n = 1$ and then assuming it is true for n and showing it is true for $n + 1$.

  Example. $1 + 2 + 4 + \cdots + 2^{n-1} = 2^n - 1$.
  Proof. Base case: for $n = 1$, we have 1 on the left hand side and $2^1 - 1 = 1$ on the right hand side.
  Assume the statement is true for our inductive hypothesis. We want to show that the statement holds for $n + 1$.
  Take $1 + 2 + 4 + \cdots + 2^{n-1} = 2^n - 1$ and add 2^n to both sides. We get

  $$1 + 2 + 4 + \cdots + 2^{n-1} + 2^n = 2^n - 1 + 2^n$$

  $$1 + 2 + 4 + \cdots + 2^n = 2(2^n) - 1 = 2^{n+1} - 1.$$

  So the statement is true for n + 1. □

Ending a Proof

It is typical to end a proof with one of the following:

- QED (Quod Erat Demonstrandum) that which was to be shown
- □ the halmos (tombstone) symbol

Other Comments

- Quantifiers are important.
  For instance, the phrase "for every x" (sometimes "for all x") is called a universal quantifier and is denoted by $\forall x$. The phrase "there exists an x such that" is called an existential quantifier and is denoted by $\exists x$. A statement that contains variables is not simply true or false unless each of these variables is bound by a quantifier. If a variable is not bound, the truth of the formula is contingent on the value assigned to the variable from the universe of discourse.

- A theorem cannot be proved by example; however, to show that a statement is not true, a counterexample is used.

- Never assume any hypothesis that is not explicitly stated in the theorem.

- Sometimes it is easier to prove the contrapositive of a statement (see above).

- If you need to show that an object exists and is unique, first show that there actually is such an object. To show its uniqueness, assume that there are two such objects and show that they are the same.