PROOFS

In mathematics, a **proof** is a demonstration that, assuming certain axioms, some statement is necessarily true. A proof is a logical argument, not an empirical one. That is, one must demonstrate that a proposition is true in all cases before it is considered a theorem of mathematics.

Proving is based on reasoning. It is usually a multi-step process**.** Reasoning is a procedure of thoughts, when on the basis of knowing truth values of certain statements another statements may be considered true or false. The proof may consist of one single judgment/thinking, or it may be composed of more complicated judgments.

What is a proof?

A proof tests a hypothesis only in the sense of validating it once and for all. It is a sequence of statements, each of which is either validly derived from those preceding it or is an axiom or assumption, and the final member of which, the *conclusion*, is the statement of which the truth is thereby established. Proof is a chain of reasoning using rules of inference, ultimately based on a set of axioms, which lead to a conclusion.

There are more types of proofs. We will prove statements of this type:

$\forall x \in M, A(x) \Rightarrow B(x)$

1. **DIRECT PROOF**

   The logical scheme of a direct proof follows a chain of implications valid for each $x \in M$.

   I.e. $\forall x \in M, A(x) \Rightarrow A_1(x), A_1(x) \Rightarrow A_2(x) \Rightarrow \ldots \Rightarrow A_n(x) \Rightarrow B(x)$

   So we may conclude that $A(x) \Rightarrow B(x)$ is true and valid for $\forall x \in M$.

   In direct proof, the conclusion is established by logically combining the axioms, definitions, and earlier theorems.

2. **INDIRECT PROOF = PROOF BY TRANSPOSITION**

   Now we utter an alterated implication $\forall x \in M; B'(x) \Rightarrow A'(x)$ and we will prove this by means of a chain of implications as in direct proof, i.e.

   $\forall \; x \in M; B'(x) \Rightarrow B_1(x) \Rightarrow B_2(x) \Rightarrow B_n(x) \Rightarrow A'(x)$.

   Since $B'(x) \Rightarrow A'(x)$ is true, we know that the original implication $A(x) \Rightarrow B(x)$ will have the *same* truth value, thus it will be true as well.

   Proof by transposition establishes the conclusion "if *p* then *q*" by proving the equivalent contrapositive statement "if *not q* then *not p*".

3. **PROOF BY CONTRADICTION**

This type of proof is based on uttering the negated statement to the given one. We will prove, that this negation is false, and therefore the original statement is true.

V: $\forall x \in M, A(x) \Rightarrow B(x)$

V': $\exists x \in M, A(x) \wedge B'(x)$

$[A(x) \wedge B'(x)] \Rightarrow C_1(x) \Rightarrow C_2(x) \Rightarrow \ldots \Rightarrow C(x)$, which is completely nonsense, i.e. we have come to the contradiction of the starting presuppositions. Since the result is false, then the presuppositions are false, and therefore the original statement is true.

In **proof by contradiction** (also known as *reductio ad absurdum*, Latin for "reduction into the absurd"), it is shown that if some statement were false, a logical contradiction occurs, hence the statement must be true. A famous example of a proof by contradiction shows that $\sqrt{2}$ is irrational:

Suppose that $\sqrt{2}$ is rational, so $\sqrt{2} = \frac{a}{b}$ where a and b are non-zero integers with no common factor (definition of rational number). Thus, $b\sqrt{2} = a$. Squaring both sides yields $2b^2 = a^2$. Since 2 divides the left hand side, 2 must also divide the right hand side (as they are equal and both integers). So a^2 is even, which implies that a must also be even. So we can write $a = 2c$, where c is also an integer. Substitution into the original equation yields $2b^2 = (2c)^2 = 4c^2$. Dividing both sides by 2 yields $b^2 = 2c^2$. But then, by the same argument as before, 2 divides b^2, so b must be even. However, if a and b are both even, they share a factor, namely 2. This contradicts our assumption, so we are forced to conclude that $\sqrt{2}$ is irrational.

4. **PROOF BY MATHEMATICAL INDUCTION**

These proofs are used for proving certain properties of natural numbers. If we need to prove, that some statement is valid for all natural numbers n, then it will be enough to prove, that

1) the statement is true for n = 1
2) and if the statement is true for n, then it is true for n + 1 as well.

In **proof by induction**, first a "base case" is proved, and then an "induction rule" is used to prove a series of other cases. Since the base case is true, the infinity of other cases must also be true, even if all of them cannot be proved directly because of their infinite number.

The principle of mathematical induction states that: Let *N* { 1, 2, 3, 4, ... } be the set of natural numbers and ***P(n)*** be a mathematical statement involving the natural number n belonging to **N** such that ***(i)*** *P(1)* is true, ie, *P(n)* is true for n=1 ***(ii)*** *P(m+1)* is true whenever P(m) is true, ie, *P(m)* is true implies that *P(m+1)* is true. **Then *P(n)* is true for the set of natural numbers N.**

MI is a way of *proving* math statements for all integers (perhaps excluding a finite number.)
Statements proven by math induction all depend on an integer, say, n. For example,
(1) $1 + 3 + 5 + ... + (2n-1) = n^2$
(2) If $x_1, x_2, ..., x_n > 0$ then $(x_1 + x_2 + ... + x_n)/n \geq (x_1 \cdot x_2 \cdot ... \cdot x_n)^{1/n}$
etc. n here is an "arbitrary" integer.
Assume you want to prove that for some statement P, P(n) is true for all n starting with n = 1.
The *Principle* of *Math Induction* states that, to this end, one should accomplish just two steps:
Prove that P(1) is true.
Assume that P(k) is true for some *k*. Derive from here that P(k+1) is also true.
The idea of MI is that a finite number of steps may be needed to prove an infinite number of statements P(1), P(2), P(3), ... Therefore, P(n) is true for all n starting with 1.
Intuitively, the inductive (second) step allows one to say, look P(1) is true and implies P(2). Therefore P(2) is true. But P(2) implies P(3). Therefore P(3) is true which implies P(4) and so on. Math induction is just a shortcut that collapses an infinite number of such steps into the two above.