Tutorial #5: Methods of Proof

What is Proof? A carefully reasoned argument to convince a skeptical listener

Importance: It is difficult to overestimate the importance of proofs in mathematics. If you have a conjecture, the only way that you can safely be sure that it is true, is by presenting a valid mathematical proof.

Formally, "A mathematical proof of a statement is a chain of logical deductions leading to the statement from a base set of axioms".

There are different ways of Proof any statement, such as Theorems, Propositions, Axioms, Lemma's etc.

Propositions that are simply accepted as true, e.g. "there is a straight line segment between every pair of points".

There are different ways of Proofs, but the basic thing is your "Understanding" the methods that is a key component of learning how to read and construct mathematical proofs.

Once you choose a method, axioms, definitions, previously proved results, and rules of inference are used to complete the proof.

Let's consider the following well known mathematical theorem:

Theorem 1: For those of you who don't remember, a prime number is a positive integer $p > 1$ that cannot be written as a product of two strictly smaller positive integers **a** and **b**.

For example, the number 91 is not prime since it can be written as 91 = 13*7, but 67 is a prime.

Although most people have a hunch that there are infinitely many primes, it is not obvious at all.

Even today with the powerful computers, all we can do is to verify that there are very large prime numbers, but we still can say nothing about the existence of prime numbers whom size is beyond the ability of the current computers. The only reason that we are one hundred percent sure that the theorem is true, is because a mathematical proof was presented by Euclid some 2300 years ago.

What is the Mathematical Proof? The Rules of the Game: All of you are aware of the fact that in mathematics "we should follow the rules." This is indeed the case of writing a mathematical proof. Before we see how proofs work, let us introduce the "rules of the game".

Mathematics is composed of statements. The Law of the *excluded middle* says that every statement must be either true of false, never both or none. If it is not true, then it is considered to be false.

For example, consider the statement $y = x^2$.

In real life's terminology, like with most statements, it is sometimes true and sometimes false. In mathematics, it is false since it is not completely true. **Take for example** y = 1 and x = 2.

We can make up new statements from old ones. If P and Q are statements, then we have.

Statement	**Notations**
P and Q	$P \wedge Q$ (or P & Q)
P or Q	$P \vee Q$
If P Then Q (or P implies Q)	$P \Rightarrow Q$
P if and only if Q (or P and Q are equivalent)	$P \Longleftrightarrow Q$
not P	$\neg P$

The statement $\mathbf{P \wedge Q}$ is true if and only if both P and Q are true.

The statement $\mathbf{P \vee Q}$ is true if and only if at least one of the statements P, Q is true.

This is what we called the inclusive or as opposed to the exclusive or that we use in everyday's life. **For example**, the statement: "**We will have class in the morning or in the afternoon**" means in real life that only one of the alternatives will take places (exclusive or).

In mathematics however, this includes the possibility that we will have class in the morning as well as in the afternoon (inclusive or).

$\mathbf{P \Rightarrow Q}$ is considered to be false only in the case that P is true and Q is false. Otherwise, it is true.

This is also in contrast to the plain English.

For example, a statement like: "If it rains now then 2 is a prime number" is mathematically true, despite the fact that there is no relation between the two parts of the statement, and regardless of whether the first part is true or not.

The statement $\mathbf{P \Longleftrightarrow Q}$ is true if and only if P and Q have the same truth-values. We also say that P and Q are equivalent.

Finally, $\mathbf{\neg P}$ is true if and only if P is false.

Using the above operations, we can make more complex statements like,

$$\mathbf{((\neg (P \Rightarrow Q) \vee (T \wedge P)) \Longleftrightarrow (R \Rightarrow \neg T)}$$

Two additional players in this game are the quantifiers, $\forall$ and $\exists$. **For example,** the statement $\forall x > 0 \; \exists y(y^2 = x)$, reads: For all $x > 0$ there exists y such that $y^2 = x$.

Let us denote by Z^+ the set of all positive integers. The following statement about $p \in Z^+$ says that p is a prime:

$$\forall\, a \in Z^+ \forall\, b \in Z^+ [p = ab \Rightarrow (a = 1) \vee (b = 1)]$$

Tautologies and Contradictions: Logical deductions are based tautologies. If we try to give an informal definition, a tautology is a general statement that is true under all possible circumstances.
Examples are $P \Rightarrow P$, $P \Rightarrow \sim P$, Modus Ponens: $[P \wedge (P \Rightarrow Q)] \Rightarrow Q$ or another form of Modus Ponens: $[(P \Rightarrow Q) \wedge (Q \Rightarrow R)] \Rightarrow (P \Rightarrow R)$.
Notice that the truth of each of these statements is independent of whatever are P and Q and R and whether they are true or false. We can establish a tautology by our understanding of the statement or by constructing a truth table.
A logical deduction is obtained by substituting in a tautology.
For example, look at the following deduction: All fish are living creatures; All living creatures can move; Therefore all fish can move.
This logical deduction is a substitution in the second form of Modus Ponens where P= "x is a fish"; Q="x is an living creature"; R="x can move".
On the other extreme of logical statements are the contradictions. Contradictions are false under all circumstances. In fact every contradiction is the negation of a tautology, and conversely, every tautology is the negation of a contradiction. A typical contradiction is $P \wedge \sim P$.
Try to think yourself of some other examples.

Direct proofs leads from premises to the conclusion of a theorem, however sometimes attempts at direct proof lead to dead ends.

Indirect Proof: Proof by Contrapositive is an example of indirect proof. Another common kind of indirect proof is "proof by contradiction".

Contrapositive: Proof by Contrapositive is an example of indirect proof. Another common kind of indirect proof is "proof by contradiction". "You show that if a proposition were false, then same false fact would be true."

Example: If r is irrational then sqrt(r) is also irrational?

Proof by Division into Cases: Suppose at some stage of a proof, we know that A_1 or A_2 or A_3 or … or A_n is true; want to deduce a conclusion C.

Use division into cases: Show $A_1 \rightarrow C$, $A_2 \rightarrow C$, …, $A_n \rightarrow C$. Conclude that C is true.

Proof by Contradiction: Suppose the statement to be proved is false. Show that this supposition logically leads to a contradiction. Conclude that the statement to be proved is true.