

Logic and Proof

What proving something means in mathematics

All of us have some inherent understanding of the nature of truth. A common act in communication is to evaluate the truthfulness of a statement we read or hear. In some sense, logic is an attempt to provide a formal framework in which truth can be discussed.

Definition 1. A *statement or proposition* is a sentence which is either true or false, but not both.

For example, “Canberra is the capital of Australia” is a proposition. In a sense, we assign a truth statement to the sentence. We (hopefully) assign the value true (T) to this proposition.

For pure mathematicians, logic plays a central role in the way they conduct research. Unlike in life, a statement *proved* to be true by a correct and rigorous argument in mathematics is true for ever. In life, this is not necessarily the case. For example, the truth value of the example we gave above could change in some possible future if Australians chose to move their capital to Sydney, say. From then on, the statement would be false (F).

But returning to logic and mathematicians, what is relevant for us here is the process by which something is proved in mathematics.

In most cases, the statement of a theorem or lemma (which means small theorem; i.e. not significant enough to warrant being called a theorem) takes the form:

If ⟨hypothesis⟩, then ⟨conclusion⟩.

Reading this, we have an implicit understanding of what is being said.

The hypothesis is the condition or set of conditions which must first be satisfied, the conclusion is the consequences of the conditions holding.

A statement of this form is known as an *implication* and denoted $p \rightarrow q$, where p is a symbol representing the hypothesis and q is a symbol representing the conclusion. Note that both p and q are themselves statements, each with their own (undetermined) truth value.

In a sense, a theorem is really the recording of a *true* proposition.

For mathematicians (and for you guys too!) the key part is how to go about establishing an implication is true. This is the fundamental part of proof.

So let us consider what it technically means to say “If p , then q ” is a true statement.

Firstly, do we care whether q is true or not if we start off with p being false? When we read “If p , then q ”, what truth value of p are we naturally concerned about?

The truth of the sentence “If p , then q ” really only concerns us when p is *true* so as far as we’re concerned, when p is false, we don’t really care what the truth value of q is. Since we want “If p , then q ” to be a true statement, we therefore define (for mathematical purposes) $p \rightarrow q$ to be true whenever p is false.

Now lets think about the case where we start off with p true. In that case, when we think of the statement “If p , then q ”, we naturally view it as true if q is true and false if q is false.

We can summarise with the following truth table:

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

A glance at the truth table shows that there is only one case where we view “If p , then q ” to be false: when p is T and q is F .

So to *prove* an implication is true we need only worry about showing that whenever p is true, q is true also.

What does this mean when we come to constructing a proof? It means that we *assume* the hypothesis is true and then try to show that the conclusion must be true as a consequence.

Let us work through an example – we need the following definition.

Definition 2. An integer n is *even* if there exists an integer k such that $n = 2k$. An integer n is *odd* if there exists an integer k such that $n = 2k + 1$. Alternatively, an integer n is odd if it is *not* even.

Theorem 3. Let n, m be integers. If n and m are odd, then nm is odd.

Proof. Remember, to prove this implication, we assume the hypothesis and show the conclusion is true. So...

Suppose n and m are odd. We want to show nm is odd. By the definition, there exist integers k and t such that $n = 2k + 1$ and $m = 2t + 1$ (if we used k for both we’d be making $n = m$). We have

$$\begin{aligned} nm &= (2k + 1)(2t + 1) \\ &= 4kt + 2t + 2k + 1 \\ &= 2(2kt + t + k) + 1 \\ &= 2s + 1, \end{aligned}$$

where $s = 2kt + t + k$ is an integer. It follows from the definition that nm is odd and so we have shown “If n and m are odd, then nm is odd”. \square

Converse and Contrapositive

When dealing with an implication $p \rightarrow q$, there are two associated implications of importance also: the converse and the contrapositive.

Definition 4. The *converse* of the implication $p \rightarrow q$ is

$$\text{Converse: } q \rightarrow p.$$

So for the converse you just swap the hypothesis with the conclusion.

The *contrapositive* of the implication $p \rightarrow q$ is

$$\text{Contrapositive: } \neg q \rightarrow \neg p.$$

So for the contrapositive you swap the hypothesis and conclusion but also change (negate) the truth value of each – so this reads “If *not* q , then *not* p ”.

Why are these important? The converse is sort of the opposite – exactly what we think of when we see converse in the English language. The contrapositive is actually a statement which is equivalent to the original implication. In other words $p \rightarrow q$ and $\neg q \rightarrow \neg p$ are either both true or both false. (Try it by constructing a truth table – extend the table above with columns for $\neg q$, $\neg p$ and $\neg q \rightarrow \neg p$.) So the contrapositive gives us an alternative way of proving an implication – if we’re having trouble proving an implication, we can try using the contrapositive instead.

We’ll use this approach to prove the converse of our first theorem.

Theorem 5. *Let n, m be integers. If nm is odd, then n and m are odd.*

Proof. What is the contrapositive of this statement? Swap the hypothesis and conclusion and negate each. So the contrapositive reads

“If not (n and m are odd), then not (nm is odd)”

or more clearly

“If n or m are even, then nm is even”.

We’ll prove this implication now – so assume hypothesis, show conclusion.

Suppose one of n or m is even. There are two cases: n is even, or m is even. (Note that both being even fits in either case and so we are covering all possibilities – this is crucial in a proof by cases such as this.)

If n is even, then $n = 2k$ for some integer k . Then $nm = 2km = 2s$ where $s = km$ is an integer. Hence nm is even.

Likewise, if m is even, then $m = 2k$ for some integer k and $nm = 2kn = 2s$ where $s = kn$ is an integer. Hence nm is even.

In either case, we find the conclusion of our contrapositive statement true. Hence the contrapositive is a true statement and so too must be the original implication, which is the statement in the theorem. \square

Finally, note that if we combine the original implication with its converse (i.e. we combine the two theorems we’ve established), we get the following all encompassing statement.

Theorem 6. *Let n, m be integers. Then nm is odd if and only if n and m are odd.*