

A (very brief) Introduction to Proofs ¹

“The unique feature that sets mathematics apart from other sciences, from philosophy, and indeed from all other forms of intellectual discourse, is the use of rigorous proof...It is proof that is our device for establishing the absolute and irrevocable truth of statements in our subject. This is the reason that we can depend on mathematics that was done by Euclid 2300 years ago as readily as we believe in the mathematics that is done today. No other discipline can make such an assertion.” ²

Definition. A **mathematical proof** is a mathematical argument which begins with known statements and proceeds by irrefutable logical steps to a conclusion which then must also be true.

Remark: It is crucial that you distinguish between the mathematical concept of *proof* and the much weaker notion used in everyday language. In mathematics, there is no such thing as a *reasonable* amount of doubt and so no amount of supporting evidence, however convincing, constitutes a mathematical proof. This is a key idea: while specific examples may support general statements, they cannot prove them.

Before we jump into proving things, we need to be aware of the certain vocabulary and “grammar” which underlies all mathematical proofs. In particular, logical words such as ‘or’ and ‘if...then’ have very precise definitions in mathematics which can differ slightly from everyday usage.

1 Propositional Logic

1.1 Statements

Definition. A **statement** is a sentence that is either true or false but not both.

Example 1. Determine whether the following are statements and, if so, whether they are true or false.

- a. 6 is an even integer.
- b. 4 is an odd integer.
- c. He is a college student.
- d. $x + y > 0$

1.2 Logical Operations

Similar to numerical operations (like ‘+’, ‘−’, etc.) which allow us to combine or modify numbers, logical operations (like ‘not’, ‘and’, etc.) let us combine and modify statements. For the following let p and q denote statements.

1. **Not** — ‘not p ’ is defined to be

- *true*, when p is false.
- *false*, when p is true.

The statement ‘not p ’ is called the **negation** of p .

2. **And** — ‘ p and q ’ is defined to be

- *true*, when *both* p and q are true.
- *false*, when at least one of p/q is false.

¹This is taken almost entirely from the handout *Introduction to mathematical arguments* by Michael Hutchings which can be found here: <http://math.berkeley.edu/~hutching/teach/113/proofs.pdf>.

²Steven G. Krantz, *The History and Concept of Mathematical Proof*.

3. **Or** — ‘ p or q ’ is defined to be

- *true*, when *at least one* of p/q is true.
- *false*, when both p and q are false.

In everyday English, ‘ p or q ’ is often used to express that either p is true or q is true, but not both. ‘Or’ should **never** be interpreted this way in mathematics.

4. **If...then** — ‘if p , then q ’ (alternatively, ‘ p implies q ’ or ‘ $p \Rightarrow q$ ’) is defined to be

- *true*, when p and q are both true *or* when p is false.
- *false*, when p is true and q is false.

If p is false, we say that $p \Rightarrow q$ is **vacuously true**.

Definition. Given a statement ‘ $p \Rightarrow q$ ’, we call the related statements ‘ $q \Rightarrow p$ ’ and ‘not $q \Rightarrow$ not p ’ its **converse** and **contrapositive** respectively.

Beginning proofs students often make the mistake of thinking that a statement ‘ $p \Rightarrow q$ ’ and its converse ‘ $q \Rightarrow p$ ’ are interchangeable. Sadly, this is not the case. However, it is true (and very useful) to note that ‘ $p \Rightarrow q$ ’ is interchangeable with its contrapositive ‘not $q \Rightarrow$ not p ’. They are in fact completely equivalent statements.

5. **If and only if** — ‘ p if and only if q ’ (alternatively, ‘ p iff q ’ or ‘ $p \Leftrightarrow q$ ’) is defined to be

- *true*, when p and q are both true *or* both false.
- *false*, when one of p/q is true and the other is false.

It is worthwhile to notice that ‘ p iff q ’ is the same as ‘($p \Rightarrow q$) and ($q \Rightarrow p$)’. When we have ‘ p iff q ’, we say that p and q are **logically equivalent**.

Example 2. Determine whether the statements are true or false.

- 5 is not odd and 6 is even.
- 5 is odd or 6 is not even.
- 5 is odd or 6 is even.
- If today is Monday, then I’m wearing cabbage.
- If the moon is made of cheese, then I’m wearing cabbage.
- Dogs are cats iff pigs fly.

1.3 Quantifiers

Consider the sentence ‘ x is even’. This is not a statement because its truth depends on the value of the unknown variable x . There are three basic ways to turn sentences like this into statements:

1. Specify the value of x : ‘When $x = 6$, x is even’.
2. Use ‘for all/any’: ‘For any integer x , x is even’.
3. Use ‘there is/exists’: ‘There exists an integer x such that x is even’.

The phrases ‘for all’ and ‘there exists’ are called **quantifiers**.

Notation: We denote a **universal** quantifier (i.e. for all/any/each/every) by \forall . Similarly, we denote an **existential** quantifier (i.e. there is/exists) by \exists .

These are very useful in making convoluted definitions and theorems precise.

Example 3. Formulate the following definitions and theorems using logical operation and quantifiers.

- a. Define: even number
- b. Define: odd number
- c. Theorem: A multiple of 4 is also a multiple of 2.

Notice that the order in which quantifiers appear is very important.

Example 4. Determine the truth of the statements.

- a. $\forall x \in \mathbb{Z}, \exists y \in \mathbb{Z}$ such that $x < y$.
- b. $\exists x \in \mathbb{Z}$ such that $\forall y \in \mathbb{Z}, x < y$.

1.4 How to Negate Statements

1. Negating 'not' — $\text{not}(\text{not } p) = p$
2. Negating 'and' — $\text{not}(p \text{ and } q) = (\text{not } p) \text{ or } (\text{not } q)$
3. Negating 'or' — $\text{not}(p \text{ or } q) = (\text{not } p) \text{ and } (\text{not } q)$
4. Negating 'if...then' — $\text{not}(p \Rightarrow q) = p \text{ and } (\text{not } q)$
5. Negating 'iff' — $\text{not}(p \Leftrightarrow q) = [p \text{ and } (\text{not } q)] \text{ or } [q \text{ and } (\text{not } p)]$
6. Negating ' \forall ' — $\text{not}[\forall x \in S, p(x)] = \exists x \in S, \text{not } p(x)$
7. Negating ' \exists ' — $\text{not}[\exists x \in S, p(x)] = \forall x \in S, \text{not } p(x)$

Example 5. Negate the following statement: $\forall x \in \mathbb{Z}, [(\exists y \in \mathbb{Z}, x = 3y + 1) \Rightarrow (\exists z \in \mathbb{Z}, x^2 = 3z + 1)]$

2 Basic Proof Methods

Not surprisingly, the most crucial step in constructing a proof is determining exactly what it is you are trying to show. Now that we've examined logical operations and quantifiers, the basic building blocks of definitions and theorems, this is relatively straightforward.

2.1 Translating from Informal to Formal Language

If we are able to determine how to prove something we need to be able to express it in the precise mathematical language that we've been studying.

Example 6. Rewrite each of the following statements using quantifiers and variables.

- a. Triangles have three sides.
- b. No dogs have wings.
- c. Some people are weird.
- d. If a real number is an integer, then it is also a rational number.
- e. An integer whose square is even is itself even.
- f. There is a prime number between every integer and its double.

Statement (f) is a good example of how the ordering of a sentence in “plain English” doesn't always agree with the correct logical ordering.

2.2 Common Types of Proofs

The first step in any proof is to clearly write out the statement that is to be proved (or disproved). For the sake of illustration, we'll assume the statement to be proved is of the form ‘ $\forall x \in S, p \Rightarrow q$ ’ (a very common type). Now there are several possible ways to try and prove this statement.

1. **Direct Proof** — Prove the statement ‘ $\forall x \in S, p \Rightarrow q$ ’ exactly as it is written.

Form: Let $x \in S$ be arbitrarily chosen.
 Suppose p is true.
 $\downarrow \cdots$ (body) $\cdots \downarrow$
 Thus q is true.

Example: Prove that the square of an even integer is even.

Claim: $\forall n \in \mathbb{Z}$, if n is even, then n^2 is even.
Proof: Let $n \in \mathbb{Z}$ be arbitrarily chosen.
 Suppose that n is even.
 Since n is even, $\exists k \in \mathbb{Z}$ st $n = 2k$.
 Then $n^2 = 4k^2 = 2(2k^2)$ where $2k^2 \in \mathbb{Z}$.
 Thus n^2 is even.

2. **Indirect Proof (Contrapositive)** — Prove the equivalent statement ‘ $\forall x \in S, (\text{not } q \Rightarrow \text{not } p)$ ’.

Form: Let $x \in S$ be arbitrarily chosen.
 Suppose q is false.
 $\downarrow \cdots$ (body) $\cdots \downarrow$
 Thus p is false.

Example: Prove that if the square of an integer is even, then so is that integer.

Claim: $\forall n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: (direct attempt) Let $n \in \mathbb{Z}$ be arbitrarily chosen.
 Suppose that n^2 is even.
 Since n^2 is even, $\exists k \in \mathbb{Z}$ st $n^2 = 2k$.
 Then $n = \pm\sqrt{2k} = \dots?$

Proof: (contrapositive) We proceed using the contrapositive.
 That is, we’d like to show that $\forall n \in \mathbb{Z}$, if n is odd, then n^2 is odd.

 Let $n \in \mathbb{Z}$ be arbitrarily chosen.
 Suppose that n is odd.
 Since n is odd, $\exists k \in \mathbb{Z}$ st $n = 2k + 1$.
 Then $n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ where $(2k^2 + 2k) \in \mathbb{Z}$.
 Thus n^2 is odd.

3. **Indirect Proof (Contradiction)** — Suppose the statement is false. Show this yields a contradiction.

Form: Suppose not. Suppose that there exists an $x \in S$ such that p and not q .
 $\downarrow \cdots$ (body) $\cdots \downarrow$
 This is a contradiction. Thus the original statement must be true.

Example: Prove that if the square of an integer is even, then so is that integer.

Claim: $\forall n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: (contradiction) Suppose not. Suppose $\exists n \in \mathbb{Z}$ st n^2 is even and n is odd.

 Since n is odd, $\exists k \in \mathbb{Z}$ st $n = 2k + 1$.
 Then $n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ where $(2k^2 + 2k) \in \mathbb{Z}$.
 Thus n^2 is odd. This contradicts our supposition that n^2 is even.
 Thus the original statement must be true.

We should also note how to disprove a statement like this (i.e. prove it is false).

4. **Disproof (Counterexample)** — Prove the negation of the statement is true.

Example: Disprove the claim that ‘ $\forall a, b \in \mathbb{Z}$, if $a^2 = b^2$ then $a = b$ ’.

Note: This means we need to prove that $\exists a, b \in \mathbb{Z}$ st $a^2 = b^2$ and $a \neq b$.

Disproof: Choose $a = 1$ and $b = -1$.
 Then $a^2 = b^2 = 1$ and $a \neq b$.
 Thus the original statement is false.

Example 7. Prove the following.

a. For any nonzero $x, y \in \mathbb{R}$ where $x + y = 1$, we have $\left(1 - \frac{1}{x}\right) \left(1 - \frac{1}{y}\right) = 1$.

b. For any positive $x, y \in \mathbb{R}$, we have $xy \leq \left(\frac{x+y}{2}\right)^2$ (arithmetic-geometric mean inequality).