How to Prove It

- What is a proof?
- What can I prove?
- What to do after you have the outline of your proof.
- More useful proof techniques.

What is a proof? A proof is a rigorous argument that some statement is true. Using only things that are established to be true, such as Theorems, Propositions, and Lemmas that have already been proven, and the definitions of the terms in use, a proof takes baby steps from one true statement to a consequence of it that should be obvious to the reader. A proof should be written in complete, grammatically correct sentences, or some combination of words and symbols that when replaced by the words they stand for form complete, grammatically correct sentences. This is not just important so that the proof can be read and verified by others, but also so that there is no doubt what is being assumed and what is being asserted.

What can I prove? Here are some general types of statements you can prove:

(1) $A = B$.
(2) P $\Rightarrow$ Q.
(3) P $\Leftrightarrow$ Q.
(4) Every W is a Q; every W has property Q.
(5) Some W is a Q; some W has property Q.
(6) No W is a Q; no W has property Q.
(7) $X \subseteq Y$.
(8) $X = Y$, where X and Y are sets.
(9) X is unique.
(10) There is a unique X.

(1). $A = B$**.** Example of this type of statement:

- $x^3 - 1 = (x-1)(x - \frac{1-\sqrt{-3}}{2})(x - \frac{1+\sqrt{-3}}{2})$.

How to prove it:

Start with one side of the equation, and keep changing it in ways that are obvious until it becomes the other side, OR change each side separately until they equal the same thing.

Outline of proof:

$$\begin{aligned} A &= \dots \\ &= \dots \\ &\ddots \\ &= B \end{aligned}$$

Example of outline:

$$\begin{aligned}(x-1)(x-\frac{1-\sqrt{-3}}{2})(x-\frac{1+\sqrt{-3}}{2}) &= \ldots \\ &= \ldots \\ &\ddots \\ &= x^3-1\end{aligned}$$

(2). P ⇒ Q.

Examples of this type of statement:

- If it is raining, then it is cloudy outside.
- If n is an even number greater than two, then n is composite.

Outline of a proof:

Assume that P. .... Therefore, Q.

Examples of outlines:

- Assume it if raining. ...Thus it is cloudy outside.
- Assume that n is an even number greater than two. ...Thus n is composite.

(3). P ⇔ Q. Examples of this type of statement:

- The jury will convict the defendant if and only if there is proof of guilt beyond a reasonable doubt.
- Two numbers m and n have no common factor if and only if their least common multiple is their product.

Outline of a proof:

Assume P. .... Therefore, Q. Now, assume Q. ...Therefore, P.

Examples of outlines:

- Suppose there if proof of guilt beyond a reasonable doubt. ...Thus, the jury will convict the defendant. Now, suppose the jury will convict the defendant. ...Thus, there is proof of guilt beyond a reasonable doubt.
- Assume m and n have no common factor. ...Thus, their LCM is mn. On the other hand, assume that the LCM of m and n is mn. ...Thus there is no common factor of m and n.

(4). Every W is a Q. Examples of this type of statement:

- Every rose is red.
- Every prime greater than two is odd.

Outline of a proof:

Let w[1] be a W. .... Thus w is a Q.

Examples of outlines:

- Let r be a rose. .... Thus r is red.
- Let p be a prime greater than two. .... Thus p is odd.

Alternatively, if you are proving something about every integer, or for each of infinitely many things listed by the integers, consider a proof by induction.

(5). Some W is a Q. Examples of this type of statement:

- Some rose is white.
- There exists an even prime number.

Outline of a proof:

Consider w[2] ...Hence w is a W....Hence w is also a Q. Thus there exists a W that is Q.

Examples of outlines:

- Consider this rose, R. .... Hence R is white, so R is a white rose.
- Consider the number 2....Thus 2 is prime. Note also that 2 is even. Thus, there is an even prime, namely, the prime 2.

Such a proof as above is called constructive. There are examples of nonconstructive existence theorems.

(6). No W is a Q. Examples of this type of statement:

- No rose is blue.
- No prime number greater than two is even.

This is saying exactly the same thing as “Every W is not a Q.” Replace “Q” with “not Q” and go to **(4)**.

Alternatively, consider a proof by contradiction, and go to **??**.

(7). $X \subseteq Y$. Examples of this type of statement:

- $\{D \mid D \text{ is a dog}\} \subseteq \{M \mid M \text{ is a mammal}\}$.
- $\mathbb{N} \subset \mathbb{Q}$.

Outline of a proof:

[1] Here, w is a variable for an arbitrary W.

[2] Here w is a particular thing.

Let $x \in X$. …Thus $x \in Y$.

Examples of outlines:

- Let $D \in \{D \mid D \text{ is a dog}\}$. …Thus $D \in \{M \mid M \text{ is a mammal}\}$.
- Let $n \in \mathbb{N}$. …Thus $n \in \mathbb{Q}$.

(8). $X = Y$**.** Examples of this type of statement:

- $\{x \mid x \text{ is a species of egg-laying mammals}\} = \{\text{platypus, echidna}\}$.
- $\{x \mid f(x) = 0\} = \{x \mid (f(x))^3 = 0\}$.

Outline of a proof:

Let $x \in X$. …Thus $x \in Y$. Let $y \in Y$. …Thus $y \in X$.

Examples of outlines:

- Let $x \in \{x \mid x \text{ is a species of egg-laying mammals}\}$ …Thus $x \in \{\text{platypus, echidna}\}$. Conversely, if $x \in \{\text{platypus, echidna}\}$, …so $x \in \{x \mid x \text{ is a species of egg-laying mammals}\}$.
  It is much better to write our proof in the following less awkward way:
  Let x be an egg-laying mammal. …Thus x is either a platypus or an echidna. Conversely if x is a platypus or an echidna, …so x is an egg-laying mammal.
  We will write the next outline in the less awkward way.
- Let x be such that $f(x) = 0$. …Thus, $(f(x))^3 = 0$. Conversely, suppose x is such that $(f(x))^3 = 0$. …Thus $f(x) = 0$.

(9). X is unique. Examples of this type of statement:

- There is at most one positive solution to $x^2 = a$.

Outline of a proof:

Suppose that x and y are X. …Thus $x = y$.

Example of outline:

- Suppose that x and y are positive numbers such that $x^2 = a$ and $y^2 = a$. …Thus, $x = y$.

(10). There is a unique X**.** Examples of this type of statement:

- One of the restaurants is good.
- There is a unique number x such that $x + a = a$ for all a.

Outline of a proof:

Consider x. …Thus x is an X so there exists an X. Now suppose that y is also an X. …Thus $y = x$.

Examples of outlines:

- Consider restaurant x. …Thus x is good. Now, if y is a good restaurant …so y is x.
- Consider the number 0. …Thus 0 has the property that $0 + a = a$ for all a. Now, suppose that $y + a = a$ for all a. …Thus $y = 0$.

What to do after you have the outline of your proof.

Odds are, the most useful thing for you to do now is USE THE DEFINTION(S) of the technical term(s) in the statement you are trying to prove. You may even want to write out the definition in the proof.

Examples:

- To prove: *Every prime greater than two is odd.*
  Let p be a prime number greater than two. By definition of prime number, p is a natural number not divisible by any natural number other than one or p. …Thus, p is odd.
- To prove: *There exists an even prime number.*
  Consider the number 2. Recall that a natural number is prime if the only natural numbers that divide it are 1 and itself.…Thus 2 is prime. Note also that 2 is even. Thus, there is an even prime, namely, the prime 2.
- To prove: $\mathbb{N} \subset \mathbb{Q}$.
  Let $n \in \mathbb{N}$. …Recall that $\mathbb{Q}$ is the set of numbers that can be written in the form $\frac{n}{m}$ for integers m and n. Thus, $n \in \mathbb{Q}$.

Note how the gaps in the …parts of the proofs are much smaller now. We can now fill them in.

Same examples:

- To prove: *Every prime greater than two is odd.*
  Let p be a prime number greater than two. By definition of prime number, p is a natural number not divisible by any natural number other than one or p. In particular, since $p \neq 2$, p is not divisible by 2. Thus, p is odd.
- To prove: *There exists an even prime number.*
  Consider the number 2. Recall that a natural number is prime if the only natural numbers that divide it are 1 and itself. The only natural number less than 2 is 1, so the only possible number that can divide 2 other than itself is 1. Thus 2 is prime. Note also that 2 is even. Thus, there is an even prime: the prime 2.
- To prove: $\mathbb{N} \subset \mathbb{Q}$.
  Let $n \in \mathbb{N}$. Rewrite $n = \frac{n}{1}$. Recall that $\mathbb{Q}$ is the set of numbers that can be written in the form $\frac{n}{m}$ for integers m and n. Thus, $n \in \mathbb{Q}$.

Some useful proof techniques.

(1). Proof by contradiction. We want to prove a certain `fact`. We assume that the `fact` is false, and try to reach a contradiction.

Fact: There are infinitely many prime numbers.

Proof: Suppose there are finitely many primes. We can now list all the prime numbers: say they are $P_1, \dots, P_n$, and P_n. What are the primes that divide the integer $P_1 \cdots P_n + 1$? Certainly not any of the primes in our list! Then there must be some other prime we did not list, which is a contradiction, because we listed all the primes!

Proof by contradiction is a useful technique when the *opposite* of what you are trying to prove is a statement you can get your hands on. In the example above, the *opposite* of the statement that there are infinitely many prime numbers is a useful hypothesis, since we can then get our hands on the finite set of all primes.

(2). Proof by contraposition. The *contrapositive* of the implication $A \Rightarrow B$ is the implication "`not` B" $\Rightarrow$ "`not` A". It is logically equivalent to the original $A \Rightarrow B$!

Fact: Let n be an integer. If n^2 is odd, then n is odd.

Proof: We will show the contrapositive statement: if n is *even*, then n^2 is *even*. Let n be even. By definition of even, can write $n = 2k$ for some k. Then, $n^2 = (2k)^2 = 2(2k^2)$ is even as well.

Proof by contraposition is useful when the conclusion of the implication (B) or moreover its opposite (`not` B) is easier to get your hands on than the hypothesis. In our example, it is a bit easier to understand when n is even or odd as opposed to n^2.

It is often useful to take the contrapositive in one direction of an "if and only if" statement. For example, to show something like "n^2 is odd if and only if n is odd", you may want to show "n is odd implies n^2 is odd" and "n is even implies n^2 is even."

(3). Proof by induction. We want to prove that all integers $n \geqslant$ `base number` has a certain property `P`. A proof by induction consists of the following steps:

1) Prove the **base case**: the `base number` has our property `P`.
2) Prove **induction step**: if an integer n has property `P`, then $n + 1$ also has property `P`.

These steps are enough to show that all integers $n \geqslant$ `base number` have property `P`.

Fact: For every $n \geqslant 1$, the sum of all integers between 1 and n is $\frac{n(n+1)}{2}$.

Proof: We will prove this statement by induction.

1) **Base case**:

$$1 = \frac{1 \cdot 2}{2}.$$

2) **Induction step**:

Suppose that $1 + \cdots + n = \frac{n(n+1)}{2}$ for some value of n. Then

$$\begin{aligned} 1 + \cdots + (n+1) &= (1 + \cdots + n) + (n+1) \\ &= \frac{n(n+1)}{2} + (n+1) \qquad\qquad \text{(by our induction hypothesis)} \\ &= \frac{n(n+1) + 2(n+1)}{2} \\ &= \frac{(n+1)(n+2)}{2} \end{aligned}$$