What is a proof?

When asked to "show" or "prove" something, you are being asked to supply an airtight logical argument leading *from* the hypothesis *to* the conclusion.

A written proof is a one-way conversation between the writer and the reader. This conversation takes place in English. To save space and time, mathematical symbols may be used to stand for words, but each mathematical symbol has a fixed, conventional word (or a small set of words) that it is allowed to substitute for; you are not free to make up your own (unless you explicitly state what you are defining your symbols). For example, "=" stands for "equals", "which equals", or "is equal to"; it does not stand for "Doing the next step in this problem, I arrive at the expression I'm writing to the right of the equals sign". Your written work should have the property that, when the conventional meanings of your symbols are substituted for the symbols themselves, the result is a collection of sentences, with correct grammar and punctuation, detailing the logical flow of the argument. Some useful mathematical abbreviations are the following:

- "$\forall$" stands for "for all", "for every", or "for each"
- "$\exists$" stands for "there exists" or "there exist"
- "$\Rightarrow$" stands for "implies" or "which implies"
- "$\Leftarrow$" stands for "which is implied by" (this can also be read "implies", if you read from right to left or from the bottom of a page up)
- "$\Longleftrightarrow$" stands for "if and only if" or "which is equivalent to"

When you see someone else's final proof, it may appear that he or she has pulled something out of thin air. This is a common misunderstanding of what's being asked in "show" and "prove" problems. Your approach to any such problem involves some *thought process*, which you hope will lead you to an *answer* (i.e. a proof). As far as the thought process goes, anything is valid—you can work backwards, make leaps of faith, make mistakes, etc. This is all okay because at this stage you are not claiming to have an answer. All you are doing is trying to collect facts and ideas that you will *later* assemble into an answer. This thought process is not what you are being asked to write down; you are only being asked to write down the final proof. When you write this down correctly, you are showing two things: (i) that you recognize what a valid proof is, and (ii) in all likelihood, you came upon your proof by an intelligent thought process, because the chance that you stumbled onto a correct proof by pure luck is very small.

There is no single method guaranteed always to lead you to a proof, but here are a few methods that work well in certain problems:

- If you're instructed "Show that this thing here is a widget", usually what you have to do is write down the definition of *widget* and check that this thing here meets all the criteria of the definition. If the problem reads "Show that this thing here is *not* a widget", you have to exhibit a property of widgets that this thing here lacks.

- In many instances, proof by contradiction works. The logic is as follows. You are asked to prove "If P is true, then Q is true." Start by assuming that P is true but Q is *false*. If, after a series of logical deductions, you reach a contradiction, then the assumption that Q is false must be wrong, and hence Q must be true. For an example, see Example 2 below (the part labeled "valid proof").

- Sometimes proof by induction works. This potentially applies when you are trying to prove something that can be expressed that a collection of statements S_n is true for every natural number n. (The *natural numbers* are the positive integers 1,2,3, ...) Proof by induction proceeds by first showing that S_1 is true, and then showing that whenever n is such that S_n is true (called the "inductive hypothesis"), then S_{n+1} is true. This proves what's wanted, because then S_1 true $\Rightarrow$ S_2 true $\Rightarrow$ S_3 true $\Rightarrow S_4$ true $\Rightarrow \ldots$.

  Example. Prove that for all $n \geq 1$, the sum of the first n natural numbers is $n(n+1)/2$.

  Proof. Let S_n be the statement that the sum of the first n natural numbers is $n(n+1)/2$. S_1 asserts that 1=1(1+1)/2, which is true. Suppose that n is such that S_n is true. Then the sum of the first $n+1$ natural numbers is $\frac{n(n+1)}{2} + (n+1) = (n+1)(\frac{n}{2}+1) = (n+1)\frac{n+2}{2} = (n+1)(n+2)/2$, so S_{n+1} is true. ∎

  Example Let $V = \mathcal{F}(\mathbf{R}, \mathbf{R})$ (the vector space of real-valued functions on the real line), let $n \geq 1$, and let $r_1, \ldots, r_n$ be distinct real numbers (*i.e.* $r_i \neq r_j$ if $i \neq j$). Define elements $f_i \in V$, $1 \leq i \leq n$, by $f_i(t) = e^{r_i t}$. Prove that the set of functions $\{f_1, \ldots, f_n\}$ is linearly independent.

  Proof. We proceed by induction on n. First let n=1. Let $r_1 \in \mathbf{R}$ and suppose c is a scalar for which $cf_1 = 0_V$, *i.e.* $ce^{r_1 t} = 0\ \forall t \in \mathbf{R}$. Multiplying by $e^{-r_1 t}$, we obtain $c = 0$. Hence $\{f_1\}$ is a linearly independent set.

  Now suppose that n is such that whenever $r_1, \ldots r_n$ are distinct, the set $\{f_1, \ldots, f_n\}$ is linearly independent. Let $r_1, \ldots, r_{n+1}$ be distinct real numbers; without loss of generality we may assume they are listed in increasing order ($r_{n+1} > r_n > r_{n-1} > \ldots > r_1$). Suppose $c_1, \ldots, c_{n+1}$ are scalars for which $c_1 f_1 + \ldots + c_n f_n + c_{n+1} f_{n+1} = 0_V$. Then for all $t \in \mathbf{R}$, $c_1 e^{r_1 t} + \ldots + c_n e^{r_n t} + c_{n+1} e^{r_{n+1} t} = 0$. Multiplying both sides by $e^{-r_{n+1} t}$, we obtain $c_1 e^{(r_1 - r_{n+1})t} + \ldots + c_n e^{(r_n - r_{n+1})t} + c_{n+1} = 0\ \forall t \in \mathbf{R}$. But $r_i - r_{n+1} < 0$ for $1 \leq i \leq n$, so taking the limit as $t \to \infty$ in the preceding equation, we have $0 + \ldots + 0 + c_{n+1} = 0$, so $c_{n+1} = 0$, and therefore $0_V = c_1 f_1 + \ldots + c_n f_n + c_{n+1} f_{n+1} = c_1 f_1 + \ldots + c_n f_n$. By the inductive hypothesis, $\{f_1, \ldots, f_n\}$ is linearly independent,

so $c_i = 0$ for $1 \leq i \leq n$. We've already shown that $c_{n+1} = 0$. Thus whenever $c_1 f_1 + \ldots + c_n f_n + c_{n+1} f_{n+1} = 0_V$, all the scalars c_i are zero. Hence $\{f_1, \ldots f_{n+1}\}$ is linearly independent. ∎

Other times, to find proofs you have to struggle to understand why something is true. Experience and thorough knowledge of examples are your best friends here. Another approach is to try to look for a counterexample of what you're being asked to prove. You should be able to find a reason why each of your attempted counterexamples fails.

For students in MAS 4105 who want to see examples of correctly written proofs, look at the proofs of Theorems, Propositions, etc., in your textbook (for example Propositions 1.1 and 1.2, and Theorem 1.3. Also look at the examples in sections 1.2 and 1.3. In each case, the argument showing that something is a vector space(or a subspace) is a proof, despite not being labeled as such.

Some pitfalls to avoid when doing proofs.

Here are a few common methods of non-proof that are often mistaken for proofs.

1. "Proof" by lack of contradiction (not to be confused with the valid method *proof by contradiction*).

   In this method, you start by assuming what was supposed to be your conclusion as your hypothesis, and then say that you're finished when you reach no contradiction. Here is an example.

   Example 1. Given that the total number of points scored in a certain Gator football game was 80, prove that the Gators scored 73 and their opponents scored 7.

   "Proof": $73 + 7 = 80$ $\surd$. ∎

   That we reached no contradiction shows only that the conclusion is *consistent* with the hypothesis, not that it *follows* from the hypothesis. In fact, what the argument actually proves is exactly the *converse* of what we were supposed to prove (it proves that *if* the Gators scored 73 and their opponents 7, *then* the total number of points scored was 80, not the other way around).

   This brings us to the next pitfall.

2. Proving the converse of what you are supposed to prove.

   The converse of a statement "if P then Q" is the statement "if Q then P". Students sometimes fall into this trap because of the way they were taught to "prove" trigonometric identities in high school. For example, suppose that you were asked to prove

the trigonometric identity $\sec^2 x = \tan^2 x + 1$, knowing that $\sin^2 x + \cos^2 x = 1$. The most natural thing in the world *for a thought process* is to start with the conclusion and work backwards: write down the equation $\sec^2 x = \tan^2 x + 1$; on the next line rewrite $\sec^2$ as $1/\cos^2$, and $\tan^2$ as $\sin^2/\cos^2$; on the next line multiply through by $\cos^2$ to obtain $1 = \cos^2 + \sin^2$, and then stop because you've reached an identity you know to be true. If you were to write this down as a logical sequence of operations, detailing what followed from what in your mind, you'd write

$$\begin{aligned} \sec^2 x &= \tan^2 x + 1, \\ \Rightarrow \frac{1}{\cos^2 x} &= \frac{\sin^2 x}{\cos^2 x} + 1, \\ \Rightarrow \quad 1 &= \sin^2 x + \cos^2 x. \end{aligned}$$

But this is not what you were told to prove! You were told to prove that $\sec^2 x = \tan^2 x + 1$, assuming $\sin^2 + \cos^2 x = 1$; what you did instead is to prove that $\sin^2 x + \cos^2 x = 1$, assuming $\sec^2 x = \tan^2 x + 1$. The actual argument you want reads from the bottom of what you wrote to the top, not the other way around. But any human being looking at what you wrote is going to read from the top down, not bottom up. So for the proof you were asked for you should rewrite the three lines above in the other order. Alternatively, you could have noticed that in the three lines above, the implications are still valid as if-and-only-if statements (each line is *logically equivalent* to the line before or after, which would not have been true if your first line had been, say, $x = 5$, and your second line, say, $x^2 = 25$). Then you could have gotten around the need to rewrite the argument, by simply replacing the "$\Rightarrow$" symbols by " $\Longleftrightarrow$ " symbols.

3. Starting a proof with an unconditional assertion of what you are supposed to be proving. This is a common mistake when you are asked to prove two things are equal. See "Proving the converse of what you are supposed to prove" above.

4. "Proof" by example. Suppose you are given the problem "Show that every even positive integer greater than two is the sum of two prime numbers." You observe that 4=2+2, 6=3+3, 8=3+5, 10=3+7, 12=5+7, 14=7+7, 16=5+11, 18=5+13, 20=7+13, etc. You list example after example. That still doesn't mean there isn't some even number you haven't listed that *isn't* the sum of two primes.

   Here's another example: "Prove that if n is prime, then $2^n - 1$ is prime". You start checking: $2^2 - 1 = 3$ is prime, $2^3 - 1 = 7$ is prime, $2^5 - 1 = 31$ is prime, $2^7 - 1 = 127$ is prime. You might now think the statement is true. But $2^{11} - 1 = 2047 = 23 \cdot 89$ is not prime. The statement you were told to prove is actually false!

5. "Proof" by notation. For example, you can't prove that addition of matrices is commutative by saying that since a + sign is used, the operation must be commutative.

6. "Proof" by lack of imagination. "I don't see how the theorem can possibly be false, so it must be true." Alternatively, "I don't know a counterexample, so the theorem must be true."

7. "Proofs" using math symbols for objects that do not exist. This is also related to "proof by gibberish".

   Example 2. Prove that there does not exist a real number x such that $0x = 1$.

   Invalid Proof: "If there were such a number, it would have to be $1/0$, which is undefined."

   The main reason this is invalid is that it relies on an undefined term. The secondary reason is that the argument makes the nonsensical assertion that something *has* to equal this undefined object. There is a big difference between reaching a contradiction, such as $1 = 2$, and thinking you've reached a contradiction just because you don't know how to make sense of what you've written!

   Valid Proof: "Assume there is such a number x. Then $0 = 0x = 1$, a contradiction. Hence no such x exists." ■

8. "Proof" by inapplicability of what you know. This is sometimes related to "proof by lack of imagination". The invalid proof above (in which something "had" to be $1/0$) is an example.

9. Writing all the correct steps for a proof, but writing them in an invalid order. (This is sometimes how people end up proving the converse of what they were supposed to prove.)

10. "Proof" by gibberish. There are two ways this generally happens. Remember that your proof should be readable as ordinary, grammatical English once the conventional word-substitutions are made for mathematical abbreviations. So you can go wrong two places: the English you actually write can be ambiguous or (in extreme cases) incomprehensible, or the English you get after making word-substitutions for the math symbols can have the same problem. See the handout "Mathematical Grammar and Correct Use of Terminology".

11. Assuming the reader can read your mind even if what you wrote does not make sense in English or means something wrong. This is related to "proof by gibberish"

12. "Proofs" based on assuming an empty set is nonempty. For an example, see Example 1 of the handout called "One-to-one, Onto, and What you are really doing when you solve equations."