

A Few Words About Proofs

What is a proof?

A proof is nothing more than a water-tight logical argument. There is no special way a proof has to look on a page (don't worry about the "two column" format they teach in high-school geometry). As long as you state precisely what you're trying to show, and then make your case logically and coherently, it counts as a proof.

How can you tell if an argument is good enough to be a proof? Imagine that your annoying (but clever) little sister is looking over your shoulder, always nagging at you: "And why is this? And how do you know that?" Whenever you say that something is obvious, she'll ask, "How come?". Whenever you are tempted to be a little vague, she'll say, "I don't get it—what do you mean by that?" If your argument passes the annoying little sister test, then it's a proof!

Proof pitfalls

- *The "obviously" claim.* Be very careful when you say that something is "obvious". This word rings a warning bell in the reader's mind, because too often people use it to cover up their ignorance. If by "obviously" you mean "my intuition tells me that this is so, but I can't quite explain why," then think again: that's not good enough!

On the other hand, if something is "obvious" because its justification is clear in your mind and you think that the reader can easily fill in the details, then you can choose to leave it without further explanation. Of course, every time you do this, you are taking a risk: the reader might not think it was so easy, and might suspect that you simply did not know how to justify your claim. So, if in doubt, always explain!

- *Backwards reasoning.* All too often in a proof, students will write down the thing they are trying to show, derive a true statement from it, and think they are done! (This happens most often when the claim to be demonstrated is an equation or an inequality, so that the bulk of the proof is a string of algebraic manipulations.) Such reasoning does *not* constitute a proof, even though it's usually not very difficult to turn it into one: just start with the true statement you ended with, and show that the desired result can be derived *from* it.
- *Losing the thread of the argument.* Always remember where your proof is heading, and say only what you need to get there. Some people try to write down as many true facts as they can, in the hope that at least one of them will be relevant. Not only does this make the proof difficult to follow, it also tells your reader that you don't really know what you're doing. Succinctness, in a proof, is key!

If the logical structure of your argument is very complicated, it might help to break it down into intermediate steps. For example, you might

first state and prove an auxiliary result (usually called a *lemma*), and then use this to prove your main claim. Even something as simple as labeling the steps in your argument and putting them into separate paragraphs can make your proof much easier to follow. Feel free to introduce new notation and symbols as well, if it contributes to the clarity of your presentation.

Not considering all the cases. Be sure that you pay attention to all the possibilities in a problem, not just the most obvious ones. If you're dividing by a number, did you check that it's not 0? If you have just solved a quadratic equation, did you remember to consider both solutions? If the problem asks you to prove something for all integers, did you consider the negative as well as the positives?

Examples vs. proofs You have probably been told many times that an example is not a proof, but this is not entirely correct. Indeed, if you are asked to prove that something is true *in general*, you must provide a general argument: no number of examples will suffice. On the other hand, if you want to prove that something is *not* always true, general arguments about why it doesn't have to be true are completely futile: in this case, the *only* correct proof is a single, concrete counterexample.

Another valid use of examples is to illustrate a complicated argument or definition. This is entirely optional, and no substitute for a clear exposition; but as long as it is clear that the examples are not an actual *part* of your argument, you are welcome to put them in for clarification.

Checking your work

Suppose you've written your proof, and looked over carefully it to check that you haven't fallen into any of the pitfalls listed above. Everything seems logical and clear, and even your annoying little sister is satisfied. Now what?

When the answer to a problem is a number, it is usually easy to check whether your solution is correct: just plug the number back in, and see if everything works out. But how do you check whether a *proof* is correct?

First make sure that what you're proving really is true: a proof of a false statement cannot possibly be right! Look for counterexamples to your claim. If you find one, plug it into your proof and see where things go wrong. Sometimes, it's easy to fix the problem: for example, maybe you just needed to specify that your claim holds only for positive integers, which is the only case you cared about anyway. But other times, you will discover a serious gap in your reasoning. Pay attention to exactly what went wrong with the counterexample—it might give you an idea of how to fix the mistake.

What if you're sure that the statement you're proving is true—for example, if the problem specifically asks you to prove it? In that case, reread statement of the problem carefully. Does your proof use *all* the information that you are given? If not, chances are that somewhere you are missing a step. For example, suppose that the problem is:

Show that for every prime number $p > 3$, $p^2 - 1$ is divisible by 24,

and you notice that in your solution, you never use the assumption that $p > 3$. Then your proof should, in theory, work for $p = 2$ as well! But $2^2 - 1 = 3$ is *not* divisible by 24, so you know you must have made a mistake somewhere. Go back through the proof, substituting 2 for p everywhere. At some point you'll get to a step that sounds ridiculous; that's the one you need to fix.

(Every year, the Department of Mathematics at Harvard University receives dozens of letters in which people claim to give an elementary proof of the celebrated Fermat's Last Theorem: $x^n + y^n = z^n$ has no non-trivial integer solutions for $n > 2$. But most of these "proofs" never even make use of the assumption that $n > 2$. There's no need to look for the exact place where such an argument fails: you know it can't be right, since $3^2 + 4^2 = 5^2$.)

Additional comments

- Potentially obscure theorems that help in the proof may be used, with appropriate references. It's also fine to use advanced material if this leads to a simpler solution of a problem stated in elementary terms. However, if the problem asks for a common theorem to be proved or follows immediately from a well-known result, then the theorem should be proved, not just cited. Don't trivialize the problem!
- Sometimes, a problem can be solved by lengthy exhaustive computer searches. Such solutions generally will not receive full credit since they defeat the mathematical purpose of the problem.

A few sample proofs and non-proofs

The Problem: You are given two boxes, A and B. Box A contains 100 white marbles, and box B contains 100 black marbles. First you take out 10 marbles from box A and put them into box B. Then you take out 10 marbles from box B and put them into box A. Which is now larger: the number of black marbles in box A or the number of white marbles in box B?

Solution 1: The two numbers are the same.

- *Comments:* This is the correct answer, but because no explanation is given, the solution will receive only partial credit at best!

Solution 2: The two numbers are the same. Even though not all the marbles we move from B to A might be black, if they are not all black then we must be moving some white marbles back to A. So both boxes will end up with fewer than 10 marbles of the "wrong" color in them, and they will have the same number of "wrong" marbles.

- *Comments:* This is the correct general idea, but much too vague for a proof. In particular, the final statement does not follow logically from anything that came before.

Solution 3: The two numbers are the same. Even though not all the marbles we move from B to A might be black, if they are not all black then we must be moving some white marbles back to A, so both boxes will end up with fewer than 10 marbles of the “wrong” color in them. For example, if among the 10 marbles we move from B to A, 3 are white and 7 are black, then A will end up with 7 black marbles, and B will have $10-3=7$ white marbles. Thus A and B will have the same number of marbles of the “wrong” color.

- *Comments:* This is better: it relies on an example to clarify the vague idea, and does succeed in conveying the intuition that the numbers really will be the same. However, an example is just not enough: a general argument is still missing.

Solution 4: After we have moved the 10 white marbles from A to B, the fraction of white marbles in B is $1/11$, which is close to $1/10$. So we expect approximately one out of the 10 marbles we move from A to B to be white. Thus, at the end, B is left with 9 white marbles, and A gets 9 black marbles. So the answer is: the numbers are the same.

- *Comments:* This solution brings in an irrelevant consideration—probability. Unless otherwise indicated, a problem always asks not for the most probable but for all possible solutions. Moreover, this solution assumes that between the two transfers of 10 marbles, the marbles in box B were thoroughly mixed—which is nowhere indicated in the statement of the problem!

Solution 5: If the batch of 10 marbles we moved from B to A contained k black ones and $10 - k$ white ones, then A, at the end, has k black marbles, and B has $10 - (10 - k) = k$ white marbles. Thus the two numbers are the same.

- *Comments:* A valid proof! Notice that it is shorter than any of the other solutions (except 1). An argument need not be long to make its point—it only needs to be logical and complete.