A Note on Proofs

Joe Rabinoff

October 4, 2002

I know you have heard people explain proofs before, but seeing as I'm one of the people who actually grades you on them, I figure I should tell you what I'm looking for. If you're confused about what a proof is or how to write one, then this note is for you.

A proof, at its base, is an argument. I assume that you know how to make persuasive arguments — everybody has had late-night philosophical debates with roommates. If you are asked to prove that, for instance, there are an infinite number of primes, then your job is to convince the reader of the truth of that statement. Therefore, your proof should read like an essay — it should be in grammatically-correct English, it should have a thesis, and it should have a logical argument. But there is an essential difference between a mathematical proof and a biology paper: a mathematical proof should be so precise that there is (theoretically) no room for error. None. It's not enough to find overwhelming evidence for a statement in order to prove its truth. You can leave no room to doubt that what you say is absolutely correct.

The proof then, were you to write it out in full, would be extremely long-winded, because every step must be meticulously exact. This is where mathematical notation comes in — common precise constructions like "for all x in the set A" can be shortened to "$\forall x \in A$." This is the first important point about writing proofs: were you to expand out all of the notation (i.e. replace each "$\exists x$" with "there exists an x"), *you should have a grammatically correct sentence.*

As with any argument, a proof is a logical path from a starting point to an ending point. So in order to write one, the first thing to do is start with a *precise statement of your assumptions* and work towards a *precisely stated conclusion*. By precise, I mean something totally unambiguous, with nothing left for interpretation. For example, "Every $n \in \mathbf{N}$ can be written as $n = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$ for some primes p_i and positive exponents a_i." For more examples, read the statements of the lemmas and theorems in your textbooks.

The only mathematical way to get from the assumptions to the conclusions is by making *precise logical deductions*, that is, statements that use facts that you know and imply other facts. Each statement should again be totally unambiguous, and have impeccable support, i.e. you must be able to justify each statement with a mathematical reason that *cannot* be argued, like a theorem out of a book (e.g. if p is prime and n is any natural number then there exists a maximal natural number m such that p^m divides n *because of the existence of*

prime factorizations). There cannot be any room for the reader to say "but what if" or "now why is that" — every statement must be infallible. This may at first seem pedantic, but if you think about it, it is the reason why mathematics is so beautiful in the first place — there is no other field of study where you can state conclusions that *cannot* be argued, that are purely true.

Of course, if you actually wrote *every* step, your proofs would be impossibly long even with generous use of math notation. For instance, you do not have to go back to first principles to say something like, "if a and b are positive then $ab > 0$" (but you do have to know how to justify such things from the axioms of the real numbers!). In each case, use your judgment about whether the logical leap you are about to make is small enough that it does not require further justification. You may think that I'm contradicting the hyperbole I wrote in the last paragraph (about leaving no room for questions), but what's really happening is that you're making sure that you leave out few enough logical steps that the reader can easily fill them in. (In this case, though, what you should consider is whether the grader will believe that *you* know how to fill them all in, and until you have more experience, we won't assume much.)

As for what not to do in a proof, the most obvious note is that a "proof" by example is *not* a proof. In fact, examples are almost utterly irrelevant in a proof, unless there are only a finite number of examples and you prove them all. You can not in general prove something by example. For instance, if you prove that 10 has a prime factorization $2 \cdot 5$, then that's great, but you haven't proved that 12 has a prime factorization too. If your proof for 10 generalizes to any natural number, then just write the general proof; I don't care about the specific case. It is often helpful to work out an example if you don't know how to prove something in general, but you do need to do the general proof afterwards. You can thus usually leave out your examples — if you find yourself needing to insert them for clarity (at this level at least) then you should usually just make your general proof more clear. If you do run into a situation where e.g. a definition would be made much more clear if you inserted an example, then use your judgment about whether or not to insert one; just make sure that you have treated the general case too, and that that really does work in general.

You can also almost always forego writing down your intuition for the problem. Don't get me wrong, mathematical intuition is the absolute most valuable thing a mathematician can have; it's what makes a problem concrete instead of a bunch of scrawls on paper. However, it is a means to an end, the end being a proof of something. In this class, all you are graded on is the end, so it is usually not very helpful to give a long exposition of your intuition (something like "intuitively, one would think that $x_n \to 0$, so we will work towards proving that" is probably the extent of what you should include). It is perhaps best to leave out intuitive realizations altogether at this point just so there is no chance of you or your reader confusing them with logical deductions.

Some more things not to do: be very careful that you don't at some point during a proof implicitly assume a result that follows from what you are trying to prove. That is circular reasoning. For instance, if you are going to prove that any integer n is divisible by some prime p, you cannot assume the existence

of prime factorizations, since the former is used to prove the latter. Also, the easiest way to confuse a reader is to use a variable that you didn't define. *Always* define your variables in the same sentence as you first used them.

Lastly, always remember that the reason you are writing a proof is so that someone else can read it. When you write a proof, read over it with the mindset of someone who's half as smart as you are and doesn't have any idea what you're talking about before your proof begins. If that person gets confused, you need to clarify.

I hope you find this helpful.