A Note on Proofs

Joe Rabinoff

August 23, 2010

> I originally wrote this note in the fall of 2002 for the benefit of the students taking Math 23a at Harvard University, who were under the excellent instruction of John Boller. Math 23 is a first-year class introducing rigorous calculus and linear algebra, and was designed to be the first experience most of its students had with pure math, and in particular, with proofs. Being a course assistant and grader, I wrote this note from a grader's perspective, immediately after having graded the first homework assignment.[1] It addresses the more important things one must do when writing proofs, and points out some common mistakes. If you've never written a mathematical proof before (and have some desire to do so), then this note is for you.

Problems in abstract mathematics generally involve proving a statement to be true or false. And unlike in a basic math class, finding a solution to one of these problems is only half the battle: afterwards you have to explain it to someone else. In other words, when the answer is "42" it's easy to write it down, but when the answer is a series of ideas that can be strung together to prove Fermat's Last Theorem, the exposition becomes much more difficult. I'm not going to talk about Step One (figuring out what the answer is) — I'm going to talk about Step Two, how to write a proof in a comprehensible way.

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, for instance, that there are an infinite number of prime numbers, then your job is to convince the reader of the truth of that statement. Your proof should read like any other written argument: it should have a thesis, it should have a logical progression, and it should be in grammatically-correct English.[2] But there is an essential difference between a mathematical proof and a philosophy paper: a mathematical proof should be so precise that there is (theoretically) no room for error. None. That's the beautiful thing about pure mathematics: it's the only subject in which you can be absolutely sure of the truth of your statements. It's not enough to find overwhelming

[1] I then threw that version away and rewrote it the next morning so that I would sound helpful instead of frustrated. I have since re-written it several times.

[2] Or whatever language your reader prefers — although I've never seen a proof in Klingon before.

evidence for a statement in order to prove its truth — evidence is logically irrelevant. You can leave no room to doubt whether what you say is completely 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 — a common phrase 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 (e.g., replace each "$\exists x$" with "there exists an x"), *you should have a grammatically correct paper.*

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, the prime factorization theorem might be stated as follows: "Let n be a natural number. There exist distinct prime numbers $p_1, \ldots, p_m$, uniquely determined by n up to reordering, and uniquely determined natural numbers $a_1, \ldots, a_m$ such that $n = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$." An imprecise way of stating this theorem might be, "all numbers are a product of primes." For more examples, read the statements of the lemmas and theorems in a textbook on an abstract mathematical topic. (Reading and understanding well-written proofs is a great way to learn how a proof should be written.) It is often a good idea to include lemmas, propositions, etc. in your writing as well — if you find that it's unclear from the exposition what exactly your assumptions are or what you're aiming to show, stating a lemma is a good way to make sure you and your reader are on the same page, so to speak.

The only mathematical way to get from the assumptions to the conclusions is by making *precise logical deductions*. Each statement should again be totally unambiguous, and have impeccable support: you must be able to justify it with a mathematical reason that cannot be argued. This isn't to say that you have to re-prove the Pythagorean theorem every time you need to calculate the length of the hypotenuse of a triangle — it is fine to say "if T is a right triangle such that the sides of T that adjoin the right angle have lengths 3 and 4, then the length of the hypotenuse of T is $\sqrt{3^2 + 4^2} = 5$ *by the Pythagorean theorem*." In other words, you may cite a theorem in a book to which the reader can refer for justification if she doesn't believe you. In general, there cannot be any room for the reader to say "but what if" or "now why is that"[3]. Again, this is the beauty of mathematics — whereas one rarely wins a philosophical debate with one's roomates (especially at three in the morning), the correctness of a mathematical argument cannot be debated. Or rather, every mathematical debate will have a winner.

This does not mean that you have to write down *every* step in a proof; this would make your proofs impossibly long, even with generous use of math notation. For instance, you do not have to cite the distributive and associative

[3] That said, an interesting quirk about American mathematical culture is that, during a talk or a lecture, anyone can demand justification of any statement, at any time (within reason). So ask questions in class — your professor is used to it.

properties of the real numbers to say that $(a+b)(c+d) = ac+ad+bc+bd$ (but you should know how to prove it, in case someone doesn't believe that step). 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. If done well, this will make your proofs much less tedious, while still not leaving any of your statements up for debate; you simply leave out few enough logical steps that the reader can easily fill them in. (When writing up a problem set, however, what you should consider is whether the grader will believe that *you* know how to fill them in.)

There are also several things to avoid when writing a proof. One of the most common mistakes is to write a proof by example. A "proof" by example is *not* a proof. Examples are never necessary in a proof, and are only relevent if there are only a finite number of cases and you prove them all. 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 write the general proof; the specific case will follow. It is often helpful to work out an example if you don't know how to prove something in general, but you still need to do the general proof afterwards. In long papers it is often useful to include examples for clarity, but in a homework assignment it's generally not a good idea to include them.

The same rules apply to writing down your intuition for a proof — it's never logically necessary, and it is usually best to omit it on a homework assignment. I don't mean to say that intuition is unimportant — on the contrary, it's what makes the scrawls on the blackboard concrete to you. However, it is a means to an end, and the end is a complete proof. Think about what you are writing from the perspective of your reader — if it is helpful for the reader if you write something like, "intuitively, one would think that $x_n \to 0$ because of such-and-such a heuristic, so we will work towards proving that," then by all means write it, but if it is not helpful for the exposition of your proof, just omit it.

Another common mistake to avoid is using circular reasoning. Be very careful that you don't implicitly assume a result that only follows once you already know what you are trying to prove. For instance, if you are going to prove the existence of prime factorizations, the first thing you will likely want to do is to prove that that any integer n is divisible by some prime number p — but you cannot assume that n can be expressed as a product of prime numbers in order to find a prime divisor, since that's what you're trying to show.

An easy way to confuse a reader is to use a variable that you didn't define. *Always* define your variables *before* you first use them, or at the very latest, later in the same sentence. This is a very common mistake, especially after you've been thinking about a problem for a while — all the relevant objects have names in your head, but you have to remember that your reader doesn't know what they are.

Lastly, always remember that the reason you are writing a proof is so that someone else can read it. As with any writing, keep in mind who your audience is. When you write a proof, read over it through the eyes of your audience, and remember that *a priori* they do not have any idea what you're talking about.

I hope you find this helpful.