

Math 25 - Proof writing

Luke Gustafson and Elizabeth Schemm

So, you've decided to take Math 25, you've somehow convinced your advisor to sign your study card with Physics 16, CS 50, and Expos as your other classes, and now all that's standing between you and the perfect semester are a few pesky problem sets. Unfortunately we probably can't help you much with your other classes, but we can give you some pointers in this one.

As you have seen already, this course is meant to be an in-depth introduction to rigorous, proof-based, abstract mathematics. Proofs are central to the course; reading, understanding, and of course writing them are things that you will be expected to do and that you will become quite familiar with as the semester progresses. Some of you have probably already worked with proofs before; for others of you this may be the first time you have ever seen one, much less had to write one. In either case this handout is meant to introduce—or reintroduce—you to some of the basic techniques and strategies of rigorously proving mathematical statements. This is of course meant to be only a guide; soon you will see be asked to come up with proofs that are more sophisticated than the ones we give as examples here, but it is our hope that this will be of use to you as you start out in Math 25.

Proof writing 101

A proof is a sequence of reasoning, beginning with the premises and proceeding to the desired result. Each step of the proof should be a well-known fact, a theorem, or a clear implication. Be sure that each step follows from the *previous* steps of the proof. A common mistake is to make statements that follow from later steps, which is known as circular reasoning.

It is critical that you understand what parts of the problem are part of the premises. When a problem reads “Let $a = 5$,” the statement “ $a = 5$ ” is a part of the premise, and you should assume it is true throughout the problem. Similarly, the statement “Given $a = 5$ ” means that “ $a = 5$ ” is part of the premise. On the other hand, if the problem reads “Given a , find x ” then the value of a is not part of your premise, so you can't assume anything about it. You must find x for *any* a , not just a particular case.

Sometimes, your proof will contain an equation to which you want to refer later. In these instances, just put a number or symbol next to the equation in parentheses, and then refer to the equation using its symbol in parentheses. For example, you might write “ $2 + 2 = 4$ (*)” so that you can just write “(*)” to refer to this equation.

The amount of detail to include in a proof is important. You want to include enough detail so the reader knows what you are doing and doesn't have to get scratch paper to figure it out. On the other hand, you don't want to bog down your proof with too many unnecessary steps. When manipulating equations, include enough steps so the reader can follow it in his/her head, but you don't need any more than that. When in doubt, include details rather than leaving them out.

Write your proofs with the steps in order, so each step of your proof follows from the previous. Say right away if you are doing a proof by contradiction or induction (see below for a review of these proof methods). If you are using induction, state what variable you are inducting on and what the base case is. Say when a contradiction is reached or when your induction is complete, so the reader realizes that your proof is finished.

Make your proof grammatically correct. A proof is an essay: use words and sentences to explain what you are doing, not just equations (but you don't need to talk about anything unrelated to the proof itself; for example, don't talk about what motivated you to come up with your solution). Name theorems you use, and cite other people if you got help from them (don't plagiarize). For longer proofs, you should use paragraphs to naturally divide your proof into parts. Keep your wording and notation clear, concise, and unambiguous. This includes defining any variable you use.

Proof by contradiction

The idea behind a proof by contradiction is to assume that a statement is false and derive from that something that is uncontestably ridiculous (like $1 = 2$, or a Cauchy sequence is unbounded). A contradiction is often denoted by $*$ or $\Rightarrow \Leftarrow$.

Proposition 1. *There are infinitely many prime numbers.*

Proof: Suppose that there are finitely many prime numbers $p_1, \dots, p_n$, and consider the number $m = p_1 \dots p_n + 1$. Now m is a candidate to be a prime number, since none of the p_i divides it. Either m is prime, or it has some divisor p not equal to any of the p_i . In both instances we have a prime not in the set $\{p_1, \dots, p_n\}$, contradicting our original assumption.

One variant on this method is to demonstrate a counterexample if you are trying to prove that a statement is false.

Proving the contrapositive

Not unrelated to proof by contradiction is proving the contrapositive. To prove a claim of the form $a \Rightarrow b$, you can show instead that $(\text{not } b) \Rightarrow (\text{not } a)$. This is an equivalent statement, and it's sometimes easier to prove.

This gives you some options for proving $a \Leftrightarrow b$. You can show $a \Rightarrow b$ and then $b \Rightarrow a$, or you can show $a \Rightarrow b$ and $(\text{not } a) \Rightarrow (\text{not } b)$.

Proof by induction

Only statements that depend on a natural number (1, 2, 3, ...) can be proved by induction. It is not uncommon to use induction on the dimension of a vector space or on the number of elements of a set, for instance, to prove that some properties hold true in all such (finite) objects. Let $p(n)$ be the statement you want to prove for all natural numbers n (the "inductive hypothesis"). The proof proceeds in two steps:

- (1) Prove the base case $p(1)$ (sometimes you will need to prove two base cases $p(1)$ and $p(2)$, depending on the problem).
- (2) Show that if $p(n)$ holds for some $n \geq 1$, then $p(n+1)$ holds.

In this way you show that the claim is true for all n . An occasionally useful variant on induction, known as strong induction, is to show that if $p(k)$ holds for $1 \leq k \leq n$, then $p(n+1)$ holds.

Proposition 2 (Problem Set 2, Math 25a, 2000). *If $0 < b < a$ are real numbers and $n \in \mathbb{N}$, then $a^n - b^n < na^{n-1}(a - b)$.*

Proof: The proof proceeds by induction. Here we will need to make use of two base cases, since it turns out that $n = 1$ needs to be treated separately.

(1) First base case ($n = 1$): here $a^1 - b^1 \leq 1 \cdot a^0(a - b) = a - b$, so the statement holds.

(2) Second base case ($n = 2$):

$$\begin{aligned} a^2 - b^2 &= (a + b)(a - b) \\ &< 2a(a - b) \quad \text{since } a > b \\ &= na^{n-1}(a - b), \text{ for } n = 2 \end{aligned}$$

(3) Inductive step: Now suppose that $a^n - b^n < na^{n-1}(a - b)$, where $0 < b < a$. Then

$$\begin{aligned} a^{n+1} - b^{n+1} &= a^n(a - b) + b(a^n - b^n) \\ &< a^n(a - b) + bna^{n-1}(a - b) \quad \text{by the inductive hypothesis} \\ &< a^n(a - b) + ana^{n-1}(a - b) \quad \text{since } b < a \\ &= (n + 1)a^n(a - b) \end{aligned}$$

so that $a^{n+1} - b^{n+1} < (n + 1)a^n(a - b)$ for $n > 2$.