Tips on Proof Writing

This guide includes some things that I like to keep in mind when I am writing proofs. They will hopefully become second-nature after a while, but it helps to actively think about them when one is first learning to write proofs.

There are some books out there that are designed to help you learn to read and write proofs. (A commonly–used one is *How to Read and Do Proofs* by Daniel Solow. It should be on reserve at Baker-Berry soon, and the library has two additional older copies available.) However, they can be somewhat dry and slow in getting off the ground. For me, the best way to learn to write proofs is to dive in and try to write up proofs of some reasonably simple statements. With this in mind, there are two fundamental aspects of proof writing that need to be mastered.

Logic: The first step to writing a proof, and probably the biggest hurdle for most people, is determining the logical steps needed to verify the given statement. In other words, this involves laying down an outline of the argument that you intend to make. There are some things to keep in mind when trying to do this.

- **What am I being asked to prove?** Often this will require you to unravel a definition or two to figure out what you're *really* trying to prove.
- **What are the hypotheses?** You're usually given some assumptions, and then you are asked to deduce something from them. This would usually be written in the form

  "If ..., then ..."

  Again, look back at the definitions and decide what the hypotheses are really saying.
- **What theorems might help?** Try to think of definitions and theorems that are related to the given statement. Determine which ones might help you get from the hypotheses to the desired result.
- **Put it all together.** Try to piece together the theorems that you've found in a logical way to deduce the result.

Example 1. Let's try to put these ideas into action.

> **Prove:** If a and b are relatively prime and $a \mid bc$, then $a \mid c$.

Let's think about what we need to do here.

- What are we being asked to prove? We want to show that $a \mid c$, which means that we need to show that there is an integer n such that $c = na$.
- What are the hypotheses? There are two: we are told that a and b are relatively prime **and** that $a \mid bc$. The first means that
$$\gcd(a, b) = 1,$$
and the second tells us that there exists $m \in \mathbb{Z}$ such that
$$bc = ma.$$

- What theorems do we have at our disposal? One of the theorems we proved regarding gcds was Bézout's lemma (or the extended Euclidean algorithm), which said that

$$\gcd(a, b) = ax + by$$

for some $x, y \in \mathbb{Z}$.

- Let's put it together:

$$\gcd(a, b) = 1 \underset{\text{Bézout}}{\implies} 1 = ax + by \underset{\text{multiply by } c}{\implies} acx + bcy = c$$

Now use the other hypothesis:

$$\begin{aligned} a \mid bc &\implies bc = ma \\ &\implies bcy = may \\ &\implies acx + bcy = acx + may \\ &\implies c = a(cx + my) \\ &\implies a \mid c \end{aligned}$$

In this example we didn't actually write a proof. We simply outlined the argument, which is the backbone of the proof. Now we need to turn it into something readable. This brings us to the second major aspect of proof writing.

Style: Once you have your argument laid out, the next thing you need to do is to write it up in a nice way. Here are some tips for doing this.

- **Write in proper English.** Use complete sentences, with proper grammar and punctuation. The goal is to make it easy for the reader to understand. If you are unsure of how a particular sentence looks, read it back to yourself and think about how it would sound to the reader.
- **Be clear and precise.** Try to say what you mean in as simply as possible, while still using proper mathematical language. Be careful how you say things, and explain yourself at each step. If there is a step that you have to think about, or that you think may give the reader pause, explain it.
- **Don't say too much (or too little).** Again, explain yourself thoroughly, but don't overdo it. Get to the point, and avoid using overly ornate or mellifluous language. At this stage in the game, it's okay to err on the side of writing too much, but try to not overdo it.

These are all things that will become much easier with practice. Also, reading proofs in the book (or seeing them in class) will give you a better idea of how people tend to talk when they are writing proofs.

Example 2. Let's write up a proper proof of the example.

> **Prove:** If a and b are relatively prime and $a \mid bc$, then $a \mid c$.

Proof. Since a and b are relatively prime, $\gcd(a, b) = 1$, and Bézout's lemma lets us write

$$ax + by = 1$$

for some $x, y \in \mathbb{Z}$. If we multiply both sides by c, we get

$$acx + bcy = c.$$

We are assuming that $a \mid bc$, so there is an $m \in \mathbb{Z}$ such that $bc = ma$. Then

$$bcy = may,$$

so

$$c = acx + bcy = acx + may.$$

Factoring out a, we get

$$c = a(cx + my).$$

But $cx + my \in \mathbb{Z}$, and this is precisely what it means for a to divide c. □

As a final note on style, people usually use a symbol to indicate the end of a proof. The most common is a simple square, which can be open or filled: □ or ■. (The default in LaTeX is an open square.) Some people will also use an open or closed diamond, or double or triple hatch marks (// or ///). Older proofs sometimes end with Q.E.D, which is an abbreviation of the Latin "quod erat demonstrandum," or "which was to be demonstrated."