A few words about proofs

Introduction

One of the biggest differences between Math 307 and most earlier math courses is that Math 307 involves a lot more writing of proofs.[1] The first thing you need to know about proofs is that they aren't as complicated or as new to you as you might think. Whether you realize it or not, you've probably read and written lots of proofs in every math class you've taken in the last few years. Every homework problem that was phrased "Explain why..." or "Show that..." was really asking you to write a proof. All a *proof* is is a careful explanation of why something is true, with each statement justified by what's already been said. A proof certainly doesn't have to be in anything like the two-column format you may have seen in your high school geometry class, and almost all proofs are written mostly in English prose (not just with mathematical notation). In fact, you should write all of your proofs in a paragraph format with complete English sentences. Take a look at any of the proofs in the Math 307 textbook to see what your proofs should look like. A big part of the difference between Math 307 and your earlier math courses, as far as proofs are concerned, is that in Math 307 we just use the words "prove" and "proof" more often.

Nevertheless, it is true that in Math 307 you are asked to prove statements about more abstract concepts than was the case in earlier classes. So this is a (very) brief introduction to some basic proof techniques which will be useful to you this quarter. These are all techniques you've probably seen in action before, but without necessarily having them pointed out.

1 Using a definition

Definitions are at the heart of every mathematical statement. You can't tell whether or not a statement is true, or even make sense of what it says, without knowing exactly what the definition of each term is. Many statements can be proved using nothing but the definition of the key term that appears. In fact, many statements have to be proved using nothing but definitions, since you sometimes don't know anything else. Here are a couple examples.

Definition 1. *A function f whose domain and range are $\mathbb{R}$ is called* additive *if $f(x+y) = f(x)+f(y)$ for every x and y in $\mathbb{R}$.*

Notice that in giving this definition, I'm assuming you already know the definitions of the terms *function*, *domain*, and *range*, and the symbol $\mathbb{R}$ (the set of real numbers). Now we'll prove the following two statements about additive functions. Notice that we don't know

[1] Another course, Math 305, is designed to help students make the transition from problem-oriented math courses to proof-oriented math courses. If you think you would prefer starting with a class that addresses this transition explicitly, you might consider taking Math 305 first.

anything at all about additive functions right now, except for the definition itself, so we have no choice but to use the definition.

Theorem 1. *If c is any real number, then the function f defined by*

$$f(x) = cx$$

is additive.

Proof. According to the definition of an additive function, we need to show that for every pair of real numbers x and y, $f(x+y) = f(x) + f(y)$. To do this, we also need to use the given definition of f. So let x and y be any two real numbers. Then

$$f(x+y) = c(x+y) = cx + cy = f(x) + f(y),$$

using the definition of f in the first and last equalities, and the distributive law in the second equality. Therefore f is additive. □

Notice that in this proof we used the definition of f given in the statement as well as the definition of an additive function. This proof also illustrates the principle of *picking a name*, discussed below in Section 2.

Theorem 2. *If f is an additive function, then $f(0) = 0$.*

It is easy to check that this is true for the function defined in the statement of Theorem 1, but this theorem is making a claim about *every* additive function – not just ones we already know more about. So Theorem 1 is no help to us, and again, the definition of an additive function is the only thing we have to use.

Proof. If f is additive, then $f(0+0) = f(0) + f(0)$. Rewriting this and solving, we get

$$f(0) = 2f(0),$$

$$0 = f(0).$$

□

This proof illustrates another important principle: *making a convenient choice*. If the definition of a thing you're working with says that some statement is true for every (*fill-in-the-blank*), you are free to fill in the blank with whatever is convenient for you. In this case, we are told that $f(x+y) = f(x) + f(y)$ for any real numbers x and y that we'd like to plug in. We have in mind that we want to find out something about $f(0)$. So how can we make $f(0)$ show up? Well, the easiest way would be if $x = 0$ and $y = 0$, because then $f(0)$ pops up all over the place. Since 0 *is* a real number, we're perfectly free to plug those values in.

2 Picking a name

A very simple but often overlooked point is that it is often necessary to make up a name for some object in order to write a proof. You may need to give a name to some object which is mentioned in the statement of the theorem but not named there. Very often you need to name some object that isn't mentioned in the statement of the theorem at all, but that appears in the definition of a term used in the statement. For our first example, we'll start by giving another definition.

Definition 2. *Two integers m and n* have the same parity *if they are either both even or both odd.*

Theorem 3. *In any set of three integers, some two of them have the same parity.*

In this case, we are asked to think about three integers, but we don't have any name for them. So our proof will start out by naming these integers.

Proof. Let a, b, and c be any integers. Now either a and b have the same parity or they don't. If a and b have the same parity, then we're done.

On the other hand, if a and b don't have the same parity, then one of them is even and the other is odd. We know that c is either even or odd. Therefore c has the same parity as either a or b. □

Notice that we start out by not just writing down the names a, b, and c, but also by telling the reader what these things are (they're some integers, and we don't know which ones). This is usually phrased, "Let (*the name you've made up*) be (*whatever kind of object you're working with*)." The statement "Suppose (*name*) is a (*kind of object*)" means the same thing.

This proof also illustrates the strategy of *splitting into cases*. It's often useful, as here, to think first about what if one possibility is true, then another, and so on until every possibility has been covered. In the proof above, we dealt first with the case in which a and b have the same parity, then with the case in which a and b don't have the same parity. It is clear that those two cases exhaust all the possibilities. Since we showed that the theorem is true in either of those two cases, it must be true.

Our second example of picking a name has already been done, in the proof of Theorem 1. Now that we've discussed picking names, go back and reread that proof. Notice that in order to show that the given function was additive, we had to show that a certain statement was true for any pair of real numbers. So we introduced a pair of real numbers, saying, "So let x and y be any two real numbers." In this case we used the same names for the two real numbers that appeared in the definition of an additive function, but we didn't have to. We could replace x and y with a and b everywhere in the proof of Theorem 1, just as we used a, b, and c in the proof of Theorem 3 even though the definition before it referred to two integers as m and n.

3 Contradiction

Proof by contradiction is an especially useful strategy for proving a negative statement, that is, a statement that says something is not true, or something cannot be done. The idea is, you assume the opposite statement – that the something *is* true, or the something *can* be done – and show that assuming that leads you to some statement that contradicts something you already know is true. This contradiction means that some mistake has been made, which must have been your original assumption. Here is a classic example of a theorem which can be proved by contradiction.

Theorem 4. *The number $\sqrt{2}$ is irrational.*

Although it doesn't look like it, this is exactly the kind of statement described above for which contradiction is a good strategy. Remember that by the definition of an irrational number, this is really saying, "it's impossible to write $\sqrt{2}$ as $\frac{m}{n}$, where m and n are integers". Notice that it's important here to have a good definition of a rational number to work with – it would be much harder to prove this theorem thinking of an irrational number as a number with a non-repeating decimal expansion.

Proof. We begin by assuming the opposite. That means, we assume that actually $\sqrt{2}$ a rational number, which means there are integers m and n such that

$$\sqrt{2} = \frac{m}{n}.$$

We know that we can assume m and n are both positive (because $\sqrt{2} > 0$) and that they have no common factors, so that $\frac{m}{n}$ is written in lowest terms. Squaring both sides of this equation and multiplying by n^2, we find that

$$m^2 = 2n^2.$$

Therefore m^2 is divisible by 2. Since 2 is prime, this means that m is divisible by 2, so we can write $m = 2p$, where p is some other positive integer. Substituting this, we obtain

$$4p^2 = 2n^2,$$

so

$$2p^2 = n^2.$$

Therefore n^2 is divisible by 2, which means that n is divisible by 2.

Now we've found that m and n are both divisible by 2, but we said earlier that m and n had no common factors. These statements contradict each other. So our original assumption, that $\sqrt{2}$ is rational, must have been incorrect. □

Notice that this proof also gives yet another example of picking names: we introduced the numbers m, n, and p, and explained what each one was supposed to be.