Guide to Proofs

Thanks to Michael Kim for writing some of the proofs used in this handout.

What makes a proof a "good proof?" It's hard to answer this question directly – it's like asking what makes an essay a "good essay." There are many traits that good essays have in common, and there are many traits that bad essays have in common, but no hard and fast rules governing how to write essays.

In this handout, we've compiled several different proofs that are similar to the proofs that have been submitted in past quarters. We've annotated each of them with our feedback about what we like about them and ways in which they could be improved. Our hope is that by giving you various examples of good proofs, you'll have a better sense for what we're looking for.

If you'd like some additional resources on good proofwriting, we suggest checking out Chapter 2.4 of the online course reader (which has some general style and design tips for proofs), or looking at these links, which have useful information about how to write proofs:

- ***Mathematical Writing*** by Knuth, Larrabee, and Roberts, which you can find online by visiting http://jmlr.org/reviewing-papers/knuth_mathematical_writing.pdf. This is a set of notes for a class that Don Knuth taught at Stanford back in 1987. The "Minicourse in Technical Writing" has great advice if you want a quick summary.
- ***Some Remarks on Writing Mathematical Proofs*** by John M. Lee (available online at http://www.math.washington.edu/~lee/Writing/writing-proofs.pdf). I often refer to these notes myself when trying to write mathematical proofs, as they're accessible, clearly-written, and well-motivated.

Example: Pythagorean Triples

A Pythagorean triple is a triple (a, b, c) where a, b and c are positive integers and $a^2 + b^2 = c^2$. Here's a fun fact about Pythagorean triples:

> There are no positive integers a and b for which (a, a, b) is a Pythagorean triple.

Here is one sample proof of this result:

> ***Proof:*** If (a, a, b) is a Pythagorean triple, $2a^2 = b^2 \Rightarrow b / a = \sqrt{2}$, which is impossible. ■

This proof is definitely on the short side, but even so it's (somewhat) possible to follow the reasoning. Starting with the assumption that (a, a, b) is a Pythagorean triple, we get that $2a^2 = b^2$ (though you might have to pause for a second to see why). This in turn implies that $b / a = \sqrt{2}$, which can't happen because $\sqrt{2}$ is irrational.

That said, this proof is terse to a fault. Although the reasoning is correct, this proof requires a lot of work from the reader to rehydrate. In particular, let's look at three steps:

If (a, a, b) is a Pythagorean triple, $2a^2 = b^2$
$b / a = \sqrt{2}$
Which is impossible.

Each of these steps, in the context of the preceding steps, is correct. However, unless you already know *why* they're valid, it's difficult to determine it from the proof itself. Proofs exist to convey a line of reasoning to a reader who does not know why the result is true. Consequently, when writing proofs, it is important to include details that would let a mathematically educated reader understand why your result is true.

Here is an alternative version of the above proof, in which we've added additional details to clarify the reasoning:

Proof: By contradiction; assume there exists some positive integers a and b for which (a, a, b) is a Pythagorean triple. Since (a, a, b) is a Pythagorean triple, we have $a^2 + a^2 = b^2$, so $2a^2 = b^2$. Because (a, a, b) is a Pythagorean triple, we have $a > 0$, so a is nonzero. Because $2a^2 = b^2$, we can divide both sides by a^2 to get $2 = b^2 / a^2$. Taking the square root of both sides gives us that $b / a = \sqrt{2}$. This means we can write $\sqrt{2} = b / a$ for integers b and a, where $a \neq 0$. Thus $\sqrt{2}$ is rational. However, as proven earlier, $\sqrt{2}$ is irrational. We have reached a contradiction, so our assumption must have been wrong. Thus (a, a, b) cannot be a Pythagorean triple. ■

There are several important differences between this proof and the original:

- *The proof gives guideposts to its overall structure*. The original proof starts off with the assumption that (a, a, b) is a Pythagorean triple without actually explaining why it's doing so. This might confuse the reader – if you're trying to prove that (a, a, b) can't possibly be a Pythagorean triple, why are you assuming it? Additionally, it concludes by explaining that the contradiction that has been reached implies the main result to be proved, which helps explain the arc of the proof.
- *The proof explains how the steps follow from one another*. With some simple arithmetic, it's easy to see why if (a, a, b) is a Pythagorean triple, then $2a^2 = b^2$. The initial proof omits the steps necessary to show this, which forces the reader to stop reading the proof, grab a sheet of paper, and work through the math. This disrupts the narrative flow of the proof, and, in the event that the reader can't determine how the first part implies the second, the reader won't fully understand the proof's logic.
- *The proof justifies its contradiction*. The initial proof concludes by noting that it's impossible for b / a to be equal to $\sqrt{2}$. However, it doesn't explain *why* this is impossible. Calling back to the definition of a rational number helps the reader better understand what is going on.
- *The proof has better narrative flow*. Remember: **treat proofs as essays**. The purpose of a proof is to convey a valid line of reasoning, not to describe a calculation. Therefore, a proof should function as a piece of writing that, while using mathematical symbols, can still be read with ease. A good test for whether a proof is clear and elegant is whether you can read it aloud; the original proof fails this test. Try reading the phrase "If (a, a, b) is a Pythagorean triple, $2a^2 = b^2 \Rightarrow b / a = \sqrt{2}$" aloud; you'll probably get stuck at the comma after "triple" (does the comma indicate "then" or a continuation of what's being assumed?) and at the $\Rightarrow$ symbol (which cannot easily be articulated.)

A helpful piece of advice to keep in mind when writing proofs: ***use mathematical notation to convey facts and English to convey structure***. Any proof that (a, a, b) can't be a Pythagorean triple is ultimately going to have to introduce some mathematical notation to describe the relationship between a and b, but that doesn't mean that the whole proof should be dense mathematical notation. The second version of the proof above uses plain English to describe how each step in the proof flows into the next, but doesn't try to explain that $2a^2 = b^2$ in English.

So is the above proof the "best" proof of the theorem? Not necessarily. Contrast that second proof with this third proof:

Proof: By contradiction; assume there exists some positive integers a and b for which (a, a, b) is a Pythagorean triple. Since (a, a, b) is a Pythagorean triple, we see that $a^2 + a^2 = b^2$. Therefore, we know that

$$2a^2 = b^2. \tag{1}$$

We know from our initial assumption that a is nonzero. This means that a^2 is nonzero, so we can divide both sides of equation (1) by a^2 to get

$$2 = b^2 / a^2. \tag{2}$$

Taking the square root of both sides of equation (2) yields

$$\sqrt{2} = b / a. \tag{3}$$

Statement (3) tells us that we can express $\sqrt{2}$ as the ratio of two nonzero integers, or equivalently that $\sqrt{2}$ is rational. But this is impossible – we already know that $\sqrt{2}$ is irrational. Therefore, our assumption must be wrong, so there are no positive integers a and b for which (a, a, b) is a Pythagorean triple. ■

In our opinion, this proof is much cleaner than the second proof. Here are a few reasons why:

- *The proof gives names to intermediary results*. It's enlightening to compare the paragraph after intermediary result (2) with the equivalent step from the previous proof. The above proof explicitly states what it's doing in this step: "Taking the square root of both sides of (2) yields $\sqrt{2} = b / a$." The previous proof says this instead: "Taking the square root of both sides gives us that $b / a = \sqrt{2}$." In both cases, the reader needs to look back in the proof to find something that was written earlier. In the newer proof, the statement to refer back to is on its own line, clearly labeled, and explicitly referenced. In the older proof, it's clear that we're supposed to take the square root of both sides of *something*, but it's not clear what. The reader has to go backwards through the paragraph – which is already quite dense – to figure out what's being discussed. In many cases, a complex proof can be made much clearer simply by giving names to important intermediary results. If you find that your own proofs are too dense, it may be helpful to expand them out in this way.
- *There is more variation in sentence structure.* Read back over the second proof – do you notice anything about the sentence structure? Lots of consecutive sentences have the same structure: "Because X, we have Y." In this newer proof, there's more diversity in the sentence structure. Some sentences just state facts, while others show how those facts flow together. If you find that your own proofs feel tough to read, check your sentence structure – you might be repeating the same pattern over and over again.

- *The proof is visually more spread out.* When reading a proof, it's not uncommon to have to pause and think about the argument. Sometimes, it will be necessary to refer back to something earlier in the proof. When that happens, it can be tough for a reader to jump back to where they were. Notice how this third proof is physically more spread out than the second – there's more whitespace, more labeling, and more natural breaks. This makes it easier for the reader to jump back to a location and find where they were before.

Example: Rational and Irrational Numbers

There are infinitely more irrational numbers than rational numbers, though actually showing a particular number is irrational might take some effort. Here's an interesting statement to prove:

$\log_2 3$ is irrational.

Here is one attempted proof of this result:

> ***Proof:*** Here, we set out to prove that $\log_2 3$ is irrational. Remember that a rational number is a number r where there exists integers p and q such that $p / q = r$. Thus, we need to show that no such p and q exists for $p / q = \log_2 3$. Thus, we will proceed by contradiction and a false statement to prove a true one. If we assume that $\log_2 3 = p / q$ for some integers p and q, then we know by properties of logs that this means $2^{\log_2 3} = 2^{p/q}$. Thus, we have that $3 = 2^{p/q}$. If we raise each side to the qth power we see $2^p = 3^q$, which means we have to find p and q to solve this equation. We see that one such solution is $p = 0$ and $q = 0$ and both sides of the equation are 1. But this is not allowed because we had a q in the denominator, so if $q = 0$, then $\log_2 3$ would be infinite or undefined and wouldn't make sense. Since we know that we can calculate this value, then it can't be that $q = 0$. Thus, we must find another way to prove this fact. To do this, we note the first few powers of 2 and of 3. These are 2, 4, 8, 16, 32, ... and 3, 9, 27, 81, 243, ... As you can see, the powers of 2 are always even and the powers of 3 are always odd. It's now clear that even numbers are closed under exponentiation and so are the odd ones. Thus, we discover that $2^p \neq 3^q$ for any p, q that would be legal to choose. Because we discover this, we know that we have reached a contradiction, so we know it must be false. ■

This is an excellent *first draft* of a proof. It reads as an exploration of the topic at hand – why it's going to use a proof by contradiction, what the first powers of two and powers of three are, why q can't be zero, etc. However, because of this, it's far more verbose than is necessary and contains many pieces that could be significantly condensed or eliminated. Take this part as an example:

> Here, we set out to prove that $\log_2 3$ is irrational. Remember that an irrational number is a number r such that there exists integers p and q such that $p / q = r$. Thus, we need to show that no such p and q exists for $p / q = \log_2 3$. Thus, we will proceed by contradiction and a false statement to prove a true one.

As part of a draft, this is a great line of reasoning to follow. When writing this up as a formal proof, though, it should probably be restructured:

- Since the proof is a proof by contradiction, the proof should probably start off by announcing itself as such.

- You can assume that the reader knows what a proof by contradiction is, so there's no need to justify how it works (assuming a false statement to prove a true one). This reminder of how a proof by contradiction works doesn't add anything of substance to the proof.
- The proof tries to outline how it's going to work – it says that it will show that there aren't any integers p and q such that $p / q = \log_2 3$ – but if you look later in the proof, it doesn't actually directly show this. This is problematic, since the proof is not making good on its promises!

Here's how we might start the proof off, using the same core ideas but without as much exposition:

> ***Proof:*** By contradiction; assume that $\log_2 3$ is rational. Then there must exist some $p, q \in \mathbb{Z}$ such that $p / q = \log_2 3$ and $q \neq 0$. …

Let's look at another part of this proof that could use some cleanup. In the middle of the proof, the author tries to get a contradiction by noting that if $p / q = \log_2 3$, then $2^p = 3^q$. I've reprinted part of this proof below:

> If we raise each side to the qth power we see $2^p = 3^q$, which means we have to find p and q to solve this equation. We see that one such solution is $p = 0$ and $q = 0$ and both sides of the equation are 1. But this is not allowed because we had a q in the denominator, so if $q = 0$, then $\log_2 3$ would be infinite or undefined and wouldn't make sense.

If you'll notice, in the tail end of this section, the author needs to justify why we can't have $p = 0$ and $q = 0$. The author justifies this by saying

> But this is not allowed because we had a q in the denominator, so if $q = 0$, then $\log_2 3$ would be infinite or undefined and wouldn't make sense.

You might be wondering what the author is talking about. Earlier in the proof, the author assumed that $\log_2 3$ is rational, meaning that there's some choice of integers p and q such that $p / q = \log_2 3$. We can't have $q = 0$ if we have q in the denominator of a fraction, since then we'd be dividing by zero. Looking back over the above sentence from the proof, though, you might not have been able to figure out why.

On the one hand, technically speaking, the author is right – if q were equal to zero, then $\log_2 3$ would be infinite or undefined because it would be equal to $p / 0$. On the other hand, the proof does a poor job of actually explaining why this is true; the reader has to figure this out on his or her own. The goal of a proof is to convey an argument, and in this case the author has failed to do so.

So how could we clean this up? One way to do so would be to rewrite the section as

> If we raise each side to the qth power we see $2^p = 3^q$, which means we have to find p and q to solve this equation. We see that one such solution is $p = 0$ and $q = 0$ and both sides of the equation are 1. Earlier, we wrote $\log_2 3 = p / q$, so we know that q isn't zero. Therefore, we need to look for a solution other than $p = 0$ and $q = 0$. …

This works out much better than before – it gives a rigorous justification for why $p = 0$ and $q = 0$ isn't a valid solution in this case and motivates the search for another solution.

Here's one last part of the proof that needs to be cleaned up:

> We note the first few powers of 2 and of 3. These are 2, 4, 8, 16, 32, ... and 3, 9, 27, 81, 243, ... As you can see, the powers of 2 are always even and the powers of 3 are always odd. It's now clear that even numbers are closed under exponentiation and so are the odd ones.

When exploring why the result is true, it's perfectly reasonable to start listing off powers of two and powers of three and looking for a trend. The trend the proof notes is that powers of two are always even (except for 1, which was accounted for earlier in the proof) and powers of three are always odd, which will cause a problem.

However, the way that this is written could use some work. Writing out the first several powers of two and powers of three is a good way to see whether there are some patterns (in this case, that powers of two are even and that powers of three are odd), but that's not in of itself a proof. To be more rigorous, the proof might note that two is a divisor of 2^p for $p > 1$ but is never a divisor of 3^q, could use induction, etc.

There's actually a small logic hole in this proof. In this discussion, p and q are assumed to be positive, though it's possible that at least one of p and q are negative. Therefore, it's possible that 2^p or 3^q might not be an integer, in which case arguments about whether these numbers are even or odd would be meaningless. It's worth updating the proof to account for this case.

To summarize our feedback on this proof:

- It's great initially to write out your thoughts, simple examples, basic definitions, etc., but be sure to clean them up in your final draft.
- Adding precision into definitions of variables makes it easier to reason about them later on and can save you a lot of time on what might seem like a difficult digression.
- Avoid phrases like “clearly,” “obviously,” or “as you can see.” Usually, but not always, these phrases indicate that you are skipping a step or failing to justify a statement.

Additionally, the final proof should probably get a bit of a style cleanup along the lines of the Pythagorean Triples example given earlier in this handout. It would be good to label important equations, to vary the sentence structure, etc.

Example: Pythagorean Triples, Again

Let's look at another sample proof involving Pythagorean triples. Here's something you may have noticed about Pythagorean triples:

> If k is any positive integer and (ka, kb, kc) is a Pythagorean triple, then (a, b, c) is a Pythagorean triple.

For example, since (6, 8, 10) is a Pythagorean triple and each number has two as a divisor, we can divide it out to leave (3, 4, 5), which must be a Pythagorean triple. Similarly, since (50, 120, 130) is a Pythagorean triple and each number has 10 as a divisor, we can divide out the 10 to get (5, 12, 13), which must be a Pythagorean triple.

Here's one possible proof of this result:

Proof: Consider any Pythagorean triple (ka, kb, kc) where k is a positive integer. This means that

$$(ka)^2 + (kb)^2 = (kc)^2$$
$$k^2a^2 + k^2b^2 = k^2c^2$$
$$a^2 + b^2 = c^2 \text{ (since } k^2 \neq 0)$$

Clearly, neither a, b, nor c can be zero, and so (a, b, c) is a Pythagorean triple. ■

There are a couple of parts of this proof that could use some work. Let's start with the formatting and structure of the proof. Look at this part:

> This means that
> $$(ka)^2 + (kb)^2 = (kc)^2$$
> $$k^2a^2 + k^2b^2 = k^2c^2$$
> $$a^2 + b^2 = c^2 \text{ (since } k^2 \neq 0)$$

Try reading this out loud as if you were reading an essay. You might run into trouble because you'll read off "This means that..." as the start of a sentence, but the math that follows it isn't actually a continuation of that sentence. It starts off as "This means that $(ka)^2 + (kb)^2 = (kc)^2$," which is a valid sentence, but the next line of the proof, "$k^2a^2 + k^2b^2 = k^2c^2$," can't be added on to the end of the previous sentence and isn't a sentence by itself. We can correct this by rewriting the proof so that it works in complete sentences. Here's an example:

Proof: Consider any Pythagorean triple (ka, kb, kc) where k is a positive integer. From the definition of a Pythagorean triple, we see that

$$(ka)^2 + (kb)^2 = (kc)^2. \qquad (1)$$

Since k is a positive integer, we know that $k \neq 0$ and therefore that $k^2 \neq 0$. Simplifying equation (1) and dividing both sides by k^2 gives the following:

$$k^2a^2 + k^2b^2 = k^2c^2$$

$$a^2 + b^2 = c^2$$

Clearly, neither a, b, nor c can be zero, and so (a, b, c) is a Pythagorean triple. ■

There's actually now *more* in this proof (an explanation of why we can divide by k^2 that was previously not explained), and there's another sentence motivating the algebraic simplifications. Additionally, the proof is now more grammatically correct: the sentence stating what manipulations will happen ends with a colon (ending the previous clause and introducing a justification) rather than trailing off into some math. Try reading this out loud – a bit easier, isn't it?

However, there is one aspect of this proof that isn't ideal. Look at this last sentence:

> Clearly, neither a, b, nor c can be zero, and so (a, b, c) is a Pythagorean triple. ■

We (the CS103 staff) sometimes like to joke that proofs like this are “proof by intimidation;” they assert that something is true because it's *clearly* true or *obviously* true, but without actually backing it up. If you ever find yourself wanting to justify something by saying that it's “clearly” or “obviously” true, take the time to make sure you see why it's actually true. You might find that what you initially thought was “clearly” and “obviously” true is actually false (in which case you've just spotted a logical flaw in your argument), or you might figure out a way to explain why it is true (in which case you've deepened your understanding of the math).

In the case of this proof, it's illustrative to rewrite the proof to explain exactly why none of these values can be zero. Here's one reasonable way to do this:

Proof: Consider any Pythagorean triple (ka, kb, kc) where k is a positive integer. From the definition of a Pythagorean triple, we see that

$$(ka)^2 + (kb)^2 = (kc)^2. \qquad (1)$$

Since k is a positive integer, we know that $k \neq 0$ and therefore that $k^2 \neq 0$. Simplifying equation (1) and dividing both sides by k^2 gives the following:

$$k^2a^2 + k^2b^2 = k^2c^2$$

$$a^2 + b^2 = c^2 \qquad (2)$$

Because (ka, kb, kc) is a Pythagorean triple, we know that ka, kb, and kc are positive. Since k is a positive integer, this means that a, b, and c are all positive as well. This, combined with equation (2), means that (a, b, c) is a Pythagorean triple, which is what we needed to show. ■

The end of this proof now actually takes the time to explain why a, b, and c must be positive, which is necessary for showing that (a, b, c) must be a Pythagorean triple. That's certainly better than saying that it's "clearly" true, since as you can see above there's actually a few details to check.

However, this is probably not an ideal ending to the proof. Reread this new proof from start to finish. In our opinion, the ending of this proof is a bit abrupt; it switches from a calculation on a, b, and c to the fact that ka, kb, and kc are positive. Ultimately this leads somewhere – we need that fact to show that a, b, and c are all positive – but it's not clear where the proof is going until it gets there. When you have a proof with two or more distinct parts (which will be most of the proofs you write over the course of this quarter), it's important to give landmarks throughout the proof explaining what you're going to do and when. That makes it easier for a reader to understand what they're about to read and how everything ties together. Here's a final proof with guideposts put in:

Proof: Consider any Pythagorean triple (ka, kb, kc) where k is a positive integer. We will prove that (a, b, c) is also a Pythagorean triple.

First, we'll prove that $a^2 + b^2 = c^2$. From the definition of a Pythagorean triple, we see that

$$(ka)^2 + (kb)^2 = (kc)^2. \qquad (1)$$

Since k is a positive integer, we know that $k \neq 0$ and therefore that $k^2 \neq 0$. Simplifying equation (1) and dividing both sides by k^2 gives the following:

$$k^2a^2 + k^2b^2 = k^2c^2$$

$$a^2 + b^2 = c^2 \qquad (2)$$

Next, we'll prove that a, b, and c are positive. Because (ka, kb, kc) is a Pythagorean triple, we know that ka, kb, and kc are positive. Since k is a positive integer, this means that a, b, and c are all positive as well.

Since a, b, and c are positive and $a^2 + b^2 = c^2$, we conclude that (a, b, c) is a Pythagorean triple, as required. ■

This proof is much clearer and cleaner than the earlier attempts. It starts off with a lead-in explaining what the big picture is ("We will prove that (a, b, c) is also a Pythagorean triple.") It then breaks the proof into two steps, announcing what it will prove and then following through with that prom-

ise. Finally, it aggregates these pieces together to conclude with the statement that needed to be proven.

Example: Subsets and Differences

Here's a fact about sets that's often useful when manipulating sets:

For any sets A and B: $A - B = \varnothing$ iff $A \subseteq B$

Here is one possible proof of this fact:

> ***Proof:*** Let's assume that $A - B = \varnothing$. By definition of set difference, this means that the set of elements in A that are not in B (that is, $A - B$) is empty. Thus, there are no elements in A that are not also in B. In other words, for every element, if $x \in A$, then $x \in B$. We know that a set S is a subset of T if and only if for every element $x \in S$, $x \in T$ as well. Thus, by definition, we conclude that $A - B = \varnothing$ if and only if $A \subseteq B$. ■

Unlike the other proofs in this handout, which are essentially correct but could use some stylistic corrections, this proof actually contains a serious logic error and does not prove what it needs to prove. In particular, look at the statement to prove:

For any sets A and B: $A - B = \varnothing$ iff $A \subseteq B$

Did this proof actually show this? If you look at the very last line, it seems like it might be the case. However, there is something flawed with this reasoning. To prove a biconditional statement like this one, the proof needs to show the following:

If $A - B = \varnothing$, then $A \subseteq B$

If $A \subseteq B$, then $A - B = \varnothing$

Looking at this proof again, you'll notice that it only proves the first of these statements – it starts off by assuming $A - B = \varnothing$, then concludes that $A \subseteq B$. However, it hasn't proven the other direction of implication by starting with the assumption that $A \subseteq B$ and concluding $A - B = \varnothing$. In other words, what the proof says is correct, but it's incomplete. To round out this proof, we'd need to prove the other direction of implication as well.

Before we do that, though, let's look at the writing style of this proof. Here's a little game you can play – read the sentences of the proof one at a time and stop at the end of each sentence. Ask yourself this question: is it clear where the proof is going?

You might have noticed that this proof keeps stating facts one after the other. These facts do follow from one another, but it's unclear where the proof is going. It's important to put guideposts in proofs that cue the reader into what's going to happen later on, and this proof hasn't done that.

Here's a rewrite of the above proof with some more guideposts put in. Half of the proof is still missing (we only proved one direction of implication), but hopefully you can see why this new proof is cleaner:

> ***Proof:*** We will prove both directions of implication.

> First, we'll prove that if $A - B = \emptyset$, then we will have $A \subseteq B$. Let A and B be arbitrary sets where $A - B = \emptyset$. We'll show $A \subseteq B$ by proving that every element of A is also an element of B.
>
> We know that $A - B = \emptyset$, meaning that the set of elements in A that are not in B (that is, $A - B$) is empty. Thus, there are no elements in A that are not also in B. Consequently, every element of A also belongs to B, and therefore $A \subseteq B$, as required.
>
> *(the other direction of implication goes here.)* ■

Notice that the proof starts off by announcing how it's going to prove that A is a subset of B: it's going to prove that every element of A is also an element of B. Once the proof announces it's going to do this, it's a lot easier to see why the proof chooses to go down the route that it does.

Now, let's think about that other direction of implication. We need to prove for any sets A and B that if $A \subseteq B$, we'll have $A - B = \emptyset$. We can prove this in lots of different ways, but I think one of the easier approaches would be to use the contrapositive – let's prove that if $A - B \neq \emptyset$, then A is not a subset of B. The completed proof is shown here:

> ***Proof:*** We will prove both directions of implication.
>
> First, we'll prove that if $A - B = \emptyset$, then we will have $A \subseteq B$. Let A and B be arbitrary sets where $A - B = \emptyset$. We'll show $A \subseteq B$ by proving that every element of A is also an element of B.
>
> We know that $A - B = \emptyset$, meaning that the set of elements in A that are not in B (that is, $A - B$) is empty. Thus, there are no elements in A that are not also in B. Consequently, every element of A also belongs to B, and therefore $A \subseteq B$, as required.
>
> Next, we'll prove that if $A \subseteq B$, then $A - B = \emptyset$. To do so, we'll prove the contrapositive and show that if $A - B \neq \emptyset$, then A is not a subset of B. If $A - B \neq \emptyset$, then there is at least one element $x \in A - B$. Since $x \in A - B$, we know that $x \in A$ and that $x \notin B$. Therefore, it's not the case that every element of A is an element of B, so A is not a subset of B, as required. ■

Notice that this proof mixes and matches proof styles – we use a direct proof for one part of the iff and a proof by contrapositive for the other. This is fairly common; in fact, most interesting proofs contain elements of all sorts of types of proofs.

Example: Odd and Even Numbers

Consider the following theorem:

For any natural number n, the number $n^2 + n$ is even.

Here's one potential proof:

> ***Proof:*** By contradiction; assume there is some natural number n where $n^2 + n$ is odd. Consider the parity of n. If n is even, then n^2 is even and n is even, so their sum $n^2 + n$ must be even as well. This contradicts that $n^2 + n$ is odd. Otherwise, n is odd. Then n is odd and n^2 is odd, so their sum $n^2 + n$ must be even. This again contradicts that $n^2 + n$ is odd. In either case we reach a contradiction, so our assumption must have been wrong. Thus for any natural number n, the number $n^2 + n$ is even. ■

This proof is logically sound and stylistically has many nice aspects: it's easy to read and clearly lays out its argument. But while there's nothing *logically* wrong with this proof, but there is something *structurally* amiss. The argument of this proof is, essentially, the following:

1. Assume $n^2 + n$ is odd.
2. If n is even, then $n^2 + n$ is even, which is a contradiction.
3. If n is odd, then $n^2 + n$ is even, which is a contradiction.
4. Both cases reach a contradiction, so the assumption was wrong.
5. Thus $n^2 + n$ is even.

Notice that steps (2) and (3), collectively, form a direct proof that $n^2 + n$ is always even. Instead of structuring it as a proof by contradiction, we could just write it as a direct proof. Compare the above proof to this simpler proof given here, which uses the same basic argument but omits the proof by contradiction:

> ***Proof:*** Let n be an arbitrary integer. If n is even, then n^2 is even and n is even, so their sum $n^2 + n$ must be even as well. Otherwise, if n is odd, then n is odd and n^2 is odd, so their sum $n^2 + n$ must be even. Therefore, the sum $n^2 + n$ must be even. ■

This is much simpler, more compact, and to the point.

Proof by contradiction is often the easiest or simplest way to prove a result. If you want a challenge, try showing that the square root of two is irrational without using a proof by contradiction. However, in many cases proof by contradiction obscures a much simpler line of reasoning that could proceed directly. When writing a proof by contradiction, it's worth double-checking your argument after writing up a draft to see if it's actually necessary. If you can get away with a direct proof, it's often more elegant to do so.

Example: Contract Rummy

Contract rummy is a card game for any number of players (usually between three and five) in which players are dealt a hand of cards and, through several iterations of drawing and discarding cards, need to accumulate *sets* and *sequences*. A set is a collection of three cards of the same value, and a sequence is a collection of four cards of the same suit that are in ascending order. The game proceeds in multiple rounds in which players need to accumulate a different number of sets and sequences. The rounds are:

- Two sets (six cards)
- One set, one sequence (seven cards)
- Two sequences (eight cards)
- Three sets (nine cards)
- Two sets and a sequence (ten cards)
- One set and two sequences (eleven cards)
- Three sequences (twelve cards)

Notice that in each round, the requirements are such that the number of cards required increases by one. It's interesting that it's always possible to do this, since the total number of cards must be made using just combinations of three cards and four cards. In fact, we can prove this theorem:

> Any integer greater than five can be written as $3m + 4n$ for natural numbers m and n.

Let's take a look at an attempted proof of this result:

> ***Proof:*** Consider any natural number k that's greater than five (equivalently, k is greater than or equal to six). First, let's consider the case where k is a multiple of three. In that case, we can write $k = 3m$ for some integer m, as required.
>
> Next, consider the case where k is congruent to one modulo three. In that case, we can express the number k as $k = 3m + 1$ for some integer m. Clearly m has to be greater than or equal to two, so we can equivalently write k as $k = 3(m - 1) + 4 \cdot 1$, as required.
>
> Finally, consider the case where k is congruent to two modulo three. Using similar logic as above, we can then write $k = 3(m - 2) + 4 \cdot 2$, as required. ■

This proof is interesting in that it contains all the elements of a complete proof, but has a few issues. The basic outline of the proof is reasonable: we start with some arbitrary k, split into cases based on whether k is a multiple of three, is congruent to one modulo three, or is congruent to two modulo three, then show that in each case we can massage those definitions into something that's of the form $k = 3m + 4n$ for natural numbers m and n.

That said, the proof is skipping a few important steps that we think would be important to justify. Let's take a look at the last sentence of the first paragraph:

> In that case, we can write $k = 3r$ for some integer r, as required.

The goal, overall, is to show that there are natural numbers m and n such that $k = 3m + 4n$. Here, the proof has shown that there's an *integer* m where $k = 3m$. This isn't exactly what's needed in this

proof, since although all the natural numbers are integers, not all the integers are natural numbers. The proof needs to go one more step and explain why m would have to be nonnegative. This would probably use the fact that k is greater than or equal to six, meaning that k has to be positive, so m couldn't be negative.

There's a similar sort of error in the next paragraph, which I've reprinted here:

> Next, consider the case where k is congruent to one modulo three. In that case, we can express the number k as $k = 3m + 1$ for some integer m. Clearly m has to be greater than or equal to two, so we can equivalently write k as $k = 3(m - 1) + 4 \cdot 1$, as required.

The second sentence starts with “clearly,” which is probably an indicator that something's up. Remember from before - “clearly” and “obviously” are usually red flags! Here, the fact that m has to be at least two follows from the fact that k is at least six – if m *isn't* at least two, then k wouldn't be at least six. The proof would need to state this somewhere.

There's another problem with this paragraph. The paragraph concludes by saying that it's possible to write $k = 3(m - 1) + 4 \cdot 1$. That's great, but remember that the result specifically talks about writing out k as $3a + 4b$ for some *natural numbers* a and b. Here, $m - 1$ is most definitely a natural number because m is at least two. However, the readers of this proof have to figure this out for themselves, since the proof doesn't give any guidance.

For the purposes of CS103, we'd prefer if this proof were written out with some more guidance to the reader.

Now, let's suppose that the person who wrote the above proof got our feedback and decided to put in more detail. Here's one possible proof that might come back:

> ***Proof:*** Consider any natural number k that's greater than five (equivalently, k is greater than or equal to six). First, let's consider the case where k is a multiple of three. In that case, we can write $k = 3m$ for some integer m. Because $k = 3m$ and k is positive, we know that m is positive. Every positive integer is a natural number, because each natural number is either 0 or a positive whole number, and the integers consist of 0, the positive whole numbers, and the negative whole numbers. Therefore, we can write $k = 3m$ for some natural number m. As a further observation, notice that $3m$ is the same as $3m + 4 \cdot 0$, and 0 is a natural number. This means that we can choose natural numbers m and n such that $k = 3m + 4n$.
>
> […]

This proof has definitely cleaned up the previous issue (lack of detail), but the pendulum has swung too far in the opposite direction this time. While the extra justifications do help, in this case the proof spends a lot of time justifying statements that, from our perspective, are sufficiently obvious and don't need to be explained. For example, we think it's fine to just say that a positive integer is a natural number, and it's okay to leave out the part about $3m + 4 \cdot 0$ being the same as $3m$. The level of justification that we're looking for is a lot more along these lines:

Proof: Consider any natural number k that's greater than five (equivalently, k is greater than or equal to six). First, let's consider the case where k is a multiple of three. In that case, we can write $k = 3m$ for some integer m. Because $k = 3m$ and k is positive, we know that m is positive, so m is a natural number. Thus in this case, we can express k as needed.

[…]

This is about all that we'd need – I think this is perfectly fine as written and that the justifications are given at an appropriate level.

Just for fun, here's one last proof of this result, though it's definitely not something you should submit in CS103:

Proof: This follows as a special case of the Frobenius coin theorem with two coins, which says that given natural numbers a and b, all natural numbers greater than $ab - a - b$ can be written as the sum $am + bn$ for some natural numbers m and n. Here, $ab - a - b = 3 \cdot 4 - 3 - 4 = 12 - 7 = 5$, so the theorem follows. ■

This proof really isn't appropriate in CS103: we haven't talked about the Frobenius coin problem, few (if any) CS103 students have seen the result, and the course staff aren't likely to have seen it either. We're evaluate your ability to demonstrate clear lines of reasoning following from our general assumptions (essentially, high school algebra and what we've proven so far), and given that metric this proof doesn't quite work.

That said, the proof hopefully does open up your eyes to the fact that there's a *lot* of math out there and lots of fun results to explore. I'd recommend looking up the Frobenius coin problem in your spare time if you have the chance – it's quite an interesting read!