5. N is not divisible by any number less than or equal to p. *[by definition, $p!$ is divisible by each number less than or equal to p, so $p! + 1$ is not.]*
6. The prime factorization of N contains prime numbers greater than p. *[since N is divisible by each prime number in the prime factorization of N, and by line 5.]*
7. Therefore p is not the largest prime. *[by line 6, N is divisible by a prime larger than p.]*
8. This is a contradiction. *[from line 2 and line 7: the largest prime is p and there is a prime larger than p.]*
9. Therefore there are infinitely many primes. *[from line 1 and line 8: our only premise lead to a contradiction, so the premise is false.]*

We should say a bit more about the last line. Up through line 8, we have a valid argument with the premise "there are only finitely many primes" and the conclusion "there is a prime larger than the largest prime." This is a valid argument as each line follows from previous lines. So if the premises are true, then the conclusion *must* be true. However, the conclusion is NOT true. The only way out: the premise must be false.

The sort of line-by-line analysis we did above is a great way to really understand what is going on. Whenever you come across a proof in a textbook, you really should make sure you understand what each line is saying and why it is true. Additionally, it is equally important to understand the overall structure of the proof. This is where using tools from logic is helpful. Luckily there are a relatively small number of standard proof styles that keep showing up again and again. Being familiar with these can help understand proof, as well as give ideas of how to write your own.

Direct Proof

The simplest (from a logic perspective) style of proof is a **direct proof**. Often all that is required to prove something is a systematic explanation of what everything means. Direct proofs are especially useful when proving implications. The general format to prove $P \to Q$ is this:

> Assume P. Explain, explain, ..., explain. Therefore Q.

Often we want to prove universal statements, perhaps of the form $\forall x(P(x) \to Q(x))$. Again, we will want to assume $P(x)$ is true and deduce $Q(x)$. But what about the x? We want this to work for *all* x. We accomplish this by fixing x to be an arbitrary element (of the sort we are interested in).

Here are a few examples. First, we will set up the proof structure for a direct proof, then fill in the details.

Example 3.2.2

Prove: For all integers n, if n is even, then n^2 is even.

Solution. The format of the proof will be this: Let n be an arbitrary integer. Assume that n is even. Explain explain explain. Therefore n^2 is even.

To fill in the details, we will basically just explain what it means for n to be even, and then see what that means for n^2. Here is a complete proof.

Proof. Let n be an arbitrary integer. Suppose n is even. Then $n = 2k$ for some integer k. Now $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$. Since $2k^2$ is an integer, n^2 is even. QED

Example 3.2.3

Prove: For all integers a, b, and c, if $a|b$ and $b|c$ then $a|c$. (Here $x|y$, read "x divides y" means that y is a multiple of x, i.e., that x will divide into y without remainder).

Solution. Even before we know what the divides symbol means, we can set up a direct proof for this statement. It will go something like this: Let a, b, and c be arbitrary integers. Assume that $a|b$ and $b|c$. Dot dot dot. Therefore $a|c$.

How do we connect the dots? We say what our hypothesis ($a|b$ and $b|c$) really means and why this gives us what the conclusion ($a|c$) really means. Another way to say that $a|b$ is to say that $b = ka$ for some integer k (that is, that b is a multiple of a). What are we going for? That $c = la$, for some integer l (because we want c to be a multiple of a). Here is the complete proof.

Proof. Let a, b, and c be integers. Assume that $a|b$ and $b|c$. In other words, b is a multiple of a and c is a multiple of b. So there are integers k and j such that $b = ka$ and $c = jb$. Combining these (through substitution) we get that $c = jka$. But jk is an integer, so this says that c is a multiple of a. Therefore $a|c$. QED

Proof by Contrapositive

Recall that an implication $P \to Q$ is logically equivalent to its contrapositive $\neg Q \to \neg P$. There are plenty of examples of statements which are hard to prove directly, but whose contrapositive can easily be proved directly. This is all that **proof by contrapositive** does. It gives a direct

proof of the contrapositive of the implication. This is enough because the contrapositive is logically equivalent to the original implication.

The skeleton of the proof of $P \to Q$ by contrapositive will always look roughly like this:

Assume $\neg Q$. Explain, explain, ... explain. Therefore $\neg P$.

As before, if there are variables and quantifiers, we set them to be arbitrary elements of our domain. Here are two examples:

Example 3.2.4

Is the statement "for all integers n, if n^2 is even, then n is even" true?

Solution. This is the converse of the statement we proved above using a direct proof. From trying a few examples, this statement definitely appears to be true. So let's prove it.

A direct proof of this statement would require fixing an arbitrary n and assuming that n^2 is even. But it is not at all clear how this would allow us to conclude anything about n. Just because $n^2 = 2k$ does not in itself suggest how we could write n as a multiple of 2.

Try something else: write the contrapositive of the statement. We get, for all integers n, if n is odd then n^2 is odd. This looks much more promising. Our proof will look something like this:

Let n be an arbitrary integer. Suppose that n is not even. This means that .... In other words .... But this is the same as saying .... Therefore n^2 is not even.

Now we fill in the details:

Proof. We will prove the contrapositive. Let n be an arbitrary integer. Suppose that n is not even, and thus odd. Then $n = 2k + 1$ for some integer k. Now $n^2 = (2k+1)^2 = 4k^2+4k+1 = 2(2k^2+2k)+1$. Since $2k^2 + 2k$ is an integer, we see that n^2 is odd and therefore not even. QED

Example 3.2.5

Prove: for all integers a and b, if $a + b$ is odd, then a is odd or b is odd.

Solution. The problem with trying a direct proof is that it will be hard to separate a and b from knowing something about $a + b$. On the other hand, if we know something about a and b separately, then combining them might give us information about $a + b$. The

contrapositive of the statement we are trying to prove is: for all integers a and b, if a and b are even, then $a + b$ is even. Thus our proof will have the following format:

Let a and b be integers. Assume that a and b are both even. la la la. Therefore $a + b$ is even.

Here is a complete proof:

Proof. Let a and b be integers. Assume that a and b are even. Then $a = 2k$ and $b = 2l$ for some integers k and l. Now $a + b = 2k + 2l = 2(k+1)$. Since $k+l$ is an integer, we see that $a+b$ is even, completing the proof. QED

Note that our assumption that a and b are even is really the negation of a or b is odd. We used De Morgan's law here.

We have seen how to prove some statements in the form of implications: either directly or by contrapositive. Some statements are not written as implications to begin with.

Example 3.2.6

Consider the following statement: for every prime number p, either $p = 2$ or p is odd. We can rephrase this: for every prime number p, if $p \neq 2$, then p is odd. Now try to prove it.

Solution.

Proof. Let p be an arbitrary prime number. Assume p is not odd. So p is divisible by 2. Since p is prime, it must have exactly two divisors, and it has 2 as a divisor, so p must be divisible by only 1 and 2. Therefore $p = 2$. This completes the proof (by contrapositive). QED

Proof by Contradiction

There might be statements which really cannot be rephrased as implications. For example, "$\sqrt{2}$ is irrational." In this case, it is hard to know where to start. What can we assume? Well, say we want to prove the statement P. What if we could prove that $\neg P \rightarrow Q$ where Q was false? If this implication is true, and Q is false, what can we say about $\neg P$? It must be false as well, which makes P true!

This is why **proof by contradiction** works. If we can prove that $\neg P$ leads to a contradiction, then the only conclusion is that $\neg P$ is false, so P is true. That's what we wanted to prove. In other words, if it is impossible for P to be false, P must be true.

Here are three examples of proofs by contradiction:

Example 3.2.7

Prove that $\sqrt{2}$ is irrational.

Solution.
Proof. Suppose not. Then $\sqrt{2}$ is equal to a fraction $\frac{a}{b}$. Without loss of generality, assume $\frac{a}{b}$ is in lowest terms (otherwise reduce the fraction). So,

$$2 = \frac{a^2}{b^2}$$

$$2b^2 = a^2.$$

Thus a^2 is even, and as such a is even. So $a = 2k$ for some integer k, and $a^2 = 4k^2$. We then have,

$$2b^2 = 4k^2$$

$$b^2 = 2k^2.$$

Thus b^2 is even, and as such b is even. Since a is also even, we see that $\frac{a}{b}$ is not in lowest terms, a contradiction. Thus $\sqrt{2}$ is irrational. QED

Example 3.2.8

Prove: There are no integers x and y such that $x^2 = 4y + 2$.

Solution.
Proof. We proceed by contradiction. So suppose there *are* integers x and y such that $x^2 = 4y + 2 = 2(2y + 1)$. So x^2 is even. We have seen that this implies that x is even. So $x = 2k$ for some integer k. Then $x^2 = 4k^2$. This in turn gives $2k^2 = (2y + 1)$. But $2k^2$ is even, and $2y + 1$ is odd, so these cannot be equal. Thus we have a contradiction, so there must not be any integers x and y such that $x^2 = 4y + 2$. QED

Example 3.2.9

The **Pigeonhole Principle**: If more than n pigeons fly into n pigeon holes, then at least one pigeon hole will contain at least two pigeons. Prove this!

Solution.
Proof. Suppose, contrary to stipulation, that each of the pigeon holes contain at most one pigeon. Then at most, there will be n pigeons. But we assumed that there are more than n pigeons, so this is impossible. Thus there must be a pigeonhole with more than one pigeon. QED

While we phrased this proof as a proof by contradiction, we could have also used a proof by contrapositive since our contradiction was simply the negation of the hypothesis. Sometimes this will happen, in which case you can use either style of proof. There are examples however where the contradiction occurs "far away" from the original statement.

Proof by (counter) Example

It is almost NEVER okay to prove a statement with just an example. Certainly none of the statements proved above can be proved through an example. This is because in each of those cases we are trying to prove that something holds of all integers. We claim that n^2 being even implies that n is even, *no matter what integer* n we pick. Showing that this works for $n = 4$ is not even close to enough.

This cannot be stressed enough. If you are trying to prove a statement of the form $\forall x P(x)$, you absolutely CANNOT prove this with an example.[1]

However, existential statements can be proven this way. If we want to prove that there is an integer n such that $n^2 - n + 41$ is not prime, all we need to do is find one. This might seem like a silly thing to want to prove until you try a few values for n.

n	1	2	3	4	5	6	7
$n^2 - n + 41$	41	43	47	53	61	71	83

So far we have gotten only primes. You might be tempted to conjecture, "For all positive integers n, the number $n^2 - n + 41$ is prime." If you wanted to prove this, you would need to use a direct proof, a proof by contrapositive, or another style of proof, but certainly it is not enough to give even 7 examples. In fact, we can prove this conjecture is *false* by proving its negation: "There is a positive integer n such that $n^2 - n + 41$ is not prime." Since this is an existential statement, it suffices to show that there does indeed exist such a number.

In fact, we can quickly see that $n = 41$ will give 41^2 which is certainly not prime. You might say that this is a counterexample to the conjecture

[1]This is not to say that looking at examples is a waste of time. Doing so will often give you an idea of how to write a proof. But the examples do not belong in the proof.