Proving the division algorithm (what we did in class):

For everything that follows, we are working with an integer a that is the dividend, and a positive integer $b > 0$ that is the divisor.

Now, no matter what integer you pick as a stand-in for the quotient (we'll call it *k*), you can always solve division equation to get another integer (like the remainder) that will let us write a true equation that is in the format of the division equation:
$a = bk + (a - bk)$
In order to really count as division, that remainder number has to be positive and less than the divisor.

The first thing to do is to go out looking for a way to be sure that you can get $a - bk$ to be at least 0. An example where it has to be 0 or positive would be great. It turns out, by trial and error (and looking in the textbook) that if $k = -|a|$, that works:

if $k = -|a|$

then $a - bk = a - b(-|a|) = a + b|a|$

Think about that:

If *a* is positive, then of course $a + b|a|$ is positive.

If *a* is negative, $b|a| \geq |a|$, because $b > 0$ and so $b \geq 1$

and so $a + b|a| \geq a + |a| = 0$, so $a + b|a|$ is positive or 0

If *a* is 0, then $a + b|a| = 0$

That covers all of the possibilities: no matter what *a* is, $a + b|a| = a - bk \geq 0$

That means, if we look at all of the integers of the form $a - bk$, then some of them will be greater than or equal to 0. (in particular the one when $k = -|a|$)

So, now we can define the set of these remainder-like-numbers that are non-negative:

$$S = \{a - bk \mid a + bk \geq 0 \text{ and } k \in \mathbb{Z}\}$$

Everything in the set is an integer (because *a*, *b*, and *k* are all integers). We haven't proved it, but there are infinitely many numbers in the set. We have proved that there is at least one number in the set, so the set is non-empty.

Now we can use the Well-Ordering axiom, which says S will have a smallest element. I want to do some algebra on that smallest element, so I'm going to name it: $r = a - bK$

I want to be able to say that $r < b$ because it's the smallest element in the set, but that's hard to explain, so instead I go for a contradiction argument:

Suppose that $a - bK \geq b$

That would mean that $a - bK - b \geq 0$
And I can rewrite that to say $a - b(K + 1) \geq 0$
This contradicts one of the statements above. *Which one does it contradict?*

Note that when you start a proof by contradiction, you always start by "**supposing**" the logical opposite of what you want to prove true.