CIS260-201/204–Spring 2008

How To Begin a Proof

Friday, February 15

In this course we will be, and have been, proving many statements. One problem that one who just begins to learn how to prove is that one does not know where to start. This guide should give you some clues about how you tackle some particular kinds of proofs, step by step.

1 Know What You Want To Prove

First of all, you need to know what result you want to obtain at the end of the proof. Though this comes at the end of the proof, it is the first thing you need to keep in mind all the time when writing the proof so you don't digress on the way from the beginning to the end. For example, referring to Exercise 9.6 in Homework 2, define

$$A = \{x \in \mathbb{Z} : a \mid x\}$$

and

$$B = \{x \in \mathbb{Z} : b \mid x\}.$$

Prove that if $b \mid a$, then $A \subseteq B$.

Note that this is only one part of the question; there is another but we will not talk about it for now.

So, what do you want to prove in this case? The answer seems obvious: Prove that $A \subseteq B$. What this means is that you should try to think about proving that one set is a subset of another right away.

2 Unravel the Definition

Once you know the goal, try to extract as much information as you can from it. Usually, your goal will be short. As in the previous example (that will be used throughout this document), your goal is to show that $A \subseteq B$. What does this mean? Now you probably want to consider the *definition* of subset: A is a subset of B if for every element x in A, x is also an element in B.

Once you can expand what you have, you had better not forget it. Write it down! This is usually the first sentence in your proof. So, you write

> To prove that $A \subseteq B$, we need to show that for all $x \in A$, $x \in B$.

Now look at what you wrote. Can you expand more? In some cases, you can; in others, you cannot. If you cannot expand the statement more, that is the best you can do at this point, so skip to the next step. For our example, however, you can. We need to show that for every element x in A, x is also an element of B. So, no matter how we pick an element in A, that element should be in B. This is what we need to show for the moment. Here comes the second sentence in the proof:

> Let x be an arbitrary element in A.

Look again. What does it mean for an element to be in A? By the *definition* of A, $x \in A$ if $a \mid x$. So, now we know that $a \mid x$, and what should we do next? Expand it! Here come the next sentences:

> Since $x \in A$, $a \mid x$. By the definition of divisibility, there exists an integer k such that $ak = x$.

One thing to note: The book uses letter c instead of k. Why doesn't it matter? If you try to change k to c, you will not alter the meaning of the statement in any way. We call this kind of variable a *dummy* variable. You can use any letter, as long as it does not conflict with the letters already in the statement.

At this point you probably agree that we cannot do better by just expanding statements. Here is where this step ends. As you see, we already have several lines of proof by just expanding what we know.

3 Utilize Other Information

Once you get stuck, you should seek other information provided to you. In our example, you see the condition "if $b \mid a$." This should be a good place to use it. Again, expand the information as much as you can. The next statements follow:

> By assumption, $b \mid a$. By the definition of divisibility, there exists an integer ℓ such that $b\ell = a$.

Stop! Before you go on, make sure that you did not introduce any variables already in use. In this case, introducing k again will lead you to trouble. Use something else. When you are certain that you did not make this simple mistake, proceed.

Stop! What? We have the statement, "If $b \mid a$, then $A \subseteq B$," but why didn't we use the fact that $b \mid a$ in the first place–at the beginning? The first proof you learned in this course does use the given fact in the first sentence, but not this proof. The reason is that the information given in the "if" part of the statement is the *assumption* that should hold true for this statement. Note the period at the end of the last statement: It says that the assumption is true *at any time* in the proof. Therefore, you are allowed use this assumption at any point in the proof, not just at the beginning. The first proof you learned happens to use the assumption at the beginning, but many other proofs use it somewhere on the way. Our example uses it right at the middle. This is a crucial point. Don't go on to the next section if you don't understand this paragraph.

4 Connect the Logic

Now that we have utilized all the tools, it is time to put them together. Let's summarize what we have so far:

> To prove that $A \subseteq B$, we need to show that for all $x \in A$, $x \in B$. Let x be an arbitrary element in A. Since $x \in A$, $a \mid x$. By the definition of divisibility, there exists an integer k such that $ak = x$. By assumption, $b \mid a$. By the definition of divisibility, there exists an integer ℓ such that $b\ell = a$.

So, we know that $ak = x$ and $b\ell = a$. Let's substitute $b\ell$ in the first statement and obtain

$$b\ell k = x.$$

And let's write that down:

> Hence, there exist integers k and ℓ such that $b\ell k = x$.

This is the crux of the proof. The hardest part is connecting one end to the other. Most people will get stuck at this point because they have no clue where to go next. Don't worry. It comes with practice. The more you practice, the more you are able to see which way you should go.

5 Proceed To the Goal

The logic part is like the climax of a mountain. When we unraveled the definition, we climb the mountain. Once we reached the climax, we try to go down. If you have a hiking experience, going down is just as difficult as climbing up. Being careless will pull you down too fast and quite often will result in you being on the ground, sometimes rolling down. Same here. We need to be as careful as when we start the proof. And why are we talking about climbing up and down? Because the two processes are just (quite) the reverse of each other. For the up part, we unravel the definition, i.e., use the longhand version of a shorthand version. Now that we have the longhand version and are going down, let's roll back and use the shorthand version.

So, we need to show, in the end, that $x \in B$. This means that, by the definition of B, $b \mid x$. By the definition of divisibility, there exists an integer m such that $bm = x$. Wait a second. We already have $b\ell k = x$. So, if we just let m equal ℓk, then we should be in a good shape. Let's do that and finish the proof:

> Let $m = \ell k$. Then there exists an integer m such that $bm = x$. By the definition of divisibility, $b \mid x$. By the definition of B, this means that $x \in B$.

Notice that the quotation just states the reverse of what we have right before the quotation.

Looks like we are done, but the final step is to recognize our goal: $A \subseteq B$. Here comes the summary of the proof at the end:

> Since we have shown that for any element x in A, $x \in B$, we have shown that $A \subseteq B$, as required.

And we are done.

Here is the full proof of the statement "If $b \mid a$, then $A \subseteq B$:"

> To prove that $A \subseteq B$, we need to show that for all $x \in A$, $x \in B$. Let x be an arbitrary element in A. Since $x \in A$, $a \mid x$. By the definition of divisibility, there exists an integer k such that $ak = x$. By assumption, $b \mid a$. By the definition of divisibility, there exists an integer ℓ such that $b\ell = a$. Hence, there exist integers k and ℓ such that $b\ell k = x$. Let $m = \ell k$. Then there exists an integer m such that $bm = x$. By the definition of divisibility, $b \mid x$. By the definition of B, this means that $x \in B$. Since we have shown that for any element x in A, $x \in B$, we have shown that $A \subseteq B$, as required. □

6 Another Example

Now we want to prove the converse of the last statement: If $A \subseteq B$, then $b \mid a$. First, the goal is to prove that $b \mid a$. The assumption we have is that $A \subseteq B$, i.e., if we know that an element is in A, that element is in B for sure.

What does it mean for $b \mid a$? You might be tempted to go back to the definition of divisibility and say that there must exist an integer k such that $bk = a$. But look around. Do we have any other definition in hand? Given with the statement are the definitions of A and B. Let's remind ourselves of those definitions:

$$A = \{x \in \mathbb{Z} : a \mid x\}$$

and

$$B = \{x \in \mathbb{Z} : b \mid x\}.$$

So, the definition of B looks close to our goal. Let's think about it. If we want to show that $b \mid a$, we can just show that $a \in B$ and be done in this case. What else do we know? The assumption. So, going further, if we can just show that $a \in A$, then by assumption, $a \in B$, and by the definition of B, $b \mid a$. Now our goal comes down to showing that $a \in A$.

What does it mean for $a \in A$? By the definition of A, a must divide a. Now, we just need to show that $a \mid a$. At this point you might say that, well, it's just true that any integer divides itself. If you are convinced, that's fine. If not, there is of course one other argument, using the definition of divisibility. If $a \mid a$, there exists an integer k such that $ak = a$. Don't confuse this k with the k above. The previous k was not used in any way, so we can use it here. What is this k? Now it should be obvious to you that $k = 1$.

From the whole argument, we should be able to complete the proof now. Let's do it.

> In order to show that $b \mid a$, it suffices to show that $a \in B$. First, $a \mid a$ because there exists an integer, namely 1, such that $a \cdot 1 = a$. By the definition of A, $a \in A$. By assumption, $A \subseteq B$. Since $a \in A$, $a \in B$. By the definition of B, $b \mid a$, as required. □