Proof Series Episode 2: Direct Proofs (Non-Assessable)

The most important skill in computer science is communicating your ideas. A proof is an argument to explain why your statement is true to someone else. This document will walk you through the thought process behind a proof.

Keep in Mind

- **Who is your audience?** This is important since you need to identify what knowledge the reader has and the tone of your proof. For this course, you can imagine that the reader is another student who has watched the lectures but does not know the proof for this fact. This means you can use the definitions and theorems in the lectures in your proof.
- **Write in full English sentences.** Avoid shorthand abbreviations or symbols such as $\therefore$ (this symbol can be replaced with "Therefore") and write in full sentences. You should be able to read your proof out loud to someone else.

Starting the Proof

We will be tackling Exercise 7 from Tutorial 1. We want to prove the following statement:

"For positive integers a, b, c where $ab \mid bc$, show that $a \mid c$."

A good starting point is to state your hypotheses and conclusion. That is, write the facts that you can assume and the statement you want to conclude with. From this statement, our hypotheses are

- The values of a, b, c are positive integers,
- We have $ab \mid bc$.

Our conclusion should be that $a \mid c$. From here, one good way to progress is to see if any simplifications can be made or if any facts can be rewritten through definitions. Consider the following definition:

"We say that $x \mid y$ when $y = kx$ for some integer k."

We can rewrite our second hypothesis to create a new fact we can use! We know that $ab \mid bc$ so there exists an integer k such that $bc = kab$.

Working Backwards

When you are not sure how to progress, a good idea is working on the conclusion. Keep in mind that the steps you do on the conclusion have to be reversible!

Unfolding definitions is always reversible so we can change our goal from $a \mid c$ to $c = ja$ for some integer j. I have given a different name to j since it could be different to k.

Connecting the Bridge

We can now re-examine what we know and what we want to prove. We know that

- The values of a, b, c are positive integers,
- We have $ab \mid bc$,
- There exists an integer k such that $bc = kab$.

We want to conclude that $c = ja$. A clear path has formed! We can divide both sides of $bc = kab$ by b and get our conclusion. It is always important to examine why we can do certain steps. Division requires the condition that b is not 0! We can justify division since b is positive meaning it is not 0.

Writing the Proof

Answer(s)

Let a, b, c be positive integers such that $ab \mid bc$. By definition, we know that there exists an integer k such that $bc = kab$. We know $b \neq 0$ as b is positive. This means we can divide both sides by b to obtain $c = ka$. By definition, we find that $a \mid c$.

1. The first statement states our hypotheses.
2. We use our definitions to create new facts.
3. We derive new facts from justified logical steps.
4. We prove our goal after working on the conclusion.
5. We state the steps that we took, when working backwards, in reverse order.

This is called direct proof since we started with what we knew and derived facts through logical steps until we concluded. This was a direct path from start to finish.

Another Example

From the lecture, we know that

$$a =_{(n)} b \text{ if and only if } a \,\%\, n = b \,\%\, n.$$

This is can be broken down into two statements:

- If $a =_{(n)} b$ then $a \,\%\, n = b \,\%\, n$,
- If $a \,\%\, n = b \,\%\, n$ then $a =_{(n)} b$.

We will work towards proving the first statement, which is

$$\text{“For } a, b \in \mathbb{Z} \text{ and } n \in \mathbb{Z}_{>0}, \text{ if } a =_{(n)} b \text{ then } a \,\%\, n = b \,\%\, n.\text{”}$$

We state our hypotheses as

- The values of a, b are integers,
- We know n is a positive integer.

Our conclusion is “if $a =_{(n)} b$ then $a \,\%\, n = b \,\%\, n$”.

Concept(s)

When our conclusion is in the form of “If Statement1 then Statement2”, we can place Statement1 into our hypotheses and change our conclusion to Statement2.

Using this idea, we have a new hypothesis that $a =_{(n)} b$ and our conclusion becomes $a \,\%\, n = b \,\%\, n$. We can now begin to uncover our definitions. In particular, $a =_{(n)} b$ means that $a - b = kn$ for some integer k. From here, there are many ways to progress the proof.

One method is to consider the conclusion. If we want to work with $a \,\%\, n$ and $b \,\%\, n$, we need some way to introduce these ideas. We can do this by Euclid's division lemma which states

$$a = \left\lfloor \frac{a}{n} \right\rfloor n + a \,\%\, n \text{ and } b = \left\lfloor \frac{b}{n} \right\rfloor n + b \,\%\, n.$$

We can create a new fact by substituting these forms into our statement that $a - b = kn$. This gets us

$$\left\lfloor \frac{a}{n} \right\rfloor n + a \,\%\, n - \left\lfloor \frac{b}{n} \right\rfloor n - b \,\%\, n = kn.$$

You might notice the terms $a \,\%\, n$ and $-b \,\%\, n$ on the left-hand side. One logical step we can do is to isolate these terms by making them the subject where

$$a \,\%\, n - b \,\%\, n = kn - \left\lfloor \frac{a}{n} \right\rfloor n + \left\lfloor \frac{b}{n} \right\rfloor n.$$

If we can prove our left-hand side, $a \,\%\, n - b \,\%\, n$, is equal to 0, then we can prove our conclusion so we can update our goal to be $a \,\%\, n - b \,\%\, n = 0$. If you get stuck on a step, don't be afraid to write out some ideas or related theorems! Here are some ideas that I had:

- $0 \leq a \,\%\, n < n$ and $0 \leq b \,\%\, n < n$
- All terms on the right-hand side are multiples of n
- Any properties the left-hand side has is true for the right-hand side and vice versa

Since the right-hand side is divisible by n, we know that $n \mid a \,\%\, n - b \,\%\, n$ as well. From our intervals, we also know that $-n < a \,\%\, n - b \,\%\, n < n$ (Why? Try verify this yourself). We can combine these two facts: the only number between $-n$ and n that is divisible by n is 0! This means that $a \,\%\, n - b \,\%\, n = 0$ is the only possibility. This proves our goal and completes our path. Let's put it into one clear proof!

Answer(s)

Let a, b be integers and let n be a positive integer such that $a =_{(n)} b$. By definition, there exists an integer k such that $a - b = kn$. From Euclid's division lemma, we know that

$$a = \left\lfloor \frac{a}{n} \right\rfloor n + a \,\%\, n \text{ and } b = \left\lfloor \frac{b}{n} \right\rfloor n + b \,\%\, n.$$

We can substitute these values for a and b into our equation to get

$$\left\lfloor \frac{a}{n} \right\rfloor n + a \,\%\, n - \left\lfloor \frac{b}{n} \right\rfloor n - b \,\%\, n = kn.$$

Rearranging our equation, we find that

$$a \,\%\, n - b \,\%\, n = n \left(k - \left\lfloor \frac{a}{n} \right\rfloor + \left\lfloor \frac{b}{n} \right\rfloor \right).$$

Since $k - \left\lfloor \frac{a}{n} \right\rfloor + \left\lfloor \frac{b}{n} \right\rfloor$ is an integer, we find that $n \mid a \,\%\, n - b \,\%\, n$. We know that $0 \leq a \,\%\, n < n$ and $0 \leq b \,\%\, n < n$. This means that $-n < a \,\%\, n - b \,\%\, n < n$. The only number which is divisible by n in this range is 0. Therefore, we must have

$$a \,\%\, n - b \,\%\, n = 0.$$

We have shown that $a \,\%\, n = b \,\%\, n$ and this concludes our proof.

Exercises

Write a formal proof for each statement below:

1. Let A, B, C be sets. If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.
2. Let a, b, c, d be integers. If $a =_{(n)} b$ and $c =_{(n)} d$, then $a - b =_{(n)} c - d$.
3. For $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}_{>0}$, if $a \,\%\, n = b \,\%\, n$ then $a =_{(n)} b$.