question 4 views

Daily Challenge 1.6

(**Due: Sunday 4/29 at 12:00 noon Eastern**.)

Review

Let's take stock of what we've learned about proofs so far.

A **proof** of a statement like "p implies q" is a series of logical deductions which begins by assuming that p is true and ends by showing that q must be true. For instance,

Theorem. If a is an even integer, then $a+1$ is an odd integer.

Proof. We begin by assuming that a is an even integer. By the definition of even, it follows that $a=2k$ for some integer k. Then the number $a+1$ can be written as $2k+1$, where again k is an integer. But the definition of "odd" says that a number m is odd if $m=2n+1$ for some integer n, so the preceding sentence shows that $a+1$ satisfies this definition. Therefore, we have found that $a+1$ is odd. $\square$.

This proof is really a series of separate "moves":

1. First assume a is even.
2. Use the definition of "even" to conclude something about a: it is twice an integer.
3. Apply (2) to find that $a+1$ is twice an integer plus one.
4. Use the definition of "odd" to show that $a+1$ is odd.

I find it very helpful to think of a proof the way one thinks of a chess game: there is some big-picture *strategy* which you move toward by using specific *tactics* like the moves above (I learned this way of thinking about proofs from Paul Zeitz's book).

Let's see another example. First, some definitions: we say that a *divides* b, and write $a \mid b$, if $\frac{b}{a}$ is an integer. For instance, 2 divides 10 because $\frac{10}{2}$ is 5 (we also say that 2 is a *divisor* of 10).

If a does not divide b, we write $a \nmid b$. For example, $3 \nmid 10$.

Theorem. Let a, b, c be integers. If a divides b and b divides c, then a divides c.

Proof. We have two assumptions: a divides b and b divides c. Our goal is to show that, whenever these assumptions are true, it must also be true that a divides c.

Our first move is to replace statements with their definitions, using named variables. If a divides b, then $\frac{b}{a}$ is an integer. Let's name this integer n, so that $\frac{b}{a}=n$.

We do the same thing for the second assumption. If b divides c, then $\frac{c}{b}$ is an integer. Call that integer m, so that $\frac{c}{b}=m$.

The thing we want to show is that a divides c. So we need to prove that $\frac{c}{a}$ is an integer. To show this, we can re-write $\frac{c}{a}$ as

$$\frac{c}{a}=\frac{c}{b}\times\frac{b}{a}=m\times n.$$

We know that m and n are integers, so their product $m\times n$ is also an integer. Therefore, we have shown that $\frac{c}{a}$ is an integer, so $c \mid a$. This is what we wanted to show. $\square$

Problem

Read the divisibility proof above carefully and make sure you understand it. Then try to prove the following.

Theorem. Suppose a, b, c are integers. If a divides b and a divides c, then a divides $(b-c)$.

daily_challenge

Updated 11 months ago by Christian Ferko

the students' answer, *where students collectively construct a single answer*

Proof (Corbin) -
We must prove the statement that "a,b,c are integers. If a divides b and a divides c, then a divides (b−c)." First I would like to expand this out so the statement becomes $\frac{b-c}{a}=\frac{b}{a}-\frac{c}{a}$. From here I will assign $\frac{b}{a}=x$ and $\frac{c}{a}=y$. This means that $\frac{b}{a}-\frac{c}{a}=x-y$ And since both x and y are in $\mathbb{Z}$ this means that $x-z$ is also in $\mathbb{Z}$. $\square$

Proof (Logan) - **I must prove that: "a,b,c are integers. If a divides b and a divides c, then a divides (b−c)." First, I can assign each of these statements a variable. a divides b can be written as $\frac{b}{a}=g$, and similarly a divides c can be written as $\frac{c}{a}=h$. I must prove that $\frac{(b-c)}{a}\in\mathbb{Z}$. Unfortunately I do not know where to to progress beyond this point, and a reasonable amount of time has been spent staring and making no logical progress.**

Updated 10 months ago by Corbin and 3 others

the instructors' answer, *where instructors collectively construct a single answer*

Proof (Christian). If a divides b, then $\frac{b}{a} = m$ for some integer m. Likewise, if a divides c, then $\frac{c}{a} = n$ for some integer n.

Now we wish to show that a divides $(b - c)$, which means that we must prove that $\frac{b-c}{a}$ is an integer. But we can express $\frac{b-c}{a}$ as

$$\frac{b-c}{a} = \underbrace{\frac{b}{a}}_{=m} - \underbrace{\frac{c}{a}}_{=n} = m - n,$$

where we have used the variables m and n defined above.

Since m and n are integers, the difference $m - n$ is also an integer. Therefore we have shown that $\frac{b-c}{a}$ is an integer, which means that a divides $(b - c)$. $\square$

Updated 11 months ago by Christian Ferko

followup discussions *for lingering questions and comments*