CSC110 Lecture 9: Programming and Proofs

Print this handout

Exercise 1: Practice with proofs

Definition. Let $n, d \in \mathbb{Z}$. We say that d **divides** n, or n **is divisible by** d, when there exists a $k \in \mathbb{Z}$ such that $n = dk$.

Using the symbols of predicate logic, we can define divisibility as follows:

$$d \mid n : "\exists k \in \mathbb{Z},\ n = dk" \quad \text{where } n, d \in \mathbb{Z}$$

1. Consider the following statement.

$$\forall n, d, a \in \mathbb{Z},\ d \mid n \Rightarrow d \mid an$$

   a. Rewrite this statement in symbolic logic, but with the definition of divisibility expanded.

$$\forall n, d, a \in \mathbb{Z},\ (\exists k_1 \in \mathbb{Z},\ n = dk_1) \Rightarrow (\exists k_2 \in \mathbb{Z},\ an = dk_2)$$

   b. Prove this statement.

Let $n, d, a \in \mathbb{Z}$.
Assume there is a $k_1 \in \mathbb{Z}$ that is such that $n = dk_1$. We need to show $\exists k_2 \in \mathbb{Z},\ an \stackrel{?}{=} dk_2$.

We filled in this blank after

Let $k_2 = \underline{\ ak_1\ }$.

$k_2 \in \mathbb{Z}$.

aside:

an/d

doing this rough work

Then $\boxed{dk_2} = d(ak_1)$

want to go from here to here

$\vdots = adk_1$

$= an$

work backwards to determine value for k_2

can't assume this is $\in \mathbb{Z}$.

$\therefore \exists k_2 \in \mathbb{Z},\ an = dk_2$ as required.

2. Consider this statement:

$$\forall n, d, a \in \mathbb{Z},\ d \mid an \Rightarrow d \mid a \vee d \mid n$$

This statement is *False*, so here you'll disprove it.

a. First, write the negation of this statement. You might need to review the negation rules in the [Course Notes Section 3.2 (https://www.teach.cs.toronto.edu/~csc110y/fall/notes/03-logic/02-predicate-logic.html#manipulating-negation)](https://www.teach.cs.toronto.edu/~csc110y/fall/notes/03-logic/02-predicate-logic.html#manipulating-negation).

$\neg(\forall n, d, a \in \mathbb{Z},\ d \mid an \Rightarrow (d \mid a) \vee (d \mid n))$

or, equivalently

$\exists n, d, a \in \mathbb{Z},\ \neg(d \mid an \Rightarrow (d \mid a) \vee (d \mid n))$

$\therefore \exists n, d, a \in \mathbb{Z},\ \neg(\neg(d \mid an) \vee ((d \mid a) \vee (d \mid n)))$

$\therefore \exists n, d, a \in \mathbb{Z},\ (d \mid an) \wedge \neg((d \mid a) \vee (d \mid n))$

$\therefore \exists n, d, a \in \mathbb{Z},\ (d \mid an) \wedge d \nmid a \wedge d \nmid n$

b. Prove the negation of the statement. (By proving the statement's negation is True, you'll prove that the original statement is False.)

we want to find (because of $\exists$) a setting for $n, d, a \in \mathbb{Z}$ that satisfies each of $d \mid an$, $d \nmid a$, $d \nmid n$

Let $n = 4$
$d = 6$
$a = 3$

Then $d \mid (an)$ ✓

$d \nmid a$ ✓ since $d > a$

$d \nmid n$ ✓ since $d > n$

(and apply result from slides that gives an upper bound on divisors)

Additional Exercises

1. Prove the following statement, which extends the first statement in Exercise 1.

$$\forall n, m, d, a, b \in \mathbb{Z},\ d \mid n \land d \mid m \Rightarrow d \mid (an + bm)$$

2. *Disprove* the following statement, which is very similar to the one we proved in the second part of today's lecture.

$$\forall p \in \mathbb{Z},\ Prime(p) \Leftrightarrow \big(p > 1 \land (\forall d \in \mathbb{N},\ 2 \leq d < \sqrt{p} \Rightarrow d \nmid p)\big).$$

Hint: the change is from $\leq \sqrt{p}$ to $< \sqrt{p}$

so prove by considering a number p that is not prime and whose square root is an integer.