CSC110 Lecture 15: Proofs

Hisbaan Noorani

October 19, 2020

Contents

1 Ex 1: Practice with proofs

1. Prove the following statement, using the definition of divisibility.

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

We can rewrite this as: $\forall n, d, a \in \mathbb{Z}, (\exists k_1 \in \mathbb{Z}, n = dk_1) \implies (\exists k_2 \in \mathbb{Z}, an = dk_2)$

Let $n, d, a \in \mathbb{Z}$

Take $k_1 = \frac{n}{d}$

Take $k_2 = ak_1$

Assume $d \mid n$

Prove $d \mid an$:

$an = dk_2$

$an = dak_1$

$n = dk_1$

$n = dk_1 \iff an = dk_2$

Therefore we have proven $\forall n, d, a \in \mathbb{Z},\ d \mid n \Rightarrow d \mid an$, as needed.

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

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

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

Let $n = 3$
Let $d = 12$
Let $a = 4$

Here we can see that $d \mid an$ is true by inputting the values of $d, a,$ and n:
$12|(3 \cdot 4)$
$12 \mid 12$
which we know is true since $\forall n \in \mathbb{R}, n \mid n$.

We now need to show that $d \nmid a$
We can show this by simply doing the division:
$= \frac{a}{d}$
$= \frac{4}{12}$
$= \frac{1}{3}$
$\notin \mathbb{Z}$. Thus $d \nmid a$ as needed

We now need to show that $d \nmid n$
$= \frac{n}{d}$
$= \frac{3}{12}$
$= \frac{1}{4}$
$\notin \mathbb{Z}$. Thus $d \nmid n$ as needed

And therefore, we have proven $\exists n, d, a \in \mathbb{Z},\ d \mid an \wedge d \nmid a \wedge d \nmid n$, as needed which implies that the original statement, $\forall n, d, a \in \mathbb{Z},\ d \mid an \Rightarrow d \mid a \vee d \mid n$, is true. ■

2 Ex 2: Primality testing

In lecture, we saw an algorithm for checking whether a number p prime that checks all of the possible factors of p between 2 and $\lfloor \sqrt{p} \rfloor$, inclusive.

We can prove that this algorithm is correct by proving the follow statement:

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

This is a larger statement than the ones we've looked at so far, so this exercise we've broken down the proof of this statement for you complete.

Proof.

Let $p \in \mathbb{Z}$. We need to prove an if and only if, which we do dividing the proof into two parts.

2.1 Part 1: Proving that $Prime(p) \Rightarrow \big(p > 1(\forall d \in,\ 2 \leq d \leq \sqrt{p} \Rightarrow d \nmid\big)$.

1. Write down what we can **assume** in this part of the proof.

   $Prime(p) : p > 1 \wedge (\forall d \in \mathbb{N},\ d \mid p \implies d = 1 \vee d = p)$, where $p \in \mathbb{Z}$

   We assume this entire predicate.

2. To prove an AND, we need to prove that both parts are true. First, prove that $p > 1$.

   $p > 1$, as we have assumed such (as seen above)

3. Now, prove that $\forall d \in,\ 2 \leq d \leq \sqrt{p} \Rightarrow d \nmid p$.

   Assume $d \in (2, \sqrt{p})$

   This implies that $2 \leq d$ which implies $d > 1$ therfore $d \neq 1$.

   Since $p > 1$, $\sqrt{p} < p$. This implies that $d < \sqrt{p} < p$ therefore $d \neq p$

   We know that since p is prime d must be either 1 or p to divide p. Since $d \neq 1$ and $d \neq p$ we have proven $d \nmid p$ ■

2.2 Part 2: Proving that $p > 1 \wedge (\forall d \in,\ 2 \leq d \leq \sqrt{p} \Rightarrow d \nmid p) \Rightarrow Prime(p)$.

1. Write down what we can **assume** in this part of the proof.

   - $p > 1$
   - $\forall d \in \mathbb{N}, 2 \leq d \leq p \implies d \nmid p$

2. We need to prove that $Prime(p)$, which expands into $p > 1 \wedge (\forall d \in,\ d \mid p \Rightarrow d = 1 \vee d = p)$.

   First, prove that $p > 1$.

   We have proven $p > 1$ by assumption.

3. Now for the proof of $\forall d \in \mathbb{N},\ d \mid p \Rightarrow d = 1 \vee d = p$. Start by writing the appropriate proof header, introducing the variable d and assumption about d.

   Assume

   $\forall d_1 \in \mathbb{N}, d_1 \mid p$

   OR

   $\forall d_1 \in \mathbb{N}, \exists k \in \mathbb{Z}, p = kd_1$

4. Use the **contrapositive** of a part of your original assumption. What can you conclude about d?

   $\forall d_1 \in \mathbb{N} d_1 \mid p \implies d_1 < 2 \vee d_1 > \sqrt{p}$

   From this contrapositive, we can conlude that $d_1 < 2$ or $d_1 < \sqrt{p}$

5. Using the cases from the previous part, prove that $d = 1 \vee d = p$.

   Case 1: $d_1 < 2$.

   $d_1 \in \mathbb{N} \wedge d_1 < 2$, then $d_1 = 0$ or $d_1 = 1$
   But $0 \nmid p$, because $p > 1$, $d \neq 0$
   Therefore $d_1 = 1$

   Case 2: $d_1 < \sqrt{p}$

   $p = d_1 k$
   $k < \sqrt{p}$, but k also divides p which means that $k < 2$ therefore $k = 1$
   $d_1 = p$

   Therefore in both cases, either $d_1 = p$ or $d_1 = 1$ ■

3 Additional Exercises

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

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

2. *Disprove* the following statement, which is very similar to the one you proved in Exercise 2.

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