More Proofs

CSC165 Week 4 - Part 2

Lindsey Shorser, Winter 2021

Last time, we proved:

- $\forall\, x \in \mathbb{Z},\ \exists\, y \in \mathbb{Z},\ x \neq y+1$
- $\forall\, d \in \mathbb{N},\ \forall\, x \in \mathbb{N},\ x \mid (x+d) \Rightarrow x \mid d$ (Fact 1)
- $\forall\, x, \in \mathbb{N},\ \forall\, p \in \mathbb{N},\ \text{Prime}(p) \wedge x \mid (x+p) \Rightarrow x=1 \vee x=p$

Notice that the "$\mathbb{Z}$"s were replaced by "$\mathbb{N}$"
to make the last statement true and provable.

All Dogs are Animals

$\land \quad \lor \quad \neg \quad \Rightarrow \quad \Leftrightarrow \quad \exists \quad \forall$

$\forall x \in U, D(x) \Rightarrow A(x)$ ✓ ←

Let U = { living things }

Let D(x) = " x is a dog"

Let A(x) = "x is an animal"

~~$\forall x \in U, \; D(x) \land A(x)$~~ ←

not always true

$D(x) \Rightarrow A(x)$ ✓

$A(x) \Rightarrow D(x)$ ✗

Example: $\forall\ a,b \in \mathbb{Z},\ \underline{2 \nmid a} \wedge \underline{2 \nmid b} \implies \underline{2 \nmid ab}$

Rough Work:

$$\underbrace{(2n+1)}_{=\,a}\underbrace{(2k+1)}_{=\,b} = 4nk + 2n + 2k + 1$$

Generalization? $\forall\, d \in \cancel{\mathbb{Z}}\,\mathbb{N}, \forall\, a,b \in \mathbb{Z},\ d \nmid a \wedge d \nmid b \implies d \nmid ab$

Rough Work

$d = 6$, $a = 4$, $b = 3$

$ab = 12$

$d \mid ab$

Proof: WTS $\exists d \in \mathbb{Z}, a,b \in \mathbb{Z}, (d \nmid a \wedge d \nmid b) \wedge d \mid ab$

Let $d = 6$, $a = 4$, and $b = 3$.

$6 \nmid 4$ and $6 \nmid 3$ (because 6 is bigger)

$ab = 3x4 = 12 = 2(6)$.

$\implies \exists k \in \mathbb{Z}$, $ab = kd$ where $ab = 12$ and $k = 2$ and $d = 6$.

QED.

Example: $\forall\, d \in \cancel{\mathbb{Z}}\ \mathbb{N}\ \boxed{(\forall\, a,b \in \mathbb{Z},\ d \nmid a \wedge d \nmid b \implies d \nmid ab)}$

$$\Rightarrow \boxed{\mathrm{Prime}(d) \vee d \leq 1}$$

$A \Rightarrow B$

A direct proof would start with "Assume A is true"

Instead we can do an indirect proof, by directly proving the contrapositive:

$\neg B \Rightarrow \neg A$

$B \Rightarrow A$ is the converse

Example: $\boxed{\forall d} \in \mathbb{N} \left((\forall a,b \in \mathbb{Z},\ d \nmid a \wedge d \nmid b \implies d \nmid ab) \implies \neg (\text{Prime}(d) \vee d \leq 1) \right)$

Rough Work

Recall: Prime(p) = "p>1 ∧ ∀d∈ℕ, d|p ⟹ d=1 ∨ d=p"

When we start the proof, we will assume ¬(Prime(d) ∨ d ≤ 1)

This is equivalent to ¬Prime(d) AND ALSO d > 1.

¬Prime(d) ∧ d > 1 $\quad \forall d \in \mathbb{Z}$

We can assume that d is not prime and also > 1.

Want to show: $\forall d \in \mathbb{Z}, \left[\exists a,b \in \mathbb{Z}, (d \nmid a \wedge d \nmid b) \wedge d \mid ab \right]$

$$\mathrm{Prime}(p) \iff \boxed{\underline{p > 1} \wedge \left(\forall_{q \in \mathbb{N}},\ q \mid p \Rightarrow q = 1 \vee q = p\right)}$$

$$\underline{\neg \mathrm{Prime}(d)} \wedge d > 1$$

$$\Longrightarrow \underline{\exists q \in \mathbb{N}},\ \underline{q \mid d} \wedge \underline{(q \neq 1 \wedge q \neq d)}$$

We can take q and use it the same way we used 2x3 in our counterexample.

$$(q \nmid a \wedge q \nmid b) \wedge (q \mid ab) \quad \ldots$$

$$\forall d \in \mathbb{N} \left(\text{Prime}(d) \vee d \leq 1 \right) \Rightarrow \left(\forall a, b \in \mathbb{Z} \right.$$

$$\left. d \nmid a \wedge d \nmid b \Rightarrow d \nmid ab \right)$$

A direct proof of this would have cases because you start by assuming a disjunction (OR statement).

Case 1: d is prime.

Case 2: $d \leq 1$ $\rightarrow d = 0$

$\rightarrow d = 1$

Note: We are now trying to prove the Converse.

To prove the converse, you can use:

If $d \nmid a$ then you can say $\exists r,s \in \mathbb{Z}$, $rd + sa = 1$

$\gcd(d,a)$

How to prove a biconditional (iff) statement:

Step 1: Show this

Step 2: Show the converse

If $(A \Rightarrow B) \wedge (B \Rightarrow A)$ then

Step 3: Conclude the biconditional: $A \Leftrightarrow B$