More Proofs

CSC165 Week 4 - Part 1

Lindsey Shorser, Winter 2021

Example: $\exists x \in \mathbb{Z}, \forall y \in \mathbb{Z}, x \neq y+1$

False

3?

$3 = 2+1$

$\neg(\exists x \in \mathbb{Z}, \forall y \in \mathbb{Z}, x = y+1)$

We want to show that $\forall\ x \in \mathbb{Z},\ \exists\ y \in \mathbb{Z},\ x \neq y+1$

Let $x \in \mathbb{Z}$, let $y = x$

$$x = y$$

$$\neq y+1$$

Therefore, for every x we choose, we can find a y that makes x not equal y+1.

Q.E.D.

Example: $\forall d \in \mathbb{Z}, \forall x \in \mathbb{Z}, x \mid (x+d) \Rightarrow x \mid d.$

$x \mid x+5 \Rightarrow x \mid 5$

Rough Work:

Let $d \in \mathbb{Z}$, $x \in \mathbb{Z}$

Assume $x \mid (x+d)$

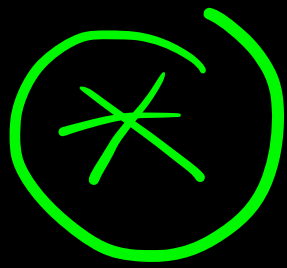
A	B	A ⇒ B
T	T	T
T	F	F
		T
		T

$A \Leftrightarrow B$

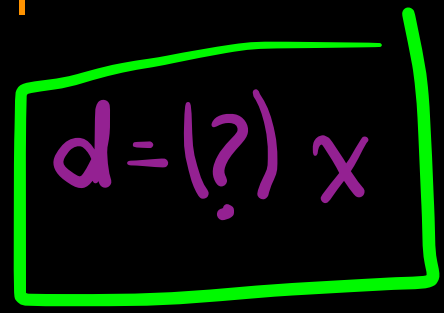
$(A \Rightarrow B) \wedge (B \Rightarrow A)$

$a \mid b \Rightarrow \exists k \in \mathbb{Z},\ b = ka$

Proof: We want to show that



$$\forall\, d \in \mathbb{Z},\ \forall\, x \in \mathbb{Z},\ x \mid (x+d) \Rightarrow x \mid d$$



Let $x \in \mathbb{Z}$. The value of $d \in \mathbb{Z}$ is fixed.
Assume $x \mid (x+d)$.

$\Rightarrow \exists m \in \mathbb{Z}$, $(x+d) = (m)x$ (by definition of "|")

$d = mx - x$ (by arithmetic)

$d = (m-1)x$ (by arithmetic)

Let $k = m-1$. $k \in \mathbb{Z}$

Therefore, there exists $k \in \mathbb{Z}$ such that $d = kx$ and therefore x divides d for any d in the integers. Q.E.D.

Since it has now been prove, we will let Fact 1 be:

$$\forall\, d \in \mathbb{Z}, \forall\, x \in \mathbb{Z},\ x \mid (x+d) \Rightarrow x \mid d.$$

$d = p$

$A \Rightarrow B$

Example:

$$\forall x \in \mathbb{Z}, \forall p \in \mathbb{Z}, \left(\text{Prime}(p) \wedge x \mid (x+p)\right) \Rightarrow (x=1 \vee x=p)$$

$$\text{Prime}(p) = \text{“}p>1 \wedge \left(\forall d \in \mathbb{N}, d \mid p \Longrightarrow d=1 \vee d=p\right)$$

Want to show:

$$\forall\, x, \in \mathbb{Z},\ \forall\, p \in \mathbb{Z},\ \Big(\text{Prime}(p) \wedge x \mid (x+p)\Big) \Rightarrow x=1 \vee x=p$$

Let $x \in \mathbb{Z}$, and let $p \in \mathbb{Z}$.

Assume, Prime(p) is true.
Also assume $x \mid x+p$.

Fact 1 $\Longrightarrow x \mid p$

$\Longrightarrow x = 1 \vee x = p$ (by definition of prime).

Q.E.D.

Want to show:

$\forall x, \in \mathbb{Z}, \forall p \in \mathbb{Z}, \ \text{Prime}(p) \wedge x \mid (x+p) \Rightarrow x=1 \vee x=p$

Let $x \in \mathbb{Z}$, and let $p \in \mathbb{Z}$.

Assume, Prime(p) is true.
Also assume x | x+p.

Prime(p) = "$p>1 \wedge \forall d \in \mathbb{N}, d \mid p \Longrightarrow d=1 \vee d=p$"

$d = x$

Want to show:

$\forall x, \in \mathbb{Z}, \forall p \in \mathbb{Z}, \ \text{Prime}(p) \wedge x \mid (x+p) \Rightarrow x=1 \vee x=p$

Let $x \in \mathbb{Z}$, and let $p \in \mathbb{Z}$.

Assume, Prime(p) is true.
Also assume $x \mid x+p$. ←

→ Prime(p) = "$p>1 \wedge \forall r \in \mathbb{N}, r \mid p \Rightarrow r=1 \vee r=p$"

(Here r can be any natural number including x, if it is positive)

Fact 1 $\Rightarrow$ $x \mid p$

In the definition of Prime(p), any value of r, including r = p, implies $r = 1$ or $r = p$.

If x is a natural number, Fact 1 implies the hypothesis in the second part of the definition of "prime". Otherwise, x could be -1, -p, too.

Want to show:

$\forall x, \in \mathbb{Z}, \forall p \in \mathbb{Z}, \ \text{Prime}(p) \wedge x \mid (x+p) \Rightarrow x=1 \vee x=p$

Assume, Prime(p) is true.
Also assume x | x+p.

Prime(p) = “$p>1 \wedge \forall d \in \mathbb{N}, d|p \implies d=1 \vee d=p$”

Fact 1 $\implies x|p$

$\exists k \in \mathbb{Z}, p = kx$

Want to show:

$\forall x, \in \mathbb{Z}, \forall p \in \mathbb{Z}, \ \text{Prime}(p) \wedge x \mid (x+p) \Rightarrow x=1 \vee x=p$

Assume, Prime(p) is true.
Also assume x | x+p.

Prime(p) = "$p>1 \wedge \forall d \in \mathbb{N}, d|p \implies d=1 \vee d=p$"

Fact 1 $\implies x|p$

If you know $x \in \mathbb{N}$, then we can let d = x (since d can be any natural number)

$\exists k \in \mathbb{Z}$, p = kx, but p is prime, if x|p then x = 1 or x = p

$A \Rightarrow B$

$B \Rightarrow C$

$\therefore A \Rightarrow C$

deduction

$A \Rightarrow B$

Assume A (so we are in one of the first two rows of the truth table).

Prove that B has to be true so that we cannot be in the second row of the truth table.

This is a direct proof.

$A \Rightarrow B$

$\neg B \Rightarrow \neg A$

If you assume B is false and use that to get that A is also false, then we call that strategy "Proof by Contrapositive"

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

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

$\exists\, d \in \mathbb{Z},\ \exists\, a \in \mathbb{Z},\ \exists\, b \in \mathbb{Z}$

T F

$d = 6$

Proof: We want to show that
$\exists\, d \in \mathbb{Z},\ \exists\, a \in \mathbb{Z},\ \exists\, b \in \mathbb{Z}$, such that
$(d \nmid a) \wedge (d \nmid b) \wedge (d \mid ab)$

$d \mid ab$

Let $a = 8$

Let $b = 9$

$(6 \nmid 8 \wedge 6 \nmid 9) \wedge (6 \mid 72)$

$\neg(A \implies B) \iff A \wedge (\neg B)$

$A \implies B$

Example: $\forall\ d \in \mathbb{Z}\ (\forall\ a,b \in \mathbb{Z},\ d \nmid a \wedge d \nmid b \Longrightarrow d \nmid ab)$

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