

Quantifiers

\forall universal (for all / for every)

\exists existential (there exists some)

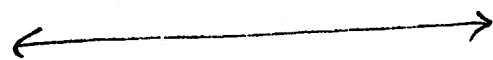
Ex For every integer $n > 1$, $2^n - 1$ is prime

$\hookrightarrow \forall n \in \mathbb{Z}, n > 1 : 2^n - 1$ is prime

Ex For some integer $n > 1$, $2^n - 1$ is prime

$\hookrightarrow \exists n \in \mathbb{Z}, n > 1 : 2^n - 1$ is prime

[existential are harder to prove]



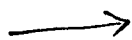
o Sometimes you can swap order of quantifiers and statement remains if the combination of quantifiers includes only one of them.

$\rightarrow \forall m \in \mathbb{Z}, \forall n \in \mathbb{Z} : (m+n)(m+n-1) \geq 0$

$\forall (m,n) : \mathbb{Z} \times \mathbb{Z} \rightarrow$ swappable

o if it was two \exists 's it would be swappable too

When you have a mixture of quantifiers order matters



Ex $\forall n \in \mathbb{Z} \exists m \in \mathbb{Z} : m = n+5$ [T]

$\exists m \in \mathbb{Z} \forall n \in \mathbb{Z} : m = n+5$ [F]

continually \rightarrow

Ex $\forall \epsilon > 0 \exists \delta > 0 : |x-a| < \delta \Rightarrow |f(x) - f(a)| < \epsilon$ [T]

vs $\forall \delta > 0 \exists \epsilon > 0 : |x-a| < \delta \rightarrow |f(x) - f(a)| < \epsilon$ [F]

vs $\exists \delta > 0 \forall \epsilon > 0 : |x-a| < \delta \rightarrow |f(x) - f(a)| < \epsilon$ [F]



Duality under Negation

" $\neg \forall \sim \exists \neg \dots$ "

" $\neg \exists \sim \forall \neg \dots$ "

so $\neg (\forall x : P(x)) \rightarrow \exists x : \neg P(x)$

$\neg (\exists x : P(x)) \rightarrow \forall x : \neg P(x)$

Ex $\neg (\forall n \in \mathbb{Z} \setminus \{0\}, n^2 \geq 1)$

$\hookrightarrow \exists n \in \mathbb{Z} \setminus \{0\} : n^2 < 1$

Ex $\neg (\forall p \in \mathbb{N} \text{ prime } \exists q \in \mathbb{N} \text{ prime} : q > p)$

$\Rightarrow \exists p \in \mathbb{N} \text{ prime } \forall q \in \mathbb{N} \text{ prime} : q \leq p$

Ex Note $\neg(p \Rightarrow Q) = P \wedge \neg Q$

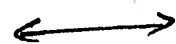
So $\neg(\forall \epsilon > 0 \exists \delta > 0 : |x-a| < \delta \rightarrow |f(x) - f(a)| < \epsilon)$
 $= \exists \epsilon > 0 \forall \delta > 0 : \neg(|x-a| < \delta \rightarrow |f(x) - f(a)| < \epsilon)$

use Note $\exists \epsilon > 0 \forall \delta > 0 : |x-a| < \delta \wedge |f(x) - f(a)| \geq \epsilon$



Number Theory

- 1) Divisibility
- 2) LCM & GCD
- 3) Euclid Algorithm
- 4) primes
- 5) congruence



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

a divides b (or a is a divisor of b , or b is a multiple of a)



if there exists $m \in \mathbb{Z} : b = ma$

These statements can be written as

Notation $\rightarrow a \nmid b$ (and $a \nmid b$ if a does not divide b)



40

Examples $1 \mid b$ for all $b \in \mathbb{Z}$

$0 \mid b$ for $b=0$ only

$b \mid 0$ for all $b \in \mathbb{Z}$

$\begin{cases} 2 \mid b & b \text{ is even} \\ 2 \nmid b & b \text{ is odd} \end{cases}$

Further ex ~~$b \mid (b+1)^n - 1$~~ for all $n \geq 1, b \in \mathbb{Z}$

$$\text{so } (b+1)^n = \sum_{k=0}^n \binom{n}{k} b^k$$

$$\xrightarrow{k=0} 1 + \sum_{k=1}^n \binom{n}{k} b^k = b \left[\sum_{k=1}^n \binom{n}{k} b^{k-1} \right]$$

being
b out

⋮

41

Prop 1) $a|a$

2) $a|b, b|c \rightarrow a|c$

3) $a|b, b|a \rightarrow a = \pm b$

Note if a, b positive integers then
 $a|b, b|a \rightarrow a=b$, so
 Divisibility is an ordered relation

$$\begin{aligned} & \begin{cases} b = ma \\ c = m'b \\ c = m'(ma) \\ c = (m'm)a \end{cases} \\ & \begin{cases} b = ma \\ a = m'b \\ a = (mm')b \\ mm' = 1 \text{ if } a \neq 0 \\ \text{so } m = \pm 1 \\ b = \pm a \\ \text{if } a=0 \text{ or } b=0 \\ \text{so } b = \pm a \text{ as well} \end{cases} \end{aligned}$$

Prop 1) $a|b, a|c \rightarrow a|b \pm c$
 2) $a|b \Rightarrow a|bc$

Proof i) $a|b$ means $b=ma$ (Some $m \in \mathbb{Z}$)
 $a|c$ means $c=m'a$ (Some $m' \in \mathbb{Z}$)

ii) $a|b$ means $b=ma$

$$b|c = m(ma)|c = \underbrace{(mc)}_{\in \mathbb{Z}} a$$

Def $p \in \mathbb{N}, p \geq 2$ is prime if the only positive integers dividing p are 1 and p

Remark if we list out all prime numbers, 2 ends up being the only even Number

Thm. Every Positive integer ≥ 2 has a prime divisor.

[what made you choose?
Strong induction?]

Proof by :- for $n \geq 2$ integers
INDUCTION
 [STRONG] $P(n)$: there exists a prime p dividing n

Base Case: $P(2)$ is true for $2|2$

Induction Step: if n is prime, take $p=n$
 else there exists some integer $k, k|n$
 and $k \neq 1, n$

$$\text{so if } k|n \rightarrow k \in \{1, 2, \dots, n\} \rightarrow k \in \{2, \dots, n-1\}$$

By Strong induction hyp, $P(k)$ holds true, so there is some prime p with $p|k$.

AS $k|n$, it follows that $p|n$.