9- October - 2018

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]

$\longleftrightarrow$

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

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

$\forall (m,n) : \mathbb{Z} \times \mathbb{Z} \longrightarrow$ swapable

- If it was two $\exists$'s it would be swappable too

When you have a mixture of quantifiers order matters

$\longrightarrow$

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]

Continuity $\longrightarrow$

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

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

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

$\longleftrightarrow$

Duality under Negation

"$\neg \forall \rightsquigarrow \exists \neg \dots$"

"$\neg \exists \rightsquigarrow \forall \neg \dots$"

so $\neg(\forall x : P(x)) \longrightarrow \exists x : \overline{P(x)}$

$\neg(\exists x : P(x)) \longrightarrow \forall x : \overline{P(x)}$

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

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

Ex

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

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

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

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

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

Use Note $\exists\ \varepsilon > 0\ \forall \delta > 0 : |x-a| < \delta\ , |f(x) - f(a)| \geq \varepsilon$

$\longleftrightarrow$

Number Theory

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

$\longleftrightarrow$

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

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 $\longrightarrow$ $a|b$ (and $a \nmid b$ if a does not divide b)

$\Longrightarrow$

Examples $1|b$ for all $b \in \mathbb{Z}$
$0|b$ for $b = 0$ only
$b|0$ for all $b \in \mathbb{Z}$

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

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

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

$\hookrightarrow \underbrace{1}_{k=0} + \underbrace{\sum_{k=1}^{n} \binom{n}{k} b^k}_{\text{Bring } b \text{ out}}$ $\quad b\left[\sum_{k=1}^{n} \binom{n}{k} b^{k-1}\right]$

$\vdots$

Prop 1) $a|a$

2) $a|b$, $b|c \longrightarrow a|c \longrightarrow$ $b = ma$, $c = m'b$, $c = m'(ma)$, $c = (m'm)a$

3) $a|b$, $b|a \longrightarrow a = \pm b \longrightarrow$ $b = ma$, $a = m'b$, $a = (mm')a$

$mm' = 1$ if $a \neq 0$

so $m = \pm 1$, $b = \pm a$

if $a = 0$ or $b = 0$ so $b = \pm a$ as well

Note If a, b positive integers then $a|b$, $b|a \longrightarrow a = b$, so

Divisibility is an ordered relation

Prop 1) $a|b$, $a|c \longrightarrow a|b \pm c$

2) $a|b \Rightarrow \longrightarrow a|bc$

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 $b = ma$

$$bc = \cancel{ma}\,(ma)c = \underbrace{(mc)}_{\in \mathbb{Z}}a$$

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 INDUCTION [STRONG] :- for $n \geq 2$ integers

$P(n)$: 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 $k \neq 1, n$

so if $k|n \rightarrow k \in \left\{\begin{matrix} 1, 2 \cdots\cdots n \\ k \neq 1, n \end{matrix}\right\} \longrightarrow k \in \{2 \cdots\cdots n-1\}$

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

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