Math 4460
1/22/25

Assumptions

We will assume the set of integers exists.

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

We will assume all the basic algebraic properties of $\mathbb{Z}$ like:

(closure) If $a, b \in \mathbb{Z}$, then $a+b \in \mathbb{Z}$ and $a \cdot b \in \mathbb{Z}$

other kinds of properties

$$a \cdot (b+c) = ab + ac$$

$$a \cdot 1 = a$$

$$a + 0 = a$$

If $a < b$ and $c > 0$, then $ca < cb$

EXAMPLES

Topic 1 — Division and primes

__Def:__ Let x and y be integers with $x \neq 0$. We say that x __divides__ y if there exists an integer k with $y = xk$.

If x divides y then we call x a __divisor__ of y and write $\underbrace{x \mid y}_{\text{read: "x divides y"}}$.

If x doesn't divide y then we write $x \nmid y$.

Ex:

$$\boxed{\begin{array}{l}\text{Divisors of } 12: \\ 1, 2, 3, 4, 6, 12 \\ -1, -2, -3, -4, -6, -12\end{array}}$$

$12 \mid 12$ because $\underbrace{12}_{y} = \underbrace{(12)}_{x}\underbrace{(1)}_{k}$

$-4 \mid 12$ because $\underbrace{12}_{y} = \underbrace{(-4)}_{x}\underbrace{(-3)}_{k}$

$100 \nmid 12$ because if $12 = 100k$ you'd need $k = \frac{12}{100} \notin \mathbb{Z}$.

Def: Let $p \in \mathbb{Z}$ with $p > 1$. We say that p is <u>prime</u> if the only positive divisors of p are 1 and p.
If p is not prime, then we call p a <u>composite</u> number

Ex: Let's circle the primes.

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, ...

Theorem: Let x and y be positive integers. If $x \mid y$, then $1 \leq x \leq y$.

proof:

Suppose x and y are positive integers with $x \mid y$.

Since x and y are positive integer we get $1 \leq x$ and $1 \leq y$.

Since $x \mid y$ there exists an integer k with $xk = y$.

Then $k = \frac{y}{x}$ is positive.

(Using dividing two positive #'s is positive)

So, $1 \leq k$.

Multiply by x and since x is positive we get that $x \leq \underbrace{xk}_{y}$.

So, $x \leq y$.

Thus, $1 \leq x \leq y$.

<u>Theorem:</u> Let p and q be prime numbers. If $p \mid q$, then $p = q$.

Proof:

Suppose p and q are primes with $p \mid q$.

Since p is prime we have $p > 1$.

Since q is prime, the only positive divisors are 1 and q.

Thus since p is a positive divisor of q we know either $p = 1$ or $p = q$.

Since $p > 1$ we must have $p = q$.