<u>Warm-Up</u>: Let $d, n, m \in \mathbb{Z}$. Prove that if $d \mid n$ and $d \mid m$, then $d \mid (n+m)$.

<u>Thm</u>: For any $a, b, c \in \mathbb{N}$,

1. $a \mid a$. [Reflexivity]
2. If $a \mid b$ and $b \mid a$, then $a = b$. [Antisymmetry]
3. If $a \mid b$ and $b \mid c$, then $a \mid c$. [Transitivity]

<u>Proof</u>: HW 10.

This theorem says divisibility is a <u>partial order</u> on $\mathbb{N}$.

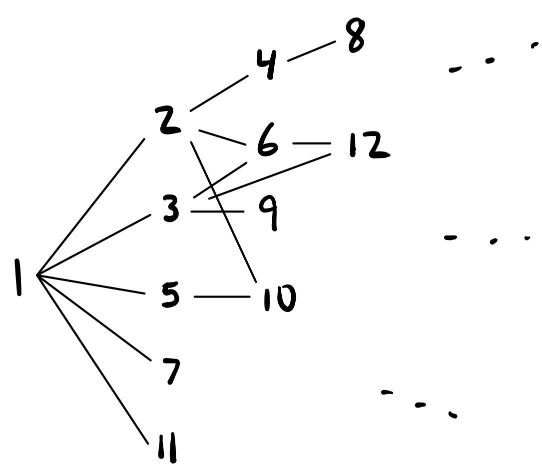
Another partial order is $\leq$.

$\mathbb{N}$ ordered by $\le$

$$1 \le 2 \le 3 \le 4 \le \cdots$$

Boring. This is a <u>total order</u> - it arranges $\mathbb{N}$ along a line.

$\mathbb{N}$ ordered by divisibility



This looks much more interesting...

Primes

Def: An integer p is a prime number if

① $p > 1$

and

② For any $a, b \in \mathbb{N}$, if $p = ab$ then $a = 1$ or $b = 1$

Ex: 2, 3, 5, 7, 11 are prime

Warning: You sometimes hear that p is prime if its only divisors are 1 and p. This isn't quite right.

- 1 and p are the only positive divisors of a prime p
- We also need $p \in \mathbb{N}$ and $p \neq 1$ for p to be prime.

Non-Ex: 21 is not prime, because $21 = 3 \cdot 7$. If we set $a = 3$ and $b = 7$, then $21 = ab$ but $a \neq 1$ and $b \neq 1$.

Def: An integer n is <u>composite</u> if

① $n > 1$

and

② n is not prime

By Generalized de Morgan, ② means there exist $a, b \in \mathbb{N}$ such that $n = ab$ and $a \neq 1$ and $b \neq 1$.

Thm: If p is prime, then its only positive divisors are 1 and p.

Proof: Suppose p is prime and let d be a positive divisor of p.

By definition of divisibility, there exists $k \in \mathbb{Z}$ such that $p = dk$. Since p and d are positive, so is k. Thus, $d, k \in \mathbb{N}$ with $p = dk$, so $d = 1$ or $k = 1$.

If $d = 1$, we're done.
If $k = 1$, then $p = dk = d \cdot 1 = d$.

Thus, $d = 1$ or $d = p$. ∎

In fact, the converse is true.

Thm: Let n be an integer with $n > 1$.
If the only divisors of n are 1 and n, then n is prime.

Proof: Suppose $n > 1$ is an integer, and the only positive divisors of n are 1 and n.

We must show, for all $a, b \in \mathbb{N}$, if $n = ab$ then $a = 1$ or $b = 1$.

So suppose $n = ab$ for some $a, b \in \mathbb{N}$.
Then, by definition of divisibility, $a \mid n$.
Thus, $a = 1$ or $a = n$.

If $a = 1$, then we're done.
If $a = n$, then $n = n \cdot b$. So $n \cdot 1 = n \cdot b$.
By cancellation, $1 = b$.

Thus, $a = 1$ or $b = 1$. ∎

Together, the last two theorems prove

p is prime $\iff$ $p > 1$ and the only positive divisors of p are 1 and p.

Equivalently,

n is composite $\iff$ $n > 1$ and n has a positive divisor d with $d \neq 1$ and $d \neq n$.

<u>Note</u>: We can think of these biconditional ($\iff$) sentences as alternate (but equivalent) definitions.