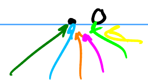
$a \to b$ means $a \le b$.

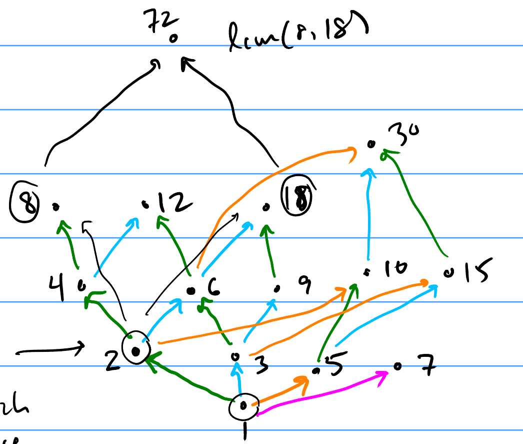
$0 \to 1 \to 2 \to 3 \to 4 \to \cdots$

↑ usual number line, $\mathbb{N}$ ordered by $\le$. Boring.

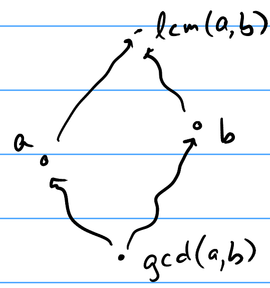
$\mathbb{N}$ where we only care about addition.

What picture do we get if we draw $\mid$ relationships between numbers instead of $\le$?



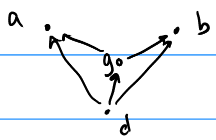


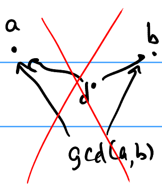
gcd(8, 18) = 2
highest pt from which we can reach both.



__Def'n__ Let $a, b \in \mathbb{N}$. The greatest common divisor of a and b, written $\gcd(a,b)$, is the unique natural number such that for all $d \in \mathbb{N}$,

$$(d \mid \gcd(a,b)) \leftrightarrow (d \mid a \wedge d \mid b).$$





Ex. gcd(6, 10) = 2
gcd(2, 3) = 1
gcd(2, 4) = 2
gcd(3, 3) = 3
gcd(0, 7) = 7
gcd(0, 0) = 0

We can compute GCD by factoring & looking for common primes.

e.g. $\gcd(18, 60) = \gcd(2\cdot 3^2, 2^2\cdot 3\cdot 5) = 2\cdot 3 = 6.$

But there is a better way! Euclidean Algorithm.

Lemma. $\gcd(a,b) = \gcd(b,a)$.
Proof: stare at definition.

Thm. For all $k \in \mathbb{Z}$, $\gcd(a,b) = \gcd(a+kb, b)$.
Proof: see lecture notes.

Thm. $\gcd(a,b) = \gcd(b, a \bmod b)$.
Proof: By the division algorithm, $a = bq + r$ for some q, r.

$$
\begin{aligned}
& \gcd(a,b) \\
= \; & \qquad\qquad \{\text{div alg}\}. \\
& \gcd(bq+r, b) \\
= \; & \qquad\qquad \{\text{by above theorem}\} \\
& \gcd(bq+r-bq, b) \\
= \; & \qquad\qquad \{\text{algebra}\} \\
& \gcd(r, b) \\
= \; & \qquad\qquad \{\gcd \text{ is commutative}\} \\
& \gcd(b, r) \\
= \; & \qquad\qquad \{r = a \bmod b\}. \\
& \gcd(b, a \bmod b).
\end{aligned}
$$

Notice $a \bmod b < b$, so if we do this repeatedly, the 2nd argument to gcd gets smaller every time.
Hence:

<u>Euclidean Algorithm</u>

$$\gcd(a, 0) = a$$
$$\gcd(a, b) = \gcd(b, a \bmod b).$$

$$\begin{aligned}
&\gcd(18, 60) \\
&= \gcd(60, 18 \bmod 60) \\
&= \gcd(60, 18) \\
&= \gcd(18, 60 \bmod 18) = \gcd(18, 6) \\
&= \gcd(6, 18 \bmod 6) = \gcd(6, 0) = 6.
\end{aligned}$$