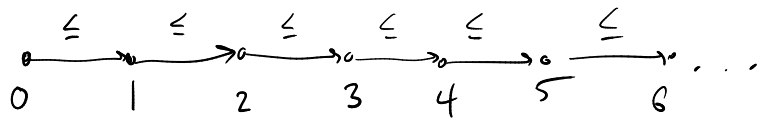
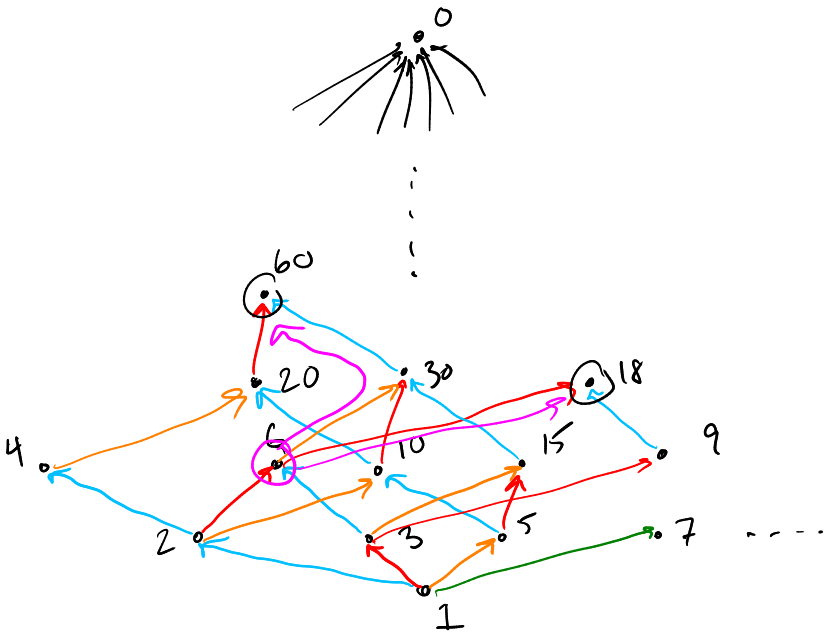


Let's draw a similar picture, but for $a \mid b$ instead of $a \leq b$.

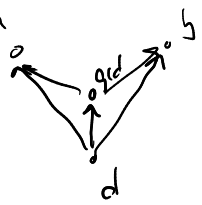


Defn For all $a, b \in \mathbb{N}$, the greatest common divisor of a and b, written $\gcd(a,b)$, is the unique natural number such that for all $d \in \mathbb{N}$,

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

Note:

1. If we pick $d = \gcd(a,b)$, the $\rightarrow$ direction tells us $\gcd(a,b) \mid a$ and $\gcd(a,b) \mid b$.
2. $\gcd(a,b)$ is the "greatest" common divisor since it must be "above" any common divisor of a, b.



Example:

$\gcd(6,18) = 2$

$\gcd(2,3) = 1$

$\gcd(2,4) = 2$

$\gcd(3,3) = 3$

$\gcd(0,7) = 7$

$\gcd(0,0) = 0$

Computing the GCD?

— Prime factorization of each, choose common factors.

e.g. $18 = 2 \cdot 3 \cdot 3$

$60 = 2 \cdot 3 \cdot 2 \cdot 5$ $\longrightarrow$ $\gcd(18,60) = 6$.

Formally: write a number as

$$a = 2^{a_2} \cdot 3^{a_3} \cdot 5^{a_5} \cdot 7^{a_7} \cdot \dots$$

infinite product of prime powers, where all but some finite # of powers are 0.

Then $\gcd(2^{a_2}3^{a_3}5^{a_5}7^{a_7}\dots, 2^{b_2}3^{b_3}5^{b_5}7^{b_7}\dots)$

$$= 2^{\min(a_2,b_2)}\, 3^{\min(a_3,b_3)} \dots$$

$\gcd(7169, 7811)$?

↳ Difficult to factor!

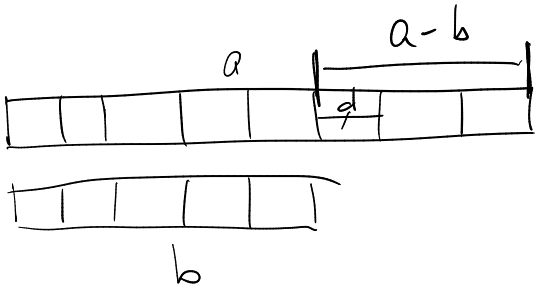
lcm uses max instead of min

Exercise: show why

$\gcd(a,b) \cdot \operatorname{lcm}(a,b) = ab$

Is there a better way? Yes!

Claim: If $a \geq b$, then $\gcd(a,b) = \gcd(a-b, b)$.



$d = \gcd(a,b)$

If a + b can be chopped evenly into pieces of common size, then so can $a-b$ and b, and vice versa.

Claim: $\gcd(a,b) = \gcd(b,a)$.

Hence here is a procedure for calculating gcd (Euclidean Algorithm, baby version)

Repeat these steps:

- $\gcd(a, 0) = a$
- if $a \geq b$, $\gcd(a,b) = \gcd(a-b, b)$
- otherwise, $\gcd(a,b) = \gcd(b,a)$

Example.

$\gcd(60, 18)$
$= \gcd(42, 18)$
$= \gcd(24, 18)$
$= \gcd(6, 18)$
$= \gcd(18, 6)$
$= \gcd(12, 6)$
$= \gcd(6, 6)$
$= \gcd(0, 6)$
$= \gcd(6, 0)$
$= 6.$

Notice:

$$\gcd(a,b) = \gcd(a-b, b) = \gcd(a-2b, b) = \dots = \gcd(a-kb, b)$$

for any k.

in fact $\gcd(a,b) = \gcd(a \bmod b, b)$

Subtract as many copies of b as you can + see what's left.

Euclidean Algorithm

To find $\gcd(a,b)$, repeatedly apply these 2 rules:

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

— b is always getting smaller, so must eventually reach 0.

Examples.

$\gcd(60, 18)$

$= \gcd(18, 60 \bmod 18) = \gcd(18, 6)$

$= \gcd(6, 18 \bmod 6) = \gcd(6, 0) = 6.$

$\gcd(7169, 7811)$

$= \gcd(7811, 7169 \bmod 7811)$

$= \gcd(7811, 7169)$

$= \gcd(7169, 7811 \bmod 7169) = \gcd(7169, 642)$

$= \gcd(642, 7169 \bmod 642) = \gcd(642, 107)$

$= \gcd(107, 642 \bmod 107) = \gcd(107, 0) = 107.$

$$\gcd(742813, 24680)$$

$$= \gcd(24680, 2413)$$

$$= \gcd(2413, 550)$$

$$= \gcd(550, 213)$$

$$= \gcd(213, 124)$$

$$= \gcd(124, 89)$$

$$= \gcd(89, 35)$$

$$= \gcd(35, 19)$$

$$= \dots$$

$$= 1$$