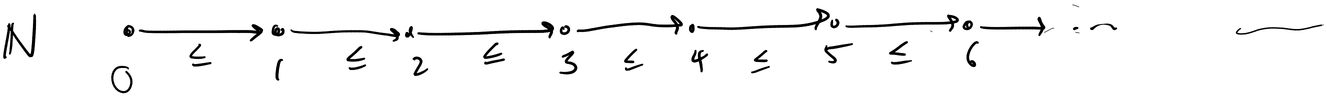
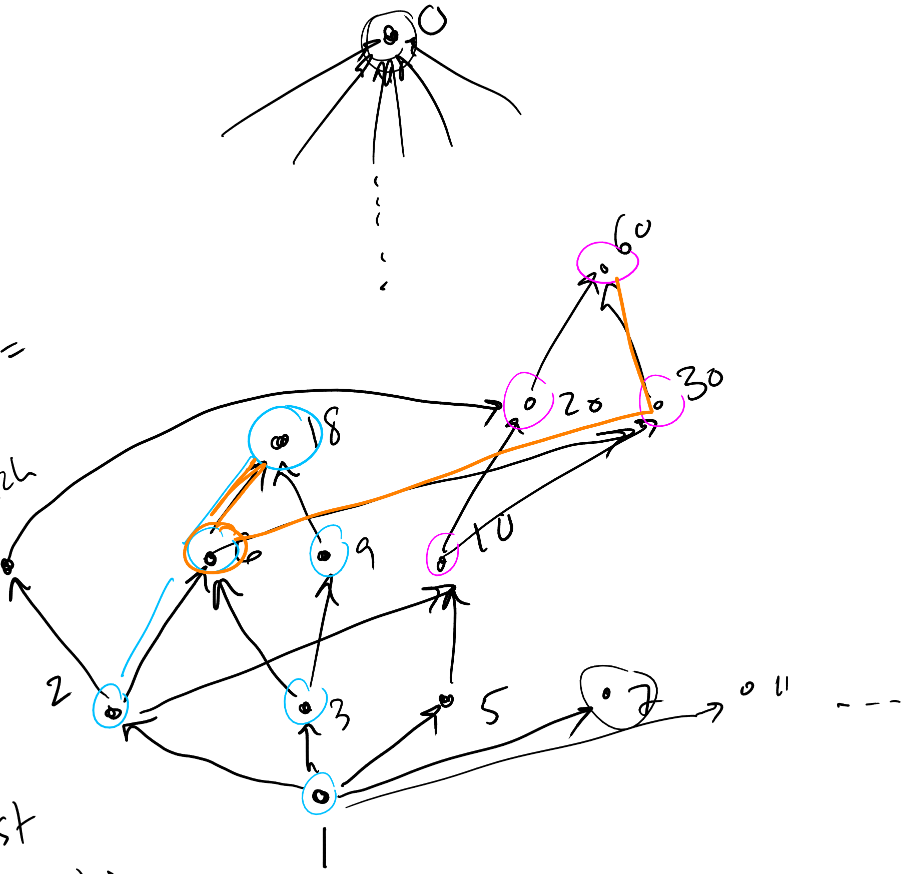
GCD + the Euclidean Algorithm

What is the greatest common divisor (GCD) of...

- 60 and 18? 6
- 7169 and 7811?



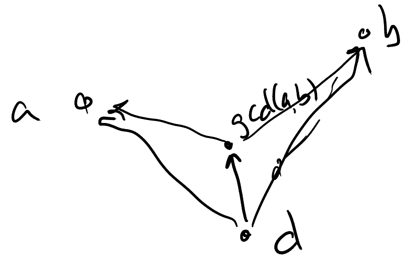
GCD of x, y = highest common point from which we can reach both x and y.

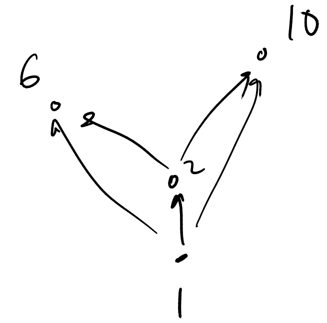


(LCM = lowest meeting point going up).

<u>Def$_n$</u> Let $a, b \in \mathbb{N}$. The greatest common divisor of a and b, denoted $\gcd(a,b)$, is the unique natural number such that for all $d \in \mathbb{N}$,

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





eg. $\gcd(6, 10) = 2$
$\gcd(2, 3) = 1$
$\gcd(6, 35) = 1$
$\gcd(2, 4) = 2$
$\gcd(3, 3) = 3$
$\gcd(0, 7) = 7$
$\gcd(0, 0) = 0$

a, b w/ $\gcd(a,b) = 1$ are "relatively prime" (ie. share no common factors)

<u>Computing gcd</u>

(1) – See what prime factorizations have in common.

eg. $18 = 2 \cdot 3^2$
$60 = 2^2 \cdot 3 \cdot 5$

$\Big\}$ $\gcd = 2 \cdot 3$.

② Euclidean Algorithm.

<u>Lemma</u>. $\gcd(a,b) = \gcd(b,a)$

<u>Theorem</u>. Let $a, b \in \mathbb{N}$. For all $k \in \mathbb{Z}$,

$$\gcd(a,b) = \gcd(a + kb, b).$$

eg. $\gcd(60, 18) = \gcd(78, 18)$

$= \gcd(24, 18)$

Proof – omitted.

<u>Theorem</u>. $\gcd(a,b) = \gcd(b, a \bmod b)$.

<u>Proof</u>. By Division Algorithm, write $\underline{a = qb + r}$ where $0 \leq r < b$.

$\gcd(\underline{a}, b)$

$\{ a = qb + r \}$.

$= \gcd(\underline{qb+r}, b)$

$\{$ Theorem – add or sub copies of $b \}$.

$= \gcd(qb + r - qb, b)$

$= \gcd(r, b)$

$= \gcd(b, r)$

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

Euclidean Algorithm

Let $a, b \in \mathbb{N}$. To find $\gcd(a,b)$, repeatedly apply these 2 rules:

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

eg.
$$\gcd(60, 18)$$
$$= \gcd(18, 6)$$
$$= \gcd(6, 0) = 6.$$

eg.
$$\gcd(13, 9)$$
$$= \gcd(9, 4)$$
$$= \gcd(4, 1)$$
$$= \gcd(1, 0) = 1.$$

eg
$$\gcd(7169, \underline{7811})$$
$$= \gcd(7811, 7169)$$
$$= \gcd(7169, 642)$$
$$= \gcd(642, 107)$$
$$= \gcd(107, 0) = 107$$