GCD's

for $a, b \in \mathbb{Z}$, $\gcd(a,b)$ is the largest positive integer d s.t.

$d \mid a$ and $d \mid b$.

if $a = \prod_{i=1}^{k} p_i^{e_i}$, $b = \prod_{i=1}^{k} p_i^{e_i'}$

(maybe some $e_i, e_i' = 0$) (e.g. $10 = 2^1 \cdot 3^0 \cdot 5^1$)

then $\gcd(a,b) = \prod_{i=1}^{k} p_i^{\min\{e_i, e_i'\}}$.

Other gcd characterizations:

$$\gcd(a,b) = \min_{x,y \in \mathbb{Z}} \{ |xa + yb| \}$$

How to compute?

Slow way:

```
let d = min{a,b}
while (a%d != 0 || b%d != 0)
    d--;
```

But for large integers (say 1000's of digits) this would be very slow. Let's find a better way.

(*) Observation: common divisors of a,b

are the same as the common divisors of b, r, where $r = a \,\%\, b$.

Aside: How to prove $S = T$ for sets S, T?

Let $x \in S$. Show this $\Rightarrow x \in T$.

$(S \subseteq T)$

Then let $y \in T$. Show $\Rightarrow y \in S$.

$(T \subseteq S)$

$(S \subseteq T) \wedge (T \subseteq S) \Rightarrow S = T$.

Say $a = qb + r$ $\quad q \in \mathbb{Z}, \ 0 \leq r < b$

Denote by $D(a,b)$ all common divisors of a, b.

So $D(b,r)$ = all common divisors of b, r.

Want: $D(a,b) = D(b,r)$

where $a = qb + r$.

let $d \in D(a,b)$. So $d|a$ & $d|b$.

$\Rightarrow \exists A, B \in \mathbb{Z}$ s.t. $a = dA$, $b = dB$.

Since $a = qb + r$,

$$\begin{aligned} r &= a - qb \\ &= dA - qdB \\ &= d(\underbrace{A - qB}_{\in \mathbb{Z}}). \end{aligned}$$

$\therefore\ d|r$. (So $D(a,b) \subseteq D(b,r)$)

Now let $d \in D(b,r)$.

Then $\exists B, R \in \mathbb{Z}$ s.t. $b = dB$, $r = dR$

So $a = qb + r = qdB + dR$

$= d(qB + R)$

$\Rightarrow d|a$. ✓

$\therefore\ D(a,b) = D(b,r)$

Time for recursion!

Above says $\gcd(a,b) = \gcd(\underset{\uparrow}{b}, \underset{\substack{\uparrow \\ r \lneq b}}{r})$.

So, <u>second</u> input is smaller!

Base case: second input = 0 :

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

This will actually work :

```
size_t gcd (size_t a, size_t b)
{
        if (b==0) return a;
        return gcd (b, a%b);
}
```