Warm-Up:
- Compute $\gcd(936, 650)$ using the Euclidean algorithm.
- Find the prime factorizations of 936 and 650.

Fundamental Theorem of Arithmetic

Every integer $n \geq 2$ can be factored uniquely as a product of primes.

up to commutativity

In practice, finding the prime factorization is HARD.

But the FTA has many "applications" in theoretical math.

As we see from the Warm-Up, we can easily compute $\gcd(a, b)$ if we have prime factorizations for both a and b.

Key points: Let $a, b \geq 2$ be integers.

- For any prime p,

  $p \mid a \iff$ p appears in the prime factorization of a

- $a \mid b \iff$ every prime in the prime factorization of a appears at least as many times in the prime factorization of b.

- The prime divisors of $\gcd(a,b)$ are the prime divisors that a and b have in common.

  The number of times a prime p appears in the factorization of $\gcd(a,b)$ is the smaller of
  - the number of times p appears in the factorization of a
  - " " " " " b

- $\gcd(a,b) = 1 \iff$ a and b have no prime divisors in common

  "a and b are relatively prime"

Let $p_1, \ldots, p_k$ be the complete list of primes which divide a or divide b.

We can write the prime factorizations as

$$a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

and

$$b = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k},$$

where $e_i \geq 0$ and $f_i \geq 0$ for all i.

Then

$$\gcd(a,b) = p_1^{\min(e_1,f_1)} p_2^{\min(e_2,f_2)} \cdots p_k^{\min(e_k,f_k)}.$$

Also,

$$\operatorname{lcm}(a,b) = p_1^{\max(e_1,f_1)} p_2^{\max(e_2,f_2)} \cdots p_k^{\max(e_k,f_k)}.$$

Why? This is the smallest positive integer divisible by both a and b.

Ex: $a = 96 = 2^5 \cdot 3 \cdot 5^0$, $\quad b = 180 = 2^2 \cdot 3^2 \cdot 5$

$$\gcd(96,180) = 2^2 \cdot 3 = 12$$
$$\operatorname{lcm}(96,180) = 2^5 \cdot 3^2 \cdot 5 = 1440$$

Thm: Let $a, b \in \mathbb{N}$. Then

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

Equivalently, $\operatorname{lcm}(a,b) = \dfrac{ab}{\gcd(a,b)}$ and $\gcd(a,b) = \dfrac{ab}{\operatorname{lcm}(a,b)}$.

Proof: Write

$$a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \quad \text{and} \quad b = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$$

as above.

Since $\min(e_i, f_i) + \max(e_i, f_i) = e_i + f_i$, we have

$$\begin{aligned} \gcd(a,b) \cdot \operatorname{lcm}(a,b) &= p_1^{e_1+f_1} p_2^{e_2+f_2} \cdots p_k^{e_k+f_k} \\ &= ab. \end{aligned}$$

∎

__Thm:__ Let $a, b, c \in \mathbb{Z}$.

① If $\gcd(b,c) = 1$, then
$$\gcd(a, bc) = \gcd(a,b) \cdot \gcd(a,c).$$

② If $\gcd(a,b) = 1$ and $\gcd(a,c) = 1$, then $\gcd(a, bc) = 1$.

③ Let $d = \gcd(a,b)$. Then $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

__Proof:__ ① Let $b = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ and $c = q_1^{f_1} q_2^{f_2} \cdots q_s^{f_s}$ be the unique prime factorizations of b and c, where $p_1, \ldots, p_r$ are the __distinct__ prime divisors of b and $q_1, \ldots, q_s$ are the __distinct__ prime divisors of c, and the exponents e_i and f_j are positive integers.

Since $\gcd(b,c) = 1$, $p_i \neq q_j$ for all i and j.

So $bc = \underbrace{p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}} \cdot \underbrace{q_1^{f_1} q_2^{f_2} \cdots q_s^{f_s}}$.

No primes in common

Now, the unique prime factorization of a will look like

$$a = p_1^{x_1} p_2^{x_2} \cdots p_r^{x_r} \cdot q_1^{y_1} q_2^{y_2} \cdots q_s^{y_s} \cdot (\text{other primes}),$$

where the exponents x_i, y_j are non-negative (some might be 0).

Thus,
$$\gcd(a,b) = p_1^{\min(e_1,x_1)} p_2^{\min(e_2,x_2)} \cdots p_r^{\min(e_r,x_r)},$$

$$\gcd(a,c) = q_1^{\min(f_1,y_1)} q_2^{\min(f_2,y_2)} \cdots q_s^{\min(f_s,y_s)},$$

and

$$\gcd(a,bc) = \gcd(a,b) \cdot \gcd(a,c).$$

② + ③ HW 16.