Write FTA on side board

Warm-Up: Given that

$$10{,}192 = 2^4 \cdot 7^2 \cdot 13$$

and

$$271{,}656 = 2^3 \cdot 3^2 \cdot 7^3 \cdot 11$$

compute $\gcd(10{,}192,\ 271{,}656)$

and

$\operatorname{lcm}(10{,}192,\ 271{,}656)$.

Thm (Division by a prime): Let p be a prime number. Then for all $x, y \in \mathbb{Z}$, if $p \mid xy$ then $p \mid x$ or $p \mid y$.

i.e.,

$$xy \equiv 0 \bmod p \implies \begin{array}{l} x \equiv 0 \bmod p \\ \text{or} \\ y \equiv 0 \bmod p \end{array}$$

Note: The requirement that p be prime is important!

Ex: $4 \mid 6 \cdot 10$ (since $6 \cdot 10 = 60 = 4 \cdot 15$), but $4 \nmid 6$ and $4 \nmid 10$.

Proof: Let p be a prime and $x, y \in \mathbb{Z}$. Suppose $p \mid xy$.

If $p \mid x$, then we are done. So suppose $p \nmid x$. We must show that $p \mid y$.

Since $p \nmid x$, $\gcd(p, x) = 1$ (HW 15).

Thus, by the reverse Euclidean Algorithm, there exist $u, v \in \mathbb{Z}$ such that

$$pu + xv = 1$$

Multiply by y to get

$$puy + xyv = y$$

Since $p \mid puy$ and $p \mid xyv$, we have $p \mid y$, as desired. $\blacksquare$

Cor: Let p be a prime. For each $n \in \mathbb{N}$ and all $x_1, x_2, \ldots, x_n \in \mathbb{Z}$, if $p \mid (x_1 x_2 \cdots x_n)$ then p divides at least one of $x_1, x_2, \ldots, x_n$.

Proof: Let $P(n)$ be the sentence

"For all $x_1, \ldots, x_n \in \mathbb{Z}$, if $p \mid (x_1 \cdots x_n)$ then p divides at least one of the x_i."

We will prove $P(n)$ holds for all $n \in \mathbb{N}$ by induction.

Base Case: $P(1)$ is automatically true, since if $p \mid x_1$, then $p \mid x_1$

Inductive Step: Let $n \in \mathbb{N}$ and suppose $P(n)$ is true.

Let $x_1, \ldots, x_{n+1} \in \mathbb{Z}$ and suppose

$$p \mid (x_1 \cdots x_n) \cdot (x_{n+1}).$$

By the theorem on division by a prime, $p \mid (x_1 \cdots x_n)$ or $p \mid x_{n+1}$.

If $p \mid (x_1 \cdots x_n)$, then by $P(n)$, $p \mid x_i$ for some $1 \leq i \leq n$, and we have the desired conclusion.

If $p \mid x_{n+1}$, then we also have the desired conclusion.

In either case, $P(n+1)$ is true, completing the inductive step.

$\blacksquare$

Applications of FTA

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.

In particular, we can re-cast statements about divisibility in terms of prime factorizations.

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"

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

$$\gcd(96, 180) = 2^2 \cdot 3 = 12$$

We can compute the least common multiple (HW 14) similarly:

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

In heavier notation:

Let $a, b \geq 2$. We can write their 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 $p_1, \ldots, p_k$ is the complete list of primes which divide a or b, and

$$e_i \geq 0 \quad \text{and} \quad f_i \geq 0$$

for all i.

Then $\boxed{a \mid b \iff e_i \le f_i \quad \text{for all } i.}$

It follows that

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

and

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

<u>Thm</u>: 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 $\gcd(a,b) = \dfrac{ab}{\operatorname{lcm}(a,b)}$.

<u>Proof</u>: 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

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

$\blacksquare$