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

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

In general, let $p_1, \dots, p_k$ be the complete list of primes which divide a <u>or</u> 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.

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

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

$\blacksquare$

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 $p_1, \dots, p_r$ are the distinct prime divisors of b and $q_1, \dots, q_s$ 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 17.

Proof of FTA part 1

Let S be the set of all counterexamples to FTA 1.

That is, for $n \in \mathbb{N}$,

$n \in S \iff n \geq 2$ and n is not equal to a product of primes.

We want to argue that FTA 1 is true, meaning S is empty.

Suppose, to get a contradiction, that S is not empty. Then, by the Well-Ordering Axiom, there is a smallest element in S.

Call it a.

Since $a \geq 2$, we know there is some prime p such that $p \mid a$.

Thus, $a = pk$ for some $k \in \mathbb{Z}$.

Since a and p are both positive, so is k. So $k \geq 1$.

If $k = 1$, then $a = p$ is prime. But then $a \notin S$, a contradiction.

If $k > 1$, then $k \geq 2$ (since $k \in \mathbb{Z}$) but $k < pk = a$ (since $p \geq 2$).

So k is smaller than a, the smallest element in S. Thus, $k \notin S$, meaning k is a product of primes.

But then $a = pk$ is a product of primes. So $a \notin S$, a contradiction. ∎