Here are a few more applications of FTA:

<u>Thm</u>: 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 $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

<u>Proof</u>: 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 <u>distinct</u> prime divisors of b and $q_1, \dots, q_s$ are the <u>distinct</u> 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 HW 15.

③ HW 16. $\blacksquare$

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. $\blacksquare$

Proof of FTA part 2

Let $P(k)$ be the sentence

"Any integer $n \geq 2$ which is equal to a product of k primes has a unique prime factorization."

We will prove $P(k)$ is true for all $k \in \mathbb{N}$ by induction.

Base Case: $k=1$. If n is a product of one prime, then

$$n = p$$

is prime.

If $n = p = q_1 q_2 \cdots q_\ell$ is another factorization into primes q_i, then $p \mid q_1 \cdots q_\ell$, so by the corollary p divides one of the q_i.

WLOG, $p \mid q_1$. But p and q_1 are both prime, so $p = q_1$. If $\ell \geq 2$, then

$$\cancel{p} = \cancel{p} q_2 \cdots q_\ell$$

so

$$1 = q_2 \cdots q_\ell.$$

But this is impossible, so $\ell = 1$ and

$$n = p$$

is the unique prime factorization. $\blacksquare$

<u>Inductive Step</u>: Let $k \in \mathbb{N}$ and suppose $P(k)$ is true.

Now, let $n \in \mathbb{N}$ be such that

$$n = p_1 p_2 \cdots p_{k+1}$$

is a product of $k+1$ primes p_i

If $n = q_1 q_2 \cdots q_\ell$ is another prime factorization, then since $p_1 \mid n$, we have $p_1 \mid (q_1 \cdots q_\ell)$.

Similar to above, we deduce that p_1 is equal to one of the q_i's. WLOG, $p_1 = q_1$.

Then $\cancel{p_1} p_2 \cdots p_{k+1} = \cancel{p_1} q_2 \cdots q_\ell$, so

$$p_2 \cdots p_{k+1} = q_2 \cdots q_\ell.$$

But the left-hand side is a product of k primes, so it has a unique prime factorization by $P(k)$.

Thus, $\ell = k+1$ and, up to reordering, the primes $q_2, \ldots, q_{k+1}$ are exactly the primes $p_2, \ldots, p_{k+1}$.

That is, n has a unique prime factorization.

This proves $P(k+1)$, completing the inductive step. $\blacksquare$