Goal: Prove the Fundamental Theorem of Arithmetic (Every natural number other than 1 can be factored into primes in only one way, except for the order of the factors.)

Well Ordering Principle Axiom: Every nonempty set of positive integers contains a smallest member.

Suppose the Fundamental Theorem of Arithmetic is **false**.

Then by the **Well Ordering Principle** there is some smallest positive integer Smallest that has at least two distinct factorizations.

Let us consider one set with r primes... ...and another set with s primes.

$$\text{Smallest} = p_1 p_2 p_3 \cdots p_r \qquad \text{Smallest} = q_1 q_2 q_3 \cdots q_s$$

We want to prove as a **Lemma** the prime sets are disjoint: that **the primes in the "first set" $p_1 \cdots p_r$ and "second set" $q_1 \cdots q_s$ are disjoint.**

Suppose it is **false** that the prime sets are disjoint, so the "first set" and "second set" have a common prime.

We can reorder the primes such that $p_1 = q_1$. Then we can divide both sets by p_1:

$$\text{Smallest} = p_1 p_2 p_3 \cdots p_r \qquad \text{Smallest} = q_1 q_2 q_3 \cdots q_s$$

$$\frac{\text{Smallest}}{p_1} = p_2 p_3 \cdots p_r \qquad \frac{\text{Smallest}}{p_1} = q_2 q_3 \cdots q_s$$

This produces an positive integer smaller than Smallest that has two unique factorizations. This is a contradiction.

Therefore it is **true** that the prime sets are disjoint.

Because the prime sets are disjoint between the "first set" and "second set", $p_1 \neq q_1$. Let $p_1 < q_1$. (By symmetry, the same argument will work for if $p_1 > q_1$, so we are just picking as a convention which is smaller.)

Define an positive integer New such that

$$\boxed{\text{New} = (q_1 - p_1) q_2 q_3 \cdots q_s}$$

so $\text{New} = q_1 q_2 q_3 \cdots q_s - p_1 q_2 q_3 \cdots q_s$

and by substitution $\text{New} = \text{Smallest} - p_1 q_2 q_3 \cdots q_s$

From this statement it is clear New < Smallest.

We chose Smallest to be the smallest positive integer with at least two distinct factorizations. Therefore New must have only one factorization, so any prime in one factorized form of New must also divide any other factorized form of New.

Continuing with the last equation $\text{New} = \text{Smallest} - p_1 q_2 q_3 \cdots q_s$

Substituting again $\text{New} = p_1 p_2 p_3 \cdots p_r - p_1 q_2 q_3 \cdots q_s$

and extracting the p_1 $\text{New} = p_1 (p_2 p_3 \cdots p_r - q_2 q_3 \cdots q_s)$

So New has a factoring form with a prime factor of p_1.

Returning to the original form of New, $\boxed{\text{New} = (q_1 - p_1) q_2 q_3 \cdots q_s}$

Suppose it is **true** New has a prime factor of p_1 in this form.

We know that because the prime sets are disjoint that $q_2 q_3 \cdots q_s$ must be distinct from p_1, so $q_1 - p_1$ is the only term that can be considered: it must have a prime factor of p_1.

Since p_1 divides $q_1 - p_1$ there is some integer b such that

$$p_1 b = q_1 - p_1$$
$$p_1 b + p_1 = q_1$$
$$p_1 (b+1) = q_1$$

so p_1 divides q_1, but q_1 is a prime. This is a contradiction.

So the original supposition is **false** and New has a factoring form without a prime factor of p_1.

So we have two forms, one where
New has a factoring form with a prime factor of p_1
and another where
New has a factoring form without a prime factor of p_1.

Hence New has two factorizations. But New must have only one factorization, so we have a contradiction.

Since we supposed the Fundamental Theorem of Arithmetic is **false**, it must be **true**.