Unique Factorization Theorem Proof

Adithya Prabha, Louis Hu, Sophia Tatar, Carmen Zhang, Mert Efe Çankaya

Ross Mathematics Program

1 Axioms

The system $\mathbb{Z}$ of integers satisfies the axioms listed below.

1.1 Ring Axioms

The set $\mathbb{Z}$ has two binary operations, addition $(+)$ and multiplication $(\cdot)$. This means that whenever $a, b \in \mathbb{Z}$ then the numbers $a+b$ and $a \cdot b$ are defined. Multiplication is often abbreviated by omitting the dot: $ab = a \cdot b$.
In the following statements, a, b, c, x etc. represent arbitrary elements of $\mathbb{Z}$. 0 and 1 are particular elements of $\mathbb{Z}$, whose definitions are consequences of the axioms.

1. Commutative: $a + b = b + a$ and $ab = ba$
2. Associative: $a + (b + c) = (a + b) + c$ and $a(bc) = (ab)c$
3. Distributive: $a(b + c) = ab + ac$.
4. Zero: $(\exists 0)$ such that $(\forall a) a + 0 = a$.
5. Negatives: $(\forall a)$ $(\exists x)$ $a + x = 0$.
6. One: $(\exists 1)$ such that $(\forall a)$ $a \cdot 1 = a$.

1.2 Order Axioms

There is a nonempty subset $P \subseteq \mathbf{Z}$ with following properties:

1. $P + P \subseteq P$: $(\forall a, b \in P) a + b \in P$.
2. $P \cdot P \subseteq P$: $(\forall a, b \in P) ab \in P$.
3. Nontriviality: $0 \notin P$.
4. Trichotomy: $(\forall a \in \mathbf{Z})$ exactly one of the properties holds: $a \in P, a = 0, -a \in P$.

1.3 Well Ordering Principle (WOP)

Let S be a subset of $\mathbb{Z}^+$ such that $S \neq \emptyset$.
Then S contains a least element. In other words
there exists an $s \in S$ such that
for all $t \in S$,
$s \leq t$.

2 Definitions

2.1 Min

Definition: Minimum of Set
$m \in S$ is defined as the minimum of set S if and only if $\forall k \in S, m \leq k$.

2.2 Less Than

Definition: Less Than
Let a, b be integers. a is said to be less than b when $b + (-a) \in P$. This is denoted as $a < b$.

2.3 Less Than or Equal to

Definition: Less Than or Equal to
Let a, b be integers. a is said to be less than or equal to b when $b + (-a) \in P \cup \{0\}$. This is denoted as $a \leq b$.

2.4 Greater Than

Definition: Greater Than
Let a, b integers. a said to be greater than b when $b < a$. This is denoted as $a > b$.

2.5 Greater Than or Equal to

Definition: Greater Than or Equal to
Let a, b integers. a said to be greater than or equal to b when $b \geq a$.

2.6 Divides

Definition: Divides (§|§)
For two integers a, b we denote $a|b$ if $\exists k \in \mathbf{Z}$ s.t. $b = a * k$.
$\neg(a|b)$ is denoted as $(a \nmid b)$ meaning $\nexists k \in \mathbf{Z}$ s.t. $b = a * k$.

2.7 Prime-Composite Numbers

Definition: Prime and Composite Numbers
<u>Prime</u>
A positive integer $p \neq 1$ is characterized as a prime when $k \in P$, $k|p \implies k = 1$ or $k = p$.
<u>Composite</u>
An integer m is characterized as a composite number when it is not a prime. Meaning $\exists k \in P$ s.t. $k|m$ but $k \neq m$ and $k \neq 1$.

2.8 Product Notation

Let the product be defined recursively.

$$p_{n+1} = \prod_{i=1}^{n+1} f(i) = p_n \cdot f_n \textbf{ where } p_0 = 1$$

2.9 Exponents

$$a^n = a \quad \text{for } n = 1$$

$$a^n = a \cdot a^{n-1} \quad \text{for } n > 1$$

Further,

$$\prod_{i=1}^{n} a = a^n$$

2.10 Power Rules

$$a^{m+n} = a^m \cdot a^n$$

Let $S = \{m \mid a^{m+n} \neq a^m \cdot a^n, \quad m, n \in P\}$
Suppose, for the sake of contradiction, $S \neq \emptyset$. Since set S is a subset of P, by W.O.P. there must exist a smallest element $m \in S$. By the definition of minimum, $m - 1 \notin S$, and by NIBZO (Negative Integers Belong to $\mathbb{Z}$ and $\mathbb{O}$), $m - 1 \in P$. By the definition of S, for all $n \in P$, $a^{(m-1)+n} = a^{m-1} \cdot a^n$. We also know, by the Negatives Axiom, that $m = (m - 1) + 1$.

$$n = \prod_{i=1}^{c} a_i = \prod_{j=i}^{k} b_j$$

$b_1|a_i$. b_1, a_i are primes so $b_1 = a_i$.

$$\text{Therefore } a_1 = b_1 \text{ substitute } a_1 \text{ for } b_1, a_1 \cdot \prod_{2}^{c} = a_1 \cdot \prod_{2}^{k}$$

3 Lemmas

3.1 Multiplication with 0

Using the commutative property of multiplication, we have $a \cdot 0 = 0 \cdot a$. By applying the zero axiom and the distributive property, we can simplify the equation to $a \cdot 0 + a \cdot 0 = a \cdot 0$. Cancelling the common term $a \cdot 0$ on both sides, we obtain $a \cdot 0 = 0$. Assuming for contradiction that $0 = 1$, substituting 0 with 1 gives us $a \cdot 1 = 0$. However, this contradicts the one axiom, which states that $a \cdot 1 = a$ and cannot be equal to 0. Therefore, we conclude that 0 cannot be equal to 1, proving that $a \cdot 0 = 0$.

3.2 Uniqueness of Negatives

Claim: $\forall a$, let $-a$ be solution to $a + x = 0$. This solution is unique.

Proof. Let b, c be solutions to $a + x = 0$. Meaning $a + b = 0$ and $a + c = 0$. By transitivity, $a + b = a + c$. Add inverse of a to both sides. $(a + b) + (-a) = (a + c) + (-a)$. By commutativity and associativity we can give the equation the form, $b + (a + (-a)) = c + (a + (-a))$. By definition this means, $b + 0 = c + 0$. Which implies $b = c$ by zero axiom. So for all $a \in \mathbb{Z}$ any number satisfying $a + x = 0$ is equal and therefore $-a$ is unique. $\square$

3.3 Opposite of a Product

Claim: $\forall a, b - (ab) = (-a)b = a(-b)$

Proof. $-(ab)$ is the unique solution to the equation $ab + x = 0$.

1. $-(ab) = (-a)b$ $ab + x = 0$

   Let x be $(-a)b$

   $ab + (-a)b = ba + b(-a)$

   $b(a+(-a)) = b \cdot 0$ Which we now equates to 0. Therefore $(-a)b$ satisfies $ab+x = 0$ so -$(ab) = (-a)b$

2. $-(ab) = a(-b)$ $ab + x = 0$

   Let x be $a(-b)$

   $ab + a(-b) = b(a + (-a))$

   $= b \cdot 0$ Which we now equates to 0. Therefore $a(-b)$ satisfies $ab + x = 0$ so $-(ab) = a(-b)$

$\square$

3.4 Opposite of an Opposite

Claim: $\forall a - (-a) = a$

Proof. $-(-a)$ is the unique solution to the equation $-a+x = 0$. If a satisfies $-a+x = 0$, then $-(-a) = a$. $-a + a = a + (-a)$ Which we know equates to zero by zero axiom. Therefore $a = -(-a)$ $\square$

3.5 Product of Opposites

Claim: $\forall a, b$ $(-a)(-b) = ab$

Proof. By lemma 3.3, $(-a)(-b) = -(a(-b))$ and by the same lemma, $-(-(ab))$. By the lemma 3.4, $-(-(ab)) = ab$. Therefore $(-a)(-b) = ab$. $\square$

3.6 Zero Product

Claim:

$$\forall a, b \in \mathbb{Z}\ ab = 0 \implies a = 0 \text{ or } b = 0$$

Proof. For the sake of contradiction assume there exists $a, b \in \mathbb{Z}$ s.t. $ab = 0, a \neq 0\ b \neq 0$.
By trichotomy, we know there are 4 possibilities for a,b which we'll inspect separately:

1. $a \in P, b \in P$

   By $P \cdot P \subseteq P$ axiom, $ab \in P$ so $ab \neq 0$ by trichotomy.

   Therefore $a, b \in P$ doesn't work

2. $a \in P, -b \in P$ By lemma 3.4 $ab = a(-(-b))$ By lemma 3.3, $a(-(-b)) = -(a(-b))$ By $P \cdot P \subseteq P$ axiom, $a(-b) \in P$ so $a(-b) = -(-(a(-b)))$ So by trichotomy $-(a(-b)) = ab \neq 0$.

3. $-a \in P, b \in P$

   By lemma 3.4 $ab = -(-(a))b$ By lemma 3.3, $-(-(a))b = -((-a)b)$ By $P \cdot P \subseteq P$ axiom, $(-a)b \in P$ so $(-a)b = -(-((-a)b))$ So by trichotomy $-((-a)b) = ab \neq 0$.

4. $-a \in P, -b \in P$

   By lemma 3.4 $ab = (-(-a))(-(-b))$ By lemma 3.3 $(-(-a))(-(-b)) = -((-a)(-(-b)))$ Again, $-((-a)(-(-b))) = -(-((-a)(-b)))$ Which we know is equal to $(-a)(-b)$ by lemma 3.4. By $P \cdot P \subseteq P$ axiom, $(-a)(-b) \in P$, so $ab \in P$. By trichotomy this means, $ab \neq 0$.

   Contradiction: For all cases, if $a \neq 0$ and $b \neq 0$, ab is never equal to zero. By contrapositive, $\forall a, b \in \mathbb{Z}, ab = 0 \implies a = 0$ or $b = 0$.

□

3.7 Cancellation

Claim:

$$\forall a, b, b' \in \mathbb{Z} \text{ if } a \neq 0 \text{ then } ab = ab' \implies b = b'$$

Proof. Take a, b, b' $\in \mathbb{Z}$ where $ab = ab'$. By negative axiom we know there exists. An inverse of ab' that is $-(ab')$. Add this to both sides and you get $ab + (-(ab')) = ab' + (-(ab'))$. We know the left sides equates to zero by negative axiom. $ab + (-(ab')) = 0$. By lemma 3.3, we say $ab + a(-b') = 0$. By distribution we get $a(b + (-b')) = 0$. By lemma 3.5, we know a=0 or b+(-b')=0. Since a $\neq 0$ is given, b+(-b')=0. When we add b' to both sides, by commutativity and associativity, we get b+ (b'+(-b'))=b'. Which implies b=b' by definition of negative and axiom of zero.
Therefore

$$\forall a, b, b' \in \mathbb{Z} \text{ if } a \neq 0 \text{ then } ab = ab' \implies b = b'$$

□

3.8 Exponent Lemma

Claim: $a^{m+n} = a^m \cdot a^n$ **for any real number** a **and any numbers in P** m **and** n

Proof. Let $S = \{m \mid a^{m+n} \neq a^m \cdot a^n,\ m, n \in P\}$
Suppose FTSOC, $S \neq \emptyset$
By WOP, $\exists\ (m, n)$ such that $m = \min(S)$, and by the definition of S, $\exists\ n$ s.t., $a^{m+n} \neq a^m \cdot a^n$
By NIBZO, $m - 1 \in P$, and $(m-1, n) \notin S$
$\forall n \in P$, $a^{(m-1)+n} = a^{m-1} \cdot a^n$
Then, $m = (m-1) + 1$
By substitution, $a^{m+n} = a^{(m-1)+(1+n)}$
By the definition of S, $a^{(m-1)+(1+n)} = a^{m-1} \cdot a^{1+n}$
By the definition of exponents, $a^{1+n} = a^n \cdot a$, and by substitution, $a^{(m-1)+(1+n)} = a^{m-1} \cdot (a^n \cdot a)$
Through associative and commutative property, $a^{(m-1)+(1+n)} = (a^{m-1} \cdot a) \cdot a^n$
By the definition of exponents, $a^{m-1} \cdot a = a^m$, and again through associative, commutative, negative, zero and substitution, $a^{m+n} = a^m \cdot a^n$
$\Rightarrow\!\Leftarrow$
Thus, $S = \emptyset$

$\square$

3.9 Product of Products

Claim:

$$\forall\ n, m \in P \text{ s.t. } \prod_{i=1}^{n} a_i \cdot \prod_{i=1}^{m} b_i = \prod_{i=1}^{m+n} c_i$$

where $c_i = g_i$ and $1 \leq i \leq n$
$h_{i-n}, n + 1 \leq i \leq m$

Proof. Let $S = \{m \mid m \in P \text{ s.t. } \exists\ n \in P,\ \prod_{i=1}^{n} a_i \cdot \prod_{i=1}^{m} b_i = \prod_{i=1}^{m+n} c_i\}$
By WOP,

$\exists\ m = \min(S)$

$\exists\ n \in P$

$\prod_{i=1}^{n} a_i \cdot \prod_{i=1}^{m} b_i = \prod_{i=1}^{m+n} c_i$

$\forall n \in P\ \prod_{i=1}^{n} a_i \cdot \prod_{i=1}^{0} b_i \cdot 1 = \prod_{i=1}^{m+n} c_i$ by the One Axiom

$m \neq 1$
By NIBZO, $m > 1$. Then, for $m - 1$

Multiply b_m on both sides yields, $\prod_{i=1}^{n} a_i \cdot \prod_{i=1}^{m-1} b_i \cdot b_m = \prod_{i=1}^{m-1+n} c_i \cdot b_m$

$\prod_{i=1}^{n} a_i \cdot \prod_{i=1}^{m} b_i = \prod_{i=1}^{m+n} c_i$

$\prod_{i=1}^{n} a_i \cdot \prod_{i=1}^{m-1} b_i = \prod_{i=1}^{m-1+n} c_i$

$\Rightarrow\!\Leftarrow$
Thus, $S = \emptyset$

$\square$

3.10 Set 1, P5)

Claim: If $a, b, c \in \mathbb{Z}, a \mid b \Rightarrow a \mid bc$

Proof. Given $a \mid b$, by the definition of divides $\exists\ k \in \mathbb{Z}$, s.t., $ak = b$.
Multiplying both sides by c, $c(ak) = c(b)$. By associative property, $a(ck) = bc$. By the definition of divides, $a \mid bc$

□

3.11 Divides Implies LEQ

Claim:

$$\forall a, b, \in P. \text{ If } a \mid b, \text{ then } a \leq b$$

Proof. By the definition of divisibility, and $a \mid b$, $\exists\ k \in \mathbb{Z},\ ak = b$

If $k = 0, b = ak = a \cdot 0 = 0$. But by non triviality, $0 \notin P$. Thus, $k \neq 0$

If $k \notin P$, by Trichotomy $-k \in P$. Then, by $P \cdot P \subseteq P$, and $a \in P, a \cdot (-k) = -ak \in P$. But this contradicts $ak = b \in P$, and trichotomy. Therefore $k \in P$.

By NIBZO, $0 < k < 1$ is not true.

When $k = 1$, $b = ak = a$
When $k > 1$, by the definition of greater than, $k - 1 \in P$
By $a \in P$ and by $P \cdot P \subseteq P$, $a(k-1) = ak - a = b - a \in P$, and by the definition of less than, $b > a$

Therefore, $a \leq b$

□

3.12 Divides is reflexive

$a|a \implies \exists x$ such that $a \cdot x = a$ meaning $x = 1 \in \mathbb{Z}$ forcing a to divide itself.

3.13 Prime Power Lemma

Claim:

$$p^c = p \implies c = 1$$

Proof. Let $S = \{c > 1 | p^c = p,\ \text{p is prime}\}$. FTSOC, suppose $S \neq \emptyset$. Because $\forall c \in S$, $c \in P$, we have $S \subseteq P$.
By NIBZO, theorem 4.1, $\nexists a$ s.t. $0 < a < 1$. Thus $\forall c \in S, c > 1 \implies c \geq 2$. This implies by WOP, we would get $min(S) = 2$. By the description of $p, p^2 = p \implies p^2 - p = 0 \implies p(p-1) = 0$. By Lemma 3.5,$p = 0 or p - 1 = 0 \implies p = 1$. This contradicts the primality of p. Then we get $S = \emptyset$ and there are no $c > 1$ such that $p^c = p$ for prime p. By NIBZO, $\nexists a$ s.t. $0 < a < 1$. Thus the only integer c such that $p^c = p$ for all primes is 1.

□

4 Theorems

4.1 No Integer Between Zero and One (NIBZO)

Claim: $\nexists\ a \in P$ **s.t.** $0 < a < 1$

Proof. Let P represent the set of all positive integers. Let $S = \{a \mid a \in P, 0 < a < 1\}$
By W.O.P, $\exists\ m$ s.t. $\min(S) = m$,
Assume $0 < m < 1$
then $m < 1$, and $1 - m \in P$ by the definition of less than
Since $m \in P$, then $m(1-m) \in P$ by $P \cdot P \subseteq P$
$\Rightarrow m - mm \in P$ by the Distributive Property
$mm < m$ by the definition of less than
Also, since $m \in P$,
then $m = m - 0 \in P$
By $P \cdot P \subseteq P$, $m(m-0) \in P$
By the Distributive Property, $mm - 0 \in P$
$0 < mm$ by the definition of less than
and $mm \in S$, as $S \subseteq P$
$\Rightarrow 0 < mm < m$
$\Rightarrow\!\Leftarrow$
As we found a smaller positive integer less than m, which contradicts with $min(S) = m$
Therefore, 1 is $min(S)$, and there is no integer between zero and one

□

4.2 Prime Division Theorem

Claim: If $p \mid a_1 a_2 \ldots a_n$, then $p \mid a_i$, for some index i, $1 \leq i \leq n$

Proof. Let $S = \{n \mid n \in P, \exists\ p$ prime $\mid \prod_{i=1}^{n} a_i$, and $\forall i, 1 \leq i \leq n, p \nmid a_i$

By WOP, $\exists\ m = \min(S)$
then, $\exists\ p$ prime, s.t. $p \mid \prod_{i=1}^{m} a_i$, but $\forall i, 1 \leq i \leq m, p \nmid a_i\}$

Since 1 is not prime, $1 \notin S$, therefore, $m \neq 1$. By NIBZO $m > 1$, therefore, $m - 1 \in P$.

Then, $\exists\ p$ prime, s.t. $p \mid \prod_{i=1}^{m} a_i = \prod_{i=1}^{m-1} a_i \cdot a_m$ by Set 1, P5).

Then, for some i, $p|a_i$ from "m-1". $\Rightarrow\!\Leftarrow$

Therefore, $S = \emptyset$

□

4.3 Every Positive Integer Except 1, Has a Prime Divisor

Claim: Every positive integer has a prime divisor except 1

Proof. Let S = $\{x \mid x \in P, x \neq 1$ s.t. x has no prime divisor$\}$
By Well Ordering Principle, $\exists\, m = \min(S), m = ab$, and $a, b \in P$
Case 1: $m = 1$,
exclude
$\Rightarrow\!\Leftarrow$
as $m \notin S$
Case 2: m is prime
as $m = 1 \cdot m$, by the one axiom
$\Rightarrow\!\Leftarrow$
Case 3: m is composite
$m = ab$, and $1 < a, b < m$
By the definition of GCD, $a \mid m$ and $b \mid m$,
and by Divides Implies LEQ, $\Rightarrow a < m$, and $b < m$,
Since $a, b \notin S$, as $a, b < m$, then
Let $a = pc$, where p is a prime divisor
Given $m = ab$, by substitution, $m = (pc)b$
By associativity, $m = p(cb)$
$\Rightarrow\!\Leftarrow$
Therefore, S = $\emptyset$, meaning every positive integer, except 1 has a prime divisor.

□

4.4 Every Positive Integer Except 1, Can be Expressed as a Product of Positive Primes

Let $S = \{x \in Ps.t.\ x$ can't be expressed as a product of positive primes$\}$. $S \subseteq P$ and FTSOC, assume $S \neq \emptyset$. By WOP, $\min(S) = m$. Because m can't be expressed as a product of primes, m cannot be prime. This is because $\prod_{i=1}^{1} m = m$. This, m can be expressed as a product. Thus, m is composite and $m = a \cdot b$ for composite a, b. Because $a, b|m$; $a, b < m$ and $a, b \notin S$ meaning that a, b can be expressed as a product of positive primes. Let $a = \prod_{i=1}^{n} p_i^{e_i}$ and $b = \prod_{j=1}^{m} q_j^{e_j}$. Thus, $m = a \cdot b = \prod_{i=1}^{n} p_i^{e_i} \cdot \prod_{j=1}^{m} q_j^{e_j}$ where both product terms are a product of primes. Thus, m can be expressed as a product of primes.

4.5 Every Positive Integer Except 1 has a Prime Factorization

Proof. Consider a positive integer greater than 1.
Case 1: n is prime,
$n = 1 \cdot n$ by the One Axiom.
Therefore, 1 has a prime factorization
Case 2: n is not prime
By the definition, $n = ab$, where a and b are not ± 1
Let $S = \{x \mid x \in P$ and x is composite s.t. x does not have a prime factorization$\}$
By W.O.P.,
$\exists\ m = \min(S)$
$m = ab$, where a, b are composite.
Let $a, b \in P$, and since $a \mid m$ and $b \mid m$, by Divides Implies LEQ, $a, b < m$
let $a = \prod_{i=1}^{n} g_i$
let $b = \prod_{i=1}^{f} h_i$
Then $m = ab = (\prod_{i=1}^{n} g_i)(\prod_{i=1}^{f} h_i) = \prod_{i=1}^{n+f} c_i$
where $c_i =$
g_i and $1 \leq i \leq$ n
h_{i-n} and $1 \leq i \leq$ n

$\Rightarrow\!\Leftarrow$
As m can be expressed as a product of primes.
Therefore, $s = \emptyset$ $\square$

4.6 Every Integer Except 1 Can Be Expressed as a Product of Ordered Primes

Let $S = \{a \in P | \nexists \prod_{i=1}^{n} p_i = a$ **such that** $p_{i+1} \geq p_i\}$ and $\forall a \in S, a \in P$. Proved tht all numbers can be expressed as a product of primes. Let $S_1 = \{p | p$ is a prime divisor of a$\}$. Because all prime numbers are positive $S_1 \subset P$. By WOP, $\exists \min(S_1) = p_1$. This implies p_1 is the smallest prime that divides a. By $p_1 | a$ and the definition of divisibility, $\exists x, a = p_1 \cdot x$. By lemma Divides Implies LEQ, $x \leq a$. Supposed $x = a$. That gives $1 \cdot a = p_1 \cdot a$. By Lemma 3.2, $p_1 = 1$ which contradicts the primality of p_1. Therefore, $x \neq a$, $x \leq a \implies x < a$.

No, because a is the smallest integer that cannot be written as a product of ordered primes, x must be able to be written as a product of ordered primes. Therefore, let's say $x = \prod_{i=1}^{b} q_i$ such that $\forall w, 1 \leq w \leq b$, there is $q_w \leq q_{w+1}$.

Let $S_2 = \{q \in P | q | x$ and $q < p_1\}$. Because $\forall q \in S_2, q \in P$, we have $S_2 \subset P$. By WOP, $\min(S_2) = q_1$. By Lemma Set 1, P5), $q_1 | x \implies q_1 | x \cdot p_1 \implies q_1 | a$. This contradicts p_1 is the smallest prime divisor of a. That leads to $S_2 = \emptyset$ or $\forall i, p_i \leq q_i$.

Now we know $a = p_1 \cdot x = p_1 \cdot \prod_{i=1}^{n} q_i$, where $\forall i$ such that $1 \leq i \leq n-1$, there is $p_1 \leq q_i$.

That means I can now define a as a product of ordered primes. Let $a = \prod_{i=1}^{b+1} k_i$ where $k_1 = p_1$ and $k_n = q_{n-1}$ for $2 \leq n \leq b+1$. This is ordered because the numbers q_i are ordered and $\forall i, 1 \leq i \leq n-1$, $k_1 = p_1 \leq q_i = k_{i+1}$

This contradicts the assumption that a cannot b e written as a product of ordered primes. Therefore $S = \emptyset$. It follows that every $a \in P$ can be written as a product of ordered primes.

4.7 Unique Factorization Theorem

Let's prove prime factorizations are unique. In mathematical language

$$\forall n \in P, n = \prod_{i=1}^{c} p_i = \prod_{i=1}^{k} q_i \text{ where } p_i, q_i \text{ are primes.}$$

This implies $p_i = q_i$ and $c = k$, $\forall i$ where $1 \leq i \leq c$. Since all prime factorization can be ordered from smallest prime to largest, $p_i \leq p_{i+1}$ and $q_i \leq q_{i+1}$ for $1 \leq i \leq c$ and $1 \leq i \leq k$ respectively.

Also, by the previous section in this write up, we know every number has a prime factorization. $S - \{c | \exists m \in P, m = \prod_{i=1}^{c} p_i = \prod_{i=1}^{k} q_i$ where p_i, q_i are primes $, p_i \leq p_{i+1}$ and $q_i \leq q_{i+1}$ and $c \neq k$ or $p_i \neq q_i \forall i, 1 \leq i \leq n\}$

Assume, FTSOC, $S \neq \emptyset$. Since $S \subset P$, by WOP, there exists a smallest element $c \in S$.

Let's look at the base case where the prime factorization of m is just one number. Hence $m = p$ for some prime p. If $m = \prod_{i=1}^{c} p_i$ then $p | \prod_{i=1}^{c} p_i$. by substitution and reflexive property. By Prime Division Theorem, $p | p_i$ for $1 \leq i \leq n$. Since p and p_i are prime, by definition of prime $p = p_i$.

Therefore $m = \prod_{i=1}^{c} p_i = \prod_{i=1}^{c} p$ and $\prod_{i=1}^{c} p = p^c$ by power notation and exponentiation.

By reflexive property, $m|m$, and by substitution of m for p^c, we get $p^c | m$. Since $m = p$, substitution also gives us $p^c | p$. By definition of primes, p^c must be 1 or p. Since 1 is not prime, $p^c = p$. $c = 1$Therefore, there is only one prime factorization for m, and it is $m = p$. Therefore $1 \notin S$ because we have shown that any prime factorization with only one prime has a unique prime factorization is hence not in S, By NIBZO, $c > 1$.

By production notation rules: $\prod_{i=1}^{c} p_i = p_c \cdot \prod_{i=1}^{c-1} p_i$. By substitution, $p_c \cdot \prod_{i=1}^{c-1} p_i = \prod_{i=1}^{k} q_i$. By definition of divides, $p_c | \prod_{i=1}^{k} q_i$.
$\implies p_c | q_i$ for some index i where $1 \leq i \leq k$.

By the same logic, $q_k | p_i$ for some index i where $1 \leq i \leq c$.

Since $p_c | q_i \implies p_c \leq q_i$ by our lemma for some i s.t. $1 \leq i \leq k$. By same logic, since $q_k | p_i \implies q_k \leq p_i$ for some i s.t. $1 \leq i \leq c$.

Suppose FTSOC $p_c > q_k$. Since $q_k \geq q_i$, by transitive $p_c > q_i$. $p_c \leq q_i$ and $p_c > q_i$ cannot both be true at the same time. Therefore $p_c \leq q_k$.

Supposed FTSOC $p_c < q_k$. Since $q_k \geq q_i$, then $p_c < q_i$ by transitive property. This is a contradiction once again so $p_c \geq q_k$.

Since $p_c \leq q_k$ and and $p_c \geq q_k$, $p_c = q_k$. Recall $p_c \cdot \prod_{i=1}^{n-1} p_i = q_k \cdot \prod_{i=1}^{k-1} q_i$ and replace q_k with p_c to yield $p_c \cdot \prod_{i=1}^{c-1} p_i = p_c$

By Lemma 3.6,

$$\prod_{i=1}^{c-1} p_i = \prod_{i=1}^{k-1} q_i$$

By NIBZO, since $c > 1$ and $c \in P$, then $c \geq 2$. Subtracting 1 from both sides yields $c - 1 \geq 1$. By definition of min, $c - 1 \notin S$. Since $p_i = q_k$ and $c - 1 \notin S$, by definition of not is $S, c - 1 = k - 1 \implies c = k$.

Therefore, since $p_c = q_k$ and $c = k$ for all i s.t. $1 \leq i \leq c$, c is not the minimum element of S since its not in S. Hence our original assumption was wrong and $S = \emptyset$.

Product Notation

Let the product be defined recursively.

$$p_{n+1} = \prod_{i=1}^{n+1} f(i) = p_n \cdot f_n \textbf{ where } p_0 = 1$$