CELEBRATION SET

JACOB GREENE, HAOYU GUAN, JIWU JANG, AVA MARTOMA, ISABELLE YANG

1. Introduction

In this paper, we prove the Unique Factorization Theorem (UFT) for $\mathbb{Z}$, starting from the Ring Axioms, Order Axioms, and Well-Ordering Principle. We begin by looking at properties and lemmas of general rings, before moving on to integers and product notation. Then, we look at factorization until we finally prove the UFT.

2. General Rings

Axiom 1 (Ring Axioms)**.** R is said to be a ring if $\forall a,\, b,\, c \in R$:

$$\begin{aligned}
\text{Commutative:} \quad & a+b=b+a, \quad a\cdot b=b\cdot a \\
\text{Associative:} \quad & a+(b+c)=(a+b)+c, \quad a\cdot(b\cdot c)=(a\cdot b)\cdot c \\
\text{Distributive:} \quad & a\cdot(b+c)=a\cdot b+a\cdot c \\
\text{Zero:} \quad & (\exists 0\in R)\ (\forall a\in R)\ a+0=a \\
\text{Negatives:} \quad & (\forall a\in R)\ (\exists\,(-a)\in R)\ a+(-a)=0 \\
\text{One:} \quad & (\exists 1\in R) \text{ such that } (\forall a\in R)\ a\cdot 1=a
\end{aligned}$$

Lemma 2 (Uniqueness of Zero)**.** *In a ring R, let $0'\in R$ such that $(\exists a\in R)$ $a+0'=a$. Then $0'=0$.*

Proof. We have $a+0'=a$ for some $a\in R$. By commutativity, we have $0'+a=a$. By negatives, $\exists(-a)\in R$ such that $a+(-a)=0$; we add $(-a)$, giving $(0'+a)+(-a)=a+(-a)$. By associativity, $0'+(a+(-a))=a+(-a)$. By negatives, that $a+(-a)=0$; substituting, we get $0'+0=0$. But also by definition of 0, $0'+0=0'$; thus, by substitution, $0'=0$. □

Lemma 3 (Uniqueness of One)**.** *In a ring R, let $1'\in R$ such that $(\forall a\in R)$ $(a\cdot 1'=a)$. Then $1'=1$.*

Proof. Note $a\cdot 1'=a$ holds for all $a\in\mathbb{Z}$. $1\in\mathbb{Z}$, so substitute $a=1$; then $1\cdot 1'=1$. By commutativity, then $1'\cdot 1=1$; but by the one axiom, $1'\cdot 1=1'$. Thus, substituting, $1'=1$. □

Lemma 4 (Multiplication by Zero)**.** *In a ring R, $(\forall a\in R)$ $(a\cdot 0=0)$*

Proof. By the zero axiom, $a\cdot 0=a\cdot(0+0)$. By left distribution, $a\cdot(0+0)=a\cdot 0+a\cdot 0$. Then $a\cdot 0+a\cdot 0=a\cdot 0$, so by uniqueness of zero, $a\cdot 0=0$. □

Lemma 5 (Trivial Ring)**.** *$0=1$ in a ring R if and only if $R=\{0\}$.*

Proof. Suppose $0=1$ in a ring R. Then $\forall a\in R$, $a=a\cdot 1$ by the one axiom; substituting 0 for 1, $a=a\cdot 0$. Recall $a\cdot 0=0$; thus $a=0$. Thus, $a\in R \implies a=0$, and by the zero axiom we know $0\in R$, so we must have $R=\{0\}$. For the other direction, suppose $R=\{0\}$. By definition of a ring, $\exists 1\in R$; thus $1=0$. □

Lemma 6 (Additive Cancellation)**.** *In a ring R, $(\forall a,\, b,\, b'\in R)$ $a+b=a+b' \implies b=b'$*

Date: July 2, 2023.

Proof. Let $a+b=a+b'$. Adding $(-a)$ to both sides, $(a+b)+(-a)=(a+b')+(-a)$. By commutativity, $(b+a)+(-a)=(b'+a)+(-a)$. By associativity, $b+(a+(-a))=b'+(a+(-a))$. By the definition of negatives, $b+0=b'+0$; thus by the zero axiom, $b=b'$. □

Lemma 7 (Uniqueness of Negatives)**.** In a ring R, $(\forall a,\, x \in R)\;\; a+x=0 \implies x=-a$.

Proof. Let $a, x \in R$ such that $a+x=0$. Adding $(-a)$ to both sides, $(a+x)+(-a)=0+(-a)$. By commutativity, $(x+a)+(-a)=(-a)+0$. By associativity, $x+(a+(-a))=(-a)+0$. By definition of negatives, then $x+0=(-a)+0$. Thus, by the zero axiom, $x=-a$. □

Lemma 8 (Properties of Negatives)**.** $\forall a, b \in R$:

(i) $-(-a)=a$
(ii) $-(ab)=(-a)b$
(iii) $(-a)(-b)=ab$
(iv) $-a=(-1)\cdot a$
(v) $-(a+b)=(-a)+(-b)$
(vi) $-0=0$
(vii) $(-1)\cdot(-1)=1$

Proof of (i). By definition of $(-a)$, $a+(-a)=0$. Then by commutativity $(-a)+a=0$. Thus by uniqueness of negatives, $a=-(-a)$. □

Proof of (ii). By definition of $(-a)$, $a+(-a)=0$. Then, multiplying by b, $b(a+(-a))=b\cdot 0$. Thus $ba+b(-a)=b\cdot 0$. Then, by commutativity, $ab+(-a)b=b\cdot 0$. Recall $b\cdot 0=0$; thus $ab+(-a)b=0$. Thus by uniqueness of negatives $(-a)b=-(ab)$. □

Proof of (iii). Note $-(ab)=(-a)b$ by section (ii) Then by commutativity $-(ab)=b(-a)$. Applying section (ii) again, $-(-(ab))=(-b)(-a)$. By section (i), we get $ab=(-b)(-a)$, so by commutativity $(-a)(-b)=ab$. □

Proof of (iv). Note $(-a)=(-(a\cdot 1))$ by the one axiom. By commutativity, then $(-a)=(-(1\cdot a))$. Thus by section (ii), $(-a)=(-1)\cdot a$. □

Proof of (v). By section (iv), $-(a+b)=(-1)\cdot(a+b)$. Moreover, by left distribution, we have $-(a+b)=((-1)\cdot a)+((-1)\cdot b)$. Then, by section (iv), we have $-(a+b)=(-a)+(-b)$, and we are done. □

Proof of (vi). Note that by the zero axiom, we have $0+0=0$. Thus, by uniqueness of negatives, we have $-0=0$. □

Proof of (vii). By section (iii), we know that $\forall a, b \in R$, $(-a)(-b)=ab$. Now, we can specify a and b such that $a=b=1$. In this case, $(-1)\cdot(-1)=1\cdot 1$. Moreover, by the one axiom, $1\cdot 1=1$. Thus, $(-1)\cdot(-1)=1$, hence we are done. □

Definition 9 (Subtraction)**.** Define $a-b$ to be a solution y to the equation $a=b+y$.

Lemma 10 (Existence, Uniqueness, and Properties of Subtraction)**.** In any ring R, $\forall a, b \in R$:

(i) $(\exists (a-b) \in R)\;\; a=b+(a-b)$ (Existence of Subtraction)
(ii) $(\forall y \in R)\;\; a=b+y \implies y=a-b$ (Uniqueness of Subtraction)
(iii) $a-b=(-b)+a=a+(-b)$. In particular, $a-0=a$.
(iv) $-(a-b)=b-a$

(v) $a - b = 0 \iff a = b$

Proof of (i). Consider $(-b) + a$. Note $b + ((-b) + a) = (b + (-b)) + a$, by associativity. Then, by definition of $(-b)$, $b + ((-b) + a) = 0 + a$. By commutativity, $b + ((-b) + a) = a + 0$. By the zero axiom, we have $a = b + ((-b) + a)$. Hence, $(-b) + a$ is a solution to the equation $a = b + y$. Thus, at least one value of $a - b$ exists. □

Proof of (ii). Let $y \in \mathbb{Z}$ such that $a = b + y$. Note by definition of $a - b$, $a = b + (a - b)$. Thus by transitivity $b + y = b + (a - b)$; thus adding $(-b)$ to both sides, $y = a - b$. That is, there exists exactly one solution to $a = b + y$, equal to $a - b$. □

Proof of (iii). Note, as in section (i), $(-b) + a$ is a solution to $a = b + y$. Thus by part (ii), $(-b) + a = a - b$. Then, by commutativity, $a - b = (-b) + a = a + (-b)$.

In particular, letting $b = 0$, $a - 0 = a + (-0) = a + 0 = a$. □

Proof of (iv). By definition, $a = b + (a - b)$. Adding $-(a - b)$ to both sides, then $a + (-(a - b)) = (b + (a - b)) + (-(a - b))$. By associativity, $a + (-(a - b)) = b + ((a - b) + (-(a - b)))$. By definition of $-(a - b)$, $a + (-(a - b)) = b + 0$. By the zero axiom, $a + (-(a - b)) = b$. Thus, by uniqueness of subtraction, $-(a - b) = (b - a)$. □

Proof of (v). Let $a - b = 0$. Then by definition of subtraction $a = b + 0$; thus by the zero axiom, $a = b$. This proves one direction of conditionality.

Now, let $a = b$. Then by the zero axiom, $a = b + 0$. Thus by uniqueness of subtraction, $a - b = 0$. Thus $a - b = 0 \iff a = b$. □

Definition 11 (Divisibility)**.** $a \mid b$ if and only if $(\exists d \in \mathbb{Z})$ such that $a \cdot d = b$.

Lemma 12 (Properties of Divisibility)**.** In a ring R, $\forall a, b, c, x, y \in R$:

(i) $a \mid a$
(ii) $a \mid b \wedge a \mid c \implies a \mid (b + c)$
(iii) $a \mid b \wedge b \mid c \implies a \mid c$
(iv) $a \mid b \implies a \mid bc$
(v) $a \mid b \wedge a \mid c \implies a \mid (bx + cy)$

Proof of (i). Let $a \in R$. Then by the one axiom, $a \cdot 1 = a$ (and $1 \in R$). Thus by definition of divisibility, $a \mid a$. □

Proof of (ii). Let $a \mid b$ and $a \mid c$. Then, by definition of divisibility, $(\exists m, n \in R)\ a \cdot m = b$, $a \cdot n = c$. Adding these equations, $a \cdot m + a \cdot n = b + c$. By left distribution, $a \cdot (m + n) = b + c$. By additive closure, $(m + n) \in R$. Thus, by definition of divisibility, $a \mid (b + c)$. □

Proof of (iii). Let $a \mid b$ and $b \mid c$. By the definition of divisibility, $(\exists k, l \in R)\ a \cdot k = b$, $b \cdot l = c$. After combining two equations, we have $(a \cdot k) \cdot l = c$. By associativity, $a \cdot (k \cdot l) = c$. By multiplicative closure, $k \cdot l \in R$. By definition of divisibility, $a \mid c$. □

Proof of (iv). Let $a \mid b$. Then for some $k \in R$, $a \cdot k = b$. Then $(a \cdot k) \cdot c = b \cdot c$; thus by associativity $a \cdot (k \cdot c) = b \cdot fc$. Thus by definition of divisibility $a \mid bc$. □

Proof of (vi). Let $a \mid b, a \mid c$. Then $a \mid bx, a \mid cy$ by section (iv); then $a \mid (bx + cy)$ by section (iii). □

3. Integers

Axiom 13 (Order Axioms)**.** $\mathbb{Z}$ is a ring containing a non-empty subset $\mathbb{Z}^+ \subseteq \mathbb{Z}$ with the following properties:

$$\begin{aligned}
\text{Additive Closure:}\quad & (\forall a, b \in \mathbb{Z}^+)\ a + b \in \mathbb{Z}^+ \\
\text{Multiplicative Closure:}\quad & (\forall a, b \in \mathbb{Z}^+)\ a \cdot b \in \mathbb{Z}^+ \\
\text{Trichotomy:}\quad & (\forall a \in \mathbb{Z}^+) \text{ exactly one of the following holds:} \\
& \qquad a \in \mathbb{Z}^+ \ \vee\ a = 0 \ \vee\ (-a) \in \mathbb{Z}^+
\end{aligned}$$

Definition 14 (Inequalities)**.** The relations $<$, $>$, $\leq$, $\geq$ are defined on $\mathbb{Z}$ as follows:

$$\begin{aligned}
a < b\text{:}\quad & (\exists c \in \mathbb{Z}^+)\ a + c = b \\
a \leq b\text{:}\quad & (a < b) \vee (a = b) \\
a > b\text{:}\quad & b < a \\
a \geq b\text{:}\quad & b \leq a
\end{aligned}$$

Axiom 15 (The Well-Ordering Principle (WOP))**.** For any set $S \subseteq \mathbb{Z}^+$ with $S \neq \emptyset$, $(\exists n \in S)$ such that $(\forall s \in S)\ n \leq s$. The number n is denoted $\min\{S\}$.

Definition 16 (Absolute Value)**.** $\forall a \in \mathbb{Z}$: if $(-a) \in \mathbb{Z}^+$, $|a| := -a$; else, $|a| := a$.

Lemma 17 ($\mathbb{Z}$ is nontrivial)**.** $1 \neq 0$ in $\mathbb{Z}$. Furthermore, $1 \in \mathbb{Z}^+$.

Proof. By Trichotomy, taking $a = 0$, observe that $0 \notin \mathbb{Z}^+$. However, $\mathbb{Z}^+ \subseteq \mathbb{Z}$ is non-empty. Thus $(\exists a \in \mathbb{Z}) a \neq 0$. Thus $\mathbb{Z}$ is not the trivial ring, so $1 \neq 0$ in $\mathbb{Z}$.

Now consider Trichotomy, taking $a = 1$. As $1 \neq 0$ in $\mathbb{Z}$, we have exactly one of $1 \in \mathbb{Z}^+$ or $(-1) \in \mathbb{Z}^+$. Assume for the sake of contradiction $(-1) \in \mathbb{Z}^+$, and thus $1 \notin \mathbb{Z}^+$. Then, as $\mathbb{Z}^+$ is closed under multiplication, $(-1) \cdot (-1) = 1 \in \mathbb{Z}^+$; contradiction. Thus $(-1) \notin \mathbb{Z}^+$, so $1 \in \mathbb{Z}^+$. □

Lemma 18 (Properties of Inequalities)**.** $\forall a, b, c \in \mathbb{Z}$:

(i) $a - b \in \mathbb{Z}^+ \iff a > b$
(ii) $a \in \mathbb{Z}^+ \iff a > 0$
(iii) $a < b \iff (-a) > (-b)$ (Similarly): $a > b \iff (-a) < (-b)$
(iv) $a < b \iff a + c < b + c$
(v) $a < b \ \wedge\ b < c \implies a < c$
(vi) $a < b \ \wedge\ c < d \implies a + c < b + d$
(vii) Exactly one of $a < b$, $a = b$, and $a > b$ holds. (Trichotomy for Inequalities)
(viii) $a \leq b \ \wedge\ b \leq a \implies a = b$ (Antisymmetry)
(ix) If $c \in \mathbb{Z}^+$, then $a < b \implies a \cdot c < b \cdot c$

Proof of (i). Let $a, b \in \mathbb{Z}$ such that $a - b \in \mathbb{Z}^+$. Then by definition of subtraction, we have some $c = a - b \in \mathbb{Z}^+$ where $a = b + c$; thus by definition of inequalities, $b < a$, so $a > b$. This proves one direction of conditionality.

Let $a, b \in \mathbb{Z}$ such that $a > b$. Then by definition of inequalities, $\exists c \in \mathbb{Z}^+$ such that $a = b + c$. By uniqueness of subtraction, $c = a - b$; thus, $(a - b) \in \mathbb{Z}^+$. This concludes both directions of conditionality; thus, $a - b \in \mathbb{Z}^+ \iff a > b$. □

Proof of (ii). Let $a \in \mathbb{Z}^+$. Then by properties of subtraction section (iii), $a - 0 \in \mathbb{Z}^+$. Thus by section (i), $a > 0$. □

Proof of (iii). Let $a < b$. Then, $(\exists c \in \mathbb{Z}^+)\ \ a+c = b$. By uniqueness of negatives, $-(a+c) = -b$. By properties of negatives section (v), $(-a)+(-c) = -b$. Adding c to both sides, then $((-a)+(-c))+c = -b+c$. By associativity and commutativity, this becomes $(-a)+(c+(-c)) = -b+c$. By negatives and the zero axiom, thus, $-a = -b+c$. Then, as $c \in \mathbb{Z}^+$, by definition of inequalities we have $-b < -a$ and thus $-a > -b$. This proves one direction of conditionality.

Now, let $(-a) > (-b)$; then $(-b) < (-a)$, and so similarly to above $-(-b) > -(-a)$. Then by properties of negatives section (i), $b > a$, so by definition of inequalities, $a < b$. Thus, $a < b \iff (-a) > (-b)$. Substituting b for a, we get $b < a \iff (-b) > (-a)$. By definition of inequalities, we can rearrange to get $a > b \iff (-a) < (-b)$. □

Proof of (iv). Let $a < b$. Then $(\exists x \in \mathbb{Z}^+)\ \ a+x = b$. Adding c to both sides, $(a+x)+c = b+c$. By commutativity and associativity, then $(a+c)+x = b+c$. $c \in \mathbb{Z}^+$, so by definition of inequalities, $a+c < b+c$. This proves one direction of conditionality.

Now, let $a+c < b+c$. Then, similarly to above, $(a+c)+(-c) < (b+c)+(-c)$; by associativity, $a+(c+(-c)) < b+(c+(-c))$; thus $a < b$. Thus, $a < b \iff a+c < b+c$. □

Proof of (v). By definition of inequalities, $a < b$ means that $\exists p \in \mathbb{Z}^+$ such that $a+p = b$. Similarly, $b < c$ means that $\exists q \in \mathbb{Z}^+$ such that $b+q = c$. By combining both equations, $a+p+q = c$. Then, by associativity, $a+(p+q) = c$. By additive closure, $p+q \in \mathbb{Z}^+$. Again, by the definition of inequalities, $a < c$. □

Proof of (vi). By definition of inequalities, $a < b$ means that $\exists p \in \mathbb{Z}^+$ such that $a+p = b$. Similarly, $c < d$ means that $\exists q \in \mathbb{Z}^+$ such that $c+q = d$. By combining both equations, $a+c+p+q = b+d$. Then, by associativity, $a+c+(p+q) = b+d$. By additive closure, $p+q \in \mathbb{Z}^+$. Again, by the definition of inequalities, $a+c < b+d$. □

Proof of (vii). Let $a, b \in \mathbb{Z}$ be arbitrary. By Trichotomy, exactly one of $(a-b) \in \mathbb{Z}^+$, $a-b = 0$, or $-(a-b) \in \mathbb{Z}^+$. In the first case, by section (i), $a > b$; in the second case, $a = b$ by properties of subtraction section (v). In the third case, by properties of subtraction section (iv), $-(a-b) = (b-a) \in \mathbb{Z}^+$; thus, again by section (i), $b > a$, so $a < b$. Again, exactly one of the three cases holds; that is, exactly one of $a > b$, $a = b$, or $a < b$ holds. □

Proof of (viii). By definition of inequalities, $a \leq b$ is $a < b$ or $a = b$, and $a \geq b$ is $a > b$ or $a = b$. If $a < b$, then $a \ngeq b$; if $a > b$, then $a \nleq b$. By Trichotomy of inequalities, $a = b$. □

Proof of (ix). Let $c \in \mathbb{Z}^+$ and a, $b \in \mathbb{Z}$ such that $a < b$. Then, $(\exists x \in \mathbb{Z}^+)\ \ a+x = b$. Multiplying c to both sides, $(a+x)\cdot c = b \cdot c$. By commutativity, associativity, and right distribution, we have $a \cdot c + x \cdot c = b \cdot c$. We have c, $x \in \mathbb{Z}^+$, so by multiplicative closure, $x \cdot c \in \mathbb{Z}^+$. Then, by definition of inequalities, $a \cdot c < b \cdot c$. □

Lemma 19. $\forall a$, b, $c \in \mathbb{Z}$, if a, $c \in \mathbb{Z}^+$ and $ab = c$, then $b \in \mathbb{Z}^+$.

Proof. We know a,$c \in \mathbb{Z}^+$ and $ab = c$. Assume for the sake of contradiction $b \notin \mathbb{Z}^+$. Thus, either $b = 0$ or b is negative. If $b = 0$, we can substitute b in $ab = c$, and we get $a \cdot 0 = c$. By multiplication by zero, we know that $a \cdot 0 = 0$. Thus, $c = 0$. However, this means that $c \notin \mathbb{Z}^+$. Thus our first case is disproven and $b \neq 0$. In our second case b is negative. Thus, $b = -x$, where $x \in \mathbb{Z}^+$. So, $ab = a(-x) = c$. By associativity, $(-x)a = c$. By properties of negatives section (ii),$-(xa) = c$. Thus, $-(xa)$ is some number where $xa \in \mathbb{Z}^+$. Thus, $-xa \notin \mathbb{Z}^+$ and $c \notin \mathbb{Z}^+$. However, this is a contradiction, so the assumption made in our second case is false. Therefore, $b \in \mathbb{Z}^+$. □

Definition 20 (Nonnegative Integers)**.** $\mathbb{Z}_{\geq 0} = \{x \in \mathbb{Z} \mid x \geq 0\}$. This set is referred to as the *nonnegative* integers.

Lemma 21 (Generalized WOP)**.** WOP holds for bounded sets of integers in general, beyond just $\mathbb{Z}^+$. In particular:

(i) Let $S \subseteq \mathbb{Z}$ and $S \neq \emptyset$ where $(\exists x \in \mathbb{Z})$ such that $(\forall s \in S)$ $(x \leq s)$. Thus, $(\exists n \in S)$ such that $(\forall s \in S)$ $(n \leq s)$. That is, any set of integers which is bounded below has a minimum.
(ii) Let $S \subseteq \mathbb{Z}$ and $S \neq \emptyset$ where $(\exists x \in \mathbb{Z})$ such that $(\forall s \in S)$ $(x \geq s)$. Thus, $(\exists n \in S)$ such that $(\forall s \in S)$ $(n \geq s)$. That is, any set of integers which is bounded above has a maximum.
(iii) In particular, if $S \subseteq \mathbb{Z}_{\geq 0}$ and $S \neq \emptyset$, then S has a minimum element.
(iv) Furthermore, if S contains a minimum, then that minimum is unique. (Similarly, if S contains a maximum, then that maximum is unique)

Proof of (i). Let $S \subseteq \mathbb{Z}$ and $S \neq \emptyset$ such that $\exists x \in \mathbb{Z}$ where $(\forall s \in S)$ $x \leq s$. Construct $S' = \{(s - x) + 1 \mid s \in S\}$. As $x \leq s$, we have $x - x \leq s - x$, so $0 \leq s - x$. Thus, $1 \leq (s - x) + 1$. As $1 \in \mathbb{Z}^+$ and $0 < 1$, by transitivity, we have $0 < (s - x) + 1$. Hence, $(\forall s \in S)$ $(s - x) + 1 \in \mathbb{Z}^+$, so $S' \subseteq \mathbb{Z}^+$. As $S \neq \emptyset$, we have $S' \neq \emptyset$, since any given element of S has an image in S'. By WOP, S' contains a minimum element $n' = (n - x) + 1$ for some $n \in S$ such that $\forall s' = (s - x) + 1 \in S'$, where $n' \leq s'$. Thus, $(n - x) + 1 \leq (s - x) + 1$, which implies $(n - x) \leq (s - x)$, so $n + (-x) \leq s + (-x)$ and $n \leq s$. That is, $n \in S$, and $(\forall s \in S)$ $n \leq s$. Hence, S has a minimum element. □

Proof of (ii). Let $S \subseteq \mathbb{Z}$ and $S \neq \emptyset$ such that $\exists x \in \mathbb{Z}$ where $(\forall s \in S)$ $x \geq s$. Construct $S' = \{-s \mid s \in S\}$. Then $(\forall (-s) \in S')$ $(-x) \leq (-s)$. Thus S' has a minimum element $(-n)$ for some $n \in S$ such that $(\forall s \in S)$ $(-n) \leq (-s)$. Thus, $(\forall s \in S)$ $n \geq s$, which implies that S has a maximum element n. □

Proof of (iii). Let $S \subseteq \mathbb{Z}_{\geq 0}$. Then $\forall x \in S$, we have $x \in \mathbb{Z}_{\geq 0}$; in particular, $x \geq 0$. Thus, S is bounded below, and by section (i), $\exists n \in S$ such that $(\forall s \in S)$ $n \leq s$. □

Proof of (iv). Let $S \subseteq \mathbb{Z}$ contain a minimum element $s \in S$ such that $(\forall x \in S)$ $s \leq x$. Let s, s' be any two such minima. Then $s \leq s'$, and $s' \leq s$. Thus $s = s'$ - that is, the minimum element is unique. Similarly, the maximum of a set is unique. □

Lemma 22 ($\mathbb{Z}$ is an integral domain)**.** $(\forall a, b \in \mathbb{R})$ $ab = 0 \implies a = 0 \lor b = 0$.

Proof. We prove the contrapositive. Let $a \neq 0$ and $b \neq 0$. By Trichotomy $a \in \mathbb{Z}^+$ or $(-a) \in \mathbb{Z}^+$ and $b \in \mathbb{Z}^+$ or $(-b) \in \mathbb{Z}^+$. There are four cases:

Case 1: $a, b \in \mathbb{Z}^+$

Then $ab \in \mathbb{Z}^+$; thus by Trichotomy $ab \neq 0$.

Case 2: $(-a), b \in \mathbb{Z}^+$

Then $-(ab) = (-a)b \in \mathbb{Z}^+$; thus by Trichotomy $ab \neq 0$.

Case 3: $a, (-b) \in \mathbb{Z}^+$

Then $-(ab) = -(ba) = (-b)a \in \mathbb{Z}^+$; thus by Trichotomy $ab \neq 0$.

Case 4: $(-a), (-b) \in (Z)^+$

Then $ab = (-a)(-b) \in \mathbb{Z}^+$; thus by Trichotomy $ab \neq 0$.

□

Lemma 23 (Multiplicative Cancellation in $\mathbb{Z}$)**.** $(\forall a, b \in \mathbb{Z})\ a \neq 0 \wedge ab = ab' \implies b = b'$

Proof. We know that $ab = ab'$. By adding the $-ab'$ to both sides, we get $ab + (-ab') = ab' + (-ab')$. By negatives, $ab + (-ab') = 0$. By property of negatives, $ab + (-ab') = ab + (-1)(ab') = 0$. Using associativity, we get $ab + a((-1)b') = 0$. By right distribution, $a(b + (-1)b') = 0$. By property of negatives, $a(b + (-1)b') = a(b + (-b')) = 0$. Then, as $\mathbb{Z}$ is an integral domain, either $a = 0$ or $b + (-b') = 0$. But $a \neq 0$, so $(b + (-b') = 0$. By addition, $b + (-b') + b' = 0 + b'$. By associativity, $b + b' + (-b') = b' + 0$. By negatives, $b = b' + 0$. By the zero axiom, $b = b'$. □

Lemma 24 (NIBZO: No Integer Between Zero and One)**.** $(\nexists n \in \mathbb{Z})\ 0 < n < 1$.

Proof. By the order axioms $\mathbb{Z}^+$ is nonempty, and $\mathbb{Z}^+ \subseteq \mathbb{Z}^+$. Thus, by WOP, $\mathbb{Z}^+$ has a minimum element o such that $(\forall p \in \mathbb{Z}^+)\ o \leq p$. Then, as $1 \in \mathbb{Z}^+$, $o \leq 1$.

As $o \in \mathbb{Z}^+$, we can multiply, which gives $o \cdot o \leq o$. But by multiplicative closure of $\mathbb{Z}^+$, $o \cdot o \in \mathbb{Z}^+$; thus, by the minimality of o, $o \leq o \cdot o$.

Hence, $o = o \cdot o$. That is, $o \cdot 1 = o \cdot o$. As $o \in \mathbb{Z}^+$, by Trichotomy, $o \neq 0$; thus we may cancel, giving $o = 1$. Therefore, $(\forall a \in \mathbb{Z}^+)\ 1 \leq a$.

Furthermore, we know that $a \in \mathbb{Z}^+ \iff a > 0$. Thus, $(\forall a \in \mathbb{Z})\ a > 0 \implies a \geq 1$, so by Trichotomy $a \not< 1$. Thus, $(\nexists a \in \mathbb{Z})\ 0 < a < 1$. □

Lemma 25. If $a, b \in \mathbb{Z}^+$ and $a \mid b$, then $a \leq b$.

Proof. Let $a, b \in \mathbb{Z}^+$, $a \mid b$. By definition of divisibility, $\exists k \in \mathbb{Z}$ such that $a \cdot k = b$. If $k = 0$, by multiplication by zero, $a \cdot 0 = 0$; if $k < 0$, by properties of negatives, $a \cdot k < 0$. Thus, $k > 0$. By NIBZO, there is no integer between zero and one, so $k \geq 1$. Hence $a \cdot k \geq a \cdot 1$. But then, $b \geq a$, or equivalently, $a \leq b$. □

4. Product Notation

Definition 26 (Product Notation)**.** Define for a, b, $\{p_i\}_{i=a}^{b} \in \mathbb{Z}$:

$$\prod_{i=a}^{b} p_i = \begin{cases} 1 & \text{if } a > b \\ \left(\prod_{i=a}^{b-1} p_i\right) \cdot p_b & \text{if } a \leq b \end{cases}$$

Lemma 27 (Splitting Product)**.** For $\{p_i\}_{i=a}^{c}$, $a \leq b \leq c$, we have $\left(\prod_{i=a}^{b} p_i\right)\left(\prod_{i=b+1}^{c} p_i\right) = \prod_{i=a}^{c} p_i$.

Proof. Fix a, b, $\{p_i\}$ such that $a \leq b$. Let $S = \left\{ c \in \mathbb{Z}^+ \,\middle|\, c \geq b,\ \left(\prod_{i=a}^{b} p_i\right)\left(\prod_{i=b+1}^{c} p_i\right) \neq \prod_{i=a}^{c} p_i \right\}$. Suppose for the sake of contradiction $S \neq \emptyset$. Then, by WOP, $(\exists c \in S)$ s.t. $(\forall s \in S)\ c \leq s$. If $c = b$, then $c < b+1$, by definition of inequalities, as $1 \in \mathbb{Z}^+$. Thus $\prod_{i=b+1}^{c} p_i = 1$, so $\prod_{i=a}^{b} p_i \cdot 1 = \prod_{i=a}^{b} p_i = \prod_{i=1}^{c} p_i$. Therefore we cannot have $c \neq b$.

So $c > b$. Then by NIBZO $c \geq b + 1$; thus $c - 1 \geq b$. But we know $c - 1 \notin S$, so we must have $\left(\prod_{i=a}^{b} p_i\right)\left(\prod_{i=b+1}^{c-1} p_i\right) = \prod_{i=a}^{c-1} p_i$. Multiplying by p_c, $\left(\prod_{i=a}^{b} p_i\right)\left(\prod_{i=b+1}^{c-1} p_i\right) \cdot p_c = \left(\prod_{i=a}^{c-1} p_i\right) \cdot p_c$; but this simplifies to $\left(\prod_{i=a}^{b} p_i\right)\left(\prod_{i=b+1}^{c} p_i\right) = \prod_{i=a}^{c} p_i$. Therefore $c \notin S$; contradiction. Thus, $S = \emptyset$; that is, for all $c \in \mathbb{Z}^+$ such that $c \geq b$, $\left(\prod_{i=a}^{b} p_i\right)\left(\prod_{i=b+1}^{c} p_i\right) = \prod_{i=a}^{c} p_i$. □

Definition 28. For $a \in \mathbb{Z}$ and $b \in \mathbb{Z}_{\geq 0}$, define $a^b = \prod_{i=1}^{b} a$. Observe that this is equivalent to: $a^0 = 1$ and $a^b = a \cdot a^{b-1}$ for $b \geq 1$.

5. Factorization

Definition 29 (Prime)**.** For $p \in \mathbb{Z}^+$, we say that p is a *prime* if and only if $p \nmid 1$ and $\gcd(n, p) = 1$ $\forall n \in \mathbb{Z}^+$ where $n < p$.

Lemma 30 (Euclidean Division)**.** Let $a, b \in \mathbb{Z}$ and $b > 0$. Then, $\exists q, r \in \mathbb{Z}$ such that $0 \leq r < b$ and $a = bq + r$.

Proof. Let $a, b \in \mathbb{Z}, b > 0$. By Trichotomy, there are three cases:

Case 1: $a \in \mathbb{Z}^+$.

Let $S = \{n \in \mathbb{Z}_{\geq 0} \mid (\exists q \in \mathbb{Z})\ n = a - bq\}$. Taking $q = 0$, note $a - b \cdot 0 = a - 0 = a \in S$; thus $S \neq \emptyset$. Then, by WOP (for $\mathbb{Z}_{\geq 0}$), $(\exists r \in S)$ such that $(\forall s \in S)\ r \leq s$.

Assume for the sake of contradiction $r \geq b$. Then $r - b \in \mathbb{Z}_{\geq 0}$. Furthermore, $r - b = a - bq - b = a - b(q+1)$. As $q + 1 \in \mathbb{Z}$, thus, $r - b \in S$. But $b \in \mathbb{Z}^+$, so $r - b < r$; thus r cannot be the minimum element of S; contradiction. Thus, $r < b$. As $a - bq = r$, by definition of subtraction, $a = bq + r$.

Thus, $\exists q, r \in \mathbb{Z}$ such that $0 \leq r < b$ and $a = bq + r$.

Case 2: $a = 0$.

Take $q = r = 0$; then $bq + r = b \cdot 0 + 0 = 0 = a$. Also note $0 \leq r < b$. Thus here we can find q, r.

Case 3: $(-a) \in \mathbb{Z}^+$.

Then, $\exists q', r'$ such that $(-a) = bq' + r'$ and $0 \leq r' < b$. Hence, $-a = bq' + r' < bq' + b = b(q' + 1)$. Thus, $a + (-a) < a + b(q' + 1)$. This implies $a + b(q' + 1) > 0$; thus $a + b(q' + 1) \in \mathbb{Z}^+$.

Let $S = \{n \in \mathbb{Z}_{\geq 0} \mid (\exists q \in \mathbb{Z}\ n = a - bq\}$. Recall that $a + b(q' + 1) \in \mathbb{Z}^+$. Moreover, note that $a + b(q' + 1) = a + (-(-(b(q' + 1)))) = a - (-(b(q' + 1)))$. Thus, $a - (-(b(q' + 1))) \in S$, so $S \neq \emptyset$. Hence, S has a minimum element r. Similar to above, $0 \leq r < b$; thus $a = bq + r$ for $0 \leq r < b$.

□

Definition 31 (Greatest Common Divisor (GCD))**.** For $a, b \in \mathbb{Z}$ such that either $a \neq 0$ or $b \neq 0$, define

$$\gcd(a, b) := \max\{d \in \mathbb{Z} : d \mid a \ \wedge \ d \mid b\}$$

Lemma 32 (Existence and Uniqueness of GCD)**.** Let $a, b \in \mathbb{Z}$ such that $a \neq 0 \vee b \neq 0$. Then, $\exists! \gcd(a, b) \in \mathbb{Z}$. Moreover, $\gcd(a, b) \in \mathbb{Z}^+$.

Proof. Let $a, b \in \mathbb{Z}$ such that either $a \neq 0$ or $b \neq 0$. Without loss of generality, suppose $a \neq 0$.

Let $D = \{d \in \mathbb{Z} \mid d \mid a \wedge d \mid b\}$. Then, $(\forall d \in D)\ d \leq |a|$. Hence, D is bounded above in $\mathbb{Z}$. Thus, by Generalized WOP, D has a unique maximum, so gcd is defined.

For brevity, let $d = \gcd(a, b)$. Suppose for the sake of contradiction $d = 0$ or $(-d) \in \mathbb{Z}^+$.

If $d = 0$, then $\exists k \in \mathbb{Z}$ such that $a = dk = k \cdot 0$, which implies $a = 0$. Similarly, $b = 0$, which is a contradiction to the initial assumption.

If $(-d) \in \mathbb{Z}^+$, then $d < (-d)$, since $(-d) + (-d) \in \mathbb{Z}^+$ and thus $(-d) - d \in \mathbb{Z}^+$, which implies $d < (-d)$. Thus, we may take $(-d)$, which also satisfies $(-d) \mid a$ and $(-d) \mid b$, yet $d < (-d)$, which contradicts the maximality of d.

Hence, $d \in \mathbb{Z}^+$. □

Lemma 33 (Bézout's Lemma)**.** For all $a, b \in \mathbb{Z}$ where $a \neq 0$, $\exists x, y \in \mathbb{Z}$ such that $ax + by = \gcd(a, b)$. In particular, $\gcd(a, b) = \min\{d \in \mathbb{Z}^+ \mid (\exists x, y \in \mathbb{Z})\ d = ax + by\}$.

Proof. Fix $a, b \in \mathbb{Z}$, $a \neq 0$. Let $S = \{d \in \mathbb{Z}^+ \mid (\exists x, y \in \mathbb{Z})\ d = ax + by\}$.

Claim. $S \neq \emptyset$.

Proof. By Trichotomy, since $a \neq 0$, either $a \in \mathbb{Z}^+$ or $(-a) \in \mathbb{Z}^+$.

If $a \in \mathbb{Z}^+$, we take $x = 1, y = 0$. Thus,

$$\begin{aligned} ax + by &= a \cdot 1 + b \cdot 0 \\ &= a + 0 = a \in \mathbb{Z}^+ \end{aligned}$$

which implies $S \neq \emptyset$.

If $(-a) \in \mathbb{Z}^+$, we take $x = -1, y = 0$. Thus,

$$\begin{aligned} ax + by &= a \cdot (-1) + b \cdot 0 \\ &= (-1) \cdot a + b \cdot 0 \\ &= (-a) + b \cdot 0 \\ &= (-a) + 0 = (-a) \in \mathbb{Z}^+ \end{aligned}$$

Hence, $S \neq \emptyset$ for this case as well. ■

Now, by WOP, $(\exists d \in S)$ such that $(\forall s \in S)\ d \leq s$. We have $d = ax + by$ for some $x, y \in \mathbb{Z}$.

By definition of GCD, we have $\gcd(a, b) \mid a$ and $\gcd(a, b) \mid b$. Then, as $d = ax + by$ for $x, y \in \mathbb{Z}$, by properties of divisibility part (v), $\gcd(a, b) \mid d$.

By Euclidean Division, $\exists q, r \in \mathbb{Z}, 0 \leq r < d$ such that $a = dq + r$. Assume for the sake of contradiction $r > 0$. Then:

$$\begin{aligned} r &= a - dq \\ &= a - (ax + by)q \\ &= a - a(xq) + b(yq) \\ &= a(1 - xq) + b(yq) \in S \end{aligned}$$

That is, $r \in S$. Hence $d \leq r$, as d is the minimum element of S. But $r < d$; contradiction. Thus $r \not> 0$, so $r = 0$.

Therefore, $a = dq + 0 = dq$ by the zero axiom. By definition of divisibility, $d \mid a$. Similarly, $d \mid b$. Moreover, by definition of GCD, we have $d \leq \gcd(a, b)$. But recall that $\gcd(a, b) \mid d$. Thus, $\gcd(a, b) \leq d$, which implies $d = \gcd(a, b)$.

Thus, given $a, b \in \mathbb{Z}$ with $a \neq 0$, then $\gcd(a, b) = \min\{d \in \mathbb{Z}^+ \mid (\exists x, y \in \mathbb{Z})\ d = ax + by\}$. □

Lemma 34 (Euclid's Lemma)**.** Let p be a prime and $a, b \in \mathbb{Z}$. Then, $p \mid ab$ implies $p \mid a$ or $p \mid b$.

Proof. Let $p \mid ab$ and $p \nmid a$. Then, it suffices to show that $p \mid b$. Because $p \nmid a$, we have that $\gcd(p, a) = 1$. Hence, by Bézout's Lemma, $\exists x, y \in \mathbb{Z}$ such that $ax + py = 1$. But then, since $p \mid ab$, $\exists k \in \mathbb{Z}$ such that $ab = pk$. Observe that $abx + pby = b$, so $pkx + pby = b$. Then, $p(kx + by) = b$, so $p \mid b$, and we are done. □

Lemma 35 (Extended Euclid's Lemma)**.** Let p be a prime. If $p \mid \displaystyle\prod_{i=1}^{k} a_i$, then at least one of $p \mid a_i$ holds, for $i \in \{1, 2, \ldots, k\}$.

Proof. Let $p \mid a_1 \cdot \displaystyle\prod_{i=2}^{k} a_i$ and $p \nmid a_1$. By Euclid's Lemma, then $p \mid \prod_{i=2}^{k} a_i$. Now, let $p \mid a_2 \cdot \prod_{i=3}^{k} a_i$ and $p \nmid a_2$. Again, by Euclid's Lemma, $p \mid \displaystyle\prod_{i=3}^{k} a_i$. Repeat this process until we find a value $i \in \{1, 2, \ldots, k\}$ such that $p \mid a_i$. There must be at least one of $p \mid a_i$ holds by Euclid's Lemma. □

Definition 36 (Prime Factor)**.** Let $a \in \mathbb{Z}$ and p be a prime number. We say that p is a *prime factor* of a if and only if $p \mid a$.

Definition 37 (Prime Factorization)**.** A *prime factorization* of n is an expression of the form $n = \displaystyle\prod_{i=1}^{a} p_i$, where all of the p_i are prime.

Definition 38. Every positive integer $n > 1$ that is not prime is said to be *composite.*

Lemma 39 (Composite Numbers)**.** A number is composite if and only if it can be represented as $n = ab$, where a, $b \in \mathbb{Z}^+$ and $1 < a$, $b < n$.

Proof. We first prove the ($\Longrightarrow$) direction.

Proof of ($\Longrightarrow$)*.* There must exist some $a \in \mathbb{Z}^+$ with $1 \leq a < n$ such that $\gcd(a, n) \neq 1$, since otherwise n is prime by definition.

Let $\gcd(a, n) = d$. If $d = n$, then $n \mid a$, but that contradicts $1 \leq a < n$. Hence, $d < n$.

Note that $d \mid n$ implies that $\exists k \in \mathbb{Z}$ such that $n = dk$. Because $n \in \mathbb{Z}^+$ and $d \in \mathbb{Z}^+$, by Trichotomy, we know that $k \in \mathbb{Z}^+$, since otherwise $k = 0$ or $(-k) \in \mathbb{Z}^+$ gives a contradiction.

Observe that $k \neq 1$ since if $k = 1$ then $d = n$, which is a contradiction. Thus, $n = dk$ where $d > 1$ and $k > 1$. Moreover, if $d \geq n$, then $dk > n$, which is a contradiction, so $d < n$. Similarly, $k < n$, and we are done. ■

Proof of ($\Longleftarrow$)*.* If $\exists a$, $b \in \mathbb{Z}^+$ such that $1 < a$, $b < n$ and $n = ab$ for fixed n, then $\gcd(n, b) = b > 1$, hence n is not prime; moreover, $n > 1$, so n is composite. ■

□

Lemma 40 (Existence of a Prime Factor)**.** Every integer greater than 1 has a prime factor.

Proof. Let $S := \{n \mid \nexists p \text{ such that } p \mid n \text{ where } n \in \mathbb{Z}^+ \text{ and } n \neq 1\}$. Note that $S \subseteq \mathbb{Z}^+$.

Suppose for the sake of contradiction that $S \neq \emptyset$. Then, by WOP, S must have a least element, which we shall denote as n.

If n was prime, then n has n itself as a prime factorization, which is a contradiction. Moreover, n cannot be 1 by our assumption. Hence, n must be composite. This means that $\exists a, b \in \mathbb{Z}$ such that $n = ab$, where $1 < a, b < n$.

Because $a, b < n$, we know that a and b are not in S, by minimality of n. Thus, they have prime factors, i.e., $p \mid a$ and $q \mid b$, where p and q are primes.

Thus, $pq \mid ab \mid n$, which means $p \mid n$. Hence, n has a prime factor, so $n \notin S$, which contradicts our assumption that $S \neq \emptyset$. Thus, all integers must have a prime factor. □

Lemma 41 (Existence of a Prime Factorization)**.** Every integer greater than 1 has a prime factorization.

Proof. Let S be the set of positive integers that does not have a factorization as a product of primes. Assume for the sake of contradiction that $S \neq \emptyset$. Then, by WOP, S must have a minimum element n.

If n is prime, then $n \notin S$.

If n is not prime, then since $n > 1$, we know that n is composite, that is, $\exists a, b \in \mathbb{Z}^+$ with $1 < a, b < n$ such that $n = ab$.

If both a and b had a factorization as a product of primes, that is,

$$a = \prod_{i=1}^{k} p_i \quad \text{and} \quad b = \prod_{i=1}^{l} q_i$$

then define $\{p'_i\} := \begin{cases} p_i & \text{if } 1 \leq i \leq k \\ q_{i-k} & \text{if } k+1 \leq i \leq k+l \end{cases}$

Then,

$$\begin{aligned} n &= \left(\prod_{i=1}^{k} p_i\right)\left(\prod_{i=1}^{l} q_i\right) \\ &= \left(\prod_{i=1}^{k} p'_i\right)\left(\prod_{i=k+1}^{k+l} p'_i\right) \\ &= \prod_{i=1}^{k+l} p'_i \end{aligned}$$

so n has a prime factorization, contradiction.

Hence, at least one of a and b does not have a prime factorization. Without loss of generality, suppose a did not have a factorization as a product of primes, which in turn implies $a \in S$. But $1 < a < n$, which contradicts the minimality of n. Hence, $S = \emptyset$, and thus every integer greater than 1 has a prime factorization. □

6. Unique Factorization Theorem (UFT)

Definition 42. We say an integer n has a unique prime factorization if given any two prime factorizations

$$n = \prod_{i=1}^{a} p_i = \prod_{i=1}^{b} q_i \quad (p_i,\, q_i \text{ prime})$$

then (i) $a = b$ and (ii) $(\forall i \leq a)\ (\exists j \leq b)\ p_i = q_j$. That is, the primes in each product differ from each other by at most a reordering.

Theorem 43 (Unique Factorization in $\mathbb{Z}$)**.** Every positive integer greater than 1 has a unique prime factorization.

Proof. Let S be the set of positive integers greater than 1 that do not have a unique prime factorization. Assume for the sake of contradiction that $S \neq \emptyset$. Then, by WOP, there exists a least element of S, which we denote as n, that is,

$$n = \prod_{k=1}^{a} p_k = \prod_{k=1}^{b} q_k$$

where p_k and q_k are primes and either $(\exists k \leq a)\ (\nexists l \leq b)\ p_k = q_l$ or $a \neq b$.

Case 1: $(\exists k \in \mathbb{Z},\ 1 \leq k \leq a)\ (\nexists l \leq b)\ p_k = q_l$.

Let $P \subseteq S$ be the set of positive integers whose prime factorizations fail in this way. Recall that $\prod_{i=1}^{a} p_i = \prod_{i=1}^{b} q_i$. Hence, we may split the first product into three distinct products, giving

$$\left(\prod_{i=1}^{k-1} p_i\right) p_k \left(\prod_{i=k+1}^{a} p_i\right) = \prod_{i=1}^{b} q_i$$

Thus, $p_k \mid \prod_{i=1}^{b} q_i$. As p_k is prime, by Extended Euclid's Lemma, we know that $(\exists l \in \mathbb{Z},\ 1 \leq l \leq b)\ p_k \mid q_l$.

By definition of divisibility, $(\exists n \in \mathbb{Z})\ p_k \cdot n = q_l$. As $p_k, q_l \in \mathbb{Z}^+$, we also have $n \in \mathbb{Z}^+$, i.e., $n \geq 1$.

Assume for the sake of contradiction $n > 1$. Then if $p_k \geq q_l$, $p_k \cdot n > q_l$, but $p_k = q_l$; thus $p_k < q_l$. Note as p_k is prime, $p_k > 1$; similarly, therefore, $n < q_l$. In summary, $q_l = p_k \cdot n$, where $1 < p_k < q_l$ and $1 < n < q_l$. Then q_l is composite; contradiction.

Thus, $n = 1$, which implies $p_k = q_l$. But this contradicts our assumption that $(\nexists l \leq b)\ p_k = q_l$.

Hence, P is empty, so $S \setminus P = S$. Indeed, we can assume that, for the factorizations of our minimum n of S, $(\forall k \leq a)\ (\exists l \leq b)\ p_k = q_l$ but $a \neq b$. It remains to deal with the other case.

Case 2: $a \neq b$.

Without loss of generality, assume $a > b$.

If $b = 0$, then $\prod_{i=1}^{b} q_i = 1$, by definition of the product notation. Thus $\prod_{i=1}^{a} p_i = 1$. But recall $a > b = 0$; thus by NIBZO, $a \geq 1$. Therefore, by definition of the product notation, $\left(\prod_{i=1}^{a-1} p_i\right) \cdot p_a = 1$; thus $p_a \mid 1$. But p_a is prime, so by definition, $p_a \nmid 1$, which is a contradiction. Thus $b \neq 0$.

Thus $b > 0$, so by NIBZO $b \geq 1$. Then also $a \geq 1$. Then by definition of the product notation, we know that $\left(\prod_{i=1}^{a-1} p_i\right) \cdot p_a = \prod_{i=1}^{b} q_i$. But recall, we above showed $(\exists a' \leq b) \quad p_a = q_{a'}$. Then, we can split the product, giving

$$\begin{aligned}\left(\prod_{i=1}^{a-1} p_i\right) \cdot p_a &= \left(\prod_{i=1}^{a'-1} q_i\right)\left(\prod_{i=a'}^{a'} q_i\right)\left(\prod_{i=a'+1}^{b} q_i\right) \\ &= \left(\prod_{i=1}^{a'-1} q_i\right)\left(\prod_{i=a'+1}^{b} q_i\right) \cdot q_{a'}\end{aligned}$$

We can define a new sequence $\{q'_i\}$ by $q'_k = \begin{cases} q_k & \text{if } k < a' \\ q_{k+1} & \text{if } k \geq a' \end{cases}$. Then we continues simplifying:

$$\begin{aligned}\left(\prod_{i=1}^{a-1} p_i\right) \cdot p_a &= \left(\prod_{i=1}^{a'-1} q_i\right)\left(\prod_{i=a'+1}^{b} q_i\right) \cdot q_{a'} \\ &= \left(\prod_{i=1}^{a'-1} q'_i\right)\left(\prod_{i=a'}^{b-1} q'_i\right) \cdot q_{a'} \\ &= \left(\prod_{i=1}^{a'-1} q'_i\right)\left(\prod_{i=a'}^{b-1} q'_i\right) \cdot p_a \\ &= \left(\prod_{i=1}^{b-1} q'_i\right) \cdot p_a\end{aligned}$$

Let $n' = \left(\prod_{i=1}^{a-1} p_i\right)$, so that $n' \cdot p_a = n$. As p_a is prime, we have $p_a > 1$, thus $n' < n$.

Observe that we may write:

$$n' \cdot p_a = \left(\prod_{i=1}^{a-1} p_i\right) \cdot p_a = \left(\prod_{i=1}^{b-1} q'_i\right) \cdot p_a$$

As $p_a \neq 1$, we may cancel, giving

$$n' = \left(\prod_{i=1}^{a-1} p_i\right) = \left(\prod_{i=1}^{b-1} q'_i\right)$$

Recall that $a > b$. Then $a - 1 > b - 1$, implying $a - 1 \neq b - 1$. Thus, n' does not have a unique factorization, yet $n' < n$, contradicting the minimality of n.

Therefore, $S = \emptyset$, and consequently, every positive integer greater than 1 has a unique prime factorization. □