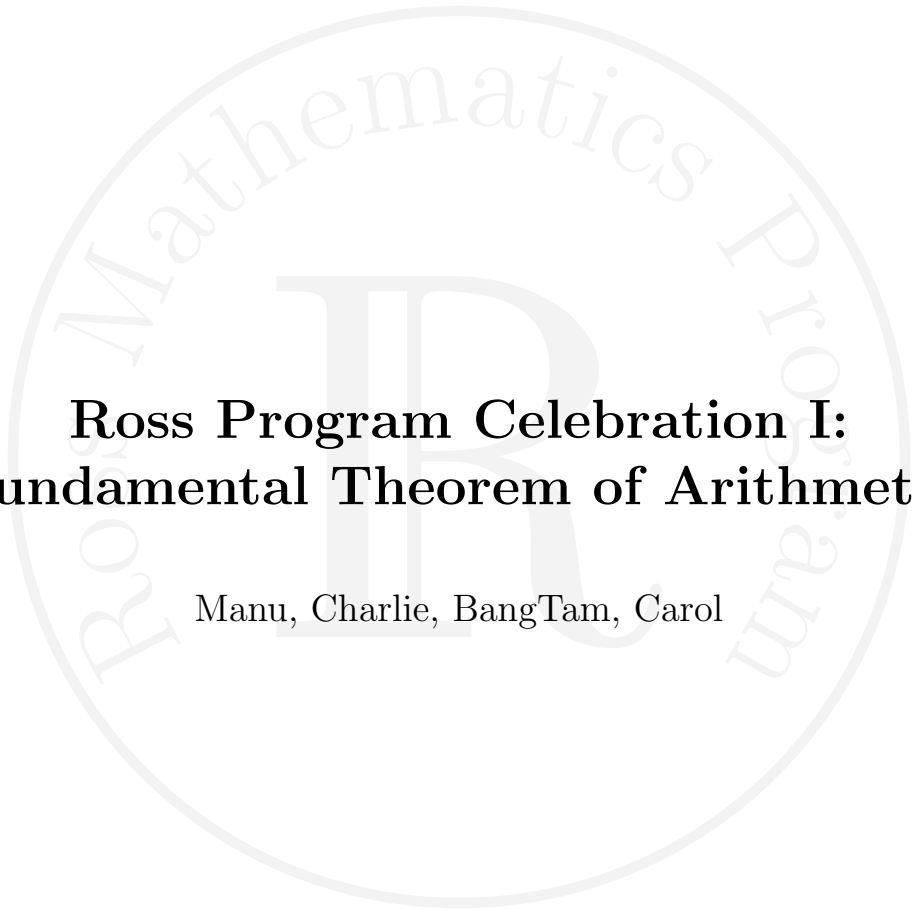

Ross Program Celebration I: Fundamental Theorem of Arithmetic

Manu, Charlie, BangTam, Carol

Table of Contents

1. Introduction

"Please forget everything you have learned in school; for you haven't learned it. Please keep in mind at all times the corresponding portions of your school curriculum; for you haven't actually forgotten them."

— Edmund Landau, Foundations of Analysis Prefaces

1.1. Motivation

In this celebration, we will prove the Fundamental Theorem of Arithmetic given a few axiomatic assumptions (2.1, 2.3, 2.4). We aim to maximize the celebratory effect of our endeavor, and thus our exposition shall meet the following specifications:

1. **Rigor and Clarity**: We will present a rigorous and clear proof of the Fundamental Theorem of Arithmetic, ensuring that each step is justified and comprehensible.
2. **Intuition**: While the proof may involve complex concepts, we will provide intuitive explanations and examples to help deepen understanding.
3. **Deep Thoughts About Simple Things**: We encourage readers to reflect on the profound implications of seemingly simple concepts, such as prime numbers and factorization. By exploring the depths of these elementary ideas, we can uncover the remarkable intricacies of number theory and appreciate the power of mathematical reasoning.

1.2. Problem Statement

The **Fundamental Theorem of Arithmetic** states that every integer whose absolute value is greater than 1 can be represented uniquely as a product of prime numbers, up to the order of the factors.

Specifically, for all $a \in \mathbb{Z} \setminus \{-1, 0, 1\}$, there exist unique sets $P \subseteq \mathbb{P}$, $E \subseteq \mathbb{Z}^+$ with $n \in \mathbb{Z}^+$ terms such that $a = \pm \prod_{i=1}^{n} p_i^{e_i}$, for $p_i \in P$, $e_i \in E$.

1.3. Roadmap

1. Given our three axiomatic assumptions (2.1, 2.3, 2.4), we can construct the set $\mathbb{Z}$ and discuss fundamental properties of the set.
    - Define order in the set, inequalities.
    - Then we define basic arithmetic operations, addition, subtraction, exponents.
2. We then look at divisibility in $\mathbb{Z}$ and understand the concept of gcd and subsequent properties.
3. With the new idea of divisibility we begin defining prime numbers and properties we may use.
4. We explore prime numbers further and prove important theorems like Euclid's lemma and the existence of prime factorizations.
5. Using all these results and tools we construct an argument to prove the fundamental theorem of arithmetic.

1.3.1. Read me!

Proofs for some lemmas omitted and instead referred to in the appendix for readability.

2. Axioms

2.1. Ring Axioms

The following Ring Axioms define properties of addition $(+)$ and multiplication $(\cdot)$ under $\mathbb{Z}$. The operations are binary — that is, for all $a, b \in \mathbb{Z}$, $a + b \in \mathbb{Z}$ and $a \cdot b$ or simply $ab \in \mathbb{Z}$.

For all $a, b, c \in \mathbb{Z}$,

Axiom 1 (Commutativity)**.** $a + b = b + a$, $ab = ba$.

Axiom 2 (Associativity)**.** $a + (b + c) = (a + b) + c$, $a(bc) = (ab)c$.

Axiom 3 (Distributivity)**.** $a(b + c) = ab + ac$.

Axiom 4 (Additive Identity)**.** There exists some $0 \in \mathbb{Z}$ such that $a + 0 = a$.

Axiom 5 (Additive Inverse)**.** There exists some $-a \in \mathbb{Z}$ such that $a + (-a) = 0$.

Axiom 6 (Multiplicative Identity)**.** There exists some $1 \in \mathbb{Z}$ such that $a \cdot 1 = a$.

2.1.1. Facts by Logic

Fact 1. *For all $a, b, c \in \mathbb{Z}$, if $a = b$, then $a + c = b + c$.*

Fact 2. *For all $a, b, c \in \mathbb{Z}$, if $a = b$, then $ac = bc$.*

Definition 1 (Unequal)**.** For all $a, b \in \mathbb{Z}$, $a \neq b \iff \neg(a = b)$.

2.2. Subsequent Properties of Ring Axioms

These lemmas can be derived using the ring and order axioms. The proofs for these lemmas are omitted here for readability; you can find them listed in the appendix here: 1.

Lemma 1 (Uniqueness of Additive Identity)**.** *For all $a \in \mathbb{Z}$, there is only one $0 \in \mathbb{Z}$ such that $a + 0 = a$.*

Lemma 2 (Uniqueness of Multiplicative Identity)**.** *For all $a \in \mathbb{Z}$, there is only one $1 \in \mathbb{Z}$ such that $a \cdot 1 = a$.*

Lemma 3. *For all $a, b, c \in \mathbb{Z}$, if $a + b = a + c$, then $b = c$.*

Lemma 4 (Uniqueness of Additive Inverse)**.** *For all $a \in \mathbb{Z}$, there is only one $-a \in \mathbb{Z}$ such that $a + (-a) = 0$.*

Lemma 5. *For all $a \in \mathbb{Z}$, $a \cdot 0 = 0$.*

Lemma 6. *For all $a \in \mathbb{Z}$, $-a = (-1) \cdot a$.*

Corollary 1. *For all $a, b \in \mathbb{Z}$, $-(a + b) = -a + (-b)$.*

Corollary 2. $0 = -0$.

Corollary 3. *For all $a \in \mathbb{Z}$, $-a \in \mathbb{Z}$.*

Lemma 7. *For all $a \in \mathbb{Z}$, $-(-a) = a$.*

Lemma 8. *For all $a, b \in \mathbb{Z}$, $-(ab) = (-a)b = a(-b)$.*

Lemma 9. *For all $a, b \in \mathbb{Z}$, $(-a)(-b) = ab$.*

Definition 2 (Subtraction)**.** For all $a, b \in \mathbb{Z}$, define $a - b = a + (-b)$.

Lemma 10 (Closure Under Subtraction)**.** *For all $a, b \in \mathbb{Z}$, $a - b \in \mathbb{Z}$.*

Lemma 11 (Inverse Associativity of Subtraction)**.** *For all $a, b, c \in \mathbb{Z}$, $a-(b-c) = (a-b)+c$.*

Lemma 12 (Distributivity of Subtraction)**.** *For all $a, b, c \in \mathbb{Z}$, $a(b - c) = ab - ac$.*

Lemma 13. *For all $a, b, c \in \mathbb{Z}$, $a = b \iff a - c = b - c$.*

2.3. Order Axioms

To establish a clear notion of order in $\mathbb{Z}$, we introduce the following set of axioms that describes a nonempty $\mathbb{Z}^+ \subseteq \mathbb{Z}$:

For all $a, b \in \mathbb{Z}^+$,

Axiom 7 (Additive Closure)**.** $a + b \in \mathbb{Z}^+$.

Axiom 8 (Multiplicative Closure)**.** $ab \in \mathbb{Z}^+$.

Axiom 9 (Trichotomy)**.** For all $n \in \mathbb{Z}$, exactly one of the following holds: $n \in \mathbb{Z}^+$, $n = 0$, or $-n \in \mathbb{Z}^+$.

2.3.1. Negative Integers

Definition 3 ($\mathbb{Z}^-$)**.** By Axiom 9 (Trichotomy), there exists a nonempty $\mathbb{Z}^- \subseteq \mathbb{Z}$ where $\mathbb{Z}^- = \mathbb{Z} \setminus \{\, \mathbb{Z}^+ \cup 0 \,\}$.

Lemma 14. *For all $a, b \in \mathbb{Z}^-$, $ab \in \mathbb{Z}^+$.*

2.3.2. Inequalities

Definition 4. For all $a, b \in \mathbb{Z}$, we define $a > b \iff a + (-b) \in \mathbb{Z}^+$, $a \geq b \iff a > b$ or $a = b$. Furthermore, $a < b \iff b > a$, and $a \leq b \iff b \geq a$.

Theorem 1 (Relation Trichotomy)**.** *For all $a, b \in \mathbb{Z}$, exactly one of the following is true: $a < b$, $a = b$, or $a > b$.*

Proof. Let $a, b \in \mathbb{Z}$. Consider $a + (-b)$. By Trichotomy, either $a + (-b) \in \mathbb{Z}^+$, $a + (-b) = 0$, or $-(a + (-b)) \in \mathbb{Z}$. Notice, $-(a + (-b)) \overset{\text{(Corollary 1)}}{=} -a + -(-b) \overset{\text{(Lemma 7)}}{=} -a + b \overset{\text{(Axiom 1: Commutativity)}}{=} b + (-a)$. Further, notice

$$\begin{aligned} a - b &= 0 \\ a - b + b &= 0 + b \\ a + ((-b) + b) &= 0 + b \\ a + 0 &= b \\ a &= b \end{aligned}$$

As such, either $a > b$, $a = b$, or $b > a \implies a < b$. □

Corollary 4 (Unequal)**.** *For all $a, b \in \mathbb{Z}$, $a \neq b \iff a > b$ or $a < b$.*

Lemma 15. *For $a, b, c \in \mathbb{Z}$, if $a \leq b$ and $b \leq c$, $a \leq c$.*

Proof. Let $a, b, c \in \mathbb{Z}$.

□

Lemma 16. *For all $a, b, c, d \in \mathbb{Z}$, if $a < b \implies c < d$, then $a \leq b \implies c \leq d$.*

Lemma 17. *For all $a, b, c, d \in \mathbb{Z}$, if $a < b \implies c < d$, then $a > b \implies c > d$.*

Lemma 18. *For all $a, b \in \mathbb{Z}$, $c \in \mathbb{Z}^+$, $a < b \iff ac < bc$.*

Lemma 19. *For all $a, b \in \mathbb{Z}$, $c \in \mathbb{Z}^-$, $a < b \iff ac > bc$.*

Lemma 20. *For all $a, b, c \in \mathbb{Z}$, $a < b \iff a + c < b + c$.*

2.4. Well-Ordering Principle

Axiom 10. Every nonempty subset S of positive integers contains a least element; that is, there is some element a of S such that $a \leq b$ for all elements b of S.

2.4.1. Ordering Principles

Corollary 5. *For all $a \in \mathbb{Z}^+$, $1 \leq a$.*

Proof. Consider set $S = \mathbb{Z}^+$. By the Well-Ordering Principle, there is a least element of S called l. The number 1 is an element in $\mathbb{Z}^+$, so $l \leq 1$. The number l is in $\mathbb{Z}^+$, so $(l)(l) \leq (l)(1) = l$. There cannot be an element smaller than l, so $(l)(l) = (l)(1)$, and $l = 1$. Therefore, the least element l is 1. □

Corollary 6. *For all $a \in \mathbb{Z}^-$, $-1 \geq a$.*

Proof. Let $a \in \mathbb{Z}^-$. Consider a □

Theorem 2. *For all nonempty $D \subseteq \mathbb{Z}$ where D has a finite number of terms, there exist $l, g \in D$ such that for all $d \in D$, $l \leq d \leq g$.*

3. Divisibility

3.1. Division

An important property of the elements of $\mathbb{Z}$ is that given any $a, b \in \mathbb{Z}$ it follows that $a|b$ or $a \nmid b$

Definition 5 (Divisibility)**.** For all $a, b \in \mathbb{Z}$, we write $a \mid b$ if and only if there exists $q \in \mathbb{Z}$ such that $b = aq$.

Definition 6. For all $a, b \in \mathbb{Z}$, we write $a \nmid b$ if and only if there does not exist $q \in \mathbb{Z}$ such that $b = aq$.

Lemma 21. *For all $a, b \in \mathbb{Z}^+$, if $a \mid b$, then $a \leq b$.*

Proof. Let $a, b \in \mathbb{Z}^+$. Suppose $a \mid b$, then for some $k \in \mathbb{Z}$, $b = ak$. As such, $a \leq b \iff a(k-1) \geq 0$, so we now show $k \in \mathbb{Z}^+$. Assume otherwise for contradiction, then either $k = 0$ or $-k \in \mathbb{Z}^+$. In the first case, $b = ak = a \cdot 0 = 0$, which is a contradiction. In the second, $-b = -ak = a(-k) \in \mathbb{Z}^+$, which is a contradiction. As such, $k \in \mathbb{Z}^+$, and we are done. □

Lemma 22. *For all $a, b, c \in \mathbb{Z}$, if $c \mid a$ and $c \mid b$, then $c \mid ar + bs$ for $r, s \in \mathbb{Z}$.*

Proof. Let $a, b, c \in \mathbb{Z}$. Suppose $c \mid a$ and $c \mid b$, then there exist m, n such that $a = cm$, $b = cn$. Notice,

$$\begin{aligned} ar + bs &= (cm)r + (cn)s \\ &= c(mr) + c(ns) \\ &= c(mr + ns) \end{aligned}$$

. As such, $c \mid ar + bs$. □

Theorem 3 (Division Algorithm)**.** *For all $a, b \in \mathbb{Z}$ where $b \neq 0$, $a = bq+r$ for some $q, r \in Z$ where $0 \leq r < |b|$.*

Proof. Let $a \in \mathbb{Z}$. Then, exactly one of the following holds: $a = 0$, $a \in \mathbb{Z}^+$, $-a \in \mathbb{Z}^+$. We proof the statement by showing it is true for each case.
Consider $a = 0$. Notice, for all $b \in \mathbb{Z}$ where $b \neq 0$, $a = bq + r$ for $q = 0$, $r = 0$, as desired.
Consider $a \in \mathbb{Z}^+$. Let $S = \{ n \in \mathbb{Z}^+ : n \neq bq + r \text{ for } b, q, r \in \mathbb{Z} \text{ where } b \neq 0, 0 \leq r < |b| \}$. Since $S \subseteq \mathbb{Z}^+$, there exists $s \in S$ such that for all $n \in S$, $1 \leq s \leq n$. As such, $s - 1 \notin S$ and is either 0 or an element of $\mathbb{Z}^+$. Thus, there exist $b, q, r \in \mathbb{Z}$ where $b \neq 0$ and $0 \leq r < |b|$ such that $s - 1 = bq + r \implies s = bq + (r + 1)$. Put $\hat{r} = r + 1$. Now, the value of $\hat{r}$ lies within exactly one of two cases: $1 \leq \hat{r} < |b|$, or $\hat{r} = |b|$. We aim to show that both cases would lead to contradictions, which would imply $S = \varnothing$. In the former, since $\hat{r}$ is within the range $[0, |b|)$, we have a contradiction. In the latter, we have $s = bq + \hat{r} = bq + |b|$. Since $b \neq 0$, it is either positive, where $s = bq + b = b(q + 1) + 0$, or negative, where $s = bq - b = b(q - 1) + 0$. Since $q + 1 \in \mathbb{Z}$, $q - 1 \in \mathbb{Z}$, and $0 \in [0, |b|)$, this case also yields a contradiction. As such, the statement is also true under the second condition.
By the symmetry of integers across 0, the case where $-a \in \mathbb{Z}^+$ may be proven in a similar fashion to that of when $a \in \mathbb{Z}^+$. □

Corollary 7. *For all $a, b \in \mathbb{Z}$, we write $a \nmid b \iff b = aq+r$ for $q, r \in \mathbb{Z}$ where $0 < r < |b|$.*

3.2. Greatest Common Divisor

Definition 7 (Greatest Common Divisor)**.** For all $a, b \in \mathbb{Z}$, put $D = \{ d \in \mathbb{Z}^+ : d \mid a \text{ and } d \mid b \}$, then if there exists $g \in D$ such that for all $d \in D$, $d \leq g$, $\gcd(a, b) = g$.

Lemma 23. *For all $a, b \in \mathbb{Z}$ where $a \neq 0$ or $b \neq 0$, there exists a nonempty, finite $D = \{ d \in \mathbb{Z}^+ : d \mid a \text{ and } d \mid b \}$.*

Proof. Let $a, b \in \mathbb{Z}$ where $a \neq 0$ or $b \neq 0$. We first show non-triviality of D. Put $D = \{ d : d \mid a \text{ and } d \mid b \}$. Since for all $n \in \mathbb{Z}$, the multiplicative identity $1 \mid n$, $1 \in D$, so D is nonempty. We now show that $D \subseteq \mathbb{Z}^+$ is finite. Let $k \in \mathbb{Z}^+$, so $b + k > b$. By the contrapositive of Lemma 21, $(b + k) \nmid b$, so $b + k \notin D$. As such, for all $d \in D$, $d \leq b$. Therefore, D is finite. □

Proposition 1 (Existence of Greatest Common Divisor)**.** *For all $a, b \in \mathbb{Z}$ where $a \neq 0$ or $b \neq 0$, there exists $gcd(a, b) \in \mathbb{Z}^+$.*

Proof. Let $a, b \in \mathbb{Z}$ where $a \neq 0$ or $b \neq 0$. By Lemma 23, there exists a nonempty, finite $D = \{\, d \in \mathbb{Z}^+ : d \mid a \text{ and } d \mid b \,\}$. As such, there exists $g \in D$ such that for all $d \in D$, $1 \leq d \leq g$. Thus, there exists positive integer $\gcd(a, b) = g$. □

Theorem 4 (Euclidean Algorithm)**.** *For all $a, b \in \mathbb{Z}$, $gcd(a - b, b) = gcd(a, b)$.*

Proof. Let $a, b \in \mathbb{Z}$. Put $x_1 = gcd(a, b)$, so by Definition 7, there exist $m, n \in \mathbb{Z}$ such that $a = x_1 m$ and $b = x_1 n$. Similar,y put $x_2 = gcd(a - b, b)$, so there exist $p, q \in \mathbb{Z}$ such that $a - b = x_2 p$ and $b = x_2 q$. Notice, $x_2 p = a - b = x_1(m - n)$, and $x_1 n = b = x_2 q$.
We aim to show that $x_1 = x_2$ by proving the other two relations impossible. Suppose for contradiction that $x_1 < x_2$. By Definition 7, there exists no $\mu > x_1$ such that $b = \mu\mu'$ for $\mu' \in \mathbb{Z}^+$. Since $b = x_2 q$ and $x_2 > x_1$, this is a contradiction. Thus, $x_1 \geq x_2$. Similarly, suppose for contradiction that $x_1 > x_2$, so there exists no $\mu > x_2$ such that $a - b = \mu\mu'$ for μ' in $\mathbb{Z}^+$. Since $a - b = x_1(m - n)$, this is also a contradiction.
As such, $gcd(a - b, b) = gcd(a, b)$, as desired. □

Lemma 24 (Bezout's Identity)**.** *For all $a, b \in \mathbb{Z}$, there exist $x, y \in \mathbb{Z}$ such that $ax + by = gcd(a, b)$.*

Proof. Let $a, b \in \mathbb{Z}$. Put $S = \{\, ax + by : x, y \in \mathbb{Z} \,\}$. Define $S^+ = S \cap \mathbb{Z}^+$, so there exists $k \in S^+$ such that for all $s \in S^+$, $1 \leq k \leq s$. By Theorem 3 (Division Algorithm), $a = kq + r$ for $q, r \in \mathbb{Z}$, where $0 \leq r < k$. As such,

$$\begin{aligned} r &= a - kq \\ &= a - (ax + by)q \\ &= a - axq - byq \\ &= a(1 - qx) + b(-qy) \end{aligned}$$

, so $r \in S$. Since $r < k$, $r \notin S^+$. Furthermore, since $r \geq 0$, $r = 0$. As such, $a = kq \implies k \mid a$. With a similar process, it may be shown that $k \mid b$. Then, by Definition 7, $k \leq gcd(a, b)$. Since $gcd(a, b) \mid a$ and $gcd(a, b) \mid b$, by Lemma 22, $gcd(a, b) \mid k$. By Lemma 21, $gcd(a, b) \leq k$. As such, $gcd(a, b) = k = ax + by$. We note further that it is in fact the least positive linear combination of a, b. □

Lemma 25 (The Fundamental Lemma)**.** *For all $a, b, c \in \mathbb{Z}$, if $a \mid bc$ and $gcd(a, b) = 1$, then $a \mid c$.*

Proof. Suppose $a \mid bc$ and $gcd(a, b) = 1$. Then, by Lemma 24 (Bezout's Identity),

$$\begin{aligned} ax + by &= 1 \\ c(ax + by) &= c \\ (ac)x + (bc)y &= c \end{aligned}$$

Since $a \mid bc$, $bc = an$ for $n \in \mathbb{Z}$. As such,

$$\begin{aligned} (ac)x + (an)y &= c \\ a(cx + ny) &= c \end{aligned}$$

As such, $a \mid c$. □

4. Primes

Definition 8 (Prime Numbers)**.** For all $p \in \mathbb{Z}^+ \setminus \{1\}$, p is prime if and only its set of divisors $D = \{1, p\}$.

Definition 9. We define the set of primes $\mathbb{P} = \{p : \text{p is prime}\}$.

Definition 10. For all $c \in \mathbb{Z}^+ \setminus \{1\}$, c is composite if and only if $c \notin \mathbb{P}$.

Theorem 5. *For all $p \in \mathbb{Z}^+ \setminus \{1\}$, $p \in \mathbb{P} \iff$ for all $k \in (0, p)$, $\gcd(k, p) = 1$.*

Proof. We prove the contrapositive. Let $p \in \mathbb{Z}^+ \setminus \{1\}$. Suppose there exists $k \in (0, p)$ such that $\gcd(k, p) \neq 1$. Put $d = gcd(k, p)$. Then by Definition 7, $d \mid p$. Notice, by Lemma 21, $d < k < p$. Further, since $d \in \mathbb{Z}^+$, $d > 1$. As such, there exists a third element in the set of divisors of p, so by Definition 8, $p \notin \mathbb{P}$. □

Corollary 8. *For all $c \in \mathbb{Z}^+ \setminus \{1\}$ where c is composite, $c = ab$ for $a, b \in \mathbb{Z}^+ \setminus \{1\}$. Notice, $a, b < c$.*

4.1. Existence of Prime Divisors

Lemma 26. *For all $a \in \mathbb{Z}^+$ where $a \neq 1$, there exists $p \in \mathbb{P}$ such that $p \mid a$.*

Proof. Let $a \in \mathbb{Z}^+$ where $a \neq 1$. Then, a is either prime or composite. The first case is trivial, as $a \mid a$ and $a \in \mathbb{P}$. Now we consider the second case, where we aim to show that there exists no positive composite number without prime factors.
Put $S = \{ s \in \mathbb{Z}^+ \setminus \{1\} : s \text{ is composite, and for all } d \in \mathbb{Z}^+ \text{ where } d \mid s, d \notin \mathbb{P} \}$, then there exists $l \in S$ such that for all $s \in S$, $s \geq l$. Since s is composite, by Corollary 8, $s = mn$ for $m, n \in \mathbb{Z}^+$ where $m < s$, $n < s$. As such, $m, n \notin S$, so there exist $p_1, p_2 \in \mathbb{P}$ such that $p_1 \mid m$, $p_2 \mid n$. Then, for $k_1, k_2 \in \mathbb{Z}^+$, $m = p_1 k_1, n = p_2 k_2$. It follow that $s = ab = p_1 k_1 p_2 k_2$, so $p_1 \mid s$ and $p_2 \mid s$, which is a contradiction. Therefore, $s = \varnothing$, and we are done. □

Lemma 27. *For all $a \in \mathbb{Z} \setminus \{-1, 0, 1\}$, there exists $p \in \mathbb{P}$ such that $p \mid a$.*

Proof. Let $a \in \mathbb{Z} \setminus \{-1, 0, 1\}$, then either $a \in \mathbb{Z}^+ \setminus \{1\}$ or $-a \in \mathbb{Z}^+ \setminus \{-1\}$. The first case is true by Lemma 26. We now consider the second. By Lemma 26, there exists $p \in \mathbb{P}$ such that $p \mid -a$. As such, for $k \in \mathbb{Z}$,

$$\begin{aligned} -a &= pk \\ (-1)a &= pk \\ a &= (-1)pk \end{aligned}$$

Thus, $p \mid a$, and we are done. □

Lemma 28. *For all $a \in \mathbb{Z} \setminus \{-1, 0, 1\}$, $a = \pm \prod_{i=1}^{n} p_i$ for $p_i \in \mathbb{P}$.*

Proof. Given the symmetry of integers over 0, we simply need to show that the statement is true for positive integers. Let $a \in \mathbb{Z}^+$. Put $S = \{ s \in \mathbb{Z}^+ \setminus \{1\} : s \neq \prod_{i=1}^{n} p_i \text{ for } p_i \in \mathbb{P} \}$, then there exists $l \in S$ such that for all $s \in S, l \leq s$. By Lemma 27, there exists $p \in \mathbb{P}$ such that $l = pm$ for $m \in \mathbb{Z}^+$. Notice, l cannot be prime, as $l \mid l$. Thus, l is composite, so $m < s$. As such, $m \notin S$, so $m = \prod_{i=1}^{n} p_i$ for $p_i \in \mathbb{P}$. As such, $l = pm = p \prod_{i=1}^{n} p_i$. This is a contradiction, so $S = \varnothing$ and we are done. □

5. Fundamental Theorem of Arithmetic

5.1. Euclid's Lemma

Lemma 29 (Euclid's Lemma)**.** *For all $p \in \mathbb{P}$, if $p \mid ab$, then $p \mid a$ or $p \mid b$.*

Proof. Let $p \in \mathbb{P}$. We prove by contradiction. Suppose $p \mid ab$, and that $p \nmid a$ and $p \nmid b$ for contradiction. We aim to show that $gcd(a, p) = gcd(b, p) = 1$. If this is true, by Lemma 25 (Fundamental Lemma), $p \mid b$, which is a contradiction as $gcd(b, p) = 1$.
We consider two cases: $a < p$ and $a > p$. In the former, by Theorem 5, $gcd(a, p) = 1$. In the latter, by Corollary 7 $a = pq + r$ for $q, r \in \mathbb{Z}$ where $0 < r < p$. By Theorem 4, $gcd(a, p) = gcd(pq+r, p) = gcd(r, p) = 1$. Notice, $gcd(b, p) = 1$ could be proved similarly. □

Lemma 30 (Generalized Euclid's Lemma)**.** *For all $p \in \mathbb{P}$, if $p \mid \prod_{i=1}^{n} a_i$ for $a_i \in \mathbb{Z}$, then $p \mid a_i$ for some i where $1 \leq i \leq n$.*

Proof. Let $p \in \mathbb{P}$. Suppose $p \mid \prod_{i=1}^{n} a_i$ for $a_i \in \mathbb{Z}$. Put $S = \{\, s \in \mathbb{Z}^+ : p \nmid a_i \text{ for all } i \in [1, n] \,\}$, then there exists $l \in S$ such that for all $s \in S$, $l \leq s$. By Lemma 29, $p \mid a_1$ or $p \mid \prod_{i=2}^{n} a_i$. Then, $a_2 a_3 ... a_s = \frac{s}{a_1} \leq s$. This means that $\frac{s}{a_1} \notin S$ since s is the least element of S. So, $p \mid a_2$ or $p \mid a_3 \ldots p \mid a_n$. However, this is a contradiction since we assumed that $p \nmid a_1$, $p \nmid a_2$, ... and, $p \nmid a_k$. Therefore, S is empty and so, if $p \mid a_1 a_2 ... a_n$ for all rational primes p, then $p \mid a_i$ for some index i with $1 \leq i \leq n$. □

5.2. Fundamental Theorem of Arithmetic

Theorem 6 (Fundamental Theorem of Arithmetic)**.** *For all $a \in \mathbb{Z} \setminus \{\, -1, 0, 1 \,\}$, there exist unique sets $P \subseteq \mathbb{P}$, $E \subseteq \mathbb{Z}^+$ with $n \in \mathbb{Z}^+$ terms such that $a = \pm \prod_{i=1}^{n} p_i^{e_i}$, for $p_i \in P$, $e_i \in E$.*

Proof. Let $a \in \mathbb{Z} \setminus \{\, -1, 0, 1 \,\}$. By Lemma **??**, $a = \pm \prod_{i=1}^{n} p_i$ for $p_i \in P$. In order to prove its uniqueness, we must show no $a \in \mathbb{Z}$ admits 2 different prime factorizations. If there is any such a, we pick the smallest. We can factor $a = \pm \prod_{i=1}^{n} p_i = \pm \prod_{i=1}^{m} q_i$, where we assume $p_1, p_2, ... p_n \neq q_1, q_2, ... q_m$. Clearly, $p_1 \neq q_1$, so without loss of generality, we assume $p_1 < q_1$ such that $p_1 - q_1 > 0$. So we can write $(p_1 - q_1) p_2 \cdots p_k = a$. Then:

$$\underbrace{p_1 p_2 \cdots p_k}_{a} - q_1 p_2 \cdots p_k = a$$

Therefore this is equivalent to: $q_1q_2\cdots q_k - q_1p_2\cdots p_k = a \implies q_1(q_2\cdots q_k - p_2\cdots p_k) = a$. It follows that $q_1|a$. Then it follows that $\frac{a}{q_1}$ is another factorization for a violating the minimality of a assumed under WOP. Therefore by contradiction there can only exist one unique factorization for any given $a \in \mathbb{Z}$.

□

6. Appendix

6.1. Subsequent Properties of Ring Axioms

Lemma 1 (Uniqueness of Additive Identity)**.** *For all $a \in \mathbb{Z}$, there is only one $0 \in \mathbb{Z}$ such that $a + 0 = a$.*

Proof. Suppose for contradiction that there exists $\hat{0} \in \mathbb{Z}$ such that for all $a \in \mathbb{Z}$, $a + \hat{0} = a$ and $\hat{0} \neq 0$. Notice, $\hat{0} \overset{\text{(Axiom 4: Additive Identity)}}{=} \hat{0} + 0 \overset{\text{(Axiom 1: Commutativity)}}{=} 0 + \hat{0} \overset{\text{(Supposition)}}{=} 0$, which is a contradiction. As such, 0 is unique. □

Lemma 2 (Uniqueness of Multiplicative Identity)**.** *For all $a \in \mathbb{Z}$, there is only one $1 \in \mathbb{Z}$ such that $a \cdot 1 = a$.*

Proof. Suppose for contradiction that there exists $\hat{1} \in \mathbb{Z}$ such that for all $a \in \mathbb{Z}$, $a \cdot \hat{1} = a$ and $\hat{1} \neq 1$. Notice, $\hat{1} \overset{\text{(Axiom 6: Multiplicative Identity)}}{=} \hat{1} \cdot 1 \overset{\text{(Axiom 1: Commutativity)}}{=} 1 \cdot \hat{1} \overset{\text{(Supposition)}}{=} 1$, which is a contradiction. As such, 1 is unique. □

Lemma 3. *For all $a, b, c \in \mathbb{Z}$, if $a + b = a + c$, then $b = c$.*

Proof. Let $a, b, c \in \mathbb{Z}$. Suppose $a+b = a+c$. Notice, by Fact 1, $(-a)+(a+b) = (-a)+(a+c)$. With Axiom 2 (Associativity), $(-a+a)+b = (-a+a)+c$. Swapping the terms by Axiom 1 (Commutativity), $(a + (-a)) + b = (a + (-a)) + c$. Then, by Axiom 5 (Additive Inverse), $0 + b = 0 + c$. As such, by Axiom 4 (Additive Identity), $b = c$. □

Lemma 4 (Uniqueness of Additive Inverse)**.** *For all $a \in \mathbb{Z}$, there is only one $-a \in \mathbb{Z}$ such that $a + (-a) = 0$.*

Proof. Let $a \in \mathbb{Z}$. Suppose for contradiction that there exists $\hat{-a} \in \mathbb{Z}$ such that $a+(\hat{-a}) = 0$ and $-a \neq \hat{-a}$. Notice, $a + (-a) = 0 = a + (\hat{-a})$. By Lemma 3, $-a = \hat{-a}$. This is a contradiction, and we are done. □

Lemma 5. *For all $a \in \mathbb{Z}$, $a \cdot 0 = 0$.*

Proof. Let $a \in \mathbb{Z}$. Notice, by Axiom 2.1 (Additive Identity), $0 + 0 = 0$, and by Fact 1 $a \cdot (0 + 0) = a \cdot 0$. Then, by Axiom 3 (Distributivity), $a \cdot 0 + a \cdot 0 = a \cdot 0$. By Fact 1, $-(a \cdot 0) + (a \cdot 0 + a \cdot 0) = -(a \cdot 0) + a \cdot 0$. We arrange the equation with Axiom 2 (Associativity) and Axiom 1 (Commutativity), deriving $a \cdot 0 + (a \cdot 0 + (-(a \cdot 0))) = a \cdot 0 + (-(a \cdot 0))$. Then, by Axiom 5 (Additive Inverse), $a \cdot 0 + 0 = 0$. Now, by Axiom 4 (Additive Identity), $a \cdot 0 = 0$. □

Lemma 6. *For all $a \in \mathbb{Z}$, $-a = (-1) \cdot a$.*

Proof. Let $a \in \mathbb{Z}$. Notice, by Axiom 5 (Additive Inverse), $1 + (-1) = 0$. By Fact 2, $a \cdot (1 + (-1)) = a \cdot 0$ which can be rewritten as $a \cdot 1 + a \cdot (-1) = a \cdot 0$ because (2.1 Distributivity). This evaluates to $a + a \cdot (-1) = a \cdot 0$ due to (2.1 Multiplicative Identity) and then to $a + a \cdot (-1) = 0$ because of (Lemma 5). Afterwards, we add to both sides, $-a + (a + a \cdot (-1)) = -a + 0$(2.1.1 Logic) which gives us $-a + (a + a \cdot (-1)) = -a$ by (2.1 Additive Identity). This equation can be regrouped as, $(-a + a) + a \cdot (-1) = -a$ by (2.1 Associativity) and then $(-1) \cdot a + (a + (-a)) = -a$ by (2.1 Commutativity). It evaluates to $(-1) \cdot a + 0 = -a$ by (2.1 Additive Inverse) and finally giving us $(-1) \cdot a = -a$ from (2.1 Additive Identity). □

Corollary 2. $0 = -0$.

Proof. Notice, $-0 \overset{\text{(Lemma 6)}}{=} (-1) \cdot 0 \overset{\text{(Lemma 5)}}{=} 0$. □

Lemma 8. *For all $a, b \in \mathbb{Z}$, $-(ab) = (-a)b = a(-b)$.*

Proof. Let $a, b \in \mathbb{Z}$. Notice, that $(-a)b = ((-1) \cdot a)b$ from (Lemma 6) which is the equivalent of $(-a)b = (-1)(ab)$ by (2.1 Associativity). This gives us $(-a)b = -(ab)$ by (Lemma 6). Similarly, $a(-b) = a((-1) \cdot b) = a(b \cdot (-1)) = (ab)(-1) = (-1)(ab) = -(ab)$ by (Lemma 6), (2.1 Commutativity), (2.1 Associativity), (2.1 Commutativity), (Lemma 6) respectively. □

Lemma 9. *For all $a, b \in \mathbb{Z}$, $(-a)(-b) = ab$.*

Proof. Let $a, b \in \mathbb{Z}$. Notice, $-(-a) = a$ by (Lemma 7). Then we multiply both sides by, $(-(-a))(-b) = a(-b)$ (2.1.1 Logic) which is simplified to $(-(-a))(-b) = -(ab)$ due to (Lemma 8). Then rewrite it as, $((-1)(-a))(-b) = (-1)(ab)$ by following (Lemma 6) which can also be rewritten as $(-1)((-a)(-b)) = (-1)(ab)$ by (2.1 Associativity). We then multiply both sides by, $(-1)((-1)((-a)(-b))) = (-1)((-1)(ab))$ (2.1.1 Logic). This is rewritten as $((-1)(-1))((-a)(-b)) = ((-1)(-1))(ab)$ because of (2.1 Associativity). It

then evaluates to $(-(-1))((-a)(-b)) = (-(-1))(ab)$ by (Lemma 6) and further simplified as $(1)((-a)(-b)) = (1)(ab)$ due to (Lemma 7). This is the equivalent of $(-a)(-b) = ab$ by (2.1 Multiplicative Identity). □

Lemma 11. *For all $a, b, c \in \mathbb{Z}$, $a - (b - c) = (a - b) + c$.*

Proof. Let $a, b, c \in \mathbb{Z}$. Notice, $a-(b-c) = a+(-(b+(-c)))$ (Definition 2) $= a+((-1)(b+(-1)\cdot c))$ (Lemma 6) $= a+((-1)\cdot b+(-1)\cdot((-1)\cdot c))$ (Axiom 3) $= (a+(-1)\cdot b)+((-1)\cdot(-1))\cdot c$ (Axiom 2) $= (a+(-1)\cdot b)+(1\cdot 1)\cdot c$ (Lemma 9) $= (a+(-1)\cdot b)+c\cdot(1\cdot 1)$ (Lemma 1) $= (a+(-1)\cdot b)+c$ (Axiom 6) $= (a+(-b))+c$ (Lemma 6) $= (a-b)+c$ (Definition 2) Hence, for all $a, b, c \in \mathbb{Z}$, $a - (b - c) = (a - b) + c$. □

Lemma 12. *For all $a, b, c \in \mathbb{Z}$, $a(b - c) = ab - ac$.*

Proof. Let $a, b, c \in \mathbb{Z}$. Put $d = -c$, then by Corollary 3, $d \in \mathbb{Z}$. By Definition 2, we are essentially showing $a = b \iff a + d = b + d$. By Fact 1 and Lemma 3, both directions are true. □

Lemma 13. *For all $a, b, c \in \mathbb{Z}$, $a = b \iff a - c = b - c$.*

Proof. Let $a, b, c \in \mathbb{Z}$. Put $d = -c$, then by Corollary 3, $d \in \mathbb{Z}$. By the Definition 2, we are essentially showing $a = b \iff a + d = b + d$. By Fact 1 and Lemma 3, both directions are true. □

Lemma 18. *For all $a, b \in Z, c \in \mathbb{Z}^+, a < b \iff ac < bc$.*

Proof. Assume for the sake of contrapositive that $ac > bc$, this means that $ac - bc > 0$. We can rewrite it as $c(a - b) > 0$. This means we have two cases of either both c and $a - b$ being positive or both or negative(but we don't consider the negative case because $c \in \mathbb{Z}^+$). In the case where both integers are positive, we have $c > 0$ and $a - b > 0$. $a - b > 0$ can be rewritten as $a > b$ since you add b to both sides. This means that $a < b$ isn't possible. □

Lemma 19. *For all $a, b \in Z, c \in \mathbb{Z}^-, a < b \iff ac > bc$.*

Proof. Assume for the sake of contrapositive that $ac < bc$, this means that $0 < bc - ac$. We can rewrite it as $0 < c(b - a)$. This means we have two cases of either both c and $b - a$ being positive or both or negative(but we don't consider the positive case because $c \in \mathbb{Z}^-$). In the case where both integers are negative, we have $c < 0$ and $b - a < 0$. $b - a < 0$ can be rewritten as $b < a$ since you add a to both sides. This means that $a < b$ isn't possible. □

6.2. Subsequent Properties of Order Axioms

Lemma 31. *For all $a, b \in \mathbb{Z}$, if $ab = 0$, then either $a = 0$ or $b = 0$.*

Proof. We prove the contrapositive. Suppose $a \neq 0$, $b \neq 0$. Then there are four cases: either $a > 0$, $b > 0$ and Suppose for contradiction that both of a, $b \in \mathbb{Z}$. However this is impossible since by 2.3, Multiplicative Closure, if $a, b \in \mathbb{Z} \implies ab \in \mathbb{Z}$ however, $0 \notin \mathbb{Z}^+$. Therefore, at least one of a, b must be $\in \mathbb{Z}^+$. Since $a \neq b$, $a - b \neq 0$. Therefore, $a - b \in \mathbb{Z}^+$ (WLOG). Therefore, $c = 0$ (from 2.1 (Zero)). Then it follows: $a - b = 0$, and from 2.1 (Additive Inverse) $a = b$ as desired. □

Lemma 32. *For all $a, b, c \in \mathbb{Z}$ where $c \neq 0$, if $ac = bc$, then $a = b$.*

Proof. We prove the contrapositive. Let $a, b, c \in \mathbb{Z}$ such that $c \neq 0$. Suppose $a \neq b$, then for $k \in \mathbb{Z}$ where $k \neq 0$, $a = b + k$. Notice, $ac = (b + k)c \overset{\text{2.1 Distributivity}}{=} bk + kc$. By Lemma x, since $k \neq 0$, $c \neq 0$, $kc \neq 0$, so $ac \neq bc$. □