The Fundamental Theorem of Arithmetic

Matthew Li, Evelyn Song

Contents

1. Introduction

The Fundamental Theorem of Arithmetic (FTA), also known as the Unique Factorization Theorem, is a crucial result in elementary number theory. It states that every integer greater than 1 can be expressed as a unique product of prime numbers.

The Fundamental Theorem of Arithmetic is often taken for granted. For example, the idea of a prime factorization, which is often taught early in school, relies on the FTA. Although the statement seems intuitively true, the proof is sophisticated and complex.

In this expository paper, we will prove the Fundamental Theorem of Arithmetic, beginning with the axiomatic description of the integers and introducing key lemmas that will eventually lead to a complete proof of the FTA.

2. Axioms

We begin by asking some basic questions. What is an integer? What operations can we do with the integers? What other properties do the integers have?

Definition 1 (Set of Integers)**.** An integer is an element of the set $\mathbb{Z}$. We call $\mathbb{Z}$ the set of integers.

Definition 2 (Binary Operation)**.** A binary operation is a mapping $f : X \times X \to X$ where X is a set.

Example 1 (Addition and Multiplication are Binary Operations)**.** Addition and multiplication are very common binary operations. The former is typically denoted with the symbol $+$ while the latter is denoted with the symbol $\times$. Note that there are many other ways to represent multiplication. For example, all of the following mean the same thing: $a \times b$, $a \cdot b$ and ab.

Now, we will introduce the axioms that gives $\mathbb{Z}$ its unique properties and are the foundation for all the following results.

Definition 3 (Ring Axioms)**.** The set of integers is a ring equipped with two binary operations, addition and multiplication, with the following properties.

1. Closure Under Addition and Multiplication – If x and y are in $\mathbb{Z}$, then $x+y$ and $x \cdot y$ are also in $\mathbb{Z}$.

2. Associativity of Addition and Multiplication – If x, y, and z are in $\mathbb{Z}$, then the following are true.

$$(x \cdot y) \cdot z = x \cdot (y \cdot z) \quad \text{and}$$
$$(x + y) + z = x + (y + z)$$

3. Commutativity of Addition and Multiplication – If x and y are in $\mathbb{Z}$, then the following are true.

$$x \cdot y = y \cdot x \quad \text{and}$$
$$x + y = y + x$$

4. Existence of a Additive and Multiplicative Identity – We typically denote the additive identity as 0 and the multiplicative identity as 1. If a is in $\mathbb{Z}$, then the following are true.

$$a \cdot 1 = 1 \cdot a = a \quad \text{and}$$
$$a + 0 = 0 + a = a$$

5. Existence of Additive Inverses – For all elements a in $\mathbb{Z}$, there exists a element $-a$ such that

$$a + (-a) = 0$$

6. Distributivity – If x, y, and z are in $\mathbb{Z}$, then the following holds.

$$x \cdot (y + z) = x \cdot y + x \cdot z \quad \text{and}$$
$$(y + z) \cdot x = y \cdot x + z \cdot x$$

Now, we introduce some facts that are very often taken for granted while doing arithmetic. We will prove these facts very rigorously and these facts will be used freely in later sections.

Fact 1. *The multiplicative and additive identities are unique.*

Proof. We first show the additive identity is unique. For the sake of contradiction, assume there are two distinct additive identities that we will call 0_1 and 0_2. Consider the value of $0_1 + 0_2$. If we let 0_1 act like the identity, then $0_1 + 0_2 = 0_2$. On the other hand, if we let 0_2 act like the identity, then $0_1 + 0_2 = 0_1$. But, this implies $0_1 = 0_2$, which contradicts the assumption that they are distinct. Thus, additive inverses are unique.

Next we show the multiplicative identity is unique using a very similar approach. We assume for the sake of contradiction that there are two distinct multiplicative identities called 1_1 and 1_2. Then, we will have $1_1 \cdot 1_2 = 1_1$ and $1_1 \cdot 1_2 = 1_2$ if we let 1_2 and 1_1 be the multiplicative identity, respectively. But, this implies $1_1 = 1_2$, a contradiction. So multiplicative identities are also unique. □

Fact 2. *Given an integer a in $\mathbb{Z}$, we have $a \cdot 0 = 0$.*

Proof. From the definition of an additive identity, we have $0 + 0 = 0$. Multiplying both sides by a gives us $a(0 + 0) = a0$. From the distributive property, we may write $a0 + a0 = a0$. If we add the additive inverse of $a0$ to both sides, we get

$$-(a0) + a0 + a0 = -(a0) + a0$$
$$a0 = 0$$

which is what we wanted. □

Fact 3. *Given an integer a in $\mathbb{Z}$, then: $-(-a) = a$ and $-(ab) = (-a)(b) = a(-b)$. Moreover, $(-a)(-b) = ab$ and $-a = (-1) \cdot a$.*

Proof. We first show $-(-a) = a$. We know $-a + -(-a) = 0$ is true due to the definition of additive inverses. Add a to both sides to get $-(-a) = a$, as desired.

Now we show $(-ab) = (-a)b$. From Fact 2, $a0 = 0$. Now, by definition of additive inverses, $a(b + (-b)) = 0$ and $ab + a(-b) = 0$ by distributivity. Finally, adding the additive inverse of ab to both sides gives us $a(-b) = -(ab)$, as desired. Showing $(-ab) = a(-b)$ is analogous.

Next, we show $(-a)(-b) = ab$. We know $(-a)0 = 0$ from Fact 2 and by definition of additive inverses, we can rewrite this to get $(-a)(b + (-b)) = 0$. From distributive property, we get $(-a)b + (-a)(-b) = 0$ which is also $-(ab) + (-a)(-b) = 0$ from the previous property. Then, adding ab to both sides gives $(-a)(-b) = ab$, as desired.

Finally, we show $-a = (-1)a$. From Fact 2, we have $a0 = 0$ so $a(1 + (-1)) = 0$ as well. By distributive and adding the additive inverse of a to both sides, we get $a(-1) = -a$, as desired. □

Fact 4. *Let a and b be integers. If $ab = 0$, then $a = 0$ or $b = 0$.*

Proof. For the sake of contradiction, assume neither of a nor b are 0. Then, we will do casework on the sign of a and b. If a and b are both positive integers, then $ab \in \mathbb{Z}^+$. But, this violates trichotomy since $ab = 0$. Now, suppose one of a or b is positive and the other is negative. Without loss of generality, we may assume a is positive and b is negative. So a and $-b$ are both in $\mathbb{Z}^+$. Then, $a(-b) = -ab \in \mathbb{Z}^+$ which violates trichotomy since $ab = 0$. Now, the final case is when both a and b are negative integers. Then, $-a$ and $-b$ are in $\mathbb{Z}+$ so $(-a)(-b) = ab \in \mathbb{Z}^+$, which also violates trichotomy. Since we have a contradiction in all cases, we must have at least one of a or b equal to 0, as desired. □

Corollary 5. *Let a, b and b' be integers with $a \neq 0$. If $ab = ab'$, then $b = b'$.*

Proof. If $ab = ab'$, then $a(b - b') = 0$. By the previous fact, at least one of $a = 0$ or $b - b' = 0$ are zero. But, $a \neq 0$ so $b - b'$ must be zero. Then, $b = b'$, as desired. □

The next set of axioms is what allows us to observe inequalities in $\mathbb{Z}$.

Definition 4 (Order Axioms)**.** We define $\mathbb{Z}^+$ to be a nonempty subset of $\mathbb{Z}$ and we call it the set of positive integers. The positive integers have the following properties.

1. Additive and Multiplicative Closure – If a and b are positive integers, then $a + b$ and ab are also positive integers

2. Trichotomy – For all integers a exactly one of the following holds: a is a positive integer, a is zero, or $-a$ is a positive integer.

If $a \in \mathbb{Z}^+$ then we say a is a positive integer. If $-a \in \mathbb{Z}^+$ then we say a is a negative integer. We also say that $a < b$ for integers a and b if $b - a \in \mathbb{Z}^+$. We also define $a \leq b$ if either $a < b$ or $a = b$. We also use $a > b$ if $b < a$ and we define $a \geq b$ if $b \leq a$.

Appealing to trichotomy in proofs can be a very powerful technique, especially if we want to prove some integer is in $\mathbb{Z}^+$ or is 0.

Fact 6. *For integers a and b, exactly one of the following is true: $a < b$, $a = b$, or $b < a$.*

Proof. By Trichotomy, the value $a - b$ satisfies exactly one of the following: $a - b \in \mathbb{Z}^+$, $a - b = 0$, or $-(a - b) \in \mathbb{Z}^+$. If $a - b \in bZ^+$, by our definition of less than, we have $b < a$. If $a - b = 0$, then $a = b$. Finally, if $-(a - b) \in \mathbb{Z}^+$, we have

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

So $b + (-a) \in \mathbb{Z}^+$ and by definition of less than, we have $a < b$. Thus, we have shown that exactly one of $a < b$, $a = b$, and $b < a$ is true. □

Fact 7. *For integers a, b, x and y, if $a \leq b$ and $x \leq y$, then $a + x \leq b + y$.*

Proof. If $a \leq b$ and $x \leq y$, then the following are true by definition: $b - a \in \mathbb{Z}^+ \cup \{0\}$ and $y - x \in \mathbb{Z}^+ \cup \{0\}$. Since $\mathbb{Z}^+$ is closed under addition and multiplication, we can show $\mathbb{Z}^+ \cup \{0\}$ is also closed under addition and multiplication. If $a \in \mathbb{Z}^+ \cup \{0\}$, clearly $a + 0 = a$ is also in $\mathbb{Z}^+ \cup \{0\}$. So, $b - a + y - x = b + y - (a + x)$ is in $\mathbb{Z}^+ \cup \{0\}$ and by definition of $\leq$, we have $a + x \leq b + y$, as desired. □

Fact 8. *If a and b are integers with $a \leq b$ and c is a nonnegative integer, then $ac \leq bc$. If c is a negative integer, then $ac \geq bc$.*

Proof. If $a \leq b$, then $b - a \in \mathbb{Z}^+ \cup \{0\}$, by definition. If c is nonnegative, then $c(b - a) \in \mathbb{Z}^+ \cup \{0\}$ since we have already shown in the previous proof that $\mathbb{Z}^+ \cup \{0\}$ is also closed under addition and multiplication. Then, by definition, $ac \leq bc$. Now, if c is negative, $-c \in \mathbb{Z}^+$ so it is also in $\mathbb{Z}^+ \cup \{0\}$. Then, $-c(b - a) \in \mathbb{Z}^+ \cup \{0\}$ or $ac \geq bc$, as desired. □

Now, we introduce an extremely important axiom known as the Well-Ordering Principle.

Definition 5 (Well-Ordering Principle)**.** For any subset S of $\mathbb{Z}^+$, there exists a least element l in S. In other words, for all elements x in S, we have $l \leq x$.

Lemma 9 (OLE)**.** *One is the least element of $\mathbb{Z}^+$*

Proof. First, we must show $1 \in \mathbb{Z}^+$. To do this, we use casework based on trichotomy. If $-1 \in \mathbb{Z}^+$, then $-1 \cdot -1 = 1$ is also in $\mathbb{Z}^+$, which violates trichotomy. Now, we show $1 \neq 0$. For the sake of

contradiction, assume $1 = 0$. Then, consider an arbitrary integer a. We have the following.

$$a0 = a0$$
$$a1 = 0$$
$$a = 0$$

This shows that any integer in $\mathbb{Z}$ is 0, so all elements of $\mathbb{Z}$ are 0. However, we defined $\mathbb{Z}^+$ to be a nonempty subset of $\mathbb{Z}$ so zero will be in $\mathbb{Z}^+$. This violates trichotomy, so we must have $1 \neq 0$. Then, 1 must be in $\mathbb{Z}^+$, by trichotomy.

Now, we know by the Well-Ordering Principle that there is a least element l of $\mathbb{Z}^+$. Then $l \leq 1$ by definition of a least element. For the sake of contradiction, assume $l < 1$. Then $l \cdot l < l$, which is a contradiction since we assumed l is the least element. Thus, $l = 1$, as we desired. □

Corollary 10 (NIBZO)**.** *There is no integer between* 0 *and* 1*. In other words, there is no integer* a *such that* $0 < a < 1$*.*

Proof. For the sake of contradiction, there is an integer a satisfying $0 < a < 1$. Then, a is a positive integer by definition but this contradicts the fact that 1 is the least element of $\mathbb{Z}^+$. So, there are no integers betweeen 0 and 1, as desired. □

Remark 1. In the later sections, the Well-Ordering Principle will be used frequently, sometimes acting as a replacement for mathematical induction. The general format of a Well-Ordering Principle proof that mimics induction is as follows. Given a certain property we want to be true for all positive integers, we define a set $S \subseteq \mathbb{Z}^+$ where all elements in S do not satisfy the property. We assume for the sake of contradiction that S is nonempty and then we can apply the Well-Ordering Principle to say there is some least element l in S. Then, we do a step similar to showing the base case is true for induction. We show that $1 \neq S$ and then, by Lemma 9, we say $l > 1$ or $l - 1 \in \mathbb{Z}^+$. Then, since we know $l - 1 < l$ and it is positive, we know the property holds for the positive integer $l - 1$. Then, we usually do some algebraic manipulation using the fact it is true for $l - 1$ to show it is also true for l. This will leave us with a contradiction which means S is empty. Thus, we are finished since we have showed the property holds for all positive integers.

3. Divisibility and Primes

After establishing some basic facts about the integers, we will define a notion of divisibility and what it means to be a prime. We will prove several properties of divisibility that will be used frequently later on.

Definition 6 (Divisibility)**.** We say that a divides b for integers a and b if there exists an integer k such that $b = ak$. We usually use the notation $a \mid b$ to say a divides b. We also use the notation $a \nmid b$ to say that a does not divide b.

Fact 11. *Let d, a, and b be integers. If $d \mid b$ and $d \mid a$, then $d \mid ax + by$, where x and y are also integers.*

Proof. Since $d \mid b$, there exists an integer k_1, such that $b = k_1 d$. Also, since $d \mid a$, there exists an integer k_2, such that $a = k_2 d$. Then, consider $ax + by$.

$$\begin{aligned} ax + by &= (k_2 d)x + (k_1 d)y \\ &= d(k_2 x) + d(k_1 y) \\ &= d(k_2 x + k_1 y) \end{aligned}$$

Since k_1, x, k_2, and y are all integers, then $k_2 x + k_1 y$ is an integer as well. Thus, by definition, we have $d \mid ax + by$, as desired. □

Fact 12. *If $a \mid b$ and $b \mid c$, then $a \mid c$.*

Proof. Since $a \mid b$, there exists an integer n_1 such that $b = an_1$. Also, since $b \mid c$, there exists an integer n_2 such that $c = bn_2$. Then, we can substitute to get

$$\begin{aligned} c &= bn_2 \\ &= (an_1)n_2 \\ &= a(n_1 n_2) \\ &= an_3 \end{aligned}$$

Then, by definition, this implies $a \mid c$. □

Lemma 13. *For positive integers a and b, $a \mid b$ implies $a \leq b$*

Proof. Since $a \mid b$, there exists an integer k, such that $b = ak$. Now consider $b - a$, we have

$$\begin{aligned} b - a &= ak - a \\ &= a(k - 1) \end{aligned}$$

Thus, if we show $a(k-1) \in \mathbb{Z}^+ \cup \{0\}$, then $a \leq b$, by definition. Motivated by Trichotomy, we will do casework on the value of k. If $k - 1 = 0$, then $a(k-1) = 0$ which is in $\mathbb{Z}^+ \cup \{0\}$, as desired. If $(k-1) \in \mathbb{Z}^+$, then by multiplicative closure of $\mathbb{Z}^+$, we have $a(k-1) \in \mathbb{Z}^+$, as desired. Now, note $-(k-1) \notin \mathbb{Z}^+$. To prove this, we assume for the sake of contradiction that $-(k-1) \in \mathbb{Z}^+$. Then,

by definition, we have $k < 1$ and we can get a contradiction if $k \in \mathbb{Z}^+$ since 1 is the least element of $\mathbb{Z}^+$. To show $k \in \mathbb{Z}^+$, we will proceed with casework on k. If $k = 0$, then $b = ak = 0$ which violates trichotomy as $b \in \mathbb{Z}^+$. If $-k \in \mathbb{Z}^+$, then $b = -ak \in \mathbb{Z}^+$ which violates trichotomy as well since $ak \in \mathbb{Z}^+$. So k must be a positive integer. Thus, we have shown $a(k-1) \in \mathbb{Z}^+$ for all working cases of k and $a \leq b$, as desired. □

Now we will introduce what it means for an integer d to be the greatest common divisor of integers a and b. We will be using the greatest common divisor in later sections.

Definition 7. We say an integer d is the greatest common divisor of integers a and b if $d \mid a$ and $d \mid b$ and if there is another integer e such that $e \mid a$ and $e \mid b$, then $e \leq d$. We can represent this by writing $\gcd(a, b) = d$.

We will now build up some knowledge to define a prime.

Definition 8 (Unit)**.** Let R be an arbitrary ring. If an element a in R has an element b in R such that $a \cdot b = 1$, where $\cdot$ is an operation in R and 1 is the multiplicative identity, then a is a unit. We say that b is the multiplicative inverse of a and we can denote b as a^{-1}.

Corollary 14. *The integers* 1 *and* -1 *are the only units in* $\mathbb{Z}$*.*

Proof. Consider an element $a \in \mathbb{Z}$ and suppose it is a unit. So there exists an integer b such that $ab = 1$. Note that $a \neq 0$. Then, by trichotomy, either $a \in \mathbb{Z}^+$ or $-a \in \mathbb{Z}^+$. Consider the case where $a \in \mathbb{Z}^+$. We know $a \mid ab$ so $a \mid 1$. Then, by 13, we have $a \leq 1$. Since a is a positive integer and 1 is the least element, a must be 1. Otherwise, suppose $-a \in \mathbb{Z}^+$. We know $-a \mid ab$ so $-a \mid 1$. Then, by 13, $-a \leq 1$. So, by the same argument as the previous case, $-a = 1$ or $a = -1$. Thus, we have shown if a is a unit, the only possible values for it are 1 and -1, as desired. □

Definition 9 (Prime)**.** An integer p is a prime if it satisfies the following conditions.

1. If $p = ab$ for integers a and b, then exactly one of a or b is a unit.
2. p is not a unit.
3. p is a positive integer.

Fact 15. *Every positive integer other than* 1 *has a prime divisor.*

Proof. Consider the set S that is defined by $S = \{x \in \mathbb{Z}^+ \setminus \{1\} \mid x \text{ has no prime divisor}\}$. We assume for the sake of contradiction that this set is nonempty. Then, since S is a subset of $\mathbb{Z}^+$ and it is nonempty, from the Well-Ordering Principle, there is a least element l in S. Clearly, if l is prime, then we have an obvious contradiction since l is a prime divisor of itself. So, assume l is not prime. Then, we know $l = ab$, where a and b are integers that are not units. Then $a < l$ so $a \notin S$.

Then a has some prime divisor p. But we also know that $a \mid l$ so $p \mid l$. This contradicts the fact l has no prime divisor, so S is empty. Thus, all positive integers greater than 1 have a prime divisor, as desired. □

The next lemma we prove will be the first essential part in proving the Fundamental Theorem of Arithmetic. We will first prove the existence of a product of primes here and uniqueness will be done later.

Lemma 16. *Every positive integer other than* 1 *can be expressed as a product of primes. We consider a prime number itself to also be a product of primes.*

Proof. Consider the set $S = \{n \in \mathbb{Z}^+ \setminus \{1\} \mid n \text{ is not expressible as a product of primes}\}$. We assume for the sake of contradiction that this set is nonempty. Then, since S is a subset of $\mathbb{Z}^+$ and it is nonempty, from the Well-Ordering Principle, there is a least element l in S. Clearly, l should not be prime or else we have an obvious contradiction. So, assume l is not a prime. Then, consider $\frac{l}{p}$, where p is a prime divisor of l. We know $\frac{l}{p} < l$ so $\frac{l}{p} \notin S$ and thus, it can be expressed as a product of primes. Then, l can be expressed as $p \cdot$ the product of primes in $\frac{l}{p}$. So, l is also a product of primes which contradicts l being in S. Thus, S is empty and all positive integers greater than 1 can be expressed as a product of primes. □

4. Important Lemmas

In this section, we will prove several important results that will build up to the key component we need for proving uniqueness.

Definition 10 (Absolute Value)**.** We define the absolute value of an integer a to be

$$|a| = \begin{cases} a & a \in Z^+ \\ -a & -a \in Z^+ \\ a = 0 & a = 0 \end{cases}$$

Lemma 17 (Division Algorithm)**.** *If a and b are integers and $b \neq 0$, then there exists integers q and r such that $a = bq + r$ and $0 \leq r < |b|$.*

Proof. Suppose we are given integers a and b. We will casework based on the sign of b. If $b > 0$, let us define a set $S = \{n \in \mathbb{Z}^+ \cup \{0\} \mid n = a - bq\}$. Note that if $b \mid a$, then $a - bq = 0$. So, let's consider the case where $b \nmid a$ and restrict n to be the positive integers in our definition of S. We will now show that S is a nonempty set through casework. If $a > 0$, we can choose $q = 0$ which gives us $n = a$, so $n \in \mathbb{Z}^+$. If $a < 0$, choose $q = ab$. Then $n = a - b(ab) = a(1 - b^2)$. Now, consider the value of b. Since $b \neq 0$, by Corollary 10, we can have $b \geq 1$.

Fact 18. *We can extend Corollary 10 to say there are no integers satisfying* $-1 < x < 0$.

Proof. For the sake of contradiction, assume there is an integer x satisfying $-1 < x < 0$. We can add 1 to x which will result in the inequality $0 < x + 1 < 1$. However, this contradicts Corollary 10. Thus, there are no integers between -1 and 0, as desired. □

Then, using the previous fact and $b \neq 0$, we can also say $b \leq -1$. However, note that b cannot be 1 or -1 or else b will always divide a. So, we have $b > 1$ or $b < -1$. In either case, we will have $b^2 > 1$. Equivalently, we have $-b^2 < -1$ or $1 - b^2 < 0$. Then, $a(1 - b^2) > 0$, which shows n is in S, as we desired. Finally, note that a cannot be zero or else b will always divide a. Thus, we have shown S is nonempty. Since S is nonempty and is also a subset of $\mathbb{Z}^+$, by the Well-Ordering Principle, there is some least element r in S. Then, $r \geq 0$. For the sake of contradiction, assume $r \geq b$. Then

$$\begin{aligned} r - b &\geq 0 \\ a - bq - b &\geq 0 \\ a - b(q + 1) &\geq 0 \end{aligned}$$

But this contradicts the minimality of r. So we must have $0 \leq r < b$ when b is positive. Now, if b is negative, we wish to prove $a - bq < -b$ for some q. Let $b = -b'$, where b' is a positive integer. Then, if b' is positive, we know that $a - b'q < b'$. Then, let $q = -q'$. We will get $a + b'q' < b'$ and after substituting $b = -b'$ back in, we will get $a - bq' < -b$ which is what we wanted. □

Lemma 19 (Bézout's Lemma)**.** *Let* a *and* b *be integers, not both zero. Then, there exists integers* m *and* n *such that* $am + bn = \gcd(a, b)$.

Proof. Suppose we are given two integers a and b, not both zero. Consider the set $S = \{x \in \mathbb{Z}^+ \mid x = am + bn$, where m and n are integers$\}$. First, we will show that S is nonempty by doing casework on the values of a and b. We summarize our results in a table below.

	$a > 0$	$a < 0$	$a = 0$
$b > 0$	Choose $m = 1$ and $n = 0$	Choose $m = 0$ and $n = 1$	Choose $m = 0$ and $n = 1$
$b < 0$	Choose $m = 1$ and $n = 0$	Choose $m = -1$ and $n = 0$	Choose $m = 0$ and $n = -1$
$b = 0$	Choose $m = 1$ and $n = 0$	Choose $m = -1$ and $n = 0$	

Thus, S is nonempty and since S is also a subset of $\mathbb{Z}^+$, by the Well-Ordering Principle, there exists a least element that we will call d. We wish to show $d = \gcd(a, b)$ and we start by showing it's a common divisor. To prove that $d \mid a$, write $a = dq + r$, where q and r are integers using the

division algorithm and substitute $d = ax + by$ where x and y are also integers to get

$$a = q(ax + by) + r = aqx + bqy + r$$

We can rewrite this to get $a(1 - qx) + b(-qy) = r$ From the division algorithm we know that $0 \leq r < d$. However, if $r > 0$, then r will be in S since it is of the form $ax + by$ but this contradicts d is the least element since $r < d$. So, we must have $r = 0$ which implies $a = dq$ or $d \mid a$, as desired. We can use a similar argument to show that $d \mid b$ so d is indeed a common divisor. Now, consider a different common divisor d_1. By definition, $d_1 \mid a$ and $d_1 \mid b$ so d_1 also divides linear combinations of a and b; namely, $d_1 \mid ax + by$ or $d_1 \mid d$. So, $d_1 \leq d$ where d_1 is any common divisor of a and b so by definition, $\gcd(a, b) = d$. Thus, we have shown there exists integers m and n such that $am + bn = \gcd(a, b)$, as desired. □

Example 2. Find a pair of integers m and n such that $163m + 30n = 1$.

Solution. To begin with, since $\gcd(163, 30) = 1$, we know from Bézout's Lemma that there will be a solution. To convince ourselves that Bézout's Lemma is actually true, let us find the solution to this equation. We approach this problem by repeatedly applying the division algorithm in a systematic way.

$$163 = 30 \cdot 5 + 13 \tag{1}$$
$$30 = 13 \cdot 4 + 4 \tag{2}$$
$$13 = 4 \cdot 3 + 1 \tag{3}$$

Now, starting with (3), we will do a series of substitutions to get an expression at the end in the form of $163x + 30y = 1$. Rearrange the above equations to get

$$1 = 13 - 4 \cdot 3 \tag{4}$$
$$4 = 30 - 13 \cdot 4 \tag{5}$$
$$13 = 163 - 30 \cdot 5 \tag{6}$$

Now substitute (5) into (4)

$$\begin{aligned} 1 &= 13 - 3(30 - 13 \cdot 4) \\ &= -30 \cdot 3 + 13 \cdot 7 \end{aligned}$$

Substitute (6) into the new equation above to get

$$\begin{aligned} 1 &= -30 \cdot 3 + (163 - 30 \cdot 5) \cdot 7 \\ &= 167 \cdot 7 - 30 \cdot 38 \end{aligned}$$

Notice, we have found our exact solutions. If we take $m = 7$ and $n = -38$, we have $163m + 30n = 1$. Thus, we have found solutions, which is what Bézout's Lemma guaranteed. □

Remark 2. Realize that this repeated application of the division algorithm in a "systemic way" is simply the Euclidean Algorithm. We do not explore the Euclidean Algorithm since it is beyond the scope of this paper.

Lemma 20 (Fundamental Lemma)**.** *Let a, b, and c be integers. Then, if $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.*

Proof. If $\gcd(a, b) = 1$, by Bézout's Lemma, we have $am + bn = 1$ for some integers m and n. Multiply both sides by c to get $amc + bnc = c$. Since we know $a \mid bc$, we know $a \mid amc + bnc$ so $a \mid c$, as desired. □

Corollary 21 (Euclid's Lemma)**.** *Let p be a prime and let a and b be integers. If $p \mid ab$, then $p \mid a$ or $p \mid b$.*

Proof. We can do casework on the greatest common divisor of p and a. If $\gcd(a, p) \neq 1$, then $\gcd(a, p) = p$ since the only divisors of a prime are 1 and p. Then, clearly $p \mid a$. Otherwise, suppose $\gcd(a, p) = 1$. Then, by the Fundamental Lemma, $p \mid b$, so we are done. □

Lemma 22 (Generalized Euclid's Lemma)**.** *Let p be a prime and let a_1, a_2, ..., a_n be integers. If $p \mid a_1 \cdots a_n$, then p divides an a_i, where $1 \leq i \leq n$.*

Proof. Define a set

$$S = \{n \in \mathbb{Z}^+ \mid p \text{ is prime and } p \mid a_1 \cdots a_n \text{ but } p \text{ doesn't divide any } a_i\}$$

We assume for the sake of contradiction that S is nonempty. Then, by the Well-Ordering Principle, there is a least element l in S. We show that $l > 1$ by showing 1 is not in S. Clearly, if $p \mid a_1$, then $p \mid a_1$. So, by Lemma 9, $l > 1$, as desired. Then, $l - 1 \in \mathbb{Z}^+$ and $l - 1 < l$ so it is true that if $p \mid a_1 \cdots a_{l-1}$, then p divides one of the a_i. If we let $k = a_1 \cdots a_{l-1}$, consider $a_l \cdot k$. If $p \mid a_l \cdot k$, by Euclid's Lemma, either $p \mid a_l$ or $p \mid k$. But since $p \mid k$ implies p divides one of $a_1, \ldots, a_{l-1}$, this is equivalent to saying if $p \mid a_l \cdot k$, then p divides one of the a_i, where $1 \leq i \leq l$. However, this is a contradiction as it violates $l \in S$. So S is empty and the generalized Euclid's Lemma holds. □

5. Main Result

After starting at the very foundations of the integers itself, we have finally built enough knowledge to prove the Fundamental Theorem of Arithmetic. For our proof, we will be using Lemma 22 and Lemma 16.

Theorem 23 (Fundamental Theorem of Arithmetic)**.** *For any positive integer $n \neq 1$, n can be expressed uniquely as a product of primes. We define two products to be the same under rearrangement and under multiplication by a unit.*

Proof. We will define a set S where

$$S = \{n \in \mathbb{Z}^+ \setminus \{1\} \mid n \text{ can be expressed as a product of primes in at least 2 different ways}\}$$

For the sake of contradiction, assume this set is nonempty. Then, by the Well-Ordering Principle, there is a least element in S denoted by l. Suppose l has two distinct factorizations, as shown below.

$$\begin{aligned} l &= p_1 p_2 \cdots p_r \\ &= q_1 q_2 \cdots q_s, \end{aligned}$$

where $p_1, \ldots, p_r$ and $q_1, \ldots, q_s$ are all primes in $\mathbb{Z}$. Therefore, we know that $p_1 \mid q_1 q_2 \cdots q_s$. Since p_1 is a prime, by Lemma 22, $p_1 \mid q_i$ for some $1 \leq i \leq s$. Also, because p_1 and q_i are both primes, we must have $p_1 = q_i$ for $p_1 \mid q_i$ to be true. Without loss of generality, we can let q_i be q_1 since reorderings are the same. Then, we have

$$\begin{aligned} l &= p_1 p_2 \cdots p_r \\ &= q_1 q_2 \cdots q_s \\ &= p_1 q_2 \cdots q_s \end{aligned}$$

Then, consider the value of $k = \frac{l}{p_1}$. We have

$$k = p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s$$

So k has at least two different factorizations which implies that k is also in S. However, we know that $k = \frac{l}{p_1}$ so $k \mid l$ which implies that $k \leq l$. If $k = l$, then $p_1 = 1$ which is impossible as p_1 is a prime. So $k < l$ but this contradicts the assumption that l is the least element of S. Thus, S is empty and every positive integer that is not 1 can be expressed uniquely as a product of primes. □

With this theorem, we have shown that any positive integer n that is not 1 can be expressed

uniquely as $n = p_1 \cdots p_k$ where p_k are not necessarily distinct primes. However, we have not shown that n can be expressed uniquely as $n = p_1^{e_1} \cdots p_n^{e_n}$, where all of the p_i are distinct primes and all of the e_i are positive integers. This is usually the form we are familiar with and we usually call it the *canonical factorization* of n. We will now introduce some lemmas to prove that every positive integer not equal to 1 has a unique canonical factorization.

Lemma 24. *Consider a positive integer $n = p_1 \cdots p_k$, where $p_1, \ldots, p_k$ are not necessarily distinct primes. Then, there exists a maximal $e \in \mathbb{Z}^+$ such that $p_i^e \mid n$ for $1 \leq i \leq k$.*

Proof. Without loss of generalization, we can choose $p_i = p_1$ since reorderings are the same. Then, define a set S where $S = \{x \in \mathbb{Z}^+ \mid p_1^j \cdot x = n \text{ for some } i \in \mathbb{Z}^+\}$. Since $p_1 \mid n$, there exists a positive integer d such that $p_1 \cdot d = n$. So, S is a nonempty subset of $\mathbb{Z}^+$. Then, by the Well-Ordering Principle, there is a least element in S which we denote as l. Then, let $p_1^e \cdot l = n$. Now, we show that for any other $x \in S$ with $x \neq l$ and $p_1^k \cdot x = n$, we have $k < e$. For the sake of contradiction, assume we have $k > e$. Then, we have

$$\begin{aligned} n = p_1^k \cdot x &= p_1^e \cdot y \\ p_1^k \cdot x - p_1^e \cdot y &= 0 \\ p_1^e(p_1^{k-e} \cdot x - y) &= 0 \end{aligned}$$

Since $p_1 \neq 0$, we must have $p_1^{k-e} \cdot x - y = 0$. Then $p_1^{k-m_1} \cdot x = y$ which implies that $x \mid y$. Since $x \neq y$, we have $x < y$. However, this contradicts the minimality of y in S. So, $k < e$ for all $x > l$ where $p_1^k \cdot x = 1$ which shows e is the maximal element such that $p_1^e \mid n$, as desired. Since we can replacement p_1 with any other p_i, we are done. □

Now, we will prove that every positive integer other than 1 has a unique canonical factorization.

Theorem 25 (Unique Canonical Factorization)**.** *For any positive integer $n \neq 1$, n can be expressed in the form:*

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$$

where $p_1, p_2, \ldots, p_k$ are distinct primes, and $e_1, e_2, \ldots e_k$ are positive integers.

Proof. We first prove existsence. Begin by defining a set S where

$$S = \{n \in \mathbb{Z}^+ \setminus \{1\} \mid n = p_1 \cdots p_k \text{ but } n \text{ has no canonical factorization}$$

For the sake of contradiction, assume S is nonempty. By the Well-Ordering Principle, there exists a least element in S, which we will denote by l. Then, $l = p_1 \cdots p_k$ but it does not have a canonical factorization. By Lemma 24, there is a positive integer e_1 and a positive integer x such that $p_1^{e_1} \cdot x = l$

where $p_1 \nmid x$. We will casework on the value of x. If $x = 1$, then $l = p_1^{e_1}$, which contradicts $l \in S$. Now, notice from $p_1^{e_1} \cdot x = l$, we know that $x \mid l$ and so $x < l$. Then, if $x > 1$, this implies $x \notin S$. Therefore, x is expressible as

$$x = p_2^{e_2} p_3^{e_3} \cdots p_k^{e_k},$$

where $p_2, p_3, \ldots, p_k$ are distinct primes and $e_2, e_3, \ldots, e_k$ are positive integers. Since $l = p_1^{e_1} \cdot x$, we can substitute $x = p_2^{e_2} \cdots p_k^{e_k}$ to get

$$l = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

where $p_1, p_2, \cdots$ and p_k are distinct primes. This contradicts l being in S. Therefore, S must be empty and all positive integers not equal to 1 have a canonical factorization. Uniqueness follows directly from the Fundamental Theorem of Arithmetic. □

Example 3. The prime factorization of 3600 is $2^4 \cdot 3^2 \cdot 5^2$.

6. Conclusion

Looking back, we have successfully proved a crucial fact of number theory starting from the very foundations of the integers themselves. Using only the axioms, we proved several important lemmas that were key to our main proof. Some of the most important intermediate results showed the existence of such a factorization into a product of primes and also Euclid's Lemma, which allowed us to prove uniqueness. We also demonstrated that every positive integer that is not 1 has a canonical factorization as well, which is typically the form we consider when discussing prime factorization.

The Fundamental Theorem of Arithmetic is "fundamental" because of its importance in number theory. We will highlight a few applications where FTA is useful in this concluding section. For example, in number theory, there exists many arithmetic functions that can be defined on $\mathbb{Z}$. Some of the most well known ones are:

1. $\varphi(n)$: the number of positive integers x less than equal to n such that $\gcd(x, n) = 1$.
2. $\tau(n)$: the number of positive divisors of n
3. $\sigma(n)$: the sum of all positive divisors of n

Example 4. Evaluate $\varphi(12)$, $\tau(12)$, and $\sigma(12)$.

Solution. We can check that the only numbers x less than or equal to 12 that satisfy $\gcd(x, 12) = 1$ are $x \in \{1, 5, 7, 11\}$. So $\varphi(12) = 4$. We can also make a list of the prime divisors of 12 to find $\tau(12)$ and $\sigma(12)$. Doing so, we get set of positive of divisors of $12 = \{1, 2, 3, 4, 6, 12\}$. So, $\tau(12) = 6$ and $\sigma(12) = 28$. □

It turns out that by considering the prime factorization of a integer n, we can prove many interesting properties of these functions. For example, consider the following lemma.

Lemma 26. *If* $\gcd(a, b) = 1$*, then* $\varphi(ab) = \varphi(a)\varphi(b)$*,* $\tau(ab) = \tau(a)\tau(b)$*, and* $\sigma(ab) = \sigma(a)\sigma(b)$*. In other words, these functions are multiplicative.*

Also, consider the special case where an integer n is equal to p^e, where p is a prime and e is a positive integer. It turns out we can find a general formula for φ, τ, and σ when n is in this format.

Lemma 27. *If* $n = p^e$*, where* p *is prime and* e *is a positive integer, then* $\phi(n) = p^{e-1}(p-1)$*,* $\tau(n) = e + 1$*, and* $\sigma(n) = (1 + p + \cdots + p^e)$*.*

It turns out that if we know how to compute $\varphi(p^e)$ where p is a prime and we use fact that φ is multiplicative, then we can derive a general formula for φ using the Well-Ordering Principle. The same thing can also be done for τ and σ.

Aside from working with arithmetic functions, the idea of a unique factorization is also extremely important in other algebraic systems other than the set of integers. For example, we can show that every element in $\mathbb{Z}_p[x]$ or $\mathbb{Z}[i]$ has a unique factorization into primes. This leads to some interesting questions. Are there any other systems with this property? If so, are there any properties that these systems all satisfy that allows unique factorization to hold?