Celebration

Family 47: Ishwar Suriyaprakash, Eric Tang, Neel Kolhe

Summer 2022

§1 Introduction

In this "Celebration of Mathematics", we will prove that every number in $\mathbb{Z}$ except $1, 0, -1$ have a unique prime factorization.

Starting in Section 2, we will establish the Ring and Order axioms, as well as the Well Ordering Principle (WOP) that will be used to prove all further theorems. In the next section, some basic arithmetic properties will be established, such as the uniqueness of 0 in addition and 1 in multiplication, as well as other basic facts such as multiplication with 0. In section 4, more advanced definitions and notation will be introduced, such as product notation, as well as the definitions of prime and composite. Then, some facts about divisibility will be established. With the basics down, we then begin our proof of Bezout's lemma, which follows after the proof of the division algorithm. Then, using Bezout's, we quickly prove the fundamental lemma and then a generalization of the fundamental lemma. We then prove that all positive integers have a prime factorization by using the definition of primes and composites. Finally, by using the fact that a prime factorization exists for all positive n, and the generalized fundamental lemma, we prove that a unique prime factorization exists for all positive n. Then, we use this to show that there also exists a unique canonical prime factorization. Finally, we show that since there exists a unique canonical factorization for positive n where $n \neq 1$, it must also exist for all $-n$.

§2 Axioms

All variables used in the entire proof are in the ring $\mathbb{Z}$, in which the operations of addition $(+)$ and multiplication $(\cdot)$ are defined.

Axiom 2.1 (Closure)**.** For all $a, b \in \mathbb{Z}$, $a + b \in \mathbb{Z}$ and $ab \in \mathbb{Z}$.

Axiom 2.2 (Commutativity)**.** For all $a, b \in \mathbb{Z}$, $a + b = b + a$ and $a \cdot b = b \cdot a$.

Axiom 2.3 (Associativity)**.** For all $a, b, c \in \mathbb{Z}$, $a + (b + c) = (a + b) + c$ and $a(bc) = (ab)c$.

Axiom 2.4 (Additive Identity)**.** There exists an element $0 \in \mathbb{Z}$ such that, for all $a \in \mathbb{Z}$, $a + 0 = a$.

Axiom 2.5 (Additive Inverse)**.** For all $a \in \mathbb{Z}$, There exists an additive inverse $b \in \mathbb{Z}$ such that, for all $a \in \mathbb{Z}$, $a + b = 0$. We denote this additive inverse as $-a$.

Axiom 2.6 (Multiplicative Identity)**.** There exists an element $1 \in \mathbb{Z}$ such that, for all $a \in \mathbb{Z}$, $a \cdot 1 = a$.

Axiom 2.7 (Distributive Property)**.** For all $a, b, c \in \mathbb{Z}$, $a(b+c) = ab + ac$.

We will also need the *Order Axioms* to be able to compare elements in $\mathbb{Z}$. The *Order Axioms* define a nonempty set $P \subset \mathbb{Z}$, representing the positive integers, that satisfy the following properties.

Axiom 2.8 (Closure)**.** For all $a, b \in P$, $a + b \in P$ and $ab \in P$.

Axiom 2.9 (Nontriviality)**.** $0 \notin P$.

Definition 2.10 (Strict Comparison)**.** For all $a \in \mathbb{Z}$, define $a > 0$, or alternatively $0 < a$, to mean that $a \in P$. Furthermore, for all $a, b \in \mathbb{Z}$, $a > b$ is equivalent to the statement $a + (-b) > 0$, or that there exists $k \in P$ such that $a = b + k$. Similarly, $a < b$ is equivalent to the statement $0 < b + (-a)$, or that there exists $k \in P$ such that $a + k = b$.

Axiom 2.11 (Trichotomy)**.** For all $a \in \mathbb{Z}$, define $0 < a$ to mean that $a \in P$. Either $a > 0$, $a = 0$, or $a < 0$.

Definition 2.12 (Comparison)**.** For all $a \in \mathbb{Z}$, define $a \geq 0$, or alternatively $0 \leq a$, to mean that $a \in P \cup \{0\}$. Using the Strict Comparison definition, it can be proven that, for all $a, b \in \mathbb{Z}$, $a \geq b$ is equivalent to $a + (-b) \geq 0$, or that there exists $k \in P \cup \{0\}$ such that $a = b + k$, and $a \leq b$ is equivalent to $0 \leq b + (-a)$, or that there exists $k \in P \cup \{0\}$ such that $a + k = b$.

In this exposition, P will be used interchangeably with $\mathbb{Z}^+$, and $P \cup \{0\}$ with $\mathbb{Z}^{0+}$.

One other axiom that doesn't necessarily follow from the ring axioms or the order axioms but is crucial in proving UFT for $\mathbb{Z}$ is the *Well Ordering Principle* (WOP).

Axiom 2.13 (WOP)**.** For any nonempty set of positive integers, there exists a least element in the set.

This axiom gives a strong notion of order to the integers, more than what the order axioms can give. It allows us to define functions like $gcd(a, b)$ and $lcm(a, b)$, which both require the concept of "absolute greatest" or "absolute least". It also will be used commonly in proofs by contradiction to prove properties for all elements in $\mathbb{Z}$.

§3 Techniques

In these proofs, we will be deriving basic principles using the ring axioms and order axioms which we will be using often later on in this paper.

Theorem 3.1

$a + b = a + b' \implies b = b'$

Proof. We know $\exists -a$ such that $a + (-a) = 0$ by additive inverses. Rearranging our original equation:

$$b + a = b' + a$$

Adding $-a$ to both sides,

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

Using Associative property:

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

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

$$b + 0 = b' + 0$$

By the Additive identity definition:

$$b' = b.$$

□

Theorem 3.2

$a = -(-a)$

Proof. By additive inverses:

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

Commuting:

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

We also know by additive inverses:

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

Substituting:

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

From Theorem 3.1:

$$-(-a) = a.$$

□

Theorem 3.3

$a \cdot 0 = 0$

Proof. By Distributive Property:

$$a(0 + b) = a \cdot 0 + a \cdot b$$

Since $0 + b = b$ by the additive identity, substituting:

$$a(b) = a \cdot 0 + a \cdot b$$

Commuting:

$$a \cdot b = a \cdot b + a \cdot 0$$

Using $a \cdot b = a \cdot b + 0$ and substituting:

$$a \cdot b + 0 = a \cdot b + a \cdot 0$$

From Theorem 3.1, we get:

$$0 = a \cdot 0$$

□

Theorem 3.4
$-(ab) = a(-b)$

Proof. By additive inverses:

$$b + (-b) = 0$$

By Theorem 3.5:

$$a \cdot 0 = 0$$

Substituting:

$$a \cdot (b + (-b)) = 0$$

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

By additive inverses:

$$ab + (-(ab)) = 0$$

Substituting:

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

From Theorem 3.1:

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

□

Theorem 3.5
$ab = 0 \implies a = 0$ or $b = 0$

Proof. We proceed with proof by contradiction. Assume $a, b \neq 0$. Then, either $a > 0$ or $a < 0$ and either $b > 0$ or $b < 0$ by Trichotomy from the *Order Axioms*. We consider 4 cases in total:

Case 1: $a, b > 0$

Since $a, b > 0$, we have that

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

By Closure from the *Order Axioms*:

$$ab \in \mathbb{Z}^+ \implies ab > 0$$

By Trichotomy from the *Order Axioms*:

$$ab \neq 0.$$

Case 2: $a > 0, b < 0$

Since $b < 0$, we have by the Comparison definition that

$$0 < 0 + (-b) \implies 0 < -b.$$

By Theorem 3.4, we have

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

Since $a, (-b) \in \mathbb{Z}^+$, we have by Closure:

$$a(-b) = -(ab) \in \mathbb{Z}^+ \implies 0 < -(ab)$$

By the Comparison definition:

$$ab < 0$$

By Trichotomy:

$$ab \neq 0.$$

Case 3: $a < 0, b > 0$

Since $a < 0$, we have by the Comparison definition that

$$0 < 0 + (-a) \implies 0 < -a.$$

By Theorem 3.4, we have

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

Since $(-a), b \in \mathbb{Z}^+$, we have by Closure:

$$(-a)b = -(ab) \in \mathbb{Z}^+ \implies 0 < -(ab)$$

By the Comparison definition:

$$ab < 0$$

By Trichotomy:

$$ab \neq 0.$$

Case 4: $a < 0, b < 0$

Since $a < 0$ and $b < 0$, we have by the Comparison definition that

$$0 < 0 + (-a) \implies 0 < -a$$

and

$$0 < 0 + (-b) \implies 0 < -b.$$

By Theorem 3.4, we have

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

Since $(-a), (-b) \in \mathbb{Z}^+$, we have by Closure:

$$(-a)(-b) = ab \in \mathbb{Z}^+ \implies 0 < ab$$

By Trichotomy:

$$ab \neq 0.$$

Thus, we have shown □

Theorem 3.6

For all $a, b \in \mathbb{Z}$, if $a \neq 0$ and $ab = ab'$, then $b = b'$

Proof. Subtracting ab':

$$ab - ab' = ab' - ab'$$
$$ab - ab' = 0$$
$$a(b - b') = 0$$

From Theorem 3.5, and since $a \neq 0$:

$$b - b' = 0$$
$$b = b'$$

□

Theorem 3.7

For all $x, y, a, b \in \mathbb{Z}$, if $a < x$ and $b < y$, then $a + b < x + y$.

Proof. By the Comparison definition, there exists $k, l \in \mathbb{Z}^+$ such that

$$x = a + k$$

$$y = b + l.$$

Adding:

$$x + y = a + b + k + l$$

By Closure:

$$k + l \in \mathbb{Z}^+$$

By Associativity:

$$(x + y) = (a + b) + (k + l)$$

By the Comparison definition:

$$x + y > a + b.$$

□

Theorem 3.8

For all $a, x, b, y \in \mathbb{Z}^+$, if $a < b$ and $x < y$, $ax < by$.

Proof. By the Comparison definition, there exists $k, l \in \mathbb{Z}^+$ such that

$$b = a + k$$

$$y = x + k$$

Multiplying gets us:

$$by = (a + k)(x + l)$$

Distributing gets us:

$$by = ax + al + xk + kl$$

By Closure, $al, xk, kl \in \mathbb{Z}^+$. Then, by Closure again:

$$al + xk + kl \in \mathbb{Z}^+$$

By the Comparison definition:

$$by > ax.$$

□

Theorem 3.9 (NIBZO)

There are no positive integers between 0 and 1.

Proof. Let $S = \{x \mid 0 < x < 1\}$ Assume for the sake of contradiction that $S \neq \emptyset$. Then, by WOP, S will have a minimum, m. We will construct an element lesser than m between 0 and 1, which will cause a contradiction. We know that

$$0 < m < 1$$

Using Theorem 3.8 and multiplying by m:

$$0 \cdot m < m \cdot m < 1 \cdot m$$

$$0 < m \cdot m < m$$

Including the fact that $m < 1$:

$$0 < m \cdot m < m < 1$$

So, we have found another integer, $m \cdot m$, between 0 and 1 that is less than m, which contradicts the minimality of m. Therefore, S must be empty.

Corollary 3.10

For all $x, y \in \mathbb{Z}$, if $x > y$, then $x \geq y + 1$.

We leave the proof of this as an exercise to the reader. (Hint: use NIBZO)

□

§4 Additional Definitions and Notation

All variables used in the entire proof are in $\mathbb{Z}$. If any number is expressed as a variable, assume it's a number $n \in \mathbb{Z}$.

Definition 4.1 (Divisibility)**.** We say a number $a \mid b$ or "a divides b" if there exists some $k \in \mathbb{Z}$ such that $ak = b$.

Definition 4.2. $[n]$ denotes the set $\{k \mid k \in \mathbb{Z}^+, 1 \leq k \leq n\}$.

Definition 4.3. $(a_i)_{i=1}^k$ denotes a sequence of k elements starting from a_1 and ending with a_k.

Definition 4.4. Let $\prod_{i=1}^k a_i$ be defined as follows:

1. $\prod_{i=1}^1 a_i = a_1$
2. $\prod_{i=1}^{k+1} a_i = a_{k+1} \cdot \prod_{i=1}^k a_i$

Theorem 4.5

For all $k \in \mathbb{Z}^+$, if a_i is defined for all $i \in [k]$, then $\prod_{i=1}^k a_i$ is defined.

Proof. Let $S = \{k \mid k \in \mathbb{Z}^+, \prod_{i=1}^k a_i \text{ is not defined}\}$. We know that the ending index $1 \notin S$ because of (1) in Definition 4.4.

Assume for the sake of contradiction that S is nonempty. By WOP, there exists a minimum element $m \in S$. Since $m \geq 1$ and m cannot be equal to 1, $m \geq 2$.

Now, let's consider the ending index $m - 1$. Since $m \geq 2$, we know that $m - 1 \geq 1$, so $m - 1$ is a valid ending index. Also, using (2) in Definition 4.4, we can define $\prod_{i=1}^m a_i = a_m \cdot \prod_{i=1}^{m-1} a_i$. But, because $m \in S$, this should not be defined for m, which is a contradiction. Hence, S must be empty. □

Definition 4.6. Let $\prod_{i=1;i\neq j}^{k} a_i$ be defined as the product $\prod_{i=1}^{k-1} b_i$ such that, for $i < j$, $b_i = a_i$, and, for $i \geq j$, $b_i = a_{i+1}$.

§5 Divisibility

Theorem 5.1

$a \mid a$ for all a.

Proof.

$$a = 1 \cdot a$$

By definition, $\exists k = 1$ such that $a \cdot k = a$, so $a \mid a$. □

Theorem 5.2

$a \mid b \implies a \mid bc$

Proof. There exists $k \in \mathbb{Z}$ such that

$$b = ak$$

Multiplying by c gets us:

$$bc = akc = a(kc)$$

By Closure, $kc \in \mathbb{Z}$. Thus, $a \mid bc$. □

Theorem 5.3

If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof. Since $a \mid b$ and $b \mid c$, there exist $k, l \in \mathbb{Z}$ such that

$$b = ka$$

$$c = lb$$

Substituting $b = ka$ into the second equation, we get

$$c = l(ka)$$

$$c = (lk)a$$

By Closure, $lk \in \mathbb{Z}$. Thus, $a \mid c$. □

Theorem 5.4

For all $a, b \in \mathbb{Z}^+$, if there exists $k \in \mathbb{Z}^+$ such that $k > 1$ and $ak = b$, then $a < b$.

Proof. We get that

$$ak = b$$
$$a(k + 1 + (-1)) = b$$
$$a(1 + k + (-1)) = b$$
$$a + a(k + (-1)) = b$$

Since $k > 1$, we have that $k + (-1) > 0$, so $k + (-1) \in \mathbb{Z}^+$. Then, by Closure of $\mathbb{Z}^+$, $a(k + (-1)) \in \mathbb{Z}^+$. Using the fact that $a + a(k + (-1)) = b$, we get by the Comparison definition that

$$a \leq b.$$

□

Theorem 5.5

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

Proof. Since $a \mid b$, there exists $k \in \mathbb{Z}^+$ such that

$$b = ka$$

Since $k \in \mathbb{Z}^+$, $k \not< 1$ because of NIBZO, so, by Trichotomy, either $k > 1$ or $k = 1$.
The first case is taken care of in Theorem 5.4.
In the second case, $b = ak = a \cdot 1 = a$. □

Theorem 5.6

For $a, b, d \in \mathbb{Z}$, if $d \mid a$ and $d \mid b$, then, for all $r, s \in \mathbb{Z}$, $d \mid (ar + bs)$.

Proof. Since $d \mid a$ and $d \mid b$, there exist $k_1, k_2 \in \mathbb{Z}$ such that $a = k_1 d$ and $b = k_2 d$. Then:

$$ar + bs = (k_1 d)r + (k_2 d)s$$
$$ar + bs = d(k_1 r + k_2 s)$$

Since $k_1, r, k_2, s \in \mathbb{Z}$ we have that $(k_1 r + k_2 s) \in \mathbb{Z}$ by Closure. So, by the definition of Divisibility,

$$d \mid ar + bs.$$

□

Remark 5.7. Given a and b, we will call $ax + by$ a *linear combination* of a and b.

Now, we will define the terms that are central to this exposition:

Definition 5.8 (Prime)**.** For all $p \in \mathbb{Z}^+$, p is defined as *prime* iff $p > 1$ and, for all $a \in \mathbb{Z}^+$ such that $a \mid p$, either $a = 1$ or $a = p$.

Definition 5.9 (Composite)**.** For all $p \in \mathbb{Z}^+$, p is defined as *composite* iff $p > 1$ and p is not prime; that is, there exists $a \in \mathbb{Z}^+$ such that $1 < a < p$ and $a \mid p$.

§6 Bezout's lemma

Theorem 6.1 (Division Algorithm)
For all $a \in \mathbb{Z}$ and $b \in \mathbb{Z}^+$, there exists q and r such that $a = bq + r$ and $0 \leq r < q$.

Proof. Let set $S = \{r \mid r \in \mathbb{Z}^{0+}, r = a - bq\}$.

S is nonempty and a subset of $\mathbb{Z}^{0+}$, so by WOP, S has a minimum. Call this minimum r_1.

We will prove that r_1 is in the range $0 \leq r_1 < b$. So, for the sake of contradiction, assume that $r_1 \geq b$. Let $r_2 = r_1 + (-b)$ and $q_2 = q_1 + 1$. By the following computations, we get that

$$\begin{aligned} a &= bq_1 + r_1 \\ a &= bq_1 + r_1 + b - b \\ a &= bq_1 + b + r_1 - b \\ a &= b(q_1 + 1) + (r_1 - b) \\ a &= bq_2 + r_2 \\ \implies r_2 &= a - bq_2 \end{aligned}$$

Given that $r_1 \geq b$, we get that

$$\begin{aligned} r_1 &\geq b \\ r_2 = r_1 - b &\geq b - b = 0 \\ \implies r_2 &\geq 0 \end{aligned}$$

Since $r_2 \geq 0$ and $r_2 = a - bq_2$, r_2 must also be in S and $r_2 < r_1$, a contradiction on our definition of r_1 as the minimum of S.

Thus, there exists $r = a - bq$ such that $0 \leq r < b$.

□

Theorem 6.2 (Bezout's Lemma)
For all $a, b \in \mathbb{Z}$, there exist $x, y \in \mathbb{Z}$ such that $ax + by = gcd(a, b)$.

Proof. Given values for a and b, let $S = \{c = ax + by \mid x, y \in \mathbb{Z}; c > 0\}$. We will show that the minimum element of this set is $gcd(a, b)$.

To show this, we must first know if there even exists a minimum element in S, which can be simply shown with WOP since $S \subseteq \mathbb{Z}^+$. We will call this element d.

Next, we will show that all elements of S are divisible by d. To do this, assume there exist elements in S that do not divide d. More formally, let S' be the subset of S such that $S' = \{c = ax + by \mid x, y \in \mathbb{Z}, c > 0, d \nmid c_0\}$, and assume for the sake of contradiction that S' is not empty. We will attempt to prove that we can construct an element in S' smaller than d, which is a violation of the minimality of d.

By WOP, there exists a minimum element in S', say c_0. Since $c_0 \in S'$, we know that $d \nmid c_0$. By the Division Algorithm, there exist a quotient $q_0 \in \mathbb{Z}$ and a nonzero remainder $r_0 \in \mathbb{Z}$ such that $0 < r < d$ and $c_0 = dq_0 + r_0$.

Since $d \in S$ and $c_0 \in S$, we can write $d = ax + by$ and $c_0 = ax_0 + by_0$ for some $x, y, x_0, y_0 \in \mathbb{Z}$. Using the following manipulations, we get:

$$\begin{aligned} c_0 &= ax_0 + by_0 && (1)\\ d &= ax + by && (2)\\ -rd &= -r(ax + by) = a(-rx) + b(-ry) && (3)\\ c_0 + (-rd) &= ax_0 + by_0 + a(-rx) + b(-ry) && (4)\\ &= a(x_0 + (-rx)) + b(y_0 + (-ry)) && (5)\\ \implies r_0 &= a(x_0 + (-rx)) + b(y_0 + (-ry)) && (6) \end{aligned}$$

Here, we have just represented r_0, a positive number less than d, as a linear combination of a and b, which contradicts the minimality of d as the *least* positive linear combination of a and b. So, S' must be empty.

So, all elements of S must be divisible by d. Since a and b are also in S, it follows that $d \mid a$ and $d \mid b$.

Now, we must prove that d is the *greatest* divisor of a and b. Let d' be another common divisor of a and b. Since $d' \mid a$ and $d' \mid b$, d must divide any $ax + by$ by Theorem 5.6. Since d can be represented as a linear combination of a and b, it follows that $d' \mid d$ and, consequently, $d' \leq d$ by Theorem 5.5 . So, d must be the *greatest* common factor of a and b. □

§7 Unique Factorization Theorem

Now, we are at the final stage of proving UFT. To reach this point, we will need to prove properties of primes, such as "every number has a prime factor" and "if a prime divides a number, then that prime divides at least one of its factors" to show that a prime factorization exists and that two prime factorizations of a number must actually be the same to demonstrate uniqueness.

We will start with the "Fundamental Lemma".

Theorem 7.1 (Fundamental Lemma)
For all $a, b, m \in \mathbb{Z}$, if $m \mid ab$ and $gcd(m, a) = 1$, then $m \mid b$.

Proof. Since $gcd(m, a) = 1$, there exist $x, y \in \mathbb{Z}$ such that $mx + ay = 1$ by Bezout's Lemma. Multiplying both sides by b, we get:

$$\begin{aligned} b(mx + ay) &= b \cdot 1 = b\\ bmx + bay &= b\\ mxb + aby &= b\\ m(xb) + ab(y) &= b \end{aligned}$$

Since $m \mid m$ and $m \mid ab$, m divides any linear combination of a and b, which includes $m(xb) + ab(y) = b$. Therefore, $m \mid b$. □

Theorem 7.2 about prime divisors is a direct consequence of Theorem 7.1.

Theorem 7.2
For all $a, b, p \in \mathbb{Z}^+$, if p is prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof. There are two cases: $p \mid a$, and $p \nmid a$.

The first case means we are done.

In the second case where $p \nmid a$, the only factors of p are 1 and p, so the possible values for $gcd(a, p)$ are 1 and p. If $gcd(a, p) = p$, then $p \mid a$, which is a contradiction since $p \nmid a$ in this case. So, $gcd(a, p) = 1$. Knowing that $p \mid ab$, we can apply the Fundamental Lemma to get that $p \mid b$. □

Corollary 7.3 is an extension of Theorem 7.2 with a variable number of factors.

Corollary 7.3

Let $(n_i)_{i=1}^k$ be a sequence such that for all $i \in [k]$, $n_i \in \mathbb{Z}^+$. If p is prime and

$$p \mid \prod_{i=1}^{k} n_i,$$

then there exists $i \in [k]$ such that $p \mid n_i$.

Proof. There are two cases: $p \mid n_k$ and $p \nmid n_k$.

In the first case, let $i = k$, and we are done.

In the second case, we will have to use WOP in our argument since we are manipulating a product with a variable number of factors in our product. Let $S = \{j \mid 1 \leq j \leq k \text{ and } p \nmid \prod_{i=j}^{k} n_i\}$. To start, we know that S is nonempty since, in this case, $p \nmid n_k = \prod_{i=k}^{k} n_i$, so $k \in S$. We also know that $1 \notin S$ since it is given that $p \mid \prod_{i=1}^{k} n_i$.

By WOP, there exists a minimal element $m \in S$. We will show that $p \mid n_{m-1}$.

Because $m \in S$, $p \nmid \prod_{i=m}^{k} n_i$. Also, because $1 \notin S$, m is greater than 1, and by NIBZO, $m \geq 2$. Now, let's consider the starting index $m - 1$. Because $m \geq 2$, $m - 1$ is greater than or equal to 1, so $m - 1$ is a valid index to use. Since m is the minimal element in S, $m - 1$ is not in S, so we know that $p \mid \prod_{i=m-1}^{k} n_i$. We have that

$$p \mid \prod_{i=m-1}^{k} n_i = n_{m-1} \cdot \prod_{i=m}^{k} n_i$$

By Theorem 7.2, we find that either $p \mid n_{m-1}$ or $p \mid \prod_{i=m}^{k} n_i$. Since $p \nmid \prod_{i=m}^{k} n_i$, it must be that $p \mid n_{m-1}$. □

Theorem 7.4

For all $n \in \mathbb{Z}^+$, if $n > 1$, there exists a prime $p \in \mathbb{Z}^+$ such that $p \mid n$.

Proof. Because $n > 1$, there are two cases: n is prime or n is composite.

If n is prime, we know that $n \mid n$, so let $p = n$ and we are done.

Now, we deal with the case that n is composite. Let

$$S = \{n \mid n \in \mathbb{Z}^+, n \text{ is composite}, n \text{ doesn't have a prime factor}\}.$$

Assume for the sake of contradiction that S is nonempty. By WOP, there exists a least element $m \in S$. Since m is composite, there exist $a, b \in \mathbb{Z}^+$ such that $a, b > 1$ and $ab = m$. Because $a \mid m$ and $a, b > 1$, $a < m$ by Theorem 5.4. Since $a > 1$ and $a \notin S$, a must have a prime factor by the definition of S, say p. Since $p \mid a$ and $a \mid m$, p divides m and so m has a prime factor, which is a contradiction. Thus, S must be empty. □

The following proofs will demonstrate UFT for all integers. But, first, what is a prime factorization?

Definition 7.5. The prime factorization of n is its representation as a product of primes

$$\prod_{n=1}^{k} p_i,$$

where, for all $i \in [k]$, p_i is prime.

Theorem 7.6 (Existence of Factorization)
For all $n \in \mathbb{Z}^+$ such that $n > 1$, n is either a prime or can be represented as a product of primes.

Proof. If n is a prime, we are done. Let's prove that, if n is composite, n can be represented as a product of primes.

Let the set

$$S = \{n \mid n > 1, n \text{ is composite}, n \text{ cannot be represented as a product of primes}\}.$$

Assume for the sake of contradiction that S is nonempty. By WOP, there exists a minimum element $m \in S$. Since m is composite, there exist $a, b \in \mathbb{Z}^+$ such that $a, b > 1$ and $ab = m$. By Theorem 5.4, we have that $1 < a < m$ and $1 < b < m$. Now, there are four cases in all: a is prime or a is composite, and b is prime or b is composite. Let's explore these cases:

Case 1: a, b are prime
This is a direct contradiction since the prime factorization of m would just be ab.

Case 2: a is prime, b is composite
Since $b < m$, b is not in S. Then, because b is composite, b can be represented as a product of primes: let this product of primes be

$$\prod_{i=1}^{k} p_i.$$

Then, the prime factorization of n would be

$$ab = a \cdot \prod_{i=1}^{k} p_i,$$

which is a contradiction.

Case 3: a is composite, b is prime
Swap the values of a and b, and repeat the proof for Case 2.

Case 4: a is composite, b is composite
Since $a < m$ and $b < m$, a and b are not in S. Then, because a and b are composite, a and b can be represented as a product of primes: let these products of primes be

$$\prod_{i=1}^{k} p_i$$

and

$$\prod_{i=1}^{l} q_i,$$

respectively. Then, the prime factorization of n would be

$$ab = \prod_{i=1}^{k} p_i \cdot \prod_{i=1}^{l} q_i,$$

which is a contradiction.

Thus, the set S must be empty. □

Theorem 7.7 (Uniqueness of Factorization)
For all $n \in \mathbb{Z}^+$ such that $n > 1$, let $\prod_{i=1}^{k} p_i$ and $\prod_{i=1}^{l} q_i$ be two factorizations of n. Then the two factorizations must be identical.

Proof. Let $n = \prod_{i=1}^{k} p_i = \prod_{i=1}^{l} q_i$. We say that these two factorizations of n are *different* when either $k \neq l$ or the number of times each p_i occurs in each factorization is different.

If n is prime, then its prime factorization consists only of one prime factor: n. Otherwise, n having two different prime factorizations would suggest that n is either equal to a different prime or is composite, which is a contradiction. So, let n be composite.

Let

$$S = \{n \mid n \geq 2, n \text{ is composite}, n \text{ has two different prime factorizations}\}.$$

By WOP, there exists a minimum element $m \in S$. Let $\prod_{i=1}^{k} p_i$ and $\prod_{i=1}^{l} q_i$ be the two different factorizations of m. Because m is composite, it is straighforward that these two factorizations each have at least 2 primes, and that $k \geq 2$ and $l \geq 2$.

Now, let's take p_1, the first prime that divides m. since $\prod_{i=1}^{k} p_i = \prod_{i=1}^{l} q_i$, $p_1 \mid \prod_{i=1}^{l} q_i$. By Theorem 7.3, there must exist a q_j such that $p_1 \mid q_j$. Since q_j is prime, the only factors of q_j are 1 and q_j. Since p_1 cannot be 1, it must be that $p_1 = q_j$. Substituting, we get that

$$p_1 \cdot \prod_{i=2}^{k} p_i = p_1 \cdot \prod_{i=2; i \neq j}^{l} q_i$$

Letting m' be the other part of the prime factorization $\prod_{i=2}^{k} p_i$, we get that

$$p_1 \cdot \prod_{i=2}^{k} p_i = p_1 \cdot m' = p_1 \cdot \prod_{i=1; i \neq j}^{l} q_i$$

$$\implies m' = \prod_{i=2}^{k} p_i = \prod_{i=1; i \neq j}^{l} q_i \text{ (by Cancellation)}.$$

There are four cases here:

1. $k = 2$ and $l = 2$
2. $k = 2$ and $l > 2$
3. $k > 2$ and $l = 2$

4. $k > 2$ and $l > 2$

In **Case 1**, m' really only has 1 prime factor in each prime factorization, and so those prime factorizations must be identical. Therefore, the two prime factorizations of m, with p_1 included, must be identical, which contradicts the fact that $m \in S$.

The next two cases, **Case 2** and **Case 3**, are not possible since they imply that a single prime is equal to a product of multiple primes and, therefore, is composite.

In last case, **Case 4**, since m' is the product of multiple primes, m' is composite. Also, since $m' \mid m$ and $p_i \geq 2$, m' must be less than m by Theorem 5.4. Also, since m is the minimal element in S, m' cannot be in S, which means that the two factorizations of m' shown above must be the same. As a result, multiplying both sides by p_1 to get m actually yields two identical factorizations for m because it increases the number of factors of p_i in the two identical factorizations of m' by one. So, there cannot be two different prime factorizations for m.

Therefore, the set S is empty, and each $n \in \mathbb{Z}^+$ has to have a *unique factorization.* □

§8 Canonical Factorization

Definition 8.1 (Exponents)**.** We define a^n as follows for $n \in \mathbb{Z}^+$:

1. $a^1 = a$
2. $a^n = a \cdot a^{n-1}$

Theorem 8.2

For all $n \in \mathbb{Z}^+$ such that $n \geq 2$, n has a unique canonical factorization, i.e. a factorization such that $n = \prod_{i=1}^{k} p_i^{e_i}$, with all p_i's being distinct from each other pairwise and $e_i \geq 1$.

Proof. Say for the sake of contradiction we have two different canonical factorizations:

$$n = \prod_{i=1}^{k} p_i^{e_i} = \prod_{i=1}^{k} p_i^{f_i}$$

Since we have proven Theorem 7.7 that n must have a unique prime factorization, it follows that the set of distinct primes in the prime factorization must remain the same across canonical factorizations. Thus, we just need to prove that the exponents of corresponding primes are the same.

So, we must assume that there exists some $j \in [k]$ such that $e_j \neq f_j$. Without Loss of Generality, let $e_j < f_j$. From both factorizations, we can factor out $p_j^{e_j}$ to get

$$n = p_j^{e_j} \cdot \prod_{i=1; i \neq j}^{k} p_i^{e_i} = p_j^{e_j} \cdot p_j^{f_j - e_j} \cdot \prod_{i=1; i \neq j}^{k} p_i^{f_i}$$

$$\implies \prod_{i=1; i \neq j}^{k} p_i^{e_i} = p_j^{f_j - e_j} \cdot \prod_{i=1; i \neq j}^{k} p_i^{f_i} \text{ (by Cancellation)}$$

If $f_j - e_j > 0$, the RHS, and the LHS, is divisible by p_j. Since $p_j \mid \prod_{i=1; i \neq j}^{k} p_i^{e_i}$, p_j must divide one of the other primes in the factorization, but this is not possible since each prime in the canonical factorization must be distinct. Therefore, $f_j = e_j$.

□

Corollary 8.3

For all $n \in \mathbb{Z}$ such that $n > 1$ or $n < -1$, n has a unique factorization and a unique canonical factorization.

Proof. The result in Theorem 8.2 can be generalized to all $n \in \mathbb{Z}$. Theorem 8.2 proves that it exists for all positive integers greater than 1. For any $n \in \mathbb{Z}$ such that $n < -1$, the unique factorization can be derived by taking $(-1)n$, which is in $\mathbb{Z}^+$, finding its factorization, and then multiplying the resulting factorization by -1. The same process can be done using canonical factorizations. □