Establishing the Fundamental Theorem of Arithmetic

Ke Liang

WLSA Shanghai Academy, Shanghai, 200243, China

Abstract: *This paper proved the Fundamental Theorem of Arithmetic, which asserts the existence and uniqueness of prime factorization for every integer greater than 1, and extends it to all integers including the negatives. The proof is solely based on the ring axioms, order axioms and the well-ordering principle. After establishing the basic arithmetic operations from these axioms, the main proof is completed by defining canonical factorization, proving a key result known as the fundamental lemma (if p prime divides ab, then p divides a or b), and then demonstrating both the existence and uniqueness of prime factorizations. This proof broke free from the use of the Euclidean algorithm, Bézout's theorem, and mathematical induction—methods commonly employed in previous proofs. By doing so, it provides a new insight into the structure of the integer ring and how "fundamental" is the Fundamental Theorem of Arithmetic.*

Keywords: *Fundamental Theorem of Arithmetic; Prime Divisors; Ring Axioms; The Fundamental Lemma*

1. Introduction

The Fundamental Theorem of Arithmetic, stating that every integer can be uniquely factorized into a product of primes, up to the order of the factors, serves as a building block for number theory investigations[1-3]. The motivation of this proof is to determine the presence of the Fundamental Theorem of Arithmetic in the integer ring and to make sure that people understand these simple but important ideas. In this way, we get a better understanding of the structure and behavior of numbers by proving basic lemmas and theorems. The proof starts by establishing basic arithmetic lemmas and operations, including basic operations like $-(-a) = a$ and the concept of divisors. Some important results will be that all positive integers have a prime divisor and The Fundamental Lemma[4-5], which will involve use of the Well-Ordering Principle, a unique property of integers[6-7]. Piling up all of these results, we will prove the Fundamental Theorem of Arithmetic.

2. Math

2.1 Foundational Concepts

We will first prove some basic results from the axioms that will be essential in our proof.

Definition 1.1. For $a \in \mathbb{Z}$, $-a$ is an element such that $a + (-a) = 0$.

Theorem 1.2. For all $a \in \mathbb{Z}$, $-a$ exists.

Proof. This follows from the negatives in the ring axioms.

Lemma 1.3. $\forall a$, $a \cdot 0 = 0$.

Proof. By the zero axiom, $0 + 0 = 0$, so $a \cdot (0 + 0) = a \cdot 0 + a \cdot 0 = a \cdot 0$. We then have $a \cdot 0 + a \cdot 0 + \left(-(a \cdot 0)\right) = a \cdot 0 + \left(-(a \cdot 0)\right)$, so $a \cdot 0 + 0 = a \cdot 0 = 0$.

Theorem 1.4. 0 is uniquely defined.

Proof. Suppose for the sake of contradiction that $\exists\, z$ such that $z \neq 0$, and for all $a \in \mathbb{Z}$, $a + z = a$. Then, $0 + z = 0$. However, we also have that $0 + z = z + 0 = z$, which means that $z = 0$. This contradicts our definition of z as nonzero, so it can only be concluded that z doesn't exist.

Theorem 1.5. If a ring has at least two elements, $0 \neq 1$.

Proof. Let's assume for the sake of contradiction that $0 = 1$. By Theorem 1.4, only one element in the set can be 0, so we can choose another that is not, call it a. Then, we have $a \cdot 1 = a$, and $a \cdot 1 = a \cdot 0 = 0$ by Lemma 1.3, which means that $a = 0$. This contradicts our definition of a as nonzero, so we can only conclude that $0 \neq 1$.

Theorem 1.6. $\mathbb{Z}$ has at least two elements.

Proof. By definition, $\mathbb{Z}^+$ is nonempty, so there must be an element $a \in \mathbb{Z}$ such that $a \in \mathbb{Z}^+$. Since $0 \notin \mathbb{Z}^+$ by non-triviality, a is not 0, so a and 0 are distinct elements in $\mathbb{Z}$, making it have at least two elements.

Theorem 1.7. $\mathbb{Z}$ has $0 \neq 1$.

Proof. This follows from Theorem 1.6 and Theorem 1.4.

Theorem 1.8. If $a + b = a + b'$, $b = b'$.

Proof. If we have $a + b = a + b'$, we have $(-a) + a + b = (-a) + a + b'$, so $0 + b = 0 + b'$, which means that $b = b'$.

Theorem 1.9. For $a \in \mathbb{Z}$, $-a$ is uniquely defined.

Proof. Let's assume there exists $x, y \in \mathbb{Z}$ such that $a + x = 0$ and $a + y = 0$. By Theorem 1.8, $x = y$, so only one unique solution can exist. Then, $-a$ must be this unique solution.

Theorem 1.10. $-(-a) = a$.

Proof. By definition, $(-a) + \big(-(-a)\big) = 0$. We also have that $(-a) + a = 0$. Thus, by Theorem 1.8, $-(-a) = a$.

Theorem 1.11. $-(ab) = (-a)b$.

Proof. We have that $ab + \big(-(ab)\big) = 0$ by negativity. Thus, $ab + \big(-(ab)\big) + (-a)b = 0 + (-a)b = (-a)b$. We then get that $\big(-(ab)\big) + (ab + (-a)b) = \big(-(ab)\big) + \big(a + (-a)\big)b = \big(-(ab)\big) + 0 \cdot b$. By 1.3, then, this is equal to $\big(-(ab)\big) + 0 = \big(-(ab)\big)$, so $-(ab) = (-a)b$.

Theorem 1.12. $-(ab) = a(-b)$.

Proof. We can rewrite $-(ab)$ as $-(ba)$, which means it is equal to $(-b)a = a(-b)$ by Lemma 1.3.

$\mathbf{Theorem\ 1.13.} -(ab) = (-a)b = a(-b)$

Proof. This follows from Lemma 1.11 and Lemma 1.12.

Theorem 1.14. $(-a)(-b) = ab$.

Proof. Using Lemma 1.13, It can be found that $(-a)(-b) = -\big(a(-b)\big) = -\big(-(ab)\big)$, which is equal to ab by Lemma 1.10.

Theorem 1.15. $-a = (-1) \cdot a$.

Proof. By Lemma 1.13, $(-1) \cdot a = -(1 \cdot a) = -a$.

Definition 1.16. For $a, b \in \mathbb{Z}$, $a - b$ is defined as $y \in \mathbb{Z}$ where $a = b + y$.

Lemma 1.17. $a - b = a + (-b)$.

Proof. By definition, if $a - b = y$, then $a = y + b$. Thus, $a + (-b) = y + b + (-b) = y + 0$, so $a + (-b) = y$.

Theorem 1.18. $-1 \notin \mathbb{Z}^+$.

Proof. Let's assume for the sake of contradiction that $-1 \in \mathbb{Z}^+$. Since $\mathbb{Z}^+$ is nonempty, there exists some $a \in \mathbb{Z}^+$. Then $(-1)a \in \mathbb{Z}^+$ by multiplicative closure, so $-a \in \mathbb{Z}^+$ by Lemma 1.15. However, by Trichotomy, we cannot have $-a \in \mathbb{Z}_p$, creating a contradiction, so our assumption that $-1 \in \mathbb{Z}^+$ must be false.

Theorem 1.19. $1 \in \mathbb{Z}^+$.

Proof. By Theorem 1.7, $1 \neq 0$. We also have that $-1 \notin \mathbb{Z}^+$. Thus, by Trichotomy, $-(-1) = 1 \in \mathbb{Z}^+$.

Lemma 1.20. $b - a = -(a - b)$.

Proof. By Lemma 1.7, $b - a = b + (-a)$, and $-(a - b) = -\big(a + (-b)\big)$. By Lemma 1.15, $-\big(a + (-b)\big) = (-1)\big(a + (-b)\big) = (-1)a + (-1)(-b) = (-a) + \big(-(-b)\big)$.By Lemma 1.10, this is equal to $(-a) + b = b + (-a)$, so $b - a = -(a - b)$.

Lemma 1.21. If $ab = ab'$ and $a \in \mathbb{Z}^+$, $b - b' \notin \mathbb{Z}^+$.

Proof. If $ab = ab'$, $ab + \big(-(ab')\big) = a\big(b + (-b')\big) = 0$ using Lemma 1.13. If $b - b' \in \mathbb{Z}^+$, we would have $0 \in \mathbb{Z}^+$ by multiplicative closure, as $a \in \mathbb{Z}^+$. This contradicts non-triviality, so our assumption that $b - b' \in \mathbb{Z}^+$ must be false.

Lemma 1.22. For any nonzero a, if $ab = ab'$, $b - b' \notin \mathbb{Z}^+$.

Proof. This problem will be solved in two cases. Case 1: $a \in \mathbb{Z}^+$. This then is proved by Lemma 1.21; Case 2: $a \notin \mathbb{Z}^+$. Then, we have $-a \in \mathbb{Z}^+$ by nontriviality, as $a \neq 0$ is given. Since $ab = ab'$, $-(ab) = -(ab')$, so $(-a)b = (-a)b'$ by Lemma 1.13. This gives $b - b' \notin \mathbb{Z}^+$ by Lemma 1.21.

Lemma 1.23. For any nonzero a, if $ab = ab'$, $b' - b \notin \mathbb{Z}^+$.

Proof. If $ab = ab'$, $ab' = ab$, so $b' - b \notin \mathbb{Z}^+$, by Lemma 1.22.

Lemma 1.24. For any nonzero a, if $ab = ab'$, $b' = b$.

Proof. By Lemma 1.22, $b - b' \notin \mathbb{Z}_p$. By Lemma 1.23, $b' - b \notin \mathbb{Z}^+$, so $-(b - b') \notin \mathbb{Z}_p$ by Lemma 1.20. By Trichotomy, $b - b' = 0$, so $b = b'$.

Definition 1.25. $a < b$ if $b - a \in \mathbb{Z}^+$.

Definition 1.26. $a \leq b$ if $b - a \in \mathbb{Z}^+ \cup \{0\}$.

Definition 1.27. $\nless$ means "not <."

Theorem 1.28. If $b < a$, $a \nless b$.

Proof. If $b < a$, then $a - b \in \mathbb{Z}^+$. Thus, by trichotomy, $-(a - b) = b - a \notin \mathbb{Z}^+$ by Lemma 1.20, so $a \nless b$.

Lemma 1.29. If $x \notin \mathbb{Z}^+$, $-x \in \mathbb{Z}^+ \cup \{0\}$.

Proof. We will do this in cases.

Case 1: $x = 0$. Since $0 + (-0) = 0 + 0$, $0 = -0$ by Theorem 1.8. Then, if $x = 0$, $-x = -0 = 0$, so $-x \in \{0\}$, which implies that $x \in \mathbb{Z}^+ \cup \{0\}$.

Case 2: $x \neq 0$. If $x \neq 0$, then $-x \in \mathbb{Z}^+$ by trichotomy, so $-x \in \mathbb{Z}^+ \cup \{0\}$.

Theorem 1.30. If $a \nless b$ and $b \nless a$, then $a = b$.

Proof. If $a \nless b$, $b - a \notin \mathbb{Z}^+$, so $-(b - a) = a - b \in \mathbb{Z}^+ \cup \{0\}$ by Lemma 1.20 and Lemma 1.29. Similarly, $b - a \in \mathbb{Z}^+ \cup \{0\}$.

If $a - b = 0$, $a = b$.

Otherwise, $a - b \in \mathbb{Z}^+$, which means $b - a \notin \mathbb{Z}^+$ by trichotomy. Thus, $b - a = 0$, so $b = a$.

Theorem 1.31. If $a = b$, then $a \nless b$ and $b \nless a$.

Proof. If $a = b$, $a - b = 0 \notin \mathbb{Z}^+$ and $b - a = 0 \notin \mathbb{Z}^+$ by trichotomy, so $a \nless b$, $b \nless a$.

Theorem 1.32. For $a, b \in \mathbb{Z}$, exactly one of $a < b$, $b < a$, and $a = b$ is true.

Proof. If $a = b$, then $a \nless b$ and $b \nless a$ by Theorem 1.31. Otherwise, by the contrapositive of Theorem 1.30, at least one of $a < b$ or $b < a$ is true. If $a < b$, then $b \nless a$, and if $b < a$, then $a \nless b$ by Theorem 1.28.

Lemma 1.33. If $a, b \in \mathbb{Z}^+ \cup \{0\}$, $ab \in \mathbb{Z}^+ \cup \{0\}$.

Proof. We will do this in multiple cases.

Case 1: $a = 0$ or $b = 0$. If $a = 0$, then $ab = 0$ by Lemma 1.3, which is in $\mathbb{Z}^+ \cup \{0\}$. By symmetry, $ab \in \mathbb{Z}^+ \cup \{0\}$ when $b = 0$.

Case 2: $a, b \neq 0$. If $a, b \neq 0$, $a, b \in \mathbb{Z}^+$, so $ab \in \mathbb{Z}^+ \subseteq \mathbb{Z}^+ \cup \{0\}$.

Lemma 1.34. If for all $s \in S$ $a \leq s$, then $a < s$ for all s such that $s \neq a$.

Proof. Lets assume for the sake of contradiction that there exists $b \in S$ such that $b \neq a$, $a \leq b$, but $a \nless b$. We have then that $b - a \in \mathbb{Z}^+ \cup \{0\}$, but $b - a \notin \mathbb{Z}^+$, so $b - a \in \{0\}$. Thus, $b - a = 0$, so $b = a$. This contradicts our assumption that $b \neq a$, so we must have that $a < s$ for all $s \neq a$.

Definition 1.35. a is the smallest element of set S if $a \in S$ and $\forall s \in S$ $a \leq s$.

Lemma 1.36. If s is the smallest element of S and $a < s$, $a \notin S$.

Proof. Assume for the sake of contradiction that $a \in S$. Then, we have that $s \leq a$ by definition, so $a - s \in \mathbb{Z}^+ \cup \{0\}$, and we are given that $a < s$, so $s - a \in \mathbb{Z}^+$. If $a - s = 0$, then $a = s$, which means that $a \nless s$ by Theorem 1.32, contradicting $a < s$. Thus, $a - s \in \mathbb{Z}^+$. Since $-(a - s) = s - a$ by Lemma 1.20, $s - a \notin \mathbb{Z}^+$ by trichotomy, so $s - a \in \{0\}$, which means that $s = a$, so $a \nless s$ by Theorem 1.32. However, this again contradicts $a < s$, so this cannot happen either. Since both cases lead to contradiction, we must conclude that $a \notin S$.

Theorem 1.37. 1 is the smallest element of $\mathbb{Z}^+$.

Proof. Let us assume for the sake of contradiction that 1 is not the smallest element, which means we can define $a \in \mathbb{Z}^+$ as the smallest element by WOP. Thus, $a \leq 1$, and since $a \neq 1$, $a < 1$ according to Lemma 1.34. Thus, $1 - a \in \mathbb{Z}^+$. This means that $a(1 - a) \in \mathbb{Z}^+$ by multiplicative closure, so $a - (a)(a) \in \mathbb{Z}^+$, so $a \cdot a < a$. By Theorem 1.32, $a \cdot a \neq a$, but $a \cdot a \in \mathbb{Z}^+$ by multiplicative closure. By the definition of the smallest element, $a \leq a \cdot a$, so $a < a \cdot a$ by Lemma 1.34. However, by Theorem 1.32, we cannot have $a < a \cdot a$ and $a \cdot a < a$, which means that our assumption that a exists must be false.

Definition 1.38. $a \mid b$ if $b = ia$ for some $i \in \mathbb{Z}$.

Theorem 1.39. If $a, b \in \mathbb{Z}^+$, and $a \mid b$, $a \leq b$.

Proof. By definition, $b = ka$ for some $k \in \mathbb{Z}$. Thus, $b + (-a) = ka + (-a) = ka + (-1)a = (k - 1)a$. Since $1 \leq k$ by Theorem 1.37, $k - 1 \in \mathbb{Z}^+ \cup \{0\}$. Since $a \in \mathbb{Z}^+$, we also have that $a \in \mathbb{Z}^+ \cup \{0\}$. Thus, $a(k - 1) \in \mathbb{Z}^+ \cup \{0\}$ by Lemma 1.33, so $b - a \in \mathbb{Z}^+ \cup \{0\}$. This means that $a \leq b$.

Lemma 1.40. $\mathbb{Z}^+ \cup \{0\}$ follows the WOP.

Proof. Let S be a subset of $\mathbb{Z}^+ \cup \{0\}$. We will prove this in two cases.

Case 1: $0 \in S$. For all $s \in S$, $s = s + 0 = s + (-0) + 0 = s + (-0) = s - 0 \in \mathbb{Z}^+ \cup \{0\}$, so $0 \leq s$, making it a smallest element.

Case 2: $0 \notin S$. If $0 \notin S$, then $S \subseteq \mathbb{Z}^+$, so S has a smallest element.

Definition 1.41. For $a, n \in \mathbb{Z}$, $0 \geq n$, exponentiation is defined as a^n where $a^0 = 1$, and $a^{n+1} = a^n \cdot a$.

Lemma 1.42. a^n is defined for all $n \geq 0$.

Proof. Let M be the set of all $n \geq 0$ such that a^n is not defined by the definition of exponentiation. Assume for the sake of contradiction that M is nonempty. Then, we can define m as the smallest element of S.

We know that $m \neq 0$, as a^0 is defined as 1. Thus, $m > 0$, so $m - 1 \geq 0$. Since $m - 1 < m$, $m - 1 \notin M$ by Lemma 1.36. Thus, a^{m-1} is defined. We can then define a^m as $a^{m-1} \cdot a$, which means that $m \notin M$. However, this contradicts our definition of m as the smallest element of M, so our assumption that M is nonempty must be false. Thus, a^m is always defined for $m \geq 0$.

Theorem 1.43. If $b = ia$ for some $i \in \mathbb{Z}$ and $a, b \in \mathbb{Z}^+$, $i \in \mathbb{Z}^+$.

Proof. We will assume for the sake of contradiction that $i \notin \mathbb{Z}^+$, and contradict it in two cases.

Case 1: $i = 0$. Here, $b = ia = 0a = 0 \notin \mathbb{Z}^+$ by Lemma 1.3 and Nontriviality, which contradicts that $b \in \mathbb{Z}^+$. Thus, this case cannot happen.

Case 2: $i \neq 0$. By Trichotomy, we have that $-i \in \mathbb{Z}^+$, so $-b = -(ia) = (-i)a \in \mathbb{Z}^+$ by multiplicative closure. However, this contradicts trichotomy, as we can't have both $b, -b \in \mathbb{Z}^+$, so this case can't happen either. Since both cases fail, we can only conclude that $i \in \mathbb{Z}^+$ must be true.

Lemma 1.44. If q_i are defined on $1 \leq i \leq n$ where $q_i < q_{i+1}$, For $1 \leq i < j \leq n$, $q_i < q_j$.

Proof. Let S be the set of $i < k \leq j$ such that $q_i \nless q_k$. Lets assume for the sake of contradiction that S is nonempty. Then, we can define s as the smallest element of S by WOP. We know that $s \neq i + 1$, as we are given that $q_i < q_{i+1}$. Thus, $s - 1 > i$. Since $s - 1 < s$, $s - 1 \notin S$, so $q_i < q_{s-1}$. Since $q_{s-1} < q_s$, $q_i < q_s$, making s not in S. However, this contradicts our definition of s as the smallest element of S, so we can only conclude that our assumption that S was nonempty was false, so $j \notin S$, so $q_i < q_j$.

2.2 Prime Divisors

From here, we will begin by proving that every positive integer greater than 1 has a positive prime divisor, which will be essential in proving our main result. We will begin, of course, by defining primes, and use their properties to prove the theorem.

Definition 2.1. $p \neq 0$ is prime if p is not a unit and for all $b, c \in \mathbb{Z}$, if $bc = p$, then either b or c is a unit.

Lemma 2.2. If $p \in \mathbb{Z}^+$, then if p is not a unit, and if for all $b, c \in \mathbb{Z}^+$ such that $bc = p$ have that either b or c is 1, then p is prime.

Proof. Let $qr = p$ for some $q, r \in \mathbb{Z}$. Now, none of $q, r = 0$, as then $qr = 0 \neq p$. Thus, by trichotomy, either $q \in \mathbb{Z}_p$ or $-q \in \mathbb{Z}^+$, and similarly for r.

If $q \in \mathbb{Z}^+$, then $r \in \mathbb{Z}^+$, as if $-r \in \mathbb{Z}^+$, then $-qr \in \mathbb{Z}^+$ by multiplicative closure, so $-p \in \mathbb{Z}^+$, which means $p \notin \mathbb{Z}^+$ by trichotomy, which is a contradiction. Thus, since $qr = p$, either q or r is 1 and thus a unit, which is given.

On the other hand, if $q \notin \mathbb{Z}^+$, then $r \notin \mathbb{Z}^+$, as otherwise, if $r \in \mathbb{Z}^+$, since $-q \in \mathbb{Z}^+$, then $-qr = -p \in \mathbb{Z}^+$ by multiplicative closure, so $p \notin \mathbb{Z}^+$ by trichotomy, which is again a contradiction. Thus, $q, r \notin \mathbb{Z}^+ \cup \{0\}$, so $|q| = -q$, $|r| = -r$, so $|q||r| = (-q)(-r) = qr = p$. Since $|q|, |r| \in \mathbb{Z}^+$, it is given that either $|q|$ or $|r|$ is 1, so either q or r is -1, a unit.

Since either q or r is always a unit, p is prime. Now we want to prove the existence of prime divisors for every positive integer.

Theorem 2.3. For all $a > 1$, there exists a prime $p \in \mathbb{Z}^+$ such that $p \mid a$.

Proof. Since p is not a unit by definition, $p \neq 1$, so $p > 1$.

Let S be the set of all $a > 1$ that don't have a positive prime p that divides it, and lets assume for the sake of contradiction that it is nonempty. By WOP, it must have a smallest element, which we'll define as s. There cannot exist any $x \in \mathbb{Z}^+$ such that $x \neq 1$, $x \neq s$, and $x \mid s$, as since by Theorem 1.39, $x \leq s$, so $x < s$, so $x \notin S$. Since $x \neq 1$ and $x \in \mathbb{Z}^+$, there would be a positive prime q such that $q \mid x$, which would mean $q \mid s$, meaning $s \notin S$, a contradiction. Thus, the only elements of $\mathbb{Z}^+$ that divide s are 1 and s by Lemma 2.2. This, however, makes s a positive prime by definition. Since $s \mid s$, s has a positive prime divisor, making it again not in S. Thus, we get a contradiction again, and we can only conclude that our assumption that S is nonempty, so all $a > 1$ must have a positive prime divisor.

2.3 Equivalence Classes

We will now set up and prove some things about equivalence classes, which are the classes of integers $\pmod{p}$. This will allow us to reduce integers to better see the divisor relationships between them and a prime p, which will help us prove The Fundamental Lemma.

Theorem 3.1. For any $a, b \in \mathbb{Z}$ where $b \neq 0$, a can be expressed as $ib + c$ for some $c \in \mathbb{Z}^+ \cup \{0\}$.

Proof. Lets assume for the sake of contradiction that a can't be represented as $ib + c$. If this is the case, then there can be no i such that $ib < a$. This is because if there was, then $a - ib \in \mathbb{Z}^+$, which means we could define c as this value. We also can't have that $ib = a$, as then $ib + 0 = a$ allowing us to set c to 0. Thus, we must have that for all $i \in \mathbb{Z}$, $a < ib$. This means that for all i $ib - a \in \mathbb{Z}^+$. Now, let B be the set of all $ib - a$ where $i \in \mathbb{Z}$. Since $ib - a \in \mathbb{Z}^+$, $B \subseteq \mathbb{Z}^+$, so by WOP B has a smallest element, which we'll define as $x = jb - a$ for some $j \in \mathbb{Z}$.

Now, if $b \in \mathbb{Z}^+$, then $x - \left((j-1)b - a\right) = b \in \mathbb{Z}^+$, so $(j-1)b - a < x$. Since $(j-1)b - a \in B$, this creates a contradiction, as it is smaller than the smallest element. Thus, our assumption that a can't be represented as $ib + c$ is false.

Otherwise, if $b \notin \mathbb{Z}^+$, $-b \in \mathbb{Z}^+$ by Trichotomy, so $x - \big((j+1)b - a\big) = -b \in \mathbb{Z}^+$, so $(j+1)b - a < x$. Since $(j+1)b - a \in B$, this similarly creates a contradiction as it is smaller than the smallest element, again disproving our assumption that a can't be represented as $ib + c$.

Definition 3.2. The equivalence class of $a \in \mathbb{Z}$ with respect to $b \in \mathbb{Z}$ where $b \neq 0$ is the smallest element of the set S of $s \in \mathbb{Z}^+ \cup \{0\}$ such that $s \equiv a \pmod{b}$.

Theorem 3.3. For any $a, b \in \mathbb{Z}$ where $b \neq 0$, the equivalence class of a with respect to b exists.

Proof. Any $s \in \mathbb{Z}^+ \cup \{0\}$ that has $a = ib + s$ for some $i \in \mathbb{Z}$ is in the set S defined in the definition of equivalence classes by definition. By Theorem 3.1, a can be represented as $ib + c$ for some $i \in \mathbb{Z}$ and $c \in \mathbb{Z}^+ \cup \{0\}$. This means that $c \in S$, so S is nonempty, which means it has a least element s by WOP. This s is the equivalence class, which proves that it exists.

Theorem 3.4. The equivalence class s of $a \in \mathbb{Z}$ with respect to $p > 0$ is less than p.

Proof. Assume for the sake of contradiction that $s \nless p$, so $s \geq p$. Then, $s - p \in \mathbb{Z}^+ \cup \{0\}$. Since $s \equiv a \pmod{p}$ by definition, $a = ip + s$ for some $i \in \mathbb{Z}$. However, we find that also $s - p \equiv a \pmod{p}$, as $a = (i+1)p + s - p = ip + s$. The equivalence class is the least k in $\mathbb{Z}^+ \cup \{0\}$ with the property that $k \equiv a$, so since $s - p < s$, $s - p$ is the equivalence class of a and not s. This is a contradiction, as we assumed that s was the equivalence class of a. Thus, our assumption that $s \nless p$ is false, so $s < p$.

2.4 The Fundamental Lemma

Now, we will begin proving The Fundamental Lemma, which states that if p prime divides ab, then p divides a or b. We will start by proving it for positive primes.

Lemma 4.1. If $p \in \mathbb{Z}^+$ is prime then for all $a, b \in \mathbb{Z}$ if $p \mid ab$ then $p \mid a$ or $p \mid b$.

Proof. Since p is not a unit by definition, $p \neq 1$, so $p > 1$.

Let S be the the set of all positive prime p such that p does not satisfy this property. We will assume for the sake of contradiction that it is nonempty.

By WOP, we can define s to be the smallest element of that set. Since s does not satisfy the property, for some $b, c \in \mathbb{Z}$, $s \mid bc$ but $s \nmid b$ and $s \nmid c$.

By Theorem 3.3, we can define an equivalence class of b with respect to s as u and an equivalence class of c as v. By definition, $u \equiv b \pmod{s}$ and $v \equiv c \pmod{s}$, so for some $i, j \in \mathbb{Z}$, $b = is + u$, and $c = js + v$. This means that $u, v \neq 0$, as otherwise $b = is$ and $c = js$ so $s \mid b$ and $s \mid c$, both of which we defined as untrue. By Theorem 3.4, $u < s$ and $v < s$. Thus, we have $bc = (is + u)(js + v) = (ijs + iv + uj)s + uv$. For $s \mid bc$, we need $bc = rs$ for some $\in \mathbb{Z}$. This means $(ijs + iv + uj)s + uv = rs$, so $uv = \big(r - (ijs + iv + uj)\big)s$. Thus, $s \mid uv$. Since $u, v < s$, $s \nmid u, v$, as if $s \mid u, v$, we would have that $s \leq u, v$, which is not true. Since $u, v < s$, and $u, v, s \in \mathbb{Z}_p$, $uv < s^2$. Since $s \mid uv$, $uv = ks$ for some $k \in \mathbb{Z}$. Since $uv < s^2$, $k < s$. Since $u, v \in \mathbb{Z}_p$, $uv \in \mathbb{Z}_p$ by additive closure, so $ks \in \mathbb{Z}_p$. This means that $k \in \mathbb{Z}_p$ by Theorem 1.43.

If $k = 1$, then we get $uv = s$. Since $u, v < s$, we can't have that one of u or v is one. If we assumed that without loss of generality $u = 1$, $uv = 1v = v < s$, which contradicts $uv = s$. However, this means that s is not prime by Lemma 2.2, which is a contradiction to the fact we were given. Thus, we must conclude that $k =\neq 1$. Since $k \in \mathbb{Z}^+$, $k > 1$.

Define K as the set of all k generated by some $b, c \in \mathbb{Z}$ such that $s \mid bc$ but $s \nmid b$ and $s \nmid c$, by way of equivalence classes u and v of b and c respectively having $uv = ks$. Since we assumed that at least one instance of b, c exists, K is nonempty, since each b, c generates at least one k. Since $K \subseteq \mathbb{Z}^+$, we can define m as the smallest element of K by WOP.

For m, there exists $b, c \in \mathbb{Z}$ such that the u, v generated by b, c has the property that $uv = ms$. Since $m > 1$, there exists positive prime $q > 1$ such that $q \mid m$. Since $q \leq m$ by Theorem 1.39, and $m < s$, $q < s$. Since s is the smallest element in S, $q \notin S$, so since q is a positive prime, q satisfies the property. Thus, either $q \mid u$ or $q \mid v$. Without loss of generality, lets assume that $q \mid u$, so $u = lq$ for some $l \in \mathbb{Z}^+$ by Theorem 1.43, as $u \in \mathbb{Z}^+$ and $q \in \mathbb{Z}^+$. We also have that $q \mid m$, so $m = nq$ for $n \in \mathbb{Z}^+$ by Theorem 1.39, as $m, q \in \mathbb{Z}^+$. Thus, we have $lqv = nqs$. By Theorem 1.24, $lv = ns$. Since $q \neq 1$, $m \neq n$ by the contrapositive of Theorem 1.24, as it gives that $nq \neq n \cdot 1$. Since $n \mid m$, $n \leq m$ by Theorem 1.39, so we get $n < m$.

Now, since $lv = ns$, $s \mid lv$, and we still have that $s \nmid v$. We also have that $s \nmid l$, as if $s \mid l$, then since $l \mid u$, $s \mid u$. Thus, l, v generates some n in K. v remains is its own equivalence class. l is also its own equivalence class, as its the smallest element of the set of $g \in \mathbb{Z}^+ \cup \{0\}$ such that $l = ds + g$ for some $d \in \mathbb{Z}$, as $l = 0p + l$. If we assume that there is a smaller g, then for some $d \in \mathbb{Z}$, $l = ds + g$, so $l - ds = g$. Since $g \in \mathbb{Z}^+$, $l - ds \in \mathbb{Z}^+$, so $l > ds$. We also have $l - g = ds$. Since $g < l$, $ds \in \mathbb{Z}_p$, so by Theorem 1.43, since $s \in \mathbb{Z}_p$, $d \in \mathbb{Z}^+$. This means that $d \geq 1$, as 1 is the smallest element in $\mathbb{Z}^+$. This means that $ds \geq 1s = s$, as $s \geq s$. Since $l > ds$, $l \geq ds$, so $l \geq s$, which is not true. Thus, our assumption that l is not an equivalence class is false.

Since l and v are equivalent classes, $n \in K$, as n is generated as $lv = ns$ by equivalence classes l and v of l and v respectively. Since m is the smallest element in K, we get that $m \leq n$. However, we found earlier that $n < m$. This is a contradiction, which means we can only conclude our original assumption, that S, the set of positive primes that does not have the property, is nonempty, is false. Thus, we find that all positive primes have the property.

In order to extend this to the negative primes as well, we will need to prove that primes and the property we're trying to prove of primes carry into the negatives.

Lemma 4.2. If p is prime, $-p$ is prime.

Proof. If $-p$ is not prime, then there exists some $b, c \in \mathbb{Z}$ such that $bc = -p$, but none of b, c are units. Since, $(-b)c = p$, one of $(-b), c$ is a unit. c is not a unit, so we must have $-b$ be a unit. However, if $-b$ is 1, $b = -1$, which is a unit, and if $-b = -1$, $b = 1$, which is also a unit, both contradicting our finding of b as not a unit. Since 1 and -1 are the only units, both cases for the value of $-b$ lead to contradiction, so we can only conclude that our assumption that $-p$ is not prime is false. Thus, $-p$ is prime.

Theorem 4.3. If some $p \in \mathbb{Z}$ has that if $p \mid ab$ then $p \mid a$ or $p \mid b$, $-p$ also has this property.

Proof. For any $b, c \in \mathbb{Z}$, if $-p \mid bc$, $bc = i(-p)$ for some $i \in \mathbb{Z}$, so $bc = (-i)p$, so $p \mid bc$. By definition, $p \mid c$ or $p \mid b$; without loss of generality let $p \mid b$. Then, $b = jp$ for some $j \in \mathbb{Z}$, so $b = (-j)(-p)$, so $(-p) \mid b$. Thus, $-p$ has this property.

Combining the previous results, we can extend our the property for positive primes into the negatives as well, proving The Fundamental Lemma.

Lemma 4.4. [Fundamental Lemma] If p is prime, then if $p \mid ab$, $p \mid a$ or $p \mid b$ for $a, b \in \mathbb{Z}$.

Proof. If $p \in \mathbb{Z}^+$, this is true by Lemma 4.1. Otherwise, since $p \neq 0$, $-p \in \mathbb{Z}^+$ by trichotomy. By Lemma 4.2, $-p$ is prime, so $-p$ satisfies this property by Lemma 4.1. By Theorem 4.3, then, $-(-p) = p$ satisfies this property.

2.5 Products

To continue, we will need to define and prove some things about products in order to use them to extend The Fundamental Lemma and to define factorizations for the Fundamental Theorem of Arithmetic.

Definition 5.1. $\prod_{i=b}^{n} a_i$ for some $n \geq b$ where $n, b \in \mathbb{Z}_p \cup \{0\}$ and a_i defined for all $b \leq i \leq n$ is defined where $\prod_{i=b}^{b} a_i = a_b$, and $\prod_{i=b}^{j} a_i = a_j \cdot \prod_{i=b}^{j-1} a_i$. For $n, \ngeq b$, $\prod_{i=b}^{n} a_i = 1$.

Theorem 5.2. $\prod_{i=b}^{n} a_i$ always is defined for $n \geq b$ and a_i defined for all $b \leq i \leq n$.

Proof. Let S be the set of $m \geq b$ such that $\prod_{i=b}^{m} a_i$ is not defined for a_i such that $b \leq i \leq n$. Lets assume for the sake of contradiction that S is nonempty. Thus, by WOP, we can define a smallest element s of S.

We know that $s \neq b$, as $\prod_{i=b}^{b} a_i$ is defined as a_b. Thus, $s - 1 \geq b$. Since $s - 1 < s$, $s - 1 \notin S$, so $\prod_{i=b}^{s-1} a_i$ is defined. Then, $\prod_{i=b}^{s} a_i = a_s \prod_{i=b}^{s-1} a_i$, so it is defined, so $s \notin S$. However, this creates a contradiction, as we defined s as the smallest element of S. Thus, our original assumption that S was nonempty must be false, so $n \notin S$. Thus, $\prod_{i=b}^{n} a_i$ is defined.

Lemma 5.3. $\prod_{i=1}^{n} p = p^n$.

Proof. $\prod_{i=1}^{n} p$ is defined with $\prod_{i=1}^{1} p = p$, and $\prod_{i=1}^{j} p = p \cdot \prod_{i=1}^{j-1} p$ for $1 < j \leq n$. p^n is defined with $p^0 = 1$, and $p^j = p \cdot p^{j-1}$ for $1 < j \leq n$, which gives that $p^1 = 1$. Thus, since both are defined in the same way, they have the same value.

Lemma 5.4. $\prod_{i=b}^{n} a_i = \left(\prod_{i=b}^{k} a_i\right) \cdot (\prod_{i=k+1}^{n} a_i)$ for $b \le k \le n$.

Proof. If $k = n$, then $k + 1 > n$, so $\prod_{i=k+1}^{n} a_i = 1$. Thus,

$$\left(\prod_{i=b}^{k} a_i\right) \cdot \left(\prod_{i=k+1}^{n} a_i\right) = \prod_{i=b}^{n} a_i \cdot 1 = \prod_{i=b}^{n} a_i.$$

Otherwise, $1 < k + 1 \le n$. Then, let S be the set of $k + 1 \le c \le n$ such that $\prod_{i=b}^{c} a_i \ne \left(\prod_{i=b}^{k} a_i\right) \cdot (\prod_{i=k+1}^{c} a_i)$. Lets assume for the sake of contradiction that S is nonempty. Then, we can define s as the smallest element of S by WOP.

We know that $s \ne k + 1$, as $\left(\prod_{i=b}^{k} a_i\right) \cdot \left(\prod_{i=k+1}^{k+1} a_i\right) = \prod_{i=b}^{k} a_i \cdot a_{k+1} = \prod_{i=b}^{k+1} a_i$. Thus, $s - 1 \ge k + 1$. Since $s - 1 < s$, $s - 1 \notin S$, so $\prod_{i=b}^{s-1} a_i = \prod_{i=b}^{k} a_i \cdot \prod_{i=k+1}^{s-1} a_i$. This means that

$$\prod_{i=b}^{k} a_i \cdot \prod_{i=k+1}^{s-1} a_i \cdot a_s = \prod_{i=b}^{k} a_i \cdot \prod_{i=k+1}^{s} a_i = \prod_{i=b}^{s-1} a_i \cdot a_s = \prod_{i=b}^{s} a_i.$$

Thus, $s \notin S$. However, this is a contradiction, as we defined s as the smallest element of S. Thus, our original assumption that S is nonempty is false, so $n \notin S$. Therefore, we have that $\prod_{i=b}^{n} a_i \ne \left(\prod_{i=b}^{k} a_i\right) \cdot (\prod_{i=k+1}^{n} a_i)$.

2.6 Extension of the Fundamental Lemma

We will now extend The Fundamental Lemma to work for a finite product of integers, instead of a product of just two.

Theorem 6.1. If p is prime and $p \mid \prod_{i=1}^{n} a_i$ for a_i defined with $1 \le i \le n$, then for some $1 \le j \le n$, $p \mid a_j$.

Proof. For some sequence of a_i defined with $1 \le i \le n$, let S be the set of $1 \le m \le n$ where there exists some prime q such that $q \mid \prod_{i=1}^{m} a_i$ such that there is no $1 \le j \le m$ such that $q \mid a_j$. Lets assume for the sake of contradiction that S is nonempty. Then, we can define s as the smallest element of S by WOP.

We know that $s \ne 1$, as $\prod_{i=1}^{1} a_i = a_1$, so if any p prime has that $q \mid \prod_{i=1}^{1} a_i$, $p \mid a_1$. Thus, $1 \le s - 1 \le n$. Since $s - 1 < s$, $s - 1 \notin S$, so if any p prime has that $q \mid \prod_{i=1}^{s-1} a_i$, there exists some $1 \le j \le m$ such that $q \mid a_j$. Now, since $s \in S$, there exists some q prime such that $q \mid \prod_{i=1}^{s} a_i$, so $q \mid (a_s \prod_{i=1}^{s-1} a_i)$, but $q \nmid a_s$. By The Fundamental Lemma, then, $q \mid \prod_{i=1}^{s-1} a_i$. Thus, there exists $1 \le j \le s - 1$ such that $q \mid a_j$, which means that $s \notin S$. This contradicts our definition of s as the smallest element of S, so our assumption that S is nonempty must be false, so $n \notin S$. Thus, if p prime has that $p \mid \prod_{i=1}^{n} a_i$ for $1 \le i \le n$, then there exists $1 \le j \le n$ such that $p \mid a_j$.

2.7 The Main Proof

Using all of this, we will now prove the Fundamental Theorem of Arithmetic. We will first define a canonical factorization, and then begin by proving that a factorization exists for positive integers greater than 1.

Definition 7.1. For $|n| > 1$, $\pm \prod_{i=1}^{r} p_i^{e_i} = n$ for $e_i \in \mathbb{Z}_p$ and positive primes p_i such that $p_i < p_{i+1}$ for $1 \le i < r$ is a canonical factorization of n.

Lemma 7.2. For every $n \in \mathbb{Z}^+$ such that $n > 1$, there exists a canonical factorization.

Proof. Let K be the set of $n > 1$ that do not have a canonical representation, and thus cannot be represented as $\prod_{i=1}^{r} p_i^{e_i}$. Lets assume for the sake of contradiction that K is nonempty. Then, we can define k as the smallest element of K by WOP.

Now, if k is prime, then for $p_1 = k$, $e_1 = 1$, $k = \prod_{i=1}^{1} p_1^{e_1} = p_1^{e_1} = k^1 = k$. This means that $k \notin K$, which contradicts our definition of k as the smallest element of K. Thus, we find that k can't be prime.

If k is not prime, then there exists a positive prime p by Theorem 2.3 such that $p \mid k$, so that $k = jp$

for $j > 1$, as if $j = 1$, then $k = p$ which we proved can't happen. Thus, since $p > 1, j < k$, so we must have that $j \notin K$. This means that $j = \prod_{i=1}^{r} p_i^{e_i}$ for some $e_i \in \mathbb{Z}^+$ and distinct positive prime p_i such that $p_i < p_{i+1}$.

If $p = p_m$ for some $1 \leq m \leq r$, then we have that

$$\begin{aligned} k &= jp_m \\ &= p_m \prod_{i=1}^{r} p_i^{e_i} \\ &= p_m \prod_{i=1}^{m-1} p_i^{e_i} \cdot \prod_{i=m}^{m} p_i^{e_i} \cdot \prod_{i=m+1}^{r} p_i^{e_i} \\ &= p_m \prod_{i=1}^{m-1} p_i^{e_i} \cdot p_m^{e_m} \cdot \prod_{i=m+1}^{r} p_i^{e_i} \\ &= \prod_{i=1}^{m-1} p_i^{e_i} \cdot \prod_{i=m+1}^{r} p_i^{e_i}. \end{aligned}$$

Then, we can define f_i as

$$f_i = \begin{cases} e_i + 1 & i = m \\ e_i & \text{otherwise} \end{cases}.$$

Thus, we have

$$\begin{aligned} \mathrm{k} &= \prod_{\mathrm{i}=1}^{\mathrm{m}-1} \mathrm{p}_\mathrm{i}^{\mathrm{e}_\mathrm{i}} \cdot \mathrm{p}_\mathrm{m}^{\mathrm{e}_\mathrm{m}+1} \cdot \prod_{\mathrm{i}=\mathrm{m}+1}^{\mathrm{r}} \mathrm{p}_\mathrm{i}^{\mathrm{e}_\mathrm{i}} \\ &= \prod_{\mathrm{i}=1}^{\mathrm{m}-1} \mathrm{p}_\mathrm{i}^{\mathrm{f}_\mathrm{i}} \cdot \mathrm{p}_\mathrm{m}^{\mathrm{f}_\mathrm{m}} \cdot \prod_{\mathrm{i}=\mathrm{m}+1}^{\mathrm{r}} \mathrm{p}_\mathrm{i}^{\mathrm{f}_\mathrm{i}} \\ &= \prod_{\mathrm{i}=1}^{\mathrm{m}-1} \mathrm{p}_\mathrm{i}^{\mathrm{f}_\mathrm{i}} \cdot \prod_{\mathrm{i}=\mathrm{m}}^{\mathrm{m}} \mathrm{p}_\mathrm{i}^{\mathrm{f}_\mathrm{i}} \cdot \prod_{\mathrm{i}=\mathrm{m}+1}^{\mathrm{r}} \mathrm{p}_\mathrm{i}^{\mathrm{f}_\mathrm{i}} \\ &= \prod_{\mathrm{i}=1}^{\mathrm{r}} \mathrm{p}_\mathrm{i}^{\mathrm{f}_\mathrm{i}}. \end{aligned}$$

On the other hand, if $p \neq p_m$ for any $1 \leq m \leq r$, we can find the set I of $1 \leq i \leq r$ such that $p_i > p_m$.

If I is nonempty, we can find a smallest element j by WOP. Thus, we have that

$$k = jp = p \prod_{i=1}^{r} p_i^{e_i} = \prod_{i=1}^{j-1} p_i^{e_i} \cdot p^1 \cdot \prod_{i=j}^{r} p_i^{e_i}.$$

We can then define f_i, q_i as

$$f_i = \begin{cases} 1 & i = j \\ e_i & i < j \\ e_{i-1} & \text{otherwise} \end{cases}.$$

and

$$q_i = \begin{cases} p & i = j \\ p_i & i < j \\ p_{i-1} & \text{otherwise.} \end{cases}$$

This means that

$$k = \prod_{i=1}^{j-1} p_i^{e_i} \cdot p^1 \cdot \prod_{i=j}^{r} p_i^{e_i} = \prod_{i=1}^{j-1} q_i^{f_i} \cdot q_j^{f_j} \cdot \prod_{i=j+1}^{r+1} q_i^{f_i} = \prod_{i=1}^{j-1} q_i^{f_i} \cdot \prod_{i=j}^{j} q_i^{f_i} \cdot \prod_{i=j+1}^{r+1} q_i^{f_i} = \prod_{i=0}^{r+1} q_i^{f_i}.$$

This maintains the property that $q_i < q_{i+1}$. If $i < j - 1$, $q_i, q_{i+1} = p_i, p_{i+1}$, so this property carries over. If $i = j - 1$, $i \notin I$, as $i < j$, the smallest element, so $p_i \leq p$, and we assumed that $i \neq p_j = p$, so $p_i < p$, so $q_i = q_{j-1} < p = q_j$. If $i = j$, then since $j \in I$, $p < p_j$, so $q_i = q_j < c_j = q_{j+1}$. Finally, if $i > j$, then $p_{i-1} < p_i$ carries over, so $q_i < q_{i+1}$.

Now, if I is empty, $p \geq p_i$ for all $1 \leq i \leq r$. Define

$$f_i = \begin{cases} 1 & i = r + 1 \\ e_i & \text{otherwise} \end{cases}.$$

and

$$q_i = \begin{cases} p & i = r + 1 \\ p_i & \text{otherwise.} \end{cases}$$

Thus, we have

$$k = jp = \prod_{i=1}^{r} p_i^{e_i} \cdot p = \prod_{i=1}^{r} q_i^{f_i} \cdot q_{r+1}^{f_{r+1}} = \prod_{i=1}^{r+1} q_i^{f_i}.$$

The q_i have the property that $q_i < q_{i+1}$, as if $i < r$, then $q_i = p_i < p_{i+1} = q_{i+1}$. Otherwise, if $i = r$, $p_i \notin I$ as I is empty, so $p_i \geq p$, and $p_i \neq p$, so $p_i = q_i = q_r < p = q_{r+1} = q_{i+1}$.

Thus, we find that we always get a canonical factorization of k, so $k \notin K$. However, this contradicts our definition of k as the smallest element of K, so we can only conclude that our assumption that K is nonempty is false. Thus, all $n > 1$ have a canonical factorization.

We will now extend the previous lemma to all nonunit nonzero integers.

Lemma 7.3. For every $n \in \mathbb{Z}$ such that $|n| > 1$, there exists a canonical factorization.

Proof. If $|n| > 1$, $n \neq 0, 1, -1$, so either $n > 1$ or $-n > 1$. If $n > 1$, then by Lemma 7.2, n has a canonical factorization by definition. Otherwise, if $-n > 1$, then by Lemma 7.2, $-n$ has a canonical factorization, so $-n = \prod_{i=1}^{r} p_i^{e_i}$. Thus, $n = -\prod_{i=1}^{r} p_i^{e_i}$, so n has a canonical factorization.

We will now prove that these canonical factorizations are unique for positive integers. We will begin by proving that the canonical factorizations follow a certain form, and then prove they are all the same for any given positive integer greater than 1.

Lemma 7.4. If $n > 1$, then any canonical factorization of n is in the form $\prod_{i=1}^{r} p_i^{e_i}$.

Proof. By definition, any canonical factorization of n is in the form $\pm \prod_{i=1}^{r} p_i^{e_i}$.

Now, we will attempt to prove that $\prod_{i=1}^{r} p_i^{e_i} \in \mathbb{Z}^+$.

Let S be the set of $1 \leq j \leq r$ such that $\prod_{i=1}^{j} p_i^{e_i} \notin \mathbb{Z}^+$, and lets assume for the sake of contradiction that S is nonempty. Then, by WOP, we can choose s as the smallest element of S.

We have that $s \neq 1$, as $\prod_{i=1}^{1} p_i^{e_i} = p_1^{e_1} \in \mathbb{Z}^+$, as p_1 is a positive prime. Thus, $s - 1 \geq 1$. Since $s - 1 < s$, $s - 1 \notin s$, so $\prod_{i=1}^{s-1} p_i^{e_i} \in \mathbb{Z}_p$. Thus, $\prod_{i=1}^{s} p_i^{e_i} = p_s^{e_s} \prod_{i=1}^{s-1} p_i^{e_i} \in \mathbb{Z}^+$ by multiplicative closure, as p_s is a positive prime. Thus, $s \notin S$, which contradicts our definition of s as the smallest element of S. Thus, our original assumption that S is nonempty is false, so $r \notin S$. Thus, $\prod_{i=1}^{r} p_i^{e_i} \in \mathbb{Z}^+$.

This means that $-\prod_{i=1}^{r} p_i^{e_i} \notin \mathbb{Z}^+$. However, $n \in \mathbb{Z}^+$, so $n \neq -\prod_{i=1}^{r} p_i^{e_i}$, so $n = \prod_{i=1}^{r} p_i^{e_i}$.

Theorem 7.5. For $n > 1$, any two canonical factorizations are the same.

Proof. Using Lemma 7.4, let $\prod_{i=1}^{r} p_i^{e_i}$ and $\prod_{j=1}^{t} q_j^{f_j}$ be canonical factorizations of n, which we will prove are the same.

To prove this, we will have to prove that $r = t$, and $p_i = q_j$, $e_i = f_j$ for $1 \leq i \leq r$ and $1 \leq j \leq t$ when $i = j$. We will first prove that $p_i = q_j$ when $i = j$. Lets assume without loss of generality that $r \leq t$. First, let S be the set of $1 \leq i \leq r$ such that $p_i \neq q_i$. Lets assume for the sake of contradiction that S is nonempty. We can then define x as the smallest element of S by WOP. Using Lemma 5.4, we have that

$$n=\prod_{i=1}^{r}p_i^{e_i}=\prod_{i=1}^{s-1}p_i^{e_i}\cdot p_s^{e_s}\cdot\prod_{i=s+1}^{r}p_i^{e_i}.$$

Similarly,

$$n=\prod_{j=1}^{t}q_j^{f_j}=\prod_{j=1}^{s-1}q_j^{f_j}\cdot q_s^{f_s}\cdot\prod_{j=s+1}^{t}q_j^{f_j}.$$

Thus, $p_s, q_s \mid n$. We have $p_s \neq q_s$. Lets assume without loss of generality that $q_s > p_s$. For all $j > s$, $q_j > q_s > p_s$, and for $j < s$, $q_j = p_j < p_s$ by Lemma 1.44. Thus, there exists no j such that $q_j = p_s$. Since $p_s \mid n = \prod_{j=1}^{t} q_j^{f_j}$, by Theorem 6.1, $p_s \mid q_j^{f_j}$ for some $1 \leq j \leq r$. By Lemma 5.3, $q_j^{f_j} = \prod_{i=1}^{f_j} q_j$. Thus, again by Theorem 6.1, $p_s \mid q_j$. Thus, $dp_s = q_j$ for some $d \in \mathbb{Z}^+$, as $p_s, q_j \in \mathbb{Z}^+$. Since p_s is a positive prime, $p_s > 1$, and is thus not a unit, so d must be a unit and thus is 1. This gives that $1 \cdot p_s = p_s = q_j$. However, this contradicts what we found that $q_j \neq p_s$. Thus, our original assumption that S was nonempty must be false, so $p_i = q_i$ for all $1 \leq i \leq r$. Now, lets assume for the sake of contradiction that $r \neq t$, so $r < t$, as we assumed that $r \leq t$. Thus, q_{r+1} exists, but p_{r+1} doesn't. Now, we found that $p_r = q_r$, so for all $1 \leq i \leq r$, $p_i \leq p_r = q_r < q_{r+1}$. This means that there exists no p_i such that $p_i = q_{r+1}$. We have that $q_{r+1} \mid n$, as

$$n=\prod_{j=1}^{t}q_j^{f_j}=\prod_{j=1}^{r}{q_j}^{f_j}\cdot q_{r+1}^{f_{r+1}}\cdot\prod_{j=r+2}^{t}q_j^{f_j}.$$

Then, by Theorem 6.1, since $q_{r+1} \mid n = \prod_{i=1}^{r} p_i^{e_i}$, $q_{r+1} \mid p_i^{e_i}$ for some i. This is equal to $\prod_{i=1}^{e_i} p_i$, so again by Theorem 6.1, $q_{r+1} \mid p_i$. Thus, $p_i = dq_{r+1}$ for some $d \in \mathbb{Z}_p$. Since q_{r+1} is not a unit, d must be by the definition of prime, so $d = 1$. Thus, $p_i = 1 \cdot p_i = q_{r+1}$. We found that this is not true, so our assumption that $r \neq t$ is false, so $r = t$. Finally, we will attempt to prove that $e_k = f_k$ for all $1 \leq k \leq r = t$. Lets assume that there exists $1 \leq k \leq r$ such that $e_k \neq f_k$. Then, we have that by Lemma 5.4,

$$n=\prod_{i=1}^{r}p_i^{e_i}=\prod_{i=1}^{k-1}p_i^{e_i}\cdot p_k^{e_k}\cdot\prod_{i=k+1}^{r}p_i^{e_i},$$

$$n=\prod_{j=1}^{r}q_j^{f_j}=\prod_{i=1}^{r}p_i^{f_i}=\prod_{i=1}^{k-1}p_i^{f_i}\cdot p_k^{f_k}\cdot\prod_{i=k+1}^{r}p_i^{f_i}.$$

Now, lets assume without loss of generality that $e_k \leq f_k$, so $e_k < f_k$ as we assumed that $e_k \neq f_k$. Then,

$$n/(p^{e_k})=\prod_{i=1}^{k-1}p_i^{e_i}\cdot\prod_{i=k+1}^{r}p_i^{e_i}=\prod_{i=1}^{k-1}p_i^{f_i}\cdot p_k^{f_k-e_k}\cdot\prod_{i=k+1}^{t}p_i^{f_i}.$$

Thus, $p_k^{f_k-e_k} \mid n/(p^{e_k})$, so $p_k \mid n/(p^{e_k})$.

For any other $1 \leq i \leq n$ where $i \neq k$, $p_k \neq p_i$, as either $i < k$ or $i > k$, so $p_i < p_k$ or $p_i > p_k$ respectively. Now, define c_i as

$$c_i=\begin{cases}p_i & i<k\\ p_{i+1} & \text{otherwise}\end{cases}$$

and g_i as

$$g_i=\begin{cases}e_i & i<k\\ e_{i+1} & \text{otherwise.}\end{cases}$$

This gives us that

$$n=\prod_{i=1}^{r-1}c_i^{g_i}.$$

Since no p_i has that $p_i = p_k$ where $i \neq k$ no c_i has that $c_i = p_k$, as $c_i = p_j$ for some $j \neq k$.

By Theorem 6.1, $p_k \mid c_i^{g_i}$ for some $1 \leq i \leq r-1$. Since $c_i^{g_i} = \prod_{j=1}^{g_i} c_i$ by Lemma 5.3, $p_k \mid c_i$ by Theorem 6.1. This means that $c_i = dp_k$ for some $d \in \mathbb{Z}^+$. Since p_k is not a unit, d must be, so $d = 1$. Then, $c_i = 1 \cdot p_k = p_k$. However, this is not possible, as $c_i = p_j$ for some j, but we found that $p_j \neq p_k$. Thus, our original assumption that $f_k \neq e_k$ must be false, so for all $1 \leq i \leq r$, $e_i = f_i$. Since we have $r = t$, $p_i = q_i$, and $e_i = f_i$, both canonical factorizations are the same. We can now extend the uniqueness of the canonical factorization to all integers and then bring our results together to prove the Fundamental Theorem of Arithmetic.

Theorem 7.6 (Fundamental Theorem of Arithmetic). For all $n \in \mathbb{Z}$ such that $|n| > 1$, n has a unique canonical factorization.

Proof. We have that $n \neq 0$, as $|0| = 0 \ngtr 1$. Thus, either $n \in \mathbb{Z}^+$ or $-n \in \mathbb{Z}^+$, so either $n > 1$ or $-n > 1$. If $n > 1$, then we have by Theorem 7.5 that any two canonical factorizations of n are the same, so there is only one unique one. If $-n > 1$, $-\prod_{i=1}^{r} p_i^{e_i}$ and $-\prod_{j=1}^{t} p_j^{e_j}$ are canonical factorizations of n, then $\prod_{i=1}^{r} p_i^{e_i}$ and $\prod_{j=1}^{t} p_j^{e_j}$ are canonical factorizations for $-n$ according to Lemma 7.4. Since $\prod_{i=1}^{r} p_i^{e_i} = \prod_{j=1}^{t} p_j^{e_j}$ by Theorem 7.5, $-\prod_{i=1}^{r} p_i^{e_i} = -\prod_{j=1}^{t} p_j^{e_j}$, and since all canonical factorizations of n are the same, it has a single unique one.

3. Conclusion

Using the Fundamental Theorem of Arithmetic, relations between integers can be found much more easily by representing them as their canonical factorizations. For example, noting that $463050 = 2 \cdot 3^3 \cdot 5^2 \cdot 7^3$ and $129360 = 2^4 \cdot 3 \cdot 5 \cdot 7^2 \cdot 11$, we can find $\gcd(463050{,}43120)$ as $2^{\min(1,4)} \cdot 3^{\min(3,1)} \cdot 5^{\min(2,1)} \cdot 7^{\min(3,2)} = 2^1 \cdot 3^1 \cdot 5^1 \cdot 7^2 = 1470$. As such, it is a theorem that shows up in many places in the field of Number Theory, from simple observations like 0 and 1 are the only consecutive perfect squares, finding greatest common divisors, and thus to complex theorems including Quadratic Reciprocity Law, Chinese remainder theorem, and Minkowski's theorem.

References

[1] Rosenthal D, Rosenthal P, et al. The Fundamental Theorem of Arithmetic[J]. A Readable Introduction to Real Mathematics, 2014: 31-34.

[2] Apostol T M, The fundamental theorem of arithmetic[J]. Introduction to Analytic Number Theory, 1976: 13-23.

[3] Gauss, C. F.; Clarke, A. A., Disquisitiones Arithmeticae[M]. Yale University Press: 1965.

[4] Zhang W. The arithmetic fundamental lemma: An update[J]. Science China Mathematics, 2019, 62(11): 2409-2422.

[5] Li C, Zhu Y. Remarks on the arithmetic fundamental lemma[J]. Algebra & Number Theory, 2017, 11(10): 2425-2445.

[6] Nei jiang. A Note on Well-Ordering Principle[J].Journal of Neijiang Teachers College, 2001.

[7] Rathjen M, Vizcaíno P F V. Well-Ordering Principles and Bar Induction[J]. Gentzen's Centenary: The Quest for Consistency, 2015: 533-561.