Proving UFT

ATTICUS KUHN

June 2022

Contents

§1 Abstract

In this paper, we will start from only knowing basic rules of logic plus the axioms of the integers, and from them, prove the Unique Factorization Theorem (Canonical Prime Factorization) over the integers. To see how it will be done, look at figure A flow-chart of how we will prove the Unique Factorization Theorem.

§2 Axioms

For the purposes of this paper, we will assume the rules of logic. These include substitution, Modus Ponnedo Punnens, Modus Tullendo Tunnens, and Hypothetical Syllogism.

Definition 2.1 (Ring)**.** A **ring** is defined as the 3-tuple $(S, +, \times)$. Where S is a set, and $+ : S \to S \to S$ and $\times : S \to S \to S$ are binary operations on S that satisfy the ring axioms (see Ring Axioms).

Axiom 2.2 (Ring Axioms)**.** All rings satisfy the 8 ring axioms.

1. (Commutivity of Multiplication) $ab = ba$
2. (Commutivity of Addition) $a + b = b + a$
3. (Distributivity) $a(b + c) = ab + ac$
4. (Associativity of Addition) $a + (b + c) = (a + b) + c$
5. (Associativity of Multiplication) $a(bc) = (ab)c$
6. (Zero) $a + 0 = a$

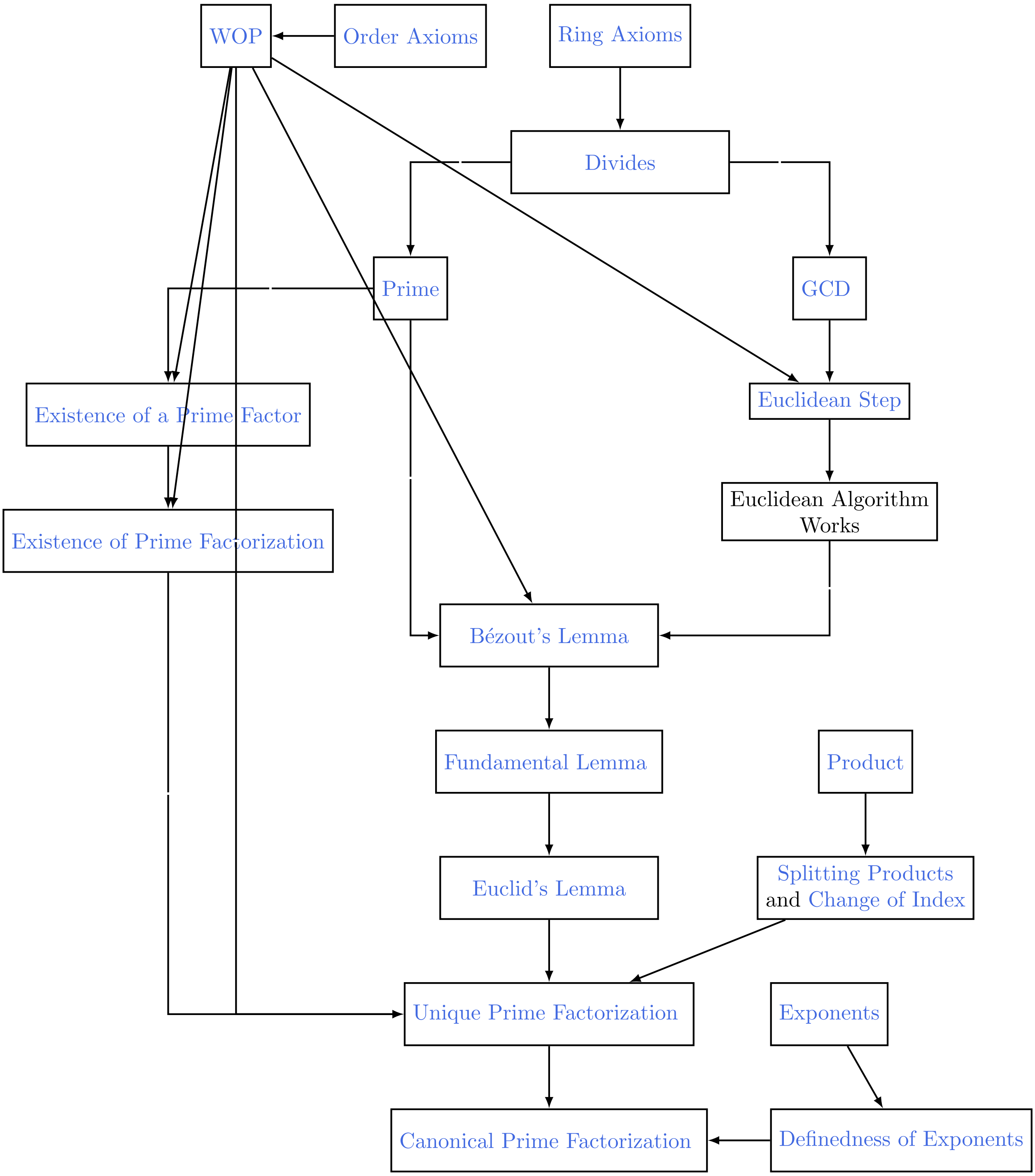

Figure 1: A flow-chart of how we will prove the Unique Factorization Theorem

7. (One) $a \cdot 1 = a$
8. (Inverses) $a + (-a) = 0$

Axiom 2.3 (Order Axioms)**.** All ordered rings satisfy the 4 order axioms. We call the set of all positive elements of a ring P.

1. (exists) P exists and is non-empty
2. (non-triviality) $0 \notin P$
3. (Addition) $P + P \in P$
4. (Multiplication) $P \cdot P \in P$

Axiom 2.4 (WOP)**.** Every non-empty positive (see axiom Order Axioms) set of integers has a minimal element. In other words, given a non-empty set of positive integers S, there exists an $m \in S$ such that for all $n \in S$, $m \leq n$.

Definition 2.5 (Integers)**.** The **integers** are defined as a as ordered ring the set of whose positive elements satisfy WOP.

Definition 2.6 (Subtraction)**.** Define the **subtraction** of a and b to be $a - b = a + (-b)$

Theorem 2.7 (Right Cancel)
If $a + c = b + c$, then $a = b$.

Proof.

$$\begin{aligned} a &= a + 0 \text{ zero axiom} \\ &= a + (c + (-c)) \text{ negatives axiom} \\ &= (a + c) + (-c) \text{ associativity} \\ &= (b + c) + (-c) \text{ substitution} \\ &= b + (c + (-c)) \text{ associativity} \\ &= b + 0 \text{ negatives axiom} \\ &= b \end{aligned}$$

□

Theorem 2.8 (Left Cancel)
If $c + a = c + b$, then $a = b$.

Proof. Apply commutativity of addition, and then Theorem Right Cancel.

□

Lemma 2.9 (Zero times Anything)
$a * 0 = 0$

Proof.

$$a = a*1 = a*(1+0) = a*1+a*0 \implies a*1+0 = a*1+a*0 \implies 0 = a*0 \implies a*0 = 0$$

□

Theorem 2.10 (Add Both)
If $a = b$, and $x = y$ then $a + x = b + y$.

Proof. Use substitution. □

Theorem 2.11 (Multiply Both)
If $a = b$, then $ac = bc$.

Proof. Use substitution. □

Definition 2.12 (Ordering)**.** For two integers a, b, we say $a > b$ if there exists a positive integer p such that $a = b + p$. We say $a < b$ if there exists a positive integer p such that $a + p = b$. We say $a \leq b$ if $a < b$ or $a = b$. We say $a \geq b$ if $a > b$ or $a = b$.

Theorem 2.13 (Positives are Greater than 0)
a is positive if and only if $a > 0$

Proof. We have $a = 0 + a$ by the ring axioms, and since a is positive, we use definition Ordering to say $a > 0$. □

Definition 2.14 (Divides)**.** Given two integers a, b, we say a **divides** b, written as $a \mid b$, if there exists an $m \in R$ such that $am = b$.

Theorem 2.15 (Trivial Divisors)
For all a, $a \mid a$ and $1 \mid a$.

Proof. From the One axioms and commutativity, we know that $a * 1 = a$ and $1 * a = a$. Use definition Divides with $a * 1 = a$ and $1 * a = a$ to see that $a \mid a$ and $1 \mid a$. □

Theorem 2.16 (Linear Combination Divides)
For all integers a, b, c, d, e, if $a \mid b$ and $a \mid c$ the $a \mid (bd + ce)$.

Proof. By Definition Divides,

$$ax = b, ay = c, x, y \in \mathbb{Z}.$$

Use Theorem Multiply Both to get

$$axd = bd, aye = ce.$$

Use Theorem Add Both to get

$$axd + aye = bd + ce.$$

Use distributivity to say

$$a(xd + ye) = bd + ce \implies a \mid (bd + ce).$$

□

Definition 2.17 (GCD)**.** Given two positive integers a, b, define $gcd(a, b) = c$ if $c \mid a$ and $c \mid b$ and if $d \mid a$ and $d \mid b$ then $c \geq d$.

Lemma 2.18 (Positives are not 0)

If a is positive, then $a \neq 0$

Proof. Proof by contradiction. If $a = 0$, then we can substitute to say that 0 is positive, but this contradicts the non-triviality axiom. □

Lemma 2.19 (Double Negative)

$-(-a) = a$

Proof. By the negatives axiom, we know $a + (-a) = 0$ and $-a + -(-a) = 0$. Use substitution to get

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

Apply commutativity of addition and then Theorem Right Cancel to get $a = -(-a)$. □

Lemma 2.20 (Distribution of Negative)

We have 3 rules

1. $(-a)b = -ab$
2. $a(-b) = -ab$
3. $(-a)(-b)$

Proof. In case (1), we have $0 = 0 * b = (a + (-a))b = ab + (-a)b$. But by negatives, we know that $ab + (-ab) = 0$, so we use substitution and then Theorem Left Cancel to get $(-a)b = -ab$. In case (2), use commutativity of multiplication and then do case (1). In case (3), apply case (1) and (2) to get $(-a)(-b) = -(-ab)$. Then use Lemma Double Negative to get $(-a)(-b) = ab$.

□

Theorem 2.21 (Zero Or)

If $ab = 0$, then $a = 0$ or $b = 0$

Proof. By the trichotomy axiom on a and b, either a is positive, $a = 0$, or $-a$ is positive and b is positive, $b = 0$, or $-b$ is positive. We can eliminate the case where $a = 0$ or $b = 0$ because from those we can immediately draw the conclusion. We have 4 remaining cases. In each case, use Lemma Distribution of Negative then Lemma Positives are not 0 to conclude that $ab \neq 0$.

1. a is positive and b is positive implies that ab is positive,so $ab \neq 0$
2. a is positive and $-b$ is positive implies that $a(-b)$ is positive, so $-ab$ is positive so $ab \neq 0$
3. $-a$ is positive and b is positive implies that $(-a)b$ is positive, so $-ab$ is positive so $ab \neq 0$
4. $-a$ is positive and $-b$ is positive implies that $(-a)(-b)$ is positive, so ab is positive so $ab \neq 0$

This means the only option is that $a = 0$ or $b = 0$, so we are done. □

Theorem 2.22 (Cancellation of Multiplication)
if $ax = ay$ and $a \neq 0$ then $a = y$

Proof.
$$ax = ay \implies ax - ay = 0 \implies a(x - y) = 0.$$
Use Theorem Zero Or to conclude that $a = 0$ or $x - y = 0$, but $a \neq 0$, so $x - y = 0$. This means that $x = y$ □

Theorem 2.23
For all positive integers a, b, if $a \mid b$ and $b \mid a$, then $a = b$

Proof. By Definition Divides, we can write $ax = b$ and $by = a$ for some integers x, y. Substituting, we get $axy = a \implies xy = 1$ by Theorem Cancellation of Multiplication. If x or y equals 1, then we are done. Otherwise, by Lemma Multiplication $\implies <$, we can say one of x, y is less than 1. But since x, y are both positive, this contradicts Theorem NIBZO. This means the only options is that $x, y = 1$ so $a = b$

□

Theorem 2.24 (Transitivity of Divisibility)
If $a \mid b$ and $b \mid c$ then $a \mid c$

Proof. By Definition Divides, we can say $ax = b$ and $by = c$ for $x, y \in \mathbb{Z}$. Substitute the first equation into the second to get $axy = c$. By Defintion Divides, we get $a \mid c$ □

Lemma 2.25 (Trichotomy of $<$)
For any a, b, exactly one of $a > b$, $a = b$ or $a < b$ holds.

Proof. Let $k = a - b$. By the trichotomy axiom, we have that exact one of the following is true: k is positive, $k = 0$, or $-k$ is positive. If k is positive, then $k + b = a$, so $b < a$ by Ordering. If $k = 0$, then $0 = a - b \implies a = b$. If $-k$ is positive, then $k = a - b \implies b = a + (-k)$, so $b > a$ by Ordering. □

Lemma 2.26 (Transitivity of $<$)
If $a < b$ and $b < c$ then $a < c$

Proof. By Ordering, we can say

$$a + p = b, b + q = c, p, q \in P.$$

By Substitution, we have

$$a + (p + q) = c.$$

The order axioms tell us that $p + q \in P$, so we can use Definition Ordering to get $a < c$. □

Lemma 2.27 (Times on $<$)
If $a < b$ and x is positive, then $ax < bx$

Proof. By Definition Ordering, we say that $a + p = b$ where p is positive. Use Theorem Multiply Both to say

$$(a + p)x = bx \implies ax + px = bx$$

. By Axiom Order Axioms, we get that px is positive. This means by Definition Ordering that $ax < bx$ □

Theorem 2.28 (NIBZO)
There is no integer between 0 and 1.

Proof. For the sake of contradiction, assume there exists an integer between 0 and 1. For WOP, construct the set

$$S = \{x \in \mathbb{N} \mid 0 < x < 1\}.$$

By our hypothesis, S is non-empty, so apply axiom WOP to produce a minimal element $m \in S$. We know x is positive by Theorem Positives are Greater than 0. We can apply lemma Times on $<$ to get

$$0 < x < 1 \implies 0 * 0 < x * x < 1 * 1 \implies 0 < x * x < 1.$$

This means $x * x \in S$. But by applying lemma Times on $<$ to $x < 1$, we see that $x * x < x$, and this contradicts the minimality of x. This means that the hypothesis was incorrect, and there is not integer between 0 and 1. □

Corollary 2.29 (Positive ≥ 1)

if a is positive, then $a \geq 1$

Proof. Apply Theorem NIBZO to Lemma Trichotomy of $<$ to get $a = 1$ or $a > 1$, and that is the definition of $a \geq 1$. □

Lemma 2.30 (Divides implies Less than)

If a and b are positive and $a \mid b$ then $a \leq b$

Proof. Apply Divides to get $ap = b$ for some positive integer p. Use algebraic manipulation to get

$$ap = b \implies p(a-1) + a = b.$$

Since a is positive, apply Corollary Positive ≥ 1 to get $a \geq 1 \implies a - 1 \geq 0$. There are 2 cases by the definition Ordering. If $a - 1 = 0$, then $p * 0 + a = b \implies a = b$. Otherwise, $a - 1 > 0$, so by Theorem Positives are Greater than 0, $a - 1$ is positive, so $p(a-1)$ is positive by Axiom Order Axioms. This means $a < b$ by Definition Divides. □

Lemma 2.31 (Squared Greater)

If a is positive and $a \neq 1$, then $a * a > a$

Proof. Apply the condition $a \neq 1$ to corollary Positive ≥ 1 to get $a > 1$. Then use lemma Times on $<$ to get $a * a > a$. □

Lemma 2.32 (Multiplication $\implies <$)

If $xy = a$ and $x \neq a$ and $y \neq a$ then at least one of x, y is less than a.

Proof. Apply lemma Trichotomy of $<$ to x and y. By our givens that $x, y \neq a$, we know that $x > a$ or $x < a$ and $y < a$ or $y > a$. If either or $x < a$ or $y < a$ holds, then we are immediately done. Otherwise, the only other option is that $x > a$ and $y > a$. Apply lemma Times on $<$ to get $xy > a * a$. Substitute in $xy = a$ to get $a > a * a$. This contradicts lemma Squared Greater by lemma Trichotomy of $<$, so we are done. □

Theorem 2.33 (Multiplication Less)

If $ab = c$ and $a > 1$ then $b < c$.

Proof. Apply Lemma Times on $<$ to $a > 1$. □

Lemma 2.34 (Reverse WOP)

Every non-empty set of integers bounded from above has a maximal element

Proof. Let S be a set of integers. Let b be an upper bound, i.e. for all $s \in S$, $b \geq s$. Construct the set

$$S' = \{b - x \mid x \in S\}.$$

All elements of S' are positive because

$$b \geq s \implies b - s \geq 0.$$

Apply WOP to get a minimal element $m \in S'$. By construction $m = b - x$. I claim that x is the maximal element of S. Choose an arbitrary element $l \in S$. Since m is the minimal element of S', we can say $m \leq b - l \implies b - x \leq b - l \implies x \geq l$. So we are done □

Lemma 2.35 (Irreflexivity of $<$)
There is no a such that $a < a$

Proof. Proof by contradiction, assume $a < a$. By Ordering, there is a positive number p such that $a + p = a$. Apply Left Cancel to get $p = 0$. But this contradicts Order Axioms because 0 is not positive, so our assumption was wrong and there is no a such that $a < a$. □

Lemma 2.36 (Anti-Symmetry of $\leq$)
if $a \leq b$ and $b \leq a$ then $a = b$

Proof. By definition Ordering, we have $a = b$ or $a < b$ and $b < a$ or $a = b$. If either of the equality cases hold, we are immediately done. If the inequalities hold, then we can conclude by Transitivity of $<$ that $a < a$, but this contradicts Irreflexivity of $<$, so we are done. □

§3 Number Theory

Theorem 3.1 (GCD Always Exists)
For any positive integers a and b, $gcd(a, b)$ always exists and is defined.

Proof. Consider the set

$$S = \{x \mid x \mid a \wedge x \mid b\}$$

We know S is non-empty because $1 \in S$ by Trivial Divisors. Use Lemma GCD Always Exists to get a maximal element of S. This maximal element satisfies GCD, so we are done. □

Definition 3.2 (Prime)**.** An integer is said to be **prime** if that for all $d \mid p$, then $d = 1$ or $d = p$.

Theorem 3.3 (Prime GCD 1)
For any prime p and any other integer $p \nmid a$, $gcd(a, p) = 1$

Proof. Let $d = gcd(a, p)$. By GCD, $d \mid a$ and $d \mid p$. By Prime, either $d = 1$ or $d = p$. If $d = 1$, we are done. If $d = p$, then we have $d \mid a \implies p \mid a$, but this contradicts our givens. The only option is that $d = 1$. □

Lemma 3.4 (Euclidean Step)

For all positive integers $a, b \in \mathbb{Z}$, there exists $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < b$

Proof. Fix a and b. Consider the set

$$S = \{a - bq \mid q \in \mathbb{Z}, a - bq \geq 0\}.$$

S is non-empty because $a - b * 0 \in S$. Furthermore, S is positive by construction. By WOP, S has a minimal element, call it m. By construction, $m = a - bq > 0$. For the sake of contradiction, assume $m \geq b$. This means

$$m - b \geq 0 \implies a - bq - b \geq 0 \implies a - (b + 1)q \geq 0.$$

We have that $a - (b + 1)q \geq 0$, which means $a - (b + 1)q \in S$. But this is a contradiction of the minimality of m. This contradicts our assumption that $m \geq b$, which means that $m < b$. Call $r = m$, and we are done. □

Theorem 3.5 (Bézout's Lemma)

For all positive integers a, b, there exist integers x, y such that $ax + by = gcd(a, b)$

Proof. Fix a and b. Consider the set

$$S = \{ax + by \mid ax + by \geq 0, x, y \in \mathbb{Z}\}.$$

S is non-empty because $a \in S$. All elements of S are positive by construction. This means S has a minimal element, call it m by WOP. By the construction of m, let

$$m = ax' + by'$$

for some integers x', y'. By lemma Euclidean Step, there exists integers q, r such that $a = mq + r$ and $0 \leq r < m$. Since $r < m$ and m is the minimal element of S, it follows that $r \notin S$. By algebraic manipulation, we have

$$r = a - mq = a - (ax' + by')q = a - ax' - by'q = a(1 - x') + b(-y'a).$$

We find that r is expressible as $ax + by$ (with $x = 1 - x'$ and $y = -y'a$), so the only way that $r \notin S$ is that $r \leq 0$. By construction, we know $r \geq 0$, so this means $r = 0$. This gives us that $0 = a - mq \implies a = mq$, which gives that $m \mid a$ by Definition Divides. By similar reasoning, we can deduce $m \mid b$. Let $d = gcd(a, b)$. By the definition of GCD, we have $d \mid a$ and $d \mid b$. This means by Theorem Linear Combination Divides that $d \mid (ax' + by')$. But $ax' + by' = m$, so $d \mid m$. By Lemma Divides implies Less than, we have $d \leq m$. But m is a common divisor of both a and b, so by Definition GCD, $d \geq m$. The only possibility by Lemma Anti-Symmetry of $\leq$ is that $d = m$. We have $m = d$. This means that there exists x, y such that $ax + by = gcd(a, b)$, and in addition, $gcd(a, b)$ is the smallest positive combination of a, b. □

§4 UFT

Theorem 4.1 (Fundamental Lemma)
For all integers a, b, c, if $a \mid bc$ and $gcd(a, b) = 1$, then $a \mid c$.

Proof. By Theorem Bézout's Lemma, then there exists integers x, y such that

$$ax + by = 1. \tag{1}$$

By Definition Divides, there exists an integer m such

$$am = bc. \tag{2}$$

Multiply both sides of (1) by c with Theorem Multiply Both to get

$$acx + bcy = c. \tag{3}$$

Substitute (2) into (3) to get

$$acx + amy = c \implies a(cx + my) = c \implies a \mid c.$$

□

Definition 4.2 (Product)**.** For a given sequence of integers $a_i : \mathbb{N} \to \mathbb{Z}$, define the notation Π to be

$$\prod_{i=n}^{n} a_i = a_n$$

and

$$\prod_{i=k}^{n} a_i = a_n \prod_{i=k}^{n-1} a_i$$

Theorem 4.3 (Definedness of Products)
For all rings R, for all sequences $a_i : \mathbb{N} \to R$, for all natural numbers $n \in \mathbb{N}$, the product

$$\prod_{i=0}^{n} a_i$$

exists and is defined

Proof. Fix a_i and R. Assume for the sake of contradiction that there is some $n \in \mathbb{N}$ so that

$$\prod_{i=0}^{n} a_i$$

does not exist. For WOP, let

$$S = \left\{ n \in \mathbb{N} \mid \nexists h \in R, h = \prod_{i=0}^{n} a_i \right\}.$$

We know S is non-empty by our assumption, and all elements of S are positive, so use Axiom WOP to get a minimal element $m \in S$. We have by construction that

$$\prod_{i=0}^{m} a_i \notin R.$$

If $m = 0$, then

$$\prod_{i=0}^{m} a_i = a_0 \in R,$$

which is a contradiction. Otherwise, apply Product to get

$$a_m \prod_{i=0}^{m-1} a_i \notin R,$$

Then, since $m - 1 < m$, we know

$$\prod_{i=0}^{m-1} a_i \in R.$$

By closure of multiplication, we know

$$a_m \prod_{i=0}^{m-1} a_i \in R,$$

which is a contradiction. This means the product is always defined. □

Theorem 4.4 (Splitting Products)

For all integers $0 \leq m < n$

$$\prod_{i=0}^{n} a_i = \prod_{i=0}^{m} a_i \prod_{i=m+1}^{n} a_i$$

Proof. For the sake of contradiction, assume there exists $m, n \in \mathbb{N}$ such that

$$\prod_{i=0}^{n} a_i \neq \prod_{i=0}^{m} a_i \prod_{i=m+1}^{n} a_i.$$

Construct the set

$$S = \{n \in \mathbb{N} \mid \exists m \in \mathbb{N}, \prod_{i=0}^{n} a_i \neq \prod_{i=0}^{m} a_i \prod_{i=m+1}^{n} a_i\}.$$

By our hypothesis, S is non-empty and by construction, all elements are positive, so apply Axiom WOP to get a minimal element $m \in S$. By construction,

$$\prod_{i=0}^{n} a_i \neq \prod_{i=0}^{m} a_i \prod_{i=m+1}^{n} a_i.$$

By $0 \geq m < n$, we know $0 < n$ (Lemma Transitivity of $<$), so apply Definition Product to get

$$a_n \prod_{i=0}^{n-1} a_i \neq \left(\prod_{i=0}^{m} a_i\right) a_n \prod_{i=m+1}^{n-1} a_i.$$

Use Theorem Cancellation of Multiplication to get that

$$\prod_{i=0}^{n-1} a_i \neq \left(\prod_{i=0}^{m} a_i\right) \prod_{i=m+1}^{n-1} a_i.$$

But $n-1 < n$, which contradicts the minimality of n. This proves the theorem. □

Theorem 4.5 (Change of Index)

For all integers x,

$$\prod_{i=k}^{n} a_i = \prod_{i=k+x}^{n+x} a_{i-x}$$

Proof. Fix a_i and x. Imagine there is an n such that

$$\prod_{i=k}^{n} a_i \neq \prod_{i=k+x}^{n+x} a_{i-x}.$$

Construct the set

$$S = \{n \in \mathbb{N} \mid \prod_{i=k}^{n} a_i \neq \prod_{i=k+x}^{n+x} a_{i-x}\}.$$

S is non-empty by our hypothesis, and S is positive by construction. Apply Axiom WOP to produce a minimal element $m \in S$. By the construction of m, we have that

$$\prod_{i=k}^{m} a_i \neq \prod_{i=k+x}^{m+x} a_{i-x}.$$

Apply definition Product to get

$$a_m \prod_{i=k}^{m-1} a_i \neq a_{m+x-x} \prod_{i=k+x}^{m+x-1} a_{i-x} = a_m \prod_{i=k+x}^{m+x-1} a_{i-x}.$$

Apply Theorem Cancellation of Multiplication to get

$$\prod_{i=k}^{m-1} a_i \neq \prod_{i=k+x}^{m+x-1} a_{i-x}.$$

But $m-1 < m$, contradicting the minimality of m. This means our hypothesis was false, so the theorem holds. □

Definition 4.6 (Exponents)**.** For an integer a and a non-negative integer e, define

$$a^0 = 1$$

and

$$a^e = a \cdot a^{e-1}.$$

Theorem 4.7 (Definedness of Exponents)
For all a, e, if a is positive, a^e exists and is defined.

Proof. Fix $a \in \mathbb{Z}$. Proof by contradiction. Assume there is some e such that a^e is not defined. Construct the set of counter-examples S such that

$$S = \{e \in \mathbb{N} \mid \nexists h \in \mathbb{Z}, h = a^e\}.$$

By our assumption, S is non-empty, and S consists of natural numbers, so use WOP to get a smallest element m. We have that

$$\nexists h \in \mathbb{Z}, h = a^m.$$

If $m = 0$, then $a^0 = 1$, which is an integer, so contradiction. Otherwise, apply Exponents to say

$$a^m = a \cdot a^{m-1}.$$

Since a is positive, we have by Divides implies Less than that $a^{m-1} < a^m$. Since a^{m-1} is less than the least exponent that isn't defined, it must be defined, say $a^{m-1} = x, x \in \mathbb{Z}$. Then, we have $a^m = ax$. By the closure of multiplication (see Ring Axioms), we have that ax is an integer. This contradicts our hypothesis, so exponents are always defined. □

Theorem 4.8 (Splitting of Exponents)
For all integers a and for all natural numbers b, c, we have that $a^b a^c = a^{b+c}$.

Proof. Fix a and b. Assume there is a c for which this statement does not hold. Construct the set

$$S = \{c \mid a^b a^c \neq a^{b+c}\}.$$

By our assumption, S is non-empty, so WOP requisitions a minimal element, call it m. We have that

$$a^b a^m \neq a^{b+m}.$$

If $m = 0$, then we have

$$a^b a^0 = a^b 1 = a^b,$$

which is a contradiction. Otherwise, apply Definedness of Exponents to get

$$a^b a a^{m-1} \neq a a^{b+m-1}.$$

If $a = 0$, the we have $0 \neq 0$, which is a contradiction, otherwise, use Cancellation of Multiplication to get

$$a^b a^{m-1} \neq a^{b+(m-1)}.$$

But $m - 1 < m$, contradicting the minimality of m, so we are done. □

Theorem 4.9 (Euclid's Lemma)
Let $a_i : \mathbb{N} \to \mathbb{Z}$ be a sequence of integers. If p is a prime such that

$$p \mid \prod_{i=0}^{n} a_i,$$

then there exists an integer $0 \leq i \leq n$ such that $p \mid a_i$

Proof. Fix p. Let's assume for the sake of contradiction that there exists an integer n such that

$$p \mid \prod_{i=0}^{n} a_i,$$

but $p \nmid a_i$ for all i. For the sake of WOP, define

$$S = \left\{ n \middle| p \mid \prod_{i=0}^{n} a_i \wedge \forall i, p \nmid a_i \right\}.$$

By our hypothesis, S is non-empty. Apply WOP to get a minimal element $m \in S$. By construction we know that

$$p \mid \prod_{i=0}^{m} a_i$$

and

$$\forall i, p \nmid a_i.$$

If $m = 0$, apply Product to say

$$p \mid \prod_{i=0}^{0} a_i = a_0,$$

but this is a contradiction because $p \nmid a_i$. Otherwise, $m > 0$, so apply Product to say that

$$p \mid a_m \prod_{i=0}^{m-1} a_i.$$

We know from Theorem Prime GCD 1 that $gcd(p, a_m) = 1$, so by Theorem Fundamental Lemma,

$$p \mid \prod_{i=0}^{m-1} a_i. \tag{1}$$

We still have that $\forall i, p \nmid a_i$, so equation (1) contradicts the minimality of m. This means the hypothesis is false and we are done. □

Theorem 4.10 (Existence of a Prime Factor)
Every integer a has a prime factor, i.e. there exists a prime number p such that $p \mid a$

Proof. For the sake of contradiction, let us imagine there is an integer a with no prime factors. Construct the set

$$S = \{a \mid \nexists p, p \text{ prime } \wedge p \mid a\}.$$

By our hypothesis, S is non-empty, so apply axiom WOP to produce a minimal element $m \in S$. We know $1 \mid a$ and $a \mid a$ by Theorem Trivial Divisors. If those were the only divisors, then a would be prime by definition Prime. But a cannot be prime because $a \mid a$. This means a has a divisor $x \mid a$ with $x \neq 1$ and $x \neq a$. We can write by defintion Divides that

$$xy = a, y \in \mathbb{Z}.$$

By Lemma Multiplication $\implies <$, we get that one of x, y is less than a, call whichever one s. Since s is smaller than the smallest element without a prime factor, then s must have a prime factor, call it p. Apply Theorem Transitivity of Divisibility on p to get that $p \mid m$. This is a contradiction, so our hypothesis was wrong and we are done. □

Lemma 4.11 (Cancellation of Products)
If
$$\prod_{i=0}^{n} a_i = \prod_{i=0}^{m} b_i.$$
and for some j, k $a_j = b_k$, then let
$$c_i = \begin{cases} a_i & i \leq j \\ a_{i-1} & i > j \end{cases}$$
and
$$d_i = \begin{cases} b_i & i \leq k \\ b_{i-1} & i > k \end{cases}$$
then
$$\prod_{i=0}^{n} c_i = \prod_{i=0}^{m} d_i.$$

Proof. Let
$$\prod_{i=0}^{n} a_i = \prod_{i=0}^{m} b_i.$$
Use Splitting Products
$$\prod_{i=0}^{j} a_i \prod_{i=j+1}^{n} a_i = \prod_{i=0}^{k} b_i \prod_{i=k+1}^{m} b_i.$$
Use Product
$$a_j \prod_{i=0}^{j-1} a_i \prod_{i=j+1}^{n} a_i = b_k \prod_{i=0}^{k-1} b_i \prod_{i=k+1}^{m} b_i.$$
Use Cancellation of Multiplication
$$\prod_{i=0}^{j-1} a_i \prod_{i=j+1}^{n} a_i = \prod_{i=0}^{k-1} b_i \prod_{i=k+1}^{m} b_i.$$
use Change of Index
$$\prod_{i=0}^{j-1} a_i \prod_{i=j}^{n-1} a_{i-1} = \prod_{i=0}^{k-1} b_i \prod_{i=k}^{m-1} b_{i-1}.$$
Substitute in the definitions of c_i and d_i to get
$$\prod_{i=0}^{j-1} c_i \prod_{i=j}^{n-1} c_{i-1} = \prod_{i=0}^{k-1} d_i \prod_{i=k}^{m-1} d_{i-1}.$$
Apply Product to get
$$\prod_{i=0}^{n-1} c_i = \prod_{i=0}^{m-1} d_i.$$
$\square$

Theorem 4.12 (Existence of Prime Factorization)

Every integer a can be written as a product of primes, i.e. there exists a sequence of primes $p_i : \mathbb{N} \to P$ such that

$$a = \prod_{i=0}^{n} p_i.$$

Proof. Let's assume for the sake of contradiction that there exists an integer without a prime factorization. Construct the set

$$S = \{a \mid \nexists p_i, na = \prod_{i=0}^{n} p_i.\}$$

By our hypothesis, S is non-empty, so apply Axioms WOP to produce a minimal element $m \in S$. By Theorem Existence of a Prime Factor, we know m has a prime factor p. Write $px = m$ for some m. By Multiplication Less, we know $x < m$. Since x is less than the minimal element without a prime factorization, we know x must have a prime factorization. Say that

$$x = \prod_{i=0}^{n} p_i, \text{ where } p_i : \mathbb{N} \to P.$$

Then, define

$$q_i = \begin{cases} p_i & \text{if } i \leq n \\ p & i = n+1 \end{cases}.$$

We have that

$$m = px = p \prod_{i=0}^{n} p_i = q_{n+1} \prod_{i=0}^{n} q_i = \prod_{i=0}^{n+1} q_i.$$

This means that m has a prime factorization, so we are done. □

Theorem 4.13 (Unique Prime Factorization)

Every integer a can be written as a unique product of primes, i.e. if $p_i : \mathbb{N} \to P$ and $q_i : \mathbb{N} \to P$ are two sequences of primes such that

$$a = \prod_{i=0}^{n} p_i = \prod_{i=0}^{m} q_i,$$

then $n = m$ and for every integer $0 \leq i \leq n$, there exists an integer $0 \leq j \leq m$ such that $p_i = q_j$.

Proof. We already know from theorem Existence of Prime Factorization that a has a prime factorization. Let's imagine that a has 2 prime factorizations, $\prod_{i=0}^{n} p_i$ and $\prod_{i=0}^{m} q_i$, and that they are not equal. Let

$$S = \left\{ m | a = \prod_{i=0}^{n} p_i = \prod_{i=0}^{m} q_i, \exists i, \forall j, p_i \neq q_j \right\}.$$

By our hypothesis, S is non-empty, so use Axiom WOP to get a minimal element m. By construction, we have

$$\prod_{i=0}^{n} p_i = \prod_{i=0}^{m} q_i.$$

By Definition Product, we have

$$p_n \prod_{i=0}^{n-1} p_i = \prod_{i=0}^{m} q_i \implies p_n \mid \prod_{i=0}^{m} q_i.$$

By Theorem Euclid's Lemma, we know there exists a j such that $p_n \mid q_j$. We defined the only divisors of a prime to be 1 and itself. $p_n \neq 1$ because 1 is not prime, so the only option is that $p_n = q_j$. Apply Cancellation of Products to get a sequence c_i such that

$$\prod_{i=0}^{n-1} p_i = \prod_{i=0}^{m-1} c_i.$$

But this is a contradiction because $m - 1 < m$, contradicting the minimality of m. This means we are done. □

Definition 4.14 (Bijection)**.** A function $f : A \to B$ is called **bijective** if it is both

1. (surjective) for all $b \in B$, there exists an $a \in A$ such that $f(a) = b$.
2. (injective) if $f(x) = f(y)$ then $x = y$.

Definition 4.15. Define the notation $[n]$ as $[0] = \{0\}$ and $[n + 1] = [n] \cup \{n + 1\}$.

Lemma 4.16 (General Commutative Property)

Given a sequence $a_i : \mathbb{N} \to \mathbb{Z}$, for all bijective functions $f : [n] \to [n]$,

$$\prod_{i=0}^{n} a_i = \prod_{i=0}^{n} a_{f(i)}$$

Proof. Fix f and a_i. Imagine there is some n such that

$$\prod_{i=0}^{n} a_i \neq \prod_{i=0}^{n} a_{f(i)}.$$

Construct the set

$$S = \left\{ m \mid \prod_{i=0}^{m} a_i \neq \prod_{i=0}^{m} a_{f(i)} \right\}.$$

By our hypothesis, S is non-empty and S consists of positive elements. Apply Axiom WOP to produce a minimal element $m \in S$. By construction we have

$$\prod_{i=0}^{m} a_i \neq \prod_{i=0}^{m} a_{f(i)}.$$

Apply Definition Product to say

$$\prod_{i=0}^{m} a_i \neq a_{f(n)} \prod_{i=0}^{m-1} a_{f(i)}.$$

Call $f(n) = j$. We know j always exists by Definition Bijection. This gives us that $a_j = a_{f(n)}$. Apply Lemma Cancellation of Products to get a sequence c_i such that

$$\prod_{i=0}^{m-1} a_i \neq \prod_{i=0}^{m-1} c_i.$$

But $m - 1 < m$, contradicting the minimality of m. □

Lemma 4.17 (Sorting)

Given a sequence $a_i : \mathbb{N} \to \mathbb{N}$, there exists a bijective function $f : [n] \to [n]$, such that for all $i, j \in \mathbb{N}$ if $i \leq j$, then $a_{f(i)} \leq a_{f(j)}$

Proof. We already know from General Commutative Property that any permutation of the sequence a_i will not change the product. For the purpose of contradiction, let's imagine that there is a sequence that cannot be sorted. Construct the set

$$S = \{n \mid \nexists f, \forall a_i, \forall (i,j), i \leq j \implies a_{f(i)} \leq a_{f(j)}\}$$

By our assumption, S is non-empty, so select the smallest element, call it m. If the sequence has length 0 or 1, it is automatically sorted by definition. Otherwise, by WOP on the a_is, there is a least a_i because all the a are natural numbers, call it a_m. Construct the sequence

$$c_i = \begin{cases} a_i & i \leq m \\ a_{i-1} & i > m \end{cases}.$$

Since the length of c_i is $m - 1$, it is smaller than the smallest sequence that cannot be sorted, so it can be sorted. Imagine c_i can be sorted by the bijection $g : [m-1] \to [m-1]$.

Then, define the function $f : [m] \to [m]$ such that

$$f(i) = \begin{cases} 0 & i = j \\ g(i) & i \neq j \end{cases}.$$

We have that f is a bijection and that f sorts the sequence a_i. This contradicts our assumption that there was no f that could sort a_i. This means every sequence can be sorted. □

Theorem 4.18 (Canonical Prime Factorization)

For every integer a, there exists a sequence of primes $p_i : \mathbb{N} \to P$ and a sequence of exponents $e_i : \mathbb{N} \to \mathbb{N}$ such that

$$a = \prod_{i=0}^{n} p_i^{e_i}$$

and such that for all integers i, j with $0 \leq i, j \leq n$, if $i < j$ then $p_i < p_j$.

Proof. Let us do a proof by contradiction. Assume there exists a number without a canonical factorization. Let S be the set of counter-examples such that

$$S = \left\{ a \mid \nexists (p_i, e_i), a = \prod_{i=0}^{n} p_i e^i \right\}$$

By our assumption, S is non-empty, so use WOP to retrieve a smallest element a. We already proved in Unique Prime Factorization that every a has a unique factorization. Apply Sorting to get a factorization of a that is sorted. Say

$$a = \prod_{i=0}^{m} q_i, \forall m, nm \leq n \implies q_m \leq q_n$$

If $m = 0$, then

$$a = q_0 = q_0^1$$

so a has a canonical prime factorization. Otherwise, we have

$$a = q_m \prod_{i=0}^{m-1} q_i.$$

We know q_m is positive, so by Divides implies Less than,

$$\prod_{i=0}^{m-1} q_i < a.$$

By Definedness of Products, we have that there is some integer k such that $k = \prod_{i=0}^{m-1} q_i$. Since $k < a$, k must have a cananical factorization, call it

$$k = \prod_{i=0}^{g} h_i^{f_i}.$$

Thus, we have,

$$a = q_m \prod_{i=0}^{g} h_i^{f_i}.$$

There are 2 options, either q_m is contained in the sequence h_i, or it isn't. If q_m is contained in h_i. Then there is some t such that $q_m = h_t$. Then, define,

$$e_i = \begin{cases} f_i + 1 & i \leq t \\ f_i & i \neq t \end{cases}.$$

Then we have that

$$a = \prod_{i=0}^{g} h_i^{e_i}.$$

This means that a has a canonical prime factorization, so we are done. In the second case where q_i is not contained in h_i, define an intermediate sequence d such that

$$d_i = \begin{cases} f_i + 1 & i \leq g \\ q_m & i \neq t \end{cases}.$$

Then apply Sorting to produce a bijection $y : [g+1] \to [g+1]$ such that $d_{y(i)}$ is sorted. Then, define

$$e_i = \begin{cases} f_{y(i)} & i \neq m \\ 1 & i = q \end{cases}.$$

Then, we have that the canonical factorization of a is

$$a = \prod_{i=0}^{g+1} d_{y(i)}^{e_i}.$$

And we are done. □

Lemma 4.19 (Prime Powers Divides)
If p and q are prime and $p \mid q^e$ for some $e \in \mathbb{N}$, then $p = q$

Proof. Fix p, q and do WOP on e. Assume there is some e such that $p \mid q^e$ but $p \neq q$. Construct the set S such that

$$S = \{e \in \mathbb{Z} \mid p \mid q^e \wedge p \neq q\}.$$

By our assumption, S is non-empty, so use WOP to procure a smallest element, call it $m \in \mathbb{N}$. We have that $p \mid q^e$. If $e = 0$, the $p \mid 1$, which is immediately a contradiction, so we are done. Otherwise, $p \mid q \cdot q^{e-1}$ by Exponents, so use Fundamental Lemma to say that either $p \mid q$ or $p \mid q^{e-1}$. If $p \mid q$, then $p = q$, which contradicts our assumption that $p \neq q$. Otherwise, $p \mid q^{e-1}$, but $e - 1 < e$, which contradicts the minimality of e. In either case, our assumption was wrong, so we must have that $p = q$. □

Theorem 4.20 (Unique Canonical Factorization)
Every integer is uniquely determined by its canonical factorization

Proof. We already know from Canonical Prime Factorization that every integer has a canonical factorization. Assume there is an integer with two different canonical factorizations. Construct the set S such that

$$S = \left\{ a \in \mathbb{N} \mid a = \prod_{i=0}^{n} p_i^{e_i} = \prod_{j=0}^{m} q_j^{f_j} \right\}.$$

By our assumption S is non-empty, so use WOP to produce a smallest element, call it m. We have that

$$m = \prod_{i=0}^{n} p_i^{e_i} = \prod_{j=0}^{m} q_j^{f_j}.$$

Use Product and Exponents to say that

$$\prod_{i=0}^{n} p_i^{e_i} = \prod_{j=0}^{m} q_j^{f_j} \implies p_n p_n^{e_n - 1} \prod_{i=0}^{n-1} p_i^{e_i} = \prod_{j=0}^{m} q_j^{f_j} \implies p_i \mid \prod_{j=0}^{m} q_j^{f_j}.$$

By Euclid's Lemma, we have that there is a term $q_d^{f_d}$ such that

$$p_n \mid q_d^{f_d}.$$

Use Prime Powers Divides to say that $p_n = q_d$. Do trichotomy on q_d. If $q_d < q_n$, then we have that q_n divides the right hand side, but not the left - a contradiction. If $q_d > q_n$, then this contradicts the fact that a canonical representation is always sorted. If $q_d = q_n$, then compare the exponents, e_n and f_d using trichotomy. If $e_n > f_d$, then by Splitting of Exponents, $p^{e_n - f_d}$ divides the left but not the right, which is a contradiction. Similar logic applies to when $e_n < f_d$. The only option is that $e_n = f_d$. Then use Cancellation of Products to get two new canonical factorizations which are less that a by Divides implies Less than. This contradicts the minimality of a, so our assumption must have been wrong. This means that we are done. □

§5 Conclusion

Prof. Jim Fowler once said "Unique factorization is a theorem that people are insufficiently appreciative of". I hope the proving UFT directly from axioms about the integers demonstrates what a phenomenal result UFT is.