UFT Proof

Sean Xiao

(Dated: June 2024)

I. DIVISION

We're all familiar with the concept of "dividing". Roughly speaking, it's how many times one thing "goes into" another thing. This is mathematics, however, and we must make this definition precise.

Definition 1 *Suppose $a, b \in \mathbf{Z}$. We say that a **divides** b if there exists another integer m such that $b = am$.*

For example, 3 divides 6 because $3 \cdot 2 = 6$. 3 does not, however, divide 5, as there does not exist an integer m such that $3m = 5$.

Naturally, one could ask questions about this definition. Does every number divide every number? And if a divides b is a less than b? Greater than b? Equal?

Lemma 2 *If a, b are positive integers and a divides b, then $a \leq b$.*

Proof. Suppose $a > b$ and say that $am = b$ for some integer m. Clearly, m must be positive (and not 1, as we assume $a > b$ not $a = b$), otherwise am would not be positive. Substituting, we get

$$a - am > 0.$$

Factoring our a, we have $a(1 - m) > 0$. Since m is positive and not one, $1 - m$ is negative meaning $a(1 - m)$ is negative. But this expression is supposed to be greater than 0, so we have reached a contradiction. Thus $a \leq b$. □

In the next subsection, we will introduce some ideas that will help us more easily decide when one integer divides another. For now, though, let's prove some more basic results.

Lemma 3 *The following are true for some integers a, b and c.*

1. *For all $a \in \mathbf{Z}$, $a \mid a$.*
2. *If $a \mid b$, then $a \mid bc$.*
3. *If $a \mid b$ and $a \mid c$, then $a \mid bx + cy$ for some integers x and y.*

Proof. We will prove these statements in order.

(1) We can write $a = a \cdot 1$, which by definition means $a \mid a$.

(2) Say that $am = b$ for some integer m. Then $bc = (am)c = a(mc)$, which means $a \mid bc$.

(3) Let $b = an$ and $c = am$. Then $bx + cy = anx + amy = a(nx + my)$, meaning $a \mid bx + cy$. □

A. Division Algorithm

Assume we now know that not every number divides every number. But every number does "go into" another number to some extent. We can capture this with the idea of the division algorithm.

Theorem 4 *For any integers a and b, $b \neq 0$, we can write $a = bq + r$, where r and q are integers and $0 \leq r < |b|$.*

Proof. We will first prove this only for $a, b \in \mathbf{Z}^+$, because that is all it's needed for in this paper. To this end, fix some $b \in \mathbf{Z}^+$ and consider the set $S = \{a \in \mathbf{Z}^+ \mid a \text{ cannot be written as } bq + r, r, q \in \mathbf{Z}, 0 \leq r < b\}$. Clearly, $1 \notin S$, because if $b \neq 1$, we can write $1 = b(0) + 1$. If $b = 1$, then $1 = b(1) + 0$. Either way, 1 does not satisfy the conditions to be an element of S.

Since S is a subset of $\mathbf{Z}^+$, we can pick a minimal element L by WOP. Since L is a minimal element of S, $L - 1 \notin S$ because $L - 1 < L$. Thus we can write $L - 1$ as $bq + r$, where $q, r \in \mathbf{Z}$ and $0 \leq r < b$. But this means $L = bq + r + 1$. If $r < b - 1$, then this is an expression of L in a manner which contradicts that it's an element of S. If $r = b - 1$, then $L = bq + r + 1 = b(q + 1)$, which still contradicts that $L \in S$. Thus S is empty, meaning the division algorithm holds. □

B. Consequences of the Division Algorithm

Before we go into consequences of the division algorithm, we'll need to introduce some terminology.

Definition 5 *The **greatest common divisor** of two integers a and b is the largest integer that divides both a and b.*

For example, the greatest common divisor of 14 and 3 is 1, and the greatest common divisor of 65 and 26 is 13. One might realize that we can write 1 as a linear combination of 14 and 3, namely $2(14) - 3(9)$. We can also write 13 as a linear combination of 65 and 26, namely as $65 - 2(23)$. This motivates the following important result.

Theorem 6 (Bezout's Lemma) *Say that $a, b \in \mathbb{Z}$. Then there exist integers $x, y \in \mathbb{Z}$ such that $ax + by = \gcd(a, b)$.*

Proof. Suppose we have two integers a and b. Then we can find integers x and y such that $ax + by \in \mathbf{Z}^+$. Simply choose x as the sign of a, that is, if a is negative choose $x = -1$, and if a is positive choose $a = 1$ (similarly for b). By WOP, there is a smallest element of the set of integers one can write in this manner. Call this smallest positive integer k. So far, we've written $ax + by = k$. By the division algorithm(4), we can write $a = kq + r$, where $q, r \in \mathbf{Z}^+$ and $0 \leq r < k$. Subtracting kq from both sides, we get $a - kq = r$. Since $k = (ax + by)$, we substitute this in to get

$$a - (ax + by)q = r$$
$$a(1 - xq) + b(-qy) = r.$$

This is an expression of r as a linear combination of a and b. We know r is non-negative and that r is less than k. However, k is the smallest positive integer that can be written as a linear combination of a and b, so $r = 0$. This means $a = kq$, so k divides a. By the exact same argument, we also show $k \mid b$. Thus $k \leq \gcd(a, b)$.

Now, $\gcd(a, b)$ divides a and b, so it divides $ax + by$, or k. Thus $\gcd(a, b) \leq k$. Since $\gcd(a, b) \leq k$ and $\gcd(a, b) \geq k$, we have $\gcd(a, b) = k$, as desired. □

II. PRIMES

You may notice that there are some numbers whose greatest common divisors with other numbers is either that number or 1. These numbers are called **prime numbers**. We'll define them precisely as follows.

Definition 7 (Prime Numbers) *An integer p is called **prime** if:*

1. *Any factorization of p into a product ab implies either a or b is ± 1.*
2. *p is positive.*
3. *$p \neq \pm 1$.*

The first few prime numbers are $2, 3, 5, 7, 11, 13, 17, 19$, etc.

A. Basic Results About Primes

In order to prove that every integer can be factored uniquely as a product of primes, we will first show some other important results.

Lemma 8 *Every positive integer except 1 has a prime divisor.*

Proof. Let $\mathbb{S} = \{n \in \mathbb{Z}^+ \mid n > 1 \text{ and } n \text{ has no prime divisors }\}$. If $S \neq \emptyset$, by WOP, $\mathbb{S}$ has a smallest element, say $n_0 \in \mathbb{S}$.
Since $n_0 > 1$ and n_0 has no prime divisors, then n_0 cannot be prime, and there exist integers $a_0, b_0 \in \mathbb{Z}^+$ such that $n_0 = a_0 \cdot b_0$ where $1 < a_0, b_0 < n$ (by 2). This is because if $n > b_0 > 1, a_0 = n$, then $a_0 \cdot b_0 > n_0$, the case that $n > a_0 > 1$, $b_0 = n$ leads us to the same result.
However, since $1 < a_0 < n_0$ and n_0 is the smallest element in S, then $a_0 \notin S$, which implies that a_0 has a prime divisor p that satisfies $p \mid a_0$, but then $p \mid n_0 = a_0 \cdot b_0$ as well, which contradicts.
As a result, the assumption that $\mathbb{S} \neq \emptyset$ leads to a contradiction, and we must have $\mathbb{S} = \emptyset$, so that every positive integer $n > 1$ has a prime divisor. □

Lemma 9 *Every positive integer greater than 1 is expressible as a product of primes.*

Proof. Let $\mathbb{S} = \{n \mid n \in \mathbb{Z}^+ \text{ and } n \text{ cannot be expressed as a product of primes}\}$, which is non-empty. By WOP, $\mathbb{S}$ has a smallest element, say n_0. By 8, we know that every positive integer greater than 1 has prime divisors, so there exist $p \mid n_0$ for some primes p, and p can be represented as $n_0 = pa$, where $p \in \mathbb{Z}^+$. Then by 2, we know that $p, a < n_0$ since $p \neq 1$. Since we assume n_0 is the smallest number which can't be written as a product of primes, a can be expressed with a product of primes. And since p is also a prime, then $n_0 = p \cdot a$ can be expressed as a product of primes, which contradicts. Hence, $\mathbb{S} = \emptyset$, so every positive integer greater than 1 is expressible as product of primes. □

B. Euclid's Lemma and its Generalization

We almost have enough tools to proof the Fundamental Theorem of Arithmetic. We just need the following two results.

Lemma 10 (Euclid's Lemma) *Suppose we have some prime p and integers a, b. Then if $p \mid ab$, either $p \mid a$ or $\mid b$.*

Proof. If $p \mid a$, then we are done. Thus suppose $p \nmid a$. Since p is a prime, $\gcd(p, a) = 1$. By Bezout's lemma, there exist $x, y \in \mathbb{Z}$ such that $px + ay = 1$. Multiplying both sides by b, we get $pbx + aby = b$. Since $p \mid ab$, ab can be written as $ab = pk$ for some $k \in \mathbb{Z}$. Hence, we have $b = pbx + aby = p(bx + ky)$. Consequently, b is the multiple of p, which means $p \mid b$. □

Proposition 11 *Suppose p is a prime and $a_1, \ldots, a_n$ are integers. Then if $p \mid a_1 \cdots a_n$, $p \mid a_i$ for some $1 \leq i \leq n$.*

Proof. Pick some sequence of integers a_i and fix some primes p. Consider the set $S = \{m : p \mid a_1 \cdots a_m, p \nmid a_i \text{ for all } 1 \leq i \leq m\}$. Clearly, $1 \notin S$. We want to show S is empty, so assume otherwise for the sake of contradiction.

Clearly, S is a subset of $\mathbf{Z}^+$, meaning we can pick a minimal element ℓ by WOP. Then, we have that $p \mid a_1 \cdots a_\ell$ and $p \nmid a_i$ for all $1 \leq i \leq \ell$. By Euclid's Lemma, this means $p \mid a_1 \cdots a_{\ell-1}$. But since $\ell - 1 \notin S$, $p \mid a_i$ for some $1 \leq i \leq \ell - 1$. Thus $p \mid a_i$ for some $1 \leq i \leq \ell$, which contradicts that ℓ is in the set S, meaning S is empty, as desired. □

III. THE FUNDAMENTAL THEOREM OF ARITHMETIC

We have now built up all the machinery needed to prove the Fundamental Theorem of Arithmetic (FTA), namely Unique Factorization Theorem (UFT).

Theorem 12 (Fundamental Theorem of Arithmetic) *Every positive integer can be **uniquely** factored as a product of primes.*

Proof. Consider the set $S = \{n \in \mathbf{Z}^+ \mid n \text{ cannot be written uniquely as a product of primes.}\}$. We would like to prove this set is empty, so assume otherwise. By WOP, we can pick a minimal element L of S. Suppose L can be factored as $p_1 \cdots p_r$ and $q_1 \cdots q_s$, where each of the p_i and q_j are primes.

Since p_1 divides L, p_1 also divides $q_1 \cdots q_s$. By 11, p_1 divides one of q_j for some $1 \leq j \leq s$. WLOG, let this be q_1. Since q_1 is a prime, $p_1 = q_1$, which means $p_2 \cdots p_r = q_2 \cdots q_s$. But if these two factorizations of n/p_1 are different, then there is a positive integer smaller than n that can be factored into primes non-uniquely. Thus these factorizations are the same. But this implies our original factorizations of $p_1 \cdots p_r$ and $q_1 \cdots q_s$ are the same. Thus unique factorization holds. □