Chapter 5

Three Famous Theorems

As the title suggests, we tackle three famous theorems in this chapter.

5.1 The Fundamental Theorem of Arithmetic

The goal of this section is to prove The Fundamental Theorem of Arithmetic, which is a theorem that you have been intimately familiar with since grade school, but perhaps don't recognize by name. The Fundamental Theorem of Arithmetic (sometimes called the Unique Factorization Theorem) states that every natural number greater than 1 is either prime or is the product of prime numbers, where this product is unique up to the order of the factors. For example, the natural number 12 has prime factorization $2^2 \cdot 3$, where the order in which we write the prime factors (i.e., 2, 2, and 3) is irrelevant. That is, $2^2 \cdot 3$, $2 \cdot 3 \cdot 2$, and $3 \cdot 2^2$ are all the same prime factorization of 12. The requirement that the factors be prime is necessary since factorizations containing composite numbers may not be unique. For example, $12 = 2 \cdot 6$ and $12 = 3 \cdot 4$, but these factorizations into composite numbers are distinct. We've just thrown around a few fancy terms; we should make sure we understand their precise meaning.

Definition 5.1. Let $n \in \mathbb{Z}$.

(a) If $a \in \mathbb{Z}$ such that a divides n, then we say that a is a **factor** of n.

(b) If $n \in \mathbb{N}$ such that n has exactly two distinct positive factors (namely, 1 and n itself), then n is called **prime**.

(c) If $n > 1$ such that n is not prime, then n is called **composite**.

Exercise 5.2. Is 1 a prime number or composite number? Explain your answer.

Exercise 5.3. List the first 10 prime numbers.

The next theorem makes up half of the Fundamental Theorem of Arithmetic.

Lemma 5.4. Let n be a natural number greater than 1. Then n can be expressed as a product of primes. That is, we can write

$$n = p_1 p_2 \cdots p_k,$$

where each of $p_1, p_2, \ldots, p_k$ is a prime number (not necessarily distinct).[1]

Lemma 5.4 states that we can write every natural number greater than 1 as a product of primes, but it does not say that the primes and the number of times each prime appears are unique. To prove uniqueness, we will need Euclid's Lemma (Theorem 5.12). To prove Euclid's Lemma, we will utilize a special case of Bezout's Lemma (Lemma 5.10), the proof of which relies on the following result, known as the Division Algorithm. One can prove the Division Algorithm using the Well-Ordering Principle (Theorem 4.34) and we have the necessary tools to do this, but we will skip proving the Division Algorithm for now. If you are interested in the proof of the Division Algorithm, I encourage you to give it a try yourself or to look up the proof in a textbook or an online resource. It's worth pointing out that we are stating the Division Algorithm for natural numbers, but the theorem holds more generally for integers, but we must replace $0 \leq r < n$ with $0 \leq r < |n|$.

Theorem 5.5 (Division Algorithm)**.** If $m, n \in \mathbb{N}$, then there exists unique $q, r \in \mathbb{N} \cup \{0\}$ such that $m = nq + r$ with $0 \leq r < n$.

The numbers q and r from the Division Algorithm are referred to as **quotient** and **remainder**, respectively.

Exercise 5.6. Suppose $m = 27$ and $n = 5$. Find the quotient and remainder that are guaranteed to exists by the Division Algorithm. That is, find the unique $q, r \in \mathbb{N}$ such that $0 \leq r < n$ and $m = nq + r$.

It's useful to have some additional terminology.

Definition 5.7. Let $m, n \in \mathbb{Z}$ such that at least one of m or n is nonzero. The **greatest common divisor** (gcd) of m and n, denoted $\gcd(m, n)$, is the largest positive integer that is a factor of both m and n. If $\gcd(m, n) = 1$, we say that m and n are **relatively prime**.

Exercise 5.8. Find $\gcd(54, 72)$.

Exercise 5.9. Provide an example of two natural numbers that are relatively prime.

The next result is a special case of a theorem known as Bézout's Lemma (or Bézout's Identity). Ultimately, we will need this theorem to prove Euclid's Lemma (Theorem 5.12), which we then use to prove uniqueness for the Fundamental Theorem of Arithmetic (Theorem 5.14).

[1] *Hint:* Use a proof by contradiction. Let S be the set of natural numbers for which the theorem fails. For sake of a contradiction, assume $S \neq \emptyset$. By the Well-Ordering Principle (Theorem 4.34), S contains a least element, say n. Then n cannot be prime since this would satisfy the theorem. So, it must be the case that n has a divisor other than 1 and itself. This implies that there exists natural numbers a and b greater than 1 such that $n = ab$. Since n was our smallest counterexample, what can you conclude about both a and b? Use this information to derive a counterexample for n.

Lemma 5.10 (Special Case of Bézout's Lemma)**.** If $p, a \in \mathbb{Z}$ such that p is prime and p and a are relatively prime, then there exists $s, t \in \mathbb{Z}$ such that $ps + at = 1$.[2]

Exercise 5.11. Consider the natural numbers 2 and 7, which happen to be relatively prime. Find integers s and t guaranteed to exist according to Lemma 5.10. That is, find $s, t \in \mathbb{Z}$ such that $2s + 7t = 1$.

The following theorem is known as Euclid's Lemma. See if you can prove it using Lemma 5.10.

Theorem 5.12 (Euclid's Lemma)**.** Assume that p is prime. If p divides ab, where $a, b \in \mathbb{N}$, then either p divides a or p divides b.[3]

In Euclid's Lemma, it is crucial that p be prime as illustrated by the next problem.

Problem 5.13. Provide an example of integers a, b, d such that d divides ab yet d does not divide a and d does not divide b.

Alright, we are finally ready to tackle the proof of the Fundamental Theorem of Arithmetic.

Theorem 5.14 (Fundamental Theorem of Arithmetic)**.** Every natural number greater than 1 can be expressed uniquely (up to the order in which they appear) as the product of one or more primes.[4]

The Fundamental Theorem of Arithmetic is one of the many reasons why 1 is not considered a prime number. If 1 were prime, prime factorizations would not be unique.

5.2 The Irrationality of $\sqrt{2}$

In this section we will prove one of the oldest and most important theorems in mathematics: $\sqrt{2}$ is irrational (see Theorem 5.16). First, we need to know what this means.

[2] *Hint:* Consider the set $S := \{ps + at > 0 \mid s, t \in \mathbb{Z}\}$. First, observe that $p \in S$ (choose $s = 1$ and $t = 0$). It follows that S is nonempty. By the Well-Ordering Principle (Theorem 4.34), S contains a least element, say d. Then there exists $s_1, t_1 \in \mathbb{Z}$ such that $d = ps_1 + at_1$. Our goal is to show that $d = 1$. Now, choose $m \in S$. Then there exists $s_2, t_2 \in \mathbb{Z}$ such that $m = ps_2 + at_2$. By the definition of d, we know $d \leq m$. By the Division Algorithm, there exists unique $q, r \in \mathbb{N} \cup \{0\}$ such that $m = qd + r$ with $0 \leq r < d$. Now, solve for r and then replace m and d with $ps_1 + at_1$ and $ps_2 + at_2$, respectively. You should end up with an expression for r involving p, a, s_1, s_2, t_1, and t_2. Next, rearrange this expression to obtain something of the form $r = p(\text{junk}) + a(\text{stuff})$. What does the minimality of d imply about r? You should be able to conclude that m is a multiple of d. That is, every element of S is a multiple of d. However, recall that $p \in S$, p is prime, and p and a are relatively prime. What can you conclude about d?

[3] *Hint:* If p divides a, we are done. So, assume otherwise. That is, assume that p does not divide a, so that p and a are relatively prime. Apply Lemma 5.10 to p and a and then multiply the resulting equation by b. Try to conclude that p divides b.

[4] *Hint:* Let n be a natural number greater than 1. By Lemma 5.4, we know that n can be expressed as a product of primes. All that remains is to prove that this product is unique (up to the order in which they appear). For sake of a contradiction, suppose $p_1 p_2 \cdots p_k$ and $q_1 q_2 \cdots q_l$ are both prime factorizations of n. Your goal is to prove that $k = l$ and that each p_i is equal to some q_j. Make repeated use of Euclid's Lemma.

Definition 5.15. Let $r \in \mathbb{R}$.

(a) We say that r is **rational** if and only if $r = \frac{m}{n}$, where $m, n \in \mathbb{Z}$ and $n \neq 0$.

(b) In contrast, we say that r is **irrational** if and only if it is not rational.

The Pythagoreans were an ancient secret society that followed their spiritual leader: Pythagoras of Samos (c. 570–495 BCE). The Pythagoreans believed that the way to spiritual fulfillment and to an understanding of the universe was through the study of mathematics. They believed that all of mathematics, music, and astronomy could be described via whole numbers and their ratios. In modern mathematical terms they believed that all numbers are rational. Attributed to Pythagoras is the saying, "Beatitude is the knowledge of the perfection of the numbers of the soul." And their motto was "All is number."

Thus they were stunned when one of their own—Hippasus of Metapontum (c. 5th century BCE)—discovered that the side and the diagonal of a square are incommensurable. That is, the ratio of the length of the diagonal to the length of the side is irrational. Indeed, if the side of the square has length a, then the diagonal will have length $a\sqrt{2}$; the ratio is $\sqrt{2}$ (see Figure 5.1).

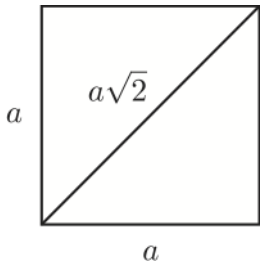

Figure 5.1: The side and diagonal of a square are incommensurable.

Theorem 5.16. The real number $\sqrt{2}$ is irrational.[5]

As one might expect, the Pythagoreans were unhappy with this discovery. Legend says that Hippasus was expelled from the Pythagoreans and was perhaps drowned at sea. Ironically, this result, which angered the Pythagoreans so much, is probably their greatest contribution to mathematics: the discovery of irrational numbers.

See if you can generalize the technique in the proof of Theorem 5.16 to prove the next two theorems.

Theorem 5.17. Let p be a prime number. Then $\sqrt{p}$ is irrational.

Theorem 5.18. Let p and q be distinct primes. Then $\sqrt{pq}$ is irrational.

[5] *Hint:* Use a proof by contradiction. That is, suppose that there exist $m, n \in \mathbb{Z}$ such that $n \neq 0$ and $\sqrt{2} = \frac{m}{n}$. We may assume that m and n are relatively prime; otherwise, we could cancel common factors. Next, square both sides and solve for m^2. How many factors of 2 are on each side of this equation according to the Fundamental Theorem of Arithmetic? Don't actually try to find the exact number of 2's, but rather see if you can figure out if there is an odd or even number of 2's on each side.

Problem 5.19. State a generalization of Theorem 5.18 and briefly describe how its proof would go. Be as general as possible.

It is important to point out that not every positive irrational number is equal to the square root of some natural number. For example, π is irrational, but is not equal to the square root of a natural number. It is also worth pointing out that our approach for proving that $\sqrt{2}$ was irrational was not the most efficient. However, our technique was easy to generalize to handle results like Theorem 5.17.

5.3 The Infinitude of Primes

The highlight of this section is Theorem 5.22, which states that there are infinitely many primes. The first known proof of this theorem is in Eulcid's *Elements* (c. 300 BCE). Euclid stated it as follows:

> **Proposition IX.20.** Prime numbers are more than any assigned multitude of prime numbers.

There are a few interesting observations to make about Euclid's proposition and his proof. First, notice that the statement of the theorem does not contain the word "infinity." The Greek's were skittish about the idea of infinity. Thus, he proved that there were more primes than any given finite number. Today we'd say that they are infinite. In fact, Euclid proved that there are more than *three* primes and concluded that there were more than any finite number. While you would lose points for such a proof in this class, we can forgive Euclid for this less-than-rigorous proof; in fact, it is easy to turn his proof into the general one that you will give below. Lastly, Euclid's proof was geometric. He was viewing his numbers as line segments with integral length. The modern concept of number was not developed yet.

Prior to tackling a proof of Theorem 5.22, we need to prove a couple lemmas. The proof of the first lemma is provided for you.

Lemma 5.20. The only natural number that divides 1 is 1.

Proof. Let m be a natural number that divides 1. We know that $m \geq 1$ because 1 is the smallest positive integer. Since m divides 1, there exists $k \in \mathbb{N}$ such that $1 = mk$. Since $k \geq 1$, we see that $mk \geq m$. But $1 = mk$, and so $1 \geq m$. Thus, we have $1 \leq m \leq 1$, which implies that $m = 1$, as desired. □

Lemma 5.21. Let p be a prime number and let $n \in \mathbb{Z}$. If p divides n, then p does not divide $n + 1$.[6]

We are now ready to prove the following important theorem.

Theorem 5.22. There are infinitely many prime numbers.[7]

[6] *Hint:* Use a proof by contradiction and utilize the previous lemma.

[7] *Hint:* Use a proof by contradiction. That is, assume that there are finitely many primes, say $p_1, p_2, \ldots, p_k$. Consider the product of all of them and then add 1.