Chapter 4

Two Famous Theorems

As the title suggests, in this chapter, we tackle two famous theorems. Most of this chapter was originally written by Dave Richeson of Dickinson College.

4.1 The Irrationality of $\sqrt{2}$

In this section we will prove one of the oldest and most important theorems in mathematics. 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[1]. 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 4.1). The goal of this section is to prove the following theorem: $\sqrt{2}$ is irrational (see Theorem 4.8). In order to do this, we need a few tools.

In case you forgot, here is the definition of a prime number.

Definition 4.1. A natural number p is called **prime** iff p is divisible by exactly two distinct natural numbers (namely, 1 and p itself).

Exercise 4.2. Is 1 a prime number? Explain your answer.

We will make use of the Fundamental Theorem of Arithmetic (see Corollary 4.7). The following result makes up half of the Fundamental Theorem of Arithmetic.

[1] Recall that a number is **rational** if it can be written in the form $\frac{m}{n}$, where $m, n \in \mathbb{Z}$ and $n \neq 0$. A number is **irrational** if it is not rational.

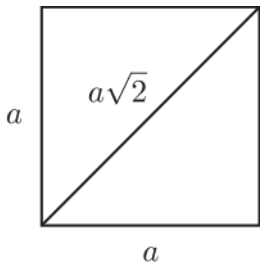

Figure 4.1: The side and diagonal of a square are incommensurable.

Theorem 4.3. 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 $p_1, p_2, \ldots, p_k$ are prime numbers (and there may possibly be repeats in this list).[2]

The previous theorem states that we can write every natural number as a product of primes, but it does not say that the primes and the number of times each prime appears are unique. We will need the following result known as the Division Algorithm, but we won't worry about proving it. Instead, we will take it for granted and use it in the proof of Theorem 4.5, which we will then use to prove uniqueness.

Theorem 4.4 (Division Algorithm)**.** Suppose that $m, n \in \mathbb{N}$. Then there exists unique $q, r \in \mathbb{N}$ 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. Now, see if you can prove the following theorem, which is known as Euclid's Lemma.

Theorem 4.5 (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]

Alright, let's now tackle the uniqueness of the product of primes.

Theorem 4.6. Let n be a natural number greater than 1. Then the expression for n as the product of one or more primes is unique (up to the order in which they appear).[4]

The following corollary follows immediately from Theorem 4.3 and Theorem 4.6.

[2] *Hint:* Use a proof by contradiction. Let n be the smallest natural number for which the theorem fails. 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.

[3] *Hint:* Use a proof by contradiction and apply the Division Algorithm to both a and b. What can you say about ab?

[4] *Hint:* Use a proof by contradiction. Write n as both $p_1 p_2 \cdots p_k$ and $q_1 q_2 \cdots q_l$, where both are products of primes. Use Euclid's Lemma to derive a contradiction.

Corollary 4.7 (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.

We are finally ready to prove that $\sqrt{2}$ is irrational.

Theorem 4.8. 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.

Now, let's tackle a few more problems dealing with irrational numbers.

Problem 4.9. Determine whether $\dfrac{1+\sqrt{2}}{3+2\sqrt{2}}$ is rational or irrational and then prove that your answer is correct.

Theorem 4.10. Let p be a prime number. Then $\sqrt{p}$ is irrational.

Theorem 4.11. Let p and q be distinct primes. Then $\sqrt{pq}$ is irrational.

Problem 4.12. State a generalization of Theorem 4.11 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 4.10.

4.2 The Infinitude of Primes

The highlight of this section is Theorem 4.15, 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

[5] *Hint:* Use a proof by contradiction. That is, suppose that there exist $m, n \in \mathbb{Z}$ such that $n \neq 0$ and $\sqrt{2} = \frac{m}{n}$. Next, square both sides and solve for m^2. How many factors of 2 does m^2 have? How many factors of 2 does $2n^2$ have? Derive a contradiction using Corollary 4.7.

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 4.15, we need to prove a couple lemmas. The proof of the first lemma is provided for you.

Lemma 4.13. 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 4.14. Let p be a prime number and let $n \in \mathbb{Z}$. If p divides n, then p does not divide $n + 1$.[6]

Now, we are ready to prove the following important theorem.

Theorem 4.15. 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. In this case, there are finitely many primes. Consider the product of all of them and then add 1.