A mathematician, like a painter or a poet, is a maker of patterns. If his patterns are more permanent than theirs, it is because they are made with ideas.

G.H. Hardy, mathematician

# Chapter 6

# Three Famous Theorems

In the last few chapters, we have encountered all of the major proof techniques one needs in mathematics and enhanced our proof-writing skills. In this chapter, we put these techniques and skills to work to prove three famous theorems, as well as numerous intermediate results along the way. All of these theorems are ones you are likely familiar with from grade school, but perhaps these facts were never rigorously justified for you.

In the first section, we develop all of the concepts necessary to state and then prove the **Fundamental Theorem of Arithmetic** (Theorem 6.17), which you may not recognize by name. The Fundamental Theorem of Arithmetic states that every natural number greater than 1 is the product of a unique combination of prime numbers. To prove the Fundamental Theorem of Arithmetic, we will need to make use of the **Division Algorithm** (Theorem 6.7), which in turn utilizes the Well-Ordering Principle (Theorem 4.38). In the second section, we prove that $\sqrt{2}$ is irrational, which settles a claim made in Section 5.1. In the final section, we prove that there are infinitely many primes.

## 6.1 The Fundamental Theorem of Arithmetic

The goal of this section is to prove The Fundamental Theorem of Arithmetic. 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 have just thrown around a few fancy terms; we should make sure we understand their precise meaning.

**Definition 6.1.** 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**.

**Problem 6.2.** According to our definition, is 1 a prime number or composite number? Explain your answer. You may have heard prime numbers defined as something like, "a prime number is a natural number that is only divisible by 1 and itself." Does this definition agree with the one above?

The upshot is that according to our definition, 1 is neither prime nor composite. However, throughout history, this has not always been the case. There were times when and mathematicians for whom the number one was considered prime. Whether 1 is prime or not is a matter of definition, and hence a matter of choice. There are compelling reasons—that we will not elaborate on here—why 1 is intentionally excluded from being prime. However, if you would like to learn more, check out the excellent article "What is the Smallest Prime?" by Chris Caldwell and Yeng Xiong.

**Problem 6.3.** List the first 10 prime numbers.

**Problem 6.4.** Prove or provide a counterexample: For all $n \in \mathbb{N}$, if $4^n - 1$ is prime, then $n$ is odd.

**Problem 6.5.** Prove or provide a counterexample: For all $n \in \mathbb{N}$, $n^2 - n + 11$ is prime.

The next result makes up half of the Fundamental Theorem of Arithmetic. We provide a substantial hint for its proof. 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 4.38), $S$ 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 $n$.

**Theorem 6.6.** If $n$ is 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).

Theorem 6.6 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 6.15). To prove Euclid's Lemma, we will utilize a special case of **Bézout's Lemma** (Theorem 6.13), the proof of which relies on the following result, known as the Division Algorithm. We include the proof of the Division Algorithm below, which makes use of the Well-Ordering Principle (Theorem 4.38).

**Theorem 6.7** (Division Algorithm)**.** If $n, d \in \mathbb{Z}$ such that $d > 0$, then there exists unique $q, r \in \mathbb{Z}$ such that $n = dq + r$ with $0 \leq r < d$.

*Proof.* Let $n, d \in \mathbb{Z}$ such that $d > 0$ such that $n > 0$. We have two tasks. First, we need to show that $q$ and $r$ exist, and then we need to show that both are unique.

If $d = 1$, it is clear that we can take $q = n$ and $r = 0$, so that $n = 1 \cdot n + 0 = dq + r$, as desired. Now, assume that $d > 1$ and define

$$S := \{n - dk \mid k \in \mathbb{Z} \text{ and } n - dk \geq 0\}.$$

If we can show that $S \neq \emptyset$, then we can apply the Well-Ordering Principle (Theorem 4.38) to conclude that $S$ has a least element of S. This least element will be the remainder $r$ we are looking for. There are two cases.

First, suppose $n \geq 0$. If we take $k = 0$, then we get $n - dk = n - d \cdot 0 = n \geq 0$, which shows that $n \in S$.

Now, suppose $n < 0$. In this case, we can take $k = n$, so that $n - dk = n - dn = n(1 - d)$. Since $n < 0$ and $d > 1$, $n(1 - d) > 0$. This shows that $n - dn \in S$.

We have shown that $S \neq \emptyset$, and so $S$ contains a least element $r = n - dq$ for some $q \in \mathbb{Z}$. Then $n = dq + r$ with $r \geq 0$. For sake of a contradiction, assume $r \geq d$. This implies that there exists $r' \in \mathbb{Z}$ such that $r = d + r'$ and $0 \leq r' < r$. But then we see that

$$n = dq + r = dq + d + r' = d(q + 1) + r'.$$

This implies that $r' = n - d(q + 1)$. Since $0 \leq r' < r$, we have produced an element of $S$ that is smaller than $r$. This contradicts the fact that $r$ is the least element of $S$, and so $r < d$.

It remains to show that $q$ and $r$ are unique. Suppose $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ such that $n = dq_1 + r_1$ and $n = dq_2 + r_2$ and $0 \leq r_1, r_2 < d$. Without loss of generality, suppose $r_2 \geq r_1$, so that $0 \leq r_2 - r_1 < d$. Since $dq_1 + r_1 = dq_2 + r_2$, we see that $r_2 - r_1 = d(q_1 - q_2)$. But then $d$ divides $r_2 - r_1$. If $r_2 - r_1 > 0$, then by Theorem 2.56, it must be the case that $r_2 - r_1 \geq d$. However, we know $0 \leq r_2 - r_1 < d$, and so we must have $r_2 - r_1 = 0$. Therefore, $r_1 = r_2$, which in turn implies $q_1 = q_2$. We have shown that $q$ and $r$ are unique. □

In the Division Algorithm, we call $n$ the **dividend**, $d$ the **divisor**, $q$ the **quotient**, and $r$ the **remainder**. It is worth pointing out that the Division Algorithm holds more generally where the divisor $d$ is not required to be positive. In this case, we must replace $0 \leq r < n$ with $0 \leq r < |n|$.

Contrary to its name, our statement of the Division Algorithm is not actually an algorithm, but this is the theorem's traditional name. However, there is an algorithm buried in this theorem. If $n$ is nonnegative, repeatedly subtract $d$ from $n$ until we obtain an integer value that lies between 0 (inclusive) and $d$ (exclusive). The resulting value is the remainder $r$ while the number of times that $d$ is subtracted is the quotient $q$. On the other hand, if $n$ is negative, repeatedly add $d$ to $n$ until we obtain an integer value that lies between 0 (inclusive) and $d$ (exclusive). Again, the resulting value is $r$. However, in this case, we take $-q$ to be the number of times that $d$ is added, so that $q$ (a negative value) is the quotient.

**Problem 6.8.** Suppose $n = 27$ and $d = 5$. Find the quotient and remainder that are guaranteed to exist by the Division Algorithm. That is, find the unique $q, r \in \mathbb{Z}$ such that $0 \leq r < n$ and $n = dq + r$.

It is a little trickier to determine $q$ and $r$ when $n$ is negative.

**Problem 6.9.** Suppose $n = -26$ and $d = 3$. Find the quotient and remainder that are guaranteed to exist by the Division Algorithm. That is, find the unique $q, r \in \mathbb{Z}$ such that $0 \leq r < n$ and $n = dq + r$.

It is useful to have some additional terminology.

**Definition 6.10.** 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 $\boxed{\gcd(m,n)}$, is the largest positive integer that divides both $m$ and $n$. If $\gcd(m,n) = 1$, we say that $m$ and $n$ are **relatively prime**.

**Problem 6.11.** Find $\gcd(54, 72)$.

**Problem 6.12.** 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 6.15), which we then use to prove uniqueness for the Fundamental Theorem of Arithmetic (Theorem 6.17). To prove our special case of Bézout's Lemma, 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 4.38), $S$ contains a least element, say $d$. This implies that 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 $r$ as a linear combination of $p$ and $a$ (i.e., a sum of a multiple of $p$ and a multiple of $a$). 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 $d$?

**Theorem 6.13** (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 $ps + at = 1$.

**Problem 6.14.** Consider the natural numbers 2 and 7, which happen to be relatively prime. Find integers $s$ and $t$ guaranteed to exist according to Theorem 6.13. That is, find $s, t \in \mathbb{Z}$ such that $2s + 7t = 1$.

The following theorem is known as Euclid's Lemma. Note that if $p$ divides $a$, the conclusion is certainly true. So, assume otherwise. That is, assume that $p$ does not divide $a$, so that $p$ and $a$ are relatively prime. Apply Theorem 6.13 to $p$ and $a$ and then multiply the resulting equation by $b$. Try to conclude that $p$ divides $b$.

**Theorem 6.15** (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 $b$.

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

**Problem 6.16.** 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. Let $n$ be a natural number greater than 1. By Theorem 6.6, 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.

**Theorem 6.17** (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.

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.

> Any creative endeavor is built on the ash heap of failure.
>
> Michael Starbird, mathematician

## 6.2 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 6.19). First, we need to know what this means.

**Definition 6.18.** Let $r \in \mathbb{R}$.

(a) We say that $r$ is **rational** 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 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 6.1).

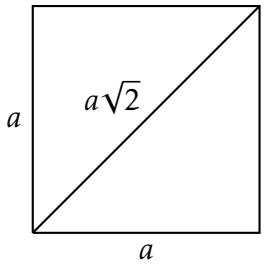


Figure 6.1: The side and diagonal of a square are incommensurable.

In Section 5.1, we took for granted that $\sqrt{2}$ was irrational. We now prove this fact. Consider using a proof by contradiction. Suppose that there exist $m, n \in \mathbb{Z}$ such that $n \neq 0$ and $\sqrt{2} = \frac{m}{n}$. Are there an odd or even number of factors of 2 on each side of this equation? Does your conclusion violate the Fundamental Theorem of Arithmetic (Theorem 6.17)?

**Theorem 6.19.** The real number $\sqrt{2}$ is irrational.

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 6.19 to prove the next two theorems.

**Theorem 6.20.** Let $p$ be a prime number. Then $\sqrt{p}$ is irrational.

**Theorem 6.21.** Let $p$ and $q$ be distinct primes. Then $\sqrt{pq}$ is irrational.

**Problem 6.22.** State a generalization of Theorem 6.21 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, $\pi$ is irrational, but is not equal to the square root of a natural number.

> Getting better is not pretty. To get good we have to be down to struggle, seek out challenges, make some mistakes, to train ugly.
>
> Trevor Ragan, thelearnerlab.com

## 6.3 The Infinitude of Primes

The highlight of this section is Theorem 6.25, which states that there are infinitely many primes. The first known proof of this theorem is in Euclid'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 would say that there are infinitely many. In fact, Euclid proved that there are more than *three* primes and concluded that there were more than any finite number. While such a proof is not considered valid in the modern era, 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 6.25, we need to prove a couple of preliminary results. The proof of the first result is provided for you.

**Theorem 6.23.** 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. □

For the next theorem, try utilizing a proof by contradiction together with Theorem 6.23.

**Theorem 6.24.** Let $p$ be a prime number and let $n \in \mathbb{Z}$. If $p$ divides $n$, then $p$ does not divide $n+1$.

We are now ready to prove the following important theorem. Use a proof by contradiction. In particular, 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.

**Theorem 6.25.** There are infinitely many prime numbers.

We conclude this chapter with a fun problem involving prime numbers. This problem comes from David Richeson (Dickinson College).

**Problem 6.26.** Start with the first $n$ prime numbers, $p_1, \ldots, p_n$. Divide them into two sets. Let $a$ be the product of the primes in one set and let $b$ be the product of the primes in the other set. Assume the product is 1 if the set is empty. For example, if $n = 5$, we could have $\{2, 7\}$ and $\{3, 5, 11\}$, and so $a = 14$ and $b = 165$. In general, what can we conclude about $a + b$ and $a - b$? Form a conjecture and then prove it.

> It does not matter how slowly you go as long as you do not stop.
>
> Confucius, philosopher