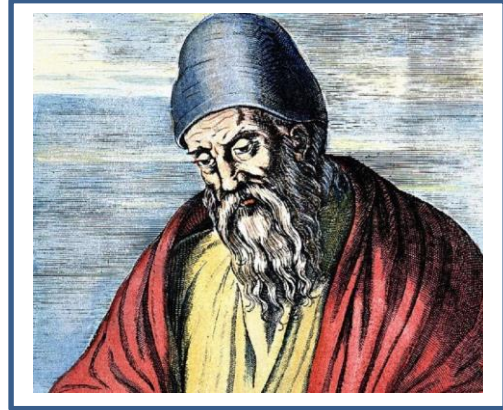# CHAPTER

Two

Prime Numbers

The laws of nature are but the mathematical

thoughts of God

Euclid, Euclid of Alexandria 325-365 B.C.

Prime Numbers

The history of prime numbers dates back to ancient civilizations. Here's a brief overview:

(1) Ancient Civilizations: The concept of prime numbers has been known since ancient times. Mathematicians in civilizations like Ancient Egypt and Ancient Greece studied prime numbers. The Greek mathematician Euclid, around 300 BCE, famously proved that there are infinitely many prime numbers in his work "Elements."

(2) Number Theory Development: Prime numbers became a central topic in number theory, a branch of mathematics dedicated to the study of integers. Mathematicians like Pierre de Fermat and Leonhard Euler made significant contributions to prime number theory in the 17th and 18th centuries.

(3) The Prime Number Theorem: In the 19th century, mathematicians like Carl Friedrich Gauss and Bernhard Riemann made substantial progress in understanding the distribution of prime numbers. This led to the development of the Prime Number Theorem, which describes the asymptotic distribution of prime numbers.

(4) Modern Research: Prime numbers continue to be a topic of active research. They play a crucial role in various fields, including cryptography (RSA algorithm), computer science (algorithms like the Sieve of Eratosthenes), and number theory (the Riemann Hypothesis, an unsolved conjecture about prime numbers).

(5) Prime Number Records: Over the years, mathematicians and computers have discovered and verified increasingly large prime numbers. Notable examples include Mersenne primes and the largest known prime numbers, which are often expressed with millions of digits.

Prime numbers remain a fascinating and essential part of mathematics with a rich history of study and discovery.

Prime numbers, the building blocks of integers, have been studied extensively over the centuries. Being able to present an integer uniquely as product of primes is the main reason behind the whole theory of numbers and behind the interesting results in this theory. Many interesting theorems, applications and conjectures have been formulated based on the properties of prime numbers.

In this chapter, we present methods to determine whether a number is prime or composite using an ancient Greek method invented by Eratosthenes. We also show that there are infinitely many prime numbers. We then proceed to show that every integer can be written uniquely as a product of primes.

We introduce as well the concept of Diophantine equations where integer solutions from given equations are determined using the greatest common divisor. We then mention the Prime Number theorem without giving a proof of course in addition to other conjectures and major results related to prime numbers.

1.1. The Sieve of Eratosthenes

Definition 1 A **prime** is an integer greater than 1 that is only divisible by 1 and itself.

Example 15. The integers 2, 3, 5, 7, 11 are prime integers. Note that any integer greater than 1 that is not prime is said to be a **composite** number.

We now present the sieve of Eratosthenes. The Sieve of Eratosthenes is an ancient method of finding prime numbers up to a specified integer. This method was invented by the ancient Greek mathematician Eratosthenes. There are several other methods used to determine whether a number is prime or composite. We first present a lemma that will be needed in the proof of several theorems.

Lemma 1 Every integer greater than one has a prime divisor.

Proof. We present the proof of this Lemma by contradiction. Suppose that there is an integer greater than one that has no prime divisors. Since the set of integers with elements greater than one with no prime divisors is nonempty, then by the well ordering principle there is a least positive integer n greater than one that has no prime divisors. Thus n is composite since n divides n. Hence

$$n = ab \text{ with } 1 < a < n, \text{ and } 1 < b < n.$$

Notice that $a < n$ and as a result since n is minimal, a must have a prime divisor which will also be a divisor of n.

Theorem 1 If n is a composite integer, then n has a prime factor not exceeding $\sqrt{n}$.

Proof. Since n is composite, then $n = ab$, where a and b are integers with $1 < a \leq b < n$. Suppose now that $a > \sqrt{n}$, then $\sqrt{n} < a \leq b$,

and as a result $ab > \sqrt{n}\sqrt{n} = n$.

Therefore $a \leq \sqrt{n}$. Also, by Lemma 1, $\boldsymbol{a}$ must have a prime divisor a_1 which is also a prime divisor of n and thus this divisor is less than $a_1 \leq a \leq \sqrt{n}$.

We now present the algorithm of the Sieve of Eratosthenes that is used to determine prime numbers up to a given integer.

1.2. The Algorithm of the Sieve of Eratosthenes

1. Write a list of numbers from 2 to the largest number n you want to test. Note that every composite integer less than n must have a prime factor less than $\sqrt{n}$. Hence you need to strike off the multiples of the primes that are less than $\sqrt{n}$

2. Strike off all multiples of 2 greater than 2 from the list. The first remaining number in the list is a prime number.

3. Strike off all multiples of this number from the list.

4. Repeat the above steps until no more multiples are found of the prime integers that are less than $\sqrt{n}$.

1.3. Exercises

1. Use the Sieve of Eratosthenes to find all primes less than 100.

2. Use the Sieve of Eratosthenes to find all primes less than 200.

3. Show that no integer of the form $a^3 + 1$ is a prime except for $2 = 1^3 + 1$.

4. Show that if $2^n - 1$ is prime, then n is prime.

Hint: Use the identity $(a^{kl} - 1) = (a^k - 1)(a^{k(l-1)} + a^{k(l-2)} + \cdots + a^k + 1)$.

1.4. The infinitude of Primes

We now show that there are infinitely many primes. There are several ways to prove this result. An alternative proof to the one presented here is given as an exercise. The proof we will provide was presented by Euclid in his book the Elements.

Theorem 2 (Euclid) There are infinitely many primes.

Proof We present the proof by contradiction. Suppose there are finitely many primes $p_1, p_2, \dots, p_n$, where n is a positive integer. Consider the integer Q such that

$$Q = p_1 p_2 \dots p_n + 1$$

By Lemma 1, Q has at least a prime divisor, say q. If we prove that q is not one of the primes listed then we obtain a contradiction. Suppose now that $q = p_i$ for $1 \leq i \leq n$. Thus q divides $p_1 p_2 \dots p_n$ and as a result q divides $Q - p_1 p_2 \dots p_n$. Therefore q divides 1. But this is impossible since there is no prime that divides 1 and as a result q is not one of the primes listed.

The following theorem discusses the large gaps between primes. It simply states that there are arbitrary large gaps in the series of primes and that the primes are spaced irregularly.

Theorem 3 Given any positive integer n, there exists n consecutive composite integers.

Proof Consider the sequence of integers

$$(n+1)! + 2, (n+1)! + 3, \dots, (n+1)! + n, (n+1)! + n + 1$$

Notice that every integer in the above sequence is composite because k divides $(n+1)!$ $+k$ if $2 \leq k \leq n+1$ by 4.

1.5. Exercises

1. Show that the integer $Q_n = n! + 1$, where n is a positive integer, has a prime divisor greater than n. Conclude that there are infinitely many primes. Notice that this exercise is another proof of the infinitude of primes.

2. Find the smallest five consecutive composite integers.

3. Find one million consecutive composite integers.

4. Show that there are no prime triplets other than 3,5,7.

1.6. The Fundamental Theorem of Arithmetic

The Fundamental Theorem of Arithmetic is one of the most important results in this chapter. It simply says that every positive integer can be written uniquely as a product of primes. The unique factorization is needed to establish much of what comes later. There are systems where unique factorization fails to hold. Many of these examples come from algebraic number theory. We can actually list an easy example where unique factorization fails.

Consider the class C of positive even integers. Note that C is closed under multiplication, which means that the product of any two elements in C is again in C. Suppose now that the only number we know are the members of C. Then we have $12 = 2.6$ is composite where as 14 is prime since it is not the product of two numbers in C. Now notice that $60 = 2.30 = 6.10$ and thus the factorization is not unique.

We now give examples of the unique factorization of integers.

Example $199 = 3 \cdot 3 \cdot 11 = 3^2 \cdot 11$, $32 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^5$

1.6.1. The Fundamental Theorem of Arithmetic

To prove the fundamental theorem of arithmetic, we need to prove some lemmas about divisibility.

Lemma 2 If a, b, c are positive integers such that $(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

Proof Since $(a, b) = 1$, then there exists integers x, y such that $ax + by = 1$. As a result, $cax + cby = c$. Notice that since $a \mid bc$, then by Theorem 4, a divides $cax + cby$ and hence a divides c.

We can generalize the above lemma as such: If $(a, n_i) = 1$ for every $i = 1, 2, \cdots, n$ and $a \mid n_1 n_2 \cdots n_{k+1}$, then $a \mid n_{k+1}$. We next prove a case of this generalization and use this to prove the fundamental theorem of arithmetic.

Lemma 3 If p divides $n_1 n_2 n_3 \ldots n_k$, where p is a prime and $n_i > 0$ for all $1 \le i \le k$, then there is an integer j with $1 \le j \le k$ such that $p \mid n_j$.

Proof We present the proof of this result by induction. For $k = 1$, the result is trivial. Assume now that the result is true for k. Consider $n_1 n_2 \ldots n_{k+1}$ that is divisible by p. Notice that either

$$(p, n_1 n_2 \ldots n_k) = 1 \text{ or } (p, n_1 n_2 \ldots n_k) = p$$

Now if $(p, n_1 n_2 \ldots n_k) = 1$ then by Lemma 4, $p \mid n_{k+1}$. Now if $p \mid n_1 n_2 \ldots n_k$, then by the induction hypothesis, there exists an integer i such that $p \mid n_i$.

We now state the fundamental theorem of arithmetic and present the proof using Lemma 5.

Theorem 4 (The Fundamental Theorem of Arithmetic) Every positive integer different from 1 can be written uniquely as a product of primes.

Proof If n is a prime integer, then n itself stands as a product of primes with a single factor. If n is composite, we use proof by contradiction. Suppose now that there is some positive integer that cannot be written as the product of primes. Let n be the smallest such integer. Let $n = ab$, with $1 < a < n$ and $1 < b < n$. As a result a and b are

products of primes since both integers are less than n. As a result, $n = ab$ is a product of primes, contradicting that it is not. This shows that every integer can be written as product of primes. We now prove that the representation of a positive integer as a product of primes is unique.

Suppose now that there is an integer n with two different factorizations say

$$n = p_1 p_2 \dots p_s = q_1 q_2 \dots q_r$$

where $p_1, p_2, \dots p_s, q_1, q_2, \dots q_r$ are primes,

$$p_1 \leq p_2 \leq p_3 \leq \dots \leq p_s \text{ and } q_1 \leq q_2 \leq q_3 \leq \dots \leq q_r$$

Cancel out all common primes from the factorizations above to get

$$p_{j_1} p_{j_2} \dots p_{j_u} = q_{i_1} q_{i_2} \dots q_{i_v}$$

Thus all the primes on the left side are different from the primes on the right side. Since any $p_{j_l} (l = 1, \cdots, n)$ divides $p_{j_1} p_{j_2} \dots p_{j_u}$, then p_{j_l} must divide $q_{i_1} q_{i_2} \dots q_{i_v}$, and hence by Lemma 3, p_{j_l} must divide q_{i_k} for some $1 \leq k \leq v$ which is impossible. Hence the representation is unique.

Remark 1 The unique representation of a positive integer n as a product of primes can be written in several ways. We will present the most common representations. For example, $\boldsymbol{n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} = \prod_{i=1}^{k} p_i^{\alpha_i}}$, where $\boldsymbol{p_1 < p_2 < \cdots < p_k}$ are primes and the $\boldsymbol{\alpha_i}$ are positive integers

This representation is called the ***canonical representation*** of $\boldsymbol{n}$, or the ***standard form*** of $\boldsymbol{n}$.

Example 2 The prime factorization of 120 is given by $120 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 = 2^3 \cdot 3 \cdot 5$. Notice that 120 is written in the two ways described in 1.

We know describe in general how prime factorization can be used to determine the greatest common divisor of two integers. Let $a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$ and $b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$,

where we exclude in these expansions any prime p with power 0 in both a and b (and thus some of the powers above may be 0 in one expansion but not the other). Of course, if one prime p_i appears in a but not in b, then $a_i \neq 0$ while $b_i = 0$, and vise versa. Then the greatest common divisor is given by

$$(a, b) = p_1^{\min(a_1, b_2)} p_2^{\min(a_2, b_2)} \dots p_n^{\min(a_n, b_n)}$$

where $\min(n, m)$ is the minimum of m and n.

The following lemma is a consequence of the Fundamental Theorem of Arithmetic.

Lemma 5 Let a and b be relatively prime positive integers. Then if d divides ab, there exists d_1 and d_2 such that $d = d_1 d_2$ where d_1 is a divisor of a and d_2 is a divisor of b. Conversely, if d_1 and d_2 are positive divisors of a and b, respectively, then $d = d_1 d_2$ is a positive divisor of ab.

Proof Let $d_1 = (a, d)$ and $d_2 = (b, d)$. Since $(a, b) = 1$ and writing a and b in terms of their prime decomposition, it is clear that $d = d_1 d_2$ and $(d_1, d_2) = 1$. Note that every prime power in the factorization of d must appear in either d_1 or d_2. Also the prime powers in the factorization of d that are prime powers dividing a must appear in d_1 and that prime powers in the factorization of d that are prime powers dividing b must appear in d_2. Now conversely, let d_1 and d_2 be positive divisors of a and b, respectively.

Then $d = d_1 d_2$ is a divisor of ab.

1.6.2. More on the Infinitude of Primes

There are also other theorems that discuss the infinitude of primes in a given arithmetic progression. The most famous theorem about primes in arithmetic progression is Dirichlet's theorem

Theorem 6 (Dirichlet's Theorem) Given an arithmetic progression of terms $an + b$, for $n = 1,2, ...$, the series contains an infinite number of primes if a and b are relatively prime,

This result had been conjectured by Gauss but was first proved by Dirichlet. Dirichlet proved this theorem using complex analysis, but the proof is so challenging.

1.7. Exercises

1. Find the prime factorization of 32, of 800 and of 289.

2. Find the prime factorization of 221122 and of 9 !!.

3. Show that all the powers of in the prime factorization of an integer a are even if and only if a is a perfect square.

4. Show that there are infinitely many primes of the form $6n + 5$.

2. Least Common Multiple

We can use prime factorization to find the smallest common multiple of two positive integers.

Definition 2 The least common multiple (*l.c.m.*) of two positive integers is the smallest positive integer that is a multiple of both.

We denote the least common multiple of two positive integers a an b by $\langle a, b \rangle$.

Example 3 $\langle 2,8 \rangle = 8, \langle 5,8 \rangle = 40$

We can figure out $\langle a, b \rangle$ once we have the prime factorization of a and b. To do that, let

$$a = p_1^{a_1} p_2^{a_2} \dots p_m^{a_n} \text{ and } b = p_1^{b_1} p_2^{b_2} \dots p_m^{b_n},$$

where (as above) we exclude any prime with 0 power in both a and b. Then $\langle a, b \rangle = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \dots p_m^{\max(a_n,b_n)}$, where $\max(a, b)$ is the maximum of the two integers a and b. We now prove a theorem that relates the least common multiple of two positive integers to their greatest common divisor. In some books, this theorem is adopted as the definition of the least common multiple. To prove the theorem we present the following lemma

Lemma 7 If a and b are two real numbers, then

$$\min(a, b) + \max(a, b) = a + b$$

Proof Assume without loss of generality that $a \geq b$. Then

$$\max(a, b) = a \text{ and } \min(a, b) = b,$$

and the result follows.

Theorem 8 Let a and b be two positive integers. Then

1. $\langle a, b \rangle \geq 0$;

2. 2. $\langle a, b \rangle = ab/(a, b)$;

3. If $a \mid m$ and $b \mid m$, then $\langle a, b \rangle \mid m$

Proof The proof of **part 1** follows from the definition.

As for **part 2**, let $a = p_1^{a_1} p_2^{a_2} \dots p_m^{a_n}$, and $b = p_1^{b_1} p_2^{b_2} \dots p_m^{b_n}$

Notice that since

$$(a, b) = p_1^{\min(a_1, b_2)} p_2^{\min(a_2, b_2)} \dots p_n^{\min(a_n, b_n)}$$

and

$$\langle a, b \rangle = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \dots p_m^{\max(a_n, b_n)}$$

then

$$
\begin{aligned}
\langle a, b \rangle (a, b) \quad &= p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \dots p_m^{\max(a_n, b_n)} p_1^{\min(a_1, b_2)} p_2^{\min(a_2, b_2)} \dots p_n^{\min(a_n, b_n)} \\
&= p_1^{\max(a_1, b_1)+\min(a_1, b_1)} p_2^{\max(a_2, b_2)+\min(a_2, b_2)} \dots p_m^{\max(a_n, b_n)+\min(a_n, b_n)} \\
&= p_1^{a_1+b_1} p_2^{a_2+b_2} \dots p_n^{(a_n+b_n)} \\
&= p_1^{a_1} p_2^{a_2} \dots p_m^{a_n} p_1^{b_1} p_2^{b_2} \dots p_m^{b_n} = ab
\end{aligned}
$$

Note also that we used Lemma 8 in the above equations.

For part 3, it would be a nice exercise to show that $ab/(a, b) \mid m$ (Exercise 6).

Thus $\langle a, b \rangle \mid m$.

2.1. Exercises

1. Find the least common multiple of 14 and 15.

2. Find the least common multiple of 240 and 610.

3. Find the least common multiple and the greatest common divisor of $2^5 5^6 7^2 11$ and $2^3 5^8 7^2 13$

4. Show that every common multiple of two positive integers a and b is divisible by the least common multiple of a and b.

5. Show that if a and b are positive integers then the greatest common divisor of a and b divides their least common multiple. When are the least common multiple and the greatest common divisor equal to each other.

6. Show that $ab/(a,b) \mid m$ where $m = < a, b >$.

3. Linear Diophantine Equations

In this section, we discuss equations in two variables called Diophantine equations. These kinds of equations require integer solutions. The goal of this section is to present the set of points that determine the solution to this kind of equations. Geometrically speaking, the Diophantine equation represents the equation of a straight line. We need to find the points whose coordinates are integers and through which the straight line passes.

Definition 3 A linear equation of the form $ax + by = c$ where a, b and c are integers is known as a linear Diophantine equation.

Note that a solution to the linear Diophantine equation (x_0, y_0) requires x_0 and y_0 to be integers. The following theorem describes the case in which the diophantine equation has a solution and what are the solutions of such equations.

Theorem 9 The equation $ax + by = c$ has integer solutions if and only if $d \mid c$ where $d = (a, b)$. If the equation has one solution $x = x_0, y = y_0$, then there are infinitely many solutions and the solutions are given by

$x = x_0 + (b/d)t \ y = y_0 - (a/d)t$, where t is an arbitrary integer.

Proof Suppose that the equation $ax + by = c$ has integer solution x and y. Thus since $d \mid a$ and $d \mid b$, then $d \mid (ax + by) = c$.

Now we have to prove that if $d \mid c$, then the equation has integral solution. Assume that $d \mid c$. By theorem 9, there exist integers m and n such that $d = am + bn$.

And also there exists integer k such that $c = dk$.

Now since $c = ax + by$, we have $c = dk = (ma + nb)k = a(km) + b(nk)$.

Hence a solution for the equation $ax + by = c$ is $x_0 = km$ and $y_0 = kn$.

What is left to prove is that we have infinitely many solutions.

Let $x = x_0 + (b/d)t$ and $y = y_0 - (a/d)t$.

We have to prove now that x and y are solutions for all integers t.

Notice that $ax + by = a(x_0 + (b/d)t) + b(y_0 - (a/d)t) = ax_0 + by_0 = c$.

We now show that every solution for the equation $ax + by = c$ is of the form

$$x = x_0 + (b/d) \text{ t} \text{and } y = y_0 - (a/d)t.$$

Notice that since $ax_0 + by_0 = c$, we have

$$a(x - x_0) + b(y - y_0) = 0.$$

Hence $a(x - x_0) = b(y - y_0)$.

Dividing both sides by d, we get $a/d(x - x_0) = b/d(y - y_0)$.

Notice that $(a/d, b/d) = 1$ and thus we get by Lemma 4 that $a/d \mid y - y_0$.

As a result, there exists an integer t such that $y = y_0 - (a/d)t$. Now substituting $y - y_0$ in the equation $a(x - x_0) = b(y - y_0)$.

We get $x = x_0 + (b/d)t$.

Example 4 The equation $3x + 6y = 7$ has no integer solution because $(3,6) = 3$ does not divide 7.

Example 5 There are infinitely many integer solutions for the equation $4x + 6y = 8$ because $(4,6) = 2 \mid 8$. We use the Euclidean algorithm to determine m and n where $4m + 6n = 2$. It turns out that $4(-1) + 6(1) = 2$. And also $8 = 2.4$. Thus $x_0 = 4.(-1) = -4$ and $y_0 = 4.1 = 4$ is a particular solution. The solutions are given by

$$x = -4 + 3t \quad y = 4 - 2t$$

for all integers t.

3.1. Exercises

1. Either find all solutions or prove that there are no solutions for the diophantine equation $21x + 7y = 147$

2. Either find all solutions or prove that there are no solutions for the diophantine equation $2x + 13y = 31$

3. Either find all solutions or prove that there are no solutions for the diophantine equation $2x + 14y = 17$. 4. A grocer orders apples and bananas at a total cost of $8.4. If the apples cost 25 cents each and the bananas 5 cents each, how many of each type of fruit did he order.

4. The Greatest Integer Function $[x]$

Definition 4 The function $[x]$ represents the largest integer not exceeding x. In other words, for real x, $[x]$ is the unique integer such that

$$x - 1 < [x] \leq x < [x] + 1.$$

We also define $((x))$ to be the fractional part of x. In other words $((x)) = x - [x]$

We now list some properties of $[x]$ that will be used in later or in more advanced courses in number theory.

1. $[x + n] = [x] + n$, if n is an integer.

2. $[x] + [y] \leq [x + y]$

3. $[x] + [-x]$ is 0 if x is an integer and -1 otherwise.

4. The number of integers m for which $x < m \leq y$ is $[y] - [x]$. 5. The number of multiples of m which do not exceed x is $[x/m]$.

Using the definition of $[x]$, it will be easy to see that the above properties are direct consequences of the definition.

5. Conjectures involving prime numbers

We have proved that there are infinitely many primes. We have also proved that there are arbitrary large gaps between primes. Several other theorems were proved concerning prime numbers. Many great mathematicians approached problems that are related to primes. There are still many open problems of which we will mention some.

Conjecture 1 (Twin Prime Conjecture) There are infinitely many pairs primes p and $p + 2$.

Conjecture 2 (Goldbach's Conjecture) Every even positive integer greater than 2 can be written as the sum of two primes.

Conjecture 3 (The $n^2 + 1$ Conjecture) There are infinitely many primes of the form $n^2 + 1$, where n is a positive integer.

Conjecture 4 (Polignac Conjecture) For every even number $2n$ are there infinitely many pairs of consecutive primes which differ by $2n$.

Conjecture 5 (Opperman Conjecture) Is there always a prime between n^2 and $(n + 1)^2$?