# An Introductory Course in Elementary Number Theory

Wissam Raji

## Preface

These notes serve as course notes for an undergraduate course in number theory. Most if not all universities worldwide offer introductory courses in number theory for math majors and in many cases as an elective course.

The notes contain a useful introduction to important topics that need to be addressed in a course in number theory. Proofs of basic theorems are presented in an interesting and comprehensive way that can be read and understood even by non-majors with the exception in the last three chapters where a background in analysis, measure theory and abstract algebra is required. The exercises are carefully chosen to broaden the understanding of the concepts. Moreover, these notes shed light on analytic number theory, a subject that is rarely seen or approached by undergraduate students. One of the unique characteristics of these notes is the careful choice of topics and its importance in the theory of numbers. The freedom is given in the last two chapters because of the advanced nature of the topics that are presented.

Thanks to professor Pavel Guerzhoy from University of Hawaii for his contribution in chapter 6 on continued fraction and to Professor Ramez Maalouf from Notre Dame University, Lebanon for his contribution to chapter 8.

# Contents

# Chapter 1

# Introduction

Integers are the building blocks of the theory of numbers. This chapter contains somewhat very simple and obvious observations starting with properties of integers and yet the proofs behind those observations are not as simple. In this chapter we introduce basic operations on integers and some algebraic definitions that will be necessary to understand basic concepts in this book. We then introduce the Well ordering principle which states basically that every set of positive integers has a smallest element. Proof by induction is also presented as an efficient method for proving several theorems throughout the book. We proceed to define the concept of divisibility and the division algorithm. We then introduce the elementary but fundamental concept of a greatest common divisor (gcd) of two integers, and the Euclidean algorithm for finding the gcd of two integers. We end this chapter with Lame's Lemma on an estimate of the number of steps in the Euclidean algorithm needed to find the gcd of two integers.

## 1.1 Algebraic Operations With Integers

The set $\mathbb{Z}$ of all integers, which this book is all about, consists of all positive and negative integers as well as 0. Thus $\mathbb{Z}$ is the set given by

$$\mathbb{Z} = \{..., -4, -3, -2, -1, 0, 1, 2, 3, 4, ...\}. \tag{1.1}$$

While the set of all *positive* integers, denoted by $\mathbb{N}$, is defined by

$$\mathbb{N} = \{1, 2, 3, 4, ...\}. \tag{1.2}$$

On $\mathbb{Z}$, there are two basic binary operations, namely **addition** (denoted by $+$) and **multiplication** (denoted by $\cdot$), that satisfy some basic properties from which every other property for $\mathbb{Z}$ emerges.

1. **The Commutativity property for addition and multiplication**

$$a + b = b + a$$
$$a \cdot b = b \cdot a$$

2. **Associativity property for addition and multiplication**

$$\begin{aligned}(a + b) + c &= a + (b + c)\\ (a \cdot b) \cdot c &= a \cdot (b \cdot c)\end{aligned}$$

3. **The distributivity property of multiplication over addition**

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

In the set $\mathbb{Z}$ there are ”identity elements” for the two operations $+$ and $\cdot$, and these are the elements $0$ and $1$ respectively, that satisfy the basic properties

$$a + 0 = 0 + a = a$$
$$a \cdot 1 = 1 \cdot a = a$$

for every $a \in \mathbb{Z}$.

The set $\mathbb{Z}$ allows **additive inverses** for its elements, in the sense that for every $a \in \mathbb{Z}$ there exists another integer in $\mathbb{Z}$, denoted by $-a$, such that

$$a + (-a) = 0. \tag{1.3}$$

While for multiplication, only the integer 1 has a **multiplicative inverse** in the sense that 1 is the only integer $a$ such that there exists another integer, denoted by $a^{-1}$ or by $1/a$, (namely 1 itself in this case) such that

$$a \cdot a^{-1} = 1. \tag{1.4}$$

From the operations of addition and multiplication one can define two other operations on $\mathbb{Z}$, namely **subtraction** (denoted by $-$) and **division** (denoted by $/$). Subtraction is a binary operation on $\mathbb{Z}$, i.e. defined for any two integers in $\mathbb{Z}$, while division is not a binary operation and thus is defined only for some specific couple of integers in $\mathbb{Z}$. Subtraction and division are defined as follows:

1. $a - b$ is defined by $a + (-b)$, i.e. $a - b = a + (-b)$ for every $a, b \in \mathbb{Z}$

2. $a/b$ is defined by the integer $c$ if and only if $a = b \cdot c$.

Some of the sets we study in Number Theory contain all these properties. Let $R$ be a set, with two operations called addition and multiplication. We say that $R$ is a **ring** if

- addition satisfies

- closure: for any $a, b \in R$, we also have $a + b \in R$;
- associativity: for any $a, b, c \in R$, we have $(a + b) + c = a + (b + c)$;
- commutativity: for any $a, b \in R$, we have $a + b = b + a$;
- identity: there exists a "zero element" 0 in $R$, which for any $a \in R$ satisfies $0 + a = a$;
- inverses: for any $a \in R$, we can find $b \in R$ such that $a + b = 0$ (we usually write $-a$ for this inverse);

while

- multiplication satisfies
  - closure: for any $a, b \in R$, we also have $a \times b \in R$;
  - associativity: for any $a, b, c \in R$, we have $(a \times b) \times c = a \times (b \times c)$;
  - commutativity: for any $a, b \in R$, we have $a \times b = b \times a$;
  - identity: there exists a "one element" 1 in $R$, which for any $a \in R$ satisfies $1 \times a = a$;
  - distributivity over addition: for any $a, b, c \in R$, we have $a \times (b + c) = a \times b + a \times c$.

Notice that we do *not* require multiplicative inverses in a ring: if the nonzero elements of a ring *do* have multiplicative inverses, then we call it a **field**.

**Remark 1.** *To be accurate, we are really talking about a* commutative *ring; in general, a ring's multiplication need not be commutative — think, for example, of matrices. However, we only consider commutative rings in here.*

**Exercises**

1. Which of the following are rings under ordinary addition and multiplication, and which are also fields?

$$\mathbb{N}, \quad \mathbb{Z}, \quad \mathbb{Q}, \quad \mathbb{R}, \quad \mathbb{C}, \quad \left\{a + b\sqrt{2} : a, b \in \mathbb{Z}\right\}$$

## 1.2 The Well Ordering Principle and Mathematical Induction

In this section, we present three basic tools that will often be used in proving properties of the integers. We start with a very important property of integers called the well ordering principle. We then state what is known as the pigeonhole principle, and then we proceed to present an important method called mathematical induction.

### 1.2.1 The Well Ordering Principle

**The Well Ordering Principle:** A least element exist in any non empty set of positive integers.

This principle can be taken as an axiom on integers and it will be the key to proving many theorems. As a result, we see that any set of positive integers is well ordered while the set of all integers is not well ordered.

### 1.2.2 The Pigeonhole Principle

**The Pigeonhole Principle:** If $s$ objects are placed in $k$ boxes for $s > k$, then at least one box contains more than one object.

*Proof.* Suppose that none of the boxes contains more than one object. Then there are at most $k$ objects. This leads to a contradiction with the fact that there are $s$ objects for $s > k$. □

### 1.2.3 The Principle of Mathematical Induction

We now present a valuable tool for proving results about integers. This tool is the principle of mathematical induction .

**Theorem 1.** ***The First Principle of Mathematical Induction:*** *If a set of positive integers has the property that, if it contains the integer $k$, then it also contains $k + 1$, and if this set contains 1 then it must be the set of all positive integers. More generally, a property concerning the positive integers that is true for $n = 1$, and that is true for the integer $n + 1$ whenever it is true for the integer $n$, must be true for all positive integers.*

We use the well ordering principle to prove the first principle of mathematical induction

*Proof.* Let $S$ be the set of positive integers containing the integer 1, and the integer $k + 1$ whenever it contains $k$. Assume also that $S$ is not the set of all positive integers. As a result, there are some integers that are not contained in $S$ and thus those integers must have a least element $\alpha$ by the well ordering principle. Notice that $\alpha \neq 1$ since $1 \in S$. But $\alpha - 1 \in S$ and thus using the property of $S$, $\alpha \in S$. Thus $S$ must contain all positive integers. □

We now present some examples in which we use the principle of induction.

**Example 1.** *Use mathematical induction to show that* $\forall n \in \mathbb{N}$

$$\sum_{j=1}^{n} j = \frac{n(n+1)}{2}. \tag{1.5}$$

First note that

$$\sum_{j=1}^{1} j = 1 = \frac{1 \cdot 2}{2}$$

and thus the the statement is true for $n = 1$. For the remaining inductive step, suppose that the formula holds for $n$, that is $\sum_{j=1}^{n} j = \frac{n(n+1)}{2}$. We show that

$$\sum_{j=1}^{n+1} j = \frac{(n+1)(n+2)}{2}.$$

to complete the proof by induction. Indeed

$$\sum_{j=1}^{n+1} j = \sum_{j=1}^{n} j + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{(n+1)(n+2)}{2},$$

and the result follows.

**Example 2.** *Use mathematical induction to prove that $n! \leq n^n$ for all positive integers $n$.*

Note that $1! = 1 \leq 1^1 = 1$. We now present the inductive step. Suppose that

$$n! \leq n^n$$

for some $n$, we prove that $(n+1)! \leq (n+1)^{n+1}$. Note that

$$(n+1)! = (n+1)n! \leq (n+1).n^n < (n+1)(n+1)^n = (n+1)^{n+1}.$$

This completes the proof.

**Theorem 2.** ***The Second Principle of Mathematical Induction:*** *A set of positive integers that has the property that for every integer $k$, if it contains all the integers 1 through $k$ then it contains $k+1$ and if it contains 1 then it must be the set of all positive integers. More generally, a property concerning the positive integers that is true for $n = 1$, and that is true for all integers up to $n+1$ whenever it is true for all integers up to $n$, must be true for all positive integers.*

The second principle of induction is also known as **the principle of strong induction**. Also, the first principle of induction is known as **the principle of weak induction**.

To prove the second principle of induction, we use the first principle of induction.

*Proof.* Let $T$ be a set of integers containing 1 and such that for every positive integer $k$, if it contains $1, 2, ..., k$, then it contains $k + 1$. Let $S$ be the set of all positive integers $k$ such that all the positive integers less than or equal to $k$ are in $T$. Then 1 is in $S$, and we also see that $k + 1$ is in $S$. Thus $S$ must be the set of all positive integers. Thus $T$ must be the set of all positive integers since $S$ is a subset of $T$. □

**Exercises**

1. Prove using mathematical induction that $n < 3^n$ for all positive integers $n$.

2. Show that $\sum_{j=1}^{n} j^2 = \frac{n(n+1)(2n+1)}{6}$.

3. Use mathematical induction to prove that $\sum_{j=1}^{n}(-1)^{j-1}j^2 = (-1)^{n-1}n(n+1)/2$.

4. Use mathematical induction to prove that $\sum_{j=1}^{n} j^3 = [n(n+1)/2]^2$ for every positive integer $n$.

5. Use mathematical induction to prove that $\sum_{j=1}^{n}(2j - 1) = n^2$

6. Use mathematical induction to prove that $2^n < n!$ for $n \geq 4$.

7. Use mathematical induction to prove that $n^2 < n!$ for $n \geq 4$.

## 1.3 Divisibility and the Division Algorithm

We now discuss the concept of divisibility and its properties.

### 1.3.1 Integer Divisibility

**Definition 1.** *If $a$ and $b$ are integers such that $a \neq 0$, then we say "$a$ divides $b$" if there exists an integer $k$ such that $b = ka$.*

If $a$ divides $b$, we also say "$a$ is a factor of $b$" or "$b$ is a multiple of $a$" and we write $a \mid b$. If $a$ doesn't divide $b$, we write $a \nmid b$. For example $2 \mid 4$ and $7 \mid 63$, while $5 \nmid 26$.

**Example 3.** *a) Note that any even integer has the form $2k$ for some integer $k$, while any odd integer has the form $2k + 1$ for some integer $k$. Thus $2|n$ if $n$ is even, while $2 \nmid n$ if $n$ is odd.*
*b) $\forall a \in \mathbb{Z}$ one has that $a \mid 0$.*
*c) If $b \in \mathbb{Z}$ is such that $|b| < a$, and $b \neq 0$, then $a \nmid b$.*

**Theorem 3.** *If $a, b$ and $c$ are integers such that $a \mid b$ and $b \mid c$, then $a \mid c$.*

*Proof.* Since $a \mid b$ and $b \mid c$, then there exist integers $k_1$ and $k_2$ such that $b = k_1 a$ and $c = k_2 b$. As a result, we have $c = k_1 k_2 a$ and hence $a \mid c$. □

**Example 4.** *Since* $6 \mid 18$ *and* $18 \mid 36$*, then* $6 \mid 36$.

The following theorem states that if an integer divides two other integers then it divides any linear combination of these integers.

**Theorem 4.** *If $a, b, c, m$ and $n$ are integers, and if $c \mid a$ and $c \mid b$, then $c \mid (ma + nb)$.*

*Proof.* Since $c \mid a$ and $c \mid b$, then by definition there exists $k_1$ and $k_2$ such that $a = k_1 c$ and $b = k_2 c$. Thus

$$ma + nb = mk_1 c + nk_2 c = c(mk_1 + nk_2),$$

and hence $c \mid (ma + nb)$. □

Theorem 4 can be generalized to any finite linear combination as follows. If

$$a \mid b_1, a \mid b_2, ..., a \mid b_n$$

then

$$a \mid \sum_{j=1}^{n} k_j b_j \tag{1.6}$$

for any set of integers $k_1, \cdots, k_n \in \mathbb{Z}$. It would be a nice exercise to prove the generalization by induction.

### 1.3.2 The Division Algorithm

The following theorem states somewhat an elementary but very useful result.

**Theorem 5.** ***The Division Algorithm*** *If $a$ and $b$ are integers such that $b > 0$, then there exist unique integers $q$ and $r$ such that $a = bq + r$ where $0 \leq r < b$.*

*Proof.* Consider the set $A = \{a - bk \geq 0 \mid k \in \mathbb{Z}\}$. Note that $A$ is nonempty since for $k < a/b$, $a - bk > 0$. By the well ordering principle, $A$ has a least element $r = a - bq$ for some $q$. Notice that $r \geq 0$ by construction. Now if $r \geq b$ then (since $b > 0$)

$$r > r - b = a - bq - b = a - b(q + 1) =\geq 0.$$

This leads to a contradiction since $r$ is assumed to be the least positive integer of the form $r = a - bq$. As a result we have $0 \leq r < b$.

We will show that $q$ and $r$ are unique. Suppose that $a = bq_1 + r_1$ and $a = bq_2 + r_2$ with $0 \leq r_1 < b$ and $0 \leq r_2 < b$. Then we have

$$b(q_1 - q_2) + (r_1 - r_2) = 0.$$

As a result we have

$$b(q_1 - q_2) = r_2 - r_1.$$

Thus we get that

$$b \mid (r_2 - r_1).$$

And since $-\max(r_1, r_2) \leq |r_2 - r_1| \leq \max(r_1, r_2)$, and $b > \max(r_1, r_2)$, then $r_2 - r_1$ must be $0$, i.e. $r_2 = r_1$. And since $bq_1 + r_1 = bq_2 + r_2$, we also get that $q_1 = q_2$. This proves uniqueness. □

**Example 5.** *If* $a = 71$ *and* $b = 6$*, then* $71 = 6 \cdot 11 + 5$*. Here* $q = 11$ *and* $r = 5$*.*

### Exercises

1. Show that $5 \mid 25, 19 \mid 38$ and $2 \mid 98$.

2. Use the division algorithm to find the quotient and the remainder when 76 is divided by 13.

3. Use the division algorithm to find the quotient and the remainder when -100 is divided by 13.

4. Show that if $a, b, c$ and $d$ are integers with $a$ and $c$ nonzero, such that $a \mid b$ and $c \mid d$, then $ac \mid bd$.

5. Show that if $a$ and $b$ are positive integers and $a \mid b$, then $a \leq b$.

6. Prove that the sum of two even integers is even, the sum of two odd integers is even and the sum of an even integer and an odd integer is odd.

7. Show that the product of two even integers is even, the product of two odd integers is odd and the product of an even integer and an odd integer is even.

8. Show that if $m$ is an integer then 3 divides $m^3 - m$.

9. Show that the square of every odd integer is of the form $8m + 1$.

10. Show that the square of any integer is of the form $3m$ or $3m + 1$ but not of the form $3m + 2$.

11. Show that if $ac \mid bc$, then $a \mid b$.

12. Show that if $a \mid b$ and $b \mid a$ then $a = \pm b$.

## 1.4 Representations of Integers in Different Bases

In this section, we show how any positive integer can be written in terms of any positive base integer expansion in a unique way. Normally we use decimal notation to represent integers, we will show how to convert an integer from decimal notation into any other positive base integer notation and vise versa. Using the decimal notation in daily life is simply better because we have ten fingers which facilitates all the mathematical operations.

**Notation** An integer $a$ written in base $b$ expansion is denoted by $(a)_b$.

**Theorem 6.** *Let $b$ be a positive integer with $b > 1$. Then any positive integer $m$ can be written uniquely as*

$$m = a_l b^l + a_{l-1} b^{l-1} + ... + a_1 b + a_0,$$

*where $l$ is a positive integer, $0 \leq a_j < b$ for $j = 0, 1, ..., l$ and $a_l \neq 0$.*

*Proof.* We start by dividing $m$ by $b$ and we get

$$m = bq_0 + a_0, \quad 0 \leq a_0 < b.$$

If $q_0 \neq 0$ then we continue to divide $q_0$ by $b$ and we get

$$q_0 = bq_1 + a_1, \quad 0 \leq a_1 < b.$$

We continue this process and hence we get

$$\begin{aligned} q_1 &= bq_2 + a_2, \quad 0 \leq a_2 < b, \\ &. \\ &. \\ &. \\ q_{l-2} &= bq_{l-1} + a_{l-1}, \quad 0 \leq a_{l-1} < b, \\ q_{l-1} &= b \cdot 0 + a_l, \quad 0 \leq a_l < b. \end{aligned}$$

Note that the sequence $q_0, q_1, ...$ is a decreasing sequence of positive integers with a last term $q_l$ that must be 0.

Now substituting the equation $q_0 = bq_1 + a_1$ in $m = bq_0 + a_0$, we get

$$m = b(bq_1 + a_1) + a_0 = b^2 q_1 + a_1 b + a_0,$$

Successively substituting the equations in $m$, we get

$$\begin{aligned} m &= b^3 q_2 + a_2 b^2 + a_1 b + a_0, \\ &. \\ &. \\ &. \\ &= b^l q_{l-1} + a_{l-1} b^{l-1} + ... + a_1 b + a_0, \\ &= a_l b^l + a_{l-1} b^{l-1} + ... + a_1 b + a_0. \end{aligned}$$

What remains to prove is that the representation is unique. Suppose now that

$$m = a_l b^l + a_{l-1} b^{l-1} + ... + a_1 b + a_0 = c_l b^l + c_{l-1} b^{l-1} + ... + c_1 b + c_0$$

where if the number of terms is different in one expansion, we add zero coefficients to make the number of terms agree. Subtracting the two expansions, we get

$$(a_l - c_l) b^l + (a_{l-1} - c_{l-1}) b^{l-1} + ... + (a_1 - c_1) b + (a_0 - c_0) = 0.$$

If the two expansions are different, then there exists $0 \leq j \leq l$ such that $c_j \neq a_j$. As a result, we get

$$b^j((a_l - c_l)b^{l-j} + ... + (a_{j+1} - c_{j+1})b + (a_j - c_j)) = 0$$

and since $b \neq 0$, we get

$$(a_l - c_l)b^{l-j} + ... + (a_{j+1} - c_{j+1})b + (a_j - c_j) = 0.$$

We now get

$$a_j - c_j = (a_l - c_l)b^{l-j} + ... + (a_{j+1} - c_{j+1})b,$$

and as a result, $b \mid (a_j - c_j)$. Since $0 \leq a_j < b$ and $0 \leq c_j < b$, we get that $a_j = c_j$. This is a contradiction and hence the expansion is unique. □

Note that base 2 representation of integers is called binary representation. Binary representation plays a crucial role in computers. Arithmetic operations can be carried out on integers with any positive integer base but it will not be addressed in this book. We now present examples of how to convert from decimal integer representation to any other base representation and vise versa.

**Example 6.** *To find the expansion of 214 base 3:*

we do the following

$$\begin{aligned} 214 &= 3 \cdot 71 + 1 \\ 71 &= 3 \cdot 23 + 2 \\ 23 &= 3 \cdot 7 + 2 \\ 7 &= 3 \cdot 2 + 1 \\ 2 &= 3 \cdot 0 + 2 \end{aligned}$$

As a result, to obtain a base 3 expansion of 214, we take the remainders of divisions and we get that $(214)_{10} = (21221)_3$.

**Example 7.** *To find the base 10 expansion, i.e. the decimal expansion, of* $(364)_7$*:*

We do the following: $4 \cdot 7^0 + 6 \cdot 7^1 + 3 \cdot 7^2 = 4 + 42 + 147 = 193$.

In some cases where base $b > 10$ expansion is needed, we add some characters to represent numbers greater than 9. It is known to use the alphabetic letters to denote integers greater than 9 in base b expansion for $b > 10$. For example $(46BC29)_{13}$ where $A = 10, B = 11, C = 12$.

To convert from one base to the other, the simplest way is to go through base 10 and then convert to the other base. There are methods that simplify conversion from one base to the other but it will not be addressed in this book.

**Exercises**

1. Convert $(7482)_{10}$ to base 6 notation.

2. Convert $(98156)_{10}$ to base 8 notation.

3. Convert $(101011101)_2$ to decimal notation.

4. Convert $(AB6C7D)_{16}$ to decimal notation.

5. Convert $(9A0B)_{16}$ to binary notation.

## 1.5 The Greatest Common Divisor

In this section we define the greatest common divisor (gcd) of two integers and discuss its properties. We also prove that the greatest common divisor of two integers is a linear combination of these integers.

Two integers $a$ and $b$, not both $0$, can have only finitely many divisors, and thus can have only finitely many common divisors. In this section, we are interested in the greatest common divisor of $a$ and $b$. Note that the divisors of $a$ and that of $\mid a \mid$ are the same.

**Definition 2.** *The greatest common divisor of two integers $a$ and $b$ is the greatest integer that divides both $a$ and $b$.*

We denote the greatest common divisor of two integers $a$ and $b$ by $(a, b)$. We also define $(0, 0) = 0$.

**Example 8.** *Note that the greatest common divisor of 24 and 18 is 6. In other words* $(24, 18) = 6$.

There are couples of integers (e.g. 3 and 4, etc...) whose greatest common divisor is 1 so we call such integers relatively prime integers.

**Definition 3.** *Two integers $a$ and $b$ are relatively prime if $(a, b) = 1$.*

**Example 9.** *The greatest common divisor of 9 and 16 is 1, thus they are relatively prime.*

Note that every integer has positive and negative divisors. If $a$ is a positive divisor of $m$, then $-a$ is also a divisor of $m$. Therefore by our definition of the greatest common divisor, we can see that $(a, b) = (\mid a \mid, \mid b \mid)$.

We now present a theorem about the greatest common divisor of two integers. The theorem states that if we divide two integers by their greatest common divisor, then the outcome is a couple of integers that are relatively prime.

**Theorem 7.** *If $(a, b) = d$ then $(a/d, b/d) = 1$.*

*Proof.* We will show that $a/d$ and $b/d$ have no common positive divisors other than 1. Assume that $k$ is a positive common divisor such that $k \mid a/d$ and $k \mid b/d$. As a result, there are two positive integers $m$ and $n$ such that

$$a/d = km \quad \text{and} \quad b/d = kn$$

Thus we get that

$$a = kmd \quad \text{and} \quad b = knd.$$

Hence $kd$ is a common divisor of both $a$ and $b$. Also, $kd \geq d$. However, $d$ is the greatest common divisor of $a$ and $b$. As a result, we get that $k = 1$. □

The next theorem shows that the greatest common divisor of two integers does not change when we add a multiple of one of the two integers to the other.

**Theorem 8.** *Let $a, b$ and $c$ be integers. Then $(a, b) = (a + cb, b)$.*

*Proof.* We will show that every divisor of $a$ and $b$ is also a divisor of $a + cb$ and $b$ and vise versa. Hence they have exactly the same divisors. So we get that the greatest common divisor of $a$ and $b$ will also be the greatest common divisor of $a + cb$ and $b$. Let $k$ be a common divisor of $a$ and $b$. By Theorem 4, $k \mid (a + cb)$ and hence $k$ is a divisor of $a+cb$. Now assume that $l$ is a common divisor of $a+cb$ and $b$. Also by Theorem 4 we have ,

$$l \mid ((a + cb) - cb) = a.$$

As a result, $l$ is a common divisor of $a$ and $b$ and the result follows. □

**Example 10.** *Notice that $(4, 14) = (4, 14 - 3 \cdot 4) = (4, 2) = 2$.*

We now present a theorem which proves that the greatest common divisor of two integers can be written as a linear combination of the two integers.

**Theorem 9.** *The greatest common divisor of two integers $a$ and $b$, not both $0$ is the least positive integer such that $ma + nb = d$ for some integers $m$ and $n$.*

*Proof.* Assume without loss of generality that $a$ and $b$ are positive integers. Consider the set of all positive integer linear combinations of $a$ and $b$. This set is non empty since $a = 1 \cdot a + 0 \cdot b$ and $b = 0 \cdot a + 1 \cdot b$ are both in this set. Thus this set has a least element $d$ by the well-ordering principle. Thus $d = ma + nb$ for some integers $m$ and $n$. We have to prove that $d$ divides both $a$ and $b$ and that it is the greatest divisor of $a$ and $b$.

By the division algorithm, we have

$$a = dq + r, \quad 0 \leq r < d.$$

Thus we have

$$r = a - dq = a - q(ma + nb) = (1 - qm)a - qnb.$$

We then have that $r$ is a linear combination of $a$ and $b$. Since $0 \leq r < d$ and $d$ is the least positive integer which is a linear combination of $a$ and $b$, then $r = 0$ and $a = dq$. Hence $d \mid a$. Similarly $d \mid b$. Now notice that if there is a divisor $c$ that divides both $a$ and $b$. Then $c$ divides any linear combination of $a$ and $b$ by Theorem 4. Hence $c \mid d$. This proves that any common divisor of $a$ and $b$ divides $d$. Hence $c \leq d$, and $d$ is the greatest divisor. □

As a result, we conclude that if $(a, b) = 1$ then there exist integers $m$ and $n$ such that $ma + nb = 1$.

**Definition 4.** *Let $a_1, a_2, ..., a_n$ be integers, not all $0$. The greatest common divisor of these integers is the largest integer that divides all of the integers in the set. The greatest common divisor of $a_1, a_2, ..., a_n$ is denoted by $(a_1, a_2, ..., a_n)$.*

**Definition 5.** *The integers $a_1, a_2, ..., a_n$ are said to be mutually relatively prime if $(a_1, a_2, ..., a_n) = 1$.*

**Example 11.** *The integers $3, 6, 7$ are mutually relatively prime since $(3, 6, 7) = 1$ although $(3, 6) = 3$.*

**Definition 6.** *The integers $a_1, a_2, ..., a_n$ are called pairwise prime if for each $i \neq j$, we have $(a_i, a_j) = 1$.*

**Example 12.** *The integers $3, 14, 25$ are pairwise relatively prime. Notice also that these integers are mutually relatively prime.*

Notice that if $a_1, a_2, ..., a_n$ are pairwise relatively prime then they are mutually relatively prime.

**Exercises**

1. Find the greatest common divisor of 15 and 35.

2. Find the greatest common divisor of 100 and 104.

3. Find the greatest common divisor of -30 and 95.

4. Let $m$ be a positive integer. Find the greatest common divisor of $m$ and $m+1$.

5. Let $m$ be a positive integer, find the greatest common divisor of $m$ and $m+2$.

6. Show that if $m$ and $n$ are integers such that $(m,n)=1$, then (m+n,m-n)=1 or 2.

7. Show that if $m$ is a positive integer, then $3m+2$ and $5m+3$ are relatively prime.

8. Show that if $a$ and $b$ are relatively prime integers, then $(a+2b,2a+b)=1$or 3.

9. Show that if $a_1, a_2, ..., a_n$ are integers that are not all 0 and $c$ is a positive integer, then $(ca_1, ca_2, ..., ca_n) = c(a_1, a_2, ...a_n)$.

## 1.6 The Euclidean Algorithm

In this section we describe a systematic method that determines the greatest common divisor of two integers. This method is called the Euclidean algorithm.

**Lemma 1.** *If $a$ and $b$ are two integers and $a = bq + r$ where also $q$ and $r$ are integers, then $(a, b) = (r, b)$.*

*Proof.* Note that by theorem 8, we have $(bq + r, b) = (b, r)$. □

The above lemma will lead to a more general version of it. We now present the Euclidean algorithm in its general form. It states that the greatest common divisor of two integers is the last non zero remainder of the successive division.

**Theorem 10.** *Let $a = r_0$ and $b = r_1$ be two positive integers where $a \geq b$. If we apply the division algorithm successively to obtain that*

$$r_j = r_{j+1}q_{j+1} + r_{j+2} \text{ where } 0 \leq r_{j+2} < r_{j+1}$$

*for all $j = 0, 1, ..., n - 2$ and*

$$r_{n+1} = 0.$$

*Then $(a, b) = r_n$.*

*Proof.* By applying the division algorithm, we see that

$$\begin{array}{rcll} r_0 & = & r_1q_1 + r_2 & 0 \leq r_2 < r_1, \\ r_1 & = & r_2q_2 + r_3 & 0 \leq r_3 < r_2, \\ & . & & \\ & . & & \\ & . & & \\ r_{n-2} & = & r_{n-1}q_{n-1} + r_n & 0 \leq r_n < r_{n-1}, \\ r_{n-1} & = & r_nq_n. & \end{array}$$

Notice that, we will have a remainder of $0$ eventually since all the remainders are integers and every remainder in the next step is less than the remainder in the previous one. By Lemma 1, we see that

$$(a, b) = (b, r_2) = (r_2, r_3) = ... = (r_n, 0) = r_n.$$

□

**Example 13.** *We will find the greatest common divisor of* $4147$ *and* $10672$*. Note that*

$$\begin{aligned}
10672 &= 4147 \cdot 2 + 2378, \\
4147 &= 2378 \cdot 1 + 1769, \\
2378 &= 1769 \cdot 1 + 609, \\
1769 &= 609 \cdot 2 + 551, \\
609 &= 551 \cdot 1 + 58, \\
551 &= 58 \cdot 9 + 29, \\
58 &= 29 \cdot 2,
\end{aligned}$$

*Hence* $(4147, 10672) = 29.$

We now use the steps in the Euclidean algorithm to write the greatest common divisor of two integers as a linear combination of the two integers. The following example will actually determine the variables $m$ and $n$ described in Theorem 9. The following algorithm can be described by a general form but for the sake of simplicity of expressions we will present an example that shows the steps for obtaining the greatest common divisor of two integers as a linear combination of the two integers.

**Example 14.** *Express 29 as a linear combination of* $4147$ *and* $10672$.

$$\begin{aligned}
29 &= 551 - 9 \cdot 58, \\
&= 551 - 9(609 - 551 \cdot 1), \\
&= 10.551 - 9.609, \\
&= 10 \cdot (1769 - 609 \cdot 2) - 9 \cdot 609, \\
&= 10 \cdot 1769 - 29 \cdot 609, \\
&= 10 \cdot 1769 - 29(2378 - 1769 \cdot 1), \\
&= 39 \cdot 1769 - 29 \cdot 2378, \\
&= 39(4147 - 2378 \cdot 1) - 29 \cdot 2378, \\
&= 39 \cdot 4147 - 68 \cdot 2378, \\
&= 39 \cdot 4147 - 68(10672 - 4147 \cdot 2), \\
&= 175 \cdot 4147 - 68 \cdot 10672,
\end{aligned}$$

*As a result, we see that* $29 = 175 \cdot 4147 - 68 \cdot 10672$.

This property is called **Bezout's Identity**:

For any two integers $a$ and $b$, we can always find integers $m$ and $n$ such that $\gcd(a, b) = am + bn$.

We can always find this expression by reversing the results of the Euclidean algorithm.

**Exercises**

1. Use the Euclidean algorithm to find the greatest common divisor of 412 and 32 and express it in terms of the two integers.

2. Use the Euclidean algorithm to find the greatest common divisor of 780 and 150 and express it in terms of the two integers.

3. Find the greatest common divisor of $70, 98, 108$.

4. Let $a$ and $b$ be two positive even integers. Prove that $(a, b) = 2(a/2, b/2)$.

5. Show that if $a$ and $b$ are positive integers where $a$ is even and $b$ is odd, then $(a, b) = (a/2, b)$.

## 1.7 Lame's Theorem and Binet's Formula

In this section, we give an estimate to the number of steps needed to find the greatest common divisor of two integers using the Euclidean algorithm. To do this, we have to introduce the Fibonacci numbers for the sake of proving a lemma that gives an estimate on the growth of Fibonacci numbers in the Fibonacci sequence. The lemma that we prove will be used in the proof of Lame's theorem. We then turn to illustrate an unexpected property of the Fibonacci sequence, called Binet's Formula.

### 1.7.1 Lame's Theorem

**Definition 7.** *The Fibonacci sequence is defined recursively by* $f_1 = 1$, $f_2 = 1$, *and*

$$f_n = f_{n-1} + f_{n-2} \quad \textit{for} \quad n \geq 3.$$

*The terms in the sequence are called Fibonacci numbers.*

In the following lemma, we give a lower bound on the growth of Fibonacci numbers. We will show that Fibonacci numbers grow faster than a geometric series with common ratio $\alpha = (1 + \sqrt{5})/2$.

**Lemma 2.** *For* $n \geq 3$*, we have* $f_n > \alpha^{n-2}$ *where* $\alpha = (1 + \sqrt{5})/2$.

*Proof.* We use the second principle of mathematical induction to prove our result. It is easy to see that this is true for $n = 3$ and $n = 4$. Assume that $\alpha^{k-2} < f_k$

for all integers $k$ where $k \leq n$. Now since $\alpha$ is a solution of the polynomial $x^2 - x - 1 = 0$, we have $\alpha^2 = \alpha + 1$. Hence

$$\alpha^{n-1} = \alpha^2.\alpha^{n-3} = (\alpha + 1).\alpha^{n-3} = \alpha^{n-2} + \alpha^{n-3}.$$

By the inductive hypothesis, we have

$$\alpha^{n-2} < f_n, \quad \alpha^{n-3} < f_{n-1}.$$

After adding the two inequalities, we get

$$\alpha^{n-1} < f_n + f_{n-1} = f_{n+1}.$$

□

We now present Lame's theorem.

**Theorem 11.** *using the Euclidean algorithm to find the greatest common divisor of two positive integers has number of divisions less than or equal five times the number of decimal digits in the minimum of the two integers.*

*Proof.* Let $a$ and $b$ be two positive integers where $a > b$. Applying the Euclidean algorithm to find the greatest common divisor of two integers with $a = r_0$ and $b = r_1$, we get

$$\begin{array}{rcll} r_0 & = & r_1 q_1 + r_2 & 0 \leq r_2 < r_1, \\ r_1 & = & r_2 q_2 + r_3 & 0 \leq r_3 < r_2, \\ & . & & \\ & . & & \\ & . & & \\ r_{n-2} & = & r_{n-1} q_{n-1} + r_n & 0 \leq r_n < r_{n-1}, \\ r_{n-1} & = & r_n q_n. & \end{array}$$

Notice that each of the quotients $q_1, q_2, ..., q_{n-1}$ are all greater than 1 and $q_n \geq 2$ and this is because $r_n < r_{n-1}$. Thus we have

$$\begin{aligned}
r_n &\geq 1 = f_2, \\
r_{n-1} &\geq 2r_n \geq 2f_2 = f_3, \\
r_{n-2} &\geq r_{n-1} + r_n \geq f_3 + f_2 = f_4, \\
r_{n-3} &\geq r_{n-2} + r_{n-1} \geq f_4 + f_3 = f_5, \\
&. \\
&. \\
&. \\
r_2 &\geq r_3 + r_4 \geq f_{n-1} + f_{n-2} = f_n, \\
b &= r_1 \geq r_2 + r_3 \geq f_n + f_{n-1} = f_{n+1}.
\end{aligned}$$

Thus notice that $b \geq f_{n+1}$. By Lemma 2, we have $f_{n+1} > \alpha^{n-1}$ for $n > 2$. As a result, we have $b > \alpha^{n-1}$. Now notice since

$$\log_{10} \alpha > \frac{1}{5},$$

we see that

$$\log_{10} b > (n-1)/5.$$

Thus we have

$$n - 1 < 5 \log_{10} b.$$

Now let $b$ has $k$ decimal digits. As a result, we have $b < 10^k$ and thus $\log_{10} b < k$. Hence we conclude that $n - 1 < 5k$. Since $k$ is an integer, we conclude that $n \leq 5k$. □

### 1.7.2 Binet's Formula

The Fibonacci sequence is an example of a **linear recurrence relation**, where one number of a sequence depends on a linear combination of earlier numbers in the sequence. An elegant technique gives us a concise formula for such relations, and we illusrate this using the Fibonacci sequence.

In general, $f_n = f_{n-1} + f_{n-2}$, and of course $f_{n-1} = f_{n-1}$, giving us the matrix equation

$$\begin{pmatrix} f_n \\ f_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} f_{n-1} \\ f_{n-2} \end{pmatrix}.$$

Let's give this $2 \times 2$ matrix a special name,

$$F = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

As usual, matrices carry more information than you might expect at first glance, and the characteristic polynomial of this one has very interesting roots:

$$\begin{aligned} 0 &= \det \begin{pmatrix} 1-\lambda & 1 \\ 1 & -\lambda \end{pmatrix} \\ &= -\lambda(1-\lambda) - 1 \\ &= \lambda^2 - \lambda - 1 \\ &\Downarrow \\ \lambda &= \frac{-(-1) \pm \sqrt{(-1)^2 - 4 \cdot 1 \cdot (-1)}}{2 \cdot 1} = \frac{1 \pm \sqrt{5}}{2}. \end{aligned}$$

These results have several wonderful aspects. For instance, $(1+\sqrt{5})/2$

- is well-known as "the Golden Ratio", and
- appeared in Lemma 2 above, in connection with Lame's theorem.

There is more! The whole point of any eigenvalue $\lambda$ of $F$ is that, for any eigenvector $\mathbf{e}$,

$$F\mathbf{e} = \lambda\mathbf{e} \qquad \Longrightarrow \qquad F\left(e_2\ e_1\right)^{\mathrm{T}} = \left(\lambda e_2\ \lambda e_1\right)^{\mathrm{T}}.$$

The eigenvectors are a basis for the eigenspace, so any solution to $F\mathbf{x} = \lambda\mathbf{x}$ has the form $\mathbf{x} = c_1\mathbf{e}_1 + c_1\mathbf{e}_2$, where $c_1$ and $c_2$ are arbitrary constants, while $\mathbf{e}_1$ and $\mathbf{e}_2$ are the eigenvectors corresponding to $(1+\sqrt{5})/2$ and $(1-\sqrt{5})/2$, respectively.

So, what are these eigenvectors? We know that $F\mathbf{e} = \lambda\mathbf{e}$ for corresponding $\lambda$ and $\mathbf{e}$; setting $e_i = 1$ and solving gives us

$$e_1 = \begin{pmatrix} 1 \\ -\frac{1-\sqrt{5}}{2} \end{pmatrix} \qquad \text{and} \qquad \mathbf{e}_2 = \begin{pmatrix} 1 \\ -\frac{1+\sqrt{5}}{2} \end{pmatrix}.$$

In addition, we can compute $f_n$ simply by applying $F$ to the matrix $(f_1\ f_0)^{\mathrm{T}}$:

$$\begin{pmatrix} f_n \\ f_{n-1} \end{pmatrix} = F \begin{pmatrix} f_{n-1} \\ f_{n-2} \end{pmatrix} = F \left[ F \begin{pmatrix} f_{n-2} \\ f_{n-3} \end{pmatrix} \right] = \cdots = F^{n-2} \begin{pmatrix} f_2 \\ f_1 \end{pmatrix}. \tag{1.7}$$

From linear algebra, we know that we can rewrite $F$ as $Q\Lambda Q^{-1}$, where

$$Q = \begin{pmatrix} 1 & 1 \\ -\frac{1-\sqrt{5}}{2} & -\frac{1+\sqrt{5}}{2} \end{pmatrix} \quad \text{and} \quad \Lambda = \begin{pmatrix} \frac{1+\sqrt{5}}{2} & 0 \\ 0 & \frac{1-\sqrt{5}}{2} \end{pmatrix}.$$

(Notice that the columns of $Q$ are the eigenvectors that correspond to the diagonal elements of $\Lambda$, the eigenvalues.) By substitution,

$$F^n = (Q\Lambda Q^{-1})^n = \underbrace{(Q\Lambda Q^{-1})(Q\Lambda Q^{-1}) \cdots (Q\Lambda Q^{-1})}_{n \text{ times}} = Q\Lambda^n Q^{-1}.$$

Combine this with the relationship in (1.7), and we have the relationship

$$\mathbf{f}_n = \begin{pmatrix} 1 & 1 \\ -\frac{1-\sqrt{5}}{2} & -\frac{1+\sqrt{5}}{2} \end{pmatrix} \begin{pmatrix} \frac{1+\sqrt{5}}{2} & 0 \\ 0 & \frac{1-\sqrt{5}}{2} \end{pmatrix}^{n-2} \begin{pmatrix} \frac{1+\sqrt{5}}{2\sqrt{5}} & \frac{1}{\sqrt{5}} \\ -\frac{1-\sqrt{5}}{2\sqrt{5}} & -\frac{1}{\sqrt{5}} \end{pmatrix} \mathbf{f}_2$$

where $\mathbf{f}_n = (f_n\ f_{n-1})^{\mathrm{T}}$ and $\mathbf{f}_2 = (f_2\ f_1)^{\mathrm{T}} = (1\ 1)^{\mathrm{T}}$. The first row of the simplified product yields a "closed" form relationship between $f_n$, $f_1$, and $f_2$,

$$\begin{aligned} f_n = {} & \frac{1}{\sqrt{5}} \left( \frac{1+\sqrt{5}}{2} \right)^{n-1} - \frac{1}{\sqrt{5}} \left( \frac{1-\sqrt{5}}{2} \right)^{n-1} \\ & + \frac{1}{\sqrt{5}} \left( \frac{1+\sqrt{5}}{2} \right)^{n-2} - \frac{1}{\sqrt{5}} \left( \frac{1-\sqrt{5}}{2} \right)^{n-2}. \end{aligned}$$

With a gentle algebraic massage, this equation simplifies to an elegant form.

**Theorem 12** (Binet's Formula)**.** *The $n$th Fibonacci number has the form*

$$f_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right].$$

This same technique works with *any* linear recurrence!

**Exercises**

1. If $f_i$ is the $i$th Fibonacci number, show that $f_1 + f_2 + \ldots + f_n = 2f_{n+2} - 1$.

2. What happens when you add the squares of consecutive Fibonacci numbers? That is, find a pattern to the sequence $1^2 + 1^2$, $1^2 + 2^2$, $2^2 + 3^2$, $3^2 + 5^2, \ldots$. Prove the property you find by induction. (One way to solve this requires proving two claims simultaneously, by induction.)

3. Find an upper bound for the number of steps in the Euclidean algorithm that is used to find the greatest common divisor of 38472 and 957748838.

4. Find an upper bound for the number of steps in the Euclidean algorithm that is used to find the greatest common divisor of 15 and 75. Verify your result by using the Euclidean algorithm to find the greatest common divisor of the two integers.

5. Using a computational aid, test Binet's formula for some large values of $n$.

6. Complete the proof of Binet's formula by filling in the "bit of algebra". *Hint:* Notice the change in exponents!

7. The **Lucas sequence** is defined by $L_1 = 2$, $L_2 = 1$, and $L_n = L_{n-1} + L_{n-2}$.

   (a) Use the formula to find $L_3$, $L_4$, $L_5$ and $L_6$.

   (b) Show that $L_n = f_{n-1} + f_{n+1}$ and $L_n = f_n + 2f_{n-1}$.

   (c) Use the same technique that we used in Binet's formula to find a closed-form expression for $L_n$.

# Chapter 2

# Prime Numbers

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.

## 2.1 The Sieve of Eratosthenes

**Definition 8.** *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 3.** *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 13.** *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 3, $a$ 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.

### 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 $\sqrt{n}$

### 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 $(a^{kl} - 1) = (a^k - 1)(a^{k(l-1)} + a^{k(l-2)} + ... + a^k + 1)$.

## 2.2 Alternate definition of prime number

The definition of a prime number given above uses a *divisibility* criterion, sometimes called *irreducibility*. We can also define a prime number using a *division* criterion, sometimes called "Euclid's criterion."

**Definition 9.** *Let $p$ be a positive integer, greater than 1. We say that $p$ is **prime** if, whenever $p$ divides the product of two integers $a$ and $b$, it also divides at least one of $a$ or $b$.*

Definition 9 might not appeal to you: why would someone want to define primality this way? To see why this definition is useful, consider the following examples.

**Example 16.** *For instance, 6 divides the product $2 \cdot 3$, but 6 divides neither 2 nor 3. Hence, 6 is not prime.*

*That example might not inspire you so much, so try this one on for size. We know that 5 is prime. Suppose 5 divides the product of 2 and an integer $m$; since 5 is prime and it does not divide 2, it must divide $m$.*

Definition 9 also has advantages when we apply the notion of a prime number to other sets; we will look at that later. For now, though, we have to ask ourselves: are Definitions 8 and 9 equivalent? After all, they say different things, so there is a possibility that they classify different numbers as prime. That would cause problems!

In fact, the two definitions *are* equivalent. To see this, let $p$, $a$, and $b$ be positive integers.

Assume first that $p$ is irreducible; that is, whenever it factors as $ab$, either $p = a$ or $p = b$. We need to show that this implies Euclid's criterion. By way of contradiction, suppose there exist integers $a$ and $b$ such that $p$ divides $ab$, but divides neither $a$ nor $b$. Choose positive $a$ and $b$ such that this product is minimized. By Exercise 5, $p \leq ab$. We consider two cases.

- If $p = ab$, then $ab$ is a factorization of $p$. We assumed $p$ is irreducible, so $p = a$ or $p = b$. Either way, $p$ divides one of $a$ or $b$, a contradiction!

- Apparently $p < ab$ instead. Use the Division Algorithm to compute quotients $q_a$ and $q_b$, and remainders $r_a$ and $r_b$, such that $a = pq_a + r_a$ and $b = pq_b + r_b$. Since $p \leq ab$ and the remainders are less than or equal to $p$, we know that $r_a < a$ or $r_b < b$. By substitution and a little arithmetic, $ab = pQ + r_a r_b$ where $Q = pq_a q_b + q_a r_b + q_b r_a$. Recall that $p$ divides $ab$; the equation above implies that it also divides $r_a r_b$. However, $r_a r_b < ab$, and by hypothesis, $ab$ is the smallest *positive* product divisible by $p$ whose factors are not divisible by $p$. Thus, $p$ divides ones of $r_a$ or $r_b$. Both are smaller than $p$, so Exercise 5 implies that one of $r_a$ or $r_b$ is 0. This contradicts the hypothesis that $p$ divides neither $a$ nor $b$.

In both cases, we encountered a contradiction. The assumption that $p$ divides neither $a$ nor $b$ is inconsistent with the other facts, so $p$ must divide one of them.

We have shown that the irreducibility criterion implies Euclid's criterion; it remains to show the converse. Assume that $p$ satisfies Euclid's criterion; that is, whenever it divides a product of two integers, it divides one of the integers. Let $a$ and $b$ be two integers, and assume $p = ab$. We can rewrite the equation as $p \cdot 1 = ab$, which tells us that $p$ divides $ab$, with the quotient 1. Euclid's criterion kicks in here: since $p$ divides the product $ab$, it must divide one of the two factors $a$ or $b$; without loss of generality, we may suppose $p$ divides $a$. Exercise 12 tells us $p = a$.

## 2.3 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 14.** *There are infinitely many primes.*

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

$$Q = p_1 p_2 ... p_n + 1.$$

By Lemma 3, $Q$ 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 $p_1 p_2 ... p_n$ and as a result $q$ divides $Q - p_1 p_2 ... p_n$. 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 15.** *Given any positive integer $n$, there exists $n$ consecutive composite integers.*

*Proof.* Consider the sequence of integers

$$(n + 1)! + 2, (n + 1)! + 3, ..., (n + 1)! + n, (n + 1)! + n + 1$$

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. □

### 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.

## 2.4 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 17.** $99 = 3 \cdot 3 \cdot 11 = 3^2 \cdot 11, \quad 32 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^5$

### 2.4.1 The Fundamental Theorem of Arithmetic

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

**Lemma 4.** *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 5.** *If $p$ divides $n_1 n_2 n_3 ... n_k$, where p is a prime and $n_i > 0$ for all $1 \leq i \leq k$, then there is an integer $j$ with $1 \leq j \leq k$ 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 $n_1 n_2 ... n_{k+1}$ that is divisible by $p$. Notice that either

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

Now if $(p, n_1 n_2 ... n_k) = 1$ then by Lemma 4, $p \mid n_{k+1}$. Now if $p \mid n_1 n_2 ... n_k$, 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 16.** ***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

$$n = p_1p_2...p_s = q_1q_2...q_r$$

where $p_1, p_2, ...p_s, q_1, q_2, ...q_r$ are primes,

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

Cancel out all common primes from the factorizations above to get

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

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 $p_{j_1}p_{j_2}...p_{j_u}$, then $p_{j_l}$ must divide $q_{i_1}q_{i_2}...q_{i_v}$, and hence by Lemma 5, $p_{j_1}$ must divide $q_{j_k}$ for some $1 \leq k \leq v$ which is impossible. Hence the representation is unique. □

**Remark 2.** *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, $n = p_1p_2p_3...p_k$ where $p_i$ for $1 \leq i \leq k$ are not necessarily distinct. Another example would be*

$$n = p_1^{a_1}p_2^{a_2}p_3^{a_3}...p_j^{a_j} \tag{2.1}$$

*where all the $p_i$ are distinct for $1 \leq i \leq j$. One can also write a formal product*

$$n = \prod_{all\ primes\ p_i} p_i^{\alpha_i}, \tag{2.2}$$

*where all but finitely many of the $\alpha_i's$ are 0.*

**Example 18.** *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 2.*

We know describe in general how prime factorization can be used to determine the greatest common divisor of two integers. Let

$$a = p_1^{a_1} p_2^{a_2} ... p_n^{a_n} \quad \text{and} \quad b = p_1^{b_1} p_2^{b_2} ... p_n^{b_n},$$

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

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

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

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

**Lemma 6.** *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 $ab$. □

### 2.4.2 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 17.** ***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. As a result, we will present a special case of this theorem and prove that there are infinitely many primes in a given arithmetic progression. Before stating the theorem about the special case of Dirichlet's theorem, we prove a lemma that will be used in the proof of the mentioned theorem.

**Lemma 7.** *If $a$ and $b$ are integers both of the form $4n + 1$, then their product $ab$ is of the form $4n + 1$*

*Proof.* Let $a = 4n_1 + 1$ and $b = 4n_2 + 1$, then

$$ab = 16n_1n_2 + 4n_1 + 4n_2 + 1 = 4(4n_1n_2 + n_1 + n_2) + 1 = 4n_3 + 1,$$

where $n_3 = 4n_1n_2 + n_1 + n_2$. □

**Theorem 18.** *There are infinitely many primes of the form $4n + 3$, where $n$ is a positive integer.*

*Proof.* Suppose that there are finitely many primes of the form $4n + 3$, say $p_0 = 3, p_1, p_2, ..., p_n$. Let

$$N = 4p_1p_2...p_n + 3.$$

Notice that any odd prime is of the form $4n + 1$ or $4n + 3$. Then there is at least one prime in the prime factorization of $N$ of the form $4n + 3$, as otherwise, by

Lemma 7, $N$ will be in the form $4n + 1$. We wish to prove that this prime in the factorization of $N$ is none of $p_0 = 3, p_1, p_2, ..., p_n$. Notice that if

$$3 \mid N,$$

then $3 \mid (N - 3)$ and hence

$$3 \mid 4p_1p_2...p_n$$

which is impossible since $p_i \neq 3$ for every $i$. Hence 3 doesn't divide $N$. Also, the other primes $p_1, p_2, ..., p_n$ don't divide $N$ because if $p_i \mid N$, then

$$p_i \mid (N - 4p_1p_2...p_n) = 3.$$

Hence none of the primes $p_0, p_1, p_2, ..., p_n$ divides N. Thus there are infinitely many primes of the form $4n + 3$. □

**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 $6n + 5$.

## 2.5 Least Common Multiple

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

**Definition 10.** *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 19.** $\langle 2, 8\rangle = 8$, $\langle 5, 8\rangle = 40$

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

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

where (as above) we exclude any prime with 0 power in both $a$ and $b$. Then $\langle a, b\rangle = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} ... p_m^{\max(a_n,b_n)}$, 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 a lemma

**Lemma 8.** *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 19.** *Let $a$ and $b$ be two positive integers. Then*

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

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

Notice that since

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

and

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

then

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

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 $\langle a,b\rangle \mid m$. □

### 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 $m =< a,b >$.

## 2.6 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 represent the equation of a straight line. We need to find the points whose coordinates are integers and through which the straight line passes.

**Definition 11.** *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 20.** *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*

$$x = x_0 + (b/d)t \qquad y = y_0 - (a/d)t$$

*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

$$x_0 = km \text{ and } y_0 = kn.$$

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

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

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

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

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

**Example 21.** *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 $t$.*

**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.

## 2.7 The function $[x]$ , the symbols "O", "o" and "$\sim$"

We start this section by introducing an important number theoretic function. We proceed in defining some convenient symbols that will be used in connection with the growth and behavior of some functions that will be defined in later chapters.

### 2.7.1 The Function $[x]$

**Definition 12.** *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.
We now define some symbols that will be used to estimate the growth of number theoretic functions. These symbols will be not be really appreciated in the context of this book but these are often used in many analytic proofs.

### 2.7.2 The ”O” and ”o” Symbols

Let $f(x)$ be a positive function and let $g(x)$ be any function. Then $O(f(x))$ (pronounced ”big-oh” of $f(x)$)denotes the collection of functions $g(x)$ that exhibit a growth that is limited to that of $f(x)$ in some respect. The traditional notation for stating that $g(x)$ belongs to this collection is:

$$g(x) = O(f(x)).$$

This means that for sufficiently large $x$,

$$\frac{\mid g(x) \mid}{|f(x)|} < M, \tag{2.3}$$

where $M$ is some positive number.

**Example 22.** $\sin(x) = O(x)$*, and also* $\sin(x) = O(1)$*.*

Now, the relation $g(x) = o(f(x))$, pronounced ”small-oh” of $f(x)$, is used to indicate that $f(x)$ grows much faster than $g(x)$. It formally says that

$$\lim_{x\to\infty} \frac{g(x)}{f(x)} = 0. \tag{2.4}$$

More generally, $g(x) = o(f(x))$ at a point $b$ if

$$\lim_{x\to b} \frac{g(x)}{f(x)} = 0. \tag{2.5}$$

**Example 23.** $\sin(x) = o(x)$ *at* $\infty$*, and* $x^k = o(e^x)$ *also at* $\infty$ *for every constant* $k$*.*

The notation that $f(x)$ is asymptotically equal to $g(x)$ is denoted by $\sim$. Formally speaking, we say that $f(x) \sim g(x)$ if

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1. \tag{2.6}$$

**Example 24.** $[x] \sim x$*.*

The purpose of introducing these symbols is to make complicated mathematical expressions simpler. Some expressions can be represented as the principal part that you need plus a remainder term. The remainder term can be expressed using the above notations. So when you need to combine several expressions, the remainder parts involving these symbols can be easily combined. We will state now some properties of the above symbols without proof. These properties are easy to prove using the definitions of the symbols.

1. $O(O(f(x))) = O(f(x))$,

2. $o(o(f(x))) = o(f(x))$.

3. $O(f(x)) \pm O(f(x)) = O(f(x))$,

4. $o(f(x) \pm o(f(x)) = o(f(x))$,

5. $O(f(x)) \pm O(g(x)) = O(\max(f(x), g(x)))$,

There are some other properties that we did not mention here, properties that are rarely used in number theoretic proofs.

**Exercises**

1. Prove the five properties of the $[x]$

2. Prove the five properties of the $O$ and $o$ notations in Example 24.

## 2.8 Theorems and 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. The question that arises naturally here is the following: Can we estimate how many primes are there less than a given number? The theorem that answers this question is the prime number theorem. We denote by $\pi(x)$ the number of primes less than a given positive number $x$. Many mathematicians worked on this theorem and conjectured many estimates before Chebyshev finally stated that the estimate is $x/logx$. The prime number theorem was finally proved in 1896 when Hadamard and Poussin produced independent proofs. Before stating the prime number theorem, we state and prove a lemma involving primes that will be used in the coming chapters.

**Lemma 9.** *Let $p$ be a prime and let $m \in \mathbb{Z}^+$. Then the highest power of $p$ dividing $m!$ is*

$$\sum_{i=1}^{\infty} \left[\frac{m}{p^i}\right]$$

*Proof.* Among all the integers from 1 till $m$, there are exactly $\left[\frac{m}{p}\right]$ integers that are divisible by $p$. These are $p, 2p, ..., \left[\frac{m}{p}\right] p$. Similarly we see that there are $\left[\frac{m}{p^i}\right]$ integers that are divisible by $p^i$. As a result, the highest power of $p$ dividing $m!$ is

$$\sum_{i\geq 1} i \left\{ \left[\frac{m}{p^i}\right] - \left[\frac{m}{p^{i+1}}\right] \right\} = \sum_{i\geq 1} \left[\frac{m}{p^i}\right]$$

□

**Theorem 21.** ***The Prime Number Theorem*** *Let $x > 0$ then*

$$\pi(x) \sim x/logx$$

So this theorem says that you do not need to find all the primes less than $x$ to find out their number, it will be enough to evaluate $x/logx$ for large $x$ to find an estimate for the number of primes. Notice that I mentioned that $x$ has to be large enough to be able to use this estimate.

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* $(n + 1)^2$*?*

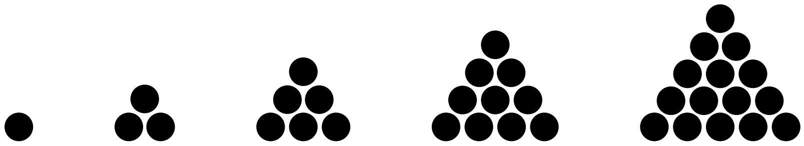
# Chapter 3

# Classical questions

This chapter visits some of the classical questions of number theory, which are a vital part of mathematical culture.

## 3.1 Geometric numbers

When you were a child, you probably played with pebbles or marbles, and you probably arranged them on the ground in certain shapes. For instance, you might have arranged them as triangles, and depending on the number of pebbles you had, you might have ended up with any of the following figures:



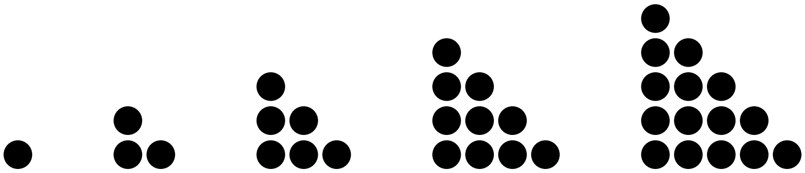
Did you ever pause to count how many pebbles were in each pile?

$$1, 3, 6, 10, 15, \ldots$$

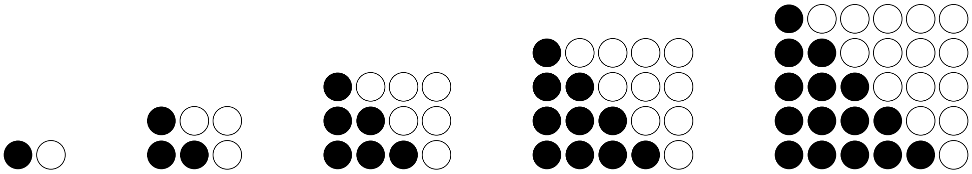
These numbers are called **triangular**, for a reason you'll probably never guess.[1] As you can see, the $i$th triangular number is built from the one before it in a reliable pattern: $t_1 = 1$, and if we know $t_i$, then the $(i+1)$th number is $t_i + (i+1)$.

This is another example of a **recursive** sequence. Sure, you saw them earlier with the Fibonacci numbers, but this one's a little easier to deal with: the recursion only requires knowledge of one previous number. Still, it would be nice to compute the $i$th triangular number without having to know the one before it, which would require us to determine the one before it, and so forth and so on, until we finally descended back down to $t_1$. Doing that all the time is boring. Wouldn't life be nicer if we had a concise little formula for it?

Indeed, it would! Let's try to find one. One way to look at this is by redrawing the picture. After all, a triangle is usually half a square:



...well, maybe not *quite* half a square. Our triangle seems to cover the entire diagonal. Well, a triangle is also half a rectangle...



That works out very nicely! The $n$th rectangle has area $n(n+1)$, so it makes sense that the $i$th triangle has area ${}^{n(n+1)}/_{2}$. This is a perfectly reasonable explanation, but if you prefer, we can resort to induction: It is clear that $t_1 = 1$. Assume that $t_n = {}^{n(n+1)}/_{2}$; we obtain $t_{n+1}$ by adding $n+1$ to $t_n$. Simplifying the sum, we

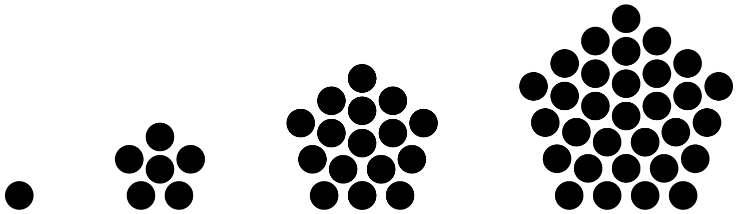
[1] Hope that gave you a chuckle.

see that

$$t_{n+1} = t_n + (n+1) = {}^{n(n+1)}\!/_{2} + {}^{2n+2}\!/_{2} = {}^{(n^2+n)+(2n+2)}\!/_{2}$$
$$= {}^{n^2+3n+2}\!/_{2} = {}^{(n+2)(n+1)}\!/_{2} = {}^{(n+1)[(n+1)+1]}\!/_{2}. \quad \square$$

**Exercises**

1. The $n$th **pentagonal** number is the number of pebbles you get when arranged in a pentagon with $n$ pebbles on a side; the first few are 1, 6, 16, 31, .... (See the diagrams below.) Conjecture a concise formula, and prove that it is correct.



*Hint:* To find a conjecture for the formula, look for triangular numbers.

2. The $n$th **hexagonal** number is the number of pebbles you get when arranged in a hexagon with $n$ pebbles on a side. Find the first few hexagonal numbers, conjecture a concise formula, and prove that it is correct.

## 3.2 Irrational numbers

The Pythagoreans of old believed that every measurement could be represented as the ratio of two integers. So, for instance, a right triangle whose legs have length 1 should have a hypotenuse whose length is the ratio of two integers. Which ones?

Applying the Pythagorean theorem of right triangles, we determine that the length $h$ of the hypotenuse is $\sqrt{2}$. Let's assume that we can, in fact, write $h$ as a ratio of two integers — and let's also assume that the integers are in reduced form. That is, $h = {}^{a}\!/\!_{b}$, where $\gcd(a, b) = 1$. It is perfectly sensible restriction to suppose that $a$ and $b$ are relatively prime, since we can reduce any fraction to lowest terms.

Naturally, we'd like to find two such integers, so let's try to identify some properties of $a$ and $b$. It seems natural to square both sides of the equation, so that $h^2 = {}^{a^2}\!/\!_{b^2}$. Recall that $h$ is the square root of 2, so $h^2 = 2$, so we can rewrite the equation again as $2 = {}^{a^2}\!/\!_{b^2}$. Multiply both sides of the equation by $b^2$ to see that $a^2 = 2b^2$.

Now, do you remember Euclid's criterion for a prime number? It said that if a prime number divides a product, then it must divide one of the factors. The equation $a^2 = 2b^2$ has a prime number, 2, that divides $a^2$; Euclid's criterion tells us that 2 divides $a$! We have discovered that a is even!

Let's see if we can find something similar about $b$. Since $a$ is even, we can write $a = 2c$, where $c$ is another integer. The equation $a^2 = 2b^2$ now becomes $(2c)^2 = 2b^2$, or, $4c^2 = 2b^2$. Divide both sides by 2 to see that $2c^2 = b^2$. Euclid's criterion tells us again that 2 divides $b$! We have discovered that $b$ is also even!

Isn't this great news? We started off looking for a representation of the square root of two as a ratio of integers. We ended up finding that it has to be the ratio of two even integers. This is incredible!

. . . uhm, wait. What was it we knew about a and b? We had assumed that they had no common factor. . . so how can they both be even?

Indeed, we have met a contradiction! We assumed two things: first, that we could represent the square root of two as the ratio of two integers; second, that these integers have no common factor. We found instead that the integers had to have a common factor. There is nothing unreasonable in the second assumption, as any fraction can reduce to lowest terms. The first assumption *must* be false: we cannot represent $\sqrt{2}$ as the ratio of two integers.

**Remark 3.** *Remember how we said the Pythagoreans believed that every measurement could be represented as the ratio of two integers. According to lore, it* *was a Pythagorean who discovered this fact. Once he told his companions, they sent him on a one-way cruise to the bottom of the Mediterranean ocean. The Pythagoreans have a well-deserved reputation for mathematical excellence, but even they were only human.*

**Exercises**

1. Show that if $p$ is prime, then we cannot write $\sqrt{p}$ as the ratio of two integers.
2. Show that if $n = pm$, where $p$ is prime and does not divide $m$, then we cannot write $\sqrt{n}$ as the ratio of two integers.

## 3.3 Gaussian integers

A **Gaussian integer** has the form $a + bi$, where $a$ and $b$ are integers, and $i$ is the square root of $-1$. For instance, $2+3i$ and $-i$ are Gaussian integers. We write $\mathbb{Z}[i]$ for the set of Gaussian integers; it enjoys certain properties which are interesting and sometimes surprising.

### 3.3.1 Ring properties of $\mathbb{Z}[i]$

The first interesting property of the Gaussian integers is that they satisfy the properties of a ring. We show some of these properties now, and leave the rest for the exercises.

Addition satisfies the properties of:

- **closure**, because

$$\begin{aligned}(a+bi)+(c+di) &= a+(bi+c)+di = a+(c+bi)+di\\ &= (a+c)+(bi+di) = (a+c)+(b+d)i,\end{aligned}$$

  and closure of integer addition implies that this number is a Gaussian integer;

- **associativity**, because

$$\begin{aligned}(a+bi)+[(c+di)+(e+fi)] &= (a+bi)+[(c+e)+(d+f)i]\\ &= [a+(c+e)]+[b+(d+f)]i\\ &= [(a+c)+e]+[(b+d)+f]i\\ &= [(a+c)+(b+d)i]+(e+fi)\\ &= [(a+bi)+(c+di)]+(e+fi)\end{aligned}$$

  — note how we relied on the associative property of integer addition for this;

- **commutativity**, as you will show in the assessment;

- **identity**, as $0+0i$ satisfies

$$\begin{aligned}&(a+bi)+(0+0i)=(a+0)+(b+0)i=a+bi \text{ and}\\ &(0+0i)+(a+bi)=(0+a)+(0+b)i=a+bi;\end{aligned}$$

  and

- **inverses**, as you will show in the assessment.

Multiplication satisfies the properties of:

- **closure**, as you will show in the assessment;

- **associativity**, because

$$\begin{aligned}
(a+bi)[(c+di)(e+fi)] &= (a+bi)[(ce-df)+(cf+de)i] \\
&= [a(ce-df)-b(cf+de)] \\
&\qquad + [a(cf+de)+b(ce-df)]i \\
&= [a(ce)-b(de)-a(df)-b(cf)] \\
&\qquad + [a(cf)-b(df)+a(de)+b(ce)]i \\
&= [(ac)e-(bd)e-(ad)f-(bc)f] \\
&\qquad + [(ac)f-(bd)f+(ad)e+(bc)e]i \\
&= [(ac-bd)e-(ad+bc)f] \\
&\qquad + [(ac-bd)f+(ad+bc)e]i \\
&= [(ac-bd)+(ad+bc)i](e+fi) \\
&= [(a+bi)(c+di)](e+fi)
\end{aligned}$$

  — note how we relied on the associative property of integer multiplication for this;

- **commutativity**, as you will show in the assessment;

- **identity**, as you will show in the assessment; and

- **distributivity over addition**, as you will show in the assessment.

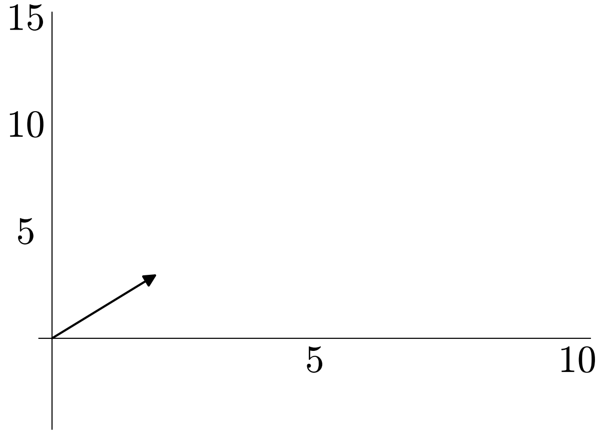
**Exercises**

1. Complete the explanation that the Gaussian integers satisfy the properties of a ring.

### 3.3.2 Division

We can think of Gaussian integers as vectors on the plane: $a + bi$ corresponds to the vector $(a, b)$.

**Example 25.** *We illustrate the vector corresponding to* $2 + 3i$*:*



Call the square of the Euclidean length of this vector the **norm** of the Gaussian integer, written as, $N(a + bi) = a^2 + b^2$. Typically, one does not multiply two vectors to each other, but here it makes sense to multiply them in a way that imitates the product of the corresponding Gaussian integers:

- If we multiply $a + bi$ by a positive integer $c$, we scale the corresponding vector to one whose length is $c \cdot N(a + bi)$.
- If we multiply $a+bi$ by a negative integer $c$, we both scale the corresponding vector *and* reverse its orientation.
- If we multiply $a + bi$ by $i$, we get $-b + ai$, which rotates the vector $90^\circ$ clockwise and preserves its length.

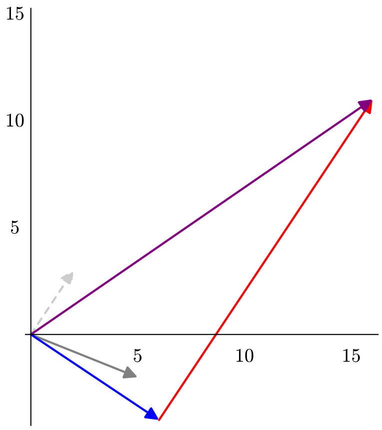
Putting these together, we obtain the following result.

**Lemma 10.** *The vector corresponding to the product of* $a + bi$ *and* $c + di$ *is obtained by adding:*

- *a vector obtained by scaling* $a + bi$ *by* $|c|$*, reversing the orientation if* $c$ *is negative, and*

- *a vector obtained by rotating $a + bi$ by $90^\circ$ counterclockwise, scaling the result by $|d|$, and reversing the orientation if $d$ is negative.*

**Example 26.** *We illustrate the products of $2 + 3i$ with $5$, $i$, and $5 - 2i$ below. See if you can pick out which of the colored vectors corresponds to which number or product of numbers.*



If we can multiply Gaussian integers, then there's a good bet that we can divide them, too — but how should we go about doing it? In particular, we'd like to do so in a way that gives us the smallest remainder possible — where, by "smallest" remainder, we refer of course to a Gaussian integer's norm.

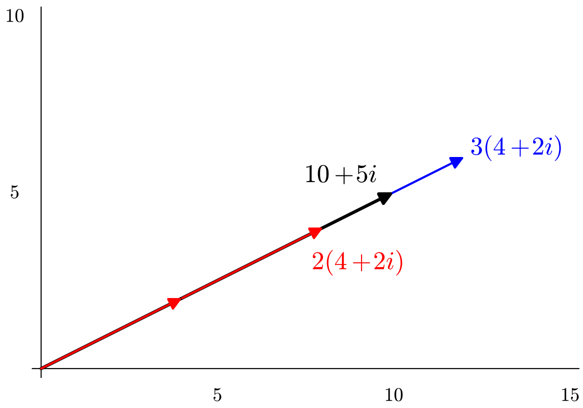
This approach implies that we can divide two Gaussian integers: let $a+bi, c+di \in \mathbb{Z}[i]$, and put

$$S = \{N((a+bi) - (m+ni)(c+di)) : m, n \in \mathbb{Z}\}.$$

Notice that $S \subseteq \mathbb{N}$. By the well ordering property, it has a smallest element, $s$, which corresponds to some $m + ni \in \mathbb{Z}[i]$. Choose these particular $m$ and $n$, and we have $s < N(c + di)$, for otherwise we lie outside a circle of radius $N(c + di)$ around $a + bi$. We elaborate on this below.

Let's start with two Gaussian integers that lie on the same line, but aren't multiples of each other: $4+2i$ and $10+5i$. It should be pretty clear that we can obtain the smallest possible remainder using either 2 or 3, since

- $(10+5i)-2\times(4+2i)=2+i$, which has norm $5$, and
- $(10+5i)-3\times(4+2i)=-2-i$, which also has norm $5$.

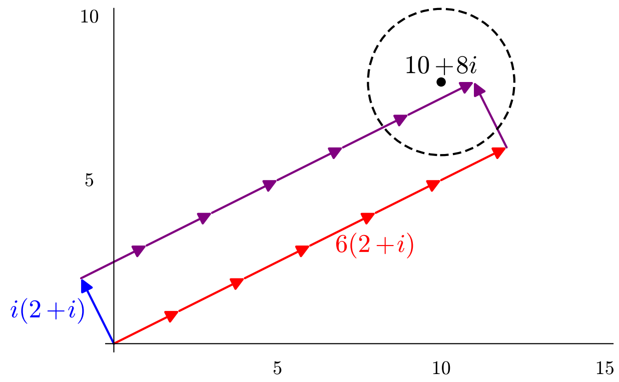


You should notice right away that there can be more than one remainder: in this example, we have $\pm(2+i)$. So that's one difference from ordinary integer division. On the other hand, the *norm* seems to be unique, at 5.

So what if the two integers aren't on the same line? Inasmuch as products of Gaussian integers consist of adding one scaling to the rotation of another scaling, it seems best to adopt the following approach for two Gaussian integers $\alpha$ and $\beta$:

- Find the integer $c$ such that the distance between $c\alpha$ and $\beta$ is minimal.
- Find the integer $d$ such that the distance between $di\alpha$ and $\beta$ is minimal.
- Use $\gamma=c+di$ for the quotient, and $\beta-\gamma\alpha$ for the remainder.

**Example 27.** *We illustrate the technique by dividing* $10+8i$ *by* $2+i$*. We minimize* $N((10+8i)-c(2+i))$ *when* $c=6$*, and minimize* $N((10+8i)-di(2+i))$ *when* $d=1$*. Adding them produces* $11+8i$*.*



*If you look carefully, you will see that there is more than one way to obtain a remainder that like within the circle: for instance, both $\gamma = 5 + i$ and $\gamma = 6 + 2i$ serve this purpose. However, they do not minimize $N((10 + 8i) - \gamma(2 + i))$, and we will use this fact to prove the general case.*

**Theorem 22.** *If $\gamma$ is chosen as described above, then $N(\beta - \gamma\alpha) < N(\alpha)$.*

*Sketch of proof.* Our proof relies highly on geometry, so it may help to draw some pictures while reading this. In particular, we frequently use the norm of a Gaussian integer as the radius of a circle around another one.

Suppose, to the contrary, that it is not; then the endpoint of $\gamma\alpha$ lies on or outside a circle of radius $N(\alpha)$ with the endpoint of $\beta$ at the center. For simplicity, we assume that $\alpha$ has positive real and imaginary parts; we can modify the easily otherwise, as indicated below. Without loss of generality, suppose $\gamma\alpha$ is closer to the origin than $\beta$. Extend $\gamma$ by adding to it one of $\check{\gamma} = \gamma + \alpha$ or $\hat{\gamma} = \gamma + i\alpha$. If the distance to $\beta$ remains unchanged in either direction, then these three points lie on a circle with $\beta$ at the center. By hypothesis, the circle has radius greater than $N(\alpha)$, so that $\gamma + (1 + i)\alpha$ lies within it, contradicting the choice of both $c$ and $d$. Otherwise, supposed that both $\check{\gamma}$ and $\hat{\gamma}$ lie further from $\beta$ than $\gamma$; in this case, $\beta$ must lie within a circle of radius $N(\alpha)$ from $\gamma$, contradicting the hypothesis that it does not. Thus, either $\check{\gamma}$ or $\hat{\gamma}$ lies closer to $\beta$ than $\gamma$, which again contradicts the choice of $c$ or $d$. We conclude that $\gamma$ □

**Remark 4.** *Usually, textbooks present Gaussian division a different way: multiply a fraction by the conjugate of the denominator, then pick "good" integers that are close to the resulting complex number. For instance, our example above would become*

$$\frac{10+8i}{2+i}\cdot\frac{2-i}{2-i}=\frac{28+6i}{5}=\frac{28}{5}+i\frac{6}{5}.$$

*This suggests that, if we let $\gamma = 6 + i$, we get the answer we need — and that was, in fact, the answer we found geometrically! See if you can visualize how this approach relates to the method given above.*

**Exercises**

1. Divide $30 + 23i$ by

   (a) $4$,

   (b) $2i$, and

   (c) $4 + 2i$.

   Use both the geometric approach, and the method of simplifying a complex fraction, then rounding. Notice that you don't always get the same answer.

### 3.3.3 Primality

The only integers which have integral multiplicative inverses are $\pm 1$. Well, which *Gaussian* integers have multiplicative inverses? Suppose $a + bi$ has an inverse $c + di$. You will show in the exercises that, in this case, $b = {}^{-d}/_{c2+d2}$. Because $c$ and $d$ are integers, the sum of their squares must be 1 (it is the only way we can get $c^2 + d^2$ to divide $d$) so $c = \pm 1$ and $d = 0$ or $c = 0$ and $d = \pm 1$. In short, the only Gaussian integers with multiplicative inverses are $\pm 1$ and $\pm i$.

Another question to ask is, what makes a Gaussian integer "prime"? According to the irreducibility criterion, an integer $p$ is prime if $p$ is divisible only by 1 and itself. As an integer, 2 is prime because the only numbers that divide it are 1 and itself.

What about the *Gaussian* integers? Rather surprisingly, many prime integers are not prime *Gaussian* integers! For example, $5 = (1 + 2i)(1 - 2i)$, $13 = (2 + 3i)(2 - 3i)$, $17 = (1 + 4i)(1 - 4i)$, and so forth.

Does this happen to *all* prime integers? We pass over 2 for the moment, but suppose there exist integers $a$ and $b$ such that $7 = (a + bi)(a - bi)$. That would mean $7 = a^2 + b^2$. The fact that $a$ and $b$ are integers means that their squares have to be positive integers, which means that they have to be smaller than 7. That limits our options, and it's easy to verify that no integer squares add up to 7: $1 + 1 = 2, 1 + 4 = 5, 4 + 4 = 8$. So, 7 remains prime even as a Gaussian integer.

We see that the question of whether a number is prime depends very much on the ring!

**Exercises**

1. Show that 2 is not a Gaussian prime.

2. Show that if an integer $p$ factors as $(a + bi)(c + di)$, then the factors are conjugate.

3. Show that 3 is a Gaussian prime.

4. Show that $1 + i$ is a Gaussian prime.

5. Show that if $a + bi$ and $c + di$ are multiplicative inverses, then $b = {}^{-d}/_{c^2+d^2}$.

6. Experiment with some small prime integers to formulate a criterion which identifies the ones that are prime Gaussian integers, and the ones that are not prime Gaussian integers. Do not try to prove your connjecture. (Yet.)

## 3.4 Algebraic and transcendental numbers

We call a number **algebraic** when it can be expressed as the root of a polynomial with integer coefficients. For example,

- 4 is algebraic, because it is a root of the polynomial $x - 4$; and
- $\sqrt{2}$ is algebraic, because it is a root of the polynomial $x^2 - 2$.

We call a number **transcendental** if it is not algebraic. It is not immediately obvious that any numbers are transcendental.

This section considers some properties of algebraic numbers, as well as the existence of transcendental numbers.

### 3.4.1 The algebraic numbers form a ring

Let $\mathbb{A}$ be the set of algebraic numbers. Is this a ring? To see that it is, let $\alpha$ and $\beta$ be algebraic numbers. Since they are roots of polynomials, supposed they are the roots of the polynomials $f$ and $g$. There are infinitely many polynomials like this, so choose $f$ and $g$ to be of minimal degree.

We first show closure of addition and multiplication. Let $\mathbb{E}$ be the smallest ring that contains both $\mathbb{Q}$ and $\alpha$, and let $\mathbb{F}$ be the smallest ring that contains $\mathbb{E}$ and $\beta$. Notice that E is a vector space of finite dimension over $\mathbb{Q}$, because its elements all have the form $\sum_{i=0}^{n} a_i \alpha^i$. In fact, $\mathbb{E}$ is itself a ring and a field, because the scalars come from $\mathbb{E}$ itself, and $\alpha$ has an inverse:

**Theorem 23.** *$\alpha$ has a multiplicative inverse in E.*

*Proof.* Let $a_0$, $a_1$, ..., $a_n$ be the coefficients of $f$, with $a_i$ the coefficient of $x_i$. Since $\alpha$ is a root of $f$, we know that

$$a_0\alpha^0 + a_1\alpha^1 + \ldots + a_n\alpha^n = 0.$$

Rewrite this equation as

$$\alpha\left(a_1 + a_2\alpha^1 + \ldots + a_n\alpha^{n-1}\right) = -a_0.$$

Since 0 is not a root of $f$, we can divide both sides by $-a_0$, obtaining

$$\alpha\left(-\frac{a_1}{a_0} - \frac{a_2}{a_0}\alpha^1 - \ldots - \frac{a_n}{a_0}\alpha^{n-1}\right) = 1.$$

So, we have found a multiplicative inverse, after all — but is it in $\mathbb{E}$? The quotients $-{}^{a_i}\!/_{a_0}$ are all rational numbers, and $\mathbb{E}$ is the smallest ring that contains both $\mathbb{Q}$ and $\alpha$, implying that, indeed,

$$-\frac{a1}{a_0} - \frac{a2}{a_0}\alpha^1 - \ldots - \frac{an}{a_0}\alpha^{n-1} \in \mathbb{E}.$$

□

A similar argument shows that $\mathbb{F}$ is both a vector space of finite dimension over $\mathbb{E}$, and a field. Notice that this makes $\mathbb{F}$ a vector space of finite dimension over $\mathbb{Q}$, just as $\mathbb{E}$ is.

Since $\mathbb{F}$ is a field that contains both $\alpha$ and $\beta$, it must also contain both $\alpha + \beta$ and $\alpha\beta$. But $\mathbb{F}$ is finite dimensional over $\mathbb{Q}$, say of dimension $n$, which means that we can find rational numbers $c_0$, $c_1$, …, $c_n$ and $d_0$, $d_1$, …, $d_n$ such that

$$c_0 + c_1(\alpha + \beta)^1 + ... + c_n(\alpha + \beta)^n = 0$$

and

$$d_0 + d_1(\alpha\beta)^1 + ... + d_n(\alpha\beta)^n = 0.$$

These equations remain true even if we multiply both sides by the greatest common denominators of the $c_i$ and the $d_i$, so we may assume that these coefficients *are actually integers*! (If the first choice was wrong, just reassign them to the coefficients obtained by clearing the denominators from the equations above.)

So, let

$$\begin{aligned}\hat{f} &= c_0 + c_1 x + \cdots + c_n x^n, \text{ and}\\ \hat{g} &= d_0 + d_1 x + \cdots + d_n x^n.\end{aligned}$$

Per the discussion above, $\hat{f}$ and $\hat{g}$ are polynomials with integer coefficients. Since $\alpha + \beta$ is a root of $\hat{f}$ and $\alpha\beta$ is a root of $\hat{g}$, we see that $\alpha + \beta$ and $\alpha\beta$ are algebraic. Our choice of $\alpha$ and $\beta$ was arbitrary in $\mathbb{A}$, so the algebraic numbers are closed under addition and multiplication.

We have shown that $\mathbb{A}$ is closed under addition and multiplication. The remaining properties of a ring are immediate, as $\mathbb{A}$ is a subset of the set $\mathbb{C}$ of complex numbers, which is itself a ring.

### 3.4.2 Liouville's number

It would be nice if all numbers were algebraic, but they are not. In fact, some fairly important numbers, such as $e$ and $\pi$, are not algebraic. Showing that these numbers are transcendental lies beyond the scope of these notes. Instead, we look at **Liouville's number**,

$$\lambda = \sum_{i=1}^{\infty} \frac{1}{10^{i!}}.$$

If you've taken Calculus, then you'll agree that this sum converges. The first "few" digits of its decimal representation are

$$0.110001000000000000000001\ldots.$$

As the digits proceed on to the right, the number of 0's between two 1's grows huge, thanks to the factorial. Since the decimal expansion neither terminates nor repeats, $\lambda$ must be irrational. What's more, this particular pattern of non-repetition is critical to transcendence. The require two steps, neither of which is obvious.

The first step is to show **Liouville's inequality**, which states that an irrational algebraic number is not "especially close" to any rational number. What does that mean? Suppose that $\alpha$ is algebraic and irrational, while ${}^{a}\!/\!{}_{b}$ is rational. Choose a minimal polynomial $f$ of degree $n$ that has $\alpha$ as a root; since $f$ is minimal, it does not factor. We will show that only finitely many rational numbers ${}^{a}\!/\!{}_{b}$ are closer to $\alpha$ than ${}^{1}\!/\!{}_{b^{n+1}}$.

The second step is to show that $\lambda$ does not satisfy Liouville's inequality. Were $\lambda$ algebraic, only finitely many rational numbers ${}^{a}\!/\!{}_{b}$ would be closer to $\alpha$ than ${}^{1}\!/\!{}_{b^{n+1}}$, regardless of the choice of ${}^{a}\!/\!{}_{b}$. Remember that $\lambda$ has all those increasing lengths of 0's: that will give us an infinite sequence of rational numbers that are closer to $\lambda$ than ${}^{1}\!/\!{}_{10^{n+1}}$, *regardless of the choice of* $n$.

*Proof of Liouville's Inequality.* Let $\alpha$ be an arbitrary algebraic number, and $f$ a polynomial of minimal degree, whose root is $\alpha$. Suppose ${}^{a}\!/\!{}_{b}$ is closer to $\alpha$ than ${}^{1}\!/\!{}_{b^{n+1}}$. Without loss of generality, we may assume that $b$ is positive; after all, if it isn't, we can switch the signs of $a$ and $b$ and have the same equation. Then $f({}^{a}\!/\!{}_{b})$ can be written as a fraction whose denominator is the integer $b_n$ and whose numerator is an integer. Hence, $|f({}^{a}\!/\!{}_{b})| \geq {}^{1}\!/\!{}_{b^n}$.

The Factor Theorem tells us that $f$ factors as $g \cdot (x - \alpha)$, where $g$ is some polynomial (not necessarily with integer coefficients). Hence $|f({}^{a}\!/\!{}_{b})| = |{}^{a}\!/\!{}_{b} - \alpha| \cdot |g({}^{a}\!/\!{}_{b})|$. By substitution, ${}^{1}\!/\!{}_{b^n} \leq |{}^{a}\!/\!{}_{b} - \alpha| \cdot |g({}^{a}\!/\!{}_{b})|$. If ${}^{a}\!/\!{}_{b}$ is as close to $\alpha$ as we claim, then ${}^{a}\!/\!{}_{b}$ is within ${}^{1}\!/\!{}_{b^n}$ of $\alpha$, and ${}^{1}\!/\!{}_{b^n}$ is smaller than 1, so ${}^{1}\!/\!{}_{b^n}$ is within 1 of $\alpha$, so $|{}^{a}\!/\!{}_{b}| \leq |\alpha| + 1$. Substitute this into $g$, and by using the triangle inequality on the terms of $g$ we find that

$$|g({}^{a}\!/\!{}_{b})| \leq \text{ some expression in terms of } \alpha\text{, but not in terms of } a \text{ or } b.$$

Call this expression $c$. By substitution, we have

$${}^{1}\!/\!{}_{b^n} \leq |{}^{a}\!/\!{}_{b} - \alpha| \cdot |g({}^{a}\!/\!{}_{b})| \leq {}^{1}\!/\!{}_{b^{n+1}} \cdot c.$$

Multiply both sides of the opposite ends of the inequality to find that

$$b \leq c.$$

Since $b$ is positive, there are only finitely many $b$ that we can choose to be smaller than $c$. For each of these, only finitely many $a$ satisfy ${}^{1}/_{b^{n+1}} \leq |{}^{a}/_{b} - \alpha|$. Hence, there are only finitely many rational numbers ${}^{a}/_{b}$ closer to $\alpha$ than ${}^{1}/_{b^{n+1}}$. □

*Proof that $\lambda$ is transcendental.* Let $n$ be any positive integer, and let

$$\frac{a_n}{b_n} = \frac{1}{10} + \frac{1}{10^2} + \cdots + \frac{1}{10^n}.$$

We can write ${}^{a}/_{b}$ in lowest terms as ${}^{1+10+\cdots+10^{n-1}}/_{10^n}$. Consider that $\lambda - {}^{a_n}/_{b_n} = {}^{1}/_{10^{n+1}} + {}^{1}/_{10^{n+2}+\ldots}$; we have

$$|\lambda - \frac{a_n}{b_n}| < \frac{2/10^{n+1}}{<}\frac{1}{b^{n+1}}.$$

We have found an infinite sequence of integers ${}^{a}/_{b}$ that are closer to $\lambda$ than ${}^{1}/_{b^{n+1}}$. As this violates Liouville's inequality, and $\lambda$ is irrational, it cannot be algebraic: $\lambda$ must be transcendental. □

### Exercises

1. Find a polynomial $f$ whose roots include $\sqrt{2}$. Try to give $f$ as low a degree as possible.

2. (a) Let $\mathbb{E}$ be the smallest ring that contains both $\mathbb{Q}$ and $\sqrt{2}$. What is the dimension of $\mathbb{E}$ as a vector space over $\mathbb{Q}$?

   (b) Let $\mathbb{F}$ be the smallest ring that contains both $\mathbb{E}$ and $\sqrt[4]{3}$. What is the dimension of $\mathbb{F}$ as a vector space over $\mathbb{E}$, and as a vector space over $\mathbb{Q}$?

3. Suppose that the polynomials $f$ and $g$ in the discussion of Section 3.4.1 have degree $k$ and $m$. What are the dimensions of $\mathbb{E}$ and $\mathbb{F}$, as vector spaces over $\mathbb{Q}$?

4. Find the value of $c$ that satisfies the proof of Liouville's Inequality for $\sqrt{2}$.

# Chapter 4

# Congruences

A congruence is nothing more than a statement about divisibility. The theory of congruences was introduced by Carl Friedreich Gauss. Gauss contributed to the basic ideas of congruences and proved several theorems related to this theory. We start by introducing congruences and their properties. We proceed to prove theorems about the residue system in connection with the Euler $\phi$-function. We then present solutions to linear congruences which will serve as an introduction to the Chinese remainder theorem. We present finally important congruence theorems derived by Wilson, Fermat and Euler.

## 4.1 Introduction to congruences

As we mentioned in the introduction, the theory of congruences was developed by Gauss at the beginning of the nineteenth century.

**Definition 13.** *Let m be a positive integer. We say that $a$ is congruent to $b$ modulo m if $m \mid (a-b)$ where $a$ and $b$ are integers, i.e. if $a = b + km$ where $k \in \mathbb{Z}$.*

If $a$ is congruent to $b$ modulo $m$, we write $a \equiv b(\bmod m)$.

**Example 28.** $19 \equiv 5(\mathrm{mod}\ 7)$. *Similarly* $2k+1 \equiv 1(\mathrm{mod}\ 2)$ *which means every odd number is congruent to 1 modulo 2.*

There are many common properties between equations and congruences. Some properties are listed in the following theorem.

**Theorem 24.** *Let* $a, b, c$ *and* $d$ *denote integers. Let* $m$ *be a positive integers. Then:*

1. *If* $a \equiv b(\mathrm{mod}\ m)$*, then* $b \equiv a(\mathrm{mod}\ m)$*.*

2. *If* $a \equiv b(\mathrm{mod}\ m)$ *and* $b \equiv c(\mathrm{mod}\ m)$*, then* $a \equiv c(\mathrm{mod}\ m)$*.*

3. *If* $a \equiv b(\mathrm{mod}\ m)$*, then* $a+c \equiv b+c(\mathrm{mod}\ m)$*.*

4. *If* $a \equiv b(\mathrm{mod}\ m)$*, then* $a-c \equiv b-c(\mathrm{mod}\ m)$*.*

5. *If* $a \equiv b(\mathrm{mod}\ m)$*, then* $ac \equiv bc(\mathrm{mod}\ m)$*.*

6. *If* $a \equiv b(\mathrm{mod}\ m)$*, then* $ac \equiv bc(\mathrm{mod}\ mc)$*, for* $c > 0$*.*

7. *If* $a \equiv b(\mathrm{mod}\ m)$ *and* $c \equiv d(\mathrm{mod}\ m)$ *then* $a+c \equiv (b+d)(\mathrm{mod}\ m)$*.*

8. *If* $a \equiv b(\mathrm{mod}\ m)$ *and* $c \equiv d(\mathrm{mod}\ m)$ *then* $a-c \equiv (b-d)(\mathrm{mod}\ m)$*.*

9. *If* $a \equiv b(\mathrm{mod}\ m)$ *and* $c \equiv d(\mathrm{mod}\ m)$ *then* $ac \equiv bd(\mathrm{mod}\ m)$*.*

*Proof.*

1. If $a \equiv b(\mathrm{mod}\ m)$, then $m \mid (a-b)$. Thus there exists integer $k$ such that $a-b = mk$, this implies $b-a = m(-k)$ and thus $m \mid (b-a)$. Consequently $b \equiv a(\mathrm{mod}\ m)$.

2. Since $a \equiv b(\mathrm{mod}\ m)$, then $m \mid (a-b)$. Also, $b \equiv c(\mathrm{mod}\ m)$, then $m \mid (b-c)$. As a result, there exit two integers $k$ and $l$ such that $a = b+mk$ and $b = c+ml$, which imply that $a = c+m(k+l)$ giving that $a = c(\mathrm{mod}\ m)$.

3. Since $a \equiv b(\bmod m)$, then $m \mid (a-b)$. So if we add and subtract $c$ we get

$$m \mid ((a+c)-(b+c))$$

and as a result

$$a+c \equiv b+c(\bmod m).$$

4. Since $a \equiv b(\bmod m)$, then $m \mid (a-b)$ so we can subtract and add $c$ and we get

$$m \mid ((a-c)-(b-c))$$

and as a result

$$a-c \equiv b-c(\bmod m).$$

5. If $a \equiv b(\bmod m)$, then $m \mid (a-b)$. Thus there exists integer $k$ such that $a-b=mk$ and as a result $ac-bc=m(kc)$. Thus

$$m \mid (ac-bc)$$

and hence

$$ac \equiv bc(\bmod m).$$

6. If $a \equiv b(\bmod m)$, then $m \mid (a-b)$. Thus there exists integer $k$ such that $a-b=mk$ and as a result

$$ac-bc=mc(k).$$

Thus

$$mc \mid (ac-bc)$$

and hence

$$ac \equiv bc(\bmod mc).$$

7. Since $a \equiv b(\text{mod } m)$, then $m \mid (a-b)$. Also, $c \equiv d(\text{mod } m)$, then $m \mid (c-d)$. As a result, there exits two integers $k$ and $l$ such that $a-b = mk$ and $c-d = ml$. Note that

$$(a-b)+(c-d) = (a+c)-(b+d) = m(k+l).$$

As a result,

$$m \mid ((a+c)-(b+d)),$$

hence

$$a+c \equiv b+d(\text{mod } m).$$

8. If $a = b+mk$ and $c = d+ml$ where $k$ and $l$ are integers, then

$$(a-b)-(c-d) = (a-c)-(b-d) = m(k-l).$$

As a result,

$$m \mid ((a-c)-(b-d)),$$

hence

$$a-c \equiv b-d(\text{mod } m).$$

9. There exit two integers $k$ and $l$ such that $a-b = mk$ and $c-d = ml$ and thus $ca-cb = m(ck)$ and $bc-bd = m(bl)$. Note that

$$(ca-cb)+(bc-bd) = ac-bd = m(kc-lb).$$

As a result,

$$m \mid (ac-bd),$$

hence

$$ac \equiv bd(\text{mod } m).$$

□

**Example 29.**

1. *Since* $14 \equiv 8 (\mathrm{mod}\ 6)$*, we conclude* $8 \equiv 14 (\mathrm{mod}\ 6)$.

2. *Since* $22 \equiv 10 (\mathrm{mod}\ 6)$*, we conclude that* $10 \equiv 4 (\mathrm{mod}\ 6)$*. Notice that, in turn,* $22 \equiv 4 (\mathrm{mod}\ 6)$.

3. *Since* $50 \equiv 20 (\mathrm{mod}\ 15)$*, we conclude* $50 + 5 = 55 \equiv 20 + 5 = 25 (\mathrm{mod}\ 15)$.

4. *Since* $50 \equiv 20 (\mathrm{mod}\ 15)$*, we conclude* $50 - 5 = 45 \equiv 20 - 5 = 15 (\mathrm{mod}\ 15)$.

5. *Since* $19 \equiv 16 (mod 3)$*, we conclude* $2(19) = 38 \equiv 2(16) = 32 (\mathrm{mod}\ 3)$.

6. *Since* $19 \equiv 16 (mod 3)$*, we conclude* $2(19) = 38 \equiv 2(16) = 32 (\mathrm{mod}\ 2(3) = 6)$.

7. *Since* $19 \equiv 3 (\mathrm{mod}\ 8)$ *and* $17 \equiv 9 (\mathrm{mod}\ 8)$*, we conclude* $19 + 17 = 36 \equiv 3 + 9 = 12 (\mathrm{mod}\ 8)$.

8. *Since* $19 \equiv 3 (\mathrm{mod}\ 8)$ *and* $17 \equiv 9 (\mathrm{mod}\ 8)$*, then* $19 - 17 = 2 \equiv 3 - 9 = -6 (\mathrm{mod}\ 8)$.

9. *Since* $19 \equiv 3 (\mathrm{mod}\ 8)$ *and* $17 \equiv 9 (\mathrm{mod}\ 8)$*, we conclude* $19(17) = 323 \equiv 3(9) = 27 (\mathrm{mod}\ 8)$.

We now present a theorem that will show one difference between equations and congruences: we cannot cancel across congruence in all cases. For instance, $8 \times 6 \equiv 8 (\mathrm{mod}\ 20)$ and $16 \times 8 \equiv 8 (\mathrm{mod}\ 20)$, so the transitive property implies that $2 \times 3 \equiv 4 \times 3 (\mathrm{mod}\ 6)$. However, it is obviously a bad idea to cancel 8 from both sides of this congruence, as 6 is not congruent to 16 modulo 10.

In general, this means that we cannot solve congruences in quite the same way as we solve equations: the congruence $2x \equiv 0 (\mathrm{mod}\ m)$ does not force $x \equiv 0 (\mathrm{mod}\ m)$! Nevertheless, there are some cases where this is possible, and we can also find some similar properties that do hold. In other words, dividing both sides of the congruence by the same integer doesn't preserve the congruence.

**Theorem 25.**

1. *If* $a, b, c$ *and* $m$ *are integers such that* $m > 0$*,* $d = (m, c)$ *and* $ac \equiv bc(\text{mod } m)$*, then* $a \equiv b(\text{mod } m/d)$*.*

2. *If* $(m, c) = 1$ *then* $a = b(\text{mod } m)$ *if* $ac \equiv bc(\text{mod } m)$*.*

*Proof.* Part 2 follows immediately from Part 1. For Part 1, if $ac \equiv bc(\text{mod } m)$, then

$$m \mid (ac - bc) = c(a - b).$$

Hence there exists $k$ such that $c(a - b) = mk$. Dividing both sides by $d$, we get $(c/d)(a - b) = k(m/d)$. Since $(m/d, c/d) = 1$, it follows that $m/d \mid (a - b)$. Hence $a \equiv b(\text{mod } m/d)$. □

**Example 30.** $38 \equiv 10(\text{mod } 7)$. *Since* $(2, 7) = 1$ *then* $19 \equiv 5(\text{mod } 7)$.

The following theorem combines several congruences of two numbers with different moduli.

**Theorem 26.** *If*

$$a \equiv b(\text{mod } m_1), a \equiv b(\text{mod } m_2), ..., a \equiv b(\text{mod } m_t)$$

*where* $a, b, m_1, m_2, ..., m_t$ *are integers and* $m_1, m_2, ..., m_t$ *are positive, then*

$$a \equiv b(\text{mod } \langle m_1, m_2, ...m_t \rangle)$$

*Proof.* Since $a \equiv b(\text{mod } m_i)$ for all $1 \leq i \leq t$. Thus $m_i \mid (a - b)$. As a result,

$$\langle m_1, m_2, ..., m_t \rangle \mid (a - b)$$

(prove this as an exercise). Thus

$$a \equiv b(\text{mod } \langle m_1, m_2, ...m_t \rangle).$$

□

## Exercises

1. Determine whether 3 and 99 are congruent modulo 7 or not.

2. Show that if $x$ is an odd integer, then $x^2 \equiv 1(\text{mod } 8)$

3. Show that if $a, b, m$ and $n$ are integers such that $m$ and $n$ are positive, $n \mid m$ and $a \equiv b(\text{mod } m)$, then $a \equiv b(\text{mod } n)$.

4. Show that if $a_i \equiv b_i(\text{mod } m)$ for $i = 1, 2, ..., n$, where $m$ is a positive integer and $a_i, b_i$ are integers for $j = 1, 2, ..., n$, then $\sum_{i=1}^{n} a_i \equiv \sum_{i=1}^{n} b_i(\text{mod } m)$

5. For which $n$ does the expression $1 + 2 + ... + (n - 1) \equiv 0(\text{mod } n)$ holds.

6. Show that a number is divisible by three if and only if the sum of its digits is divisible by 3.
   *Hint:* Write 3 base 10, and use Theorem 24.

7. Show that a number is divisible by nine if and only if the sum of its digits is divisible by 9.

8. Show that a number is divisible by four if and only if its last two digits (tens and ones place) make a number that is divisible by four.

9. Show that a number is divisible by eight if and only if its last three digits make a number that is divisible by eight.

10. Show that a number is divisible by eleven if and only if the alternating sum of its digits is divisible by 11. For instance, the alternating sum of $11^2 = 121$ is $1-2+1 = 0$, and the alternating sum of $46 \times 11 = 506$ is $5-0+6 = 11$.

11. Using techniques similar to those of the previous exercises, formulate and prove rules of divisibility for 6 and 7.

## 4.2 Residue Systems and Euler's $\phi$-Function

### 4.2.1 Residue Systems

Suppose $m$ is a positive integer. Given two integers $a$ and $b$, we see that by the division algorithm that $a = bm + r$ where $0 \leq r < m$. We call $r$ the least nonnegative residue of $a$ modulo $m$. As a result, we see that any integer is congruent to one of the integers $0, 1, 2, ..., m - 1$ modulo m.

**Definition 14.** *A complete residue system modulo $m$ is a set of integers such that every integer is congruent modulo $m$ to exactly one integer of the set.*

The easiest complete residue system modulo $m$ is the set of integers $0, 1, 2, ..., m-1$. Every integer is congruent to one of these integers modulo $m$. This is important enough that mathematicians call it the set of **canonical residues modulo** $m$.

**Example 31.** *The set of integers $\{0, 1, 2, 3, 4\}$ form a complete residue system modulo $5$. Another complete residue system modulo $5$ could be $6, 7, 8, 9, 10$.*

**Definition 15.** *A reduced residue system modulo $m$ is a set of integers $r_i$ such that $(r_i, m) = 1$ for all $i$ and $r_i \neq r_j (\bmod m)$ if $i \neq j$.*

Notice that, a reduced residue system modulo $m$ can be obtained by deleting all the elements of the complete residue system set that are not relatively prime to $m$.

**Example 32.** *The set of integers $\{1, 5\}$ is a reduced residue system modulo $6$.*

The following lemma will help determine a complete residue system modulo any positive integer $m$.

**Lemma 11.** *A set of $m$ incongruent integers modulo $m$ forms a complete residue system modulo $m$.*

*Proof.* We will prove this lemma by contradiction. Suppose that the set of $m$ integers does not form a complete residue system modulo $m$. Then we can find at least one integer $a$ that is not congruent to any element in this set. Hence non of the elements of this set is actually congruent to the remainder when $a$ is divided by $m$. Thus dividing by $m$ yields to at most $m-1$ remainders. Therefore by the pigeonhole principle, at least two integers in the set that have the same remainder modulo $m$. This is a contradiction since the set of integers is formed of $m$ integers that are incongruent modulo $m$. □

**Theorem 27.** *If $a_1, a_2, ..., a_m$ is a complete residue system modulo $m$, and if $k$ is a positive integer with $(k, m) = 1$, then*

$$ka_1 + b, ka_2 + b, ..., ka_m + b$$

*is another complete residue system modulo $m$ for any integer $b$.*

*Proof.* Let us prove first that no two elements of the set $\{ka_1+b, ka_2+b, ..., ka_m+b\}$ are congruent modulo $m$. Suppose there exists $i$ and $j$ such that

$$ka_i + b \equiv ka_j + b (\bmod m).$$

Thus we get that

$$ka_i \equiv ka_j (\bmod m).$$

Now since $(k, m) = 1$, we get

$$a_i \equiv a_j (\bmod m)$$

But for $i \neq j$, $a_i$ is inequivalent to $a_j$ modulo $m$. Thus $i = j$. Now notice that there are $m$ inequivalent integers modulo m and thus by Lemma 10, the set form a complete residue system modulo $m$. □

### 4.2.2 Euler's $\phi$-Function

We now present a function that counts the number of positive integers less than a given integer that are relatively prime to that given integer. This function is called Euler $\phi$-function. We will discuss the properties of Euler $\phi$-function in details in chapter 5. It will be sufficient for our purposes in this chapter to the notation.

**Definition 16.** *The Euler $\phi$-function of a positive integer n, denoted by $\phi(n)$ counts the number of positive integers less than $n$ that are relatively prime to n.*

**Example 33.** *Since 1 and 3 are the only two integers that are relatively prime to 4 and less than 4, then $\phi(4) = 2$. Also, 1,2,...,6 are the integers that are relatively prime to 7 that are less than 7, thus $\phi(7) = 6$.*

Now we can say that the number of elements in a reduced residue system modulo $n$ is $\phi(n)$.

**Theorem 28.** *If $a_1, a_2, ..., a_{\phi(n)}$ is a reduced residue system modulo $n$ and $(k, n) = 1$, then $ka_1, ka_2, ..., ka_{\phi(n)}$ is a reduced residue system modulo $n$.*

*Proof.* The proof proceeds exactly in the same way as that of Theorem 24. □

**Exercises**

1. Give a reduced residue system modulo 12.

2. Give a complete residue system modulo 13 consisting only of odd integers.

3. Find $\phi(8)$ and $\phi(101)$.

4. Show that any reduced residue system satisfies the properties of a ring.

## 4.3 Linear Congruences

Because congruences are analogous to equations, it is natural to ask about solutions of linear equations. In this section, we will be discussing linear congruences of one variable and their solutions. We start by defining linear congruences.

**Definition 17.** *A congruence of the form $ax \equiv b(\bmod m)$ where $x$ is an unknown integer is called a linear congruence in one variable.*

It is important to know that if $x_0$ is a solution for a linear congruence, then all integers $x_i$ such that $x_i \equiv x_0(\bmod m)$ are solutions of the linear congruence. Notice also that $ax \equiv b(\bmod m)$ is equivalent to a linear Diophantine equation i.e. there exists $y$ such that $ax - my = b$. We now prove theorems about the solutions of linear congruences.

**Theorem 29.** *Let $a, b$ and $m$ be integers such that $m > 0$ and let $c = (a, m)$. If $c$ does not divide $b$, then the congruence $ax \equiv b(\bmod m)$ has no solutions. If $c \mid b$, then*

$$ax \equiv b(\bmod m)$$

*has exactly $c$ incongruent solutions modulo $m$.*

*Proof.* As we mentioned earlier, $ax \equiv b(\bmod m)$ is equivalent to $ax - my = b$. By Theorem 19 on Diophantine equations, we know that if $c$ does not divide $b$, then the equation, $ax - my = b$ has no solutions. Notice also that if $c \mid b$, then there are infinitely many solutions whose variable $x$ is given by

$$x = x_0 + (m/c)t$$

Thus the above values of $x$ are solutions of the congruence $ax \equiv b(\bmod m)$. Now we have to determine the number of incongruent solutions that we have. Suppose that two solutions are congruent, i.e.

$$x_0 + (m/c)t_1 \equiv x_0 + (m/c)t_2(\bmod m).$$

Thus we get

$$(m/c)t_1 \equiv (m/c)t_2(\text{mod } m).$$

Now notice that $(m, m/c) = m/c$ and thus

$$t_1 \equiv t_2(\text{mod } c).$$

Thus we get a set of incongruent solutions given by $x = x_0 + (m/c)t$, where $t$ is taken modulo $c$. □

**Remark 5.** *Notice that if $c = (a, m) = 1$, then there is a unique solution modulo m for the equation $ax \equiv b(\text{mod } m)$.*

**Example 34.** *Let us find all the solutions of the congruence $3x \equiv 12(\text{mod } 6)$. Notice that $(3, 6) = 3$ and $3 \mid 12$. Thus there are three incongruent solutions modulo $6$. We use the Euclidean algorithm to find the solution of the equation $3x - 6y = 12$ as described in chapter 2. As a result, we get $x_0 = 6$. Thus the three incongruent solutions are given by $x_1 = 6(\text{mod } 6)$, $x_1 = 6 + 2 = 2(\text{mod } 6)$ and $x_2 = 6 + 4 = 4(\text{mod } 6)$.*

As we mentioned earlier in Remark 2, the congruence $ax \equiv b(mod\ m)$ has a unique solution if $(a, m) = 1$. This will allow us to talk about modular inverses.

**Definition 18.** *A solution for the congruence $ax \equiv 1(\text{mod } m)$ for $(a, m) = 1$ is called the modular inverse of $a$ modulo m. We denote such a solution by $\bar{a}$.*

**Example 35.** *The modular inverse of 7 modulo 48 is 7. Notice that a solution for $7x \equiv 1(\text{mod } 48)$ is $x \equiv 7(\text{mod } 48)$.*

### Exercises

1. Find all solutions of $3x \equiv 6(\text{mod } 9)$.

2. Find all solutions of $3x \equiv 2(\text{mod } 7)$.

3. Find an inverse modulo 13 of 2 and of 11.

4. Show that if $\bar{a}$ is the inverse of $a$ modulo $m$ and $\bar{b}$ is the inverse of $b$ modulo $m$, then $\bar{a}\bar{b}$ is the inverse of $ab$ modulo $m$.

## 4.4 The Chinese Remainder Theorem

In this section, we discuss the solution of a system of congruences having different moduli. An example of this kind of systems is the following; find a number that leaves a remainder of 1 when divided by 2, a remainder of 2 when divided by three and a remainder of 3 when divided by 5. This kind of question can be translated into the language of congruences. As a result, in this chapter, we present a systematic way of solving this system of congruences.

### 4.4.1 Direct solution

**Theorem 30.** *The system of congruences*

$$\begin{aligned} x &\equiv b_1 (\bmod\ n_1), \\ x &\equiv b_2 (\bmod\ n_2), \\ &\vdots \\ x &\equiv b_t (\bmod\ n_t), \end{aligned}$$

*has a unique solution modulo* $N = n_1 n_2 ... n_t$ *if* $n_1, n_2, ..., n_t$ *are pairwise relatively prime positive integers.*

*Proof.* Let $N_k = N/n_k$. Since $(n_i, n_j) = 1$ for all $i \neq j$, then $(N_k, n_k) = 1$. Hence by Theorem 26 , we can find an inverse $y_k$ of $N_k$ modulo $n_k$ such that $N_k y_k \equiv 1 (\bmod\ n_k)$. Consider now

$$x = \sum_{i=1}^{t} b_i N_i y_i$$

Since

$$N_j \equiv 0(\bmod n_k) \text{ for all } j \neq k,$$

thus we see that

$$x \equiv b_k N_k y_k (\bmod n_k).$$

Also notice that $N_k y_k \equiv 1(\bmod n_k)$. Hence $x$ is a solution to the system of t congruences. We have to show now that any two solutions are congruent modulo $N$. Suppose now that you have two solutions $x_0, x_1$ to the system of congruences. Then

$$x_0 \equiv x_1 (\bmod n_k)$$

for all $1 \leq k \leq t$. Thus by Theorem 23, we see that

$$x_0 \equiv x_1 (\bmod N).$$

Thus the solution of the system is unique modulo $N$. □

We now present an example that will show how the Chinese remainder theorem is used to determine the solution of a given system of congruences.

**Example 36.** *Solve the system*

$$\begin{aligned} x &\equiv 1(\bmod 2) \\ x &\equiv 2(\bmod 3) \\ x &\equiv 3(\bmod 5). \end{aligned}$$

*We have* $N = 2.3.5 = 30$. *Also*

$$N_1 = 30/2 = 15, N_2 = 30/3 = 10 \textit{and } N_3 = 30/5 = 6.$$

*So we have to solve now* $15y_1 \equiv 1(\bmod 2)$. *Thus*

$$y_1 \equiv 1(\bmod 2).$$

*In the same way, we find that*

$$y_2 \equiv 1(\text{mod } 3)\textit{and } \; y_3 \equiv 1(\text{mod } 5).$$

*As a result, we get*

$$x \equiv 1.15.1 + 2.10.1 + 3.6.1 \equiv 53 \equiv 23(\text{mod } 30).$$

**Exercises**

1. Find an integer that leaves a remainder of 2 when divided by either 3 or 5, but that is divisible by 4.
2. Find all integers that leave a remainder of 4 when divided by 11 and leaves a remainder of 3 when divided by 17.
3. Find all integers that leave a remainder of 1 when divided by 2, a remainder of 2 when divided by 3 and a remainder of 3 when divided by 5.

### 4.4.2 Incremental solution

An alternate approach, which works with a more general class of systems of congruence, is to solve incrementally. We have observed already that a linear congruence corresponds to a linear Diophantine equation; thus, it is possible to take a system of linear congruences, solve one, use its solution to solve a second, use the resulting solution to solve a third, etc. In these cases, you can often find a "unique" solution to the system even when the moduli are not pairwise prime.

For instance, suppose that $x \equiv (\text{mod } 6)$, $x \equiv 2(\text{mod } 10)$, and $x \equiv 7(\text{mod } 15)$. Here, no pair of moduli is relatively prime, but we can still find a unique solution by rewriting the congruences as linear Diophantine equations.

Start by looking at the first congruence. Its solutions have the form $x = 6q+4$, where $q$ is an integer. Substitute this into the second congruence, and we have $6q + 4 \equiv 2(\text{mod } 10)$. This tells us that $6q + 4 = 10r + 2$, where $r$ is an integer.

Solving this in the usual fashion for linear Diophantine equations, we find that all solutions of the equation have the form $q = -2 + 5a$ and $r = -1 + 3a$, where $a$ is an integer. By substitution, $x = 6(-2 + 5a) + 4 = 30a - 8$.

Substitute this into the third congruence, and we have $30a - 8 \equiv 15s + 7$. Solving this again in the usual fashion for linear Diophantine equations, we find that all solutions of the equation have the form $a = 1 + b$, $s = 1 + 2b$, where $b$ is an integer. By substitution, $x = 30(1 + b) - 8 = 30b - 8$. We can now verify that

$$\begin{aligned} x &\equiv 4 \ (\text{mod } 6), \text{ since } 30b - 8 = (30b - 12) + 4 = 6(5b - 2) + 4; \\ x &\equiv 2 \ (\text{mod } 10), \text{ since } 30b - 8 = (30b - 10) + 2 = 10(3b - 1) + 2; \text{ and} \\ x &\equiv 7 \ (\text{mod } 15), \text{ since } 30b - 8 = (30b - 15) + 7 = 15(2b - 1) + 7. \end{aligned}$$

We found a solution to the system!

But in what sense is this solution “unique”? After all, there are infinitely many solutions for $x$! Each new solution comes by adding or subtracting a multiple of 30 to a known solution, and $30 = \text{lcm}(6, 10, 15)$. Thus, the solution is unique modulo the least common multiple! Notice how this generalizes the Chinese Remainder Theorem: in that case, $\text{lcm}(n_1, n_2, \ldots, n_t) = N$ precisely because the $n_i$ are pairwise relatively prime.

**Exercises**

1. Solve the system of linear congruences $x \equiv 4(\text{mod } 14)$, $x \equiv 7(\text{mod } 15)$, $x \equiv 4(\text{mod } 21)$.

2. Show that there is no solution to the system of linear congruences $x \equiv 0(\text{mod } 6)$, $x \equiv 7(\text{mod } 15)$, $x \equiv 2(\text{mod } 10)$.

3. Show that if a solution of a system of linear congruences modulo $n_1$, $n_2$, $\ldots$, $n_t$ exists, then the solution is unique modulo $\text{lcm}(n_1, n_2, \ldots, n_t)$.

## 4.5 Field properties of residues modulo a prime, and a primality test

Recall that "primality" is a fancy word for "the property of being prime", and a "primality test" is a criterion that determines whether an integer is prime. Currently, we have two theoretical criteria for primality of an integer:

- the irreducibility criterion (Definition 8); and
- Euclid's criterion (Definition 9).

These are not especially useful for testing whether an integer is prime. To start with, Euclid's criterion isn't even finite, as we'd have to test every product of integers. At least the irreducibility criterion requires us to check only finitely many factors (2, 3, 4, …, $\sqrt{p}$) but even this gets tedious and wasteful as the numbers grow beyond toy size. This section gives a third criterion for primality, also finite, that takes a different approach.

### 4.5.1 When is a system of residues a field?

A set $\mathbb{F}$ is a field if addition and multiplication work the same in $\mathbb{F}$ as they do for rational numbers:

- Addition satisfies the properties of:
  - closure, associativity, and commutativity;
  - there is an identity $z$ such that $z + x = x = x + z$ for every $x \in \mathbb{F}$; and
  - every $x \in \mathbb{F}$ has an inverse $y \in \mathbb{F}$ such that $x + y = z = y + x$.
- Multiplication satisfies the properties of:
  - closure, associativity, and commutativity;

  - there is an identity $\iota \in \mathbb{F}$ such that $\iota x = x = x\iota$ for every $x \in \mathbb{F}$;
  - every $x \in \mathbb{F}$ has an inverse $y \in \mathbb{F}$ such that $xy = \iota = yx$; and
  - distribution over addition.

Guess what? If $p$ is prime, then the set $\mathbb{F}_p = \{0, 1, ..., p - 1\}$ is a field, where addition and multiplication are performed modulo $p$. How so?

- **Closure:** Let $x, y \in \mathbb{F}_p$. If we perform addition and multiplication modulo $p$, then the sum and product can both be rewritten as elements of $\mathbb{F}_p$ by computing the remainder from division by $p$.

- **Associative:** Let $x, y, z \in \mathbb{F}_p$. Let $w$ be the element of $\mathbb{F}_p$ satisfy $w \equiv (x + y) + z \pmod p$. By definition of congruence, we can find an integer $q$ such that $(x + y) + z = pq + w$. Integer addition is associative, so $x + (y + z) = pq + w$, also. By definition, $w \equiv x + (y + z)\ (\text{mod} p)$. Hence $x + (y + z) \equiv w \equiv (x + y) + z$: addition is associative modulo $p$. A similar argument shows that multiplication is associative modulo $p$.

- **Identity:** Let $x \in \mathbb{F}_p$. Notice that $0, 1 \in \mathbb{F}_p$; they satisfy the properties $x + 0 = x = 0 + x$ and $1 \cdot x = x = x \cdot 1$ as integers, so substitution implies that they are congruent modulo $p$.

- ***Additive* inverse:** Let $x$ be in $\mathbb{F}_p$. We claim that $p - x$ is an additive inverse of $x$. Indeed, $(p - x) + x = p = x + (p - x)$ as integers, and $p \equiv 0 \pmod p$, so an additive inverse exists. In addition, $p - x \in \mathbb{F}_p$, so the inverse exists in $\mathbb{F}_p$.

- ***Multiplicative* inverse:** See Theorem 31.

- **Distributive:** Let $x, y, z \in \mathbb{F}_p$. Notice that $x(y + z) = xy + xz$ as integers, so substitution implies that they are congruent modulo $p$.

All the properties of a field are fairly clear, except multiplicative inverses. We turn our attention to that now.

**Theorem 31** (Fermat's Little Theorem)**.** *If $p$ is prime, then $x^{p-1} \equiv 1$ for any $x \in \mathbb{F}_p$. In other words, $x^{p-2}$ is the multiplicative inverse of $x$.*

**Example 37.** *In $\mathbb{F}_7$, we see that*

- $2 \cdot 2^5 \equiv 2 \cdot 32 \equiv 2 \cdot 4 \equiv 8 \equiv 1$ $(\textit{mod}\ 7)$*;*
- $3 \cdot 3^5 \equiv 3 \cdot 243 \equiv 729 \equiv 1$ $(\textit{mod}\ 7)$*;*
- $\ldots$
- $6 \cdot 6^5 \equiv 6 \cdot 7776 \equiv 46656 \equiv 1$ $(\textit{mod}\ 7)$.

Alas, we cannot test it for all possible prime numbers, because (as we saw earlier) there are infinitely many primes. To show that this is true for all primes, we adopt a different approach.

*Proof.* Let $x \in \mathbb{F}_p$, and consider the product

$$x \times 2x \times 3x \times \ldots \times ((p-1)x) = (p-1)!x^{p-1}. \tag{4.1}$$

On the other hand, Theorem 27 tells us that $\{x, 2x, \ldots, (p-1)x\}$ is a complete system of residues, so its elements are congruent to $\{1, 2, \ldots, p-1\}$. By substitution, then,

$$x \times 2x \times 3x \times \ldots \times ((p-1)x) \equiv 1 \times 2 \times 3 \times \ldots \times (p-1) = (p-1)!. \tag{4.2}$$

Combining equations (4.1) and (4.2) via the transitive property, we see that

$$(p-1)!x^{p-1} \equiv (p-1)!\ (\mathrm{mod} p).$$

The nonzero elements of $\mathbb{F}_p$ are all relatively prime to $p$. Thus, their product is also relatively prime to $p$. By Theorem 25, we can cancel $(p-1)!$ from both sides of this last equation to obtain the desired result:

$$x^{p-1} \equiv 1 \pmod{p}.$$

□

### 4.5.2 Fermat's Last Theorem as a primality test

If you think about it, you can see that Fermat's Little Theorem gives us a primality test. Recall that if a statement is true, then its contrapositive is also true. Fermat's Little Theorem states that if $p$ is prime, then $a^{p-1} \equiv 1 \pmod{p}$. The contrapositive of this statement is that if $a^{p-1} \not\equiv 1 \pmod{p}$, then $p$ is not prime!

**Example 38.** *We use $a = 2$ and $p = 77$ to show that 77 is not prime:*

$$\begin{aligned} 2^{76} &\equiv 2^6 \times (2^7)^{10} \equiv 2^6 \times 51^{10} \equiv 2^6 \times 60^5 \\ &\equiv 2^6 \times 60 \times 58^2 \equiv 64 \times 60 \times 53 \equiv 9 \pmod{77}. \end{aligned}$$

*We did not end up with 1, so 77 is not prime.*

Notice how we used properties of exponents to simplify the computation considerably.

Unfortunately, the converse of the statement is not true: we can have $a^{m-1} \equiv 1 \pmod{m}$, even when $m$ is not prime and $a \neq 1$. For example, if $m = 341$, then $a^{m-1} \equiv 1$ for 98 elements in $\{2, 3, ..., 341\}$, even though 341 factors as the product of 11 and 31.

**Exercises**

1. Use Fermat's Little Theorem to show that 12 and 1001 are not prime. As a hint, when computing $a^{p-1}$, try to group products so that you minimize the number of multiplications necessary.

## 4.6 Theorems of Fermat, Euler, and Wilson

In this section we present three applications of congruences. The first theorem is Wilson's theorem which states that $(p-1)!+1$ is divisible by $p$, for $p$ prime. Next, we present Fermat's theorem, also known as Fermat's little theorem which states that $a^p$ and $a$ have the same remainders when divided by $p$ where $p \nmid a$. Finally we present Euler's theorem which is a generalization of Fermat's theorem and it states that for any positive integer $m$ that is relatively prime to an integer $a$, $a^{\phi(m)} \equiv 1(mod\, m)$ where $\phi$ is Euler's $\phi$-function. We start by proving a theorem about the inverse of integers modulo primes.

**Theorem 32.** *Let $p$ be a prime. A positive integer $m$ is its own inverse modulo $p$ if and only if $p$ divides $m+1$ or $p$ divides $m-1$.*

*Proof.* Suppose that $m$ is its own inverse. Thus

$$m.m \equiv 1(\bmod p).$$

Hence $p \mid m^2-1$. As a result,

$$p \mid (m-1) \text{or } \ p \mid (m+1).$$

We get that $m \equiv 1(\bmod p)$ or $m \equiv -1(\bmod p)$.

Conversely, suppose that

$$m \equiv 1(\bmod p) \text{or } \ m \equiv -1(\bmod p).$$

Thus

$$m^2 \equiv 1(\bmod p).$$

□

**Theorem 33.** ***Wilson's Theorem*** *If $p$ is a prime number, then $p$ divides $(p-1)!+1$.*

*Proof.* When $p = 2$, the congruence holds. Now let $p > 2$. Using Theorem 26, we see that for each $1 \leq m \leq p$, there is an inverse $1 \leq \bar{m} \leq p$ such that $m\bar{m} \equiv 1(\text{mod } p)$. Thus by Theorem 28, we see that the only two integers that have their own inverses are $1$ and $p - 1$. Hence after coupling the integers from 2 to $p - 2$ each with its inverse, we get

$$2.3.....(p-2) \equiv 1(\text{mod } p).$$

Thus we get

$$1.2.3.....(p-2)(p-1) \equiv (p-1)(\text{mod } p)$$

As a result, we have $(p-1)! \equiv -1(\text{mod } p)$. □

Note also that the converse of Wilson's theorem also holds. The converse tells us whether an integer is prime or not.

**Theorem 34.** *If $m$ is a positive integer with $m \geq 2$ such that*

$$(m-1)! + 1 \equiv 0 \ (\text{mod } m)$$

*then $m$ is prime.*

*Proof.* Suppose that $m$ has a proper divisor $c_1$ and that

$$(m-1)! + 1 \equiv 0(\text{mod } m).$$

That is $m = c_1 c_2$ where $1 < c_1 < m$ and $1 < c_2 < m$. Thus $c_1$ is a divisor of $(m-1)!$. Also, since

$$m \mid ((m-1)! + 1),$$

we get

$$c_1 \mid ((m-1)! + 1).$$

As a result, by Theorem 4, we get that

$$c_1 \mid ((m-1)! + 1 - (m-1)!),$$

which gives that $c_1 \mid 1$. This is a contradiction and hence $m$ is prime. □

We now present Fermat's Theorem or what is also known as Fermat's Little Theorem. It states that the remainder of $a^{p-1}$ when divided by a prime $p$ that doesn't divide $a$ is 1. We then state Euler's theorem which states that the remainder of $a^{\phi(m)}$ when divided by a positive integer $m$ that is relatively prime to $a$ is 1. We prove Euler's Theorem only because Fermat's Theorem is nothing but a special case of Euler's Theorem. This is due to the fact that for a prime number $p$, $\phi(p) = p - 1$.

**Theorem 35.** ***Euler's Theorem*** *If $m$ is a positive integer and $a$ is an integer such that $(a, m) = 1$, then*

$$a^{\phi(m)} \equiv 1(\text{mod } m)$$

**Example 39.** *Note that* $3^4 = 81 \equiv 1(\text{mod } 5)$. *Also,* $2^{\phi(9)} = 2^6 = 64 \equiv 1(\text{mod } 9)$.

We now present the proof of Euler's theorem.

*Proof.* Let $k_1, k_2, ..., k_{\phi(m)}$ be a reduced residue system modulo $m$. By Theorem 25, the set

$$\{ak_1, ak_2, ..., ak_{\phi(m)}\}$$

also forms a reduced residue system modulo $m$. Thus

$$ak_1ak_2...ak_{\phi(m)} = a^{\phi(m)}k_1k_2...k_{\phi(m)} \equiv k_1k_2...k_{\phi(m)}(\text{mod } m).$$

Now since $(k_i, m) = 1$ for all $1 \leq i \leq \phi(m)$, we have $(k_1k_2...k_{\phi(m)}, m) = 1$. Hence by Theorem 22 we can cancel the product of $k$'s on both sides and we get

$$a^{\phi(m)} \equiv 1(\text{mod } m).$$

□

An immediate consequence of Euler's Theorem is:

**Corollary 1.** ***Fermat's Theorem*** *If $p$ is a prime and $a$ is a positive integer with $p \nmid a$, then*

$$a^{p-1} \equiv 1(\text{mod } p).$$

We now present a couple of theorems that are direct consequences of Fermat's theorem. The first states Fermat's theorem in a different way. It says that the remainder of $a^p$ when divided by $p$ is the same as the remainder of $a$ when divided by $p$. The other theorem determines the inverse of an integer $a$ modulo $p$ where $p \nmid a$.

**Theorem 36.** *If $p$ is a prime number and $a$ is a positive integer, then $a^p \equiv a (\bmod p)$.*

*Proof.* If $p \nmid a$, by Fermat's theorem we know that

$$a^{p-1} \equiv 1 (\bmod p).$$

Thus, we get

$$a^p \equiv a (\bmod p).$$

Now if $p \mid a$, we have

$$a^p \equiv a \equiv 0 (\bmod p).$$

□

**Theorem 37.** *If $p$ is a prime number and $a$ is an integer such that $p \nmid a$, then $a^{p-2}$ is the inverse of $a$ modulo $p$.*

*Proof.* If $p \nmid a$, then Fermat's theorem says that

$$a^{p-1} \equiv 1 (\bmod p).$$

Hence

$$a^{p-2} a \equiv 1 (\bmod p).$$

As a result, $a^{p-2}$ is the inverse of $a$ modulo $p$. □

### Exercises

1. Show that 10!+1 is divisible by 11.

2. What is the remainder when $5!25!$ is divided by 31?

3. What is the remainder when $5^{100}$ is divided by 7?

4. Show that if $p$ is an odd prime, then $2(p-3)! \equiv -1(\text{mod } p)$.

5. Find a reduced residue system modulo $2^m$, where $m$ is a positive integer.

6. Show that if $a_1, a_2, ..., a_{\phi(m)}$ is a reduced residue system modulo $m$, where $m$ is a positive integer with $m \neq 2$, then $a_1 + a_2 + ... + a_{\phi(m)} \equiv 0(\text{mod } m)$.

7. Show that if $a$ is an integer such that $a$ is not divisible by 3 or such that $a$ is divisible by 9, then $a^7 \equiv a(\text{mod } 63)$.

# Chapter 5

# Multiplicative Number Theoretic Functions

In this chapter, we study functions, called multiplicative functions, that are defined on integers. These functions have the property that their value at the product of two relatively prime integers is equal to the product of the value of the functions at these integers. We start by proving several theorems about multiplicative functions that we will use later. We then study special functions and prove that the Euler $\phi$-function that was seen before is actually multiplicative. We also define the sum of divisors and the number of divisors functions.

Later define the Mobius function which investigate integers in terms of their prime decomposition. The summatory function of a given function takes the sum of the values of $f$ at the divisors of a given integer $n$. We then determine the Mobius inversion of this function which writes the values of $f$ in terms of the values of its summatory function. We end this chapter by presenting integers with interesting properties and prove some of their properties.

## 5.1 Definitions and Properties

**Definition 19.** *An arithmetic function is a function whose domain of definition is the set $\mathbb{N}$ of positive integers.*

**Definition 20.** *An arithmetic function $f$ is called multiplicative if $f(ab) = f(a)f(b)$ for all $a, b \in \mathbb{N}$ such that $(a, b) = 1$.*

**Definition 21.** *An arithmetic function $f$ is called completely multiplicative if*

$$f(ab) = f(a)f(b) \tag{5.1}$$

*for all positive integers $a, b$.*

**Example 40.** *The function $f(a) = 1$ where $k$ is a completely multiplicative function since*

$$f(ab) = 1 = f(a)f(b).$$

*Notice also that a completely multiplicative function is a multiplicative function but not otherwise.*

We now prove a theorem about multiplicative functions. We will be interested in studying the properties of multiplicative functions rather than the completely multiplicative ones.

**Theorem 38.** *Given a multiplicative function $f$. Let $n = \prod_{k=1}^{s} p_k^{a_k}$ be the prime factorization of $n$. Then*

$$f(n) = \prod_{k=1}^{s} f(p_k^{a_k}).$$

*Proof.* We prove this theorem by induction on the number of primes in the factorization of $n$. Suppose that $n = p_1^{a_1}$. Thus the result follow easily. Suppose now that for

$$n = \prod_{k=1}^{s} p_k^{a_k},$$

we have

$$f(n) = \prod_{k=1}^{s} f(p_k^{a_k}).$$

So we have to prove that if

$$n = \prod_{k=1}^{s+1} p_k^{a_k},$$

then

$$f(n) = \prod_{k=1}^{s+1} f(p_k^{a_k}).$$

Notice that for

$$n = \prod_{k=1}^{s+1} p_k^{a_k},$$

we have $(\prod_{k=1}^{s} p_k^{a_k}, p_{s+1}^{a_{s+1}}) = 1$. Thus we have

$$f(n) = f\left(\prod_{k=1}^{s+1} p_k^{a_k}\right) = f\left(\prod_{k=1}^{s} p_k^{a_k}\right) f\left(p_{s+1}^{a_{s+1}}\right)$$

which by the inductive step gives

$$f\left(\prod_{k=1}^{s+1} p_k^{a_k}\right) = f(n) = \prod_{k=1}^{s+1} f(p_k^{a_k}).$$

□

From the above theorem, we can see that to evaluate a multiplicative function at an integer, it will be enough to know the value of the function at the primes that are in the prime factorization of the number.

We now define summatory functions which represents the sum of the values of a given function at the divisors of a given number.

**Definition 22.** *Let $f$ be an arithmetic function. Define*

$$F(n) = \sum_{d|n} f(d)$$

*Then $F$ is called the summatory function of $f$.*

This function determines the sum of the values of the arithmetic function at the divisors of a given integer.

**Example 41.** *If $f(n)$ is an arithmetic function, then*

$$F(18) = \sum_{d|18} f(d) = f(1) + f(2) + f(3) + f(6) + f(9) + f(18).$$

**Theorem 39.** *If $f$ is a multiplicative function, then the summatory function of $f$ denoted by $F(n) = \sum_{d|n} f(d)$ is also multiplicative.*

*Proof.* We have to prove that $F(mn) = F(m)F(n)$ whenever $(m,n) = 1$. We have

$$F(mn) = \sum_{d|mn} f(d).$$

Notice that by Lemma 6, each divisor of $mn$ can be written uniquely as a product of relatively prime divisors $d_1$ of $m$ and $d_2$ of $n$, moreover the product of any two divisors of $m$ and $n$ is a divisor of $mn$. Thus we get

$$F(mn) = \sum_{d_1|m, d_2|n} f(d_1 d_2)$$

Notice that since $f$ is multiplicative, we have

$$\begin{aligned} F(mn) &= \sum_{d_1|m, d_2|n} f(d_1 d_2) \\ &= \sum_{d_1|m, d_2|n} f(d_1) f(d_2) \\ &= \sum_{d_1|m} f(d_1) \sum_{d_2|n} f(d_2) = F(m)F(n) \end{aligned}$$

□

## Exercises

1. Determine whether the arithmetic functions $f(n) = n!$ and $g(n) = n/2$ are completely multiplicative or not.

2. Define the arithmetic function $g(n)$ by the following. g(n)=1 if $n = 1$ and 0 for $n > 1$. Prove that $g(n)$ is multiplicative.

## 5.2 Multiplicative Number Theoretic Functions

We now present several multiplicative number theoretic functions which will play a crucial role in many number theoretic results. We start by discussing the Euler phi-function which was defined in an earlier chapter. We then define the sum-of-divisors function and the number-of-divisors function along with their properties.

### 5.2.1 The Euler $\phi$-Function

As defined earlier, the Euler $\phi$-function counts the number of integers smaller than and relatively prime to a given integer. We first calculate the value of the $phi$-function at primes and prime powers.

**Theorem 40.** *If $p$ is prime, then $\phi(p) = p - 1$. Conversely, if $p$ is an integer such that $\phi(p) = p - 1$, then $p$ is prime.*

*Proof.* The first part is obvious since every positive integer less than $p$ is relatively prime to $p$. Conversely, suppose that $p$ is not prime. Then $p = 1$ or $p$ is a composite number. If $p = 1$, then $\phi(p) \neq p - 1$. Now if $p$ is composite, then $p$ has a positive divisor. Thus $\phi(p) \neq p - 1$. We have a contradiction and thus $p$ is prime. □

We now find the value of $\phi$ at prime powers.

**Theorem 41.** *Let $p$ be a prime and $m$ a positive integer, then $\phi(p^m) = p^m - p^{m-1}$.*

*Proof.* Note that all integers that are relatively prime to $p^m$ and that are less than $p^m$ are those that are not multiple of $p$. Those integers are $p, 2p, 3p, ..., p^{m-1}p$. There are $p^{m-1}$ of those integers that are not relatively prime to $p^m$ and that are less than $p^m$. Thus

$$\phi(p^m) = p^m - p^{m-1}.$$

□

**Example 42.** $\phi(7^3) = 7^3 - 7^2 = 343 - 49 = 294$. *Also* $\phi(2^{10}) = 2^{10} - 2^9 = 512$.

We now prove that $\phi$ is a multiplicative function.

**Theorem 42.** *Let $m$ and $n$ be two relatively prime positive integers. Then $\phi(mn) = \phi(m)\phi(n)$.*

*Proof.* Denote $\phi(m)$ by $s$ and let $k_1, k_2, ..., k_s$ be a reduced residue system modulo $m$. Similarly, denote $\phi(n)$ by $t$ and let $k'_1, k'_2, ..., k'_t$ be a reduced residue system modulo $n$. Notice that if $x$ belongs to a reduced residue system modulo $mn$, then

$$(x, m) = (x, n) = 1.$$

Thus

$$x \equiv k_i (\bmod\, m) \text{and } \; x \equiv k'_j (\bmod\, n)$$

for some $i, j$. Conversely, if

$$x \equiv k_i (\bmod\, m) \text{and } \; x \equiv k'_j (\bmod\, n)$$

some $i, j$ then $(x, mn) = 1$ and thus $x$ belongs to a reduced residue system modulo $mn$. Thus a reduced residue system modulo $mn$ can be obtained by by determining all $x$ that are congruent to $k_i$ and $k'_j$ modulo $m$ and $n$ respectively. By the Chinese remainder theorem, the system of equations

$$x \equiv k_i (\bmod\, m) \text{and } \; x \equiv k'_j (\bmod\, n)$$

has a unique solution. Thus different $i$ and $j$ will yield different answers. Thus $\phi(mn) = st$. □

We now derive a formula for $\phi(n)$.

**Theorem 43.** *Let $n = p_1^{a_1} p_2^{a_2} ... p_s^{a_s}$ be the prime factorization of $n$. Then*

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) ... \left(1 - \frac{1}{p_s}\right).$$

*Proof.* By Theorem 37, we can see that for all $1 \leq i \leq k$

$$\phi(p_i^{a_i}) = p_i^{a_i} - p_i^{a_i-1} = p_i^{a_i}\left(1 - \frac{1}{p_i}\right).$$

Thus by Theorem 38,

$$\begin{aligned}
\phi(n) &= \phi(p_1^{a_1}p_2^{a_2}...p_s^{a_s}) \\
&= \phi(p_1^{a_1})\phi(p_2^{a_2})...\phi(p_s^{a_s}) \\
&= p_1^{a_1}\left(1-\frac{1}{p_1}\right)p_2^{a_2}\left(1-\frac{1}{p_2}\right)...p_s^{a_s}\left(1-\frac{1}{p_s}\right) \\
&= p_1^{a_1}p_2^{a_2}...p_k^{a_k}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)...\left(1-\frac{1}{p_s}\right) \\
&= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)...\left(1-\frac{1}{p_s}\right).
\end{aligned}$$

□

**Example 43.** *Note that*

$$\phi(200) = \phi(2^3 5^2) = 200\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 80.$$

**Theorem 44.** *Let $n$ be a positive integer greater than 2. Then $\phi(n)$ is even.*

*Proof.* Let $n = p_1^{a_1}p_2^{a_2}...p_k^{a_k}$. Since $\phi$ is multiplicative, then

$$\phi(n) = \prod_{j=1}^{k} \phi(p_j^{a_j}).$$

Thus by Theorem 39, we have

$$\phi(p_j^{a_j}) = p_j^{a_j-1-1}(p_j - 1).$$

We see then $\phi(p_j^{a_j})$is even if $p_j$ is an odd prime. Notice also that if $p_j = 2$, then it follows that $\phi(p_j^{a_j})$ is even. Hence $\phi(n)$ is even. □

**Theorem 45.** *Let $n$ be a positive integer. Then*

$$\sum_{d|n} \phi(d) = n.$$

*Proof.* Split the integers from 1 to $n$ into classes. Put an integer $m$ in the class $C_d$ if the greatest common divisor of $m$ and $n$ is $d$. Thus the number of integers in the $C_d$ class is the number of positive integers not exceeding $n/d$ that are relatively prime to n/d. Thus we have $\phi(n/d)$ integers in $C_d$. Thus we see that

$$n = \sum_{d|n} \phi(n/d).$$

As $d$ runs over all divisors of $n$, so does $n/d$. Hence

$$n = \sum_{d|n} \phi(n/d) = \sum_{d|n} \phi(d).$$

□

### 5.2.2 The Sum-of-Divisors Function

The sum of divisors function, denoted by $\sigma(n)$, is the sum of all positive divisors of $n$.

**Example 44.** $\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28$.

Note that we can express $\sigma(n)$ as $\sigma(n) = \sum_{d|n} d$.

We now prove that $\sigma(n)$ is a multiplicative function.

**Theorem 46.** *The sum of divisors function $\sigma(n)$ is multiplicative.*

*Proof.* We have proved in Theorem 35 that the summatory function is multiplicative once $f$ is multiplicative. Thus let $f(n) = n$ and notice that $f(n)$ is multiplicative. As a result, $\sigma(n)$ is multiplicative. □

Once we found out that $\sigma(n)$ is multiplicative, it remains to evaluate $\sigma(n)$ at powers of primes and hence we can derive a formula for its values at any positive integer.

**Theorem 47.** *Let $p$ be a prime and let $n = p_1^{a_1}p_2^{a_2}...p_t^{a_t}$ be a positive integer. Then*

$$\sigma(p^a) = \frac{p^{a+1}-1}{p-1},$$

*and as a result,*

$$\sigma(n) = \prod_{j=1}^{t} \frac{p_j^{a_j+1}-1}{p_j-1}$$

*Proof.* Notice that the divisors of $p^a$ are $1, p, p^2, ..., p^a$. Thus

$$\sigma(p^a) = 1 + p + p^2 + ... + p^a = \frac{p^{a+1}-1}{p-1}.$$

where the above sum is the sum of the terms of a geometric progression.

Now since $\sigma(n)$ is multiplicative, we have

$$\begin{aligned}
\sigma(n) &= \sigma(p^{a_1})\sigma(p^{a_2})...\sigma(p^{a_t}) \\
&= \frac{p_1^{a_1+1}-1}{p_1-1}.\frac{p_2^{a_2+1}-1}{p_2-1}...\frac{p_t^{a_t+1}-1}{p_t-1} \\
&= \prod_{j=1}^{t} \frac{p_j^{a_j+1}-1}{p_j-1}
\end{aligned}$$

□

**Example 45.** $\sigma(200) = \sigma(2^3 5^2) = \frac{2^4-1}{2-1}\frac{5^3-1}{5-1} = 15.31 = 465.$

### 5.2.3 The Number-of-Divisors Function

The number of divisors function, denoted by $\tau(n)$, is the sum of all positive divisors of $n$.

**Example 46.** $\tau(8) = 4.$

We can also express $\tau(n)$ as $\tau(n) = \sum_{d|n} 1$.

We can also prove that $\tau(n)$ is a multiplicative function.

**Theorem 48.** *The number of divisors function $\tau(n)$ is multiplicative.*

*Proof.* By Theorem 36, with $f(n) = 1$, $\tau(n)$ is multiplicative. □

We also find a formula that evaluates $\tau(n)$ for any integer $n$.

**Theorem 49.** *Let $p$ be a prime and let $n = p_1^{a_1} p_2^{a_2} ... p_t^{a_t}$ be a positive integer. Then*

$$\tau(p^a) = a + 1,$$

*and as a result,*

$$\tau(n) = \prod_{j=1}^{t} (a_j + 1).$$

*Proof.* The divisors of $p^a$ as mentioned before are $1, p, p^2, ..., p^a$. Thus

$$\tau(p^a) = a + 1$$

Now since $\tau(n)$ is multiplicative, we have

$$\begin{aligned} \tau(n) &= \tau(p^{a_1})\tau(p^{a_2})...\tau(p^{a_t}) \\ &= (a_1 + 1)(a_2 + 1)...(a_t + 1) \\ &= \prod_{j=1}^{t} (a_j + 1). \end{aligned}$$

□

**Example 47.** $\tau(200) = \tau(2^3 5^2) = (3 + 1)(2 + 1) = 12$.

**Exercises**

1. Find $\phi(256)$ and $\phi(2.3.5.7.11)$.

2. Show that $\phi(5186) = \phi(5187)$.

3. Find all positive integers $n$ such that $\phi(n) = 6$.

4. Show that if $n$ is a positive integer, then $\phi(2n) = \phi(n)$ if $n$ is odd.

5. Show that if $n$ is a positive integer, then $\phi(2n) = 2\phi(n)$ if $n$ is even.

6. Show that if $n$ is an odd integer, then $\phi(4n) = 2\phi(n)$.

7. Find the sum of positive integer divisors and the number of positive integer divisors of 35

8. Find the sum of positive integer divisors and the number of positive integer divisors of $2^5 3^4 5^3 7^3 13$.

9. Which positive integers have an odd number of positive divisors.

10. Which positive integers have exactly two positive divisors.

## 5.3 The Mobius Function and the Mobius Inversion Formula

We start by defining the Mobius function which investigates integers in terms of their prime decomposition. We then determine the Mobius inversion formula which determines the values of the a function $f$ at a given integer in terms of its summatory function.

**Definition 23.** $\mu(n) = \begin{cases} 1 \ \textit{if} \ n = 1; \\ (-1)^t \ \textit{if} \ n = p_1 p_2 ... p_t \ \textit{where the} \ p_i \ \textit{are distinct primes}; \\ 0 \ \textit{otherwise}. \end{cases}$

Note that if $n$ is divisible by a power of a prime higher than one then $\mu(n) = 0$. In connection with the above definition, we have the following

**Definition 24.** *An integer $n$ is said to be* **square-free, if no square divides it, i.e. if there does not exist an integer $k$ such that $k^2 \mid n$.**

It is immediate (prove as exercise) that the prime-number factorization of a square-free integer contains only distinct primes.

**Example 48.** *Notice that $\mu(1) = 1$, $\mu(2) = -1$, $\mu(3) = -1$ and $\mu(4) = 0$.*

We now prove that $\mu(n)$ is a multiplicative function.

**Theorem 50.** *The Mobius function $\mu(n)$ is multiplicative.*

*Proof.* Let $m$ and $n$ be two relatively prime integers. We have to prove that

$$\mu(mn) = \mu(m)\mu(n).$$

If $m = n = 1$, then the equality holds. Also, without loss of generality, if $m = 1$, then the equality is also obvious. Now suppose that $m$ or $n$ is divisible by a power of prime higher than 1, then

$$\mu(mn) = 0 = \mu(m)\mu(n).$$

What remains to prove that if $m$ and $n$ are square-free integers say $m = p_1 p_2 ... p_s$ where $p_1, p_2, ..., p_s$ are distinct primes and $n = q_1 q_2 ... q_t$ where $q_1, q_2, ..., q_t$. Since $(m, n) = 1$, then there are no common primes in the prime decomposition between $m$ and $n$. Thus

$$\mu(m) = (-1)^s, \mu(n) = (-1)^t \text{and } \mu(mn) = (-1)^{s+t}.$$

□

In the following theorem, we prove that the summatory function of the Mobius function takes only the values 0 or 1.

**Theorem 51.** *Let $F(n)=\sum_{d|n}\mu(d)$, then $F(n)$ satisfies*

$$F(n)=\begin{cases} 1 \text{ if } n=1; \\ 0 \text{ if } n>1. \end{cases}$$

*Proof.* For $n=1$, we have $F(1)=\mu(1)=1$. Let us now find $\mu(p^k)$ for any integer $k>0$. Notice that

$$F(p^k)=\mu(1)+\mu(p)+...+\mu(p^k)=1+(-1)+0+...+0=0$$

Thus by Theorem 36, for any integer $n=p_1^{a_1}p_2^{a_2}...p_t^{a_t}>1$ we have,

$$F(n)=F(p_1^{a_1})F(p_2^{a_2})...F(p_t^{a_t})=0$$

□

We now define the Mobius inversion formula. The Mobius inversion formula expresses the values of $f$ in terms of its summatory function of $f$.

**Theorem 52.** *Suppose that $f$ is an arithmetic function and suppose that $F$ is its summatory function, then for all positive integers $n$ we have*

$$f(n)=\sum_{d|n}\mu(d)F(n/d).$$

*Proof.* We have

$$\begin{aligned}\sum_{d|n}\mu(d)F(n/d) &= \sum_{d|n}\mu(d)\sum_{e|(n/d)}f(e) \\ &= \sum_{d|n}\sum_{e|(n/d)}\mu(d)f(e) \\ &= \sum_{e|n}\sum_{d|(n/e)}\mu(d)f(e) \\ &= \sum_{e|n}f(e)\sum_{d|(n/d)}\mu(d)\end{aligned}$$

Notice that $\sum_{d|(n/e)} \mu(d) = 0$ unless $n/e = 1$ and thus $e = n$. Consequently we get

$$\sum_{e|n} f(e) \sum_{d|(n/d)} \mu(d) = f(n).1 = f(n).$$

□

**Example 49.** *A good example of a Mobius inversion formula would be the inversion of $\sigma(n)$ and $\tau(n)$. These two functions are the summatory functions of $f(n) = n$ and $f(n) = 1$ respectively. Thus we get*

$$n = \sum_{d|n} \mu(n/d)\sigma(d)$$

*and*

$$1 = \sum_{d|n} \mu(n/d)\tau(d).$$

**Exercises**

1. Find $\mu(12)$, $\mu(10!)$ and $\mu(105)$.

2. Find the value of $\mu(n)$ for each integer $n$ with $100 \leq n \leq 110$.

3. Use the Mobius inversion formula and the identity $n = \sum_{d|n} \phi(n/d)$ to show that $\phi(p^t) = p^t - p^{t-1}$ where $p$ is a prime and $t$ is a positive integer.

## 5.4 Perfect, Mersenne, and Fermat Numbers

Integers with certain properties were studied extensively over the centuries. We present some examples of such integers and prove theorems related to these integers and their properties.

We start by defining perfect numbers.

**Definition 25.** *A positive integer $n$ is called a perfect number if $\sigma(n) = 2n$.*

In other words, a perfect number is a positive integer which is the sum of its proper divisors.

**Example 50.** *The first perfect number is 6, since $\sigma(6) = 12$. You can also view this as $6 = 1 + 2 + 3$. The second perfect number is 28, since $\sigma(28) = 56$ or $28 = 1 + 2 + 4 + 7 + 14$.*

The following theorem tells us which even positive integers are perfect.

**Theorem 53.** *The positive integer $n$ is an even perfect number if and only if*

$$n = 2^{l-1}(2^l - 1),$$

*where $l$ is an integer such that $l \geq 2$ and $2^l - 1$ is prime.*

*Proof.* We show first that if $n = 2^{l-1}(2^l - 1)$ where $l$ is an integer such that $l \geq 2$ and $2^l - 1$ is prime then $n$ is perfect. Notice that $2^l - 1$ is odd and thus $(2^{l-1}, 2^l - 1) = 1$. Also, notice that $\sigma$ is a multiplicative function and thus

$$\sigma(n) = \sigma(2^{l-1})\sigma(2^l - 1).$$

Notice that $\sigma(2^{l-1}) = 2^l - 1$ and since $2^l - 1$ is prime we get $\sigma(2^l - 1) = 2^l$. Thus

$$\sigma(n) = 2n.$$

We now prove the converse. Suppose that $n$ is a perfect number. Let $n = 2^r s$, where $r$ and $s$ are positive integers and $s$ is odd. Since $(2^r, s) = 1$, we get

$$\sigma(n) = \sigma(2^r)\sigma(s) = (2^{r+1} - 1)\sigma(s).$$

Since $n$ is perfect, we get

$$(2^{r+1} - 1)\sigma(s) = 2^{r+1}s.$$

Notice now that $(2^{r+1} - 1, 2^{r+1}) = 1$ and thus $2^{r+1} \mid \sigma(s)$. Therefore there exists an integer $q$ such that $\sigma(s) = 2^{r+1}q$. As a result, we have

$$(2^{r+1} - 1)2^{r+1}q = 2^{r+1}s$$

and thus we get

$$(2^{r+1}-1)q = s$$

So we get that $q \mid s$. We add $q$ to both sides of the above equation and we get

$$s+q = (2^{r+1}-1)q + q = 2^{r+1}q = \sigma(s).$$

We have to show now that $q = 1$. Notice that if $q \neq 1$, then $s$ will have three divisors and thus $\sigma(s) \geq 1 + s + q$. Hence $q = 1$ and as a result $s = 2^{r+1} - 1$. Also notice that $\sigma(s) = s + 1$. This shows that $s$ is prime since the only divisors of $s$ are $1$ and $s$. As a result,

$$n = 2^r(2^{r+1}-1),$$

where $(2^{r+1}-1)$ is prime. □

In theorem 50, we see that to determine even perfect numbers, we need to find primes of the form $2^\ell - 1$. It is still unknown whether there are odd perfect numbers or not.

**Theorem 54.** *If $2^\ell - 1$ is prime where $\ell$ is a positive integer, then $\ell$ must be prime.*

*Proof.* Suppose that $\ell$ is composite, that is $\ell = rs$ where $1 < r < \ell$ and $1 < s < \ell$. Thus after factoring, we get that

$$2^\ell - 1 = (2^r - 1)(2^{r(s-1)} + 2^{r(s-2)} + ... + 2^r + 1)$$

Notice that the two factors above are both greater than 1. Thus $2^\ell - 1$ is not prime. This is a contradiction. □

The above theorem motivates the definition of interesting numbers called Mersenne numbers.

**Definition 26.** *Let $\ell$ be a positive integer. An integer of the form $M_\ell = 2^\ell - 1$ is called the $\ell$th Mersenne number; if $\ell$ is prime then $M_\ell = 2^\ell - 1$ is called the $\ell$th Mersenne prime.*

**Example 51.** $M_3 = 2^3 - 1 = 7$ *is the third Mersenne prime.*

We prove a theorem that help decide whether Mersenne numbers are prime.

**Theorem 55.** *Divisors of* $M_p = 2^p - 1$ *for prime* $p$ *is of the form* $2mp + 1$*, where* $m$ *is a positive integer.*

*Proof.* Let $p_1$ be a prime dividing $M_p = 2^p - 1$. By Fermat's theorem, we know that $p_1 \mid (2^{p_1-1} - 1)$. Also, it is easy to see that

$$(2^p - 1, 2^{p_1-1} - 1) = 2^{(p,p_1-1)} - 1.$$

Since $p_1$ is a common divisor of $2^p - 1$ and $2^{p_1-1} - 1$ and thus not relatively prime. Hence $(p, p_1 - 1) = p$. Hence $p \mid (p_1 - 1)$ and thus there exists a positive integer $k$ such that $p_1 - 1 = kp$. Since $p_1$ is odd, then $k$ is even and thus $k = 2m$. Hence

$$p_1 = kp + 1 = 2mp + 1.$$

Because any divisor of $M_p$ is a product of prime divisors of $M_p$, each prime divisor of $M_p$ is of the form $2mp + 1$ and the result follows. □

**Example 52.** $M_{23} = 2^{23} - 1$ *is divisible by* $47 = 46k + 1$*. We know this by trial and error and thus looking at all primes of the form* $46k + 1$ *that are less than* $\sqrt{M_{23}}$.

We now define Fermat numbers and prove some theorems about the properties of these numbers.

**Definition 27.** *Integers of the form* $F_n = 2^{2^n} + 1$ *are called Fermat numbers.*

Fermat conjectured that these integers are primes but it turned out that this is not true. Notice that $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ and $F_4 = 65,537$ while $F_5$ is composite. It turned out the $F_5$ is divisible by 641. We now present a couple of theorems about the properties of these numbers.

**Theorem 56.** *For all positive integers $n$, we have*

$$F_0F_1F_2...F_{n-1} = F_n - 2$$

*Proof.* We will prove this theorem by induction. For $n = 1$, the above identity is true. Suppose now that

$$F_0F_1F_2...F_{n-1} = F_n - 2$$

holds. We claim that

$$F_0F_1F_2...F_n = F_{n+1} - 2.$$

Notice that

$$F_0F_1F_2...F_n = (F_n - 2)F_n = (2^{2^n} - 1)(2^{2^n} + 1) = 2^{2^{n+1}} - 1 = F_{n+1} - 2.$$

□

Using Theorem 53, we prove that Fermat numbers are relatively prime.

**Theorem 57.** *Let $s \neq t$ be nonnegative integers. Then $(F_s, F_t) = 1$.*

*Proof.* Assume without loss of generality that $s < t$. Thus by Theorem 52, we have

$$F_0F_1F_2...F_s...F_{t-1} = F_t - 2$$

Assume now that there is a common divisor $d$ of $F_s$ and $F_t$. thus we see that $d$ divides

$$F_t - F_0F_1F_2...F_s...F_{t-1} = 2.$$

Thus $d = 1$ or $d = 2$. But since $F_t$ is odd for all $t$. We have $d = 1$. Thus $F_s$ and $F_t$ are relatively prime. □

### Exercises

1. Find the six smallest even perfect numbers.

2. Find the eighth perfect number.

3. Find a factor of $2^{1001} - 1$.

4. We say $n$ is abundant if $\sigma(n) > 2n$. Prove that if $n = 2^{m-1}(2^m - 1)$ where $m$ is a positive integer such that $2^m - 1$ is composite, then $n$ is abundant.

5. Show that there are infinitely many even abundant numbers.

6. Show that there are infinitely many odd abundant numbers.

7. Determine whether $M_{11}$ is prime.

8. Determine whether $M_{29}$ is prime.

9. Find all primes of the form $2^{2^n} + 5$ where $n$ is a nonnegative integer.

# Chapter 6

# Primitive Roots and Quadratic Residues

In this chapter, we discuss the multiplicative structure of the integers modulo $n$. We introduce the concept of the order of integer modulo $n$ and then we study its properties. We then define primitive roots modulo $n$ and show how to determine whether an integer is primitive modulo $n$ or not. We later find all positive integers having primitive roots and prove related results.

We define the concept of a quadratic residue and establish its basic properties. We then introduce Legendre symbol and also develop its basic properties. We also introduce the law of quadratic reciprocity. Afterwards, we generalize the notion of Legendre symbol to the Jacobi symbol and discuss the law of reciprocity related to Jacobi symbol.

## 6.1 The order of Integers and Primitive Roots

In this section, we study the order of an integer modulo $n$, where $n$ is positive. We also define primitive roots and related results. Euler's theorem in Chapter 4 states that if a positive integer $a$ is relatively prime to $n$, then $a^{\phi(n)} \equiv 1(\mathrm{mod}\ n)$. Thus by the well ordering principle, there is a least positive integer $x$ that satisfies this congruence $a^x \equiv 1 (\bmod n)$.

**Definition 1.** *Let $(a, b) = 1$. The smallest positive integer $x$ such that $a^x \equiv 1(\bmod b)$ is called the order of $a$ modulo $b$. We denote the order of $a$ modulo $b$ by $ord_b a$.*

**Example 53.** *$ord_7 2 = 3$ since $2^3 \equiv 1(\bmod 7)$ while $2^1 \equiv 2(\bmod 7)$ and $2^2 \equiv 4(\bmod 7)$.*

To find all integers $x$ such that $a^x \equiv 1(\bmod b)$, we need the following theorem.

**Theorem 58.** *If $(a, b) = 1$ with $b > 0$, then the positive integer $x$ is a solution of the congruence $a^x \equiv 1(\bmod b)$ if and only if $ord_b a \mid x$.*

*Proof.* Having $ord_b a \mid x$, then we have that $x = k.ord_b a$ for some positive integer $k$. Thus

$$a^x = a^{kord_b a} = (a^{ord_b a})^k \equiv 1(\bmod b).$$

Now if $a^x \equiv 1(\bmod b)$, we use the division algorithm to write

$$x = qord_b a + r, \quad 0 \leq r < ord_b a.$$

Thus we see that

$$a^x \equiv a^{qord_b a + r} \equiv (a^{ord_b a})^q a^r \equiv a^r (\bmod b).$$

Now since $a^x \equiv 1(\bmod b)$,we have $a^r \equiv 1(\bmod b)$. Since $ord_b a$, we get $r = 0$. Thus $x = q.ord_b a$ and hence $ord_b a \mid x$. □

**Example 54.** *Since $ord_7 2 = 3$, then $2^{15} \equiv 1(\bmod 7)$ while 10 is not a solution for $2^x \equiv 1(\bmod 7)$.*

**Theorem 59.** *If $(a, b) = 1$ with $b > 0$, then*

$$a^i \equiv a^j (\bmod b)$$

*where $i$ and $j$ are nonnegative integers, if and only if*

$$i \equiv j (\text{mod } ord_b a)$$

*Proof.* Suppose that

$$i \equiv j (\text{mod } ord_b a) \text{ and } 0 \leq j \leq i.$$

Then we have $i - j = k.ord_b a$, where $k$ is a positive integer. Hence

$$a^i = a^{j+k.ord_b a} = a^j (a^{ord_b a})^k \equiv a^j (\text{mod } b).$$

Assume now that $a^i \equiv a^j (\text{mod } b)$ with $i \geq j$. Thus we have

$$a^i \equiv a^j a^{i-j} \equiv a^j (\text{mod } b)$$

Since $(a, b) = 1$, we have $(a^j, b) = 1$ and thus by Theorem 22, we get

$$a^{i-j} \equiv 1 (\text{mod } b).$$

By theorem 54, we get that $ord_b a \mid (i - j)$ and hence $i \equiv j (\text{mod } b)$.

□

We introduce now primitive roots and discuss their properties. We are interested in integers whose order modulo another integer is $\phi(b)$. In one of the exercises, one is asked to prove that if $a$and $b$ are relatively prime then $ord_b a \mid \phi(b)$.

**Definition 2.** *If $(r, m) = 1$ with $m > 0$ and if $ord_m r = \phi(m)$ then $r$ is called a primitive root modulo $m$.*

**Example 55.** *Notice that $\phi(7) = 6$ hence $2$ is not a primitive root modulo $7$. While $ord_7 3 = 6$ and thus $3$ is a primitive root modulo $7$.*

**Theorem 60.** *If $(r, m) = 1$ with $m > 0$ and if $r$ is a primitive root modulo $n$, then the integers $\{r^1, r^2, ...r^{\phi(m)}\}$ form a reduced residue set modulo $m$.*

*Proof.* To prove that the set $\{r^1, r^2, ...r^{\phi(m)}\}$ form a reduced residue set modulo $m$ we need to show that every two of them are relatively prime and that no two of them are congruent modulo $m$. Since $(r, m) = 1$, it follows that $(r^n, m) = 1$ for all positive integers $n$. Hence all the powers of $r$ are relatively prime to $m$. To show that no two powers in the above set are equivalent modulo $m$, assume that

$$r^i \equiv r^j (\bmod m).$$

By Theorem 55, we see that

$$i \equiv j (\bmod ord_m \phi(m)).$$

Notice that $1 \leq i, j \leq \phi(m)$ and hence $i = j$. □

**Theorem 61.** *If* $ord_m a = t$ *and if* $u$ *is a positive integer, then*

$$ord_m(a^u) = t/(t, u).$$

*Proof.* Let

$$v = ord_m(a^u), \;\; w = (t, u), \;\; t = t_1 w \text{and } \; u = u_1 w.$$

Notice that $(t_1, u_1) = 1$.

Because $t_1 = t/(t, u)$, we want to show that $ord_m(a^u) = t_1$. To do this, we will show that $(a^u)^{t_1} \equiv 1(\bmod m)$ and that if $(a^u)^v \equiv 1(\bmod m)$, then $t_1 \mid v$. First note that

$$(a^u)^{t_1} = (a^{u_1 w})^{(t/w)} = (a^t)^{u_1} \equiv 1(\bmod m).$$

Hence by Theorem 54, we have $v \mid t_1$. Now on the other hand, since

$$(a^u)^v = a^{uv} \equiv 1(\bmod m),$$

we know that $t \mid uv$. Hence $t_1 w \mid u_1 w v$ and hence $t_1 \mid u_1 v$. Because $(t_1, u_1) = 1$, we see that $t_1 \mid v$. Since $v \mid t_1$ and $t_1 \mid v$, we conclude that $v = t_1 = t/w = t/(t, u)$. □

**Example 56.** *We see that $ord_7 3^4 = 6/(6,4)$ since $ord_7 3 = 6$.*

**Corollary 2.** *Let $r$ be a primitive root modulo $m$, where $m$ is a positive integer, $m > 1$. Then $r^u$ is a primitive root modulo $m$ if and only if $(u, \phi(m)) = 1$.*

*Proof.* By Theorem 57, we see that

$$ord_m r^u = ord_m r/(u, ord_m r) = \phi(m)/(u, \phi(m)).$$

Thus $ord_m r^u = \phi(m)$ and $r^u$ is a primitive root if and only if $(u, \phi(m)) = 1$. □

The above corollary leads to the following theorem

**Theorem 62.** *If the positive integer $m$ has a primitive root, then it has a total of $\phi(\phi(m))$ incongruent primitive roots.*

*Proof.* Let $r$ be a primitive root modulo $m$. By Theorem 56, we see that $\{r^1, r^2, ..., r^{\phi(m)}\}$ form a reduced residue system modulo $n$. By Corollary 1, it is known that $r^u$ is a primitive root modulo $m$ if and only if $(u, \phi(m)) = 1$. Thus we have exactly $\phi(\phi(m))$ such integers $u$ that are relatively prime to $\phi(m)$ and hence there are exactly $\phi(\phi(m))$ primitive roots modulo $m$. □

### Exercises

1. Determine $ord_{13} 10$.

2. Determine $ord_{11} 3$.

3. Show that 5 is a primitive root of 6.

4. Show that if $\bar{a}$ is an inverse of $a$ modulo $n$, then $ord_n a = ord_n \bar{a}$.

5. Show that if $n$ is a positive integer, and $a$ and $b$ are integers relatively prime to $n$ such that $(ord_n a, ord_n b) = 1$, then $ord_n(ab) = ord_n a.ord_n b$.

6. Show that if $a$ is an integer relatively prime to the positive integer $m$ and $ord_m a = st$, then $ord_m a^t = s$.

7. Show that if $a$ and $n$ are relatively prime with $n > 0$, then $ord_n a \mid \phi(n)$.

## 6.2 Primitive Roots for Primes

In this section, we show that every integer has a primitive root. To do this we need to introduce polynomial congruence.

Let $f(x)$ be a polynomial with integer coefficients. We say that an integer $a$ is a root of $f(x)$ modulo $m$ if $f(a) \equiv 0 (\bmod\, m)$.

**Example 57.** *Notice that* $x \equiv 3 (\bmod\, 11)$ *is a root for* $f(x) = 2x^2 + x + 1$ *since* $f(3) = 22 \equiv 0 (\bmod\, 11)$.

We now introduce Lagrange's theorem for primes. This is modulo p, the fundamental theorem of algebra. This theorem will be an important tool to prove that every prime has a primitive root.

**Theorem 63.** ***Lagrange's Theorem*** *Let*

$$m(x) = b_n x^n + b_{n-1} x^{n-1} + ... + b_1 x + b_0$$

*be a polynomial of degree* $n, n \geq 1$ *with integer coefficients and with leading coefficient* $b_n$ *not divisible by a prime* $p$*. Then* $m(x)$ *has at most* $n$ *distinct incongruent roots modulo* $p$*.*

*Proof.* Using induction, notice that if $n = 1$, then we have

$$m(x) = b_1 x + b_0 \text{ and } p \nmid b_1.$$

A root of $m(x)$ is a solution for $b_1 x + b_0 (\bmod\, p)$. Since $p \nmid b_1$, then this congruence has exactly one solution by Theorem 26.

Suppose that the theorem is true for polynomials of degree $n - 1$, and let $m(x)$ be a polynomial of degree $n$ with integer coefficients and where the leading coefficient is not divisible by $p$. Assume now that $m(x)$ has $n + 1$ incongruent roots modulo $p$, say $x_0, x_1, ..., x_n$. Thus

$$m(x_k) \equiv 0 (\bmod\, p)$$

for $0 \leq k \leq n$. Thus we have

$$\begin{aligned} m(x) - m(x_0) &= b_n(x^n - x_0^n) + b_{n-1}(x^{n-1} - x_0^{n-1}) + ... + b_1(x - x_0) \\ &= b_n(x - x_0)(x^{n-1} + x^{n-2}x_0 + ... + xx_0^{n-2} + x_0^{n-1}) \\ &+ b_{n-1}(x - x_0)(x^{n-2} + x^{n-3}x_0 + ... + xx_0^{n-3} + x_0^{n-2}) + ... + b_1(x - c_0) \\ &= (x - x_0)f(x) \end{aligned}$$

where $f(x)$ is a polynomial of degree $n - 1$ with leading coefficient $b_n$. Notice that since $m(x_k) \equiv m(x_0)(\text{mod } p)$, we have

$$m(x_k) - m(x_0) = (x_k - x_0)f(x_k) \equiv 0(\text{mod } p).$$

Thus $f(x_k) \equiv 0(\text{mod } p)$ for all $1 \leq k \leq n$ and thus $x_1, x_2, ..., x_n$ are roots of $f(x)$. This is a contradiction since we a have a polynomial of degree $n - 1$ that has $n$ distinct roots. □

We now use Lagrange's Theorem to prove the following result.

**Theorem 64.** *Consider the prime $p$ and let $p - 1 = kn$ for some integer $k$. Then $x^n - 1$ has exactly $n$ incongruent roots modulo $p$.*

*Proof.* Since $p - 1 = kn$, we have

$$\begin{aligned} x^{p-1} - 1 &= (x^n - 1)(x^{n(k-1)} + x^{n(k-2)} + ... + x^n + 1) \\ &= (x^n - 1)f(x) \end{aligned}$$

By Fermat's little theorem, we know that $x^{p-1} - 1$ has $p - 1$ incongruent roots modulo $p$. Also, roots of $x^{p-1} - 1$ are roots of $f(x)$ or a root of $x^n - 1$. Notice that by Lagrange's Theorem, we have that $f(x)$ has at most $p - n - 1$ roots modulo $p$. Thus $x^n - 1$ has at least $n$ roots modulo $p$. But again by Lagrange's Theorem, since we have that $x^n - 1$ has at most $n$ roots, thus we get that $x^n - 1$ has exactly $n$ incongruent roots modulo $p$. □

We now prove a lemma that gives us how many incongruent integers can have a given order modulo $p$.

**Lemma 12.** *Let $p$ be a prime and let $m$ be a positive integer such that $p-1 = mk$ for some integer $k$. Then*

$$S(m) = |\{m : 0 < m < p, \;\; m \in \mathbb{Z}\}| \leq \phi(m).$$

*Proof.* For each positive integer $m$ dividing $p-1$,

Notice that if $S(m) = 0$, then $S(m) \leq \phi(m)$. If $S(m) > 0$, then there is an integer $a$ of order $m$ modulo $p$. Since $ord_p a = m$, then $a, a^2, ...a^m$ are incongruent modulo $p$. Also each power of $a$ is a root of $x^m - 1$ modulo $p$ because

$$(a^k)^m = (a^m)^k \equiv 1 (\text{mod}\, p)$$

for all positive integers $k$. By Theorem 60, we know that $x^m - 1$ has exactly $m$ incongruent roots modulo $p$, so that every root is congruent to one of these powers of $a$. We also know by Theorem 57 that the powers of $a^k$ with $(k, m) = 1$ have order $m$. There are exactly $\phi(m)$ such integers with $1 \leq k \leq m$ and thus if there is one element of order $m$ modulo $p$, there must be exactly $\phi(m)$ such positive integers less than $p$. Hence $S(m) \leq \phi(m)$. □

In the following theorem, we determine how many incongruent integers can have a given order modulo $p$. We actually show the existence of primitive roots for prime numbers.

**Theorem 65.** *Every prime number has a primitive root.*

*Proof.* Let $p$ be a prime and let $m$ be a positive integer such that $p - 1 = mk$ for some integer $k$. Let $F(m)$ be the number of positive integers of order $m$ modulo $p$ that are less than $p$. The order modulo $p$ of an integer not divisible by $p$ divides $p - 1$, it follows that

$$p - 1 = \sum_{m|p-1} F(m).$$

By Theorem 42, we see that

$$p-1=\sum_{m|p-1}\phi(m).$$

By Lemma 1, $F(m)\leq\phi(m)$ when $m\mid(p-1)$. Together with

$$\sum_{m|p-1}F(m)=\sum_{m|p-1}\phi(m)$$

we see that $F(m)=\phi(m)$ for each positive divisor $m$ of $p-1$. Thus we conclude that $F(m)=\phi(m)$. As a result, we see that there are $p-1$ incongruent integers of order $p-1$ modulo $p$. Thus $p$ has $\phi(p-1)$ primitive roots. □

**Exercises**

1. Find the incongruent roots modulo 11 of $x^2+2$.
2. Find the incongruent roots modulo 11 of $x^4+x^2+1$.
3. Find the incongruent roots modulo 13 of $x^3+12$.
4. Find the number of primitive roots of 13 and of 47.
5. Find a complete set of incongruent primitive roots of 13.
6. Find a complete set of incongruent primitive roots of 17.
7. Find a complete set of incongruent primitive roots of 19.
8. Let $r$ be a primitive root of $p$ with $p\equiv 1(\text{mod } 4)$. Show that $-r$ is also a primitive root.
9. Show that if $p$ is a prime and $p\equiv 1(mod\ 4)$, then there is an integer $x$ such that $x^2\equiv -1(\text{mod } p)$.

## 6.3 The Existence of Primitive Roots

In this section, we demonstrate which integers have primitive roots. We start by showing that every power of an odd prime has a primitive root and to do this we start by showing that every square of an odd prime has a primitive root.

**Theorem 66.** *If $p$ is an odd prime with primitive root $r$, then one can have either $r$ or $r+p$ as a primitive root modulo $p^2$.*

*Proof.* Notice that since $r$ is a primitive root modulo $p$, then

$$ord_p r = \phi(p) = p-1.$$

Let $m = ord_{p^2} r$, then

$$r^m \equiv 1 (\bmod p^2).$$

Thus

$$r^m \equiv 1 (\bmod p).$$

By Theorem 54, we have

$$p-1 \mid m.$$

By Exercise 7 of section 6.1, we also have that

$$m \mid \phi(p^2).$$

Also, $\phi(p^2) = p(p-1)$ and thus $m$ either divides $p$ or $p-1$. And since $p-1 \mid m$ then we have

$$m = p-1 \text{ or } m = p(p-1).$$

If $m = p(p-1)$ and $ord_{p^2} r = \phi(p^2)$ then $r$ is a primitive root modulo $p^2$. Otherwise, we have $m = p-1$ and thus

$$r^{p-1} \equiv 1 (\bmod p^2).$$

Let $s = r + p$. Then $s$ is also a primitive root modulo $p$. Hence, $ord_{p^2}s$ equals either $p-1$ or $p(p-1)$. We will show that $ord_{p^2}s \neq p-1$ so that $ord_{p^2}s = p(p-1)$. Note that

$$\begin{aligned} s^{p-1} = (r+p)^{p-1} &= r^{p-1} + (p-1)r^{p-2}p + ... + p^{p-1} \\ &= r^{p-1} + (p-1)p.r^{p-2}(\bmod p^2). \end{aligned}$$

Hence

$$p^2 \mid s^{p-1} - (1 - pr^{p-2}.$$

Note also that if

$$p^2 \mid (s^{p-1} - 1),$$

then

$$p^2 \mid pr^{p-2}.$$

Thus we have

$$p \mid r^{p-2}$$

which is impossible because $p \nmid r$. Because $ord_{p^2}s \neq p-1$, we can conclude that

$$ord_{p^2}s = p(p-1) = \phi(p^2).$$

Thus, $s = r + p$ is a primitive root of $p^2$. □

**Example 58.** *Notice that 7 has 3 as a primitive root. Either $ord_{49}3 = 6$ or $ord_{49}3 = 42$. But since $3^6 \not\equiv 1(\text{mod } 49)$. Hence $ord_{49}3 = 42$. Hence 3 is a primitive root of 49.*

We now show that any power of an odd prime has a primitive root.

**Theorem 67.** *Let $p$ be an odd prime. Then any power of $p$ is a primitive root. Moreover, if $r$ is a primitive root modulo $p^2$, then $r$ is a primitive root modulo $p^m$ for all positive integers $m$.*

*Proof.* By Theorem 62, we know that any prime $p$ has a primitive root $r$ which is also a primitive root modulo $p^2$, thus

$$p^2 \nmid (r^{p-1} - 1). \tag{6.1}$$

We will prove by induction that

$$p^m \nmid (r^{p^{m-2}(p-1)} - 1) \tag{6.2}$$

for all integers $m \geq 2$. Once we prove the above congruence, we show that $r$ is also a primitive root modulo $p^m$. Let $n = ord_{p^m} r$. By Theorem 54, we know that $n \mid \phi(p^m)$. Also, we know that $\phi(p^m) = p^m(p-1)$. Hence $n \mid p^m(p-1)$. On the other hand, because

$$p^m \mid (r^n - 1),$$

we also know that

$$p \mid (r^n - 1).$$

Since $\phi(p) = p - 1$, we see that by Theorem 54, we have $n = l(p-1)$. also $n \mid p^{m-1}(p-1)$, we have that $n = p^s(p-1)$, where $0 \leq s \leq m-1$. If $n = p^s(p-1)$ with $s \leq m-2$, then

$$p^k \mid r^{p^{m-2}(p-1)} - 1,$$

which is a contradiction. Hence

$$ord_{p^m} r = \phi(p^m).$$

We prove now (8.5) by induction. Assume that our assertion is true for all $m \geq 2$. Then

$$p^m \nmid (r^{p^{m-2}(p-1)} - 1).$$

Because $(r, p) = 1$, we see that $(r, p^{m-1}) = 1$. We also know from Euler's theorem that

$$p^{m-1} \mid (r^{p^{m-2}(p-1)} - 1).$$

Thus there exists an integer $k$ such that

$$r^{p^{m-2}(p-1)} = 1 + kp^{m-1}.$$

where $p \nmid k$ because $r^{p^{m-2}(p-1)} \not\equiv 1(\bmod p^m)$. Thus we have now

$$\begin{aligned} r^{p^{m-1}(p-1)} &= (1 + kp^{m-1})^p \\ &\equiv 1 + kp^m (\bmod p^{m+1}) \end{aligned}$$

Because $p \nmid k$, we have

$$p^{m+1} \nmid (r^{p^{m-1}(p-1)} - 1).$$

□

**Example 59.** *Since 3 is a primitive root of 7, then 3 is a primitive root for $7^k$ for all positive integers $k$.*

In the following theorem, we prove that no power of 2, other than 2 or 4, has a primitive root and that is because when $m$ is an odd integer, $ord_2^k m \neq \phi(2^k)$ and this is because $2^k \mid (a^{\phi(2^k)/2} - 1)$.

**Theorem 68.** *If $m$ is an odd integer, and if $k \geq 3$ is an integer, then*

$$m^{2^{k-2}} \equiv 1(\bmod 2^k).$$

*Proof.* We prove the result by induction. If $m$ is an odd integer, then $m = 2n + 1$ for some integer $n$. Hence,

$$m^2 = 4n^2 + 4n + 1 = 4n(n+1) + 1.$$

It follows that $8 \mid (m^2 - 1)$.

Assume now that

$$2^k \mid (m^{2^{k-2}} - 1).$$

Then there is an integer $q$ such that

$$m^{2^{k-2}} = 1 + q.2^k.$$

Thus squaring both sides, we get

$$m^{2^{k-1}} = 1 + q.2^{k+1} + q^2 2^{2k}.$$

Thus

$$2^{k+1} \mid (m^{2^{k-1}} - 1).$$

□

Note now that 2 and 4 have primitive roots 1 and 3 respectively.

We now list the set of integers that do not have primitive roots.

**Theorem 69.** *If $m$ is not $p^a$ or $2p^a$, then $m$ does not have a primitive root.*

*Proof.* Let $m = p_1^{s_1} p_2^{s_2} ... p_i^{s_i}$. If $m$ has a primitive root $r$ then $r$ and $m$ are relatively prime and $ord_m r = \phi(m)$. We also have, we have $(r, p^s) = 1$ where $p^s$ is of the primes in the factorization of $m$. By Euler's theorem, we have

$$p^s \mid (r^{\phi(p^s)} - 1).$$

Now let

$$L = [\phi(p_1^{s_1}), \phi(p_2^{s_2}), ..., \phi(p_i^{s_i})].$$

We know that

$$r^L \equiv 1 (\text{mod } p_k^{s_k})$$

for all $1 \leq k \leq m$. Thus using the Chinese Remainder Theorem, we get

$$m \mid (r^L - 1),$$

which leads to $ord_m r = \phi(m) \leq L$. Now because

$$\phi(m) = \phi(p_1^{s_1})\phi(p_2^{s_2})...\phi(p_n^{s_n}) \leq [\phi(p_1^{s_1}), \phi(p_2^{s_2}), ..., \phi(p_n^{s_n})].$$

Now the inequality above holds only if

$$\phi(p_1^{s_1}), \phi(p_2^{s_2}), ..., \phi(p_n^{s_n})$$

are relatively prime. Notice now that by Theorem 41,

$$\phi(p_1^{s_1}), \phi(p_2^{s_2}), ..., \phi(p_n^{s_n})$$

are not relatively prime unless $m = p^s$ or $m = 2p^s$ where $p$ is an odd prime and $t$ is any positive integer. □

We now show that all integers of the form $m = 2p^s$ have primitive roots.

**Theorem 70.** *Consider a prime* $p \neq 2$ *and let* $s$ *is a positive integer, then* $2p^s$ *has a primitive root. In fact, if* $r$ *is an odd primitive root modulo* $p^s$*, then it is also a primitive root modulo* $2p^s$ *but if* $r$ *is even,* $r + p^s$ *is a primitive root modulo* $2p^s$*.*

*Proof.* If $r$ is a primitive root modulo $p^s$, then

$$p^s \mid (r^{\phi(p^s)} - 1)$$

and no positive exponent smaller than $\phi(p^s)$ has this property. Note also that

$$\phi(2p^s) = \phi(p^s),$$

so that

$$p^s \mid (r^{\phi(2p^s)} - 1).$$

If $r$ is odd, then

$$2 \mid (r^{\phi(2p^s)} - 1).$$

Thus by Theorem 56, we get

$$2p^s \mid (r^{\phi(2p^s)} - 1).$$

It is important to note that no smaller power of $r$ is congruent to 1 modulo $2p^s$. This power as well would also be congruent to 1 modulo $p^s$ contradicting that $r$ is a primitive root of $p^s$. It follows that $r$ is a primitive root modulo $2p^s$.

While, if $r$ is even, then $r + p^s$ is odd. Hence

$$2 \mid ((r + p^s)^{\phi(2p^s)} - 1).$$

Because $p^s \mid (r + p^s - r)$, we see that

$$p^s \mid ((r + p^s)^{\phi(2p^s)} - 1).$$

As a result, we see that $2p^s \mid ((r+p^s)^{\phi(2p^s)} - 1)$ and since for no smaller power of $r + p^s$ is congruent to 1 modulo $2p^s$, we see that $r + p^s$ is a primitive root modulo $2p^s$. □

As a result, by Theorem 63, Theorem 65 and Theorem 66, we see that

**Theorem 71.** *The positive integer $m$ has a primitive root if and only if $n = 2, 4, p^s$ or $2p^s$*

for prime $p \neq 2$ and $s$ is a positive integer.

### Exercises

1. Which of the following integers 4, 12, 28, 36, 125 have a primitive root.

2. Find a primitive root of 4, 25, 18.

3. Find all primitive roots modulo 22.

4. Show that there are the same number of primitive roots modulo $2p^s$ as there are modulo $p^s$, where $p$ is an odd prime and $s$ is a positive integer.

5. Find all primitive roots modulo 25.

6. Show that the integer $n$ has a primitive root if and only if the only solutions of the congruence $x^2 \equiv 1 (modn)$ are $x \equiv \pm 1 (\mathrm{mod}\ n)$.

## 6.4 Introduction to Quadratic Residues and Nonresidues

The question that we need to answer in this section is the following. If $p$ is an odd prime and $a$ is an integer relatively prime to $p$. Is $a$ a perfect square modulo $p$.

**Definition 3.** *Let $m$ be a positive integer. An integer $a$ is a quadratic residue of $m$ if $(a, m) = 1$ and the congruence $x^2 \equiv a(\bmod m)$ is solvable. If the congruence $x^2 \equiv a(\bmod m)$ has no solution, then $a$ is a quadratic nonresidue of $m$.*

**Example 60.** *Notice that $1^2 = 6^2 \equiv 1(\bmod 7)$, $3^2 = 4^2 \equiv 2(\bmod 7)$ and $2^2 = 5^2 \equiv 4(\bmod 7)$. Thus $1, 2, 4$ are quadratic residues modulo 7 while $3, 5, 6$ are quadratic nonresidues modulo 7.*

**Lemma 13.** *Let $p \neq 2$ be a prime number and $a$ is an integer such that $p \nmid a$. Then either a is quadratic nonresidue modulo $p$ or*

$$x^2 \equiv a(\bmod p)$$

*has exactly two incongruent solutions modulo $p$.*

*Proof.* If $x^2 \equiv a(\bmod p)$ has a solution, say $x = x'$, then $-x'$ is a solution as well. Notice that $-x' \not\equiv x'(\bmod p)$ because then $p \mid 2x'$ and hence $p \nmid x_0$.

We now show that there are no more than two incongruent solutions. Assume that $x = x'$ and $x = x''$ are both solutions of $x^2 \equiv a(\bmod p)$. Then we have

$$(x')^2 - (x'')^2 = (x' + x'')(x' - x'') \equiv 0(\bmod p).$$

Hence

$$x' \equiv x''(\bmod p) \text{ or } x' \equiv -x''(\bmod p).$$

□

The following theorem determines the number of integers that are quadratic residues modulo an odd prime.

**Theorem 72.** *If $p \neq 2$ is a prime, then there are exactly $(p-1)/2$ quadratic residues modulo $p$ and $(p-1)/2$ quadratic nonresidues modulo $p$ in the set of integers $1, 2..., p-1$.*

*Proof.* To find all the quadratic residues of $p$ among all the integers $1, 2, ..., p-1$, we determine the least positive residue modulo $p$ of $1^2, 2^2, ..., (p-1)^2$. Considering the $p-1$ congruences and because each congruence has either no solution or two incongruent solutions, there must be exactly $(p-1)/2$ quadratic residues of $p$ among $1, 2, ..., p-1$. Thus the remaining are $(p-1)/2$ quadratic nonresidues of $p$. □

**Exercises**

1. Find all the quadratic residues of 3.

2. Find all the quadratic residues of 13.

3. find all the quadratic residues of 18.

4. Show that if $p$ is prime and $p \geq 7$, then there are always two consecutive quadratic residues of $p$. Hint: Show that at least one of $2, 5$ or 10 is a quadratic residue of $p$.

5. Show that if $p$ is prime and $p \geq 7$, then there are always two quadratic residues of $p$ that differ by 3.

## 6.5 Legendre Symbol

In this section, we define Legendre symbol which is a notation associated to quadratic residues and prove related theorems.

**Definition 4.** *Let $p \neq 2$ be a prime and $a$ be an integer such that $p \nmid a$. The Legendre symbol $\left(\frac{a}{p}\right)$ is defined by*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if a is a quadratic residue of p} \\ -1 & \text{if a is a quadratic nonresidue of p.} \end{cases}$$

**Example 61.** *Notice that using the previous example, we see that*

$$\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1$$
$$\left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1$$

In the following theorem, we present a way to determine wether an integer is a quadratic residue of a prime.

**Theorem 73.** ***Euler's Criterion*** *Let $p \neq 2$ be a prime and let $a$ be a positive integer such that $p \nmid a$. Then*

$$\left(\frac{a}{p}\right) \equiv a^{\phi(p)/2} (\bmod\, p).$$

*Proof.* Assume that $\left(\frac{a}{p}\right) = 1$. Then the congruence $x^2 \equiv a(\bmod\, p)$ has a solution say $x = x'$. According to Fermat's theorem, we see that

$$a^{\phi(p)/2} = ((x')^2)^{\phi(p)/2} \equiv 1(\bmod\, p).$$

Now if $\left(\frac{a}{p}\right) = -1$, then $x^2 \equiv a(\bmod\, p)$ is not solvable. Thus by Theorem 26, we have that for each integer k with $(k, p) = 1$ there is an integer $l$ such that $kl \equiv a(\bmod\, p)$. Notice that $i \neq j$ since $x^2 \equiv a(\bmod\, p)$ has no solutions. Thus we can couple the integers $1, 2, ..., p-1$ into $(p-1)/2$ pairs, each has product $a$. Multiplying these pairs together, we find out that

$$(p-1)! \equiv a^{\phi(p)/2} (\bmod\, p).$$

Using Wilson's Theorem, we get

$$\left(\frac{a}{p}\right) = -1 \equiv a^{(p-1)/2} (\bmod\, p).$$

□

**Example 62.** *Let* $p = 13$ *and* $a = 3$*. Then* $\left(\frac{3}{13}\right) = -1 \equiv 3^6 (\bmod\, 13)$.

We now prove some properties of Legendre symbol.

**Theorem 74.** *Let* $p \neq 2$ *be a prime. Let* $a$ *and* $b$ *be integers such that* $p \nmid a$*,* $p \nmid b$ *and* $p \mid (a-b)$ *then*

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$

*Proof.* Since $p \mid (a-b)$, then $x^2 \equiv a (\bmod\, p)$ has a solution if and only if $x^2 \equiv b (\bmod\, p)$ has a solution. Hence

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$$

□

**Theorem 75.** *Let* $p \neq 2$ *be a prime. Let* $a$ *and* $b$ *be integers such that* $p \nmid a$*,* $p \nmid b$ *then*

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$$

By Euler's criterion, we have

$$\left(\frac{a}{p}\right) \equiv a^{\phi(p)/2} (\bmod\, p)$$

and

$$\left(\frac{b}{p}\right) \equiv b^{\phi(p)/2} (\bmod\, p).$$

Thus we get

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv (ab)^{\phi(p)/2} \equiv \left(\frac{ab}{p}\right) (\bmod\, p).$$

We now show when is $-1$ a quadratic residue of a prime $p$ .

**Corollary 3.** *If $p \neq 2$ is a, then*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 (\text{mod } 4) \\ -1 & \text{if } p \equiv -1 (\text{mod } 4). \end{cases}$$

*Proof.* By Euler's criterion, we know that

$$\left(\frac{a}{p}\right) = (-1)^{\phi(p)/2} (\text{mod } p)$$

If $4 \mid (p-1)$, then $p = 4m+1$ for some integer $m$ and thus we get

$$(-1)^{\phi(p)/2} = (-1)^{2m} = 1.$$

and if $4 \mid (p-3)$, then $p = 4m+3$ for some integer $m$ and we also get

$$(-1)^{\phi(p)/2} = (-1)^{2m+1} = -1.$$

□

We now determine when 2 is a quadratic residue of a prime $p$.

**Theorem 76.** *For every odd prime p we have*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 (\text{mod } 8) \\ -1 & \text{if } p \equiv \pm 3 (\text{mod } 8). \end{cases}$$

*Proof.* Consider the following $(p-1)/2$ congruences

$$\begin{aligned} p-1 &\equiv 1(-1)^1 \pmod p \\ 2 &\equiv 2(-1)^2 \pmod p \\ p-3 &\equiv 3(-1)^3 \pmod p \\ 4 &\equiv 4(-1)^4 \pmod p \\ &. \\ &. \\ &. \\ r &\equiv \frac{p-1}{2}(-1)^{(p-1)/2} \pmod p, \end{aligned}$$

where $r$ is either $p-(p-1)/2$ or $(p-1)/2$. Multiplying all these equations we get,

$$2.4.6...(p-1) \equiv \left(\frac{p-1}{2}\right)!(-1)^{1+2+...+(p-1)/2} \pmod p.$$

This gives us

$$2^{(p-1)/2}\left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)!(-1)^{(p^2-1)/8}(\bmod p).$$

Now notice that $\left(\frac{p-1}{2}\right)! \not\equiv 0(\bmod p)$ and thus we get

$$2^{(p-1)/2} \equiv (-1)^{(p^2-1)/8}(\bmod p).$$

Note also that by Euler's criterion, we get

$$2^{\phi(p)/2} \equiv \left(\frac{2}{p}\right) \pmod p,$$

and since each member is 1 or -1 the two members are equal. □

We now present an important lemma that determines whether an integer is a quadratic residue of a prime or not.

**Lemma 14.** ***Gauss's Lemma*** *Let $p \neq 2$ be a prime and $a$ a relatively prime integer to $p$. If $k$ counts the number of least positive residues of the integers $a, 2a, ..., ((p-1)/2)a$ that are greater than $p/2$, then*

$$\left(\frac{a}{p}\right) = (-1)^k.$$

*Proof.* Let $m_1, m_2, ..., m_s$ be those integers greater than $p/2$ in the set of the least positive residues of the integers $a, 2a, ..., ((p-1)/2)a$ and let $n_1, n_2, ..., n_t$ be those less than $p/2$. We now show that

$$p-m_1, p-m_2, ..., p-m_k, p-n_1, p-n_2, ..., p-n_t$$

are precisely the integers

$$1, 2, ..., (p-1)/2,$$

in the same order.

So we shall show that no two integers of these are congruent modulo $p$, because there are exactly $(p-1)/2$ numbers in the set, and all are positive integers less than or equal to $(p-1)/2$. Notice that $m_i \not\equiv m_j (\text{mod } p)$ for all $i \neq j$ and $n_i \not\equiv n_j (\text{mod } p)$ for all $i \neq j$. If any of these congruences fail, then we will have that $r \equiv s(\text{mod}\, p)$ assuming that $ra \equiv sa(\text{mod}\, p)$. Also any of the integers $p - m_i$ can be congruent to any of the $n_i$'s. Because if such congruence holds, then we have $ra \equiv p - sa(\text{mod}\, p)$, so that $ra \equiv -sa(\text{mod}\, p)$. Because $p \nmid a$, this implies that $r \equiv -s(\text{mod}\, p)$, which is impossible. We conclude that

$$\prod_{i=1}^{k}(p - m_i)\prod_{i=1}^{t} n_i \equiv \left(\frac{p-1}{2}\right)!(\text{mod}\, p),$$

which implies

$$(-1)^s m_1 m_2 ... (p - m_k) n_1 n_2 ... n_t \equiv \left(\frac{p-1}{2}\right)!(\text{mod}\, p),$$

Simplifying, we get

$$m_1 m_2 ... (p - m_k) n_1 n_2 ... n_t \equiv a.2a...((p-1)/2) = a^{(p-1)/2}((p-1)/2)!(mod\, p).$$

As a result, we have that

$$a^{(p-1)/2}((p-1)/2)! \equiv ((p-1)/2)!(\text{mod}\, p)$$

Note that since $(p, ((p-1)/2)!) = 1$, we get

$$(-1)^k a^{(p-1)/2} \equiv 1(\text{mod}\, p).$$

Thus we get

$$a^{(p-1)/2} \equiv (-1)^k(\text{mod}\, p).$$

Using Euler's criterion, the result follows. □

**Example 63.** *To find* $\left(\frac{5}{13}\right)$ *using Gauss's lemma, we calculate*

$$\sum_{i=1}^{6}[5i/13] = [5/13] + [10/13] + [15/13] + [20/13] + [25/13] + [30/13] = 5$$

*Thus we get* $\left(\frac{5}{13}\right) = (-1)^5 = -1.$

**Exercises**

1. Find all quadratic residues of 3
2. Find all quadratic residues of 19.
3. Find the value of Legendre symbol $\left(\frac{j}{7}\right)$ for $j = 1, 2, 3, 4, 5, 6.$
4. Evaluate the Legendre symbol $\left(\frac{7}{11}\right)$by using Euler's criterion.
5. Let $a$ and $b$ be integers not divisible by $p$. Show that either one or all three of the integers $a, b$ and $ab$ are quadratic residues of $p$.
6. Let $p$ be a prime and $a$ be a quadratic residue of $p$. Show that if $p \equiv 1(\bmod 4)$, then $-a$ is also a quadratic residue of $p$, whereas if $p \equiv 3(\bmod 4)$, then $-a$ is a quadratic nonresidue of $p$.
7. Show that if $p$ is an odd prime and a is an integer not divisible by $p$ then $\left(\frac{a^2}{p}\right) = 1.$

## 6.6 The Law of Quadratic Reciprocity

Given that $p$ and $q$ are odd primes. Suppose we know whether $q$ is a quadratic residue of $p$ or not. The question that this section will answer is whether $p$ will be a quadratic residue of $q$ or not. Before we state the law of quadratic reciprocity, we will present a Lemma of Eisenstein which will be used in the proof of the law of reciprocity. The following lemma will relate Legendre symbol to the counting lattice points in the triangle.

**Lemma 15.** *If $p \neq 2$ is a prime and $a$ is an odd integer such that $p \nmid a$, then*

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{i=1}^{(p-1)/2}[ia/p]}.$$

*Proof.* Consider the least positive residues of the integers $a, 2a, ..., ((p-1)/2)a$; let $m_1, m_2, ..., m_s$ be integers of this set such that $m_i > p/2$ for all $i$ and let $n_1, n_2, ..., n_t$ be those integers where $n_i < p/2$. Using the division algorithm, we see that

$$ia = p[ia/p] + r$$

where $r$ is one of the $m_i$ or $n_i$. By adding the $(p-1)/2$ equations, we obtain

$$\sum_{i=1}^{(p-1)/2} ia = \sum_{i=1}^{(p-1)/2} p[ia/p] + \sum_{i=1}^{s} m_i + \sum_{i=1}^{t} n_i. \tag{6.3}$$

As in the proof of Gauss's Lemma, we see that

$$p - m_1, p - m_2, ..., p - m_s, p - n_1, p - n_2, ..., p - n_t$$

are precisely the integers $1, 2, ..., (p-1)/2$, in the same order. Now we obtain

$$\sum_{i=1}^{(p-1)/2} i = \sum_{i=1}^{s}(p - m_i) + \sum_{i=1}^{t} n_i = ps - \sum_{i=1}^{s} m_i + \sum_{i=1}^{t} n_i. \tag{6.4}$$

We subtract $(6.4)$ from $(6.3)$ to get

$$\sum_{i=1}^{(p-1)/2} ia - \sum_{i=1}^{(p-1)/2} i = \sum_{i=1}^{(p-1)/2} p[ia/p] - ps + 2\sum_{i=1}^{s} m_i.$$

Now since we are taking the following as exponents for $-1$, it suffice to look at them modulo 2. Thus

$$0 \equiv \sum_{i=1}^{(p-1)/2} [ia/p] - s (\text{mod } 2).$$

$$\sum_{i=1}^{(p-1)/2} [ia/p] \equiv s (\text{mod } 2)$$

Using Gauss's lemma, we get

$$\left(\frac{a}{p}\right) = (-1)^s = (-1)^{\sum_{i=1}^{(p-1)/2}[ia/p]}.$$

□

**Theorem 77.** ***The Law of Quadratic Reciprocity*** *Let $p$ and $q$ be distinct odd primes. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}.\frac{q-1}{2}}$$

*Proof.* We consider now the pairs of integers also known as lattice points $(x, y)$ with

$$1 \leq x \leq (p-1)/2 \text{and } 1 \leq y \leq (q-1)/2.$$

The number of such pairs is $\frac{p-1}{2}.\frac{q-1}{2}$. We divide these pairs into two groups depending on the sizes of $qx$ and $py$. Note that $qx \neq py$ for all pairs because $p$ and $q$ are distinct primes.

We now count the pairs of integers $(x, y)$ with

$$1 \leq x \leq (p-1)/2, \ 1 \leq y \leq (q-1)/2 \text{and } qx > py.$$

Note that these pairs are precisely those where

$$1 \leq x \leq (p-1)/2 \text{and } 1 \leq y \leq qx/p.$$

For each fixed value of $x$ with $1 \leq x \leq (p-1)/2$, there are $[qx/p]$ integers satisfying $1 \leq y \leq qx/p$. Consequently, the total number of pairs with are

$$1 \leq x \leq (p-1)/2, \ 1 \leq y \leq qx/p, \text{and } qx > py$$

is

$$\sum_{i=1}^{(p-1)/2} [qi/p].$$

Consider now the pair of integers $(x, y)$ with

$$1 \leq x \leq (p-1)/2,\ \ 1 \leq y \leq (q-1)/2, \text{and } \ qx < py.$$

Similarly, we find that the total number of such pairs of integers is

$$\sum_{i=1}^{(q-1)/2} [pi/q].$$

Adding the numbers of pairs in these classes, we see that

$$\sum_{i=1}^{(p-1)/2} [qi/p] + \sum_{i=1}^{(q-1)/2} [pi/q] = \frac{p-1}{2}.\frac{q-1}{2},$$

and hence using Lemma 14, we get that

$$\left(\frac{p}{q}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}.\frac{q-1}{2}}$$

□

**Exercises**

1. Evaluate $\left(\frac{3}{53}\right)$.

2. Evaluate $\left(\frac{31}{641}\right)$.

3. Using the law of quadratic reciprocity, show that if $p$ is an odd prime, then

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 (\text{mod } 12) \\ -1 & \text{if } p \equiv \pm 5 (\text{mod } 12). \end{cases}$$

4. Show that if $p$ is an odd prime, then

$$\left(\frac{-3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 (\text{mod } 6) \\ -1 & \text{if } p \equiv -1 (\text{mod } 6). \end{cases}$$

5. Find a congruence describing all primes for which 5 is a quadratic residue.

## 6.7 Jacobi Symbol

In this section, we define the Jacobi symbol which is a generalization of the Legendre symbol. The Legendre symbol was defined in terms of primes, while Jacobi symbol will be generalized for any odd integers and it will be given in terms of Legendre symbol.

**Definition 28.** *Let $n$ be an odd positive integer with prime factorization $n = p_1^{a_1} p_2^{a_2} ... p_m^{a_m}$ and let $a$ be an integer relatively prime to $n$, then*

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{m} \left(\frac{a}{p_i}\right)^{c_i}.$$

**Example 64.** *Notice that from the prime factorization of 45, we get that*

$$\left(\frac{2}{55}\right) = \left(\frac{2}{5}\right)\left(\frac{2}{11}\right) = (-1)(-1) = 1$$

We now prove some properties for Jacobi symbol that are similar to the properties of Legendre symbol.

**Theorem 78.** *Let $n$ be an odd positive integer and let $a$ and $b$ be integers such that$(a, n) = 1$ and $(b, n) = 1$. Then*

1. *if $n \mid (a - b)$, then*
$$\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right).$$

2. $$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right).$$

*Proof.* **Proof of 1:** Note that if $p$ is in the prime factorization of $n$, then we have that $p \mid (a - b)$. Hence by Theorem 70, we get that

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$

As a result, we have

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{m} \left(\frac{a}{p_i}\right)^{c_i} = \prod_{i=1}^{m} \left(\frac{b}{p_i}\right)^{c_i}$$

**Proof of 2:** Note that by Theorem 71, we have $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ for any prime $p$ appearing in the prime factorization of $n$. As a result, we have

$$\begin{aligned}\left(\frac{ab}{n}\right) &= \prod_{i=1}^{m} \left(\frac{ab}{p_i}\right)^{c_i} \\ &= \prod_{i=1}^{m} \left(\frac{a}{p_i}\right)^{c_i} \prod_{i=1}^{m} \left(\frac{b}{p_i}\right)^{c_i} \\ &= \left(\frac{a}{n}\right)\left(\frac{b}{n}\right).\end{aligned}$$

□

In the following theorem, we determine $\left(\frac{-1}{n}\right)$ and $\left(\frac{2}{n}\right)$.

**Theorem 79.** *Let $n$ be an odd positive integer. Then*

*1.*

$$\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}.$$

*2.*

$$\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}.$$

*Proof.* **Proof of 1:** If $p$ is in the prime factorization of $n$, then by Corollary 3, we see that $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$. Thus

$$\begin{aligned}\left(\frac{-1}{n}\right) &= \prod_{i=1}^{m} \left(\frac{-1}{p_i}\right)^{c_i} \\ &= (-1)^{\sum_{i=1}^{m} c_i(p_i-1)/2}.\end{aligned}$$

Notice that since $p_i - 1$ is even, we have

$$p_i^{a_i} = (1 + (p_i - 1))^{c_i} \equiv 1 + c_i(p_i - 1)(\text{mod } 4)$$

and hence we get

$$n = \prod_{i=1}^{m} p_i^{c_i} \equiv 1 + \sum_{i=1}^{m} c_i(p_i - 1)(\text{mod } 4).$$

As a result, we have

$$(n-1)/2 \equiv \sum_{i=1}^{m} c_i(p_i - 1)/2 \ (\text{mod } 2).$$

**Proof of 2:** If $p$ is a prime, then by Theorem 72 we have

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Hence

$$\left(\frac{2}{n}\right) = (-1)^{\sum_{i=1}^{m} c_i(p_i^2-1)/8}.$$

Because $8 \mid p_i^2 - 1$, we see similarly that

$$(1 + (p_i^2 - 1))^{c_i} \equiv 1 + c_i(p_i^2 - 1)(\text{mod } 64)$$

and thus

$$n^2 \equiv 1 + \sum_{i=1}^{m} c_i(p_i^2 - 1)(\text{mod } 64),$$

which implies that

$$(n^2 - 1)/8 \equiv \sum_{i=1}^{m} c_i(p_i^2 - 1)/8(\text{mod } 8).$$

□

We now show that the reciprocity law holds for Jacobi symbol.

**Theorem 80.** *Let $(a, b) = 1$ be odd positive integers. Then*

$$\left(\frac{b}{a}\right)\left(\frac{a}{b}\right) = (-1)^{\frac{a-1}{2}.\frac{b-1}{2}}.$$

*Proof.* Notice that since $a = \prod_{j=1}^{m} p_i^{c_i}$ and $b = \prod_{i=1}^{n} q_i^{d_i}$ we get

$$\left(\frac{b}{a}\right)\left(\frac{a}{b}\right) = \prod_{i=1}^{n}\prod_{j=1}^{m}\left[\left(\frac{p_j}{q_i}\right)\left(\frac{q_i}{p_j}\right)\right]^{c_j d_i}$$

By the law of quadratic reciprocity, we get

$$\left(\frac{b}{a}\right)\left(\frac{a}{b}\right) = (-1)^{\sum_{i=1}^{n}\sum_{j=1}^{m} c_j\left(\frac{p_j-1}{2}\right)d_i\left(\frac{q_i-1}{2}\right)}$$

As in the proof of part 1 of Theorem 75, we see that

$$\sum_{j=1}^{m} c_j\left(\frac{p_j-1}{2}\right) \equiv \frac{a-1}{2}(mod\ 2)$$

and

$$\sum_{i=1}^{n} d_i\left(\frac{q_i-1}{2}\right) \equiv \frac{b-1}{2}(mod\ 2).$$

Thus we conclude that

$$\sum_{j=1}^{m} c_j\left(\frac{p_j-1}{2}\right)\sum_{i=1}^{n} d_i\left(\frac{q_i-1}{2}\right) \equiv \frac{a-1}{2}.\frac{b-1}{2}(\text{mod } 2).$$

□

**Exercises**

1. Evaluate $\left(\frac{258}{4520}\right)$.

2. Evaluate $\left(\frac{1008}{2307}\right)$.

3. For which positive integers $n$ that are relatively prime to 15 does the Jacobi symbol $\left(\frac{15}{n}\right)$ equal 1?

4. Let $n$ be an odd square free positive integer. Show that there is an integer $a$ such that $(a, n) = 1$ and $\left(\frac{a}{n}\right) = -1$.

# Chapter 7

# Introduction to Continued Fractions

In this chapter, we introduce continued fractions, prove their basic properties and apply these properties to solve some problems. Being a very natural object, continued fractions appear in many areas of Mathematics, sometimes in an unexpected way. The Dutch mathematician and astronomer, Christian Huygens (1629-1695), made the first practical application of the theory of ”anthyphaeiretic ratios” (the old name of continued fractions) in 1687. He wrote a paper explaining how to use convergents to find the best rational approximations for gear ratios. These approximations enabled him to pick the gears with the best numbers of teeth. His work was motivated by his desire to build a mechanical planetarium. Further continued fractions attracted attention of most prominent mathematicians. Euler, Jacobi, Cauchy, Gauss and many others worked with the subject. Continued fractions find their applications in some areas of contemporary Mathematics. There are mathematicians who continue to develop the theory of continued fractions nowadays, The Australian mathematician A.J. van der Poorten is, probably, the most prominent among them.

## 7.1 Basic Notations

In general, a (simple) continued fraction is an expression of the form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \dots}},$$

where the letters $a_0,\ a_1,\ a_2, \dots$ denote independent variables, and may be interpreted as one wants (e.g. real or complex numbers, functions, etc.). This expression has precise sense if the number of terms is finite, and may have no meaning for an infinite number of terms. In this section we only discuss the simplest classical setting.

*The letters $a_1,\ a_2, \dots$ denote positive integers. The letter $a_0$ denotes an integer.*

The following standard notation is very convenient.

**Notation 1.** *We write*

$$[a_0; a_1, a_2, \dots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \dots + \cfrac{1}{a_n}}}$$

*if the number of terms is finite, and*

$$[a_0; a_1, a_2, \dots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \dots}}$$

*for an infinite number of terms.*

Still, in the case of infinite number of terms a certain amount of work must be carried out in order to make the above formula meaningful. At the same time, for the finite number of terms the formula makes sense.

**Example 65.**

$$[-2; 1, 3, 5] = -2 + \frac{1}{1 + \frac{1}{3 + \frac{1}{5}}} = -2 + \frac{1}{1 + \frac{5}{16}} = -2 + \frac{1}{\frac{21}{16}} = -2 + \frac{16}{21} = -\frac{26}{21}.$$

**Notation 2.** *For a finite continued fraction $[a_0; a_1, a_2, \ldots, a_n]$ and a positive integer $k \leq n$, the $k$-th remainder is defined as the continued fraction*

$$r_k = [a_k; a_{k+1}, a_{k+2}, \ldots, a_n].$$

*Similarly, for an infinite continued fraction $[a_0; a_1, a_2, \ldots]$ and a positive integer $k$, the $k$-th remainder is defined as the continued fraction*

$$r_k = [a_k; a_{k+1}, a_{k+2}, \ldots].$$

Thus, at least in the case of a finite continued fraction,

$$\alpha = [a_0; a_1, a_2, \ldots, a_n] = a_0 + 1/(a_1 + 1/(a_2 + \ldots + 1/a_n))$$

we have

$$\alpha = a_0 + 1/(a_1 + 1/(a_2 + \ldots + 1/(a_{k-1} + 1/r_k))) = \text{“}[a_0; a_1, a_2, \ldots, a_{k-1}, r_k]\text{”} \tag{7.1}$$

for any positive $k \leq n$. Quotation signs appear because we consider the expressions of this kind only with integer entries but the quantity $r_k$ may be a non-integer.

It is not difficult to expand any rational number $\alpha$ into a continued fraction. Indeed, let $a_0 = [\alpha]$ be the greatest integer not exceeding $\alpha$. Thus the difference $\delta = \alpha - a_0 < 1$ and, of course, $\delta \geq 0$. If $\delta = 0$ then we are done. Otherwise put $r_1 = 1/\delta$, find $a_1 = [r_1]$ and non-negative $\delta = \alpha_1 - a_1 < 1$. Continue the procedure until you obtain $\delta = 0$.

**Example 66.** *Consider the continued fraction expansion for $42/31$. We obtain $a_0 = [42/31] = 1$, $\delta = 42/31 - 1 = 11/31$. Now $r_1 = 1/\delta = 31/11$ and $a_1 = [\alpha_1] = [31/11] = 2$. The new $\delta = 31/11 - 2 = 9/11$. Now $r_2 = 1/\delta = 11/9$ and $a_2 = [\alpha_2] = [11/9] = 1$. It follows that $\delta = 11/9 - 1 = 2/9$. Now $r_3 = 1/\delta = 9/2$ and $a_3 = [\alpha_3] = [9/2] = 4$. It follows that $\delta = 9/2 - 4 = 1/2$. Now $r_4 = 1/\delta = 2$ and $a_4 = [\alpha_4] = [2] = 2$. It follows that $\delta = 2 - 2 = 0$ and we are done.*

*Thus we have calculated*

$$42/31 = [a_0; a_1, a_2, a_3, a_4] = [1; 2, 1, 4, 2].$$

The above example shows that the algorithm stops after finitely many steps. This is in fact quite a general phenomenon. In order to practice with the introduced notations let us prove a simple but important proposition.

**Proposition 1.** *Any rational number can be represented as a finite continued fraction.*

*Proof.* By construction, all remainders are positive rationals. For a positive integer $k$ put $r_k = A/B$ and let $a_k = [r_k]$. Then

$$r_k - a_k = \frac{A - Ba_k}{B} := \frac{C}{B}. \tag{7.2}$$

with $C < B$ because $r_k - a_k < 1$ by construction. If $C = 0$, then the algorithm stops at this point and we are done. Assume now that $C \neq 0$. It follows from (7.1) that

$$r_k = a_k + \frac{1}{r_{k+1}}. \tag{7.3}$$

Compare now (7.2) with (7.3) to find that

$$r_{k+1} = \frac{B}{C}.$$

Since $C < B$, the rational number $r_{k+1}$ has a denominator which is smaller than the the denominator of the previous remainder $r_k$. It follows that after a finite number of steps we obtain an integer (a rational with $1$ in the denominator) $r_n = a_n$ and the procedure stops at this point.

There appear several natural questions in the connection with Proposition 1.

Is such a continued fraction representation unique? The immediate answer is ”no”. Here are two ”different” continued fraction representations for $1/2$:

$$\frac{1}{2} = [0; 2] = [0; 1, 1].$$

However, we require that $a_n > 1$, where $a_n$ is the last element of a finite continued fraction. Then the answer is ”yes”.

*Hint.* Make use of the formulas (7.5) below.

From now on we assume that $a_n > 1$.

Another natural question is about infinite continued fractions and (as one can easily guess) real numbers. The proof of the corresponding result is slightly more involved, and we do not give it here. In this brief introduction we just formulate the result and refer to the literature ([12, Theorem 14]) for a complete proof. We, however, provide some remarks concerning this result below. In particular, we will explain at some point, what the convergence means.

**Theorem 81.** *An infinite continued fraction converges and defines a real number. There is a one-to-one correspondence between*

- *all (finite and infinite) continued fractions $[a_0; a_1, a_2, \ldots]$ with an integer $a_0$ and positive integers $a_k$ for $k > 0$ (and the last term $a_n > 1$ in the case of finite continued fractions)*

*and*

- *real numbers.*

Note that the algorithm we developed above can be applied to any real number and provides the corresponding continued fraction.

Theorem 81 has certain theoretical significance. L.Kronecker (1823-1891) said, ”God created the integers; the rest is work of man”. Several ways to represent real numbers out of integers are well-known. Theorem 81 provides yet another way to fulfill this task. This way is constructive and at the same time is not tied to any particular base (say to decimal or binary decomposition).

We will discuss some examples later.

**Exercises**

1. Compute continued fraction representations of the following rational numbers.

(a) 2/3

(b) 2/51

(c) 2/101

(d) 3/7

(e) 7/3

2. Find a pattern for the continued fraction expansion of every rational number of the form ${}^1\!/_a$.

3. Suppose $\gcd(2, a) = 1$. Show that ${}^2\!/_a$ has the continued fraction expansion $[0; b, a]$ where $b = [{}^a\!/_2]$.

4. Find a pattern for the continued fraction expansion of ${}^3\!/_a$.

5. Show that if the continued fraction expansion of ${}^a\!/_b$ is $[0; a_1, \ldots, a_n]$, then the continued fraction expansion of ${}^b\!/_a$ is $[a_1; a_2, \ldots, a_n]$.

6. Prove that under the assumption $a_n > 1$ the continued fraction representation given in Proposition 1 is unique. In other words, the correspondence between

   • finite continued fractions $[a_0; a_1, a_2, \ldots a_n]$ with an integer $a_0$, positive integers $a_k$ for $k > 0$ and $a_n > 1$

   and

   • rational numbers

   is one-to-one.

## 7.2 Main Technical Tool

Truncate finite (or infinite) continued fraction $\alpha = [a_0; a_1, a_2, \ldots, a_n]$ at the $k$-th place (with $k < n$ in the finite case). The rational number $s_k = [a_0; a_1, a_2, \ldots, a_k]$

is called the $k$-th *convergent* of $\alpha$. Define the integers $p_k$ and $q_k$ by

$$s_k = \frac{p_k}{q_k} \tag{7.4}$$

written in the reduced form with $q_k > 0$.

The following recursive transformation law takes place.

**Theorem 82.** *For $k \geq 2$*

$$\begin{aligned} p_k &= a_k p_{k-1} + p_{k-2} \\ q_k &= a_k q_{k-1} + q_{k-2}. \end{aligned} \tag{7.5}$$

*Remark.* It does not matter here whether we deal with finite or infinite continued fractions: the convergents are finite anyway. *Proof.* We use the induction argument on $k$. For $k = 2$ the statement is true.

Now, assume (7.5) for $2 \leq k < l$. Let

$$\alpha = [a_0; a_1, a_2, \dots a_l] = \frac{p_l}{q_l}$$

be an arbitrary continued fraction of length $l + 1$. We denote by $p_r/q_r$ the $r$-th convergent $\alpha$. Consider also the continued fraction

$$\beta = [a_1; a_2, \dots, a_l]$$

and denote by $p'_r/q'_r$ its $r$-th convergent. We have $\alpha = a_0 + 1/\beta$ which translates as

$$\begin{aligned} p_l &= a_0 p'_{l-1} + q'_{l-1} \\ q_l &= p'_{l-1}. \end{aligned} \tag{7.6}$$

Also, by the induction assumption,

$$\begin{aligned} p'_{l-1} &= a_l p'_{l-2} + p'_{l-3} \\ q'_{l-1} &= a_l q'_{l-2} + q'_{l-3} \end{aligned} \tag{7.7}$$

Combining (7.6) and (7.7) we obtain the formulas

$$p_l = a_0(a_l p'_{l-2} + p'_{l-3}) + a_l q'_{l-2} + q'_{l-3} = a_l(a_0 p'_{l-2} + q'_{l-2}) + (a_0 p'_{l-3} + q'_{l-3}) = a_l p_{l-1} + p_{l-2}$$

and

$$q_l = a_l p'_{l-2} + p'_{l-3} = a_l q_{l-1} + q_{l-2},$$

which complete the induction step. We have thus proved that

$$s_k = \frac{p_k}{q_k},$$

where $p_k$ and $q_k$ are defined by the recursive formulas (7.5). We still have to check that these are the quantities defined by (7.4), namely that $q_k > 0$ and that $q_k$ and $p_k$ are relatively prime. The former assertion follows from (7.5) since $a_k > 0$ for $k > 0$. To prove the latter assertion, multiply the equations (7.5) by $q_{k-1}$ and $p_{k-1}$ respectively and subtract them. We obtain

$$p_k q_{k-1} - q_k p_{k-1} = -(p_{k-1} q_{k-2} - q_{k-1} p_{k-2}). \tag{7.8}$$

This concludes the proof of Theorem 7.5. As an immediate consequence of (7.5) we find that

$$\frac{p_{k-1}}{q_{k-1}} - \frac{p_k}{q_k} = \frac{(-1)^k}{q_k q_{k-1}} \tag{7.9}$$

and

$$\frac{p_{k-2}}{q_{k-2}} - \frac{p_k}{q_k} = \frac{(-1)^k a_k}{q_k q_{k-2}}.$$

Since all the numbers $q_k$ and $a_k$ are positive, the above formulas imply the following.

**Proposition 2.** *The subsequence of convergents $p_k/q_k$ for even indices $k$ is increasing.*

*The subsequence of convergents $p_k/q_k$ for odd indices $k$ is decreasing.*

*Every convergent with an odd index is bigger than every convergent with an even index.*

*Remark.* Proposition 2 implies that both subsequences of convergents (those with odd indices and those with even indices) have limits. This is a step towards making sense out of an infinite continued fraction: this should be *common* limit of these two subsequences. It is somehow more technically involved (although still fairly elementary!) to prove that these two limits coincide.

**Theorem 83.** *Let $\alpha = [a_0; a_1, a_2, \ldots, a_n]$. For $k < n$ we have*

$$\frac{1}{q_k(q_{k+1} + q_k)} \leq \left|\alpha - \frac{p_k}{q_k}\right| \leq \frac{1}{q_k q_{k+1}}$$

*Proof.*

Another inequality, which provides the lower bound for the distance between the number $\alpha$ and $k$-th convergent is slightly more involved. To prove it we first consider the following way to add fractions which students sometimes prefer.

**Definition 1.** *The number*

$$\frac{a+c}{b+d}$$

*is called the mediant of the two fractions $a/b$ and $c/d$. (The quantities $a, b, c$ and $d$ are integers.)*

**Lemma 16.** *If*

$$\frac{a}{b} \leq \frac{c}{d}$$

*then*

$$\frac{a}{b} \leq \frac{a+c}{b+d} \leq \frac{c}{d}.$$

Consider now the sequence of fractions

$$\frac{p_k}{q_k}, \frac{p_k + p_{k+1}}{q_k + q_{k+1}}, \frac{p_k + 2p_{k+1}}{q_k + 2q_{k+1}}, \ldots, \frac{p_k + a_k p_{k+1}}{q_k + a_k q_{k+1}} = \frac{p_{k+2}}{q_{k+2}}, \tag{7.10}$$

where the last equality follows from (7.5).

It follows that the sequence (7.10) is increasing if $k$ is even and is decreasing if $k$ is odd. Thus, in particular, the fraction

$$\frac{p_k + p_{k+1}}{q_k + q_{k+1}} \tag{7.11}$$

is between the quantities $p_k/q_k$ and $\alpha$. Therefore the distance between $p_k/q_k$ and the fraction (7.11) is smaller than the distance between $p_k/q_k$ and $\alpha$:

$$\left|\alpha - \frac{p_k}{q_k}\right| \geq \frac{p_k + p_{k+1}}{q_k + q_{k+1}} = \frac{1}{q_k(q_k + q_{k+1})}.$$

The second (right) inequality in Theorem 83 is now proved. This finishes the proof of Theorem 83.

**Exercises**

1. Check the assertion of Theorem 82 for $k = 2$.

2. Check that for $k = 2$

   $$p_2 q_1 - q_2 p_1 = -1.$$

   *Hint.* Introduce formally $p_{-1} = 1$ and $q_{-1} = 0$, check that then formulas 7.5 are true also for $k = 1$.

3. Combine the previous exercises with (7.8) to obtain

   $$q_k p_{k-1} - p_k q_{k-1} = (-1)^k$$

   for $k \geq 1$. Derive from this that $q_k$ and $p_k$ are relatively prime.

4. Prove Proposition 2

5. Combine (7.9) with Proposition 2 to prove the inequality

   $$\left|\alpha - \frac{p_k}{q_k}\right| \leq \frac{1}{q_k q_{k+1}}.$$

6. Prove Lemma 16

7. Use (7.5) to show that the sign of the difference between two consecutive fractions in (7.10) depends only on the parity of $k$.

## 7.3 Very Good Approximation

Continued fractions provide a representation of numbers which is, in a sense, generic and canonical. It does not depend on an arbitrary choice of a base. Such a representation should be the best in a sense. In this section we quantify this naive idea.

**Definition 2.** *A rational number $a/b$ is referred to as a "good" approximation to a number $\alpha$ if*

$$\frac{c}{d} \neq \frac{a}{b} \quad \textit{and} \quad 0 < d \leq b$$

*imply*

$$|d\alpha - c| > |b\alpha - a|.$$

*Remarks.* 1. Our "good approximation" is "the best approximation of the second kind" in a more usual terminology.
2. Although we use this definition only for rational $\alpha$, it may be used for any real $\alpha$ as well. Neither the results of this section nor the proofs alter.
3. Naively, this definition means that $a/b$ approximates $\alpha$ better then any other rational number whose denominator does not exceed $b$. There is another, more common, definition of "the best approximation". A rational number $x/y$ is referred to as "the best approximation of the first kind" if $c/d \neq x/y$ and $0 < d \leq y$ imply $|\alpha - c/d| > |\alpha - x/y|$. In other words, $x/y$ is closer to $\alpha$ than any rational number whose denominator does not exceed $y$. In our definition we consider a slightly different measure of approximation, which takes into the account the denominator, namely $b|\alpha - a/b| = |b\alpha - a|$ instead of taking just the distance $|\alpha - a/b|$.

**Theorem 84.** *Any "good" approximation is a convergent.*

*Proof.* Let $a/b$ be a "good" approximation to $\alpha = [a_0; a_1, a_2, \ldots, a_n]$. We have to prove that $a/b = p_k/q_k$ for some $k$.

Thus we have $a/b > p_1/q_1$ or $a/b$ lies between two consecutive convergents $p_{k-1}/q_{k-1}$ and $p_{k+1}/q_{k+1}$ for some $k$. Assume the latter. Then

$$\left|\frac{a}{b} - \frac{p_{k-1}}{q_{k-1}}\right| \geq \frac{1}{bq_{k-1}}$$

and

$$\left|\frac{a}{b} - \frac{p_{k-1}}{q_{k-1}}\right| < \left|\frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}}\right| = \frac{1}{q_k q_{k-1}}.$$

It follows that

$$b > q_k. \tag{7.12}$$

Also

$$\left|\alpha - \frac{a}{b}\right| \geq \left|\frac{p_{k+1}}{q_{k+1}} - \frac{a}{b}\right| \geq \frac{1}{bq_{k+1}},$$

which implies

$$|b\alpha - a| \geq \frac{1}{q_{k+1}}.$$

At the same time Theorem 83 (it right inequality multiplied by $q_k$) reads

$$|q_k\alpha - p_k| \leq \frac{1}{q_{k+1}}.$$

It follows that

$$|q_k\alpha - p_k| \leq |b\alpha - a|,$$

and the latter inequality together with (7.12) show that $a/b$ is not a ”good” approximation of $\alpha$ in this case.

This finishes the proof of Theorem 84.

**Exercises**

1. Prove that if $a/b$ is a ”good” approximation then $a/b \geq a_0$.

2. Show that if $a/b > p_1/q_1$ then $a/b$ is not a ”good” approximation to $\alpha$.

## 7.4 An Application

Consider the following problem which may be of certain practical interest. Assume that we calculate certain quantity using a computer. Also assume that we know in advance that the quantity in question is a rational number. The computer returns a decimal which has high accuracy and is pretty close to our desired answer. How to guess the exact answer?

To be more specific consider an example.

**Example 67.** *Assume that the desired answer is*

$$\frac{123456}{121169}$$

*and the result of computer calculation with a modest error of* $10^{-15}$ *is*

$$\begin{aligned}\alpha = \frac{123456}{121169} + 10^{-15} = 1.&01887446459077916933374047817511079566 55\\ &580222664212793701359258556231379313190 6\\ &675799915820052983849004283273774645330 0\\ &761745991136346755358218686297650389125 9\\ &31550148965494474659360067343957612920 7\end{aligned}$$

*with some two hundred digits of accuracy which, of course come short to help in guessing the period and the exact denominator of* 121169*.*

Solution. Since $123456/121169$ is a good (just in a naive sense) approximation to $\alpha$, it should be among its convergents. This is not an exact statement, but it offers a hope! We have

$$\alpha = [1; 52, 1, 53, 2, 4, 1, 2, 1, 68110, 4, 1, 2, 106, 22, 3, 1, 1, 10, 2, 1, 3, 1, 3, 4, 2, 11].$$

We are not going to check all convergents, because we notice the irregularity: one element, $68110$ is far more than the others. In order to explain this we use the left inequality from Theorem 83 together with the formula (7.5). Indeed, we have an approximation of $\alpha$ which is unexpectedly good: $|\alpha - p_k/q_k|$ is very small (it is around $10^{-15}$) and with a modest $q_k$ too. We have

$$q_k(q_{k+1} + q_k) = q_k(a_{k+1}q_k + q_{k-1}) = q_k^2(a_{k+1} + q_{k-1}/q_k)$$

and

$$\left|\alpha - \frac{p_k}{q_k}\right| \geq \frac{1}{q_k^2(a_{k+1} + q_{k-1}/q_k)}.$$

It follows that $1/q_k^2(a_{k+1} + q_{k-1}/q_k)$ is small (smaller than $10^{-15}$) and therefore, $a_{k+1}$ should be big. This is exactly what we see. Of course, our guess is correct:

$$\frac{123456}{121169} = [1, 52, 1, 53, 2, 4, 1, 2, 1].$$

In this way we conclude that in general an unexpectedly big element allows to cut the continued fraction (right before this element) and to guess the exact rational quantity. There is probably no need (although this is, of course, possible) to quantify this procedure. I prefer to use it just for guessing the correct quantities on the spot from the first glance.

## 7.5 A Formula of Gauss, a Theorem of Kuzmin and Lévi and a Problem of Arnold

In this connection Gauss asked about a probability $c_k$ for a number $k$ to appear as an element of a continued fraction. Such a probability is defined in a natural way: as a limit when $N \to \infty$ of the number of occurrences of $k$ among the first $N$ elements of the continued fraction enpension. Moreover, Gauss provided an answer, but never published the proof. Two different proofs were found independently by R.O.Kuzmin (1928) and P. Lévy (1929) (see [12] for a detailed exposition of the R.O.Kuzmin's proof).

**Theorem 85.** *For almost every real $\alpha$ the probability for a number $k$ to appear as an element in the continued fraction expansion of $\alpha$ is*

$$c_k = \frac{1}{\ln 2} \ln\left(1 + \frac{1}{k(k+2)}\right). \tag{7.13}$$

*Remarks.* 1. The words ”for almost every $\alpha$” mean that the measure of the set of exceptions is zero.
2. Even the existence of $p_k$ (defined as a limit) is highly non-trivial.

Theorem 85 may (and probably should) be considered as a result from ergodic theory rather than number theory. This constructs a bridge between these two areas of Mathematics and explains the recent attention to continued fractions of the mathematicians who study dynamical systems. In particular, V.I.Arnold formulated the following open problem. Consider the set of pairs of integers $(a, b)$ such that the corresponding points on the plane are contained in a quarter of a circle of radii $N$:

$$a^2 + b^2 \leq N^2.$$

Expand the numbers $p/q$ into continued fractions and compute the frequencies $s_k$ for the appearance of $k$ in these fractions. Do these frequencies have limits as $N \to \infty$? If so, do these limits have anything to do with the probabilities, given by (7.13)? These questions demand nothing but experimental computer investigation, and such an experiment may be undertaken by a student. Of course, it would be extremely challenging to find a phenomena experimentally in this way and to prove it after that theoretically.

Of course, one can consider more general kinds of continued fractions. In particular, one may ease the assumption that the elements are positive integers and consider, allowing arbitrary reals as the elements (the question of convergence may usually be solved). The following identities were discovered independently by three prominent mathematicians. The English mathematician R.J. Rogers found and proved these identities in 1894, Ramanujan found the identities (without proof) and formulated them in his letter to Hardy from India in

1913. Independently, being separated from England by the war, I. J. Schur found the identities and published two different proofs in 1917. We refer an interested reader to [2, 1] for a detailed discussion and just state the amazing identities here.

$$[0; e^{-2\pi}, e^{-4\pi}, e^{-6\pi}, e^{-8\pi}, \ldots] = \left(\sqrt{\frac{5+\sqrt{5}}{2}} - \frac{\sqrt{5}+1}{2}\right) e^{2\pi/5}$$

$$[1; e^{-\pi}, e^{-2\pi}, e^{-3\pi}, e^{-4\pi}, \ldots] = \left(\sqrt{\frac{5-\sqrt{5}}{2}} - \frac{\sqrt{5}-1}{2}\right) e^{\pi/5}$$

## Exercises

1. Prove that $c_k$ really define a probability distribution, namely that

$$\sum_{k=1}^{\infty} c_k = 1.$$

# Chapter 8

# Introduction to Analytic Number Theory

The distribution of prime numbers has been the object of intense study by many modern mathematicians. Gauss and Legendre conjectured the prime number theorem which states that the number of primes less than a positive number $x$ is asymptotic to $x/logx$ as $x$ approaches infinity. This conjecture was later proved by Hadamard and Poisson. Their proof and many other proofs lead to the what is known as Analytic Number theory.

In this chapter we demonstrate elementary theorems on primes and prove elementary properties and results that will lead to the proof of the prime number theorem.

## 8.1 Introduction

It is well known that the harmonic series $\sum_{n=1}^{\infty} \frac{1}{n}$ diverges. We therefore determine some asymptotic formulas that determines the growth of the $\sum_{n\leq x} \frac{1}{n}$. We start by introducing Euler's summation formula that will help us determine the asymptotic formula.

We might ask the following question. What if the sum is taken over all the primes. In this section, we show that the sum over the primes diverges as well. We also show that an interesting product will also diverge. From the following theorem, we can actually deduce that there are infinitely many primes.

**Euler's Summation Formula** If $f$ has a continuous derivative on an interval $[a, b]$ where $a > 0$, then

$$\sum_{a<n\leq b} f(n) = \int_a^b f(t)dt + \int_a^b (\{t\})f'(t)dt + f(b)(\{b\}) - f(a)(\{a\}).$$

where $\{t\}$ denotes the fractional part of $t$.

For the proof of Euler's summation formula see [3, Chapter 3].

**Proposition 3.** *If $x \geq 1$, we have that:*

$$\sum_{n\leq x} \frac{1}{n} = \log x + \gamma + O\left(\frac{1}{x}\right)$$

*Proof.* We use Euler's summation formula by taking $f(t) = 1/t$. We then get

$$\begin{aligned} \sum_{n\leq x} \frac{1}{n} &= \int_1^x \frac{1}{t}dt - \int_1^x \frac{\{t\}}{t^2}dt + 1 + O\left(\frac{1}{x}\right) \\ &= \log x + 1 - \int_1^\infty \frac{\{t\}}{t^2}dt + \int_x^\infty \frac{\{t\}}{t^2}dt + O\left(\frac{1}{x}\right) \end{aligned}$$

Notice now that $\{t\} \leq t$ and hence the two improper integrals exist since they are dominated by integrals that converge. We therefore have

$$0 \leq \int_x^\infty \frac{\{t\}}{t^2}dt \leq \frac{1}{x},$$

we also let

$$\gamma = 1 - \int_1^\infty \frac{\{t\}}{t^2}dt$$

and we get the asymptotic formula. Notice that $\gamma$ is called Euler's constant. Notice also that similar steps can be followed to find an asymptotic formulas for other sums involving powers of $n$.

We now proceed to show that if we sum over the primes instead, we still get a divergent series. □

**Theorem 86.** *Both* $\sum_p \frac{1}{p}$ *and* $\prod_p(1-\frac{1}{p})$ *diverge.*

*Proof.* Let $x \geq 2$ and put

$$P(x) = \prod_{p\leq x}\left(1-\frac{1}{p}\right)^{-1}, \quad S(x) = \sum_{p\leq x}\frac{1}{p}$$

Let $0 < u < 1$ and $m \in \mathbb{Z}$, we have

$$\frac{1}{1-u} > \frac{1-u^{m+1}}{1-u} = 1+u+...+u^m.$$

Now taking $u = \frac{1}{p}$, we get

$$\frac{1}{1-\frac{1}{p}} > 1+\frac{1}{p}+...+\left(\frac{1}{p}\right)^m$$

As a result, we have that

$$P(x) > \prod_{p\leq x}\left(1+\frac{1}{p}+...+\frac{1}{p^m}\right)$$

Choose $m > 0 \in \mathbb{Z}$ such that $2^{m-1} \leq x \leq 2^m$. Observe also that

$$\prod_{p\leq x}\left(1+\frac{1}{p}+...+\frac{1}{p^m}\right) = 1+\sum_{p_i\leq x}\frac{1}{p_1^{m_1}p_2^{m_2}...}$$

where $1 \leq m_i \leq m$ . As a result, we get every $\frac{1}{n}, n \in \mathbb{Z}^+$ where each prime factor of $n$ is less than or equal to $x$(Exercise). Thus we have

$$\prod_{p\leq x}\left(1+\frac{1}{p}+...+\frac{1}{p^m}\right) > \sum_{n=1}^{2^{m-1}}\frac{1}{n} > \sum_{n=1}^{[x/2]}\frac{1}{n}$$

Taking the limit as $x$ approaches infinity, we conclude that $P(x)$ diverges.

We proceed now to prove that $S(x)$ diverges. Notice that if $u > 0$, then

$$\log(1/u - 1) < u + \frac{1}{2}(u^2 + u^3 + ...).$$

Thus we have

$$\log(1/u - 1) < u + \frac{u^2}{2}(1/1 - u), \quad 0 < u < 1.$$

We now let $u = 1/p$ for each $p \leq x$, then

$$\log\left(\frac{1}{1 - 1/p}\right) - \frac{1}{p} < \frac{1}{2p(p-1)}$$

Thus

$$\log P(x) = \sum_{p \leq x} log(1/1 - p).$$

Thus we have

$$\log P(x) - S(x) < \frac{1}{2}\sum_{p \leq x} \frac{1}{p(p-1)} < \frac{1}{2}\sum_{n=1}^{\infty} \frac{1}{n(n-1)}$$

This implies that

$$S(x) > \log P(x) - \frac{1}{2}$$

And thus $S(x)$ diverges as $x$ approaches infinity. □

**Theorem 87** (Abel's Summation Formula)**.** *For any arithmetic function $f(n)$, we let*

$$A(x) = \sum_{n \leq x} f(n)$$

*where $A(x) = 0$ for $x < 1$. Assume also that $g$ has a continuous derivative on the interval $[y, x]$, where $0 < y < x$. Then we have*

$$\sum_{y < n \leq x} f(n)g(n) = A(x)g(x) - A(y)g(y) - \int_y^x A(t)g'(t)dt.$$

The proof of this theorem can be found in [3, Chapter 4].

**Exercises**

1. Show that one gets every $\frac{1}{n}, n \in \mathbb{Z}^+$ where each prime factor of $n$ is less than or equal to $x$ in the proof of Theorem 1.

2. Write down the proof of Abel's summation formula in details.

## 8.2 Chebyshev's Functions

We introduce some number theoretic functions which play important role in the distribution of primes. We also prove analytic results related to those functions. We start by defining the Van-Mangolt function

**Definition 5.** *$\Omega(n) = logp$ if $n = p^m$ and vanishes otherwise.*

We define also the following functions, the last two functions are called Chebyshev's functions.

1. $\pi(x) = \sum_{p \leq x} 1.$

2. $\theta(x) = \sum_{p \leq x} logp$

3. $\psi(x) = \sum_{n \leq x} \Omega(n)$

Notice that

$$\psi(x) = \sum_{n \leq x} \Omega(n) = \sum_{m=1,\ p^m \leq x}^{\infty} \sum_{p} \Omega(p^m) = \sum_{m=1}^{\infty} \sum_{p \leq x^{1/m}} logp.$$

**Example 68.** *1. $\pi(10) = 4.$*

*2. $\theta(10) = log2 + log3 + log5 + log7.$*

*3. $\psi(10) = log2 + log2 + log2 + log3 + log3 + log5 + log7$*

**Remark 6.** *It is easy to see that*

$$\psi(x) = \theta(x) + \theta(x^{1/2}) + \theta(x^{1/3}) + ...\theta(x^{1/m})$$

*where $m \leq log_2 x$. This remark is left as an exercise.*

Notice that the above sum will be a finite sum since for some $m$, we have that $x^{1/m} < 2$ and thus $\theta(x^{1/m}) = 0$.
We use Abel's summation formula now to express the two functions $\pi(x)$ and $\theta(x)$ in terms of integrals.

**Theorem 88.** *For $x \geq 2$, we have*

$$\theta(x) = \pi(x) \log x - \int_2^x \frac{\pi(t)}{t} dt$$

*and*

$$\pi(x) = \frac{\theta(x)}{\log x} + \int_2^x \frac{\theta(t)}{t \log^2 t} dt.$$

*Proof.* We define the characteristic function $\chi(n)$ to be $1$ if $n$ is prime and $0$ otherwise. As a result, we can see from the definition of $\pi(x)$ and $\theta(x)$ that they can be represented in terms of the characteristic function $\chi(n)$. This representation will enable use to apply Abel's summation formula where $f(n) = \chi(n)$ for $\theta(x)$ and where $f(n) = \chi(n) \log n$ for $\pi(x)$. So we have,

$$\pi(x) = \sum_{1 \leq n/leqx} \chi(n) \quad \text{and} \quad \theta(x) = \sum_{1 \leq n \leq x} \chi(n) \log n$$

Now let $g(x) = \log x$ in Theorem 84 with $y = 1$ and we get the desired result for the integral representation of $\theta(x)$. Similarly we let $g(x) = 1/\log x$ with $y = 3/2$ and we obtain the desired result for $\pi(x)$ since $\theta(t) = 0$ for $t < 2$. □

We now prove a theorem that relates the two Chebyshev's functions $\theta(x)$ and $\psi(x)$. The following theorem states that if the limit of one of the two functions $\theta(x)/x$ or $\psi(x)/x$ exists then the limit of the other exists as well and the two limits are equal.

**Theorem 89.** *For $x > 0$, we have*

$$0 \leq \frac{\psi(x)}{x} - \frac{\theta(x)}{x} \leq \frac{(\log x)^2}{2\sqrt{x}\log 2}.$$

*Proof.* From Remark 4, it is easy to see that

$$0 \leq \psi(x) - \theta(x) = \theta(x^{1/2}) + \theta(x^{1/3}) + ...\theta(x^{1/m})$$

where $m \leq log_2 x$. Moreover, we have that $\theta(x) \leq x \log x$. The result will follow after proving the inequality in Exercise 2. □

**Exercises**

1. Show that

$$\psi(x) = \theta(x) + \theta(x^{1/2}) + \theta(x^{1/3}) + ...\theta(x^{1/m})$$

where $m \leq log_2 x$.

2. Show that $0 \leq \psi(x) - \theta(x) \leq (\log_2(x))\sqrt{x}\log\sqrt{x}$ and thus the result of Theorem 86 follows.

3. Show that the following two relations are equivalent

$$\pi(x) = \frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right)$$

$$\theta(x) = x + O\left(\frac{x}{\log x}\right)$$

## 8.3 Getting Closer to the Proof of the Prime Number Theorem

We know prove a theorem that is related to the defined functions above. Keep in mind that the prime number theorem is given as follows:

$$\lim_{x\to\infty} \frac{\pi(x) logx}{x} = 1.$$

We now state equivalent forms of the prime number theorem.

**Theorem 90.** *The following relations are equivalent*

$$\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1 \tag{8.1}$$

$$\lim_{x\to\infty} \frac{\theta(x)}{x} = 1 \tag{8.2}$$

$$\lim_{x\to\infty} \frac{\psi(x)}{x} = 1. \tag{8.3}$$

*Proof.* We have proved in Theorem 86 that $(8.2)$ and $(8.3)$ are equivalent, so if we show that $(8.1)$ and $(8.2)$ are equivalent, the proof will follow. Notice that using the integral representations of the functions in Theorem 85, we obtain

$$\frac{\theta(x)}{x} = \frac{\pi(x)\log x}{x} - \frac{1}{x}\int_2^x \frac{\pi(t)}{t}dt$$

and

$$\frac{\pi(x)\log x}{x} = \frac{\theta(x)}{x} + \frac{\log x}{x}\int_2^x \frac{\theta(t)}{t\log^2 t}dt.$$

Now to prove that (8.1) implies $(8.2)$, we need to prove that

$$\lim_{x\to\infty} \frac{1}{x}\int_2^x \frac{\pi(t)}{t}dt = 0.$$

Notice also that $(8.1)$ implies that $\frac{\pi(t)}{t} = O\left(\frac{1}{\log t}\right)$ for $t \geq 2$ and thus we have

$$\frac{1}{x}\int_2^x \frac{\pi(t)}{t}dt = O\left(\frac{1}{x}\int_2^x \frac{dt}{\log t}\right)$$

Now once you show that (Exercise 1)

$$\int_2^x \frac{dt}{\log t} \leq \frac{\sqrt{x}}{\log 2} + \frac{x-\sqrt{x}}{\log\sqrt{x}},$$

then $(8.1)$ implies $(8.2)$ will follow. We still need to show that $(8.2)$ implies $(8.1)$ and thus we have to show that

$$\lim_{x\to\infty} \frac{\log x}{x}\int_2^x \frac{\theta(t)dt}{t\log^2 t} = 0.$$

Notice that $\theta(x) = O(x)$ and hence

$$\frac{\log x}{x}\int_2^x \frac{\theta(t)dt}{t\log^2 t} = O\left(\frac{\log x}{x}\int_2^x \frac{dt}{\log^2 t}\right).$$

Now once again we show that (Exercise 2)

$$\int_2^x \frac{dt}{\log^2 t} \leq \frac{\sqrt{x}}{\log^2 2} + \frac{x-\sqrt{x}}{\log^2 \sqrt{x}}$$

then $(8.2)$ implies $(8.1)$ will follow.

□

**Theorem 91.** *Define*

$$l_1 = \liminf_{x\to\infty} \frac{\pi(x)}{x/logx}, \qquad L_1 = \limsup_{x\to\infty} \frac{\pi(x)}{x/logx},$$

$$l_2 = \liminf_{x\to\infty} \frac{\theta(x)}{x}, \qquad L_2 = \limsup_{x\to\infty} \frac{\theta(x)}{x},$$

*and*

$$l_3 = \liminf_{x\to\infty} \frac{\psi(x)}{x}, \qquad L_3 = \limsup_{x\to\infty} \frac{\psi(x)}{x},$$

*then* $l_1 = l_2 = l_3$ *and* $L_1 = L_2 = L_3$.

*Proof.* Notice that

$$\psi(x) = \theta(x) + \theta(x^{1/2}) + \theta(x^{1/3}) + ...\theta(x^{1/m}) \geq \theta(x)$$

where $m \leq log_2 x$ □

Also,

$$\psi(x) = \sum_{p\leq x}\left[\frac{\log x}{\log p}\right]\log p \leq \sum_{p\leq x}\frac{\log x}{\log p}\log p = \log x\pi(x).$$

Thus we have

$$\theta(x) \leq \psi(x) \leq \pi(x)\log x$$

As a result, we have
$$\frac{\theta(x)}{x} \leq \frac{\psi(x)}{x} \leq \frac{\pi(x)}{x/\log x}$$
and we get that $L_2 \leq L_3 \leq L_1$. We still need to prove that $L_1 \leq L_2$.

Let $\alpha$ be a real number where $0 < \alpha < 1$, we have

$$\begin{aligned}
\theta(x) &= \sum_{p\leq x} \log p \geq \sum_{x^\alpha \leq p \leq x} \log p \\
&> \sum_{x^\alpha \leq p \leq x} \alpha \log x \quad (\log p > \alpha \log x) \\
&= \alpha logx\{\pi(x) - \pi(x^\alpha)\}
\end{aligned}$$

However, $\pi(x^\alpha) \leq x^\alpha$. Hence

$$\theta(x) > \alpha \log x\{\pi(x) - x^\alpha\}$$

As a result,
$$\frac{\theta(x)}{x} > \frac{\alpha\pi(x)}{x/\log x} - \alpha x^{\alpha-1}\log x$$
Since $\lim_{x\to\infty} \alpha \log x/x^{1-\alpha} = 0$, then

$$L_2 \geq \alpha \limsup_{x\to\infty} \frac{\pi(x)}{x/\log x}$$

As a result, we get that

$$L_2 \geq \alpha L_1$$

As $\alpha \to 1$, we get $L_2 \geq L_1$.

Proving that $l_1 = l_2 = l_3$ is left as an exercise.

We now present an inequality due to Chebyshev about $\pi(x)$.

**Theorem 92.** *There exist constants $a < A$ such that*

$$a\frac{x}{\log x} < \pi(x) < A\frac{x}{\log x}$$

*for sufficiently large $x$.*

*Proof.* Put

$$l = \liminf_{x\to\infty} \frac{\pi(x)}{x/\log x}, \qquad L = \limsup_{x\to\infty} \frac{\pi(x)}{x/\log x},$$

It will be sufficient to prove that $L \leq 4\log 2$ and $l \geq \log 2$. Thus by Theorem 2, we have to prove that

$$\limsup_{x\to\infty} \frac{\theta(x)}{x} \leq 4\log 2 \tag{8.4}$$

and

$$\liminf_{x\to\infty} \frac{\psi(x)}{x} \geq \log 2 \tag{8.5}$$

To prove $(8.4)$, notice that

$$N = C(2n,n) = \frac{(n+1)(n+2)...(n+n)}{n!} < 2^{2n} < (2n+1)N$$

Suppose now that $p$ is a prime such that $n < p < 2n$ and hence $p \mid N$. As a result, we have $N \geq \prod_{n<p<2n} p$. We get

$$N \geq \theta(2n) - \theta(n).$$

Since $N < 2^{2n}$, we get that $\theta(2n) - \theta(n) < 2n\log 2$. Put $n = 1, 2, 2^2, ..., 2^{m-1}$ where $m$ is a positive integer. We get that

$$\theta(2^m) < 2^{m-1}\log 2.$$

Let $x > 1$ and choose $m$ such that $2^{m-1} \leq x \leq 2^m$, we get that

$$\theta(x) \leq \theta(2^m) \leq 2^{m+1}\log 2 \leq 4x\log 2$$

and we get $(8.4)$ for all $x$.

We now prove $(8.5)$. Notice that by Lemma 9, we have that the highest power of a prime $p$ dividing $N = \frac{(2n)!}{(n!)^2}$ is given by

$$s_p = \sum_{i=11}^{\mu_p} \left\{ \left[\frac{2n}{p^i}\right] - 2\left[\frac{n}{p^i}\right] \right\}.$$

where $\mu_p = \left[\frac{\log 2n}{\log p}\right]$. Thus we have $N = \prod_{p\le 2n} p^{s_p}$. If $x$ is a positive integer then

$$[2x] - 2[x] < 2,$$

It means that $[2x] - 2[x]$ is 0 or 1. Thus $s_p \le \mu_p$ and we get

$$N \le \prod_{p\le e2n} p^{\mu_p}.$$

Notice as well that

$$\psi(2n) = \sum_{p\le 2n} \left[\frac{\log 2n}{\log p}\right] \log p = \sum_{p\le 2n} \mu_p \log p.$$

Hence we get

$$\log N \le \psi(2n).$$

Using the fact that $2^{2n} < (2n+1)N$, we can see that

$$\psi(2n) > 2n\log 2 - \log(2n+1).$$

Let $x > 2$ and put $n = \left[\frac{x}{2}\right] \ge 1$. Thus $\frac{x}{2} - 1 < n < \frac{x}{2}$ and we get $2n \le x$. So we get

$$\begin{aligned}\psi(x) &\ge \psi(2n) > 2n\log 2 - \log(2n+1)\\ &> (x-2)\log 2 - \log(x+1).\end{aligned}$$

As a result, we get

$$\liminf_{x\to\infty} \frac{\psi(x)}{x} \ge \log 2.$$

□

**Exercises**

1. Show that $l_1 = l_2 = l_3$ in Theorem 88.

2. Show that
$$\int_2^x \frac{dt}{\log t} \le \frac{\sqrt{x}}{\log 2} + \frac{x - \sqrt{x}}{\log \sqrt{x}},$$

3. Show that
$$\int_2^x \frac{dt}{\log^2 t} \leq \frac{\sqrt{x}}{\log^2 2} + \frac{x-\sqrt{x}}{\log^2 \sqrt{x}}$$

4. Show that
$$N = C(2n,n) = \frac{(n+1)(n+2)...(n+n)}{n!} < 2^{2n} < (2n+1)N$$

5. Show that $\frac{2^{2n}}{2\sqrt{n}} < N = C(2n,n) < \frac{2^{2n}}{\sqrt{2n}}$.
   Hint: For one side of the inequality, write
$$\frac{N}{2^n} = \frac{(2n)!}{2^{2n}(n!)^2} = \frac{1.3.5....(2n-1)}{2.4.6....(2n)}.\frac{2.4.6.....(2n)}{2.4.6...(2n)},$$
   then show that
$$1 > (2n+1).\frac{N^2}{2^{4n}} > 2n.\frac{N^2}{2^{4n}}.$$
   The other side of the inequality will follow with similar arithmetic techniques as the first inequality.

# Chapter 9

# Other Topics in Number Theory

This chapter discusses various topics that are of profound interest in number theory. Section 1 on cryptography is on an application of number theory in the field of message decoding, while the other sections on elliptic curves and the Riemann zeta function are deeply connected with number theory. The section on Fermat's last theorem is related, through Wile's proof of Fermat's conjecture on the non-existence of integer solutions to $x^n + y^n = z^n$ for $n > 2$, to the field of elliptic curves (and thus to section 2).

## 9.1 Cryptography

In this section we discuss some elementary aspects of cryptography, which concerns the coding and decoding of messages.

### 9.1.1 Public key cryptography

In cryptography, a (word) message is transformed into a sequence $a$ of integers, by replacing each letter in the message by a specific and known set of integers that represent this letter, and thus forming a large integer $a$ by concatenation.

Some transformation is then applied to $a$ using an **encryption key**, in the hopes that it will be difficult to reverse the transformation without already knowing the contents of the message. The message is then broadcast to the recipient, who uses a **decryption key** to reverse the transformation.

Difficulties arise in sharing the keys. To solve this, **public key cryptography** exploits difficult mathematical problems, where it is easy to perform a computation, but not so easy to reverse it. The general scheme is this:

- Person A wants to receive secret messages. Person A chooses an encryption function, $f$, and two keys: an encryption key, $e$, and a decryption key, $d$. The two keys are used to generate a third item, which we shall call $m$.
- Person A broadcasts $f$, $e$, and $m$. *Anyone can overhear this information.*
- Person B decides to send person A a secret message, computes $b = f(a, e, m)$, and broadcasts $b$ message to Person A. *Anyone can overhear this message.*
- Person A applies a function $g$ to $b$ using $d$, and obtains $a = g(b, d, m)$. (It is possible that $g = f$.)

The security of this approach is based on the fact that even though $f$, $g$, $e$, and $m$ are publicly known, and the method of computing $m$ from $e$ and $d$ is well-established, it is practically impossible to reverse-engineer $d$ from all this information. This gives a level of security so high that *not even the sender* can decrypt the message: only the recipient!

Let's look at an example that relates to Number Theory.

### 9.1.2 The RSA algorithm

The RSA algorithm is based on the fact that it is easy to multiply two prime numbers, but surprisingly difficult to factor them. (We talk about this a little more below.)

In RSA, the message $a$ is transformed (i.e. coded) into another integer $b$ by using a congruence of the form $b = a^k (\mathrm{mod}\ m)$ for some chosen $k$ and $m$, as described below, with $k$ publicly known. $b$ is then sent to the recipient who decodes it into $a$ again by using a congruence of the form $a = b^{\bar{k}} (\mathrm{mod}\ m)$, where $\bar{k}$ is related to $k$ and is itself only known to the recipient, and then simply transforms the integers in $a$ back to letters and reveals the message again. In this procedure, if a third party intercepts the integers $b$, $k$, and $m$ the chance of transforming this into $a$, even if the integers that represent the letters of the alphabet are exactly known, is almost impossible to do (i.e. has a fantastically small probability of being achieved) if $\bar{k}$ is not known, that practically the transformed message will not be revealed except to the intended recipient.

The basic results on congruences to allow for the above procedure are in the following two lemmata, where $\phi$ in the statements is Euler's $\phi$-function.

**Lemma 17.** *Let $a$ and $m$ be two integers, with $m$ positive and $(a, m) = 1$. If $k$ and $\bar{k}$ are positive integers with $k\bar{k} \equiv 1(\mathrm{mod}\ \phi(m))$, then $a^{k\bar{k}} \equiv a(\mathrm{mod}\ m)$.*

*Proof.* $k\bar{k} = 1(\mathrm{mod}\ \phi(m))$ thus $k\bar{k} = q\phi(m) + 1$ $(q \geq 0)$. Hence $a^{k\bar{k}} = a^{q\phi(m)+1} = a^{q\phi(m)}a$. But by Euler's Theorem, if $(a, m) = 1$ then $a^{\phi(m)} \equiv 1(\mathrm{mod}\ m)$. This gives that

$$(a^{\phi(m)})^q a \equiv 1 \cdot a(\mathrm{mod}\ m) \equiv a(\mathrm{mod}\ m), \tag{9.1}$$

and hence that $a^{k\bar{k}} \equiv a(\mathrm{mod}\ m)$, and the result follows. □

We also need the following.

**Lemma 18.** *Let $m$ be a positive integer, and let $r_1, r_2, \cdots, r_n$ be a reduced residue system modulo $m$ (i.e. with $n = \phi(m)$ and $(r_i, m) = 1$ for $i = 1, \cdots, n$). If $k$ is an integer such that $(k, \phi(m)) = 1$, then $r_1^k, r_2^k, \cdots, r_n^k$ forms a reduced residue system modulo $m$.*

Before giving the proof, one has to note that the above lemma is in fact an if-and-only-if statement, i.e. $(k, \phi(m)) = 1$ if and only if $r_1^k, r_2^k, \cdots, r_n^k$ forms a reduced residue system modulo $m$. However we only need the if part, as in the lemma.

*Proof.* Assume first that $(k, \phi(m)) = 1$. We show that $r_1^k, r_2^k, \cdots, r_n^k$ is a reduced residue system modulo $m$. Assume otherwise, i.e. assume that $\exists i, j$ such that $r_i^k = r_j^k (\bmod m)$, in which case $r_i^k$ and $r_j^k$ would belong to the same class and thus $r_1^k, r_2^k, \cdots, r_n^k$ would not form a reduced residue system. Then, since $(k, \phi(m)) = 1$, $\exists \bar{k}$ with $k\bar{k} = 1(\bmod \phi(m))$, and so

$$r_i^{k\bar{k}} = r_i (\bmod m) \quad and \quad r_j^{k\bar{k}} = r_j (\bmod m) \tag{9.2}$$

by the previous lemma. But if $r_i^k = r_j^k (\bmod m)$ then $(r_i^k)^{\bar{k}} = (r_j^k)^{\bar{k}} (\bmod m)$, and since $r_i^{k\bar{k}} = r_i (\bmod m)$ and $r_j^{k\bar{k}} = r_j (\bmod m)$, then $r_i = r_j (\bmod m)$ giving that $r_i$ and $r_j$ belong to the same class modulo $m$, contradicting that $r_1, r_2, \cdots, r_n$ form a reduced residue system. Thus $r_i \neq r_j$ implies that $r_i^k \neq r_j^k$ if $(k, \phi(m)) = 1$. □

Now to do cryptography, one proceeds as follows. Let $S$ be a sentence given in terms of letters and spaces between the words that is intended to be transformed to a destination with the possibility of being intercepted and revealed by a third party.

1. Choose a couple $p_1$ and $p_2$ of very large prime numbers, each (for example) of the order of a hundred digit integer, and these should be strictly kept known only to the recipient. Then form the product $m = p_1 p_2$, which is itself a very large number to the point that the chances of an eavesdropper's discovering the prime number factorization $p_1 p_2$ of $m$ is incredibly small, even if they know this integer $m$. Now one has, by standard results concerning the $\phi$-function, that $\phi(p_1) = p_1 - 1$ and $\phi(p_2) = p_2 - 1$, and that, since $p_1$ and $p_2$ are relatively prime, $\phi(m) = \phi(p_1)\phi(p_2) = (p_1 - 1)(p_2 - 1)$. Thus $\phi(m)$ is a very large number, of the order of $m$ itself, and hence $m$

has a reduced residue system that contains a very large number of integers of the order of $m$ itself. Hence almost every integer smaller than $m$, with a probability of the order $1 - {}^1\!/_{10^{100}}$ (almost 1), is in a reduced residue system $r_1, r_2, \cdots, r_{\phi(m)}$ of $m$. Thus almost every positive integer smaller than $m$ is relatively prime to $m$, with probability of the order $1 - {}^1\!/_{10^{100}}$.

2. Choose an integer $k$ satisfying $\gcd(m, k) = 1$, and broadcast $m$ and $k$.

3. The sender transforms $S$ into a (large) integer $a$ by replacing each letter and each space between words by a certain representative integer (e.g. three or four digit integers for each letter). $a$ is formed by concatenating the representative integers that are produced.

4. Now given that almost every positive integer smaller than $m$ is relatively prime with $m$, the integer $a$ itself is almost certainly relatively prime with $m$, and hence is in a reduced residue system for $m$. Hence, by Lemma 17 above, if $k$ is a (large) integer such that $(k, \phi(m)) = 1$, then $a^k$ belongs to a reduced residue system for $m$, and there exists a unique positive $b$ smaller than $m$ with $b = a^k (\bmod m)$.

5. The sender sends $b$ to the original broadcaster, where the original prime numbers, and hence $\phi(m)$, are known. With this information, *which was never broadcast,* the destination can determine a $\bar{k}$ such that $k\bar{k} = 1(\bmod \phi(m))$, and then finds the unique $c$ such that $c = b^{\bar{k}}(\bmod m)$. Now since, almost certainly, $(a, m) = 1$, then almost certainly $c = a$ since $c = b^{\bar{k}}(\bmod m) = (a^k)^{\bar{k}}(\bmod m) = a^{k\bar{k}}(\bmod m) \equiv a(\bmod m)$ by Lemma 17. Now the destination translates $a$ back to letters and spaces to reveal the sentence $S$.

6. Note that if any third party intercepts $b$, they almost certainly cannot reveal the integer $a$ since the chance of them knowing $\phi(m) = p_1 p_2$ is almost zero, even if they know $m$ and $k$. In this case they practically won't be able to determine a $\bar{k}$ with $k\bar{k} = 1(\bmod \phi(m))$, to retrieve $a$ and transform it to $S$.

**Exercises**

1. You will want the assistance of a computer for this. Pick two large primes, and compute the modulus, an encryption key, and a decryption key. Use these to confirm your understanding of the RSA algorithm: practice by inventing a message, encrypting it, then trying to decrypt it again. Be sure you use a computer that knows how to take large exponents modulo a number quickly, or you could be waiting a long time...

### 9.1.3 Is RSA safe?

You might wonder if RSA is really safe. After all, the method is well-known, and is based on the fact that $\bar{k}$ is the multiplicative inverse of $k$ modulo $\phi(m)$. But this is easy if you know $\phi(m)$; the fact that $\gcd(\phi(m), k) = 1$ means you can just apply the Euclidean algorithm to find two integers $\bar{k}, \ell$ such that

$$k\bar{k} + \ell\phi(m) = 1.$$

.Even worse, $m$ is the product of two primes $p$ and $q$, so $\phi(m) = (p-1)(q-1)$. Thus, breaking RSA is as simple as factoring $m$ into primes — and you already know that there are only two primes!

**Example 69.** *To drive home how simple this can be, consider that* $6 = 2 \times 3$*,* $14 = 2 \times 7$*, and so forth are fairly easy to factor. Then again, they're pretty small numbers...*

This appearance of vulnerability really is superficial: once prime numbers grow sufficiently large, no one knows how to factor them quickly. For a while, RSA Laboratories even offered large cash prizes to people who can factor such values of $m$. As of this writing, the smallest such number in the RSA Factoring

Challenge is 220 digits long:

$$\begin{gathered}
22601385262034057849416540486101975135080389157197\\
76718321197768109445641817966676608593121306582577\\
25063156288667697044807000181114971186300211248792\\
81994874820660701310665866460833279828035603792053\\
91980139946496955261.
\end{gathered}$$

Although they no longer offer the prize, you might want to give it a go if you have a lot of free time coming up.

However, one can't just pick *any* two large primes. We can illustrate this with 10403: an obvious approach to factor it (and usually a very bad one) is to start at the floor of $\sqrt{10403}$ and work one's way down; since $\sqrt{10403} \approx 102$, the first number to try is 101. Oops!

There is a large body of scientific work dedicated to finding good primes for the RSA algorithm, which is a good thing, because commerce on the internet (such as that One-click purchase at Amazon!) is based on its security. Recently, scientists working in the strange world of *quantum computing* have developed algorithms that factor primes very, very quickly — but quantum computers work only with very, very small numbers. It is not yet clear whether quantum computation will advance to the point where this will become practical for cracking formerly secure communications.

**Exercises**

1. Ask a mathematically literate friend to choose two "large" primes, but not to tell you what they are. Instead, your friend should tell you what their product is. See if you can determine the two prime numbers. (Here, "large" means two to three digits long — not RSA grade!)

## 9.2 Elliptic Curves

Elliptic curves in the $xy$-plane are the set of points $(x, y) \in \mathbb{R} \times \mathbb{R}$ that are the zeros of special types of third order polynomials $f(x, y)$, with real coefficients, in the two variables $x$ and $y$. These curves turn out to be of fundamental interest in analytic number theory. More generally, one can define similar curves over arbitrary algebraic fields as follows. Let $f(x, y)$ be a polynomial of any degree in two variables $x$ and $y$, with coefficients in an algebraic field $\mathcal{F}$. We define the *algebraic curve* $\mathscr{C}_f(\mathcal{F})$ over the field $\mathcal{F}$ by

$$\mathscr{C}_f(\mathcal{F}) = \{(x, y) \in \mathcal{F} \times \mathcal{F} : f(x, y) = 0 \in \mathcal{F}\}. \tag{9.3}$$

Of course one can also similarly define the algebraic curve $\mathscr{C}_f(\mathcal{Q})$ over a field $\mathcal{Q}$, where $\mathcal{Q}$ is either a subfield of the field $\mathcal{F}$ where the coefficients of $f$ exist, or is an extension field of $\mathcal{F}$. Thus if $f \in \mathcal{F}[x, y]$, and if $\mathcal{Q}$ is either an extension or a subfield of $\mathcal{F}$, then one can define $\mathscr{C}_f(\mathcal{Q}) = \{(x, y) \in \mathcal{Q} \times \mathcal{Q} : f(x, y) = 0\}$. Our main interest in this section will be in third order polynomials (cubic curves)

$$f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j, \tag{9.4}$$

with coefficients in $\mathcal{R}$, with the associated curves $\mathscr{C}_f(\mathbb{Q})$ over the field of rational numbers $\mathbb{Q} \subset \mathbb{R}$. Thus, basically, we will be interested in points $(x, y) \in \mathbb{R}^2$ that have rational coordinates $x$ and $y$, and called rational points, that satisfy $f(x, y) = 0$. Of course one can first imagine the curve $f(x, y) = 0$ in $\mathbb{R}^2$, i.e. the curve $\mathscr{C}_f(\mathbb{R})$ over $\mathbb{R}$, and then choosing the points on this curve that have rational coordinates. This can simply be expressed by writing that $\mathscr{C}_f(\mathbb{Q}) \subset \mathscr{C}_f(\mathbb{R})$. It has to be mentioned that ”rational curves” $\mathscr{C}_f(\mathbb{Q})$ are related to diophantine equations. This is in the sense that rational solutions to equations $f(x, y) = 0$ produce integer solutions to equations $f'(x, y) = 0$, where the polynomial $f'$ is very closely related to the polynomial $f$, if not the same one in many cases. For example every point in $\mathscr{C}_f(\mathbb{Q})$, where $f(x, y) = x^n + y^n$, i.e. every rational solution to $f(x, y) = x^n + y^n = 0$, produces an integer solution to $x^n + y^n = 0$. Thus algebraic curves $\mathscr{C}_f(\mathbb{Q})$ can be of genuine interest in this sense.

In a possible procedure to construct the curve $\mathscr{C}_f(\mathbb{Q})$ for a polynomial $f(x, y) \in \mathbb{R}[x, y]$ with real coefficients, one considers the possibility that, given one rational point $(x, y) \in \mathscr{C}_f(\mathbb{Q}) \subset \mathscr{C}_f(\mathbb{R})$, a straight line with a rational slope $m$ might intersect the curve $\mathscr{C}_f(\mathbb{R})$ in a point $(x', y')$ that is also in $\mathscr{C}_f(\mathbb{Q})$. This possibility comes from the simple fact that if $(x, y), (x', y') \in \mathscr{C}_f(\mathbb{Q})$, then the slope of the straight line that joins $(x, y)$ and $(x', y')$ is a rational number. This technique, of determining one point in $\mathscr{C}_f(\mathbb{Q})$ from another by using straight lines as mentioned, works very well in some cases of polynomials, especially those of second degree, and works reasonably well for third order polynomials.

Two aspects of this technique of using straight lines to determine points in $\mathscr{C}_f(\mathbb{Q})$, and which will be needed for defining elliptic curves, are the following. The first is illustrated by the following example.

Consider the polynomial $f(x,y) = y^2 - x^2 + y = (y - x + 1)(y + x)$. The curve $\mathscr{C}_f(\mathbb{R})$ contains the two straight lines $y = x - 1$ and $y = -x$. The point $(2, 1) \in \mathscr{C}_f(\mathbb{Q})$, and if one tries to find the intersection of the particular line $y = x - 1$ that passes through $(2, 1)$ with $\mathscr{C}_f(\mathbb{R})$, one finds that this includes the whole line $y = x - 1$ itself, and not just one or two other points (for example). This result is due to the fact that $f$ is a reducible polynomial, i.e. that can be factored in the form $f = f'f''$ with $f$ and $f''$ not just real numbers.

In this direction one has the following general theorem concerning the number of intersection points between a straight line $L$ and an algebraic curve $\mathscr{C}_f(\mathcal{R})$:

**Theorem 93.** *If $f \in \mathbb{R}[x, y]$ is a polynomial of degree $d$, and the line $L$, which is defined by the zeros of $g(x, y) = y - mx - b \in \mathbb{R}[x, y]$, are such that $L \cap \mathscr{C}_f(\mathcal{R})$ contains more than $d$ points (counting the multiplicities of intersections) then in fact $L = \mathscr{C}_g(\mathcal{R}) \subset \mathscr{C}_f(\mathcal{R})$, and $f$ can be written in the form $f(x, y) = g(x, y)p(x, y)$, where $p(x, y)$ is some polynomial of degree $d - 1$.*

In connection with the above theorem, and in defining an elliptic curve $\mathscr{C}_f(\mathcal{R})$, where $f$ is a polynomial of degree three, we shall require that this curve be such that any straight line that passes through two points $(x_1, y_1), (x_2, y_2) \in \mathscr{C}_f(\mathcal{R})$, where the two points could be the same point if the curve at one of them is differentiable with the tangent at that point to the curve having same slope as that of the line, will also pass through a unique third point $(x_3, y_3)$. By the above theorem, if a line intersects the curve $\mathscr{C}_f(\mathcal{R})$ associated with the third order polynomial $f$ in more than three points, then the line itself is a subset of $\mathscr{C}_f(\mathcal{R})$. This will be excluded for the kind of third degree polynomials $f$ whose associated algebraic curves shall be called elliptic curves.

One other thing to be excluded, to have third order curves characterized as elliptic curves, is the existence of singular points on the curve, where a singular point is one where the curve does not admit a unique tangent.

It has to be mentioned that in the previous discussion, the points on the curve $\mathscr{C}_f(\mathbb{R})$ may lie at infinity. To deal with this situation we assume that the curve is in fact a curve in the real projective plane $\mathbb{P}_2(\mathbb{R})$. We now can define an **elliptic curve** $\mathscr{C}_f(\mathbb{R})$ as being such that $f(x, y)$ is an irreducible third order polynomial with $\mathscr{C}_f(\mathbb{R})$ having no singular points in $\mathbb{P}_2(\mathbb{R})$.

The main idea behind the above definition for elliptic curves is to have a curve whereby any two points $A$ and $B$ on the curve can determine a *unique* third point, to be denoted by $AB$, using a straight line joining $A$ and $B$. The possibilities are as follows: If the line joining $A$ and $B$ is not tangent to the curve $\mathscr{C}_f(\mathbb{R})$ at any point, then the line intersects the curve in exactly three different points two of which are $A$ and $B$ while the third is $AB$. If the line joining $A$ and $B$ is tangent to the curve at some point $p$ then either this line intersects $\mathscr{C}_f(\mathbb{R})$ in exactly two points, $p$ and some other point $p'$, or intersects the curve in only one point $p$. If the line intersects $\mathscr{C}_f(\mathbb{R})$ in two points $p$ and $p'$, then either $p = A = B$ in which case $AB = p'$, or $A \neq B$ in which case (irrespective of whether $p = A$ and $p' = B$ or vice-versa) one would have $p = AB$. While if the line intersects $\mathscr{C}_f(\mathbb{R})$ in only one point $p$ then $p = A = B = AB$.

The above discussion establishes a binary operation on elliptic curves that produces, for any two points $A$ and $B$ a uniquely defined third point $AB$. This binary operation in turn produces, as will be described next, another binary operation, denoted by $+$, that defines a group structure on $\mathscr{C}_f(\mathbb{R})$ that is associated with the straight-line construction discussed so far.

A group structure on an elliptic curve $\mathscr{C}_f(\mathbb{R})$ is defined as follows: Consider an arbitrary point, denoted by $0$, on $\mathscr{C}_f(\mathbb{R})$. We define, for any two points $A$ and $B$ on $\mathscr{C}_f(\mathbb{R})$, the point $A+B$ by

$$A + B = 0(AB), \tag{9.5}$$

meaning that we first determine the point $AB$ as above, then we determine the point $0(AB)$ corresponding to $0$ and $AB$. Irrespective of the choice of the point $0$, one has the following theorem on a group structure determined by $+$ on $\mathscr{C}_f(\mathbb{R})$.

**Theorem 94.** *Let $\mathscr{C}_f(\mathbb{R})$ be an elliptic curve, and let $0$ be any point on $\mathscr{C}_f(\mathbb{R})$. Then the above binary operation $+$ defines an Abelian group structure on $\mathscr{C}_f(\mathbb{R})$, with $0$ being the identity element and $-A = A(00)$ for every point $A$.*

The proof is very lengthy and can be found in [18]. We first note that if $0$ and $0'$ are two different points on an elliptic curve with associated binary operations $+$ and $+'$, then one can easily show that for any two points $A$ and $B$

$$A +' B = A + B - 0'. \tag{9.6}$$

This shows that the various group structures that can be defined on an elliptic curve by considering all possible points $0$ and associated operations $+$, are essentially the same, up to a ”translation”.

**Lemma 19.** *Consider the group structure on an elliptic curve $\mathscr{C}_f(\mathbb{R})$, corresponding to an operation $+$ with identity element $0$. If the cubic polynomial $f$ has rational coefficients, then the subset $\mathscr{C}_f(\mathbb{Q}) \subset \mathscr{C}_f(\mathbb{R})$ of rational solutions to $f(x,y) = 0$ forms a subgroup of $\mathscr{C}_f(\mathbb{R})$ if and only if $0$ is itself a rational point (i.e. a rational solution).*

*Proof.* If $\mathscr{C}_f(\mathbb{Q})$ is a subgroup of $\mathscr{C}_f(\mathbb{R})$, then it must contain the identity $0$, and thus $0$ would be a rational point. Conversely, assume that $0$ is a rational point. First, since $f$ has rational coefficients, then for any two rational points $A$ and $B$ in $\mathscr{C}_f(\mathbb{Q})$ one must have that $AB$ is also rational, and thus (since $0$ is assumed rational) that $0(AB)$ is rational, making $A + B = 0(AB)$ rational. Thus $\mathscr{C}_f(\mathbb{Q})$ would be closed under $+$. Moreover, since for every $A \in \mathscr{C}_f(\mathbb{Q})$ one has that $-A = A(00)$, then $-A$ is also rational, which makes $\mathscr{C}_f(\mathbb{Q})$ closed under inversion. Hence $\mathscr{C}_f(\mathbb{Q})$ is a subgroup. □

Thus by lemma 18, the set of all rational points on an elliptic curve form a subgroup of the group determined by the curve and a point $0$, if and only if the identity element $0$ is itself a rational point. In other words, one finds that if the elliptic curve $\mathscr{C}_f(\mathbb{R})$ contains one rational point $p$, then there exists a group structure on $\mathscr{C}_f(\mathbb{R})$, with $0 = p$ and the corresponding binary operation $+$, such that the set $\mathscr{C}_f(\mathbb{Q})$ of all rational points on $\mathscr{C}_f(\mathbb{R})$ is a group.

One thing to note about rational solutions to general polynomial functions $f(x, y)$, is that they correspond to integer solution to a corresponding *homogeneous* polynomial $h(X, Y, Z)$ in three variables, and vice-verse, where homogeneous practically means that this function is a linear sum of terms each of which has the same power when adding the powers of the variables involved in this term. For example $XY^2 - 2X^3 + XYZ + Z^3$ is homogeneous.

In fact a rational solution $x = a/b$ and $y = c/d$ for $f(x, y) = 0$, where $a, b, c, d$ are integers, can first be written as $x = ad/bd$ and $y = cb/bd$, and thus one can always have this solution in the form $x = X/Z$ and $y = Y/Z$, where $X = ad, Y = cb$ and $Z = bd$. If $x = X/Z$ and $y = Y/Z$ are replaced in $f(x, y) = 0$, one obtains a new version $h(X, Y, Z) = 0$ of this equation written in terms of the new variables $X, Y, Z$. One can immediately see that this new polynomial function $h(X, Y, Z)$ is homogeneous in $X, Y, Z$. The homogeneous function $h(X, Y, Z)$ in $X, Y, Z$ is the form that $f(x, y)$ takes in projective space, where in this case the transformations $x = X/Z$ and $y = Y/Z$ define the projective transformation that take $f(x, y)$ to $h(X, Y, Z)$.

If we now go back to cubic equation $f(x, y) = 0$, one can transform this function into its cubic homogeneous form $h(X, Y, Z) = 0$, where

$$\begin{aligned} h(X, Y, Z) = aX^3 &+ bX^2Y + cXY^2 + dY^3 + eX^2Z \\ &+ fXYZ + gY^2Z + hXZ^2 + iYZ^2 + jZ^3, \end{aligned} \tag{9.7}$$

by using the projective transformation $x = X/Z$ and $y = Y/Z$. Then, by imposing some conditions, such as requiring that the point $(1, 0, 0)$ (in projective space) satisfy this equation, and that the line tangent to the curve at the point $(1, 0, 0)$ be the $Z$-axis that intersects the curve in the point $(0, 1, 0)$, and that the $X$-axis is the line tangent to the curve at $(0, 1, 0)$, then one can immediately show that the homogeneous cubic equation above becomes of the form

$$h(X, Y, Z) = cXY^2 + eX^2Z + fXYZ + hXZ^2 + iYZ^2 + jZ^3. \tag{9.8}$$

Which, by using the projective transformation again, and using new coefficients, gives that points on the curve $\mathscr{C}_f(\mathbb{R})$ are precisely those on the curve $\mathscr{C}_h(\mathbb{R})$, where

$$h(x, y) = axy^2 + bx^2 + cxy + dx + ey + f. \tag{9.9}$$

And with further simple change of variables (consisting of polynomial functions in $x$ and $y$ with rational coefficients) one obtains that the points on the curve $\mathscr{C}_f(\mathbb{R})$ are precisely those on $\mathscr{C}_g(\mathbb{R})$ where

$$g(x, y) = y^2 - 4x^3 + g_2x - g_3, \tag{9.10}$$

i.e. that $\mathscr{C}_f(\mathbb{R}) = \mathscr{C}_g(\mathbb{R})$. The equation $g(x, y) = 0$, where $g$ is given in (8.10), is said to be the *Weierstrass normal form* of the equation $f(x, y) = 0$. Thus, in particular, any elliptic curve defined by a cubic $f$, is *birationally equivalent* to an elliptic curve defined by a polynomial $g(x, y)$ as above. Birational equivalence between curves is defined here as being a rational transformation, together with its inverse transformation, that takes the points on one curve to another, and vice-versa.

## 9.3 The Riemann Zeta Function

The Riemann zeta function $\zeta(z)$ is an analytic function that is a very important function in analytic number theory. It is (initially) defined in some domain in the complex plane by the special type of Dirichlet series given by

$$\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z}, \tag{9.11}$$

where $Re(z) > 1$. It can be readily verified that the given series converges locally uniformly, and thus that $\zeta(z)$ is indeed analytic in the domain in the complex plane $\mathbf{C}$ defined by $Re(z) > 1$, and that this function does not have a zero in this domain.

We first prove the following result which is called the Euler Product Formula.

**Theorem 95.** $\zeta(z)$*, as defined by the series above, can be written in the form*

$$\zeta(z) = \prod_{n=1}^{\infty} \frac{1}{\left(1 - \frac{1}{p_n^z}\right)}, \tag{9.12}$$

*where* $\{p_n\}$ *is the sequence of all prime numbers.*

*Proof.* knowing that if $|x| < 1$ then

$$\frac{1}{1-x} = \sum_{k=0}^{\infty} x^k, \tag{9.13}$$

one finds that each term $\frac{1}{1-\frac{1}{p_n^z}}$ in $\zeta(z)$ is given by

$$\frac{1}{1-\frac{1}{p_n^z}} = \sum_{k=0}^{\infty} \frac{1}{p_n^{kz}}, \tag{9.14}$$

since every $|1/p_n^z| < 1$ if $Re(z) > 1$. This gives that for any integer $N$

$$\begin{aligned}
\prod_{n=1}^{N} \frac{1}{\left(1 - \frac{1}{p_n^z}\right)} &= \prod_{n=1}^{N} \left(1 + \frac{1}{p_n^z} + \frac{1}{p_n^{2z}} + \cdots\right) \\
&= \sum \frac{1}{p_{n_1}^{k_1 z} \cdots p_{n_i}^{k_j z}} \qquad (9.15) \\
&= \sum \frac{1}{n^z}
\end{aligned}$$

where $i$ ranges over $1, \cdots, N$, and $j$ ranges from $0$ to $\infty$, and thus the integers $n$ in the third line above range over all integers whose prime number factorization consist of a product of powers of the primes $p_1 = 2, \cdots, p_N$. Also note that each such integer $n$ appears only once in the sum above.

Now since the series in the definition of $\zeta(z)$ converges absolutely and the order of the terms in the sum does not matter for the limit, and since, eventually, every integer $n$ appears on the right hand side of 8.15 as $N \longrightarrow \infty$, then $\lim_{N\to\infty} \left[\sum \frac{1}{n^z}\right]_N = \zeta(z)$. Moreover, $\lim_{N\to\infty} \prod_{n=1}^{N} \frac{1}{\left(1-\frac{1}{p_n^z}\right)}$ exists, and the result follows. □

The Riemann zeta function $\zeta(z)$ as defined through the special Dirichlet series above, can be continued analytically to an analytic function through out the complex plane **C** except to the point $z = 1$, where the continued function has a pole of order 1. Thus the continuation of $\zeta(z)$ produces a meromorphic function in **C** with a simple pole at 1. The following theorem gives this result.

**Theorem 96.** *$\zeta(z)$, as defined above, can be continued meromorphically in* **C**, *and can be written in the form $\zeta(z) = \frac{1}{z-1} + f(z)$, where $f(z)$ is entire.*

Given this continuation of $\zeta(z)$, and also given the functional equation that is satisfied by this continued function, and which is

$$\zeta(z) = 2^z \pi^{z-1} \sin\left(\frac{\pi z}{2}\right) \Gamma(1-z)\zeta(1-z), \qquad (9.16)$$

(see a proof in [3]), where $\Gamma$ is the complex gamma function, one can deduce that the continued $\zeta(z)$ has zeros at the points $z = -2, -4, -6, \cdots$ on the negative real axis. This follows as such: The complex gamma function $\Gamma(z)$ has poles at the points $z = -1, -2, -3, \cdots$ on the negative real line, and thus $\Gamma(1-z)$ must have poles at $z = 2, 3, \cdots$ on the positive real axis. And since $\zeta(z)$ is analytic at these points, then it must be that either $\sin\left(\frac{\pi z}{2}\right)$ or $\zeta(1-z)$ must have zeros at the points $z = 2, 3, \cdots$ to cancel out the poles of $\Gamma(1-z)$, and thus make $\zeta(z)$ analytic at these points. And since $\sin\left(\frac{\pi z}{2}\right)$ has zeros at $z = 2, 4, \cdots$, but not at $z = 3, 5, \cdots$, then it must be that $\zeta(1-z)$ has zeros at $z = 3, 5, \cdots$. This gives that $\zeta(z)$ has zeros at $z = -2, -4, -6\cdots$.

It also follows from the above functional equation, and from the above mentioned fact that $\zeta(z)$ has no zeros in the domain where $Re(z) > 1$, that these zeros at $z = -2, -4, -6\cdots$ of $\zeta(z)$ are the only zeros that have real parts either less that 0, or greater than 1. It was conjectured by Riemann, *The Riemann Hypothesis*, that every other zero of $\zeta(z)$ in the remaining strip $0 \leq Re(z) \leq 1$, all exist on the vertical line $Re(z) = 1/2$. This hypothesis was checked for zeros in this strip with very large modulus, but remains without a general proof. It is thought that the consequence of the Riemann hypothesis on number theory, provided it turns out to be true, is immense.

# Bibliography

[1] George E. Andrews, *Number Theory*, Dover, New York, 1994.

[2] George E. Andrews, *The Theory of Partitions*. Reprint of the 1976 original., Cambridge Mathematical Library. Cambridge University Press, Cambridge, 1998

[3] Tom M. Apostol, *Introduction to Analytic Number Theory*. Springer, New York, 1976.

[4] A. Baker, *Transcendantal Number Theory*, Cambridge University Press (London), 1975.

[5] J.W.S. Cassels, *An introduction to the Geometry of Numbers*, Springer-Verlag (Berlin), 1971.

[6] H. Davenport, *Multiplicative Number Theory*, 2nd edition, Springer-Verlag (New York), 1980.

[7] H. Davenport, *The higher Arithmetic: an introduction to the Theory of Numbers*, 7th edition, Cambridge University Press 1999.

[8] H.M. Edwards, *Riemann's Zeta Function*, Dover, New York, 2001.

[9] E. Grosswald, *Topics from the Theory of Numbers*. New York: The Macmillan Co. (1966).

[10] G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers*, 5th ed. Oxford University Press, Oxford, 1979.

[11] K.F. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag (New York), 1982.

[12] A. Ya. Khinchin, *Continued fractions*. With a preface by B. V. Gnedenko. Translated from the third (1961) Russian edition. Reprint of the 1964 translation. Dover Publications, Inc., Mineola, NY, 1997.

[13] M.I. Knopp, *Modular Functions in Analytic Number Theory*, Markham, Chicago 1970.

[14] E. Landau, *Elementary Number Theory*, Chelsea (New York), 1958.

[15] W.J. Leveque, *Elementary Theory of Numbers*, Dover, New York, 1990.

[16] W.J. Leveque, *Fundamentals of Number Theory*, Dover, New York, 1996.

[17] T. Nagell, *Introduction to Number Theory*, Chelsea (New York), 1981.

[18] I. Niven, H.L. Montgomery and H.S. Zuckerman, *An Introduction to the Theory of Numbers*, 5th edition, John Wiley and Sons 1991.

[19] A. J. Van der Poorten, *Continued fraction expansions of values of the exponential function and related fun with continued fractions*, Nieuw Arch. Wisk. (4) 14 (1996), no. 2, 221–230.

[20] H. Rademacher, *Lectures on Elementary Number Theory*. Krieger, 1977.

[21] Kenneth H. Rosen, *Elementary Number Theory and its Applications*. Fifth Edition. Pearson, Addison Wesley, USA, 2005.