

Brief description

These are notes for Math 314, an introductory course in elementary number theory. Students are advised to go through all sections in detail and attempt all problems. These notes will be modified and expanded as the course proceeds.

Contents

Math 314 Course Notes: Brief description	i
1 Fundamental notions	1
1.1 Mathematical Induction	1
1.2 Divisibility	3
1.3 Greatest common divisor and Euclidean algorithm	3
1.4 Prime numbers and unique factorization	8
2 Arithmetic Functions	11
2.1 Multiplicative Functions	11
2.2 Möbius function and Möbius inversion	13
2.3 Euler's Phi function	15
2.4 Greatest Integer Function	17
2.5 The big oh and small oh notations	19
2.6 Averages of arithmetical functions	20
3 Congruences	25
3.1 Definition and basic properties	25
3.2 Congruence powers and Euler's theorem	28
3.3 Linear congruence equations	30
3.4 Simultaneous linear congruences and the Chinese Remainder Theorem	33
3.5 Polynomial congruences	36
3.6 Order and primitive roots	42
4 Quadratic residues and the quadratic reciprocity law	47
4.1 Quadratic residues	47
4.2 Legendre symbol	49

4.3	Gauss' lemma	50
4.4	The Quadratic Reciprocity Law	53
4.5	Jacobi symbol	57
5	Sums of squares	61
5.1	Pythagorean triples	61
5.2	The equation $x^4 + y^4 = z^4$	62
5.3	Sums of two squares	64
5.4	Sums of four squares: Lagrange's theorem	66
6	Binary Quadratic Forms	69
6.1	Introduction to binary quadratic forms	69
6.2	Equivalence	71
6.3	Reduction of binary quadratic forms and class number	73
6.4	The representation of a number by a form	77
7	Continued Fractions and Pell's Equation	79
7.1	Finite continued fractions	79
7.2	Infinite Continued Fractions	84
7.3	Purely periodic continued fractions	92
7.4	Continued fraction expansion for $\sqrt{N}$	97
7.5	Pell's equation	98

Chapter 1

Fundamental notions

1.1 Mathematical Induction

Throughout these notes, we will denote the set of natural numbers as $\mathbb{N}$ and the set of integers as $\mathbb{Z}$.

We start this section with the following fundamental property of integers, namely the well-ordering principle:

Principle 1.1.1 [Well-ordering principle] *Every non-empty set of non-negative integers contains a least element.*

The well-known principle of mathematical induction follows from Principle 1.1.1.

Theorem 1.1.2 [Principle of mathematical induction] *Let S be a set of positive integers with the properties*

(a) $1 \in S$

(b) *If $k \in S$, then $k + 1 \in S$.*

Then $S = \mathbb{N}$.

Proof. Let T be the set of natural numbers which do not lie in S . Let us assume that T is non-empty. By Principle 1.1.1, T contains a least element, say t . Clearly, $t > 1$, since, by (a), $1 \in S$. Thus, $0 < t - 1 < t$. Since t is the least element in T , $t - 1$ is not in T and therefore is an element of S . But,

by part (b), if $t - 1$ is an element of S , then so is $(t - 1) + 1 = t$, which is a contradiction to the fact that t is an element of T . Thus, our assumption is false. This proves that T is empty and therefore $S = \mathbb{N}$. $\square$

In the above theorem, (a) is usually called the basis hypothesis and (b) is called the induction hypothesis.

Remark 1.1.3 *In some cases, in the basis hypothesis, 1 can be replaced by some other positive integer a . In this case, we conclude that S is the set of all integers $\geq a$.*

For various purposes, we use the induction principle in another form as given below:

Theorem 1.1.4 [Second principle of induction] *Let S be a set of positive integers with the properties*

(a) $1 \in S$

(b) *If $1, 2, 3, \dots, k \in S$, then $k + 1 \in S$.*

Then $S = \mathbb{N}$.

Proof. The proof is similar to that of Theorem 1.1.2. Let T be the set of natural numbers which do not lie in S and let us assume that T is non-empty. Applying the well-ordering principle, let t be the least element in T . Thus, $t > 1$, that is $t - 1 > 0$. Since t is the least element in T , neither of the elements $1, 2, \dots, t - 1$ lie in T . Thus, $1, 2, \dots, t - 1$ are elements of S and therefore, by induction hypothesis, so is t , which contradicts the fact that $t \in T$. Thus, our assumption is false and T is empty. This proves that $S = \mathbb{N}$. $\square$

Induction is a very strong tool in Mathematics, but one needs to understand when and in what form to use it.

Exercise 1.1.5 *Prove that for every natural number n ,*

$$1.1! + 2.2! + \dots + n.n! = (n + 1)! - 1.$$

Exercise 1.1.6 *Prove that for any natural number n ,*

$$1^3 + 2^3 + \dots + n^3 = \left[\frac{n(n + 1)}{2} \right]^2.$$

Exercise 1.1.7 *Prove that the cube of any integer can be written as the difference of two squares.*

Exercise 1.1.8 *Show that*

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

[Hint: $a^{n+1} - 1 = (a + 1)(a^n - 1) - a(a^{n-1} - 1)$.]

1.2 Divisibility

Let $a, b \in \mathbb{Z}$ with $b \neq 0$. We say that b divides a if there exists an integer c such that $bc = a$. Notationally, we write this as $b|a$. This is not to be confused with the rational number b/a .

We shall frequently appeal to the division algorithm, which is stated as follows:

Theorem 1.2.1 [Division Algorithm] *For any $a, b \in \mathbb{Z}$ with $b > 0$, there exist unique $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < b$.*

We prove this theorem by the following set of exercises:

Exercise 1.2.2 *Consider the set $S = \{a - xb : x \in \mathbb{Z}, \text{ and } a - xb \geq 0\}$. Prove that S is a non-empty set.*

Exercise 1.2.3 *Use the previous exercise to show that there exists an integer q such that $a - qb < b$.*

Exercise 1.2.4 *Prove Theorem 1.2.1. [Hint: the previous two exercises take care of existence of q and r . You now have to show that q and r under the restrictions of the theorem are unique.]*

1.3 Greatest common divisor and Euclidean algorithm

Definition 1.3.1 *For non-zero integers a and b , the greatest common divisor of a and b is the largest number that divides both of them.*

The greatest common divisor of a and b is denoted as $\gcd(a, b)$ or (a, b) . If $(a, b) = 1$, we say that a and b are **relatively prime** or **co-prime**. It is not too difficult to prove the following lemma:

Lemma 1.3.2 $d = (a, b)$ if and only if the following conditions hold:

- (a) $d|a$ and $d|b$
- (b) If $e|a$ and $e|b$, then $e|d$.

How does one find the gcd of two integers? The immediate idea that comes to mind is to factorize a and b and read off the common factors. However, this method is not feasible if the numbers involved are big! A more efficient algorithm, known as Euclidean algorithm, involves a successive application of the division algorithm till one hits the zero remainder. The general method is described as follows:

$$\begin{aligned}
 a &= q_1b + r_1, \quad 0 \leq r_1 < b \\
 b &= q_2r_1 + r_2, \quad 0 \leq r_2 < r_1 \\
 r_1 &= q_3r_2 + r_3, \quad 0 \leq r_3 < r_2 \\
 r_2 &= q_4r_3 + r_4, \quad 0 \leq r_4 < r_3 \\
 &\dots\dots\dots \\
 r_{n-3} &= q_{n-1}r_{n-2} + r_{n-1}, \quad 0 \leq r_{n-1} < r_{n-2} \\
 r_{n-2} &= q_nr_{n-1} + r_n, \quad 0 \leq r_n < r_{n-1} \\
 r_{n-1} &= q_{n+1}r_n + 0.
 \end{aligned}$$

The last nonzero remainder r_n is a common divisor of a and b . By Lemma 1.3.2, in order to prove this, we need to show two things.

- (a) $r_n|a$ and $r_n|b$
- (b) If $d|a$ and $d|b$, then $d|r_n$.

In order to prove (a), we observe that the last line $r_{n-1} = q_{n+1}r_n + 0$ shows that $r_n|r_{n-1}$. Then, the line before the last line shows that $r_n|r_{n-2}$, since it divides both r_n and r_{n-1} . Working our way up, step by step, we deduce that $r_n|b$ and $r_n|a$. To prove (b), let $d|a$ and $d|b$. From the first line $a = q_1b + r_1$, we see that $d|r_1$. From the second line, since $d|b$ and $d|r_1$, we see that $d|r_2$. Working our way down till the second last line, we get that $d|r_n$. Thus, we have proved both conditions (a) and (b). This implies, by Lemma 1.3.2, that $r_n = (a, b)$. Thus, we have proved the following theorem:

1.3. GREATEST COMMON DIVISOR AND EUCLIDEAN ALGORITHM 5

Theorem 1.3.3 [Euclidean algorithm] *To compute the gcd of two numbers a and b , taking $r_{-1} = a$ and $r_0 = b$, we compute successive quotients and remainders*

$$r_{i-1} = q_{i+1}r_i + r_{i+1}$$

for $i = 0, 1, 2, \dots$ until $r_{n+1} = 0$. The last nonzero remainder r_n is the gcd of a and b .

Remark 1.3.4 *The Euclidean algorithm terminates after a finite number of steps because the successive remainders are decreasing,*

$$r_0 > r_1 > r_2 > r_3 \cdots .$$

The remainders r_i are all ≥ 0 . So, we have a strictly decreasing sequence of non-negative integers, which eventually must reach 0.

Exercise 1.3.5 *Use the Euclidean algorithm to obtain $\gcd(143, 227)$, $\gcd(272, 1479)$, and $\gcd(54321, 9876)$.*

Exercise 1.3.6 *Let a and b be two nonzero integers. Consider the set*

$$S = \{ax + by : ax + by > 0; x, y \in \mathbb{Z}\}.$$

(a) *Show that S must contain a smallest element d .*

(b) *By the definition of S and (a), there exist integers x and y for which $d = ax + by$. Prove that $d|a$ and $d|b$.*

(c) *Finally, prove that $d = \gcd(a, b)$.*

This proves that the smallest positive value of $ax + by$ is the gcd of a and b .

There is yet another way to prove that there exist integers x and y such that $ax + by = (a, b)$. Observe that

$$\begin{aligned} \begin{pmatrix} a \\ b \end{pmatrix} &= \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} b \\ r_1 \end{pmatrix} = \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} \\ &= \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix} \\ &= A \begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix}, \end{aligned}$$

where A is some matrix with determinant equal to ± 1 . Thus, A^{-1} is a matrix with integer entries, say

$$A^{-1} = \begin{pmatrix} c & d \\ x & y \end{pmatrix},$$

such that

$$\begin{pmatrix} c & d \\ x & y \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix}.$$

Thus, there exist integers x and y such that $ax + by = r_n = (a, b)$.

In practice, how do you find integers x and y for which $ax + by = (a, b)$? We again work our way through the steps of the Euclidean algorithm as follows:

$$a = q_1b + r_1 \Rightarrow r_1 = a - q_1b,$$

$$b = q_2r_1 + r_2 \Rightarrow r_2 = b - q_2r_1,$$

which implies that

$$r_2 = b - q_2(a - q_1b) = -q_2a + (1 + q_1q_2)b.$$

Similarly,

$$\begin{aligned} r_3 &= r_1 - q_3r_2 \\ &= (a - q_1b) - q_3(-q_2a + (1 + q_1q_2)b) \\ &= (1 + q_2q_3)a - (q_1 + q_3 + q_1q_2q_3)b \end{aligned}$$

and so on. Finally, as we keep moving down, we get $r_n = ax + by$ for some integers x and y . We also observe that if x and y are solutions of the above linear equation, then, for any integer k , then $a(x + kb) + b(y - ka) = r_n$. Thus, the equation $ax + by = (a, b)$ has infinitely many integer solutions in x and y .

Exercise 1.3.7 Find integers x and y such that $95x + 432y = 1$. Show that there are infinitely many such integers.

Exercise 1.3.8 Show that if $(a, b) = 1$ and x_0, y_0 is an integer solution of $ax + by = 1$, then all solutions are of the form $x = x_0 + bk$, $y = y_0 - ak$ for an integer k .

1.3. GREATEST COMMON DIVISOR AND EUCLIDEAN ALGORITHM 7

Exercise 1.3.9 Let $d = \gcd(a, b)$. Show that the linear equation $ax + by = c$ has a solution if and only if $d \mid c$. Show, also, that if x_0, y_0 is a particular solution of this equation, then all other solutions are given by

$$x = x_0 + \frac{b}{d}k, y = y_0 - \frac{a}{d}k$$

for an integer k .

Exercise 1.3.10 Find integers x, y, z such that $35x + 55y + 77z = 1$. Show that there are infinitely many such integers.

Exercise 1.3.11 Prove that if $g_1, g_2, \dots$ are integers > 1 , then every natural number can be expressed uniquely in the form

$$a_0 + a_1g_1 + a_2g_1g_2 + \dots a_kg_1g_2 \dots g_k$$

with $0 \leq a_j < g_{j+1}$. Deduce that every natural number can be written in “factorial base” as

$$a_0 + a_11! + a_22! + \dots a_kk!$$

with $0 \leq a_i \leq i$.

Exercise 1.3.12 Let g be a natural number > 1 . Show that every natural number can be expressed uniquely in the form

$$n = a_0 + a_1g + a_2g^2 + \dots a_kg^k$$

with $0 \leq a_i < g$.

Exercise 1.3.13 Let a be a natural number > 1 . If $d \mid n$, then show that $a^d - 1$ divides $a^n - 1$.

Exercise 1.3.14 Let a be a natural number greater than 1. Show that

$$(a^m - 1, a^n - 1) = a^{(m,n)} - 1.$$

1.4 Prime numbers and unique factorization

A natural number is said to be a prime number if it does not have any divisors other than 1 and itself. In these notes, the letter p will denote a prime number. Using induction, we prove the following theorem:

Theorem 1.4.1 *Every integer $n > 1$ is either a prime number or a product of (not necessarily distinct) prime numbers.*

Proof. We use the second principle of induction as stated in Theorem 1.1.4. The theorem is clearly true for $n = 2$. Let us suppose that it is true for every integer $< n$. If n is prime, we are done. If not, then it has a divisor not equal to 1 and itself. Thus, $n = cd$ for some $1 < c < n$ and $1 < d < n$. By induction hypothesis, both c and d are products of prime numbers and therefore, so is $n = cd$. Thus, the theorem is proved by the second principle of induction. $\square$

Theorem 1.4.2 *If p is a prime and $p|ab$, then $p|a$ or $p|b$.*

Proof. Suppose p is a prime such that $p|ab$. If p does not divide a , then p and a are relatively prime. By Exercise 1.3.6, there exist integers x and y such that $ax + py = 1$. Thus, $abx + pby = b$. Since $p|ab$, we have, $p|(abx + pby)$ and therefore, $p|b$. $\square$

Exercise 1.4.3 *If p divides a product $a_1a_2 \cdots a_n$ for integers a_i , prove that p divides one of the a_i 's.*

We are now ready to prove the Fundamental Theorem of Arithmetic:

Theorem 1.4.4 [Fundamental Theorem of Arithmetic] *Every integer $n \geq 2$ can be factored uniquely into a product of primes.*

Remark 1.4.5 *If n itself is a prime, we consider n to be a product of a single number. Rearrangement of prime factors of a number is not a new factorization. Thus, while Theorem 1.4.1 states that any n can be factorized into a product of primes in some way, the Fundamental Theorem of Arithmetic makes a stronger assertion that n can be factorized into such a product in only one way, up to a rearrangement of factors.*

Proof. We have already proved the factorization of n into a product of primes in Theorem 1.4.1. We are now left with proving uniqueness. Let us apply an inductive argument again. The theorem is clearly true for $n = 2$. Let us suppose that it is true for all positive integers $2 \leq k < n$. Suppose we have

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_s,$$

where p_i 's and q_j 's are primes. Thus, $p_1 | q_1(q_2 q_3 \cdots q_s)$. By Theorem 1.4.2, either $p_1 = q_1$ or $p_1 | q_2 q_3 \cdots q_s$. By a repeated application of Theorem 1.4.2, we see that $p_1 = q_j$, for some $1 \leq j \leq s$, say $j = 1$. Thus, by cancellation, we get

$$p_2 p_3 \cdots p_k = q_2 q_3 \cdots q_s.$$

Since $p_2 p_3 \cdots p_k < n$, by induction hypothesis, we get that for each $2 \leq i \leq k$, p_i equals q_j for some $2 \leq j \leq s$. This proves the theorem for n and by second principle of induction, for all positive integers ≥ 2 . $\square$

Exercise 1.4.6 Prove that if n is a composite number, then n has a prime factor not exceeding $\sqrt{n}$.

Exercise 1.4.7 Show that there are infinitely many primes. [Hint: Suppose there are only finitely many primes $p_1, p_2, \dots, p_n$. What can you say about the prime factors of $N = p_1 p_2 \cdots p_n + 1$?]

Exercise 1.4.8 Let p_n denote the n -th prime. Prove that

$$p_{n+1} \leq p_1 p_2 \cdots p_n - 1.$$

Deduce that for all $n \geq 1$,

$$p_n \leq 2^{2^n}.$$

Finally, show that if $\pi(x)$ denotes the number of primes less than or equal to x , then

$$\pi(x) \geq \log \log x \text{ for all } x \geq 2.$$

Exercise 1.4.9 (a) Recall that for any real number a such that $|a| < 1$,

$$(1 - a)^{-1} = 1 + a + a^2 + \cdots.$$

Prove that

$$\sum_{n \leq x} \frac{1}{n} \leq \prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1}.$$

(b) Recall also that if $|a| < 1$, then

$$-\log(1-a) = a + \frac{a^2}{2} + \frac{a^3}{3} + \cdots.$$

Using this, prove that for any prime p ,

$$-\log\left(1 - \frac{1}{p}\right) - \frac{1}{p} \leq \frac{1}{p(p-1)}.$$

(c) Deduce that

$$-\sum_{p \leq x} \log\left(1 - \frac{1}{p}\right) \leq \sum_{p \leq x} \frac{1}{p} + 1.$$

(d) Using the fact that the series $\sum_{n \geq 1} \frac{1}{n}$ diverges, prove that the series

$$\sum_p \frac{1}{p}$$

diverges. [Hint: Take logarithms of the inequality in (a)]

Exercise 1.4.10 (a) Let $f(t)$ be a monotonically decreasing, continuous function on $[0, \infty)$. Prove that for any $N \geq 2$,

$$\int_1^N f(t)dt \leq \sum_{n=1}^{N-1} f(n) \leq \int_0^{N-1} f(t)dt.$$

(b) Taking $f(t) = \frac{1}{t+1}$, show that for a positive real number $x \geq 2$,

$$1 + \log([x] + 1) - \log 2 \leq \sum_{n \leq x} \frac{1}{n} \leq 1 + \log([x]).$$

(c) Deduce that

$$\log \log x \leq \log \left(\sum_{n \leq x} \frac{1}{n} \right).$$

(d) Conclude that

$$\sum_{p \leq x} \frac{1}{p} \geq \log \log x - 1.$$

Chapter 2

Arithmetic Functions

2.1 Multiplicative Functions

An **arithmetic function** $f : \mathbb{N} \rightarrow \mathbb{C}$ is a complex valued function defined on the set of natural numbers. An arithmetic function is said to be **multiplicative** if $f(mn) = f(m)f(n)$ whenever $\gcd(m, n) = 1$. A function is called **completely multiplicative** if $f(mn) = f(m)f(n)$ for all $m, n \in \mathbb{N}$. Henceforth, n will denote a natural number unless otherwise specified. Also, a divisor of n will refer to a positive divisor of n .

Examples 2.1.1 • $f(n) = 1$ for all $n \in \mathbb{N}$ is a completely multiplicative function.

- For a fixed $a \in \mathbb{N}$, the function $f(n) = n^a$ is completely multiplicative.
- Let $\nu(n)$ denote the number of distinct prime divisors of n . $\nu(n)$ is not a multiplicative function. However, the function $f(n) = (-1)^{\nu(n)}$ is a multiplicative function, but not completely multiplicative.

We now state and prove an important theorem which helps us to construct new multiplicative functions out of existing ones.

Theorem 2.1.2 *If f is a multiplicative function, then the function g defined by*

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

is also multiplicative. Here the sum runs over all divisors of n . Moreover, if

$$n = \prod_{p^a || n} p^a$$

is the unique factorization of n into powers of distinct primes, then

$$g(n) = \prod_{p^a || n} (1 + f(p) + f(p^2) + \cdots + f(p^a)).$$

Proof. To begin with, we observe that if $(m, n) = 1$, then any divisor d of mn can be written as $d_1 d_2$, such that $d_1 | m$, $d_2 | n$ and $(d_1, d_2) = 1$. Thus, if $(m, n) = 1$, then

$$g(mn) = \sum_{d | mn} f(d) = \sum_{\substack{d = d_1 d_2 \\ d_1 | m \\ d_2 | n}} f(d_1 d_2).$$

Since f is multiplicative, the above is equal to

$$\sum_{\substack{d_1 | m \\ d_2 | n}} f(d_1) f(d_2) = g(m) g(n).$$

Thus, g is multiplicative. It follows that, given the above factorization of n ,

$$g(n) = \prod_{p^a || n} g(p^a) = \prod_{p^a || n} (1 + f(p) + f(p^2) + \cdots + f(p^a)). \quad (2.1)$$

□

Example 2.1.3 For any $s \in \mathbb{Z}_{\geq 0}$, let

$$\sigma_s(n) := \sum_{d | n} d^s.$$

In particular, for $s = 0$, $\sigma_0(n)$ is simply the number of positive divisors of n . $\sigma_0(n)$ is also denoted as $d(n)$ and $\tau(n)$ in the existing literature. Since the function $f(n) = n^s$ for any $s \in \mathbb{Z}_{\geq 0}$ is multiplicative, by applying Theorem 2.1.2, we deduce that σ_s is also a multiplicative function.

Exercise 2.1.4 For a prime p , we say that $p^a || n$ if $p^a | n$ but $p^{a+1} \nmid n$. For any $n \geq 1$, let

$$n = \prod_{p^a || n} p^a$$

be the unique factorization of n into powers of distinct primes. Prove that

$$\sigma_0(n) = \prod_{p^a || n} (a + 1)$$

and, for any $s \in \mathbb{N}$,

$$\sigma_s(n) = \prod_{p^a || n} \frac{p^{s(a+1)} - 1}{p^s - 1}.$$

Henceforth, we will denote $\sigma_0(n)$ as $d(n)$ and $\sigma_1(n)$ as $\sigma(n)$.

Exercise 2.1.5 Show that $d(n)$ is odd if and only if n is a perfect square.

Exercise 2.1.6 Show that the product of the divisors of n is equal to $n^{d(n)/2}$.

Definition 2.1.7 Given two arithmetic functions f and g , their **Dirichlet product** or **Dirichlet convolution** $f * g$ is the function defined by

$$f * g(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right).$$

Exercise 2.1.8 If f and g are multiplicative functions, so is their Dirichlet convolution $f * g$.

2.2 Möbius function and Möbius inversion

A number n is said to be square-free if $p^2 \nmid n$ for any prime p . In other words, a square-free number has no square factors > 1 . The Möbius function μ is defined as follows:

$$\mu(n) = \begin{cases} (-1)^{\nu(n)} & \text{if } n \text{ is square-free,} \\ 0 & \text{otherwise.} \end{cases}$$

Exercise 2.2.1 Show that μ is a multiplicative function.

By Theorem 2.1.2, we deduce that $g(n) := \sum_{d|n} \mu(d)$ is also a multiplicative function.

Exercise 2.2.2 *Prove that*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Remark 2.2.3 *The above “reinterpretation” of 1 in terms of the Möbius function is an important tool in analytic number theory. As we will see in the coming pages, it has many applications.*

Theorem 2.2.4 [Möbius inversion formula] *Let f and g be arithmetic functions. Then*

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

if and only if

$$f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right).$$

Proof. We observe that

$$\begin{aligned} \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) &= \sum_{d|n} \mu(d) \sum_{e|\frac{n}{d}} f(e) \\ &= \sum_{d: ad=n} \mu(d) \sum_{e: es=a} f(e) \\ &= \sum_{des=n} \mu(d) f(e) \\ &= \sum_{e|n} f(e) \sum_{d|\frac{n}{e}} \mu(d). \end{aligned}$$

By Exercise 2.2.2, the inner sum equals 1 if $e = n$ and 0 otherwise. Thus,

$$\sum_{e|n} f(e) \sum_{d|\frac{n}{e}} \mu(d) = f(n).$$

The converse is proved in a similar way and is left as an exercise. $\square$

Exercise 2.2.5 Let $\Lambda(n) = \log p$ if n is a power of the prime p and 0 otherwise. Show that

$$\log n = \sum_{d|n} \Lambda(d).$$

Deduce that

$$\Lambda(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \log d,$$

where μ denotes the Möbius function.

2.3 Euler's Phi function

A very important arithmetic function is Euler's ϕ -function, which is defined to be the number of positive integers less than or equal to n , which are coprime to n . That is,

$$\phi(n) := \sum_{\substack{k \leq n \\ (k,n)=1}} 1.$$

Möbius inversion formula gives us an elegant proof of the fact that $\phi(n)$ is multiplicative and also establishes a formula for $\phi(n)$.

Exercise 2.3.1 Show that $\sum_{d|n} \phi(d) = n$. From this, deduce that

$$\phi(n) = n \sum_{d|n} \frac{\mu(d)}{d}.$$

Exercise 2.3.2 Show that ϕ is a multiplicative function. Deduce that

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

Exercise 2.3.3 For any $n \geq 1$, prove that $\sqrt{n} \leq \phi(n)$. If n is composite, then prove that $\phi(n) \leq n - \sqrt{n}$.

Exercise 2.3.4 Show that if $\phi(n)$ is odd, then $n = 1$ or $n = 2$.

Exercise 2.3.5 Let $f(n)$ be the sum of the natural numbers $\leq n$ which are coprime to n .

1. Show that

$$1 + 2 + \cdots + n = \sum_{d|n} df(n/d).$$

Deduce that for $n > 1$, $f(n) = n\phi(n)/2$.

2. Show that $f(n)$ is divisible by n for $n > 2$.

3. Show that the numerator of the sum of the reciprocals of the natural numbers $\leq n$ which are coprime to n is divisible by n .

Exercise 2.3.6 Prove that

$$\sum_{d|n} \frac{\mu^2(d)}{\phi(d)} = \frac{n}{\phi(n)}.$$

Exercise 2.3.7 Prove that

$$\sum_{m|n} d(m)\phi\left(\frac{n}{m}\right) = \sigma(n)$$

and

$$\sum_{m|n} \sigma(m)\phi\left(\frac{n}{m}\right) = nd(n).$$

Exercise 2.3.8 If n is a squarefree integer, prove that

$$\sum_{d|n} \sigma(d^{k-1})\phi(d) = n^k.$$

Exercise 2.3.9 Let

$$J_r(n) = n^r \prod_{p|n} \left(1 - \frac{1}{p^r}\right).$$

For $r = 1$, $J_r(n) = \phi(n)$. Prove that

$$n^r = \sum_{d|n} J_r(d).$$

2.4 Greatest Integer Function

Let x be a real number. The **greatest integer of x** , denoted by $[x]$ is the largest integer $\leq x$. In other words, it is the unique integer satisfying $x - 1 < [x] \leq x$. For example,

$$\left[\frac{5}{2}\right] = 2, [\sqrt{2}] = 1.$$

We note that $[x] = x$ if and only if $x \in \mathbb{Z}$. The difference $x - [x]$ is called the **fractional part of x** and is denoted by $\{x\}$. Clearly, $0 \leq \{x\} < 1$.

Exercise 2.4.1 1. $[x + n] = [x] + n$ for any $n \in \mathbb{Z}$.

2. For any $x, y \in \mathbb{R}$, $[x] + [y] \leq [x + y]$.

3. For any $n \in \mathbb{N}$,

$$\left[\frac{x}{n}\right] = \left[\frac{[x]}{n}\right].$$

4. For any $n, m, k \in \mathbb{N}$,

$$\left[\frac{nm}{k}\right] \geq n \left[\frac{m}{k}\right].$$

Exercise 2.4.2 Let n be a positive integer and p be a prime.

1. Prove that for any $k \geq 1$, exactly $[n/p^k]$ multiples of p^k occur in $n!$.

2. Conclude that the highest power of p that divides $n!$ is

$$\sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right].$$

3. Prove that

$$n! = \prod_{p \leq n} p^{\sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right]}.$$

Exercise 2.4.3 Find the highest power of 10 dividing 2000!.

Exercise 2.4.4 Let $n, r \in \mathbb{N}$ and $1 \leq r < n$. Let $\binom{n}{r}$ denote the binomial coefficient defined as

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}.$$

- (a) Find the highest power of p dividing $r!(n-r)!$.
- (b) For each prime factor p of $r!(n-r)!$, prove that

$$\sum_{k \geq 1} \left[\frac{n}{p^k} \right] \geq \sum_{k \geq 1} \left[\frac{r}{p^k} \right] + \sum_{k \geq 1} \left[\frac{n-r}{p^k} \right].$$

- (c) Show that $\binom{n}{r}$ is an integer.

Exercise 2.4.5 Prove that for a positive integer r , the product of any r consecutive integers is divisible by r .

Exercise 2.4.6 Let f and g be arithmetic functions such that

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

Then, for any $x \geq 1$,

$$\sum_{n \leq x} g(n) = \sum_{n \leq x} f(n) \left[\frac{x}{n} \right].$$

Exercise 2.4.7 Prove that for any $k \geq 0$,

$$\sum_{n \leq x} \sigma_k(n) = \sum_{n \leq x} n^k \left[\frac{x}{n} \right].$$

In particular, we get

$$\sum_{n \leq x} d(n) = \sum_{n \leq x} \left[\frac{x}{n} \right].$$

Exercise 2.4.8 Prove that

$$\sum_{n \leq x} \mu(n) \left[\frac{x}{n} \right] = 1.$$

Deduce that

$$\left| \sum_{n \leq x} \frac{\mu(n)}{n} \right| \leq 1 \text{ for all } x \geq 1.$$

2.5 The big oh and small oh notations

Definition 2.5.1 For a complex valued function $f(x)$ and a real valued function $g(x)$ such that $g(x) > 0$ for all $x \geq a$, we write $f(x) = O(g(x))$ (and say that $f(x)$ is big oh of $g(x)$) if there exists a constant $C > 0$ such that

$$|f(x)| \leq Cg(x) \text{ for all } x \geq a.$$

Definition 2.5.2 For functions $f(x)$ and $g(x)$, we write $f(x) = o(g(x))$ and say that $f(x)$ is little oh of $g(x)$ if

$$\lim_{x \rightarrow \infty} \frac{f(x)}{g(x)} = 0.$$

Definition 2.5.3 For functions $f(x)$ and $g(x)$, we write $f(x) \sim g(x)$ and say that $f(x)$ is asymptotic to $g(x)$ if

$$\lim_{x \rightarrow \infty} \frac{f(x)}{g(x)} = 1.$$

Exercise 2.5.4 Show that $d(n) = O(\sqrt{n})$.

Exercise 2.5.5 Let $\nu(n)$ denote the number of distinct prime divisors of n . Prove that $\nu(n) = O(\log n)$. More precisely,

$$\nu(n) \leq \frac{\log n}{\log 2}.$$

Exercise 2.5.6 Let $f(x)$ be a monotonically decreasing, continuous function defined on $[a-1, b+1]$. Prove that

$$\int_{a-1}^b f(t)dt > \sum_{j=a}^b f(j) > \int_a^{b+1} f(t)dt.$$

Deduce that

$$\sum_{j=a}^b f(j) = \int_a^b f(t)dt + O(|f(a-1)| + |f(b)|).$$

Exercise 2.5.7 Show that

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

Exercise 2.5.8 Show that $\sigma(n) = O(n \log n)$, where $\sigma(n)$ or $\sigma_1(n)$, as defined in Example 2.1.3 refers to the sum of the (positive) divisors of n .

2.6 Averages of arithmetical functions

Many arithmetic functions of interest to us fluctuate a lot and it is difficult to study their behaviour. For example, $d(n)$ does not seem to follow any smooth pattern as n increases. It takes the value 2 infinitely often and right next to a prime may lie a composite number with a large number of prime divisors and therefore a large number of divisors. For arithmetic functions of this nature, we study the arithmetic mean

$$\frac{1}{n} \sum_{k=1}^n f(k).$$

Definition 2.6.1 *Let f be an arithmetic function and let g be a monotonically increasing function on $\mathbb{R}$. We say that the average order of $f(n)$ is $g(n)$ if*

$$\lim_{x \rightarrow \infty} \frac{\sum_{n \leq x} f(n)}{xg(x)} = 1,$$

that is, if

$$\sum_{n \leq x} f(n) \sim xg(x).$$

Exercise 2.6.2 *Show that the average order of $d(n)$ is $\log n$.*

Solution. Observe, by Exercise 2.4.7, that

$$\begin{aligned} \sum_{n \leq x} d(n) &= \sum_{n \leq x} \sum_{d|n} 1 \\ &= \sum_{n \leq x} \sum_{d: de=n} 1 \\ &= \sum_{d \leq x} \sum_{e \leq \frac{x}{d}} 1 \\ &= \sum_{d \leq x} \left[\frac{x}{d} \right]. \end{aligned}$$

Now, $[x] = x - \{x\} = x + O(1)$. Thus, from above,

$$\begin{aligned}
 \sum_{n \leq x} d(n) &= \sum_{d \leq x} \left[\frac{x}{d} \right] \\
 &= \sum_{d \leq x} \frac{x}{d} + O\left(\sum_{d \leq x} 1\right) \\
 &= x \sum_{d \leq x} \frac{1}{d} + O(x) \\
 &= x(\log x + O(1)) + O(x) \\
 &= x \log x + O(x).
 \end{aligned}$$

From this, we deduce

$$\lim_{x \rightarrow \infty} \left(\frac{\sum_{n \leq x} d(n)}{x \log x} \right) = \lim_{x \rightarrow \infty} \left(1 + O\left(\frac{1}{\log x}\right) \right) = 1.$$

Thus, the average order of $d(n)$ is $\log n$.

□

Exercise 2.6.3 Let $f(x)$ be a monotonically decreasing and continuous function on $[1, \infty)$. Prove that, for any $x \geq 1$,

$$\sum_{n > x} f(n) \leq \int_{[x]}^{\infty} f(t) dt.$$

Deduce that

$$\sum_{n \leq x} \frac{1}{n^2} = \zeta(2) + O\left(\frac{1}{x}\right),$$

where

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \text{ for any } s > 1.$$

Exercise 2.6.4 Show that the average order of $\sigma(n)$ is

$$\frac{\zeta(2)}{2} n.$$

One would be tempted to follow a procedure similar to the one followed in Exercise 2.6.2, that is, apply Exercise 2.4.7 to get

$$\begin{aligned}
 \sum_{n \leq x} \sigma(n) &= \sum_{d \leq x} d \left[\frac{x}{d} \right] \\
 &= \sum_{d \leq x} d \left(\frac{x}{d} + O(1) \right) \\
 &= x \sum_{d \leq x} 1 + \sum_{d \leq x} O(d) \\
 &= x[x] + O(x^2) \\
 &= x(x + O(1)) + O(x^2) \\
 &= O(x^2).
 \end{aligned}$$

But, this calculation does not give us the average order of $\sigma(n)$. We probably threw away too much information in this estimation and hence, do not have a main term. We re-examine $\sum_{n \leq x} \sigma(n)$ as follows:

Solution.

$$\begin{aligned}
\sum_{n \leq x} \sum_{d: de=n} e &= \sum_{d \leq x} \sum_{e \leq \frac{x}{d}} e \\
&= \sum_{d \leq x} \left\{ 1 + 2 + \cdots + \left\lfloor \frac{x}{d} \right\rfloor \right\} \\
&= \sum_{d \leq x} \frac{1}{2} \left\lfloor \frac{x}{d} \right\rfloor \left(\left\lfloor \frac{x}{d} \right\rfloor + 1 \right) \\
&= \frac{1}{2} \sum_{d \leq x} \left(\frac{x}{d} + O(1) \right) \left(\frac{x}{d} + O(1) \right) \\
&= \frac{1}{2} \sum_{d \leq x} \left[\frac{x^2}{d^2} + O\left(\frac{x}{d}\right) \right] \\
&= \frac{x^2}{2} \sum_{d \leq x} \frac{1}{d^2} + O\left(x \sum_{d \leq x} \frac{1}{d}\right) \\
&= \frac{x^2}{2} \left(\zeta(2) - \sum_{d > x} \frac{1}{d^2} \right) + O(x \log x) \\
&= \frac{x^2}{2} \left(\zeta(2) + O\left(\frac{1}{x}\right) \right) + O(x \log x) \\
&= \frac{x^2}{2} \zeta(2) + O(x \log x).
\end{aligned}$$

This proves that the average order of $\sigma(n)$ is

$$\frac{\zeta(2)}{2}n.$$

□

Exercise 2.6.5 (a) Let f and g be two arithmetic functions such that

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

and the series $\sum_{n=1}^{\infty} \frac{f(n)}{n^s}$ and $\sum_{n=1}^{\infty} \frac{g(n)}{n^s}$ are absolutely convergent for $s > 1$. Show that, for any $s > 1$,

$$\zeta(s) \sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \sum_{n=1}^{\infty} \frac{g(n)}{n^s}.$$

(b) Using (a), prove that if $s > 1$,

$$\zeta(s) \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = 1.$$

(c) Show that

$$\sum_{n \leq x} \phi(n) = \frac{x^2}{2\zeta(2)} + O(x \log x).$$

$$[\text{Hint: } \phi(n) = \sum_{d|n} \mu(d) \frac{n}{d}.]$$

(d) Conclude that the average order of $\phi(n)$ is $\frac{n}{2\zeta(2)}$.

Exercise 2.6.6 Let n and k be positive integers and $k > 1$. Then, n is said to be k -free if it is not divisible by the k -th power of any prime number. Let $s_k(n) = 1$ if n is k -free and 0 otherwise. Show that

$$\sum_{n \leq x} s_k(n) = c_k x + O(x^{1/k}),$$

where

$$c_k = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^k}.$$

Chapter 3

Congruences

3.1 Definition and basic properties

In this book *Disquisitiones Arithmeticae*, Gauss introduced the notion of congruences, which provides a natural and convenient approach to address problems related to divisibility of integers. The theory of congruences makes the theory of divisibility more or less analogous to the theory of equations.

Definition 3.1.1 *Let a, b and m be integers with $m > 0$. We say that a is **congruent to b modulo m** and write $a \equiv b \pmod{m}$ if m divides $a - b$. The number m is said to be the **modulus** of the congruence.*

Thus, $a \equiv 0 \pmod{m}$ if and only if $m|a$. If $m \nmid a - b$, we write $a \not\equiv b \pmod{m}$.

By division algorithm, given $a, n \in \mathbb{Z}$, such that $n > 0$, there exist unique integers q and r such that $0 \leq r < n$ such that $a = qn + r$. This implies that given a fixed integer $n > 0$, for any $a \in \mathbb{Z}$, there exists a unique $0 \leq r < n$ such that $a \equiv r \pmod{n}$. We call r the **residue** of $a \pmod{n}$. The set

$$\{x \in \mathbb{Z} : x \equiv r \pmod{n}\}$$

is called the **residue class** or **congruence class** $r \pmod{n}$. A set of m elements, one belonging to each residue class $r \pmod{m}$ is called a **complete residue system modulo m** .

The following theorem describes important properties of congruence:

Theorem 3.1.2 *Let a, b, c, d, n be integers with $n > 0$. Then*

- (i) $a \equiv a \pmod{n}$.
- (ii) If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.
- (iii) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.
- (iv) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a \pm c \equiv b \pm d \pmod{n}$ and $ac \equiv bd \pmod{n}$.

Proof. The above properties can be proved easily and are left to the reader as an exercise. $\square$

From the above theorem, we immediately conclude the following:

Corollary 3.1.3 *If $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$ for any positive integer k . More generally, let $f(x)$ be a polynomial with integer coefficients. If $a \equiv b \pmod{n}$, then $f(a) \equiv f(b) \pmod{n}$.*

Exercise 3.1.4 *Prove that $2^{2^5} + 1$ is divisible by 641.*

Exercise 3.1.5 *Prove that $5n^3 + 7n^5 \equiv 0 \pmod{12}$ for all integers n .*

Exercise 3.1.6 *Prove that a positive integer is divisible by 9 if and only if the sum of its digits is divisible by 9.*

Exercise 3.1.7 *What is the remainder when $1^5 + 2^5 + \cdots + 100^5$ is divided by 4?*

Exercise 3.1.8 *If p is a prime such that $n < p < 2n$, show that*

$$\binom{2n}{n} \equiv 0 \pmod{p}.$$

Theorem 3.1.9 *If $c > 0$, then $a \equiv b \pmod{n}$ if and only if $ac \equiv bc \pmod{nc}$.*

Proof. This follows trivially from the fact that $n|(b-a)$ if and only if $cn|c(b-a)$. $\square$

Theorem 3.1.10 *If $ac \equiv bc \pmod{n}$ and if $d = (c, n)$, then*

$$a \equiv b \pmod{\frac{n}{d}}.$$

Proof.

$$ac \equiv bc \pmod{n} \Rightarrow n|c(a - b).$$

By Theorem 3.1.9, the above implies

$$\frac{n}{d} \mid \frac{c}{d}(a - b).$$

Since

$$\left(\frac{n}{d}, \frac{c}{d}\right) = 1,$$

we get

$$\frac{n}{d} \mid (a - b).$$

Thus,

$$a \equiv b \pmod{\frac{n}{d}}.$$

□

Exercise 3.1.11 If $a \equiv b \pmod{n}$, then show that $(a, n) = (b, n)$.

Theorem 3.1.12 $a \equiv b \pmod{n}$ if and only if a and b give the same remainder when divided by n .

Proof. Let $a = nq_1 + r_1$ and $b = nq_2 + r_2$ such that $0 \leq r_1, r_2 < n$. Clearly, $a - b \equiv r_1 - r_2 \pmod{n}$. So $a \equiv b \pmod{n}$ if and only if $r_1 - r_2 \equiv 0 \pmod{n}$. Since, $0 \leq |r_1 - r_2| < n$, we observe that $r_1 - r_2 \equiv 0 \pmod{n}$ if and only if $r_1 - r_2 = 0$, that is $r_1 = r_2$. Thus, $a \equiv b \pmod{n}$ if and only if they have the same remainder when divided by n . □

Recall the Euler ϕ -function

$$\phi(n) = \#\{1 \leq a \leq n; (a, n) = 1\}.$$

In Exercise 2.3.2, we showed that $\phi(n)$ is a multiplicative function. In the following exercise, we will prove this again using the theory of congruences.

Exercise 3.1.13 (a) Given integers a, m, n show that $(a, mn) = 1$ if and only if $(a, m) = (a, n) = 1$. Thus,

$$\begin{aligned} & \{1 \leq a \leq mn : (a, mn) = 1\} \\ &= \{1 \leq a \leq mn : (a, m) = (a, n) = 1\}. \end{aligned}$$

- (b) Let $m, n > 1$. Let us arrange all integers between 1 and mn by clubbing them into m columns and n rows as follows:

$$\begin{array}{cccccc}
 1 & 2 & \dots & r & \dots & m \\
 m+1 & m+2 & \dots & m+r & \dots & 2m \\
 \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
 (n-1)m+1 & (n-1)m+2 & \dots & (n-1)m+r & \dots & nm
 \end{array}$$

where $1 \leq r \leq m$. We denote the r -th column as C_r .

Show that all the numbers in C_r are co-prime to m if and only if r is co-prime to m . This tells us that only $\phi(m)$ columns contain numbers co-prime to m and every number in such a column is co-prime to m .

- (c) Let $(m, n) = 1$. Show that no two numbers in C_r are congruent $(\text{mod } n)$. Deduce that elements in C_r are congruent $(\text{mod } n)$ to $0, 1, 2, \dots, n-1$ in some order.
- (d) Deduce that each C_r contains $\phi(n)$ elements co-prime to n .
- (e) Finally, deduce that if $(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.

3.2 Congruence powers and Euler's theorem

Let $n > 0$ and $(a, n) > 1$. Can we have $a^k \equiv 1 \pmod{n}$ for some $k \geq 1$? If this were possible, then we would have an integer y such that $a^k - ny = 1$. But, since $(a, n) > 1$, this would imply that $a^k - ny$ would have a divisor greater than 1, which is not possible. Hence, for a^k to be congruent to 1 mod n it is necessary that $(a, n) = 1$.

Theorem 3.2.1 Let $(a, n) = 1$. Then we have

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Proof. Let $b_1, b_2, \dots, b_{\phi(n)}$ be the $\phi(n)$ numbers lying between 1 and $n-1$ which are co-prime to n . Since $(a, n) = 1$, we have $(b_i a, n) = 1$ for all $1 \leq i \leq \phi(n)$. Thus, by Exercise 3.1.11, each number in the list

$$b_1 a, b_2 a, \dots, b_{\phi(n)} a \pmod{n}$$

is congruent to some number in the list $b_1, b_2, \dots, b_{\phi(n)}$. Suppose

$$b_i a \equiv b_j a \pmod{n} \text{ for some } 1 \leq b_i \leq b_j \leq \phi(n).$$

Then, $n \mid (b_j a - b_i a)$, which implies that $n \mid (b_j - b_i)$, since $(a, n) = 1$. But, $0 \leq |b_j - b_i| < n$. So, $n \mid (b_j - b_i)$ if and only if $b_i = b_j$. Thus, the residues of

$$b_1 a, b_2 a, \dots, b_{\phi(n)} a \pmod{n}$$

are distinct $\pmod{n}$. This means that the list of residues of

$$b_1 a, b_2 a, \dots, b_{\phi(n)} a \pmod{n}$$

is the same as the list

$$b_1, b_2, \dots, b_{\phi(n)},$$

though the numbers may be in a different order. Hence, by Theorem 3.1.12, the product of all the numbers in the first list is congruent to the product of all the numbers in the second list $\pmod{n}$. Thus,

$$b_1 b_2 \cdots b_{\phi(n)} \equiv a^{\phi(n)} b_1 b_2 \cdots b_{\phi(n)} \pmod{n}.$$

Since $(b_1 b_2 \cdots b_{\phi(n)}, n) = 1$, we deduce

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

□

Corollary 3.2.2 [Fermat's little theorem] *If p is a prime and $(a, p) = 1$, then*

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

Proof. Since $\phi(p) = p - 1$, this follows from the above theorem. □

Exercise 3.2.3 *Find the last two digits of 23^{1000} .*

Exercise 3.2.4 *Check if the integer $53^{103} + 103^{53}$ is divisible by 39 and if $111^{333} + 333^{111}$ is divisible by 7.*

3.3 Linear congruence equations

In a high school algebra class, we have learnt to solve certain equations of the form $f(x) = 0$, where $f(x)$ is a polynomial with integer coefficients. We can also consider congruence equations of the form $f(x) \equiv 0 \pmod{m}$ and ask how many solutions such an equation has. We first need to understand what we mean by a solution of a congruence equation. If an integer x satisfies the equation $f(x) \equiv 0 \pmod{m}$, so does any integer $y \equiv x \pmod{m}$, by Corollary 3.1.3. Thus, every congruence equation having one integer solution has infinitely many integer solutions. We therefore do not count solutions which belong to the same residue class as distinct. Henceforth, the number of solutions of $f(x) \equiv 0 \pmod{m}$, will refer to the number of incongruent solutions of this equation, or in other words, the number of integer solutions of this equation contained in the set $\{1, 2, \dots, m\}$.

In this section, we consider polynomials $f(x)$ of degree 1, in other words, equations of the form $ax \equiv b \pmod{m}$.

For example, how many solutions does $2x \equiv 3 \pmod{4}$ have? Observe that neither of $x = 1, 2, 3, 4$ satisfies this congruence. Therefore, this equation does not have a solution. For large values of m , it is not feasible to check for solutions to $ax \equiv b \pmod{m}$ by checking all residues mod m . We now state some theorems which explicitly determine how many solutions a linear congruence equation has and how to find those solutions.

Theorem 3.3.1 *Let $(a, m) = 1$. The linear congruence equation $ax \equiv b \pmod{m}$ has exactly one solution.*

Proof. Consider the set $\{a, 2a, 3a, \dots, ma\}$. If $ia \equiv ja \pmod{m}$ for some $1 \leq i \leq j \leq m$, then $m \mid (i - j)a$. Since $(a, m) = 1$, this implies that $m \mid (i - j)$, which is possible only when $i = j$, since $0 \leq j - i \leq m - 1$. Thus, any two elements in the above set are incongruent to each other $\pmod{m}$. That is, the above set forms a complete residue system mod m . Thus, there exists a unique integer x lying between 1 and m such that $ax \equiv 1 \pmod{m}$. $\square$

Remark 3.3.2 *How do we determine the solution of $ax \equiv b \pmod{m}$? Observe that this is equivalent to finding integers x and y such that $ax + my = b$. To do so, we first find integers X and Y such that $aX + mY = 1$. This can be done using the method described after Exercise 1.3.6. Then, $x = bX$, $y = bY$ are solutions of $ax + my = b$. We reduce x modulo m to solve $ax \equiv b \pmod{m}$.*

Theorem 3.3.3 *Let $(a, m) = d$. The linear congruence equation $ax \equiv b \pmod{m}$ has a solution if and only if $d|b$.*

Proof. Suppose $ax \equiv b \pmod{m}$ has a solution. This implies that there exist integers x, y such that $ax + my = b$. Since $d|ax$ and $d|my$, we deduce that $d|b$.

Conversely, suppose $d = (a, m)$ divides b . Since $(a/d, m/d) = 1$, the congruence

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$$

has a solution by Theorem 3.3.1. By Theorem 3.1.9, this solution is also a solution of $ax \equiv b \pmod{m}$.

□

Theorem 3.3.4 *Let $(a, m) = d$ and $d|b$. The linear congruence*

$$ax \equiv b \pmod{m} \tag{3.1}$$

has exactly d solutions modulo m . Let t be the unique solution $\pmod{m/d}$ of the linear congruence

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}. \tag{3.2}$$

Then the solutions of $ax \equiv b \pmod{m}$ are given by

$$t, t + \frac{m}{d}, t + 2\frac{m}{d}, \dots, t + (d-1)\frac{m}{d},$$

Proof. By Theorem 3.1.9, any solution of equation 7.4 is also a solution of equation 7.3. Moreover, if an integer t satisfies the congruence equation 7.4, so does any integer of the form $t + j\frac{m}{d}$, $j \in \mathbb{Z}$. Therefore,

$$t, t + \frac{m}{d}, t + 2\frac{m}{d}, \dots, t + (d-1)\frac{m}{d},$$

are solutions of equation 7.4 and therefore of equation 7.3. Suppose

$$t + j\frac{m}{d} \equiv t + k\frac{m}{d} \pmod{m} \text{ for some } 0 \leq j < k \leq d-1.$$

This implies

$$j\frac{m}{d} \equiv k\frac{m}{d} \pmod{m}$$

and therefore

$$j \equiv k \pmod{d}.$$

But $0 \leq k - j \leq d - 1$. So, $j = k$. In other words, the solutions

$$t, t + \frac{m}{d}, t + 2\frac{m}{d}, \dots, t + (d - 1)\frac{m}{d}$$

are incongruent mod m .

Finally, we show that any solution of equation 7.3 is contained in the above list. Let t_0 be a solution of equation 7.3. Then $at_0 \equiv at \pmod{m}$.

$$\begin{aligned} m|a(t - t_0) &\Rightarrow \frac{m}{d}d|a(t - t_0) \\ &\Rightarrow \frac{m}{d}|\frac{a}{d}(t - t_0) \\ &\Rightarrow \frac{m}{d}|(t - t_0) \\ &\Rightarrow t \equiv t_0 \pmod{\frac{m}{d}}. \end{aligned}$$

Thus

$$t_0 = t + l\frac{m}{d} \text{ for some } l \in \mathbb{Z}.$$

But, $l \equiv r \pmod{d}$ for some $0 \leq r \leq d - 1$. Therefore,

$$l\frac{m}{d} \equiv r\frac{m}{d} \pmod{m}.$$

Thus,

$$t_0 = t + l\frac{m}{d} \equiv r\frac{m}{d} \pmod{m} \text{ for some } 0 \leq r \leq d - 1,$$

that is any solution of equation 7.3 is contained in the list

$$t, t + \frac{m}{d}, t + 2\frac{m}{d}, \dots, t + (d - 1)\frac{m}{d}.$$

□

Exercise 3.3.5 Solve the linear congruences:

(a) $25x \equiv 15 \pmod{29}$

(b) $140x \equiv 133 \pmod{301}$

(c) $3x \equiv 20 \pmod{99}$

3.4 Simultaneous linear congruences and the Chinese Remainder Theorem

A Chinese mathematical work from the early fourth century posed the following problem:

We have a number of things, but we do not know exactly how many. If we count them by threes, we have two left over. If we count them by fives, we have three left over. If we count them by sevens, we have two left over. How many things are there?

Sun Tzu Suan Ching (Master Sun's Mathematical Manual)
Circa AD 300, Volume 3, Problem 26

In the language of congruences, Master Sun is asking us to find a positive integer x satisfying the following system of equations:

$$x \equiv 2 \pmod{3},$$

$$x \equiv 3 \pmod{5},$$

$$x \equiv 2 \pmod{7}.$$

The first equation tells us that $x = 3t + 2$ for some integer t . Substituting this in second and third equations, we have $3t \equiv 1 \pmod{5}$ and $3t \equiv 0 \pmod{7}$. Since $(3, 7) = 1$, we get $t \equiv 0 \pmod{7}$, that is, $t = 7y$ for some $y \in \mathbb{Z}$. Since $3t \equiv 1 \pmod{5}$, we have $21y \equiv 1 \pmod{5}$, which implies, $y \equiv 1 \pmod{5}$. We deduce that $y = 5k + 1$, $t = 7y = 35k + 7$ and finally, $x = 3t + 2 = 105k + 23$. So any positive integer x of the form $105k + 23$ satisfies all the congruence equations above. That is, the above system of congruences has exactly one solution between 1 and 105. That is, this system has a unique solution

$$x \equiv 23 \pmod{105}.$$

On the other hand, there is no x simultaneously satisfying $x \equiv 1 \pmod{2}$ and $x \equiv 0 \pmod{4}$. Notice that while 3, 5 and 7 are mutually co-prime, 2 and 4 are not co-prime. The following theorem describes the conditions under which systems of linear congruences can be solved.

Theorem 3.4.1 [Chinese Remainder Theorem] *Let $n_1, n_2, \dots, n_k$ be mutually coprime positive integers, that is, $(n_i, n_j) = 1$ for all $i \neq j$. Then, the system of congruences*

$$x \equiv c_1 \pmod{n_1}$$

$$\begin{aligned}
x &\equiv c_2 \pmod{n_2} \\
&\vdots \\
x &\equiv c_k \pmod{n_k}
\end{aligned}$$

has a unique solution $\pmod{n_1 n_2 \cdots n_k}$.

Proof. Let $N = n_1 n_2 \cdots n_k$ and $N_i = N/n_i$ for each $1 \leq i \leq k$. Then $(n_i, N_i) = 1$. Thus for each N_i , there exists a unique N'_i modulo n_i such that $N_i N'_i \equiv 1 \pmod{n_i}$. Consider

$$x = \sum_{i=1}^k c_i N_i N'_i.$$

For each i , $c_i N_i N'_i \equiv c_i \pmod{n_i}$ and $N_j \equiv 0 \pmod{n_i}$ whenever $i \neq j$. Thus, for each $1 \leq i \leq k$,

$$\sum_{i=1}^k c_i N_i N'_i \equiv c_i \pmod{n_i}.$$

Thus, x satisfies every congruence in the system. We now show that x is unique $\pmod{N}$. Suppose x and y are two integers satisfying all the equations above. Then $x \equiv y \pmod{n_i}$ for each $1 \leq i \leq k$. Since n_i 's are mutually co-prime, we get $x \equiv y \pmod{N}$. $\square$

Exercise 3.4.2 Show that

$$x = c_1 N_1^{\phi(n_1)} + c_2 N_2^{\phi(n_2)} + \cdots + c_k N_k N_k^{\phi(n_k)}$$

is a simultaneous solution to the above system of congruences.

In the next few exercises, we practice using Chinese Remainder Theorem and also look at systems where n_i 's are not mutually co-prime.

Exercise 3.4.3 Find a simultaneous solution $\pmod{900}$ for the system

$$x \equiv 3 \pmod{4}$$

$$x \equiv 2 \pmod{9}$$

$$x \equiv 1 \pmod{25}$$

3.4. SIMULTANEOUS LINEAR CONGRUENCES AND THE CHINESE REMAINDER THEOREM

Exercise 3.4.4 Find the last two digits in the expansion of 4^{1000} .

Exercise 3.4.5 Prove that

$$a^{560} \equiv 1 \pmod{561}$$

for every a coprime to 561.

Exercise 3.4.6 Let us consider two sets A and B where

$$A = \{a : 1 \leq a \leq mn \text{ such that } \gcd(a, mn) = 1\}$$

and

$$B = \{(b, c) : 1 \leq b \leq m, 1 \leq c \leq n, \gcd(b, m) = 1, \gcd(c, n) = 1\}$$

Remember that the set B contains pairs (or 2-tuples) of certain numbers. Now, define a function $f : A \rightarrow B$ as follows:

$$f(a \bmod mn) = (a \bmod m, a \bmod n).$$

Thus, f takes an integer a in the first set and sends it to a pair (b, c) with $a \equiv b \bmod m$ and $a \equiv c \bmod n$.

(a) Show that f is injective (one-to-one).

(b) Show that f is surjective (onto). [Hint: Use CRT]

(c) From the above, conclude that $\phi(mn) = \phi(m)\phi(n)$.

Exercise 3.4.7 Find an integer x that satisfies

$$x \equiv 6 \pmod{15}, x \equiv 9 \pmod{14}.$$

Is this integer unique? Is this integer unique $\pmod{210}$?

Exercise 3.4.8 Show that the system of congruences

$$x \equiv 5 \pmod{6}$$

$$x \equiv 7 \pmod{10}$$

has more than one solution modulo 60.

3.5 Polynomial congruences

In this section, we will study congruence equations of the form $f(x) \equiv 0 \pmod{n}$, where $f(x)$ is a polynomial with integer coefficients. To motivate this discussion, let us start with simple polynomials of degree 2, which play an important role in number theory.

Let p be a prime. Consider $f(x) = x^2 - 1$. How many solutions modulo p does the equation $x^2 \equiv 1 \pmod{p}$ have? Observe that

$$\begin{aligned} x^2 \equiv 1 \pmod{p} &\Rightarrow p \mid (x^2 - 1) \\ &\Rightarrow p \mid (x - 1)(x + 1) \\ &\Rightarrow \text{Either } p \mid (x - 1) \text{ or } p \mid (x + 1) \\ &\Rightarrow x \equiv \pm 1 \pmod{p}. \end{aligned}$$

$1 \equiv -1 \pmod{p}$ if and only if $p = 2$. Thus, $x^2 \equiv 1 \pmod{p}$ has a unique solution if $p = 2$ and has exactly two solutions if p is an odd prime. This fact has an interesting consequence:

Theorem 3.5.1 [Wilson's Theorem] *If p is a prime, then $(p - 1)! \equiv -1 \pmod{p}$.*

Proof. Consider the numbers $1, 2, \dots, p - 1$. Among these numbers, 1 and $p - 1$ satisfy $x^2 \equiv 1 \pmod{p}$. By Theorem 3.3.1, for each $2 \leq a \leq p - 2$, there exists a unique $2 \leq a' \leq p - 2$ such that $aa' \equiv 1 \pmod{p}$. Moreover $a \neq a'$, since $a^2 \equiv 1 \pmod{p}$ if and only if $a = 1, p - 1$. Thus, $2 \cdot 3 \cdots (p - 2) \equiv 1 \pmod{p}$. Moreover $p - 1 \equiv -1 \pmod{p}$. Thus, $1 \cdot 2 \cdot 3 \cdots (p - 1) \equiv -1 \pmod{p}$. $\square$

Corollary 3.5.2 $(n - 1)! \equiv -1 \pmod{n}$ if and only if n is a prime.

Proof. Sufficiency is proved by Wilson's theorem. If n is not a prime, then there exist $1 \leq a, b \leq n - 1$ such that $ab = n$. If $a \neq b$, then clearly $n \mid (n - 1)!$, since both a and b are factors of $(n - 1)!$. If $a = b$, that is, if $n = a^2$, then for $n > 4$, both a and $2a$ lie between 1 and $n - 1$. Thus, $n = a^2$ divides $(n - 1)!$. Therefore, $(n - 1)! \equiv 0 \pmod{n}$. For $n = 4$, one immediately checks that $3! \not\equiv -1 \pmod{4}$. Thus, $(n - 1)! \equiv -1 \pmod{n}$ if and only if n is a prime. $\square$

As a consequence of Wilson's theorem, we also make the following observation:

Corollary 3.5.3 *For a prime p ,*

$$(-1)^{\frac{p-1}{2}} \left[\left(\frac{p-1}{2} \right)! \right]^2 \equiv -1 \pmod{p}.$$

Proof. For any integer i lying between 1 and $(p-1)/2$, we observe that

$$p - i \equiv -i \pmod{p}.$$

Thus,

$$\begin{aligned} (p-1)! &= 1 \cdot 2 \cdots (p-1) \\ &= 1 \cdot 2 \cdots \frac{p-1}{2} \left(p - \frac{p-1}{2} \right) \cdots (p-2)(p-1) \\ &\equiv (-1)^{\frac{p-1}{2}} \left[\left(\frac{p-1}{2} \right)! \right]^2 \pmod{p}. \end{aligned}$$

Thus, by Wilson's theorem, for a prime p ,

$$(-1)^{\frac{p-1}{2}} \left[\left(\frac{p-1}{2} \right)! \right]^2 \equiv -1 \pmod{p}.$$

□

We now prove a theorem regarding the solutions of $x^2 \equiv -1 \pmod{p}$.

Theorem 3.5.4 *For an odd prime p , $x^2 \equiv -1 \pmod{p}$ has a solution if and only if $p \equiv 1 \pmod{4}$.*

Proof. Suppose $x^2 \equiv -1 \pmod{p}$ has a solution $x = a$. Thus,

$$a^{p-1} \equiv (a^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}. \quad (3.3)$$

Clearly, $(a, p) = 1$, otherwise $a^2 \equiv 0 \not\equiv -1 \pmod{p}$. Thus, by Theorem 3.2.2, we have

$$a^{p-1} \equiv 1 \pmod{p}. \quad (3.4)$$

Combining equations (3.3) and (3.4), we get

$$(-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Therefore, $(p-1)/2$ is even. That is, $p \equiv 1 \pmod{4}$. Conversely, suppose $p \equiv 1 \pmod{4}$. Then $(p-1)/2$ is even. Thus, by Corollary 3.5.3,

$$\left[\left(\frac{p-1}{2} \right)! \right]^2 \equiv -1 \pmod{p},$$

and therefore,

$$x^2 \equiv -1 \pmod{p}$$

has a solution. $\square$

Exercise 3.5.5 Find all integer solutions of $y^2 = 23x^3 + 22$ if any. [Hint: Consider the above equation modulo 23.]

Let us now try and solve some other quadratic congruences (that is, quadratic equations formed by polynomials of degree 2):

Exercise 3.5.6 Find the solutions, if any, of the following quadratic congruences:

(a) $x^2 + 4x + 12 \equiv 0 \pmod{13}$

(b) $3x^2 + 9x + 7 \pmod{11}$

Recall, from high school algebra, that to solve the quadratic equation,

$$ax^2 + bx + c = 0, a \neq 0,$$

we simplified it into

$$a \left(\left(x + \frac{b}{a} \right)^2 - \left(\frac{b^2 - 4ac}{4a^2} \right) \right) = 0.$$

Thus,

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

To what extent does this calculation hold mod p ? For an odd prime p , if $(a, p) = 1$, then we can solve

$$2ax \equiv 1 \pmod{p}.$$

If we can solve the equation

$$y^2 \equiv b^2 - 4ac \pmod{p},$$

then $x(-b \pm y)$ will be solutions of

$$ax^2 + bx + c \equiv 0 \pmod{p}.$$

Thus, solving a quadratic congruence reduces to the problem of solving a linear congruence and a congruence of the form

$$y^2 \equiv A \pmod{p},$$

for a given integer A .

Exercise 3.5.7 *Show that for any prime p , the equation*

$$x^3 \equiv 1 \pmod{p}$$

will have either one solution or three solutions. Explain under what conditions it will have three solutions.

We therefore ask the following questions:

- Under what conditions does $y^2 \equiv A \pmod{p}$ have a solution?
- How many solutions can it possibly have?

We postpone the discussion of the first question to the next section. The second question is answered by the following theorem of Lagrange:

Theorem 3.5.8 [Lagrange's theorem] *Given a prime p , let*

$$f(x) = a_0 + a_1x + \cdots + a_nx^n, \quad a_i \in \mathbb{Z}$$

be a polynomial of degree n such that $a_n \not\equiv 0 \pmod{p}$. Then the polynomial congruence

$$f(x) \equiv 0 \pmod{p}$$

has at most n solutions.

Proof. We prove this theorem by induction. Since $a_1 \not\equiv 0 \pmod{p}$, by Theorem 3.3.1, the equation

$$a_1x + a_0 \equiv 0 \pmod{p}$$

has a unique solution. Thus, the theorem is true for $n = 1$. Suppose that the theorem is true for polynomials of degree $n - 1$. Assume, also, that the equation

$$a_0 + a_1x + \cdots + a_nx^n \equiv 0 \pmod{p}, \quad a_n \not\equiv 0 \pmod{p}$$

has $n + 1$ incongruent solutions mod p , say $x_0, x_1, \dots, x_n$. We have

$$f(x) - f(x_0) = \sum_{k=1}^n a_k(x^k - x_0^k) = (x - x_0)g(x),$$

where degree of $g(x)$ is $n - 1$ and the leading coefficient of $g(x)$ is a_n which is $\not\equiv 0 \pmod{p}$. We observe that for every $1 \leq k \leq n$,

$$f(x_k) \equiv f(x_0) \pmod{p}.$$

Thus,

$$f(x_k) - f(x_0) = (x_k - x_0)g(x_k) \equiv 0 \pmod{p}.$$

Since x_k and x_0 are incongruent mod p , we get

$$g(x_k) \equiv 0 \pmod{p}$$

for every $1 \leq k \leq n$. Thus, $g(x) \equiv 0 \pmod{p}$ has n incongruent solutions mod p , which contradicts our induction hypothesis that it can have at most $n - 1$ solutions. Therefore,

$$a_0 + a_1x + \cdots + a_nx^n \equiv 0 \pmod{p}, \quad a_n \not\equiv 0 \pmod{p}$$

has at most n solutions. By induction, we have proved the result for all $n \geq 1$. $\square$

Remark 3.5.9 *The above theorem may not hold for a composite modulus n . For example,*

$$x^2 - 1 \equiv 0 \pmod{8}$$

has 4 solutions.

From Lagrange's theorem, we deduce the following corollary:

Corollary 3.5.10 *If p is a prime number and $d|p-1$, then the congruence equation*

$$x^d - 1 \equiv 0 \pmod{p}$$

has exactly d solutions.

Proof. Let $p-1 = dk$ for some integer k . Then

$$x^{p-1} - 1 = (x^d - 1)(x^{d(k-1)} + x^{d(k-2)} + \cdots + x + 1).$$

That is, $x^{p-1} - 1 = (x^d - 1)f(x)$, where $f(x)$ is a polynomial with integer coefficients of degree $p-1-d$. By Theorem 3.2.2, we know that

$$x^{p-1} - 1 \equiv 0 \pmod{p}$$

has exactly $p-1$ solutions (namely $x = 1, 2, \dots, p-1$). By Lagrange's theorem, we know that $x^d - 1 \equiv 0 \pmod{p}$ has at most d roots and $f(x) \equiv 0 \pmod{p}$ has at most $p-1-d$ roots. Therefore, $x^d - 1 \equiv 0 \pmod{p}$ must have exactly d roots, since if it has fewer than d roots, the number of roots of the equations

$$x^{p-1} - 1 \equiv 0 \pmod{p}$$

and

$$(x^d - 1)f(x) \equiv 0 \pmod{p}$$

will not match up. $\square$

Exercise 3.5.11 *If p is an odd prime, prove that the congruence equation*

$$x^{p-2} + \cdots + x^2 + x + 1 \equiv 0 \pmod{p}$$

has exactly $p-2$ solutions and they are $2, 3, \dots, p-2$.

Exercise 3.5.12 *Let $n = p_1 p_2 \cdots p_k$, where p_i 's are distinct primes.*

- (a) *Show that if all the p_i 's are odd, then the number of solutions to $x^2 \equiv 1 \pmod{n}$ is 2^k .*
- (b) *Show that if $p_i = 2$ for some i , then the above congruence has 2^{k-1} solutions.*

3.6 Order and primitive roots

Let a and m be co-prime integers such that $m > 0$. By Euler's theorem (Theorem 3.2.1), we know that

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

However, there might be a smaller power $k \leq \phi(m)$ for which $a^k \equiv 1 \pmod{m}$.

Definition 3.6.1 *The smallest positive integer k for which*

$$a^k \equiv 1 \pmod{m}$$

is called the order of a modulo m and is denoted by $\text{ord}_m(a)$. If

$$\text{ord}_m(a) = \phi(m),$$

*then a is called a **primitive root** of m or a primitive root mod m .*

Exercise 3.6.2 Find $\text{ord}_7(2)$ and $\text{ord}_7(3)$.

Theorem 3.6.3 *Let a and m be co-prime integers such that $m > 0$. Let $k = \text{ord}_m(a)$. Then*

- (a) $a^l \equiv 1 \pmod{m}$ if and only if $l \equiv 0 \pmod{k}$.
- (b) $a^i \equiv a^j \pmod{m}$ if and only if $i \equiv j \pmod{k}$.
- (c) The numbers $1, a, a^2, \dots, a^{k-1}$ are incongruent mod m .

Proof.

- (a) If $l \equiv 0 \pmod{k}$, then clearly $a^l \equiv 1 \pmod{m}$. Conversely, suppose $a^l \equiv 1 \pmod{m}$. By division algorithm, we know that there exist unique integers q and r such that $l = qk + r$, such that $0 \leq r < k$. Observe that

$$a^r \equiv 1. a^r \equiv a^{kq} a^r \equiv a^{qk+r} \equiv a^l \equiv 1 \pmod{m}.$$

Since $k = \text{ord}_m(a)$ and $r < k$, we get $r = 0$. Thus, $l = qk$ and therefore $l \equiv 0 \pmod{k}$.

- (b) This follows easily from (a).

(c) Suppose

$$a^i \equiv a^j \pmod{m} \text{ for some } 1 \leq i \leq j \leq m.$$

By part (b), this means that

$$i \equiv j \pmod{k}.$$

Since $0 \leq j - i \leq k - 1$, this is not possible unless $j - i = 0$, that is, $j = i$. Thus, the numbers $1, a, a^2, \dots, a^{k-1}$ are incongruent mod m .

□

For any modulus m , let $a_1, a_2, \dots, a_{\phi(m)}$ denote all the integers between 1 and $m - 1$ which are co-prime to m . Any collection of $\phi(m)$ integers, which are incongruent mod m and each of which is congruent to one of the a_i 's is called a **reduced residue system** (mod m). Theorem 3.6.3(c) tells us that if a is a primitive root of m , then $\{a, a^2, \dots, a^{\phi(m)}\}$ forms a reduced residue system (mod m).

Exercise 3.6.4 Let $(a, m) = 1$. Prove that a is a primitive root of m if and only if $\{a, a^2, \dots, a^{\phi(m)}\}$ forms a reduced residue system (mod m).

Exercise 3.6.5 Knowing that 2 is a primitive root of 19, find all $a \pmod{19}$ for which

$$x^2 \equiv a \pmod{19}$$

has a solution.

Theorem 3.6.6 For a prime p and a divisor d of $p - 1$, let

$$\psi(d) = \{1 \leq a \leq p - 1 : \text{ord}_p(a) = d\}.$$

Then

$$d = \sum_{d_i | d} \psi(d_i).$$

Therefore, $\phi(d) = \psi(d)$.

Proof. If $x^d \equiv 1 \pmod{p}$, then $\text{ord}_p(x)$ divides d . So, if we look at all the divisors of d and for each divisor d_i of d , consider

$$A(d_i) = \{1 \leq x \leq p - 1 : \text{ord}_p(x) = d_i\},$$

then

$$\bigcup_{d_i|d} A(d_i) = \{1 \leq x \leq p-1 : x^d \equiv 1 \pmod{p}\}.$$

From Theorem 3.5.10, we know that if $d|p-1$, then the congruence equation

$$x^d - 1 \equiv 0 \pmod{p}$$

has exactly d solutions. Thus, we deduce that

$$d = \sum_{d_i|d} |A(d_i)| = \sum_{d_i|d} \psi(d_i),$$

where $|A(d_i)|$ denotes the numbers of elements in $A(d_i)$. By Möbius inversion and Exercise 2.3.1, we get

$$\psi(d) = \sum_{d_i|d} \frac{d}{d_i} \mu(d_i) = \phi(d).$$

□

From this, we conclude one of the most important results in number theory:

Theorem 3.6.7 [Primitive Root Theorem] *Every prime p has a primitive root.*

Proof. Applying Theorem 3.6.6 for $d = p-1$ and noting that $\phi(p-1) \geq 1$ for all primes p , we see that every prime p has a primitive root. In fact, it has exactly $\phi(p-1)$ primitive roots. □

Exercise 3.6.8 *If $a = b^2$ is a perfect square and p is an odd prime, can a be a primitive root of p ?*

Exercise 3.6.9 *Find all primitive roots of 17.*

The primitive root theorem helps us to answer a question raised in the previous section, namely when does the equation $x^2 \equiv a \pmod{p}$ have a solution.

Theorem 3.6.10 [Euler's criterion] *Let p be an odd prime and $(a, p) = 1$. Then,*

$$x^2 \equiv a \pmod{p}$$

has a solution if and only if

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Proof. Suppose $x^2 \equiv a \pmod{p}$ has a solution, say $x = x_1$. Since $(a, p) = 1$, we have $(x_1, p) = 1$. Thus,

$$a^{\frac{p-1}{2}} \equiv (x_1^2)^{\frac{p-1}{2}} \equiv x_1^{p-1} \equiv 1 \pmod{p},$$

by Fermat's little theorem. Conversely, suppose

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

By primitive root theorem, p has a primitive root, say, r . So,

$$a \equiv r^k \pmod{p} \text{ for some } 1 \leq k \leq p-1.$$

This implies

$$(r^k)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

But $\text{ord}_p(r) = p-1$. Therefore, by Theorem 3.6.3(a), we have

$$(p-1) \mid \frac{k(p-1)}{2}.$$

Thus, k is an even integer, say $k = 2l$. Thus,

$$a \equiv r^k \equiv r^{2l} \equiv (r^l)^2 \pmod{p}.$$

That is, $x = r^l$ is a solution of $x^2 \equiv a \pmod{p}$. $\square$

In particular, Theorem 3.5.4 is a special case of Euler's criterion.

Exercise 3.6.11 *Prove that there exist infinitely many primes of the form $4n+1$. [Hint: Suppose there were only finitely many primes of this kind and let N denote their product. What can you say about any prime factor of $4N^2+1$?]*

Exercise 3.6.12 *Check if the congruence $x^2 \equiv -1 \pmod{95}$ has a solution.*

Exercise 3.6.13 *Does the congruence*

$$x^2 \equiv 2 \pmod{61}$$

have any solutions? Why or why not? Is 2 a primitive root of 61? Why or why not?

Exercise 3.6.14 *Does the congruence*

$$x^2 \equiv 2 \pmod{61}$$

have any solutions? Why or why not?

Chapter 4

Quadratic residues and the quadratic reciprocity law

4.1 Quadratic residues

Definition 4.1.1 *Let p be a prime. A nonzero integer that is congruent to a square modulo p is called a **quadratic residue (QR)** $(\text{mod } p)$. In other words, any nonzero integer a , which is co-prime to p is said to be a quadratic residue $(\text{mod } p)$ if the equation*

$$x^2 \equiv a \pmod{p}$$

*has a solution. A nonzero integer that is not congruent to a square modulo p is called a **quadratic nonresidue (QNR)** $(\text{mod } p)$.*

For example, 1 and 4 are QRs $(\text{mod } 5)$ and 1, 2 and 4 are QRs $(\text{mod } 7)$. 2 and 3 are QNRs $(\text{mod } 5)$ and 3, 5 and 6 are QNRs $(\text{mod } 7)$.

Theorem 4.1.2 *Let p be an odd prime. Then every reduced residue system $(\text{mod } p)$ has exactly $(p-1)/2$ quadratic residues and exactly $(p-1)/2$ quadratic nonresidues $(\text{mod } p)$. The quadratic residues are the residues containing the numbers*

$$1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2.$$

Proof. We know that the elements of a reduced residue system $(\text{mod } p)$ are

$$1, 2, 3, \dots, p-1.$$

So, the quadratic residues $(\text{mod } p)$ are

$$1^2, 2^2, \dots, (p-1)^2.$$

However,

$$\frac{p+1}{2} \leq x \leq p-1 \Rightarrow 1 \leq p-x \leq \frac{p-1}{2}$$

and

$$x^2 \equiv (p-x)^2 \pmod{p}.$$

Thus,

$$\left(\frac{p+1}{2}\right)^2, \dots, (p-1)^2 \pmod{p}$$

are congruent to

$$\left(\frac{p-1}{2}\right)^2, \dots, 1^2, \pmod{p}.$$

Thus, quadratic residues $(\text{mod } p)$ lie in the list

$$1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2.$$

No two elements in this list are congruent to each other $(\text{mod } p)$. If

$$x^2 \equiv y^2 \pmod{p} \text{ for some } 1 \leq x \leq y \leq \frac{p-1}{2},$$

then

$$p \mid (x+y)(x-y).$$

Since

$$2 \leq x+y \leq p-1,$$

we get $x \equiv y \pmod{p}$. But, $y-x \leq p-1$. Thus,

$$x \equiv y \pmod{p} \Rightarrow x = y.$$

This proves that there are exactly $(p-1)/2$ quadratic residues and therefore exactly $(p-1) - (p-1)/2 = (p-1)/2$ quadratic nonresidues $(\text{mod } p)$. $\square$

In the last chapter, we learnt in Theorem 3.6.10 that a is a quadratic residue $(\text{mod } p)$ if and only if and only if

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

4.2 Legendre symbol

For an odd prime p and $(a, p) = 1$, we define Legendre's symbol $\left(\frac{a}{p}\right)$ as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a QR (mod } p) \\ -1 & \text{if } a \text{ is a QNR (mod } p). \end{cases}$$

If $p|a$, we say that $\left(\frac{a}{p}\right) = 0$. We may rewrite Euler's criterion (Theorem 3.6.10) as follows:

Theorem 4.2.1 *If p is an odd prime and $(a, p) = 1$, then*

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

In particular, Theorem 3.5.4 is equivalent to saying that

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

Observe that

$$(ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \pmod{p}.$$

Thus, by Theorem 4.2.1, we deduce

$$\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right) \left(\frac{b}{p}\right) \pmod{p}.$$

Since the left and right hand sides of the above congruence are ± 1 and p is an odd prime, this congruence implies that

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right).$$

We summarise some important properties of Legendre's symbol in the following theorem:

Theorem 4.2.2 *Let p be an odd prime and a and b be two integers that are co-prime to p . Then*

$$\text{(a)} \quad \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

$$(b) \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right).$$

$$(c) \text{ If } a \equiv b \pmod{p}, \text{ then } \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$

$$(d) \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

$$(e) \left(\frac{a^2}{p}\right) = 1.$$

Exercise 4.2.3 Evaluate the Legendre symbols

$$\left(\frac{38}{13}\right), \left(\frac{-38}{13}\right), \left(\frac{41}{11}\right).$$

Exercise 4.2.4 If p is an odd prime, then prove that

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0.$$

4.3 Gauss' lemma

Though the beauty of Euler's criterion cannot be disputed, as a technique to find out whether an integer a is a quadratic residue of p , it is computationally not feasible for large values of p . For example, is 2 a quadratic residue of 31957? [Note that 31957 is a prime.]

We now learn another technique which helps us to evaluate $\left(\frac{a}{p}\right)$.

The nonzero residues $\pmod{p}$ can be listed as

$$\left\{1, 2, 3, \dots, \frac{p-1}{2}, p - \frac{p-1}{2}, \dots, p-1\right\}.$$

Observe that

$$\frac{p+1}{2} \leq j \leq p-1 \Rightarrow 1 \leq p-j \leq \frac{p-1}{2}.$$

Moreover, $p-j \equiv j \pmod{p}$. Thus, the elements in the set

$$\left\{1, 2, 3, \dots, \frac{p-1}{2}, p - \frac{p-1}{2}, \dots, p-1\right\}$$

are congruent, modulo p to

$$\left\{ \pm j : 1 \leq j \leq \frac{p-1}{2} \right\}.$$

The residue classes in this form are called **balanced residue classes**. In other words, if any number a is congruent to an integer $j > \frac{p-1}{2}$ modulo p , then it has a negative balanced residue class.

Theorem 4.3.1 [Gauss' lemma] *Let p be an odd prime and $(a, p) = 1$. Consider the set*

$$S = a, 2a, 3a, \dots, \frac{p-1}{2}a$$

and let

$$ja \equiv a_j \pmod{p} \text{ for each } 1 \leq j \leq \frac{p-1}{2},$$

where a_j 's are balanced residue classes. Let l be the number of a_j 's which are negative. In other words, let l denote the number of integers in the set S whose residues $\pmod{p}$ are $> \frac{p-1}{2}$. Then,

$$\left(\frac{a}{p} \right) = (-1)^l.$$

Proof. We have

$$a.2a.\dots\left(\frac{p-1}{2}\right)a \equiv a_1a_2\dots a_{\frac{p-1}{2}} \pmod{p}.$$

Note that

$$\left\{ |a_j| : 1 \leq j \leq \frac{p-1}{2} \right\} = \left\{ 1, 2, \dots, \frac{p-1}{2} \right\}.$$

This is because, for $1 \leq j, k \leq \frac{p-1}{2}$,

$$\begin{aligned} a_j \equiv \pm a_k \pmod{p} &\Leftrightarrow ja \equiv \pm ka \pmod{p} \\ &\Leftrightarrow a(j \pm k) \equiv 0 \pmod{p} \\ &\Leftrightarrow j \pm k \equiv 0 \pmod{p}, \end{aligned}$$

which is possible if and only if $j = k$. We get

$$a.2a.\dots\left(\frac{p-1}{2}\right)a \equiv (-1)^l 1.2.\dots\frac{p-1}{2} \pmod{p}.$$

$$\begin{aligned} &\Rightarrow a^{\frac{p-1}{2}} \equiv (-1)^l \pmod{p} \\ &\Rightarrow \left(\frac{a}{p}\right) \equiv (-1)^l \pmod{p} \text{ (by Theorem 4.2.1).} \end{aligned}$$

Thus,

$$\left(\frac{a}{p}\right) = (-1)^l.$$

□

Exercise 4.3.2 (a) Consider the set

$$S = \left\{ 2, 4, 6, \dots, 2 \left(\frac{p-1}{2} \right) \right\}.$$

Prove that the number of integers in S , which upon division by p have remainders greater than $(p-1)/2$ is

$$\frac{p-1}{2} - \left\lfloor \frac{p-1}{4} \right\rfloor.$$

(b) Deduce that

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8} \\ -1 & \text{if } p \equiv \pm 3 \pmod{8}. \end{cases}$$

Exercise 4.3.3 If $p > 3$ is an odd prime, prove that

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{12} \\ -1 & \text{if } p \equiv \pm 5 \pmod{12}. \end{cases}$$

Exercise 4.3.4 (a) If $p > 3$ is an odd prime, prove that

$$\left(\frac{-3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{6} \\ -1 & \text{if } p \equiv 5 \pmod{6}. \end{cases}$$

(b) Prove that there are infinitely many primes of the form $6k+1$. [Hint: Suppose there were only finitely many primes $p_1, p_2, \dots, p_r$ of the form $6k+1$ and consider the integer $N = (2p_1p_2 \cdots p_r)^2 + 3$.]

4.4 The Quadratic Reciprocity Law

The two fundamental problems in the theory of quadratic residues are the following

1. Given a prime p , determine which integers a are quadratic residues of p and which are ones are quadratic nonresidues (mod p).
2. Given an integer a , determine those primes p for which a is a quadratic residue of p and those primes for which a is a quadratic nonresidue of p .

So far, we have have seen that Euler's criterion and Gauss' lemma address the first problem, although these methods can be long. The second problem is more difficult and the next two sections will be devoted to it. To address this problem, we would like to find out the relation between $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ where p and q are odd primes. This relation is explicitly stated in a very important and interesting theorem known as the quadratic reciprocity law. This law was first conjectured by Euler in the 1740s. Legendre rediscovered it around 1785, stated it in a very elegant form (the form in which we will use it) and partially proved it. The first complete proof was given by Gauss in his book *Disquisitiones Mathematicae* in 1801. Gauss went on to give seven proofs of this law and as of now, there are approximately 150 different proofs known. We now state the theorem in the symmetric form in which it was stated by Legendre and give a classical proof by Ferdinand Eisenstein, a student of Gauss. Eisenstein's proof is a variant of a proof by Gauss.

Theorem 4.4.1 [Quadratic Reciprocity Law] *If p and q are distinct odd primes, then*

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}} (-1)^{\frac{q-1}{2}}.$$

The above theorem tells us that if p and q are distinct odd primes, then

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$

unless $p \equiv q \equiv 3 \pmod{4}$, in which case

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right).$$

In order to prove the quadratic reciprocity law, we start with proving the following lemma:

Lemma 4.4.2 *Let p be an odd prime and a be an odd integer such that $(a, p) = 1$. Then*

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{j=1}^{\frac{p-1}{2}} [ja/p]}.$$

Proof. Consider the set of integers

$$S = \left\{ a, 2a, \dots, \frac{p-1}{2}a \right\}.$$

For each $1 \leq j \leq \frac{p-1}{2}$, let

$$ja = q_j p + r_j, \quad 1 \leq r_j \leq p-1.$$

Observe that

$$\frac{ja}{p} = q_j + \frac{r_j}{p} \text{ where } \frac{r_j}{p} < 1.$$

So,

$$q_j = \left[\frac{ja}{p} \right].$$

If $r_j \leq \frac{p-1}{2}$, let it be denoted by one of $g_1, g_2, \dots, g_t$ and if $r_j > \frac{p-1}{2}$, let it be denoted by one of $b_1, b_2, \dots, b_l$. Thus,

$$\sum_{j=1}^{\frac{p-1}{2}} ja = p \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p} \right] + \sum_{i=1}^t g_i + \sum_{k=1}^l b_k. \quad (4.1)$$

For $1 \leq k \leq l$, let $c_k = b_k - p$. Then, as in the proof of Gauss' lemma (Theorem 4.3.1),

$$\left\{ g_i : 1 \leq i \leq \frac{p-1}{2} \right\} \sqcup \left\{ -c_k : 1 \leq k \leq \frac{p-1}{2} \right\} = \left\{ j : 1 \leq j \leq \frac{p-1}{2} \right\}.$$

Thus,

$$\sum_{j=1}^{\frac{p-1}{2}} j = pl + \sum_{i=1}^t g_i - \sum_{k=1}^l b_k. \quad (4.2)$$

Subtracting equation (4.2) from equation (4.1), we get

$$(a-1) \sum_{j=1}^{\frac{p-1}{2}} j = p \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p} \right] + 2 \sum_{k=1}^l b_k - pl. \quad (4.3)$$

Recalling that a is odd and reducing equation (4.3) (mod 2), we get

$$l \equiv \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p} \right] \pmod{2}.$$

Thus, by Gauss' lemma (Theorem 4.3.1),

$$\left(\frac{a}{p} \right) = (-1)^l = (-1)^{\sum_{j=1}^{\frac{p-1}{2}} [ja/p]}.$$

□

Lemma 4.4.3 *Let p and q be odd primes. Then*

$$\sum_{i=1}^{\frac{p-1}{2}} \left[\frac{iq}{p} \right] + \sum_{j=1}^{\frac{q-1}{2}} \left[\frac{jp}{q} \right] = \frac{p-1}{2} \frac{q-1}{2}.$$

Proof. Consider the following set of 2-tuples:

$$S = \left\{ (i, j) : 1 \leq i \leq \frac{p-1}{2}, 1 \leq j \leq \frac{p-1}{2} \right\}.$$

Clearly the number of elements in S is equal to

$$\frac{p-1}{2} \frac{q-1}{2}.$$

We now count the elements of S in another way: we write S as a disjoint union of two sets S_1 and S_2 as follows:

$$S = S_1 \sqcup S_2,$$

where

$$S_1 = \{(i, j) : qi < pj\}$$

and

$$S_2 = \{(i, j) : qi > pj\}.$$

[Note that with any choice of i and j given above, $qi \neq pj$. Thus, any element in S lies in exactly one of S_1 or S_2 .] The number of elements in S_1 is

$$\sum_{j=1}^{\frac{q-1}{2}} \sum_{i < \frac{pj}{q}} 1 = \sum_{j=1}^{\frac{q-1}{2}} \left[\frac{pj}{q} \right].$$

Similarly, the number of elements in S_2 is

$$\sum_{i=1}^{\frac{p-1}{2}} \left[\frac{iq}{p} \right].$$

This proves the lemma. $\square$

We are now ready to prove Theorem 4.4.1

Proof. By Theorem 4.3.1 and Lemma 4.4.2, we get that for any odd primes p and q ,

$$\left(\frac{p}{q} \right) \left(\frac{q}{p} \right) = (-1)^{\sum_{i=1}^{\frac{p-1}{2}} \left[\frac{iq}{p} \right] + \sum_{j=1}^{\frac{q-1}{2}} \left[\frac{jp}{q} \right]}.$$

Applying Lemma 4.4.3, we get

$$\left(\frac{p}{q} \right) \left(\frac{q}{p} \right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}.$$

$\square$

Exercise 4.4.4 Evaluate the Legendre symbols

$$\left(\frac{19}{47} \right), \left(\frac{22}{47} \right), \left(\frac{-72}{131} \right), \left(\frac{219}{383} \right).$$

Exercise 4.4.5 Using the quadratic reciprocity law, if $p > 3$ is an odd prime, prove that

$$\left(\frac{3}{p} \right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{12} \\ -1 & \text{if } p \equiv \pm 5 \pmod{12}. \end{cases}$$

4.5 Jacobi symbol

We now consider an extension of the Legendre symbol introduced by Jacobi for composite numbers: Let B a positive odd integer with factorization

$$B = q_1 q_2 \cdots q_s$$

where q_i 's are (not necessarily distinct) primes. For any integer A , the Jacobi symbol is defined as

$$\left(\frac{A}{B}\right) = \prod_{j=1}^s \left(\frac{A}{q_j}\right).$$

We also define $(A|1) = 1$ and $(A|B) = 0$ if and only if $(A, B) > 1$. If the congruence $x^2 \equiv A \pmod{B}$ has a solution, then $x^2 \equiv A \pmod{q_j}$ has a solution for every $1 \leq j \leq s$. Thus, $(A|q_j) = 1$ for every q_j and therefore

$$\left(\frac{A}{B}\right) = \prod_{j=1}^s \left(\frac{A}{q_j}\right) = 1.$$

However, the converse is not true. For example, observe that

$$\left(\frac{12}{31^2}\right) = \left(\frac{12}{31}\right) \left(\frac{12}{31}\right) = (\pm 1)^2 = 1.$$

But, if

$$x^2 \equiv 12 \pmod{31^2}$$

has a solution, so will the equation

$$x^2 \equiv 12 \pmod{31}.$$

This is a contradiction, since

$$\left(\frac{12}{31}\right) = \left(\frac{4}{31}\right) \left(\frac{3}{31}\right) = \left(\frac{3}{31}\right) = -1,$$

since

$$31 \equiv -5 \pmod{12} \text{ see Exercise 4.4.5.}$$

So, if

$$\left(\frac{A}{B}\right) = -1,$$

then we deduce that

$$x^2 \equiv A \pmod{B}$$

has no solution. However, if

$$\left(\frac{A}{B}\right) = 1,$$

then we cannot say whether $x^2 \equiv A \pmod{B}$ has a solution or not. The following properties of the Jacobi symbol can be deduced easily:

Theorem 4.5.1 *Let A and B be odd positive integers. Then*

- (a) $(a_1|B)(a_2|B) = (a_1a_2|B)$,
- (b) $(a|A)(a|B) = (a|AB)$,
- (c) $(a|A) = (b|A)$ whenever $a \equiv b \pmod{A}$,
- (d) $(a^2b|B) = (b|B)$ whenever $(a, B) = 1$.

Proof. The proof of this theorem is left to the students. $\square$

Exercise 4.5.2 *For an odd positive integer B , prove that*

$$\left(\frac{-1}{B}\right) = (-1)^{\frac{B-1}{2}}$$

and

$$\left(\frac{2}{B}\right) = \begin{cases} 1 & \text{if } B \equiv \pm 1 \pmod{8} \\ -1 & \text{if } B \equiv \pm 3 \pmod{8}. \end{cases}$$

For any two odd positive integers A and B , let

$$A = p_1 p_2 p_3 \cdots p_r,$$

where p_i 's are not necessarily distinct primes and

$$B = q_1 q_2 \cdots q_s,$$

where q_j 's are not necessarily distinct primes. Then, Theorem 4.5.1 tells us that

$$\left(\frac{A}{B}\right) = \prod_{i=1}^r \prod_{j=1}^s \left(\frac{p_i}{q_j}\right).$$

The following analogue of the Quadratic Reciprocity law holds for the Jacobi symbol:

Theorem 4.5.3 *If A and B are positive odd integers with $(A, B) = 1$, then*

$$\left(\frac{A}{B}\right) \left(\frac{B}{A}\right) = (-1)^{\frac{A-1}{2} \frac{B-1}{2}}.$$

Proof. We begin with the following observation: Let $a_1, a_2, \dots, a_t$ be a collection of odd numbers. Then

$$\frac{a_1 a_2 \cdots a_t - 1}{2} \equiv \frac{a_1 - 1}{2} + \frac{a_2 - 1}{2} + \cdots + \frac{a_t - 1}{2} \pmod{2}.$$

Applying the quadratic reciprocity law for Legendre symbol and properties of Jacobi symbol from Theorem 4.5.1, we get

$$\begin{aligned} \left(\frac{A}{B}\right) &= \prod_{i=1}^r \prod_{j=1}^s \left(\frac{p_i}{q_j}\right) \\ &= \prod_{i=1}^r \prod_{j=1}^s (-1)^{\frac{p_i-1}{2} \frac{q_j-1}{2}} \left(\frac{q_j}{p_i}\right) \\ &= \prod_{i=1}^r \left[\prod_{j=1}^s (-1)^{\frac{q_j-1}{2}} \right]^{\frac{p_i-1}{2}} \left(\frac{b}{p_i}\right) \\ &= \prod_{i=1}^r \left[(-1)^{\frac{q_1-1}{2} + \cdots + \frac{q_s-1}{2}} \right]^{\frac{p_i-1}{2}} \left(\frac{b}{p_i}\right) \\ &= \prod_{i=1}^r \left[(-1)^{\frac{q_1 q_2 \cdots q_s - 1}{2}} \right]^{\frac{p_i-1}{2}} \left(\frac{b}{p_i}\right) \\ &= \prod_{i=1}^r (-1)^{\frac{b-1}{2} \frac{p_i-1}{2}} \left(\frac{b}{p_i}\right) \\ &= (-1)^{\left(\frac{p_1-1}{2} + \cdots + \frac{p_r-1}{2}\right) \left(\frac{b-1}{2}\right)} \left(\frac{b}{a}\right) \\ &= (-1)^{\frac{p_1 p_2 \cdots p_r - 1}{2} \cdot \frac{b-1}{2}} \left(\frac{b}{a}\right) \\ &= (-1)^{\frac{a-1}{2} \frac{b-1}{2}} \left(\frac{b}{a}\right). \end{aligned}$$

□

Exercise 4.5.4 *Compute the Jacobi symbols*

$$\left(\frac{286}{105}\right) \text{ and } \left(\frac{123}{917}\right).$$

Chapter 5

Sums of squares

5.1 Pythagorean triples

A very interesting problem in number theory, which has received a lot of attention over the centuries is that of representing numbers as sums of squares. Before we begin our foray into this topic, it is worthwhile to recall our favourite theorem from high school, the Pythagorean Theorem, which states that the sum of squares of the sides of a right triangle equals the square of the hypotenuse. A triple (a, b, c) of natural numbers, which satisfies the equation $a^2 + b^2 = c^2$ is called a Pythagorean triple. For example, $(3, 4, 5)$, $(5, 12, 13)$, and $(8, 15, 17)$ are Pythagorean triples. It is easy to observe that there are infinitely many Pythagorean triples. This is because if we multiply each element of a Pythagorean triple (a, b, c) by some integer d , we get another Pythagorean triple. So, we ask the following modified question: How many Pythagorean triples (a, b, c) are there such that a , b and c have no common factors greater than 1? These special triples are called primitive Pythagorean triples. That is, a **primitive Pythagorean triple** is a triple of numbers (a, b, c) so that $a^2 + b^2 = c^2$ and a , b and c have no common factors greater than 1.

Exercise 5.1.1 *Let (a, b, c) be a primitive Pythagorean triple.*

- (a) *Show that either a or b is odd.*
- (b) *Show that if a is odd, then b is even. [Hint: Compare the equation $a^2 + b^2 = c^2$ modulo 4]*

(c) Conclude from above that c is odd.

Exercise 5.1.2 We now attempt to find all solutions in natural numbers to the equation $a^2 + b^2 = c^2$ under the conditions that a is odd, b is even and a, b and c have no common factors.

(a) Observe that $a^2 = c^2 - b^2 = (c-b)(c+b)$. Prove that $\gcd(c-b, c+b) = 1$.

(b) From above, we see that $\gcd(c-b, c+b) = 1$. Moreover, $a^2 = (c-b)(c+b)$. Prove that $c+b = s^2$ and $c-b = t^2$ where $s > t \geq 1$ are odd integers and $(s, t) = 1$.

(c) Conclude, from the above, that every primitive Pythagorean triple with a odd and b even is of the form

$$a = st, b = \frac{s^2 - t^2}{2}, c = \frac{s^2 + t^2}{2}$$

where s and t are as above. [**Warning:** Make sure you explain why $\frac{s^2-t^2}{2}$ and $\frac{s^2+t^2}{2}$ are (positive) integers.]

5.2 The equation $x^4 + y^4 = z^4$

In the previous section, you discovered a rule that generates all primitive Pythagorean triples!! That is, you essentially found all integer solutions of the equation $x^2 + y^2 = z^2$. This equation is an example of a **Diophantine equation**, which is a generic name for any polynomial equation which is allowed to have only integer solutions. This name is inspired by Diophantus, a Greek mathematician who lived in the 3rd century. In his book *Arithmetica*, Diophantus studied methods of solving many Diophantine equations, including the Pythagorean equation. In 1621, Bachet translated *Arithmetica* into Latin. While reading this book and in particular, the section containing the Pythagorean equation, Pierre de Fermat, a French mathematician (1607-1685), made a comment, which lies at the heart of many important mathematical developments for the next three hundred and fifty years. He wrote, “it is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general, any power higher than the second, into two like powers. I have discovered a truly marvelous proof of this, which this margin is too narrow to contain.” More precisely, Fermat made the following

conjecture, which is famously known as Fermat's Last Theorem and which was finally proved by Andrew Wiles towards the end of the twentieth century, using some of the deepest and most beautiful ideas in Mathematics:

Theorem 5.2.1 [Fermat's Last Theorem] *For any natural number $n \geq 3$, the equation*

$$x^n + y^n = z^n$$

has no integer solutions such that $xyz \neq 0$.

The proof of Fermat's Last Theorem is well beyond the purview of this course. However, the following exercise looks at the special case of Fermat's Last Theorem for $n = 4$. This special case was proved by Fermat himself. In his proof, he uses a very important technique called descent. The idea behind this technique is that if there is a nontrivial solution of Fermat's equation, say (x, y, z) with $z > 0$, then one can find yet another solution (x_1, y_1, z_1) such that $0 < z_1 < z$. This process can be replicated again and again to obtain an infinite list of solutions

$$z > z_1 > z_2 > z_3 \cdots$$

However, a decreasing list of positive integers must stop somewhere, where as the above method of descent seems to give us such a list that stops nowhere. Therefore, our fundamental assumption that Fermat's equation has a nontrivial solution is false. In the following exercise, we fill in the details of this beautiful idea of Fermat:

Exercise 5.2.2 (a) *Consider the equation $x^4 + y^4 = z^2$. Suppose it has integer solutions. After canceling common factors, we can assume that the integers x, y, z are primitive solutions. From the above problem, we deduce that there are odd integers s and t so that*

$$x^2 = st, y^2 = \frac{s^2 - t^2}{2}, z = \frac{s^2 + t^2}{2}.$$

Prove that $s \equiv t \pmod{4}$.

(b) *Deduce that $s+t = 2u^2$ and $s-t = 4v^2$ such that u and $2v$ are coprime. Further deduce that*

$$x^2 + 4v^4 = u^4.$$

- (c) Prove that $(x, 2v^2, u^2)$ forms a primitive Pythagorean triple. Thus, by Problem 2, we can find odd relatively prime integers S and T so that

$$x = ST, 2v^2 = \frac{S^2 - T^2}{2} u^2 = \frac{S^2 + T^2}{2}.$$

- (d) Show that

$$S = X^2 + Y^2, T = X^2 - Y^2$$

for some integers X and Y . [Hint: Use the middle formula in (c) and also the fact that the gcd of $S + T$ and $S - T$ is 2.]

- (e) Show that

$$X^4 + Y^4 = u^2.$$

Thus, we have a new solution (X, Y, u) to our original equation $x^4 + y^4 = z^2$. Show that u is smaller than z .

- (f) The above is Fermat's method of descent. Given a solution (x, y, z) in positive integers of the equation $x^4 + y^4 = z^2$, you generated another solution in positive integers (X, Y, u) where u is smaller than z . Repeating this process will lead to a never-ending list of solutions. Deduce from this that the equation $x^4 + y^4 = z^2$ has no solutions.
- (g) Finally, conclude that the equation $x^4 + y^4 = z^4$ has no solutions in integers. This proves Fermat's Last Theorem for $n = 4$.

5.3 Sums of two squares

In this section, we address the following question: which natural numbers n can be written as a sum of two squares? This question was first answered by a Dutch mathematician Albert Girard in 1625, but without explanation. Since Fermat's method of descent plays an important role in answering this question, it is highly probable that Fermat himself had a complete answer. However, the first person to answer this question with a proof was Euler in 1749.

The following set of exercises will help us to answer this question. Our starting point is Theorem 4.2.2 (c), which states that for an odd prime p ,

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

That is, the equation $x^2 \equiv -1 \pmod{p}$ has a solution if and only $p \equiv 1 \pmod{4}$.

Exercise 5.3.1 *If a prime p can be written as a sum of squares of two integers, that is, if $p = x^2 + y^2$ for some $x, y \in \mathbb{Z}$, then show that $p \equiv 1 \pmod{4}$. [Hint: What are the possible values of $a^2 \pmod{4}$?]*

Exercise 5.3.2 *Let m and n be two positive integers which are sums of two squares. Prove that mn is also a sum of two squares. [Hint: Let $z = a + ib$ and $w = c + id$ be two complex numbers. Then $|z|^2|w|^2 = |zw|^2$. Alternatively, observe that*

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac - bd & ad + bc \\ -ad - bc & ac - bd \end{pmatrix}.$$

Now take determinants of matrices on both sides.]

Exercise 5.3.3 *In this Exercise, we prove the converse of Exercise 5.3.1. We do so using Fermat's method of descent. The idea is that given integers A, B, M with $M > 0$ and $A^2 + B^2 = Mp$, we can find new integers a, b, m such that $a^2 + b^2 = mp$ and $0 < m \leq M - 1$. We keep repeating the descent argument until we hit $m = 1$, that is, $p = x^2 + y^2$.*

(a) *Start by recalling, from the previous exercise, that*

$$(u^2 + v^2)(A^2 + B^2) = (uA + vB)^2 + (vA - uB)^2.$$

(b) *Let $p \equiv 1 \pmod{4}$. Show that we can find positive integers A, B, M such that $A^2 + B^2 = Mp$ and $M < p$. [Hint: $x^2 \equiv -1 \pmod{p}$.]*

(c) *Show that we can find u and v such that $u \equiv A \pmod{M}$, $v \equiv B \pmod{M}$ with $-M/2 \leq u, v \leq M/2$. [Recall the notion of balanced residue classes]*

(d) *Prove that $u^2 + v^2 \equiv 0 \pmod{M}$.*

(e) *Deduce from (c) and (d) that $u^2 + v^2 = Mr$, $1 \leq r < M$.*

(f) *We now have $u^2 + v^2 = Mr$, $1 \leq r < M$ and $A^2 + B^2 = Mp$. This gives us*

$$(uA + vB)^2 + (vA - uB)^2 = M^2rp.$$

Show that $uA + vB \equiv 0 \pmod{M}$ and $vA - uB \equiv 0 \pmod{M}$. From this, find integers a and b such that $a^2 + b^2 = rp$, $1 \leq r < M$.

- (g) Prove that that one can keep repeating the descent argument until one gets $x^2 + y^2 = p$.

Combining the above with Exercise 5.3.1, you now know that an odd prime p can be written as a sum of two squares if and only if $p \equiv 1 \pmod{4}$.

- (h) In order to practice the descent method, start with $(387)^2 + 1^2 = 170.881$ and express 881 as a sum of two squares.

Exercise 5.3.4 Combining Exercises 5.3.2 and 5.3.3, we get an idea of what kind of integers (prime and composite) can be written as a sum of two squares. Exercise 5.3.2 tells us that it is sufficient to check if the prime factors of n are representable as the sum of two squares. The primes of the form $4k + 3$ are problematic. However, if such primes occur to an even power, then these prime powers are squares themselves (and every square is clearly a sum of two squares, with one term being 0).

- (a) Show that n is a sum of two squares if and only if each of its prime factors p of the form $4k + 3$ occurs to an even power.
- (b) Check if the integers 459, 3185 and 39690 can be written as the sum of two squares. If yes, find the representation in each case.

Exercise 5.3.5 On a somewhat related note, show that any odd prime can be written as a difference of two consecutive squares.

Exercise 5.3.6 Show that no positive integer of the form $8k + 7$ can be represented as a sum of three squares.

5.4 Sums of four squares: Lagrange's theorem

A classical result, known as the Four Square Theorem, states that any positive integer n can be written as a sum of squares of four integers ≥ 0 . It was first stated by Girard and Fermat. Euler made several attempts to prove this result, but could not succeed. This result was proved in 1770 by Lagrange, who built on the ideas of Euler. In the following exercises, we will build Lagrange's proof of the Four Square Theorem.

Exercise 5.4.1 Given a prime p , show that there are exactly $\frac{p+1}{2}$ squares modulo p .

Exercise 5.4.2 For a fixed prime p , let

$$S = \left\{ x^2 \bmod p : 0 \leq x \leq \frac{p-1}{2} \right\}$$

and let

$$T = \left\{ -1 - y^2 \bmod p : 0 \leq y \leq \frac{p-1}{2} \right\}.$$

Show that S and T are not disjoint. From this, we conclude that we can find integers $0 \leq x, y \leq (p-1)/2$ such that $x^2 + y^2 + 1 \equiv 0 \bmod p$.

Exercise 5.4.3 Let A, B, C, D be four complex numbers and consider matrices of the form

$$\begin{pmatrix} A & -\overline{B} \\ B & \overline{A} \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} C & -\overline{D} \\ D & \overline{C} \end{pmatrix}.$$

Find out the product of these matrices. Now, taking determinants, show that

$$(|A|^2 + |B|^2)(|C|^2 + |D|^2) = |AC - \overline{B}D|^2 + |\overline{A}D + BC|^2.$$

Using this, if m and n are sums of four squares, express mn as a sum of four squares.

Exercise 5.4.4 For a prime p , let

$$S = \{m \geq 1 : mp \text{ is a sum of four squares}\}.$$

(a) Show that S is a non-empty set. [Hint: Use Exercise 5.4.2]

(b) Let m_0 be the least element of S . In the next few steps, we will again use a descent argument to show that $m_0 = 1$, that is, p is a sum of four squares. Let us assume that $m_0 \geq 2$. Show that m_0 is odd. [In fact, if m_0 is even, we can show that $m_0/2$ is also in S , which contradicts the minimality of m_0 .]

(c) We have $m_0 p = x^2 + y^2 + z^2 + w^2$. Choose $0 \leq a, b, c, d < m_0/2$ such that $x \equiv a \bmod m_0$, $y \equiv b \bmod m_0$, $z \equiv c \bmod m_0$ and $w \equiv d \bmod m_0$. Show that

$$a^2 + b^2 + c^2 + d^2 = m_1 m_0, \quad \text{with } m_1 < m_0.$$

- (d) Using Exercise 5.4.3, express $(m_0p)(m_0m_1)$ as a sum of four squares $r^2 + s^2 + t^2 + v^2$ such that r, s, t and v are multiples of m_0 .
- (e) Deduce that $m_1 \in S$. But, since $m_1 < m_0$, this again contradicts the minimality of m_0 . Thus, our assumption in (b) is false and $m_0 = 1$.

This shows that every prime can be expressed as a sum of four squares. By Exercise 5.4.3, we deduce that every positive integer can be written as a sum of four squares.

Chapter 6

Binary Quadratic Forms

6.1 Introduction to binary quadratic forms

In the previous chapter, we were able to understand which numbers n can be represented as sums of two squares $x^2 + y^2$. We can also exploit techniques from the previous chapter to figure out which numbers can be represented as $x^2 + 2y^2$ or $x^2 + 3y^2$.

Exercise 6.1.1 (a) *Prove that*

$$(a^2 + 2b^2)(c^2 + 2d^2) = (ac - 2bd)^2 + 2(ad + bc)^2.$$

(b) *Let p be an odd prime. Show that $x^2 \equiv -2 \pmod{p}$ has a solution if and only if $p \equiv 1$ or $3 \pmod{8}$.*

(c) *Let $p \equiv 1$ or $3 \pmod{8}$. Let*

$$S = \{m \geq 1 : mp = x^2 + 2y^2, x, y \in \mathbb{Z}\}.$$

Show that the least element of S is $m = 1$. Deduce that every prime $\equiv 1$ or $3 \pmod{8}$ can be written as $x^2 + 2y^2$ with $x, y \in \mathbb{Z}$.

(d) *Determine all positive integers that can be expressed in the form $x^2 + 2y^2$ with $x, y \in \mathbb{Z}$.*

It was therefore natural for mathematicians like Euler and Lagrange to ask a similar question for general forms of the above kind, that is for forms defined as follows:

Definition 6.1.2 A **binary quadratic form** is an expression of the second degree in two variables of the form

$$f(x, y) = ax^2 + bxy + cy^2$$

where a, b, c are integers. A binary quadratic form can also be represented by the symbol $[a, b, c]$. The **discriminant** d or d_f of a binary quadratic form $f = [a, b, c]$ is defined to be the number $d = b^2 - 4ac$. A number n is said to be **represented** by f if we can find integers x and y such that $f(x, y) = n$.

Observe that multiplying the form by $4a$ and completing squares, we get

$$\begin{aligned} 4a(ax^2 + bxy + cy^2) &= (2ax)^2 + 4abxy + 4acy^2 \\ &= (2ax + by)^2 + (4ac - b^2)y^2. \end{aligned}$$

Thus, forms of discriminant 0 are simply squares of linear forms of the form $2ax + by$. We also observe that forms with negative discriminant d behave very differently from forms with positive discriminant d . Let us first consider the forms with negative discriminant. Since $4ac - b^2$ is positive, the above expression is always positive (or zero) for any integers x and y . Thus, the integers represented by $f(x, y)$ are either all positive (and zero for $x = y = 0$) or all negative (and zero) depending on whether a is positive or negative. Depending on the sign of a , the form f is said to be either **positive definite** or **negative definite**. When $d = b^2 - 4ac > 0$, then

$$\begin{aligned} 4a(ax^2 + bxy + cy^2) &= (2ax + by)^2 - dy^2 \\ &= (2ax + by + \sqrt{d}y)(2ax + by - \sqrt{d}y) = 4a^2(x - \alpha y)(x - \beta y), \end{aligned}$$

where α and β are given by

$$\frac{-b \pm \sqrt{d}}{2a},$$

assuming that $a \neq 0$. The sign of $(x - \alpha y)(x - \beta y)$ can be either positive or negative depending on where the fraction x/y lies. If $a = 0$, then $f(x, y) = y(bx + cy)$ which can also take both positive and negative values. Thus, a form f with positive discriminant can take both positive and negative values and is therefore said to be **indefinite**.

Observe that a negative definite form can be changed into a positive definite form by simply changing the signs of all the coefficients a, b, c . Henceforth, we will focus our attention on forms with negative discriminant, and without loss of generality, we may assume such forms to be positive definite, that is $a > 0$. Since $b^2 - 4ac < 0$, this necessarily implies that $c > 0$.

6.2 Equivalence

In this section, we explore the notion of equivalence of quadratic forms.

Observe that the forms $ax^2 + cy^2$ and $ay^2 + cx^2$ are equivalent in as much as they represent the same set of integers as x and y run over all integers. This is because one form has been obtained from the other by interchanging variables. Observe also that as the pair $\{x, y\}$ runs over all pairs of integers, so does the pair $\{x + y, y\}$. Thus the form

$$ax^2 + bxy + cy^2$$

represents the same set of integers as the form

$$a(x + y)^2 + bxy + cy^2 = ax^2 + (2a + b)xy + (a + c)y^2.$$

That is, any integer n that is represented by the former is also represented by the latter. In general, consider integers $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ such that $\alpha\delta - \beta\gamma = 1$. Then, for every pair of integers $x, y \in \mathbb{Z}$, we can find $X, Y \in \mathbb{Z}$, such that

$$\alpha X + \beta Y = x,$$

$$\gamma X + \delta Y = y.$$

Thus, as $\{X, Y\}$ run over all pairs of integers, so do $\{\alpha X + \beta Y, \gamma X + \delta Y\}$. So, all integers represented by

$$ax^2 + bxy + cy^2$$

are also represented by

$$a(\alpha X + \beta Y)^2 + b(\alpha X + \beta Y)(\gamma X + \delta Y) + c(\gamma X + \delta Y)^2.$$

We are now ready to define the notion of equivalence.

Definition 6.2.1 *We say that two binary quadratic forms f and g are equivalent if there exist integers $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ such that*

$$\alpha\delta - \beta\gamma = 1$$

and

$$f(\alpha x + \beta y, \gamma x + \delta y) = g(x, y).$$

In this case, we write $f \sim g$. We also say that the transformation

$$x \mapsto \alpha x + \beta y, \quad y \mapsto \gamma x + \delta y$$

is called a unimodular transformation.

Lemma 6.2.2 *For a binary quadratic form f , let*

$$\mathcal{S}_f := \{f(x, y) : x, y \in \mathbb{Z}\}.$$

If $f \sim g$, then $\mathcal{S}_f = \mathcal{S}_g$.

Proof. Let $n \in \mathcal{S}_f$. Then, there exist $x_0, y_0 \in \mathbb{Z}$ such that $f(x_0, y_0) = n$. Since $f \sim g$, there exist integers $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ such that

$$\alpha\delta - \beta\gamma = 1$$

and

$$f(\alpha x + \beta y, \gamma x + \delta y) = g(x, y).$$

The conditions on $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ above ensure that we can find integers $x_1, y_1 \in \mathbb{Z}$ such that

$$\alpha x_1 + \beta y_1 = x_0$$

and

$$\gamma x_1 + \delta y_1 = y_0.$$

Thus,

$$g(x_1, y_1) = f(\alpha x_1 + \beta y_1, \gamma x_1 + \delta y_1) = f(x_0, y_0) = n.$$

Thus, $n \in \mathcal{S}_g$. This implies that $\mathcal{S}_f \subseteq \mathcal{S}_g$. Similarly, we can show that $\mathcal{S}_g \subseteq \mathcal{S}_f$. This proves the lemma. $\square$

Remark 6.2.3 *We note that f and g will take the same set of values even when*

$$\alpha\delta - \beta\gamma = -1.$$

However, following convention, in the notion of equivalence, we only consider the integers $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ for which

$$\alpha\delta - \beta\gamma = 1,$$

to avoid complications in the theory.

Notice that

$$ax^2 + bxy + cy^2 = \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} a & \frac{b}{2} \\ \frac{-b}{2} & c \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}.$$

6.3. REDUCTION OF BINARY QUADRATIC FORMS AND CLASS NUMBER 73

Thus,

$$d_f = -4 \det \begin{bmatrix} a & \frac{b}{2} \\ \frac{-b}{2} & c \end{bmatrix}.$$

Thus

$$\begin{aligned} g(x, y) &= f(\alpha x + \beta y, \gamma x + \delta y) \\ &= \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}^t \begin{bmatrix} a & \frac{b}{2} \\ \frac{-b}{2} & c \end{bmatrix} \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}. \end{aligned}$$

Exercise 6.2.4 Show that if $f \sim g$, then the discriminant d_f is equal to the discriminant d_g .

However, the converse of the above is not true. There can be inequivalent forms with the same discriminant. For example, consider the forms $f(x, y) = x^2 + 6y^2$ and $g(x, y) = 2x^2 + 3y^2$. Both have discriminant -24 . 1 is represented by $f(x, y)$ for $x = 1, y = 0$ but it cannot be represented by $g(x, y)$. Lemma 6.2.2 tells us that f and g are inequivalent.

Exercise 6.2.5 Show that the relation $\sim$ between binary quadratic forms as defined above is

- reflexive, that is, $f \sim f$,
- symmetric, that is, if $f \sim g$, then $g \sim f$, and
- transitive, that is, if $f \sim g$ and $g \sim h$, then $f \sim h$.

Consider the set

$$S_d = \{f(x, y) : d_f = d\}.$$

Exercise 6.2.5 tells us that the equivalence relation $\sim$ partitions S_d into equivalence classes. In the next section, we will show that when $d < 0$, the number of equivalence classes is finite.

6.3 Reduction of binary quadratic forms and class number

In Chapter 3, we saw that any number can be reduced mod m to an integer (called the residue) between 0 and $m - 1$. We later also reduced numbers to

balanced residues (mod m). Residue classes can be thought of as equivalence classes with respect to the equivalence relation

$$a \sim b \text{ if } a \equiv b \pmod{m}.$$

Similarly, any binary quadratic form can also be **reduced** (in other words, is equivalent) to a form that is simple enough in a suitable sense.

Let us observe what the following two unimodular transformations do to a binary quadratic form $[a, b, c]$.

- Consider the transformation

$$H : x \rightarrow -y, y \rightarrow x.$$

By this transformation, $[a, b, c] \sim [c, -b, a]$.

- For any $u \in \mathbb{Z}$, consider the transformation

$$T_u : x \rightarrow x - uy, y \rightarrow y.$$

By this transformation,

$$[a, b, c] \sim [a, -2au + b, au^2 - bu + c].$$

Theorem 6.3.1 *Any positive definite binary quadratic form in S_d , with $d < 0$, can be reduced, by a sequence of unimodular transformations, to a form $[a, b, c]$ such that*

$$|b| \leq a \leq c.$$

Proof. For a positive definite form, we know that $a, c > 0$.

- If $c < a$, then by transformation H , we replace $[a, b, c]$ by $[c, -b, a]$.
- If $|b| > a$, let b' be the balanced residue of $b \pmod{2a}$, that is, let b' be chosen such that $b \equiv b' \pmod{2a}$ and $|b'| \leq \frac{1}{2}2a = a$. Let $u \in \mathbb{Z}$ such that $b' = b - 2au$. By transformation T_u , we get

$$[a, b, c] \sim [a, b', au^2 - bu + c],$$

such that $|b'| \leq a$.

6.3. REDUCTION OF BINARY QUADRATIC FORMS AND CLASS NUMBER 75

Thus, by applying the above operations one after the other, we will reach a form such that neither $c < a$, nor $|b| > a$. This form is clearly reached after a finite number of steps. This form satisfies the inequality

$$|b| \leq a \leq c.$$

□

Remark 6.3.2 *By a similar reasoning, one may show that any definite form, that is any form with discriminant $d < 0$ can be reduced to a form such that $|b| \leq |a| \leq |c|$.*

Corollary 6.3.3 *There are only finitely many equivalence classes of binary quadratic forms of discriminant $d < 0$.*

Proof. By Theorem 6.3.1 and Remark 6.3.2, every equivalence class has a representative of the form $|b| \leq |a| \leq |c|$. For such a form, we have

$$|d| = |4ac - b^2| \geq 4|a||c| - |b|^2 \geq 4|a|^2 - |a|^2 = 3|a|^2.$$

So,

$$|a| \leq \sqrt{\frac{|d|}{3}}.$$

Thus, there are only finitely many choices for a . This implies that there are only finitely many choices for b as $|b| \leq |a|$. Since $d = b^2 - 4ac$, once we determine a and b , there is only one choice for c . □

Theorem 6.3.4 *Any positive definite binary quadratic form in S_d , with $d < 0$, can be reduced, by a sequence of unimodular transformations, to a form $[a, b, c]$ such that either*

$$-a < b \leq a < c$$

or

$$0 \leq b \leq a = c.$$

Proof. From Theorem 6.3.1, we reduce our form to a form such that

$$|b| \leq a \leq c.$$

Two cases arise.

Case I $a = c$. In this case, by the transformation H , we can reduce f to a form such that

$$0 \leq b \leq a = c.$$

Case II $a < c$. Thus, we have

$$-a \leq b \leq a < c.$$

If $-a < b$, we are done. If $-a = b$, then applying transformation T_{-a} , we get

$$[a, -a, c] \sim [a, a, c]$$

and clearly $-a < a$. Thus, we reduce f to a form for which

$$-a < b \leq a < c.$$

□

Remark 6.3.5 By Corollary 6.3.3, we see that there are only finitely many forms of discriminant $d < 0$ which satisfy the conditions of Theorem 6.3.4.

Definition 6.3.6 A positive definite binary quadratic form whose coefficients satisfy the conditions of Theorem 6.3.4 is called a **reduced form**. The number of reduced forms of discriminant $d < 0$ is called the **class number** of d and is denoted as $h(d)$.

Remark 6.3.7 It can be shown that any two reduced forms of a given discriminant $d < 0$ are inequivalent. Thus, every equivalence class of positive definite binary quadratic forms of discriminant $d < 0$ has exactly one reduced representative. Thus, the class number $h(d)$ refers to the number of equivalence classes of positive definite binary quadratic forms in S_d .

Exercise 6.3.8 Calculate $h(-4)$ and $h(-8)$.

Exercise 6.3.9 List out all the reduced forms of discriminant -20 . Calculate $h(-20)$.

6.4 The representation of a number by a form

A number n is said to be properly represented by a form $[a, b, c]$ if $n = ax^2 + bxy + cy^2$ for relative prime integers x and y . Thus, in order to establish which numbers are represented by a given form, it is sufficient to determine which numbers are properly represented by a given form. In this context, we prove the following theorem due to Lagrange:

Theorem 6.4.1 [Lagrange] *A natural number n is properly represented by some binary quadratic form of discriminant d if and only if the congruence*

$$x^2 \equiv d \pmod{4n}$$

has a solution.

Proof. Suppose

$$x^2 \equiv d \pmod{4n}$$

has a solution, $b \in \mathbb{Z}$. We write $b^2 - d = 4nc$. Then, the form $f(x, y) = nx^2 + bxy + cy^2$ has discriminant d and $f(1, 0) = n$.

Conversely, suppose n is properly represented by some binary quadratic form of discriminant d . Let $n = f(p, r)$ for some integers p and r such that $(p, r) = 1$. There exist integers s, q such that $ps - qr = 1$. We now consider

$$g(x, y) = f(px + qy, rx + sy).$$

Clearly, $f \sim g$. One easily verifies that $g = [A, B, C]$ where $A = f(p, r) = n$ and $B^2 - 4AC = d$. Since $A = n$, we deduce that

$$B^2 \equiv d \pmod{4n}$$

has a solution. $\square$

Exercise 6.4.2 *Using Theorem 6.4.1, show that a prime p can be represented by a binary quadratic form of discriminant -4 if and only if $p \equiv 1 \pmod{4}$.*

Exercise 6.4.3 *Show that for an odd prime p , $x^2 \equiv -7 \pmod{4p}$ has a solution if and only if $x^2 \equiv -7 \pmod{p}$ has a solution. Determine all odd primes that can be expressed in the form $x^2 + xy + 2y^2$.*

Exercise 6.4.4 *Using Theorem 6.4.1, show that a number n is properly represented by the form $x^2 + y^2$ if and only if n has no prime factor of the form $4k + 3$ and is also not divisible by 4. Deduce the statement in Exercise 5.3.4 (a).*

Exercise 6.4.5 *Prove that the primes that can be represented by $x^2 + 5y^2$ are 5 and those congruent to 1 or 9 mod 20. Show also that the primes that can be represented by $2x^2 + 2xy + 3y^2$ are those congruent to 3 or 7 mod 20.*

Chapter 7

Continued Fractions and Pell's Equation

7.1 Finite continued fractions

A finite continued fraction is a fraction of the form

$$[a_0, a_1, \dots, a_n] := a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{\ddots + \frac{1}{a_{n-1} + \frac{1}{a_n}}}}}},$$

where $a_0 \geq 0$ and $a_1, a_2, \dots, a_n > 0$. If a_i 's are all positive integers (with the exception of a_0 , which may be 0), then $[a_0, a_1, \dots, a_n]$ is said to be a simple finite continued fraction. For example

$$\begin{aligned} [2, 4, 3, 4, 3] &= 2 + \frac{1}{4 + \frac{1}{3 + \frac{1}{4 + \frac{1}{3}}}} \\ &= 2 + \frac{1}{4 + \frac{1}{3 + \frac{1}{\frac{13}{3}}}} \\ &= 2 + \frac{1}{4 + \frac{1}{3 + \frac{3}{13}}} = 2 + \frac{1}{4 + \frac{42}{13}} \\ &= 2 + \frac{1}{4 + \frac{13}{42}} = 2 + \frac{1}{\frac{181}{42}} \end{aligned}$$

$$= 2 + \frac{42}{181} = \frac{404}{181}.$$

Clearly, the value of any simple finite continued fraction is always a rational number. The converse is also true.

Theorem 7.1.1 *Any positive rational number can be written as a simple finite continued fraction.*

Proof. Let us consider a rational number $\frac{a}{b}$, where a and b are co-prime non-negative integers with $b > 0$. By Euclid's algorithm,

$$\begin{aligned} a &= ba_0 + r_1, \quad 0 < r_1 < b, \\ b &= r_1a_1 + r_2, \quad 0 < r_2 < r_1, \\ r_1 &= r_2a_2 + r_3, \quad 0 < r_3 < r_2, \\ &\vdots \\ r_{n-2} &= r_{n-1}a_{n-1} + r_n, \quad 0 < r_n < r_{n-1}, \\ r_{n-1} &= r_na_n + 0. \end{aligned}$$

Since all the remainders r_i are positive, $a_1, a_2, \dots$ are also all positive integers. Rewriting the above equations, we get

$$\begin{aligned} \frac{a}{b} &= a_0 + \frac{r_1}{b} = a_0 + \frac{1}{\frac{b}{r_1}}, \\ \frac{b}{r_1} &= a_1 + \frac{r_2}{r_1} = a_1 + \frac{1}{\frac{r_1}{r_2}}, \\ &\vdots \\ \frac{r_{n-2}}{r_{n-1}} &= a_{n-1} + \frac{r_n}{r_{n-1}} = a_{n-1} + \frac{1}{\frac{r_{n-1}}{r_n}}, \\ \frac{r_{n-1}}{r_n} &= a_n \end{aligned}$$

Successively working from the first equation downwards, we get

$$\frac{a}{b} = [a_0, a_1, \dots, a_n].$$

□

Remark 7.1.2 *The above representation is not unique. If $a_n > 1$, we can write the last term as*

$$a_n = a_n - 1 + \frac{1}{1}$$

so that

$$[a_0, a_1, \dots, a_n] = [a_0, a_1, \dots, a_{n-1}, a_n - 1, 1].$$

If $a_n = 1$, we have

$$[a_0, a_1, \dots, a_n] = [a_0, a_1, \dots, a_{n-2}, a_{n-1} + 1].$$

Exercise 7.1.3 *Express the following rational numbers as finite simple continued fractions*

$$\frac{19}{51}, \frac{187}{57}, \frac{71}{55}, \frac{118}{303}.$$

Definition 7.1.4 *Given a continued fraction $[a_0, a_1, \dots, a_n]$, for each $0 \leq k \leq n$,*

$$C_k := [a_0, a_1, \dots, a_k]$$

is called the k -th convergent of $[a_0, a_1, \dots, a_n]$.

Theorem 7.1.5 *Consider a continued fraction $[a_0, a_1, \dots, a_n]$, where we treat $a_0, a_1, \dots, a_n$ as variables instead of specific numbers. For any $0 \leq k \leq n$, the k -th convergent of the continued fraction $[a_0, a_1, \dots, a_n]$ has the value*

$$C_k = \frac{p_k}{q_k}$$

where p_k and q_k are given by the formula

$$p_0 = a_0, q_0 = 1,$$

$$p_1 = a_0 a_1 + 1, q_1 = a_1,$$

$$p_k = a_k p_{k-1} + p_{k-2}, q_k = a_k q_{k-1} + q_{k-2}, k \geq 2.$$

Proof. The proof of this theorem is an exercise in induction. To start induction, we quickly check that

$$[a_0] = \frac{p_0}{q_0}, [a_0, a_1] = \frac{a_0 a_1 + 1}{a_1} = \frac{p_1}{q_1}.$$

Let us now assume that the theorem is true for $n = N$. We observe that

$$[a_0, a_1, \dots, a_N, a_{N+1}] = [a_0, a_1, \dots, a_{N-1}, a_N + \frac{1}{a_{N+1}}].$$

By induction hypothesis,

$$\begin{aligned} \frac{p_{N+1}}{q_{N+1}} &= [a_0, a_1, \dots, a_{N-1}, a_N + \frac{1}{a_{N+1}}] \\ &= \frac{\left(a_N + \frac{1}{a_{N+1}}\right) p_{N-1} + p_{N-2}}{\left(a_N + \frac{1}{a_{N+1}}\right) q_{N-1} + q_{N-2}} \\ &= \frac{a_{N+1}(a_N p_{N-1} + p_{N-2}) + p_{N-1}}{a_{N+1}(a_N q_{N-1} + q_{N-2}) + q_{N-1}} \\ &= \frac{a_{N+1} p_N + p_{N-1}}{a_{N+1} q_N + q_{N-1}} = \end{aligned}$$

Thus,

$$p_{N+1} = a_{N+1} p_N + p_{N-1}, \quad q_{N+1} = a_{N+1} q_N + q_{N-1}.$$

By induction, we prove the theorem. $\square$

Exercise 7.1.6 For a simple finite continued fraction $[a_0, a_1, \dots, a_n]$, show that

$$q_0 \leq q_1 < q_2 < q_3 < \dots < q_n.$$

Theorem 7.1.7 Given a finite simple continued fraction $[a_0, a_1, \dots, a_n]$, the convergents

$$C_k = \frac{p_k}{q_k}$$

satisfy the following properties:

(a) $p_k q_{k-1} - q_k p_{k-1} = (-1)^{k-1}$, $1 \leq k \leq n$.

(b) The even convergents form a strictly increasing sequence, that is,

$$C_0 < C_2 < C_4 < \dots$$

(c) *The odd convergents form a strictly decreasing sequence, that is,*

$$C_1 > C_3 > C_5 > \cdots$$

(d) *Every convergent with an odd subscript is greater than every convergent with an even subscript, that is,*

$$C_{2s-1} > C_{2r} \text{ for any } r \geq 0, s \geq 1.$$

Proof. For $k = 1$,

$$p_1q_0 - p_0q_1 = (a_0a_1 + 1)1 - a_0a_1 = 1,$$

hence proving the theorem for $k = 1$. Assume that the formula is true for $k = m$, where $1 \leq m < n$. Then,

$$\begin{aligned} p_{m+1}q_m - q_{m+1}p_m &= (a_{m+1}p_m + p_{m-1})q_m - (a_{m+1}q_m + q_{m-1})p_m \\ &= p_{m-1}q_m - q_{m-1}p_m = -(-1)^{m-1} \text{ (by induction hypothesis)} \\ &= (-1)^m. \end{aligned}$$

Thus, by induction, (a) holds for all $1 \leq k \leq n$. By (a), we see that

$$\begin{aligned} C_{k+2} - C_k &= C_{k+2} - C_{k+1} + C_{k+1} - C_k \\ &= \frac{p_{k+2}}{q_{k+2}} - \frac{p_{k+1}}{q_{k+1}} + \frac{p_{k+1}}{q_{k+1}} - \frac{p_k}{q_k} \\ &= \frac{(-1)^{k+1}}{q_{k+2}q_{k+1}} + \frac{(-1)^k}{q_{k+1}q_k} \\ &= \frac{(-1)^k(q_{k+2} - q_k)}{q_kq_{k+1}q_{k+2}}. \end{aligned}$$

By Exercise 7.1.6, we know that $q_i > 0$ for all $i \geq 0$ and $q_{k+2} - q_k > 0$. Thus, $C_{k+2} - C_k$ has the same sign as $(-1)^k$. By taking k even, we prove (b). Taking k odd, we prove (c).

We also observe that

$$C_k - C_{k-1} = \frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}} = \frac{(-1)^{k-1}}{q_kq_{k+1}}.$$

Thus, $C_{2j} < C_{2j-1}$ for any $j \geq 1$. Combining this inequality with (b) and (c), we get

$$C_{2r} < C_{2r+2s} < C_{2r+2s-1} < C_{2s-1}$$

for any $r \geq 0, s \geq 1$. This proves (d). $\square$

Exercise 7.1.8 If $r = [a_0, a_1, \dots, a_n]$ for $r > 1$, then show that

$$\frac{1}{r} = [0, a_0, a_1, \dots, a_n].$$

Exercise 7.1.9 Show that

$$q_k \geq 2^{\frac{k-1}{2}},$$

for $2 \leq k \leq n$. [Hint: First prove that $q_k \geq 2q_{k-2}$.]

7.2 Infinite Continued Fractions

Let $\{a_n\}_{n \geq 0}$ be an infinite sequence of integers such that $a_0 \geq 0$ and $a_i > 0$ for all $i \geq 1$. The infinite continued fraction $[a_0, a_1, a_2, \dots]$ is defined to be

$$\lim_{n \rightarrow \infty} C_n = \lim_{n \rightarrow \infty} [a_0, a_1, \dots, a_n].$$

If an infinite continued fraction contains a block of numbers that repeat indefinitely, then it is called a periodic continued fraction and is denoted as

$$[a_0, a_1, \dots, a_m, \overline{b_1, b_2, \dots, b_n}].$$

Theorem 7.2.1 The value of any infinite continued fraction is an irrational number.

Proof. Let, if possible $x = \lim_{n \rightarrow \infty} C_n$ be a rational number. By adapting Theorem 7.1.7 to infinite continued fractions, we observe that x lies strictly between C_n and C_{n+1} for any n . So,

$$0 < |x - C_n| < |C_{n+1} - C_n| = \left| \frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n} \right| = \frac{1}{q_n q_{n+1}}.$$

Suppose $x = \frac{a}{b}$, where $a, b \in \mathbb{N}$. From above, we have

$$0 < \left| \frac{a}{b} - \frac{p_n}{q_n} \right| < \frac{1}{q_n q_{n+1}}.$$

Multiplying this inequality by bq_n , we get

$$0 < |aq_n - bp_n| < \frac{b}{q_{n+1}} \text{ for any } n.$$

By Exercise 7.1.6, q_n is an increasing sequence of positive integers. Thus, we can choose n such that $b < q_{n+1}$. So, $0 < |aq_n - bp_n| < 1$. But, $|aq_n - bp_n| \in \mathbb{N}$. Thus, we reach a contradiction and therefore, our assumption that x is a rational number is false. $\square$

Observe that

$$\begin{aligned} [a_0, a_1, \dots] &= \lim_{n \rightarrow \infty} [a_0, a_1, \dots, a_n] = \lim_{n \rightarrow \infty} [a_0, a_1, \dots, a_n] \\ &= \lim_{n \rightarrow \infty} \left[a_0 + \frac{1}{[a_1, a_2, \dots, a_n]} \right] \\ &= a_0 + \frac{1}{\lim_{n \rightarrow \infty} [a_1, a_2, \dots, a_n]} \\ &= a_0 + \frac{1}{[a_1, a_2, \dots]}. \end{aligned}$$

From this, we conclude the following:

Theorem 7.2.2 *If $[a_0, a_1, \dots] = [b_0, b_1, \dots]$, then $a_n = b_n$ for all $n \geq 0$.*

Proof. Let

$$x = [a_0, a_1, \dots]$$

Observe, by Theorem 7.1.7, that

$$a_0 < x < a_0 + \frac{1}{a_1} \leq a_0 + 1, \text{ since } a_1 \geq 1.$$

Thus, $[x] = a_0$.

If $[a_0, a_1, \dots] = [b_0, b_1, \dots]$, then

$$a_0 + \frac{1}{[a_1, a_2, \dots]} = b_0 + \frac{1}{[b_1, b_2, \dots]}.$$

Thus, $b_0 = [x] = a_0$. So, we conclude that

$$[a_1, a_2, \dots] = [b_1, b_2, \dots].$$

Repeating the above reasoning, we get $a_n = b_n$ for all $n \geq 0$. $\square$

We now ask if every irrational number has an infinite continued fraction expansion.

Given $x_0 \notin \mathbb{Q}$, define the sequence of integers $\{a_n\}_{n \geq 0}$ as follows:

$$\begin{aligned} a_0 &= [x_0], \\ x_1 &= \frac{1}{x_0 - [x_0]}, \quad a_1 = [x_1], \\ &\vdots \\ x_k &= \frac{1}{x_{k-1} - [x_{k-1}]}, \quad a_k = [x_k]. \end{aligned}$$

Observe that $x_k \notin \mathbb{Q}$ for all $k \geq 0$. Thus,

$$0 < x_k - [x_k] < 1 \Rightarrow x_{k+1} = \frac{1}{x_k - [x_k]} > 1 \Rightarrow a_{k+1} = [x_{k+1}] \geq 1 \text{ for all } k \geq 0.$$

So, $a_1, a_2, \dots$ are all positive integers. Since

$$x_{k+1} = \frac{1}{x_k - a_k},$$

we get

$$x_k = a_k + \frac{1}{x_{k+1}} \text{ for all } k \geq 0.$$

Thus,

$$x_0 = a_0 + \frac{1}{x_1} = a_0 + \frac{1}{a_1 + \frac{1}{x_2}} = \dots = [a_0, x_1, \dots, x_k]$$

for every $k \geq 1$. But, why does this continued fraction expansion converge to x_0 ? We have

$$x_0 = \frac{x_n p_{n-1} + p_{n-2}}{x_n q_{n-1} + q_{n-2}}.$$

So,

$$\begin{aligned} x_0 - C_{n-1} &= \frac{x_n p_{n-1} + p_{n-2}}{x_n q_{n-1} + q_{n-2}} - \frac{p_{n-1}}{q_{n-1}} \\ &= \frac{p_{n-2} q_{n-1} - p_{n-1} q_{n-2}}{(x_n q_{n-1} + q_{n-2}) q_{n-1}} = \frac{(-1)^{n-1}}{(x_n q_{n-1} + q_{n-2}) q_{n-1}}. \end{aligned}$$

Thus,

$$|x_0 - C_{n-1}| = \frac{1}{(x_n q_{n-1} + q_{n-2}) q_{n-1}}$$

$$< \frac{1}{(a_n q_{n-1} + q_{n-2}) q_{n-1}} = \frac{1}{q_n q_{n-1}}.$$

Since q_n 's are increasing,

$$\frac{1}{q_n q_{n-1}} \rightarrow 0 \text{ as } n \rightarrow \infty.$$

Thus,

$$\lim_{n \rightarrow \infty} C_{n-1} = x_0.$$

From the above calculation and Theorem 7.2.2, we get the following theorem:

Theorem 7.2.3 *Every irrational number x_0 has a unique continued fraction expansion given by*

$$a_k = [x_k], x_{k+1} = \frac{1}{x_k - a_k}, k \geq 0.$$

Exercise 7.2.4 *Evaluate*

(a) $[2, 3]$

(b) $[2, \overline{3}]$

(c) $[0, \overline{1, 2, 3}]$

(d) $[2, \overline{1, 2, 1}]$

Exercise 7.2.5 *Determine the infinite continued fraction for*

$$\sqrt{5}, \sqrt{7}, \frac{1 + \sqrt{13}}{2}, \frac{5 + \sqrt{37}}{4}, \frac{11 + \sqrt{30}}{13}.$$

Exercise 7.2.6 *Suppose p, q and d are positive integers with d squarefree such that $p^2 - dq^2 = 1$. Assume, if possible, p/q is not a convergent of $\sqrt{d}$.*

(a) *Show that*

$$0 < \frac{p}{q} - \sqrt{d} < \frac{1}{2q^2}.$$

(b) *Let us choose $n \in \mathbb{N}$ such that $q_n \leq q < q_{n+1}$. Show that one can find unique non-zero integers w and z such that*

$$p_n w + p_{n+1} z = p,$$

$$q_n w + q_{n+1} z = q.$$

- (c) Show that w and z have opposite signs.
- (d) Show that $\sqrt{d}q_n - p_n$ and $\sqrt{d}q_{n+1} - p_{n+1}$ have opposite signs. Thus, conclude that $w(\sqrt{d}q_n - p_n)$ and $z(\sqrt{d}q_{n+1} - p_{n+1})$ have the same sign.
- (e) Show that

$$|q\sqrt{d} - p| \geq |q_n\sqrt{d} - p_n|$$

and conclude that

$$\left| \sqrt{d} - \frac{p_n}{q_n} \right| < \frac{1}{2qq_n}.$$

- (f) Observe that

$$\frac{p}{q} \neq \frac{p_n}{q_n} \Rightarrow |qp_n - pq_n| \geq 1$$

Using (a) and (e), prove that $q_n > q$. From this conclude that p/q has to be a convergent of $\sqrt{d}$.

Solution.

- (a) Since $p^2 - dq^2 = 1$, we have

$$(p - \sqrt{d}q)(p + \sqrt{d}q) = 1.$$

So,

$$\frac{p}{q} - \sqrt{d} = \frac{1}{q(p + \sqrt{d}q)}.$$

Using the above and observing that $p > q$, we get

$$0 < \frac{p}{q} - \sqrt{d} < \frac{\sqrt{d}}{q(q\sqrt{d} + q\sqrt{d})} = \frac{\sqrt{d}}{2q^2\sqrt{d}} = \frac{1}{2q^2}.$$

- (b) The matrix equation

$$\begin{bmatrix} p_n & p_{n+1} \\ q_n & q_{n+1} \end{bmatrix} \begin{bmatrix} w \\ z \end{bmatrix} = \begin{bmatrix} p \\ q \end{bmatrix}$$

has a unique solution,

$$\begin{bmatrix} w \\ z \end{bmatrix} = (-1)^{n+1} \begin{bmatrix} q_{n+1} & -p_{n+1} \\ -q_n & p_n \end{bmatrix} \begin{bmatrix} p \\ q \end{bmatrix}.$$

Thus,

$$w = (-1)^{n+1}(q_{n+1}p - p_{n+1}q, z = (-1)^{n+1}(qp_n - pq_n).$$

Since

$$\frac{p}{q} \neq \frac{p_n}{q_n} \text{ and } \frac{p}{q} \neq \frac{p_{n+1}}{q_{n+1}},$$

we get that $w, z \neq 0$.

(c) If $z < 0$, then $q_n w = q - q_{n+1}z > 0$. Thus, $w > 0$.

If $z > 0$, then since $q < q_{n+1}$, we have $q < zq_{n+1}$.

$$\Rightarrow wq_n = q - q_{n+1}z < 0 \Rightarrow w < 0.$$

So, w and z have opposite signs.

(d) By an adaptation of Theorem 7.1.7, we have

$$C_0 < C_2 < C_4 \cdots \sqrt{d} < \cdots C_5 < C_3 < C_1.$$

So, $\sqrt{d} - \frac{p_n}{q_n}$ and $\sqrt{d} - \frac{p_{n+1}}{q_{n+1}}$ have opposite signs. That is,

$$\sqrt{d}q_n - p_n \text{ and } \sqrt{d}q_{n+1} - p_{n+1}$$

have opposite signs. Thus, $w(\sqrt{d}q_n - p_n)$ and $z(\sqrt{d}q_{n+1} - p_{n+1})$ have the same sign.

(e) Observe that

$$\begin{aligned} |q\sqrt{d} - p| &= |(q_n w + q_{n+1} z)\sqrt{d} - (p_n w + p_{n+1} z)| \\ &= |w(q_n \sqrt{d} - p_n) + z(q_{n+1} \sqrt{d} - p_{n+1})| \\ &= |w(q_n \sqrt{d} - p_n)| + |z(q_{n+1} \sqrt{d} - p_{n+1})| \text{ (since both terms have same sign)} \\ &> |w||q_n \sqrt{d} - p_n| \text{ (as } |z(q_{n+1} \sqrt{d} - p_{n+1})| \neq 0) \\ &\geq |q_n \sqrt{d} - p_n|. \end{aligned}$$

So, we have

$$|q_n \sqrt{d} - p_n| \leq |q\sqrt{d} - p| = q \left| \sqrt{d} - \frac{p}{q} \right| < \frac{1}{2q},$$

where the last inequality above is true by (a). Dividing by q_n , we get

$$\left| \sqrt{d} - \frac{p_n}{q_n} \right| < \frac{1}{2qq_n}.$$

(f) Since $\frac{p}{q} \neq \frac{p_n}{q_n}$, $qp_n - pq_n \neq 0$. So,

$$1 \leq |p_n - pq_n|.$$

Thus,

$$\begin{aligned} \frac{1}{qq_n} &\leq \left| \frac{qp_n - pq_n}{qq_n} \right| \\ &= \left| \frac{p_n}{q_n} - \frac{p}{q} \right| \\ &\leq \left| \frac{p_n}{q_n} - \sqrt{d} \right| + \left| \sqrt{d} - \frac{p}{q} \right| \\ &< \frac{1}{2qq_n} + \frac{1}{2q^2} \text{ by (a) and (e).} \end{aligned}$$

Thus, we deduce, from above,

$$\frac{1}{2qq_n} < \frac{1}{2q^2},$$

that is, $qq_n > q^2$, and therefore, $q_n > q$. This contradicts our choice of n such that $q_n \leq q < q_{n+1}$. Therefore, our assumption that p/q is not a convergent of $\sqrt{d}$ is false.

□

We also prove some other recursion formulae involving the numerator and denominator of the convergents of a continued fraction. Let us also denote the numerator of $[a_0, a_1, \dots, a_n]$ as $\{a_0, a_1, \dots, a_n\}$. Note that we are treating a_i 's as symbols and not fixed numbers. These symbols can be changed as per our convenience. Observe that

$$\begin{aligned} a_0 + \frac{1}{a_1} &= \frac{a_0a_1 + 1}{a_1}, \\ a_0 + \frac{1}{a_1 + \frac{1}{a_2}} &= \frac{a_0a_1a_2 + a_0 + a_2}{a_1a_2 + 1} = \frac{\{a_0, a_1, a_2\}}{\{a_1, a_2\}}, \\ a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3}}} & \end{aligned}$$

$$= \frac{a_0 a_1 a_2 a_3 + a_0 a_1 + a_0 a_3 + a_2 a_3 + 1}{a_1 a_2 a_3 + a_1 + a_3} = \frac{\{a_0, a_1, a_2, a_3\}}{\{a_1, a_2, a_3\}}.$$

Do we observe a pattern? The denominator of $[a_0, a_1, a_2, a_3]$ seems to come from the numerator of $[a_1, a_2, a_3]$. Also

$$\{a_0, a_1, a_2, a_3\} = a_0 \{a_1, a_2, a_3\} + \{a_2, a_3\}.$$

In general, we prove the following lemmas:

Lemma 7.2.7 *The denominator of $[a_0, a_1, \dots, a_n]$ is $\{a_1, a_2, \dots, a_n\}$.*

Proof.

$$\begin{aligned} & \text{Denominator of } a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}}} \\ &= \text{Denominator of } \left(a_0 + \frac{\text{Denominator of } [a_1, a_2, \dots, a_n]}{\text{Numerator of } [a_1, a_2, \dots, a_n]} \right) \\ &= \text{Numerator of } [a_1, a_2, \dots, a_n] = \{a_1, a_2, \dots, a_n\}. \end{aligned}$$

□

Similarly, the denominator of $[a_1, \dots, a_n]$ is $\{a_2, a_3, \dots, a_n\}$. (This is obtained by simply changing symbols in the above lemma.)

Lemma 7.2.8 *For any $n \geq 2$,*

$$a_0 \{a_1, a_2, \dots, a_n\} + \{a_2, a_3, \dots, a_n\} = \{a_0, a_1, \dots, a_n\}.$$

Proof.

$$\begin{aligned} \{a_0, a_1, \dots, a_n\} &= \text{Numerator of } a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}}} \\ &= \text{Numerator of } \left(a_0 + \frac{\text{Denominator of } [a_1, a_2, \dots, a_n]}{\text{Numerator of } [a_1, a_2, \dots, a_n]} \right) \\ &= a_0 \{a_1, a_2, \dots, a_n\} + \{a_2, \dots, a_n\}. \end{aligned}$$

□

By Theorem 7.1.5, we also have

$$\{a_0, a_1, \dots, a_n\} = a_n\{a_0, \dots, a_{n-1}\} + \{a_0, \dots, a_{n-2}\} \quad (7.1)$$

and

$$\{a_1, \dots, a_n\} = a_n\{a_1, \dots, a_{n-1}\} + \{a_1, \dots, a_{n-2}\}.$$

Using this, we prove,

Lemma 7.2.9 For $n \geq 0$,

$$\{a_0, \dots, a_n\} = \{a_n, \dots, a_0\}.$$

Proof. The lemma is easily proved by induction. The base case is easily checked. Suppose the lemma is true for $k \leq n-1$. Then, by Lemma 7.2.8 for appropriate symbols,

$$\begin{aligned} \{a_n, a_{n-1}, \dots, a_0\} &= a_n\{a_{n-1}, \dots, a_0\} + \{a_{n-2}, \dots, a_0\} \\ &= a_n\{a_0, \dots, a_{n-1}\} + \{a_0, \dots, a_{n-2}\} \text{ (by induction hypothesis)} \\ &= \{a_0, a_1, \dots, a_n\} \text{ (by equation (7.1)).} \end{aligned}$$

□

7.3 Purely periodic continued fractions

We saw in Exercises 7.2.4 and 7.2.5 that the continued fraction is not always periodic from the start, but after some stage. A purely periodic continued fraction is an infinite continued fraction that is periodic from the very beginning, that is, an expansion of the form

$$[\overline{a_0, a_1, \dots, a_n}], \quad a_i \geq 1.$$

In this section, we consider the properties of irrational numbers which are represented by purely periodic continued fractions. For example, consider

$$\alpha = [\overline{4, 1, 3}].$$

We have

$$\alpha = 4 + \frac{1}{1 + \frac{1}{3 + \frac{1}{\alpha}}} = .$$

Simplifying, we get

$$4\alpha^2 - 18\alpha - 5 = 0.$$

Now, consider the purely periodic continued fraction

$$\beta = [\overline{3, 1, 4}]$$

obtained by reversing the pattern in α . It turns out that β satisfies $5\beta^2 - 18\beta - 4 = 0$. If we put $x = \frac{-1}{\beta}$, we get

$$4x^2 - 18x - 5 = 0.$$

That is, $\frac{-1}{\beta}$ satisfies the same equation as that satisfied by α . That is, α and $\frac{-1}{\beta}$ are **algebraic conjugates**, that is, two roots of the same equation. The above example is a special case of the following theorem:

Theorem 7.3.1 *Any purely periodic continued fraction represents a quadratic irrational number $\alpha > 1$ whose conjugate lies between -1 and 0 . This conjugate is $\frac{-1}{\beta}$, where β is defined by the continued fraction with the reversed period as that of α . (By a quadratic irrational number, we mean an irrational number, which satisfies an equation with integer coefficients of degree 2.)*

Proof. Let $\alpha = [\overline{a_0, a_1, \dots, a_n}]$. Then,

$$\alpha = [a_0, a_1, \dots, a_n, \alpha].$$

Let $C_k = \frac{p_k}{q_k}$ denote the k -th convergent of $[a_0, a_1, \dots, a_n, \alpha]$ for $0 \leq k \leq n$. We have, by Theorem 7.1.5,

$$\alpha = \frac{\alpha p_n + p_{n-1}}{\alpha q_n + q_{n-1}}.$$

Thus, α satisfies the equation

$$q_n \alpha^2 + (q_{n-1} - p_n) \alpha - p_{n-1} = 0. \quad (7.2)$$

That is, α is a quadratic irrational number.

We now reverse the period,

$$\beta = [a_n, a_{n-1}, \dots, a_0, \beta].$$

Thus,

$$\beta = \frac{\beta\{a_n, \dots, a_0\} + \{a_n, \dots, a_1\}}{\beta\{a_{n-1}, \dots, a_0\} + \{a_{n-1}, \dots, a_1\}}.$$

By Lemmas 7.2.7 and 7.2.9, and using notation used in definition of α , we get

$$\beta = \frac{\beta p_n + q_n}{\beta p_{n-1} + q_{n-1}}.$$

We put $\beta = \frac{-1}{x}$, and get

$$q_n \alpha^2 + (q_{n-1} - p_n) \alpha - p_{n-1} = 0.$$

Comparing this with equation (7.2), we see that $x = \frac{-1}{\beta}$ and α satisfy the same equation, that is, they are algebraic conjugates. (Note that $\frac{-1}{\beta} \neq \alpha$.) Clearly, $\alpha > 1$ (This is because, for $i \geq 1$, $a_i \geq 1$. But since α is a purely periodic continued fraction of length $n+1$, $a_0 = a_{n+1} \geq 1$.) Similarly $\beta > 1$. Thus, $-1 < \frac{-1}{\beta} < 0$. This proves the theorem. $\square$

Exercise 7.3.2 Show that the algebraic conjugate of any quadratic irrational number of the form $a + b\sqrt{d}$, where a, b are rational numbers with $b \neq 0$ and d is a squarefree positive integer is $a - b\sqrt{d}$.

We now ask if the converse of Theorem 7.3.1 is true. This question is addressed in the following exercise:

Exercise 7.3.3 Let $\alpha > 1$ be a quadratic irrational number with conjugate α' such that $-1 < \alpha' < 0$. Without loss of generality, let us express

$$\alpha = \frac{P + \sqrt{D}}{Q},$$

where P and Q are integers and D is a positive squarefree integer. Then, the conjugate α' is given by

$$\alpha' = \frac{P - \sqrt{D}}{Q}.$$

(a) Show that $\alpha - \alpha' > 0$ and therefore $Q > 0$.

(b) Show that $\alpha + \alpha' > 0$ and therefore $P > 0$.

- (c) Show that $\alpha' < 0$ and therefore, $P < \sqrt{D}$.
- (d) Show that $\alpha > 1$ and therefore $Q < P + \sqrt{D} < 2\sqrt{D}$.
Thus, from (a) - (d), we deduce that

$$\alpha = \frac{P + \sqrt{D}}{Q}, \quad P < \sqrt{D}, \quad Q^2 \sqrt{D}, \quad Q | P^2 - D.$$

- (e) We express α as

$$\alpha = a_0 + \frac{1}{\alpha_1},$$

where $a_0 = [\alpha]$. If α'_1 is the conjugate of α_1 , show that

$$\alpha' = a_0 + \frac{1}{\alpha'_1}.$$

From this, deduce that $\alpha_1 > 1$ and $-1 < \alpha'_1 < 0$.

- (f) Let

$$P_1 = -P + Qa_0 \text{ and } Q_1 = \frac{D - P_1^2}{Q}.$$

Prove that Q_1 is an integer. Also, prove that

$$\alpha_1 = \frac{P_1 + \sqrt{D}}{Q_1}.$$

- (g) Deduce that P_1 and Q_1 are positive integers satisfying $P_1 < \sqrt{D}$ and $Q_1 < 2\sqrt{D}$.
- (h) Continuing the continued fraction expansion of α , for any $n \geq 1$, let $a_n = [\alpha_n]$ and

$$\alpha_n = a_n + \frac{1}{\alpha_{n+1}}.$$

Show that for every $n \geq 1$,

$$\alpha'_n = a_n + \frac{1}{\alpha'_{n+1}}$$

and each α'_n lies between -1 and 0 .

(i) Show that

$$\alpha_n = \frac{P_n + \sqrt{D}}{Q_n},$$

where P_n and Q_n are natural numbers, $P_n < \sqrt{D}$, $Q_n < 2\sqrt{D}$, and $P_n^2 - D$ is a multiple of Q_n .

(j) Observe that there are only finitely many pairs (X, Y) of positive integers such that $X < \sqrt{D}$ and $Y < 2\sqrt{D}$. Thus, there can be only finitely many possibilities for (P_n, Q_n) . So, at some point, we will end up getting some value of the pair (P_n, Q_n) which had occurred before. So, we obtain an α_n which is equal to an earlier one and therefore, the continued fraction of α is periodic from this point.

(k) Let us define

$$\beta_n = \frac{-1}{\alpha'_n}.$$

By virtue of (h), check that $\beta_n > 1$ and

$$\beta_{n+1} = a_n + \frac{1}{\beta_n}.$$

Thus, $a_n = [\beta_{n+1}]$.

(l) Suppose $\alpha_m = \alpha_n$ for some $m < n$. Show that $\beta_m = \beta_n$ and therefore $a_{m-1} = a_{n-1}$. Conclude that $\alpha_{n-1} = \alpha_{m-1}$.

(m) Deduce that, if $\alpha_m = \alpha_n$, then $\alpha_{n-m} = \alpha$. From this, conclude that the continued fraction of α is purely periodic.

Thus, by Theorem 7.3.1 and Exercise 7.3.3, we get the following:

Theorem 7.3.4 *Let α be an irrational number. The following are equivalent:*

- (a) α has a purely periodic continued fraction expansion.
- (b) α is a quadratic irrational number > 1 , with algebraic conjugate α' such that $-1 < \alpha' < 0$. Moreover, $\alpha' = -\frac{1}{\beta}$, where β has the continued fraction expansion with the reversed period as that of α .

7.4 Continued fraction expansion for $\sqrt{N}$

Let N be a natural number which is not a perfect square. Since $-\sqrt{N} < -1$, by Theorem 7.3.4, $\sqrt{N}$ cannot have a purely periodic continued fraction expansion. We consider

$$\alpha = \sqrt{N} + a_0, \quad a_0 = [\sqrt{N}].$$

The conjugate of $\sqrt{N} + a_0$ is $a_0 - \sqrt{N}$ and $-1 < a_0 - \sqrt{N} < 0$. Once again, by Theorem 7.3.4, $\sqrt{N} + a_0$ has a purely continued fraction expansion. Moreover, this continued fraction expansion must start with $[\sqrt{N} + a_0]$, which is $2a_0$. Let us say,

$$\sqrt{N} + a_0 = [2a_0, a_1, \dots, a_n].$$

We now consider the fraction with reversed period

$$\beta = [a_n, a_{n-1}, \dots, a_1, 2a_0].$$

By Theorem 7.3.4,

$$\alpha' = a_0 - \sqrt{N} = -\frac{1}{\beta}.$$

That is,

$$-\frac{1}{\alpha'} = [a_n, a_{n-1}, \dots, a_1, 2a_0]. \quad (7.3)$$

But, we also have

$$-\frac{1}{\alpha'} - \frac{1}{a_0 - \sqrt{N}} = \frac{1}{\sqrt{N} - a_0} = [a_1, a_2, \dots, a_n, 2a_0]. \quad (7.4)$$

Comparing equations (7.3) and (7.4), we get

$$a_1 = a_n, a_2 = a_{n-1}, a_3 = a_{n-2}, \dots, a_i = a_{n-i} \text{ for every } 1 \leq i \leq n.$$

Thus, we conclude the following:

Theorem 7.4.1 *Let N be a natural number, which is not a perfect square. Then the continued fraction expansion of $\sqrt{N}$ is of the form*

$$\sqrt{N} = [a_0, \overline{a_1, a_2, a_3, \dots, a_3, a_2, a_1, 2a_0}].$$

7.5 Pell's equation

Pell's equation refers to an equation of the form

$$x^2 - dy^2 = 1, \quad (7.5)$$

where d is natural number, which is not a perfect square. We are interested in finding out integers x and y which satisfy this equation. This problem has been considered by several mathematicians since antiquity, and we refer the student to Burton's book for a detailed history of this problem. Without loss of generality, we restrict ourselves to non-negative integer solutions x and y and also assume that d is a square-free positive integer. The solution $(1, 0)$ is called the trivial solution of Pell's equation. Henceforth, we refer to such pairs $(x, y) : x \neq 0, y \neq 0$ as solutions and $(x, y), x > 0, y > 0$ as positive solutions of the Pell's equation. We now ask two questions:

- Does this equation have at least one solution (x, y) with x and y both greater than 0?
- Does this equation have finitely many or infinitely many (positive) solutions?

Assuming that the answer to the first question is yes, let (x_1, y_1) and (x_2, y_2) be solutions of equation (7.5). (We are allowed to consider $x_1 = x_2, y_1 = y_2$.) Observe that

$$(x_1 + y_1\sqrt{d})(x_2 + y_2\sqrt{d}) = (x_1x_2 + dy_1y_2) + \sqrt{d}(x_1y_2 + x_2y_1)$$

and

$$(x_1 - y_1\sqrt{d})(x_2 - y_2\sqrt{d}) = (x_1x_2 + dy_1y_2) - \sqrt{d}(x_1y_2 + x_2y_1).$$

Thus,

$$\begin{aligned} 1 &= (x_1^2 - dy_1^2)(x_2^2 - dy_2^2) \\ &= (x_1 + y_1\sqrt{d})(x_1 - y_1\sqrt{d})(x_2 + y_2\sqrt{d})(x_2 - y_2\sqrt{d}) \\ &= ((x_1x_2 + dy_1y_2) + \sqrt{d}(x_1y_2 + x_2y_1))((x_1x_2 + dy_1y_2) - \sqrt{d}(x_1y_2 + x_2y_1)) \\ &= (x_1x_2 + dy_1y_2)^2 - d(x_1y_2 + x_2y_1)^2. \end{aligned}$$

Thus, using two solutions of equation (7.5), one can generate a third solution

$$(x_1x_2 + dy_1y_2, x_1y_2 + x_2y_1). \quad (7.6)$$

If x_1, y_1 and x_2, y_2 are both positive solutions, the new solution is distinct from these solutions. Thus, once we have an initial solution, we can generate infinitely many solutions of equation (7.5).

Definition 7.5.1 A pair of positive integers (x_1, y_1) such that $x_1^2 - dy_1^2 = 1$ and $x_1 < x$, $y_1 < y$ for any solution (x, y) of Pell's equation is called the **fundamental solution** of Pell's equation.

Exercise 7.5.2 Let (x_1, y_1) be the fundamental solution of $x^2 - dy^2 = 1$ and let us denote $\epsilon_1 = x_1 + \sqrt{d}y_1$. Show that the pair of integers (x_n, y_n) defined by the condition

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$$

is also a positive solution of $x^2 - dy^2 = 1$. Show, also, that $x_n + \sqrt{d}y_n \rightarrow \infty$ as $n \rightarrow \infty$.

Theorem 7.5.3 If (x, y) is a positive solution of $x^2 - dy^2 = 1$, then

$$x + \sqrt{d}y = \epsilon_1^n$$

for some $n \geq 1$.

Remark 7.5.4 The above theorem tells us that any positive solution of Pell's equation can be generated from the fundamental solution.

Proof. Let $\eta = x + \sqrt{d}y$. Observe that

$$\epsilon_1 < \epsilon_1^2 < \cdots < \epsilon_1^n < \epsilon_1^{n+1} < \cdots .$$

Let us assume that $\eta \neq \epsilon_1^m$ for any $m \geq 1$. Then,

$$\epsilon_1^n < \eta < \epsilon_1^{n+1} \text{ for some } n.$$

Thus,

$$1 < \frac{\eta}{\epsilon_1^n} < \epsilon_1.$$

We also have

$$\begin{aligned} \frac{\eta}{\epsilon_1^n} &= \frac{x + \sqrt{d}y}{x_n + \sqrt{d}y_n} \frac{x_n - \sqrt{d}y_n}{x_n - \sqrt{d}y_n} \\ &= \frac{(xx_n - dy y_n) + \sqrt{d}(x_n y - x y_n)}{x_n^2 - dy_n^2} \\ &= xx_n - dy y_n + \sqrt{d}(x_n y - x y_n). \end{aligned}$$

Since $(x, -y)$ and (x_n, y_n) satisfy equation (7.5), by adapting equation (7.6), we get that

$$(xx_n - dy y_n, xy_n - yx_n)$$

is a solution $x^2 - dy^2 = 1$. Thus,

$$(r, s) = (xx_n - dy y_n, xy_n - yx_n)$$

is also a solution. Note, from above, that

$$1 < \frac{\eta}{\epsilon_1^n} = r + \sqrt{d}s < \epsilon. \quad (7.7)$$

We now show that (r, s) is a positive solution. Since $1 < r + s\sqrt{d}$, we have $0 < r - s\sqrt{d} < 1$. Thus,

$$2r = (r + s\sqrt{d}) + (r - s\sqrt{d}) > 1 + 0 > 0,$$

$$s\sqrt{d} = (r + s\sqrt{d}) - (r - s\sqrt{d}) > 1 - 1 = 0.$$

Thus, $r, s > 0$. Since (x_1, y_1) is a fundamental solution, $x_1 < r$, $y_1 < s$. This implies

$$x_1 + y_1\sqrt{d} < r + s\sqrt{d},$$

which contradicts equation (7.7). Thus, our assumption is false. $\square$

The above theorem therefore reduces the problem of finding all positive solutions of Pell's equation to finding the fundamental solution, if it exists. This problem is intricately connected with that of finding the continued fraction of $\sqrt{d}$. In Exercise 7.2.6, we saw that any positive solution (x, y) of $x^2 - dy^2 = 1$ is of the form $x = p_k$, $y = q_k$ for some convergent $\frac{p_k}{q_k}$ of $\sqrt{d}$. Using the continued fraction of $\sqrt{d}$, one can, in fact, find out precisely which convergent gives the fundamental solution of $x^2 - dy^2 = 1$. The following theorem answers this question:

Theorem 7.5.5 Suppose $\sqrt{d} = [a_0, \overline{a_1, a_2, \dots, a_n}]$. The fundamental solution of $x^2 - dy^2 = 1$ is

$$(p_{n-1}, q_{n-1}) \text{ if } n \text{ is even}$$

and

$$(p_{2n-1}, q_{2n-1}) \text{ if } n \text{ is odd.}$$

Exercise 7.5.6 Find the continued fraction expansions of $\sqrt{33}$ and $\sqrt{41}$. Use these to find the fundamental solution of the equations $x^2 - 33y^2 = 1$ and $x^2 - 41y^2 = 1$.