國立交通大學

資訊科學與工程研究所

碩士論文

利用複乘法產生質數點數之橢圓曲線

Generating Elliptic Curves with Prime Order by Complex Multiplication

研 究 生：蔡佩娟

指導教授：陳榮傑　教授

中華民國 九十八年十月

利用複乘法產生質數點數之橢圓曲線
Generating Elliptic Curves with Prime Order by Complex Multiplication

研究生：蔡佩娟　　Student：Pei-Chuan Tsai

指導教授：陳榮傑　　Advisor：Dr. Rong-Jaye Chen

國立交通大學
資訊科學與工程研究所
碩士論文

A Thesis
Submitted to Institute of Computer Science and Engineering
College of Computer Science
National Chiao Tung University
in partial Fulfillment of the Requirements
for the Degree of
Master
in

Computer Science

October 2009

Hsinchu, Taiwan, Republic of China

中華民國九十八年十月

利用複乘法產生質數點數之橢圓曲線

學生：蔡佩娟　　　　　　　　　　　指導教授：陳榮傑博士

國立交通大學資訊科學與工程研究所　碩士班

摘要

自從 Koblitz 和 Miller 於 1985 年首度利用橢圓曲線建構密碼系統以來，橢圓曲線密碼學因其較短之金鑰長度及較佳計算效率的優點吸引了許多密碼學家投入此研究領域中。如何有效率的產生符合安全需求之橢圓曲線來建構密碼系統一直是很重要的議題。基於雙線性配對之密碼系統爲一種橢圓曲線密碼系統，而建構此密碼系統之橢圓曲線須符合具有較小的嵌入數 (embedding degree)。在目前已知的方法中，只有複乘法能夠產生符合此種要求之橢圓曲線。

複乘法可允許使用者先決定了定義於有限體之橢圓曲線上的點數個數，而後再利用數學方法產生具有此點數之橢圓曲線。由於可事先決定點數個數，故可控制點數個數使得產生之橢圓曲線將會具有較小之嵌入數。另一方面，相較於隨機產生曲線再計算點數是否符合安全需求的方法，如 Schoof 演算法、 SEA 演算法，一旦所選定的點數符合數學定理的要求，複乘法便能準確的計算出曲線。在本篇論文中，我們詳細地介紹與複乘法相關之數學背景，並實作出計算 Weber 類別多項式 (Weber class polynomial) 之演算法，此部分在複乘法中爲最占時間之計算步驟。

關鍵字：橢圓曲線、複乘法、類別多項式。

Generating Elliptic Curves with Prime Order by Complex Multiplication

Student: Pei-Chuan Tsai

Advisor: Dr. Rong-Jaye Chen

Institute of Computer Science and Engineering
National Chiao Tung University

ABSTRACT

From the use of elliptic curves in cryptosystem first proposed by Koblitz and Miller in 1985, elliptic curve cryptography had attracted lots of cryptographic researchers. The benefits, such as shorter key size and efficient computation, make it become a popular and better solution to constructing cryptosystems. It is an important issue that efficiently generating the suitable elliptic curves for constructing the cryptosystem. One of the cryptosystems is the pairing based cryptosystem. For the pairing based cryptosystem, the smaller embedding degree is the main requirement of the elliptic curves. Currently, the only way to generate such curves is complex multiplication.

The complex multiplication allows us to determine the number of points on the elliptic curves defined over finite field first, then compute the curves with the desired order. Comparing to the method that selects random curves and uses point counting algorithm to generate secure elliptic curves, complex multiplication is a deterministic algorithm. In this thesis, we summarize the mathematical backgrounds for complex multiplication and implement the algorithm of computing the Weber class polynomial which plays an important role in complex multiplication.

Keywords: elliptic curve, complex multiplication, class polynomial

誌謝

這篇碩士論文能夠順利完成，首先要感謝指導老師陳榮傑教授，老師不僅在學術上的悉心教導令我受惠良多，對於求學過程中的照顧、以及做人處事上的提點，皆令我感念在心，由衷地感謝老師。同時也謝謝張仁俊教授、楊一帆教授與胡鈞祥博士擔任我的口試委員，並在口試時給予提點、意見，以及對論文提供修正建議，都使得本篇論文能更加完整。

感謝 Cryptanalysis 實驗室的志賢學長、定宇學長、順隆學長、家瑋學長、嘉軒學長，和同學用翔、輔國，不只是研究上的討論、或是生活上的經驗分享，都給了我很大的幫助，謝謝你們。

此外要特別感謝系上的排球隊，除了舉辦各式各樣新奇有趣的活動，讓我的研究生活充滿活力與歡笑之外，也常讓我有溫暖、窩心的感受，這都是很重要的一部分，在此想特別感謝志銘和昌裕。

最後要感謝我的家人，感謝父母的栽培以及在我求學過程中給我的建議與支持，謝謝姊姊與弟弟的關心，你們的支持是我順利完成學業過程中不可或缺的一部分。

感謝所有在我研究生涯中曾幫助過我的人，謹以此文論獻給我摯愛的家人、以及所有關心我的師長、朋友，謝謝你們。

Contents

List of Tables

List of Figures

Chapter 1

Introduction

In 1985, Koblitz and Miller first proposed the crytosystems based on elliptic curves. The advantages of the elliptic cryptography attract the researchers to involve in the related area. Since there does not exist efficient attacks, e.g. index calculus attacks, in elliptic curve cryptosystems (ECCs), the key size of ECCs can be much shorter comparing to the traditional cryptosystems based on the hardness of the discrete logarithm or the factoring problem. Table 1.1 shows the recommended key sizes provided by NIST (National Institute of Standards and Technology). Nowadays, more applications and systems apply the technology of the elliptic curve cryptography as security solutions. A lot of standards and protocols related to elliptic curve cryptography are also proposed. For standards, there are IEEE 1363, ANSI X9.62, X9.63, and ECDSA, ECMQV, ECIES are for protocols.

The points of an elliptic curve would form an addition group and it can define a variant of discrete logarithm problem on it, called elliptic curve discrete logarithm problem (ECDLP). The ECCs can devide into two categories: one based on the hardness of ECDLP and the other based on the bilinear pairing. The bilinear pairing defined on the elliptic curve makes

Symmetric Key Size (bits)	RSA and Diffie-Hellman Key Size (bits)	Elliptic Curve Key Size (bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

Table 1.1: NIST recommended key sizes

the identity based (ID-based) cryptosystem proposed by Shamir in 1984 feasible. The first ID-based encryption scheme proposed by Boneh and Franklin is using the pairings defined over elliptic curve and finite field.

To setup a cryptosystem, the parameters must be chosen carefully to satisfy the security requirements. The generation of suitable elliptic curves is a crucial problem. The best known algorithm for generating the curves used in ECCs based on ECDLP is Schoof's algorithm and the improved version, SEA algorithm. These algorithms randomly select curves and count the number of points of the curves repeatedly until the curves satisfy the ssecurity properties. In pairing based cryptosystem, the security requirements of the curve are different and the SEA algorithm can not be used. These elliptic curves suitable for pairing cryptosystems are called pairing-friendly curves. The complex multiplication is the only way to generate these kind of curves.

In this thesis, we present a clear view of complex multiplication and implement the algorithm to show how it works. Observing that computation of the class polynomial takes the most time of whole computing, we focus on this part and show our experimental results. The rest of the thesis was organized as following.

In Chapter 2, we review the related mathematical backgrounds for this thesis. The algebraic backgrounds were presented first, including the definitions of algebraic structures, the properties of finite fields. Then review the elliptic curve cryptography by introducing the general elliptic curves and the elliptic curves defined over finite fields. For the theory of complex multiplication involves the complex plane closely, we describe the elliptic curves defined over complex field more detailed.

In Chapter 3, we use examples to introduce the algorithms known to generating elliptic curves. The first one is using subfield curves. The second is the Schoof's algorithm and the SEA algorithm mentioned above. The last is the complex multiplication. We also provide an example for generating the pairing-friendly elliptic curves.

In Chapter 4, each step of the complex multiplication are described particularly. Besides point out the relevant theorems and properties, we also provide the algorithms may be used in practical. Then in Chapter 5, the experimental results of the implementation of computing the class polynomial are presented. Finally, the conlusion is given in Chapter 6.

Chapter 2

Mathematical Backgrounds

The researches of elliptic curve cryptography are related to algebraic theory closely. In this chapter, we review the mathematical backgrounds of this work in Section 2.1. And then introduce the definition of elliptic curves and its propoerties in Section 2.2.

2.1 Algebraic Backgrounds

In this section, we introduce the elementary algebraic structures and the algebraic backgrounds of the material related to the complex multiplication method (CM method), including imaginary quadratic fields, homomorphisms, and modular functions.

2.1.1 Group, Ring, and Field

The elliptic curve cryptosystems are mainly based on the hard problem of the elliptic curve discrete logarithm problem. Since the points on an elliptic curve defined over a finite field form a group, we introduce the elementary algebraic structures and some propositions, theorems related.

Definition 2.1 (Group)**.** A group G is a set with a composition law $\times$ if it satisfies the following conditions:

- $\times$ is associative, i.e. for all $x, y, z \in G$, $(xy)\,x = x\,(yz)$
- $\times$ has an identity element, i.e., for all $x \in G$, $xe = ex = x$
- For all $x \in G$, there exists an element $y \in G$ such that $xy = yx = e$. y is called the inverse of x, usually denoted $y = x^{-1}$

If the composition law is commutative, the group is said to be commutative or abelian. The cardinality of a group is also called its order, denoted by $|G|$, therefore, a group is finite if its order is finite.

Definition 2.2 (Subgroup)**.** Let G be a group. A group H is a subgroup of G if H satisfies:

- H is a subset of G
- $e \in H$, where e is the identity of group G
- for all $x, y \in H$, xy must also be in H
- if $x \in H$, $x^{-1} \in H$

For $x \in G$, denote $\langle x \rangle$ as the subgroup of G generated by x

$$\langle x \rangle = \{x^n | n \in \mathbb{Z}\}$$

Definition 2.3. A group G is said cyclic if there is an element $x \in G$ such that $\langle x \rangle = G$. If such an element x exists, it is called a generator of G.

Theorem 2.4 (Lagrange)**.** Let G be a finite group and H be a subgroup of G. Then

$$|H| \text{ devides } |G|.$$

As a result, the order of every element also divides $|G|$

Definition 2.5 (Ring)**.** A ring R is a set together with two composition laws $+$ and $\times$ such that

- R is a commutative group with respect to $+$
- $\times$ is associative and has an identity element $e_\times$ and $e_\times \neq e_+$, where e_+ is the identity of $+$
- $\times$ is distributive over $+$, i.e., for all $x, y, z \in R$, $x(y+z) = xy + xz$ and $(y+z)x = yx + zx$

Also, the ring R is commutative, if the law $\times$ is commutative. A commutative ring R such that $xy = 0$ implies $x = 0$ or $y = 0$ for all $x, y \in R$ is called an integral domain.

Definition 2.6. Let R be a ring. Define the ideal I of R as a nonempty subset of R such that

- I is a subgroup of R with respect to the law $+$
- for all $x \in R$ and $y \in I$, $xy \in I$ and $yx \in I$

Remark 2.7. In a commutative ring R of prime characteristic p, the binomial formula can be simplified as

$$(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} \quad \forall \alpha, \beta \in R\text{and } n \in \mathbb{N}.$$

Theorem 2.8 (Fermat's little theorem)**.** Let p be a prime integer, $x \in \mathbb{N}$ and $\gcd(x, p) = 1$, then

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

Definition 2.9 (Euler totient function)**.** Let $n \geqslant 1$ and define the Euler totient function (Euler's phi function) as

$$\varphi(n) = \left|\{x | 1 \leqslant x \leqslant n, \gcd(x, n) = 1\}\right|.$$

Theorem 2.10 (Euler)**.** Let n, x be integers and $\gcd(x, n) = 1$, then

$$x^{\varphi(n)} \equiv 1 \pmod{n}$$

Definition 2.11. Let R be a ring. An element x is said to be invertible if there exists an unique element y such that $xy = ya = e_{\times} = 1$, denoted $y = x^{-1}$. The set of all the invertible elements of R forms a group under multiplication, denoted by R^*.

Definition 2.12 (Field)**.** A field K is a commutative ring such that every nonzero element is invertible.

Definition 2.13 (Extension field)**.** Let K and L be fields. If there exists a field homomorphism from K into L, then L is an extension field of K, denoted by L/K.

Definition 2.14 (Number field)**.** A number field K is an algebraic extension of $\mathbb{Q}$ of finite degree. An element of K is called an algebraic number.

2.1.2 Imaginary Quadratic Field

Definition 2.15 (Quadratic field)**.** A quadratic field is a number field K of degree 2 over $\mathbb{Q}$.

A quadratic field $\mathbb{Q}\left(\sqrt{d}\right)$ is said to be real if d is positive, imaginary if d is negative.

Proposition 2.16. The quadratic fields are precisely those of the form $\mathbb{Q}\left(\sqrt{d}\right)$ for d a squarefree rational integer.

Proof. Express the quadratic field K as $\mathbb{Q}(\theta)$, then θ is an algebraic integer and θ is a zero of

$$x^2 + ax + b \quad a, b \in \mathbb{Z}.$$

Thus

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

Let $a^2 - 4b = r^2 d$ for some $r, d \in \mathbb{Z}$ and d be squarefree, then

$$\theta = \frac{-a \pm r\sqrt{d}}{2}$$

and so $\mathbb{Q}(\theta) = \mathbb{Q}\left(\sqrt{d}\right)$. □

Definition 2.17 (Algebraic integer)**.** Let $K/\mathbb{Q}$ be a number field. An algebraic number α is called integral over $\mathbb{Z}$ or an algebraic integer if α is a zero of a monic polynomial with coefficients in $\mathbb{Z}$.

The set of all the algebraic integers of K under the addition and multiplication of K is a ring, called the integer ring of K and is denoted by $\mathcal{O}_K$.

Theorem 2.18. Let d be a squarefree rational integer. Then the integers of $\mathbb{Q}\left(\sqrt{d}\right)$ are:

(1) $\mathbb{Z}\left[\sqrt{d}\right]$ if $d \not\equiv 1 \pmod 4$,

(2) $\mathbb{Z}\left[\frac{1}{2}+\frac{1}{2}\sqrt{d}\right]$ if $d \equiv 1 \pmod 4$.

Proof. Given an element $\alpha \in \mathbb{Q}\left(\sqrt{d}\right)$, it can be expressed as $\alpha = r + s\sqrt{d}$ for some $r, s \in \mathbb{Q}$. Then we can write

$$\alpha = \frac{a+b\sqrt{d}}{c}, \qquad a, b, c \in \mathbb{Z}, c > 0$$

and no prime divides all of a, b, c. By Definition 2.17, α is an algebraic integer if and only if the minimal polynomial of α

$$\left(t - \left(\frac{a+b\sqrt{d}}{c}\right)\right)\left(t - \left(\frac{a-b\sqrt{d}}{c}\right)\right) = t^2 - \frac{2a}{c}t + \frac{a^2-b^2d}{c^2}$$

has all the coefficients in $\mathbb{Z}$. Thus

$$\frac{2a}{c} \in \mathbb{Z}, \tag{2.1}$$

$$\frac{a^2-b^2d}{c^2} \in \mathbb{Z}. \tag{2.2}$$

From Equation 2.1, c must divides either 2 or a. Assume $\gcd(a, c) = p$, then Equation 2.2 implies that p divides b since d is squarefree. That contradicts the assumption: no prime divides all of a, b, c. Hence we have c divides 2, $\Rightarrow$ $c = 1$ or 2. If $c = 1$, then α is an algebraic integer in any case.

If $c = 2$, by assumption, we have both a and b be odd integers. For the square of an odd integer $2k+1$ is $4k^2+4k+1 \equiv 1 \pmod 4$, and for Equation 2.2

$$\frac{a^2-b^2d}{c^2} = \frac{a^2-b^2d}{4} \in \mathbb{Z},$$

$$\Rightarrow \quad a^2 - b^2d \equiv 0 \pmod 4,$$

it implies that $a^2 \equiv b^2 \equiv 1 \pmod 4$ and $d \equiv 1 \pmod 4$. Conversely, if $d \equiv 1 \pmod 4$, then for odd a and b, α can still be an algebraic integer because Equation 2.1 and 2.2 hold.

So we proved that:

(1) If $d \not\equiv 1 \pmod 4$, then $c = 1$. Hence the integers of $\mathbb{Q}\left(\sqrt{d}\right)$ is $\mathbb{Z}\left[\sqrt{d}\right]$.

(2) If $d \equiv 1 \pmod 4$, we can have $c = 2$, a, b odd and α also be an algebraic integer. Hence the integers of $\mathbb{Q}\left(\sqrt{d}\right)$ is $\mathbb{Z}\left[\frac{1}{2} + \frac{1}{2}\sqrt{d}\right]$.

□

Definition 2.19 (Integral bases)**.** If $\mathcal{O}_K$ is the ring of integers of an algebraic number field K, then a basis for $\mathcal{O}_K$ over $\mathbb{Z}$, or simply a $\mathbb{Z}$-basis, is called an integral basis for K

Definition 2.20 (Discriminant of a basis)**.** Let $K = \mathbb{Q}(\alpha)$ be an algebraic number field of degree d over $\mathbb{Q}$. If

$$\mathcal{B} = \{\alpha_1, \alpha_2, \ldots, \alpha_d\}$$

is a $\mathbb{Q}$-basis for K, and $\sigma_i \ (1 \leqslant i \leqslant d)$ are all of the embeddings of Kin $\mathbb{C}$, then the discriminant of the basis is given by

$$disc\,(\mathcal{B}) = \det\left(\sigma_i\left(\alpha_j\right)\right)^2,$$

where $\det$ denotes the determinant of the matrix with entry $\sigma_i\left(\alpha_j\right)$ in the i^{th} row and j^{th} column.

Note: An embedding of K in $\mathbb{C}$ is a ring homomorphism $K \to \mathbb{C}$.

Example 2.21. Let $\mathcal{B} = \left\{1, \sqrt{2}\right\}$ be an integral basis for K, and

$$\sigma_1 : \sqrt{2} \mapsto \sqrt{2}, \quad \sigma_2 : \sqrt{2} \mapsto -\sqrt{2},$$

be the embeddings of K in $\mathbb{C}$. Thus,

$$disc\left(\mathcal{B}\right) = \det\left(\sigma_i\left(\alpha_j\right)\right)^2 = \det\begin{pmatrix} \sigma_1\left(1\right) & \sigma_1\left(\sqrt{2}\right) \\ \sigma_2\left(1\right) & \sigma_2\left(\sqrt{2}\right) \end{pmatrix}^2$$

$$= \det\begin{pmatrix} 1 & \sqrt{2} \\ 1 & -\sqrt{2} \end{pmatrix}^2 = \left(-2\sqrt{2}\right)^2 = 8.$$

Lemma 2.22. Let $\mathcal{B}_1$ and $\mathcal{B}_2$ be two integral bases for an algebraic number field K. Then

$$disc\left(\mathcal{B}_1\right) = disc\left(\mathcal{B}_2\right).$$

Definition 2.23. Let $\mathcal{B}$ be an integral basis for an algebraic number field K. Then the discriminant of K is $disc\left(\mathcal{B}\right)$, denoted by Δ_K.

Theorem 2.24. Let $d \neq 1$ be a squarefree integer and set $K = \mathbb{Q}\left(\sqrt{d}\right)$, with discriminant Δ_K. Then

$$\mathcal{B} = \begin{cases} \left\{1, \frac{1}{2} + \frac{1}{2}\sqrt{d}\right\} & \text{if } d \equiv 1 \pmod{4} \\ \left\{1, \sqrt{d}\right\} & \text{if } d \not\equiv 1 \pmod{4} \end{cases},$$

and

$$\Delta_K = \begin{cases} d & \text{if } d \equiv 1 \pmod{4} \\ 4d & \text{if } d \not\equiv 1 \pmod{4} \end{cases},$$

where d is called the radicand of K.

Proof. By Theorem 2.18, the assertions regarding bases are clear. For the definition of the discriminant of a field, we compute the Δ_K in both cases:

(1) If $d \equiv 1 \pmod 4$,

$$\Delta_K = disc\left(\mathcal{B}\right) = \det \begin{pmatrix} 1 & \frac{1}{2}+\frac{1}{2}\sqrt{d} \\ 1 & \frac{1}{2}-\frac{1}{2}\sqrt{d} \end{pmatrix}^2 = \left(-\sqrt{d}\right)^2 = d.$$

(2) If $d \not\equiv 1 \pmod 4$,

$$\Delta_K = disc\left(\mathcal{B}\right) = \det \begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix}^2 = \left(-2\sqrt{d}\right)^2 = 4d.$$

□

An order in an imaginary quadratic field is a ring R such that $\mathbb{Z} \subset R \subseteq \mathcal{O}_K$ and $\mathbb{Z} \neq R$. Therefore, an order has the form

$$R = \mathbb{Z} + \mathbb{Z}f\delta, \quad \text{where } f > 0,\ \delta = \begin{cases} \frac{1}{2}+\frac{1}{2}\sqrt{d} & \text{if } d \equiv 1 \pmod 4 \\ \sqrt{d} & \text{if } d \not\equiv 1 \pmod 4 \end{cases}$$

The integer f is called the conductor of R and is the index of R in $\mathcal{O}_K$. As the result, a basis of an order in an imaginary field R can be

$$\mathcal{B}_R = \{1, f\delta\}.$$

Use the same concept of the discriminant of a number field, we obtain the discriminant of the order

(1) If $d \equiv 1 \pmod 4$,

$$\Delta_R = disc\left(\mathcal{B}_R\right) = \det \begin{pmatrix} 1 & f\left(\frac{1}{2}+\frac{1}{2}\sqrt{d}\right) \\ 1 & f\left(\frac{1}{2}-\frac{1}{2}\sqrt{d}\right) \end{pmatrix}^2 = \left(-f\sqrt{d}\right)^2 = f^2 d.$$

Quadratic Field	Integer Ring	Integral Basis	Discriminant
$K=\mathbb{Q}\left(\sqrt{d}\right)$	$\mathcal{O}_K$	$\mathcal{B}$	Δ_K
$d\equiv 1 \pmod 4$	$\mathbb{Z}\left[\frac{1}{2}+\frac{1}{2}\sqrt{d}\right]$	$\left\{1, \frac{1}{2}+\frac{1}{2}\sqrt{d}\right\}$	d
$d\not\equiv 1 \pmod 4$	$\mathbb{Z}\left(\sqrt{d}\right)$	$\left\{1, \sqrt{d}\right\}$	$4d$

Table 2.1: Properties related to the quadratic field $\mathbb{Q}\left(\sqrt{d}\right)$

Quadratic Field	Order with Index f	Basis	Discriminant
$K=\mathbb{Q}\left(\sqrt{d}\right)$	R	$\mathcal{B}_R$	Δ_R
$d\equiv 1 \pmod 4$	$\mathbb{Z}\left[f\left(\frac{1}{2}+\frac{1}{2}\sqrt{d}\right)\right]$	$\left\{1, f\left(\frac{1}{2}+\frac{1}{2}\sqrt{d}\right)\right\}$	f^2d
$d\not\equiv 1 \pmod 4$	$\mathbb{Z}\left(f\sqrt{d}\right)$	$\left\{1, f\sqrt{d}\right\}$	$4f^2d$

Table 2.2: Properties related to an order in the quadratic field $\mathbb{Q}\left(\sqrt{d}\right)$

(2) If $d\not\equiv 1 \pmod 4$,

$$\Delta_R = disc\left(\mathcal{B}_R\right) = \det\begin{pmatrix} 1 & f\sqrt{d} \\ 1 & -f\sqrt{d} \end{pmatrix}^2 = \left(-2f\sqrt{d}\right)^2 = 4f^2d.$$

We summarize the results related to a quadratic field $\mathbb{Q}\left(\sqrt{d}\right)$, for $d\neq 0,1$ an squarefree integer, discussed above in Table 2.1.

And for an order R in $K=\mathbb{Q}\left(\sqrt{d}\right)$ with index f, the related results are also concluded in Table 2.2.

2.1.3 Homomorphism

Definition 2.25 (Group homomorphism)**.** Let G_1 and G_2 be two groups with respective composition laws $\times$ and $\otimes$ and identities e_1 and e_2.

- A group homomorphism ψ between G_1 and G_2 is a map from G_1 to G_2 such that for all $x, y \in G_1$
$$\psi\left(x \times y\right) = \psi\left(x\right) \otimes \psi\left(y\right).$$
- The kernel of ψ is $Ker\left(\psi\right) = \{x \in G_1 | \psi\left(x\right) = e_2\}$.

Definition 2.26 (Ring homomorphism)**.** Let R_1 and R_2 be two rings with the respective operations $+$, $\times$ and $\oplus$, $\otimes$. A ring homomorphism ψ is a map from R_1 to R_2 such that for all $x, y \in R_1$

- $\psi\left(x + y\right) = \psi\left(x\right) \oplus \psi\left(y\right)$.
- $\psi\left(x \times y\right) = \psi\left(x\right) \otimes \psi\left(y\right)$.
- $\psi\left(e_\times\right) = e_\otimes$.

Definition 2.27 (Field homomorphism)**.** Let K and L be fields. A homomorphism of fields is a ring homomorphism between K and L.

Definition 2.28. Let R be a ring and let ψ be the natural ring homomorphism from $\mathbb{Z}$ to R.

$$\psi\left(n\right) = \begin{cases} \left(1 + \cdots + 1\right) & n \text{ times if } n \geqslant 0 \\ -\left(1 + \cdots + 1\right) & -n \text{ times otherwise.} \end{cases}$$

Definition 2.29 (Characteristic)**.** Let R be a ring and ψ be a natural ring homomorphism defined as above. The kernel of ψ is of the form $m\mathbb{Z}$, for some nonnegative integer m. Then the nonnegative integer m is called the characteristic of R, denoted by $char\,(R)$.

2.1.4 Modular Functions

Definition 2.30. Let N be a positive integer. The modular group $\Gamma_0\,(N)$ is defined as

$$\Gamma_0\,(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2\,(\mathbb{Z}) : c \equiv 0 \pmod{N} \right\}.$$

The matrix $SL_n\,(F)$, or $SL\,(n, F)$, known as the special linear group of degree n over a field F is the set of $n \times n$ matrices with determinant 1 with group operations of ordinary matrix multiplication and matrix inversion.

Definition 2.31 (Modular function)**.** A complex function f which is meromorphic on the upper half plane

$$\mathcal{H} = \{\tau \in \mathbb{C} | \Im m\,(\tau) > 0\}$$

and which satisfies

$$f\,(\tau) = f\,(M\tau)\,, \quad \text{where } M \in \Gamma_0\,(N)$$

is called a modular function.

2.2 Elliptic Curves

Here we introduce the difinitions of elliptic curves and illustrate some propoerties of elliptic curves.

2.2.1 General Elliptic Curves

We illustrate the general definitions of elliptic curves in this section and focus on the elliptic curves defined over finite fields and the complex field $\mathbb{C}$ in the Section 2.2.2 and Section 2.2.3.

Definition 2.32. An elliptic curve E defined over a field K, denoted by E/K, is given by the **Weierstrass equation**

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.3}$$

where $a_1, a_2, a_3, a_4, a_6 \in K$.

The set of K-rational points of the elliptic curve, $E(K)$, is defined as the set of the solutions to the elliptic curve equation in K^2 and the point at infinity ∞,

$$E(K) = \left\{(x, y) \middle| y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, x, y \in K\right\} \cup \infty.$$

Figure 2.1 shows some examples of the elliptic curves defined over $\mathbb{R}$.

For an elliptic curve given by Equation 2.3, defining the following constants to be used in later definition:

$$b_2 = a_1^2 + 4a_2, \quad b_4 = a_1a_3 + 2a_4, \quad b_6 = a_3^2 + 4a_6,$$

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,$$

$$c_4 = b_2^2 - 24b_4, \quad c_6 = -b_2^3 + 36b_2b_4 - 216b_6.$$

Definition 2.33 (Discriminant)**.** Define the discriminant of the curve be

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6.$$

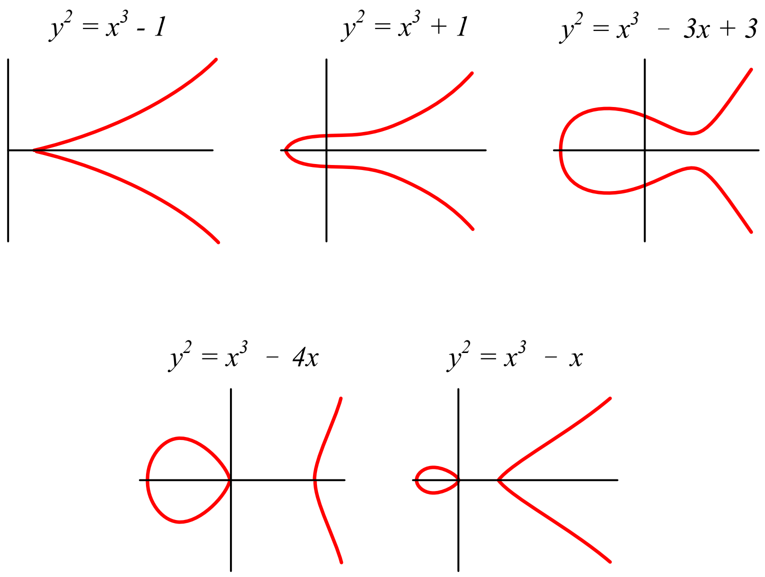


Figure 2.1: Examples of elliptic curves over $\mathbb{R}$

If the characteristic of K, $char\,(K) \neq 2, 3$, the discriminant can be expressed as

$$\Delta = \frac{c_4^3 - c_6^2}{1728}.$$

After defining the discriminant, we say a curve is non-singular if and only if $\Delta \neq 0$.

Definition 2.34 (j-invariant)**.** For a non-singular curve, i.e. $\Delta \neq 0$, define the j-invariant of the curve as

$$j\,(E) = \frac{c_4^3}{\Delta}$$

We focus on the properties of the K-rational points in the following.

Definition 2.35 (Group law)**.** Define the addition and doubling of points as below.

Addition:

Given two distinct K-rational points of E, denoted as P, Q. The straight line joining P and Q must intersect the curve E at one further points, said R'. Reflecting point R' in the x-axis, we obtain the point R. Define $R = P + Q$.

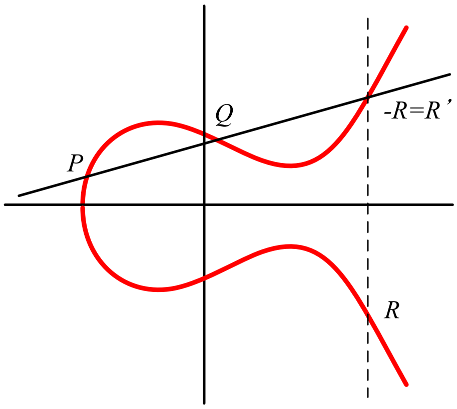


Figure 2.2: Point addition (chord process)

Doubling:

Given a rational point P on E, define the doubling, or the addition of P to itself, as the following proccess. Take the tangent to the curve E at P, the line would intersect the curve in one other point, said R'. Also, reflecting point R' in the x-axis and obtaining the point R, Then the doubling of P is defined by $R = P + P = 2P$.

Note that if the tangent of the point is vertical, we say that it intersect the curve at the point at infinity, and define $P + P = 2P = \infty$.

The process of addition and doubling is often called the chord-tangent process. Figure 2.2 illustrates the proccess of addition and Figure 2.3 of doubling.

According to the group law defined above, it can be shown that the set of the rational points of E including point at ∞ forms an additive abelian group with the point ∞ as the zero.

Lemma 2.36. Let E be an elliptic curve given by

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

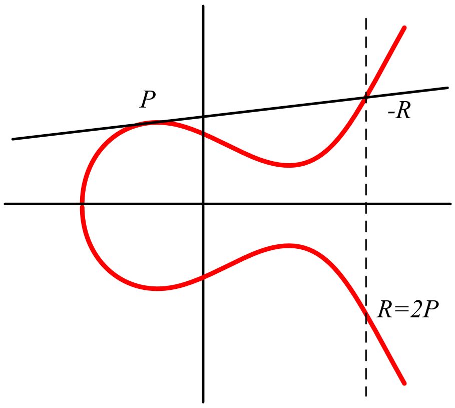


Figure 2.3: Point doubling (tangent process)

and let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be the points on the curve. Then

$$-P = (x_1, -y_1 - a_1x_1 - a_3)\,.$$

Set

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & \text{if } x_1 \neq x_2 \\ \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, & \text{if } x_1 = x_2 \text{ and } P_2 \neq -P_1 \end{cases},$$

$$\mu = \begin{cases} \dfrac{y_1x_2 - y_2x_1}{x_2 - x_1}, & \text{if } x_1 \neq x_2 \\ \dfrac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}, & \text{if } x_1 = x_2 \text{ and } P_2 \neq -P_1 \end{cases}.$$

If

$$P_3 = (x_3, y_3) = P_1 + P_2 \neq \infty,$$

then x_3, y_3 would be

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2,$$

$$y_3 = -(\lambda + a_1)\,x_3 - \mu - a_3.$$

Definition 2.37 (Multiplication-by-m map)**.** For a positive integer m, let mP denote the map that takes a point P to $P + P + \cdots + P$ (m summands). The notation mP is extended to $m \leqslant 0$ by defining $0P = \infty$ and $-mP = -(mP)$.

2.2.2 Elliptic Curves over $\mathbb{F}_q$, $q > 3$

After introducing the general elliptic curves in Section 2.2.1, now we focus on the elliptic curves defined over the finite field $\mathbb{F}_q$ for $q > 3$.

Recall the general elliptic curve equation, the **Weierstrass equation**:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

If the characteristic of the field is not 2, the equation can be wirtten as

$$\begin{aligned}\left(y + \frac{a_1x}{2} + \frac{a_3}{2}\right)^2 &= x^3 + \left(a_2 + \frac{a_1^2}{4}\right)x^2 + \left(a_4 + \frac{a_1a_3}{2}\right)x + \left(\frac{a_3^2}{4} + a_6\right) \\ \Rightarrow \quad y_1^2 &= x^3 + a_2'x^2 + a_4'x + a_6',\end{aligned}$$

where $y_1 = y + \frac{a_1x}{2} + \frac{a_3}{2}$ and new constants $a_2' = a_2 + \frac{a_1^2}{4}, a_4' = a_4 + \frac{a_1a_3}{2}, a_6' = \frac{a_3^2}{4} + a_6$.

If the characteristic is also not 3, let $x_1 = x + \frac{a_2'}{3}$

$$\begin{aligned} y_1^2 &= x^3 + a_2'x^2 + a_4'x + a_6' \\ \Rightarrow \quad y_1^2 &= x_1^3 + Ax_1 + B,\end{aligned}$$

for some constants A, B.

In the following, since the elliptic curves we are interested are defined over the fields with characteristic neither 2 nor 3, we use the simplified equation instead of the Weierstrass equation.

We reduce the related definitions and the group law for the elliptic curve equation $E : y^2 = x^3 + Ax + B$.

Definition 2.38. The discriminant of the curve can be reduced as

$$\Delta = -16\left(4A^3 + 27B^2\right).$$

Definition 2.39. For a non-singular curve, i.e. $\Delta \neq 0$, the j-invariant of the curve can be reduced as

$$j(E) = -1728 \times \frac{4A^3}{\Delta} = 1728 \times \frac{4A^3}{4A^3 + 27B^2}.$$

We obtain that when $j \neq 0, 1728$, it is the j-invariant of the elliptic curve

$$y^2 = x^3 + \frac{3j}{1728 - j}x + \frac{2j}{1728 - j}.$$

Therefore, we can construct an elliptic curve with a known j-invariant. This would be helpful in the construction of elliptic curve with complex multiplication method.

Lemma 2.40. Let E be an elliptic curve defined over K. Assume the characteristic of K is prime to 6 and E is given by the simplified Weierstrass equation

$$E : y^2 = x^3 + Ax + B.$$

The j-invariant j_E depends only on the isomorphism class of E.

- $j_E = 0$ if and only if $A = 0$.

- $j_E = 1728$ if and only if $B = 0$.

- If $j_E \in K$ is not equal to $0, 1728$, then E is a quadratic twist of the elliptic curve

$$\tilde{E}_{j_E} : y^2 = x^3 + \frac{3j_E}{1728 - j_E}x + \frac{2j_E}{1728 - j_E}.$$

Corollary 2.41. Assume $\gcd(char(K), 6) = 1$. The isomorphism classes of elliptic curves E over K are, up to twists, uniquely determined by the absolute invariant j_E, and for every $j \in K$ there exists an elliptic curve with absolute invariant j.

If K is algebraically closed then the isomorphism classes of elliptic curves over K correspond one-to-one to the elements in K via the map $E \mapsto j_E$.

Definition 2.42. Let E be an elliptic curve given by

$$E : y^2 = x^3 + Ax + B$$

and let $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ be points on E with $P_1, P_2 \neq \infty$.

Then

$$-P_1 = (x_1, -y_1).$$

Set

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & \text{if } x_1 \neq x_2 \\ \dfrac{3x_1^2 + A}{2y_1}, & \text{if } x_1 = x_2, y_1 \neq 0 \end{cases}.$$

If $P_3 = (x_3, y_3) = P_1 + P_2 \neq \infty$, then

$$x_3 = \lambda^2 - x_1 - x_2,$$

$$y_3 = (x_1 - x_3)\lambda - y_1.$$

The number of rational points on an elliptic curve E defined over a finite field $\mathbb{F}_q$ is finite, we usally denote the quantity by $\#E(\mathbb{F}_q)$.

Theorem 2.43 (Hasse theorem)**.** Let E be an elliptic curve defined over $\mathbb{F}_q$. Then

$$\#E(\mathbb{F}_q) = q + 1 - t \text{ and } |t| \leqslant 2\sqrt{q}.$$

Remark 2.44. The integer t is equal to the trace of the Frobenius endomorphism.

For any integer $t \in \left[-2\sqrt{p}, 2\sqrt{p}\right]$, there is at least one elliptic curve E defined over $\mathbb{F}_p$ such that $\#E\left(\mathbb{F}_p\right) = p + 1 - t$.

Now we introduce the Frobenius endomorphism.

Definition 2.45 (Frobenius endomorphism)**.** The Frobenius endormorphism ϕ_q on an elliptic curve E over $\mathbb{F}_q$ is a group endomorphism of defined by

$$\phi_q : \left\{ \begin{array}{ccc} E\left(\overline{\mathbb{F}_q}\right) & \longrightarrow & E\left(\overline{\mathbb{F}_q}\right) \\ (x, y) & \longmapsto & \left(x^q, y^q\right) \\ \infty & \longmapsto & \infty \end{array} \right. .$$

The characteristic polynomial of ϕ_q is $\phi_q^2 - t\phi_q + q$.

Proposition 2.46. The endomorphism $\phi_q^2 - t\phi_q + q$ is equal to the zero map on E.

It means that for any point $(x, y) \in E\left(\mathbb{F}_q\right)$, we have

$$\begin{aligned} \phi_q^2 (x, y) - t\phi_q (x, y) + q (x, y) &= \left(x^{q^2}, y^{q^2}\right) - t\left(x^q, y^q\right) + q(x, y) \\ &= \infty. \end{aligned}$$

Theorem 2.47. For the endomorphism of an elliptic curve E over $\mathbb{F}_q$ defined by

$$\phi_q^2 - a\phi_q + q.$$

Then the Frobenius trace t is the unique integer such that

$$\phi_q^2 - t\phi_q + q = 0.$$

i.e. makes the endomorphism to zero map.

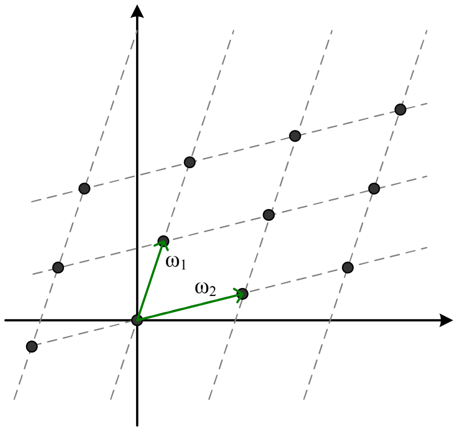


Figure 2.4: Lattic $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$

2.2.3 Elliptic Curves over $\mathbb{C}$

An elliptic curve defined over complex number $\mathbb{C}$ is isomorphic to a complex torus, denoted by $\mathbb{C}/L$. In this section, we introduce the isomorphism and the properties.

Let ω_1, ω_2 be complex numbers that are linearly independent over $\mathbb{R}$. A lattice L is of the form

$$L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \{n_1\omega_1 + n_2\omega_2 | n_1, n_2 \in \mathbb{Z}\}.$$

Figure 2.4 gives an illustration of a lattice. A torus over $\mathbb{C}$ can be expressed by $\mathbb{C}/L$.

Definition 2.48. An elliptic function with periods $\{\omega_1, \omega_2\}$ is a meromorphic function $f(x)$ on $\mathbb{C}$ such that

$$f(x + \omega_1) = f(x + \omega_2) = f(x), \quad \forall x \in \mathbb{C}$$

Definition 2.49 (Weierstrass $\wp$-function)**.** Given a lattice L, the Weierstrass $\wp$-function is defined by the series

$$\wp(z) = \wp(z, L) = \frac{1}{z^2} + \sum_{\omega \in L \setminus \{0\}} \left(\frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right).$$

Theorem 2.50. The Weierstrass $\wp$-function has the following properties

- The sum defining $\wp(z)$ converges absolutely and uniformly on compact sets not containing elements of L.
- $\wp(z)$ is meromorphic in $\mathbb{C}$ and has a double pole at each $\omega \in L$.
- $\wp(-z) = \wp(z), \forall z \in \mathbb{C}$.
- $\wp(z + \omega) = \wp(z), \forall \omega \in L$.
- The set of doubly periodic functions for L is $\mathbb{C}(\wp, \wp')$. It means that every doubly periodic function is a rational function of $\wp$ and its derivative $\wp'$.

Defferentiating $\wp(z)$ term by term yields

$$\wp'(z) = -2\sum_{\omega \in L} \frac{1}{(z-\omega)^3}.$$

Definition 2.51 (Eisenstein series). Define the Eisenstein series $G_n := G_n(L)$ of weight n for lattice L by

$$G_n(L) = \sum_{\omega \in L\backslash\{0\}} \omega^{-n}.$$

Proposition 2.52. The discriminant $\Delta = g_2^3 - 27g_3^2 \neq 0$.

Theorem 2.53. The elliptic functions $\wp$ and $\wp'$ satisfy the function

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_4\wp(z) - 140G_6.$$

To show the isomorphism of a torus $\mathbb{C}/L$ and an elliptic curve E, it is usually to set

$$g_2 = 60G_4, \quad g_3 = 140G_6.$$

Theorem 2.54. Let L be a lattice and let E be the elliptic curve $y^2 = 4x^3 - g_2 x - g_3$. The map

$$\Phi : \begin{cases} \mathbb{C}/L & \longrightarrow & E(\mathbb{C}) \\ z & \longmapsto & (\wp(z), \wp'(z)) \\ 0 & \longmapsto & \infty \end{cases}$$

is an isomorphism of groups.

For now, given a torus $\mathbb{C}/L$, it can be found the corresponding elliptic curve E over $\mathbb{C}$ by the Weierstrass $\wp$-function. The following shows the converse, given an elliptic curve E over $\mathbb{C}$, there is a lattice such that the torus $\mathbb{C}/L$ is isomorphic to E.

Definition 2.55. Two lattices L_1 L_2 are homothetic if there is an $\alpha \in \mathbb{C}^*$ suth that $\alpha L_1 = L_2$.

Let L be a lattice in $\mathbb{C}$ with basis $\{\omega_1, \omega_2\}$ and let

$$\tau = \frac{\omega_1}{\omega_2}$$

such that the imaginary part of τ, $\Im m(\tau) > 0$ (switching ω_1 and ω_2 if necessary). Let $L_\tau = \mathbb{Z} + \mathbb{Z}\tau$, then L_τ is homothetic to L.

Theorem 2.56. There is a canonical isomorphism between the set of $\mathbb{C}$-isomorphism classes of elliptic curves and the set of homothety classes of lattices in $\mathbb{C}$.

Corollary 2.57. Let $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ and $L_\tau = \mathbb{Z} + \mathbb{Z}\tau$ with $\tau = \omega_1/\omega_2$ such that τ is a complex number with $\Im m(\tau) > 0$. Then the elliptic curve E_L is isomorphic to E_{L_τ}.

Theorem 2.58. There is a canonical isomorphism between the set of $\mathbb{C}$-isomorphism classes of elliptic curves and the set of homothety classes of lattices in $\mathbb{C}$.

Recall the definitions for lattice $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, now we restrict to $L_\tau = \mathbb{Z} + \mathbb{Z}\tau$.

The Eisenstein series defined for $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ by Definition 2.51, define

$$\begin{aligned} G_k(\tau) &= G_k(L_\tau) = \sum_{(m,n)\neq(0,0)} \frac{1}{(m\tau+n)^k}, \\ g_2(\tau) &= g_2(L_\tau) = 60G_4(L_\tau), \\ g_3(\tau) &= g_3(L_\tau) = 140G_6(L_\tau) \end{aligned}$$

and let

$$q = e^{2\pi i\tau}.$$

Calculation of the discriminant Δ will get

$$\Delta(\tau) = g_2^3(\tau) - 27g_3^2(\tau) = (2\pi)^{12}(q + \cdots).$$

Definition 2.59. Define

$$j(\tau) = 1728\frac{g_2^3}{\Delta} = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \cdots.$$

Define the matrix

$$SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}.$$

and it performs on the upper half plane $\mathcal{H}$ by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\tau + b}{c\tau + d}, \quad \forall \tau \in \mathcal{H}.$$

The upper half plane of the complex plane is defined by

$$\mathcal{H} = \{x + iy \in \mathbb{C} | y > 0\}.$$

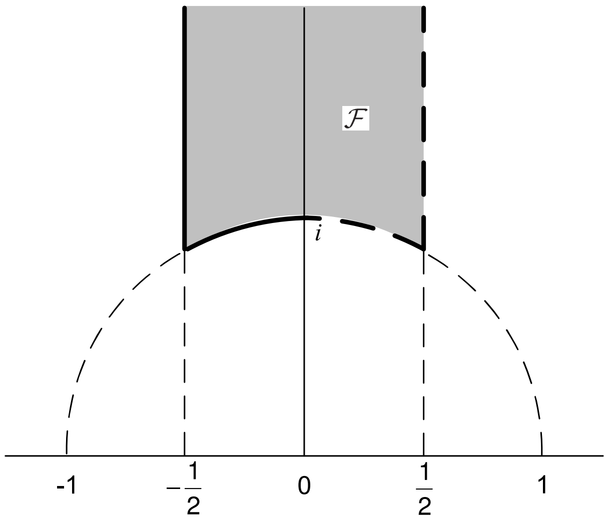


Figure 2.5: Fundamental domain for $SL_2(\mathbb{Z})$

Proposition 2.60. Let $\tau \in \mathcal{H}$ and let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$. Then

$$j\left(\frac{a\tau + b}{c\tau + d}\right) = j(\tau).$$

Definition 2.61 (Fundamental domain for $SL_2(\mathbb{Z})$)**.** Let $\mathcal{F}$ be the subset of $z \in \mathcal{H}$ such that

$$|z| \geqslant 1, \quad -\frac{1}{2} \leqslant \Re(z) < \frac{1}{2}, \quad z \neq e^{i\theta} \text{ for } \frac{\pi}{3} < \theta < \frac{\pi}{2}.$$

Figure 2.5 is the illustration of $\mathcal{F}$.

Proposition 2.62. Given $\tau \in \mathcal{H}$, there exists

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$$

such that

$$\frac{a\tau + b}{c\tau + d} = z \in \mathcal{F}.$$

Moreover, $z \in \mathcal{F}$ is uniquely determined by τ.

Corollary 2.63. If $z \in \mathbb{C}$, then there is exactly one $\tau \in \mathcal{F}$ such that $j(\tau) = z$.

Now we can prove the theorem below.

Theorem 2.64. Let $y^2 = 4x^3 - Ax - B$ be an elliptic curve E over $\mathbb{C}$. Then there exists a lattice L such that

$$g_2(L) = A \quad \text{and} \quad g_3(L) = B.$$

There is an isomorphism of groups

$$\mathbb{C}/L \simeq E(\mathbb{C}).$$

Proof. Recall the j-invariant defined by Definition 2.34, then

$$j(E) = \frac{c_4^3}{\Delta} = 1728\frac{c_4^3 - c_6^2}{c_4^3} = 1728\frac{A^3}{A^3 - 27B^2}.$$

By Corollary 2.63, there exists a lattice $L_\tau = \mathbb{Z} + \mathbb{Z}\tau$ such that $j(\tau) = j(L_\tau) = j$. Consider the following cases:

1. $g_2(L_\tau) \neq 0$

   Then $j(\tau) \neq 0 \Rightarrow A \neq 0$. Choose $\lambda \in \mathbb{C}^*$ such that

   $$g_2(\lambda L_\tau) = \lambda^{-4} g_2(L_\tau) = A.$$

   The equality $j = j(L_\tau)$ implies that

   $$g_3(\lambda L_\tau)^2 = B^2,$$

   so $g_3(\lambda L_\tau) = \pm B$. If $g_3(\lambda L_\tau) = B$, we prove the theorem. If $g_3(\lambda L_\tau) = -B$, then set $\lambda' = i\lambda$

   $$g_2(\lambda' L_\tau) = g_2(i\lambda L_\tau) = i^{-4} g_2(\lambda L_\tau) = A,$$

   $$g_3(\lambda' L_\tau) = g_3(i\lambda L_\tau) = i^{-6} g_3(\lambda L_\tau) = B.$$

Hence, either λL_τ or $i\lambda L_\tau$ would be the lattice isomorphic to E.

2. $g_2(L_\tau) = 0$

   Then $j(\tau) = 0 \Rightarrow A = 0$. According to the assumption that $A^3 - 27B^2 \neq 0$, and $g_2(L_\tau)^3 - 27g_3(L_\tau)^2 \neq 0$ by Proposition 2.52, we have $B \neq 0$ and $g_3(L_\tau) \neq 0$. Choose $\mu \in \mathbb{C}^*$ such that

   $$g_3(\mu L_\tau) = \mu^{-6} g_3(L_\tau) = B.$$

   Then $g_2(\mu L_\tau) = \mu^{-4} g_2(L_\tau) = 0 = A$. The lattice μL is the one we want.

Let the lattice L be the one we get by the above, by Theorem 2.54, the map $\mathbb{C}/L \longrightarrow E(\mathbb{C})$ is an isomorphism. □

Chapter 3

Generate Elliptic Curves

After reveiwing the mathematical backgrounds, we summarize the approaches to generate elliptic curves currently. One of these approaches is based on the efficient point counting algorithm because it can allow us to test random curves until finding a suitable one to use.

3.1 Subfield Curves

We describe the relation of the order of an elliptic curve defined over a finite field $\mathbb{F}_q$ and the one defined over the extesion field $\mathbb{F}_{q^n}$. We prove the thoerem bellow first.

Theorem 3.1. Let $\#E\left(\mathbb{F}_q\right) = q + 1 - t$. Write $X^2 - tX + q = (X - \alpha)(X - \beta)$. Then

$$\#E\left(\mathbb{F}_{q^n}\right) = q^n + 1 - \left(\alpha^n + \beta^n\right),$$

for all $n \geqslant 1$.

Proof. To prove the theorem, we start with showing that $(\alpha^n + \beta^n)$ is an integer.

Lemma 3.2. Let $s_n = (\alpha^n + \beta^n)$. Then $s_0 = 2, s_1 = t$, and $s_{n+1} = ts_n - qs_{n-1}$ for all

$n \geqslant 1$.

Proof. Since α is a root of the equation $f(X) = X^2 - tX + q = (X - \alpha)(X - \beta)$, then $f(\alpha) = (\alpha - \alpha)(\alpha - \beta) = \alpha^2 - t\alpha + q = 0$. By multiplying both side with α^{n-1}, we get $\alpha^{n+1} = t\alpha^n - q\alpha^{n-1}$. This relation holds for β, too. Adding these relations

$$\begin{aligned} \alpha^{n+1} + \beta^{n+1} = s_{n+1} &= t\alpha^n - q\alpha^{n-1} + t\beta^n - q\beta^{n-1} \\ &= t(\alpha^n + \beta^n) - q\left(\alpha^{n-1} + \beta^{n-1}\right) \\ &= ts_n - qs_{n-1}. \end{aligned}$$

For s_0, s_1, t, q are all integers, $s_n = (\alpha^n + \beta^n)$ will be integer for all $n \geqslant 0$. □

Let

$$g(X) = (X^n - \alpha^n)(X^n - \beta^n) = X^{2n} - (\alpha^n + \beta^n)X^n + q^n,$$

for α, β are roots of $g(X)$, we can write $g(X) = Q(X)(X^2 - tX + q)$. Since $g(X)$ and $(X^2 - tX + q)$ are both integer polynomials, the quotient $Q(X)$ would be with integer coefficients. Hence

$$\begin{aligned} g(\phi_q) &= \left(\phi_q^n\right)^2 - (\alpha^n + \beta^n)\phi_q^n + q^n \\ &= (\phi_{q^n})^2 - (\alpha^n + \beta^n)\phi_{q^n} + q^n \\ &= Q(\phi_q)\left(\phi_q^2 - t\phi_q + q\right) = 0 \end{aligned}$$

would be an endomorphism of E. By Theorem 2.47, there is an unique integer k such that $\phi_{q^n}^2 - k\phi_{q^n} + q^n = 0$, and k is determined by $k = q^n + 1 - \#E(\mathbb{F}_{q^n})$. Therefore,

$$\alpha^n + \beta^n = q^n + 1 - \#E(\mathbb{F}_{q^n}).$$

□

According Theorem 3.1, in order to compute the order of an elliptic curve defined over $\mathbb{F}_{q^n}$, we only need to count the points of the curve over a smaller field $\mathbb{F}_q$ instead couting the points over $\mathbb{F}_{q^n}$.

Example 3.3. Assume we want to find out the order of the elliptic curve $E : y^2 + y = x^3 + x$ over $\mathbb{F}_{2^{101}}$.

We start from counting the points of $E(\mathbb{F}_2)$. These points are

$$E(\mathbb{F}_2) = \{\infty, (0,0), (0,1), (1,0), (1,1)\}.$$

We get $\#E(\mathbb{F}_2) = 5$, $t = q + 1 - \#E(\mathbb{F}_2) = 2 + 1 - 5 = -2$, and the relation

$$\begin{aligned} X^2 - tX + q = X^2 + 2X + 2 &= \left(X - \frac{-2 + \sqrt{-4}}{2}\right)\left(X - \frac{-2 - \sqrt{-4}}{2}\right) \\ &= (X - (-1 + i))(X - (-1 - i)). \end{aligned}$$

By Theroem 3.1, we can calculate

$$\begin{aligned} \#E(\mathbb{F}_{2^{101}}) &= 2^{101} + 1 - ((-1 + i)^{101} + (-1 - i)^{101}) \\ &= 2^{101} + 1 - 2^{51} = 2^{101} - 2^{51} + 1. \end{aligned}$$

We also can compute the order by the recursive relation $s_{n+1} = ts_n - qs_{n-1}$

$$\begin{aligned} s_0 &= 2, \quad s_1 = t = -2, \\ s_2 &= ts_1 - qs_0 = -2(s_1 + s_0) = 0, \\ s_3 &= ts_2 - qs_1 = -2(s_2 + s_1) = 4, \\ s_4 &= ts_3 - qs_2 = -2(s_3 + s_2) = -8, \\ &\vdots \\ s_{101} &= 2^{51}, \end{aligned}$$

hence we get the same result, $\#E\left(\mathbb{F}_2^{101}\right) = 2^{101} - 2^{51} + 1$.

The properties of subfield curves let us compute the order of the same elliptic curve equation defined over an extension field. However, the constraint that the coefficients of the equation must be defined over the subfield makes it rarely be used to generate elliptic curves for cryptosystems in practice.

3.2 Schoof's Algorithm and SEA Algorithm

Both Shcoof's algorithm and SEA algorithm are designed to solve the point counting problem on elliptic curve. The point counting problem is to determine the number of the rational points of a randomly chosen elliptic curve over a finite field $\mathbb{F}_q$. To find the suitable elliptic curves, one usually random chooses the parameters of elliptic curve and uses the point counting algorithm to find the order of the elliptic curve. If the curve does not satisfy the requirement, then repeat the process until obtaining an appropriate curve. In this section, we introduce the Schoof's idea first and the improvements proposed by Elkies and Atkin next.

3.2.1 Schoof's Algorithm

We focus on the elliptic curve over prime field $\mathbb{F}_p$. By Hasse theorem, Theorem 2.43, the order of an elliptic curve E defined over $\mathbb{F}_p$ is

$$\#E\left(\mathbb{F}_p\right) = p + 1 - t, \quad |t| \leqslant 2\sqrt{p}$$

where t is called the Frobenius trace. The idea of Schoof is to determine the Frobenius trace t by finding $t_l \equiv t \pmod{l}$ for some small primes and using Chinese Remainder Theorem.

According to the Hasse bound, $|t| \leqslant 2\sqrt{p}$, as long as we compute enough t_l such that $\prod l > 4\sqrt{p}$, then the unique $t \in \left[-2\sqrt{p}, 2\sqrt{p}\right]$ can be determined.

For computing each t_l, we discuss the case $l = 2$ first. For determining $t_2 \equiv t \pmod 2$, observing the order modulo 2

$$
\begin{aligned}
\#E\left(\mathbb{F}_p\right) \pmod 2 &= p + 1 - t \pmod 2 \\
&\equiv t \pmod 2 \equiv t_2, \quad \text{for odd prime field } \mathbb{F}_p.
\end{aligned}
$$

Hence, $t_2 \equiv \#E\left(\mathbb{F}_p\right) \pmod 2$. If there exists a subgroup of order 2, then $t_2 = 0$, otherwise $t_2 = 1$. Since the y-coordinate of the points with order 2 would be 0, if the elliptic curve equation $E : y^2 = x^3 + Ax + B = 0$ has a root in $\mathbb{F}_p$, then $t_2 = 0$. Using the fact that the product of all the irreducible polynomial of degree 1 in $\mathbb{F}_p$ would be $g\left(x\right) = x^p - x$, we can determine t_2 as below

$$
t_2 = \begin{cases} 0 & \text{if } \deg\left(\gcd\left(x^3 + Ax + B, x^p - x\right)\right) > 0 \\ 1 & \text{otherwise} \end{cases}.
$$

Now considering the case that $l > 2$. Since the Frobenius map is a zero map on elliptic curve, for every point $P \in E\left(\overline{\mathbb{F}_p}\right)$

$$
\phi_p^2\left(P\right) - t\phi_p\left(P\right) + pP = \infty.
$$

We can restrict to the non-trivial l-torsion points $P \in E\left[l\right] \setminus \{\infty\}$ to reduce the map

$$
\phi_p^2\left(P\right) - t_l\phi_p\left(P\right) + p_lP = \infty
$$

where $t_l \equiv t \pmod l$ and $p_l \equiv p \pmod l$.

Definition 3.4 (Torsion points). Let E be an elliptic curve over K and $n \in \mathbb{Z}$. The kernel of the multiplication-by-n map, denoted by $E\left[n\right]$, is the set satisfies

$$
E\left[n\right] = \left\{P \in E\left(\overline{K}\right) \middle| nP = \infty\right\}.
$$

An element $P \in E[n]$ is called a n-torsion point.

And we introduce the concept of division polynomial. For each positive integer n, there exists a polynomial ψ_n such that the x-coordinates of n-torsion points are the roots of ψ_n.

Lemma 3.5. Let n be a positive integer. There exists polynomials $\psi_n, \theta_n, \omega_n \in \mathbb{F}_q[x, y]$. For $P = (x, y) \in E\left(\overline{\mathbb{F}_q}\right)$, where $q > 2$ and $nP \neq \infty$,

$$nP = \left(\frac{\theta_n(x, y)}{\psi_n(x, y)^2}, \frac{\omega_n(x, y)}{\psi_n(x, y)^3} \right).$$

Theorem 3.6. Let $P = (x, y) \in E\left(\overline{\mathbb{F}_q}\right)$ where $2P \neq \infty$, and let $n \geqslant 3$ be an odd integer. The division polynomial $\psi_n(x, y)$ can be expressed as $\psi_n(x)$, i.e. ψ_n has no y terms. Then $P \in E[n]$ if and only if $\psi_n(x) = 0$.

Therefore, a point $P = (x_P, y_P) \in E[l]$ would satisfy the equations

$$y_P^2 - x_P^3 - Ax_P - B = 0 \quad \text{and} \quad \psi_l(x_P) = 0$$

When dealing with the l-torsion points, the theorem allows us to reduce the computation modulo the polynomials $\psi_l(x)$ and the elliptic curve equation.

For determing t_l, we then try all $i \in \{0, 1, \cdots, l-1\}$ to find the one that makes

$$\phi_p^2(P) + p_l P = i\phi_p(P)$$

holds modulo $\psi_l(x_P)$ and the elliptic curve equation, where $P = (x_P, y_P) \in E[l]$.

We give the Schoof's algorithm in the following.

Algorithm : Schoof's algorithm

INPUT: An elliptic curve E over a finite field $\mathbb{F}_p$.

OUTPUT: The order of E, $\#E(\mathbb{F}_p)$.

```
find $t_2 \equiv t$ (mod 2), store $(t_2, 2)$
$M \leftarrow 2, \quad l \leftarrow 3$
while $M < 4\sqrt{p}$ do
    find point $P(x, y) \in E[l]$
    compute $Q(X(x, y), Y(x, y)) = \phi_p^2(P) + p_l P$
    compute $Q(X(x, y), Y(x, y)) = \phi_p(P)$
    for $t_l = 0, 1, \cdots, \frac{l-1}{2}$
        if $x$-coordinates of $t_l R$ and $Q$ are equal
            compare $y$-coordinates of $t_l P$ and $Q$
                if the same, store $(t_l, l)$
                else, store $(l - t_l, l)$
            $M \leftarrow M \times l, \quad l \leftarrow$ nextprime$(l)$, and break
compute $t$ by using $(t_l, l)$ pairs and CRT
return $p + 1 - t$
```

3.2.2 SEA Algorithm

Although Schoof proposed the polynomial time point counting algorithm in 1985, it remains inefficient while dealing with curves with large group order. Atkin and Elkies improved the Schoof's work and makes the algorithm, SEA algorithm practical.

The key observation is to consider the roots of the characteristic polynomial of Frobenius map, $x^2 - tx + p$. In Schoof's algorithm, when computing $t_l \equiv t$ (mod l), it separates into two cases:

(1) If there is a root of $x^2 - t_l x + p_l = 0$ in $\mathbb{F}_l$, then l is an Elkies prime.

(2) If there is no root of $x^2 - t_l x + p_l = 0$ in $\mathbb{F}_l$, then l is an Atkin prime.

We briefly list some definitions and properties related to SEA algorithm below.

Definition 3.7 (Classical modular polynomial)**.** Define the classical modular polynomial as below

$$\Phi_l\left(x, j\left(\tau\right)\right) = \left(x - j\left(l\tau\right)\right) \prod_{k=0}^{l-1} \left(x - j\left(\frac{\tau + k}{l}\right)\right).$$

Then $\Phi\left(x, y\right) \in \mathbb{Z}\left[x, y\right]$.

Definition 3.8 (Isogeny)**.** A non-constant morphism ψ which maps the identity element of E_1 to the identity element of E_2 is called an isogeny,

$$\psi : E_1 \longrightarrow E_2.$$

Lemma 3.9. Let E_1, E_2 be two elliptic curves. There is an isogeny of degree l from E_1 to E_2 if and only if $\Phi_l\left(j\left(E_1\right), j\left(E_2\right)\right) = 0$.

Since the coefficients of the classical modular polynomial increase significant while l increases, we usually use the alternative modular polynomial instead. The alternative modular polynomial was proposed by Müller in 1995. Let

$$s = \frac{12}{\gcd\left(12, l-1\right)}, \quad v = \frac{s\left(l-1\right)}{12}, \quad f_l\left(\tau\right) = l^s \left(\frac{\eta\left(l\tau\right)}{\eta\left(\tau\right)}\right)^{2s}$$

where $\eta(\tau)$ is the Dedekind's η-function

$$\eta(\tau) = q^{\frac{1}{24}} \prod_{n=1}^{\infty} (1 - q^n), \quad q = e^{2\pi i \tau}.$$

Definition 3.10. Define the canonical modular polynomial as

$$\Phi_l^c(x, j(\tau)) = (x - f_l(\tau)) \prod_{i=0}^{l-1} \left(x - f_l\left(\frac{-1}{\tau + i} \right) \right).$$

According to [10] we determine the type of the prime by following theorem.

Theorem 3.11. Let E be a non-supersingular elliptic curve over $\mathbb{F}_p$ with j-invariant $j \neq 0, 1728$. For an odd prime l, $\Phi_l(x, j) \in \mathbb{F}_p[x]$ is an univariate polynomial. Then there are three cases of the number of roots of $\Phi_l(x, j)$ on the field $\mathbb{F}_p$

(1) 1 root or $l + 1$ roots.

l is Elkies prime and $t^2 - 4p \equiv 0 \pmod{l}$.

(2) 2 roots.

l is Elkies prime and $t^2 - 4p$ has square roots in $\mathbb{F}_l$.

(3) No root.

l is Atkin prime and all roots would lie in $\mathbb{F}_{p^r}$ for some $r \mid l + 1$.

It can be shown that the splitting type of the canonical modular polynomial $\Phi_l^c(x, j)$ is the same as the splitting type of classical modular polynomial $\Phi_l(x, j)$. Hence, to determine which type the prime l belongs to, we compute the degree of $\gcd(\Phi_l^c(x, j), x^p - x)$. If the degree is larger then 0, l is Elkies prime, otherwise, l is Atkin prime. Following we introduce the Elkies and Atkin's improvements.

Elkies's Improvement

If l is an Elkies prime, according to Theorem 3.11, there exists an isogeny I_1 and elliptic curve E_1 such that

$$I_1 : E \longrightarrow E_1,$$

$$I_1\left(P\left(x,y\right)\right) = \left(\frac{k_1\left(x\right)}{\left(h_1\left(x\right)\right)^2}, \frac{g_1\left(x,y\right)}{\left(h_1\left(x\right)\right)^3}\right) \in E_1, \quad \text{for } P\left(x,y\right) \in E.$$

And the degree of I_1 is l, hence $\left|Ker\left(I_1\right)\right| = l$. By definition of isogeny, $I_1\left(\infty\right) = \infty$, we have $\deg\left(h_1\left(x\right)\right) = \frac{l-1}{2}$. There is a crucial result that I_1 is a homomorphism and the kernel of the isogeny I_1 is a subgroup of E. Moreover, $Ker\left(I_1\right)$ contains a subgroup of $E\left[l\right]$ and

$$\phi\left(P\right) = \lambda P, \quad \text{for } P \in Ker\left(I_1\right),$$

where ϕ is the Frobenius endomorphism and λ is a root of the characteristic polynomial of Frobenius endomorphism over $\mathbb{F}_l$. By relation of roots and coefficients, we have the other root $\mu = p_l/\lambda$ and $t_l \equiv \mu + \lambda$ (mod l).

Using the same concept of Schoof, since the points we deal with are $Ker\left(I_1\right)$, while finding the value $\lambda \in \mathbb{F}_l$ by testing the equality of $\phi\left(P\right)$ and λP, we can take the computation modulo the polynomial $h_1\left(x\right)$. This will improve the efficiency because $\deg\left(h_1\left(x\right)\right) = \frac{l-1}{2}$ is less than $\deg\left(\psi_l\left(x\right)\right) = l^2$, the division polynomial. Following we simply list the process of computing $h_1\left(x\right)$. Refer to [11] for more details of the computation.

Given an elliptic curve $E : y^2 = x^3 + Ax + B$ over field K where $char\left(K\right) > 3$, then such an isogenous curve $E_1 : y^2 = x^3 + \tilde{A}x + \tilde{B}$ and $h_1\left(x\right)$ satisfied the above descriptions can be derived from the root of $\Phi_l^c\left(x,j\right)$, $\Phi_l^c\left(x,y\right)$, and some invariants of E. Let $j = j\left(E\right)$ and a root g of the polynomial $\Phi_l^c\left(x,j\right)$. Set

$$\overline{E}_4 = -\frac{A}{3}, \quad \overline{E}_6 = -\frac{B}{2}, \quad \Delta = \frac{\overline{E}_4^3 - \overline{E}_6^2}{1728},$$

and

$$D_g = g\left(\frac{\partial}{\partial x}\Phi_l^c(x,y)\right)(g,j), \quad D_j = j\left(\frac{\partial}{\partial y}\Phi_l^c(x,y)\right)(g,j).$$

The notation means that the derivatives are to be evaluated at (g,j). By this setting, we denote the invariants of the desired curve to be $\overline{E}_4^{(l)}, \overline{E}_6^{(l)}, \Delta^{(l)}$. Then $\Delta^{(l)} = l^{-12}\Delta g^{12/s}$, where $s = 12/(\gcd(12, l-1))$.

If $D_j = 0$ then

$$\overline{E}_4^{(l)} = l^{-2}\overline{E}_4, \quad j^{(l)} = \frac{\left(\overline{E}_4^{(l)}\right)^3}{\Delta^{(l)}}$$

$$\tilde{A} = -3l^4\overline{E}_4^{(l)}, \quad \tilde{B} = \pm 2l^6\sqrt{\left(j^{(l)} - 1728\right)\Delta^{(l)}}, \quad p_1 = 0.$$

If $D_j \neq 0$, then set

$$\overline{E}_2 = \frac{-12\overline{E}_6 D_j}{s\overline{E}_4 D_g}, \quad \overline{E}_0 = \frac{\overline{E}_6}{\overline{E}_4\overline{E}_2^*}, \quad g' = -\frac{s}{12}\overline{E}_2^* g, \quad j' = -\frac{\overline{E}_4^2\overline{E}_6}{\Delta}.$$

where $\overline{E}_2^* = -12g'/(sg)$. And compute

$$\begin{aligned} D_g' =& g'\left(\frac{\partial}{\partial x}\Phi_l^c(x,y)\right)(g,j) \\ &+ g\left[g'\left(\frac{\partial^2}{\partial x^2}\Phi_l^c(x,y)\right)(g,j) + j'\left(\frac{\partial^2}{\partial x\partial y}\Phi_l^c(x,y)\right)(g,j)\right], \\ D_j' =& j'\left(\frac{\partial}{\partial y}\Phi_l^c(x,y)\right)(g,j) \\ &+ j\left[j'\left(\frac{\partial^2}{\partial y^2}\Phi_l^c(x,y)\right)(g,j) + g'\left(\frac{\partial^2}{\partial x\partial y}\Phi_l^c(x,y)\right)(g,j)\right], \end{aligned}$$

to determine

$$\overline{E}_0' = \frac{1}{D_j}\left(-\frac{s}{12}D_g' - \overline{E}_0 D_j'\right).$$

Then we have

$$\overline{E}_4^{(l)} = \frac{1}{l^2}\left(\overline{E}_4 - \overline{E}_2^*\left[12\frac{\overline{E}_0'}{\overline{E}_0} + 6\frac{\overline{E}_4^2}{\overline{E}_6} - 4\frac{\overline{E}_6}{\overline{E}_4}\right] + \overline{E}_2^{*2}\right), \quad j^{(l)} = \frac{\overline{E}_4^{(l)3}}{\Delta^{(l)}}.$$

Let $f = l^s/g$, $f' = s\overline{E}_2^* f/12$, the other invariant $\overline{E}_6^{(l)}$ is computed as

$$D_g^* = \left(\frac{\partial}{\partial x}\Phi_l^c\left(x,y\right)\right)\left(f, j^{(l)}\right), \quad D_j^* = \left(\frac{\partial}{\partial y}\Phi_l^c\left(x,y\right)\right)\left(f, j^{(l)}\right),$$

then

$$j'^{(l)} = -\frac{f' D_g^*}{l D_j^*}, \quad \overline{E}_6^{(l)} = -\frac{\overline{E}_4^{(l)} j'^{(l)}}{j^{(l)}}.$$

Therefore, we have the parameters of the curve E_1

$$\tilde{A} = -3l^4 \overline{E}_4^{()}, \quad \tilde{B} = -2l^6 \overline{E}_6^{(l)}, \quad p_1 = -\frac{l\overline{E}_2^*}{2}.$$

Now use these values to derive the polynomial $h_1\left(x\right)$. Recall the Weierstrass $\wp$-function of the elliptic curve $E : y^2 = x^3 + Ax + B$

$$\wp\left(z\right) = \frac{1}{z^2} + \sum_{\omega \in L \backslash \{0\}} \left(\frac{1}{\left(z-\omega\right)^2} - \frac{1}{\omega^2}\right) = \frac{1}{z^2} + \sum_{k=1}^{\infty} c_k z^{2k}$$

where

$$c_1 = -\frac{A}{5}, \quad c_2 = -\frac{B}{7},$$

$$c_k = \frac{3}{\left(k-2\right)\left(2k+3\right)} \sum_{j=1}^{k-2} c_j c_{k-1-j}, \text{ for } k \geqslant 3.$$

Let $\wp\left(z\right)$ and $\wp_1\left(z\right)$ denote the Weierstrass $\wp$-function of E and E_1, respectively,

$$\wp\left(z\right) = \frac{1}{z^2} + \sum_{k=1}^{\infty} c_k z^{2k}, \quad \wp_1\left(z\right) = \frac{1}{z^2} + \sum_{k=1}^{\infty} \tilde{c}_k z^{2k}.$$

Then the polynomial $h_1\left(x\right)$ satisfies

$$z^{l-1} h_1\left(\wp\left(z\right)\right) = \exp\left(-\frac{1}{2}p_1 z^2 - \sum_{k=1}^{\infty} \frac{\tilde{c}_k - l c_k}{\left(2k+1\right)\left(2k+2\right)} z^{2k+2}\right).$$

For $h_1\left(x\right)$ is a monic polynomial with degree $\left(l-1\right)/2$, we can derive $h_1\left(x\right)$ by expanding the series and comparing the coefficients of z. We summarize the Elkies procedure in the following.

Algorithm : Elkies procedure

INPUT: An elliptic curve E over a finite field $\mathbb{F}_p$ and an Elkies prime l.

OUTPUT: $t_l \equiv t$ (mod l).

```
compute the polynomial $h_1(x)$
calculate $Q(X(x,y), Y(x,y)) = \phi_p(P)$, where $P \in E$ and satisfies $h_1(x)$
for $\lambda = 0, 1, \cdots, \frac{l-1}{2}$
    if $x$-coordinates of $\lambda P$ and $Q$ are equal
        compare $y$-coordinates of $\lambda P$ and $Q$
            if the same, then $\mu = p_l/\lambda$
            if the sum of $y$-coordinates of $\lambda P$ and $Q$ is $0$, then $\lambda = l - \lambda$,    $\mu = p_l/\lambda$
        break
retuen $\lambda + \mu$ mod $l$
```

Atkin's Improvement

Now considering the case that l is an Atkin prime. From the Theorem 3.11, the equation $x^2 - t_l x + p_l = 0$ has no root in $\mathbb{F}_l$. The two roots will lie on $\mathbb{F}_{l^2}$.

Theorem 3.12. If the roots of $\Phi_l^c(x, j)$ lie on $\mathbb{F}_{p^r}$ for the smallest r, then the roots λ and μ of the equation $x^2 - t_l x + p_l = 0$ satisfy that $\frac{\lambda}{\mu}$ is an element of order exactly r in $\mathbb{F}_{l^2}$

Hence, in the case that l is an Atkin prime, we will get a set of possible value of $t_l \equiv t$ (mod l).

Let the value r of Theprem 3.11 of an Atkin prime l be r_l. It can be determined by computing the degree of $\gcd\left(\Phi_l^c(x,j), x^{q^j}-x\right)$ for increasing $i \mid l+1$. Once r_l determined, we find the set of possible values of t_l next.

Let $\mathbb{F}_{l^2}=\mathbb{F}_l\left(\sqrt{d}\right)$ for a quadratic non-residue $d\in\mathbb{F}_l$. Since $\lambda,\mu\in\mathbb{F}_{l^2}\backslash\mathbb{F}_l$, denote

$$\lambda = x_1 + x_2\sqrt{d}, \quad \mu = x_1 - x_2\sqrt{d}, \quad \text{for some } x_1, x_2 \in \mathbb{F}_l$$

Let $\gamma=\frac{\lambda}{\mu}$. By Theorem 3.12, the order of γ is r_l and we can write

$$\gamma = g_1 + g_2\sqrt{d}, \quad \text{for some } g_1, g_2 \in \mathbb{F}_l.$$

Then

$$\gamma = g_1 + g_2\sqrt{d} = \frac{\lambda}{\mu} = \frac{\lambda^2}{\lambda\mu} = \frac{x_1^2 + x_2^2 d + 2x_1x_2\sqrt{d}}{p_l}.$$

Hence

$$\begin{aligned} p_l g_1 &\equiv x_1^2 + x_2^2 d \pmod{l}, \\ p_l g_2 &\equiv 2x_1x_2 \pmod{l}, \\ p_l &\equiv \lambda \times \mu = x_1^2 - x_2^2 d \pmod{l}. \end{aligned}$$

So we can get a possible value of t_l by

$$t_l = \lambda + \mu \equiv 2x_1 \equiv \sqrt{\frac{p_l\left(g_1+1\right)}{2}}.$$

All the possible values of t_l can then be determined by finding all the elements in $\mathbb{F}_{l^2}$ with order r_l. It can be done by finding a generator g of $\mathbb{F}_{l^2}$ and $\gamma = g^{\frac{i\left(l^2-1\right)}{r_l}}$ for $0<i<r_l$ and $\gcd\left(i,r_l\right)=1$. The Atkin procedure is processed as below.

Algorithm : Atkin procedure

INPUT: An elliptic curve E over a finite field $\mathbb{F}_p$ and an Atkin prime l.

OUTPUT: A set of possible values of $t_l \equiv t$ (mod l).

```
for $r_l = 2, 3, \cdots, l+1$ where $r_l \mid l+1$
    if $\gcd\left(\Phi_l^c(x, j), x^{p^{r_l}} - x\right) \neq 1$
        break
find a quadratic non-residue $d$
find a generator $g$ of $\mathbb{F}_l\left(\sqrt{d}\right)^*$
$S \leftarrow \{\}$
for $i = 1, 2, \cdots, r_l - 1$ and $\gcd(i, r_l) = 1$
    compute $\gamma = g^{\frac{i\left(l^2-1\right)}{r_l}} = g_1 + g_2\sqrt{d}$
    find a square root $x_1$ of $\frac{p_l(g_1+1)}{2}$ in $\mathbb{F}_l$
    store $\{2x_1, -2x_1\}$ in $S$
return $S$
```

3.3 Complex Multiplication Method

The two ways to generate elliptic curve introduced in previous sections select parameters of a curve and then count the rational points on it. These kinds of methods need to test several elliptic curves until getting a desired one satisfied the security constraints. The complex multiplication method (CM method) to be introduced makes us determine the order of the

$\mathbb{F}_q \ \ (q = p^r)$	$t =$ trace (E)	embedding degree k
$12l^2 - 1$	$-1 \pm 6l$	3
$l^2 + l + 1$	$-1, l + 1$	4
$4l^2 + 1$	$1 \pm 2l$	6
$\forall q$	$t \geqslant 3$	$k \geqslant \frac{\log q}{\log(t-1)} - \epsilon$

Table 3.4: Conditions proposed by Miyaji, Nakabayashi, and Takano

curves first and compute the curves with the exact order. Since we explain each step of CM method in next chapter, we use an example to show how the CM method works in this section.

We generate a MNT curve as an example to demonstrate the process. The MNT curves are curves used to construct the pairing-based cryptosystem. These curves satisfy the conditions proposed by Miyaji, Nakabayashi, and Takano. The conditions ensure that the curves will have small embedding degree, which is important when dealing with the pairing computation. Refer to [8] for more details about the MNT curves.

Table 3.4 lists the MNT conditions, suppose we want an elliptic curve E over $\mathbb{F}_p$ with embedding degree $k = 4$. According to the Table 3.4, we have

$$p = l^2 + l + 1, \quad t = l + 1 \text{ or } -l.$$

Take $l = 71$, then

$$p = l^2 + l + 1 = 5113 \in \text{prime number}$$

$$t = l + 1 \text{ or } -l = 72 \text{ or } -71$$

$$\#E\left(\mathbb{F}_p\right) = p + 1 - t = \begin{cases} 5042 = 2 \times 2521 & \text{for } t = 72 \\ 5185 = 5 \times 17 \times 61 & \text{for } t = -71 \end{cases}$$

We use $t = l + 1 = 72$ to make the curve have larger subgroup order. Therefore, let $-D$ denote the discriminant of the endomorphism ring of the elliptic curve we want, i.e. $-D$ is a discriminant of an order of an imaginary quadratic field. Then

$$-D = t^2 - 4p = 72^2 - 4 \times 5113 = -15268.$$

For constructing the Hilbert polynomial, we find out all reduced binary quadratic forms (a, b, c) with discriminant $-D$, it means that searching the triples (a, b, c) satisfies

(1) $b^2 - 4ac = -D$

(2) $|b| \leqslant a \leqslant c$

(3) $b \geqslant 0$ if $a = |b|$ or $a = c$

(4) $\gcd(a, b, c) = 1$

For $-D = -15268$, the triples are:

$$\begin{aligned}(a, b, c) = &(1, 0, 3817), (11, 0, 347), (2, 2, 1909), (23, \pm 2, 166), (46, \pm 2, 83), \\ &(17, \pm 10, 226), (17, \pm 10, 226), (34, \pm 10, 113), (22, 22, 179), (43, \pm 30, 94), \\ &(47, \pm 30, 86), (41, \pm 36, 101), (53, \pm 46, 82).\end{aligned}$$

Let

$$\tau_i = \frac{-b_i + \sqrt{b_i^2 - 4a_i c_i}}{2a_i} = \frac{-b_i + \sqrt{-D}}{2a_i}, \quad \text{for } i = 1, 2, \cdots, 20,$$

compute the Hilbert polynomial $H_D(x)$

$$H_D = \prod_{i=1}^{20} \left(x - j(\tau_i)\right),$$

where

$$j(\tau) = \frac{(256h(\tau) + 1)^3}{h(\tau)}, \quad h(\tau) = \frac{\Delta(2\tau)}{\Delta(\tau)},$$

$$\Delta(\tau) = q\prod_{n=1}^{\infty} (1 - q^n)^{24}, \quad q = e^{2\pi i\tau}.$$

Notice that while computing the Hilbert polynomial, the computations are under complex plane. The fact is the coefficients of the Hilbert polynomial will be integer, hence we must calculate with appropriate precision to approximate the correct coefficients. In this case, the integer polynomial modulo p is

$$\begin{aligned} H_D(x)_P = H_D(x) \pmod{p} = H_D(x) \pmod{5113} \\ = x^{20} - 1384x^{19} - 5068x^{18} + 2897x^{17} + 4303x^{16} + 4515x^{15} + 964x^{14} \\ - 4023x^{13} + 3489x^{12} - 3358x^{11} + 1792x^{10} + 4864x^{9} + 5026x^{8} + 4573x^{7} \\ - 1992x^{6} - 724x^{5} + 1625x^{4} + 636x^{3} + 1264x^{2} + 2625x + 2987. \end{aligned}$$

We can use the Cantor-Zassenhaus algorithm to factor the polynomial and find the roots over $\mathbb{F}_p$. These roots of the $H_D(x)_p$ will be the j-invariants of the desired elliptic curves over $\mathbb{F}_p$. The roots of the polynomial above are

$$\begin{aligned} j_p = & 1186, 50, 2556, 514, 3089, 3535, 3218, 263, 2799, 565, \\ & 2226, 3258, 3859, 1963, 2189, 2841, 2921, 1051, 1542, 2663. \end{aligned}$$

Select $j_p = 1186$ and get the elliptic curve E_1:

$$y^2 = x^3 + \frac{3j_p}{1728 - j_p}x + \frac{2j_p}{1728 - j_p}$$

$$\Rightarrow y^2 = x^3 + \frac{3 \times 1186}{1728 - 1186}x + \frac{2 \times 1186}{1728 - 1186}$$

$$= x^3 + 1365x + 910$$

Using Schoof's algorithm to count the points of the curve E_1 will get the order $\#E_1\left(\mathbb{F}_{5113}\right) = 5186 = 5113 + 1 + 72$. Therefore, the curve with order 5042 we desired is the twist of E_1. For 5 is a quadratic non-residue in $\mathbb{F}_{5113}$, let E_1^t be the quadratic twist of E_1

$$E_1^t : y^2 = x^3 + 1365 \times 5^2 x + 910 \times 5^3$$

$$= x^3 + 3447x + 1264.$$

And the Schoof's algorithm shows that the order $\#E_1^t\left(\mathbb{F}_{5113}\right) = 5042$. So we have

$$p = 5113, \quad t = 72, \quad -D = -15268, \quad j_p = 1186,$$

$$E_1^t : y^2 = x^3 + 3447x + 1264 \pmod{5113}, \quad \#E_1^t\left(\mathbb{F}_{5113}\right) = 5042 = 2 \times 2521$$

and

$$2521 \parallel 5113^4 - 1 = 683444370987360 = 2521 \times 271100504160.$$

The notation "$n \parallel p^k - 1$" denotes $n \mid p^k - 1$ and $n \nmid p^i - 1$ for $1 \leqslant i < k$.

Assume we select another j-invarinat $j_p = 50$, use the same process to find the desired curve and we will get

$$p = 5113, \quad t = 72, \quad -D = -15268, \quad j_p = 50,$$

$$E_2 : y^2 = x^3 + 2389x + 3297, \quad E_2^t : y^2 = x^3 + 3482x + 3085,$$

and

$$\#E_2\left(\mathbb{F}_{5113}\right) = 5186, \quad \#E_2^t\left(\mathbb{F}_{5113}\right) = 5042.$$

We illustrate how the CM method can be used to generate pairing-friendly elliptic curves, next we use another example with larger discriminant $-D$ to show the process for generating elliptic curves with prime order.

Suppose we want an elliptic curve with prime order 101111, then we select a prime $p = 101359$ in Hasse bound. The parameters of the elliptic curve E we desired will be

$$\#E\left(\mathbb{F}_{101359}\right) = 101111, \quad t = 249.$$

Set the input parameters for CM method as below

$$p = 101359, \quad -D = t^2 - 4p = -343435.$$

The CM algorithm will find the reduced binary quadratic forms

$$\begin{aligned}(a,b,c) =& (1,1,85859), (23,\pm 1,3733), (19,\pm 3,4519), (5,5,17173), (13,\pm 5,6605),\\ & (65,\pm 5,1321), (43,\pm 7,1997), (157,\pm 9,547), (17,\pm 13,5053),\\ & (31,\pm 13,2771), (163,\pm 13,527), (61,\pm 19,1409), \cdots,\end{aligned}$$

and the Hilbert polynomial modulo p will be

$$\begin{aligned} H_D\left(x\right)_p = x^{94} &+ 6067x^{93} + 46253x^{92} - 64761x^{91} + 8636x^{90} + 70547x^{89} \\ &+ 100404x^{88} - 77983x^{87} + 85336x^{86} - 80849x^{85} + 80880x^{84} \\ &- 96778x^{83} + 95307x^{82} + 27454x^{81} + 5092x^{80} - 23203x^{79} \\ &+ 13278x^{78} + 89668x^{77} + 69176x^{76} - 48263x^{75} + 48176x^{74} \\ &- 76726x^{73} + 14898x^{72} + 92125x^{71} + 46898x^{70} + 42889x^{69} \\ &+ 64592x^{68} - 19972x^{67} + 82390x^{66} + \cdots . \end{aligned}$$

Therefore, we have 94 roots modulo 101359. Random select $j_p = 59501$, then we have

$$E : y^2 = x^3 + 83394x + 55596, \quad E^t : y^2 = x^3 + 83394x - 55596$$

and

$$\#E\left(\mathbb{F}_{101359}\right) = 101609, \quad \#E^t\left(\mathbb{F}_{101359}\right) = 101111.$$

Therefore, we get the desired elliptic curve $E = E^t$.

Chapter 4

Complex Multiplication for Elliptic Curve

In this chapter, we outline the complex multiplication method (CM method) first, and then describe each step in detail to show how it works.

4.1 Outline of the Complex Multiplication Method

First of all, by the property of the j-invariant of an elliptic curve over finite field $\mathbb{F}_q$, where $Char\left(q\right) > 3$, if we know the j-invariant, we can construct an elliptic curve with this j-invariant.

Let j be the j-invariant and the equation of elliptic curve E be defined as

$$y^2 = x^3 + \frac{3j}{1728 - j}x + \frac{2j}{1728 - j}. \tag{4.1}$$

Then elliptic curve E will be an elliptic curve with $j\left(E\right) = j$.

Now we review the elliptic curves defined over $\mathbb{C}$.

From Section 2.2.3, an elliptic curve $E_{\mathbb{C}}$ defined over $\mathbb{C}$ is isomorphic to $\mathbb{C}/L$, where $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2, \omega_1, \omega_2 \in \mathbb{C}$, and ω_1, ω_2 are linearly independent in $\mathbb{R}$. We can rewrite the lattice L as $L = \mathbb{Z} + \mathbb{Z}\tau$ such that the imaginary part of τ is positive, and we get $j\left(E_{\mathbb{C}}\right) = j\left(\tau\right)$.

Furthermore, the endomorphism ring of $E_{\mathbb{C}}$ will be

$$End\left(E_{\mathbb{C}}\right) \simeq \{\beta \in \mathbb{C} | \beta L \subseteq L\}$$

i.e. corresponds to an ideal A of an order $\mathcal{O}$ in an imaginary quadratic field K. It can be shown that the minimal polynomial of $j\left(E_{\mathbb{C}}\right)$ is the Hilbert class polynomial

$$H_D\left(x\right) = \prod_{i=1}^{h_D} \left(x - j\left(A_i\right)\right)$$

where h_D is the order of the ideal class group of $\mathcal{O}_K$, A_i are representatives of elements of the class group of $\mathcal{O}_K$, and $j\left(A_i\right)$ is the j-invariant of the elliptic curve corresponding to A_i.

By **Deuring's Lifting Theorem**, we can obtain an elliptic curve with complex multiplication over a finite field by reducing an elliptic curve with complex multiplication in characteristic zero.

Theorem 4.1 (Deuring's Lifting Theorem)**.** Let E be an elliptic curve defined over a finite field and let α be an endomorphism of E. Then there exists an elliptic curve $\tilde{E}$ defined over a finite extension K of $\mathbb{Q}$ and an endomorphism $\tilde{\alpha}$ of $\tilde{E}$ such that E is the reduction of $\tilde{E}$ mod some prime ideal of the ring of algebraic integers of K and the reduction of $\tilde{\alpha}$ is α.

The j-invariant of the elliptic curve E over a finite field $\mathbb{F}_p$ reduced from the elliptic curve $E_{\mathbb{C}}$ will be the root of the Hilbert polynomial $H_D\left(x\right)$ (mod p).

The idea of generating elliptic curve with presribed order by CM method is

1. Determine the prime order N of the elliptic curve and the finite field $\mathbb{F}_p$ over that E defined.

   By the order N, it determined the structure of the endomorphism ring $End\left(E\right)$ and the Hilbert class field.

2. Compute the Hilbert polynomial $H_D\left(X\right)$ and find a root j_p of $H_D\left(x\right)_p$ (mod p).

3. Compute the elliptic curve $E/\mathbb{F}_p$ and its twist $E'/\mathbb{F}_p$. Then check which one of E and E' has the order equal to N, and it would be the elliptic curve we want.

According to the idea of the CM method, the algorithm of generating elliptic curves by CM method can be designed as below. Since the Hilbert polynomials can be computed in advance, the algorithm takes the Hilbert polynomials as input.

Algorithm : Construct elliptic curve using CM method

INPUT: A squarefree integer $d \neq 1, 3$, parameters ϵ and δ, Hilbert class polynomial $H_D\left(X\right)$, desired size of p and l.

OUTPUT: A prime p of the desired size, an elliptic curve $E/\mathbb{F}_p$ with $l \mid \#E\left(\mathbb{F}_p\right)$, where l is a large prime.

```
do
    do
        choose prime $p$ of desired size
    until $\epsilon p = x^2 + dy^2$ for some $x, y \in \mathbb{Z}$
    Let $n_1 = p + 1 - \frac{2x}{\delta}$,    $n_2 = p + 1 + \frac{2x}{\delta}$
until $n_1$ or $n_2$ has a large prime factor $l$
```

```
find a root $j_p$ of $H_D(x)$ (mod $p$)
compute the elliptic curve $E_j/\mathbb{F}_p$ by 4.1 and its twist $E_j'/\mathbb{F}_p$
do
    find a point $P \in E_j(\mathbb{F}_p)$ and compute $Q = n_1 P$
    if $Q = \infty$ and $n_2 P \neq \infty$, return $p$ and $E_j$
    else if $Q \neq \infty$, return $p$ and $E_j'$
```

4.2 Endomorphism Ring

In Section 2.1.3, we formulate some definitions related to homomorphism. For studying the details of the CM-method, we start from introducing the endomorphism ring of an elliptic curve.

Definition 4.2 (Endomorphism)**.** Let $\mathcal{A}_1$ and $\mathcal{A}_2$ are abelian varieties over K and $Hom_K(\mathcal{A}_1, \mathcal{A}_2)$ denote the set of homomorphisms from $\mathcal{A}_1$ to $\mathcal{A}_2$. Then the homomorphisms $End_K(\mathcal{A}_1) := Hom_K(\mathcal{A}_1, \mathcal{A}_1)$ are the endomorphisms of $\mathcal{A}_1$.

The set $End_K(\mathcal{A}_1)$ is a ring with composition as multiplicative structure.

Given an elliptic curve E defined over K, we say that the elliptic curve E has **complex multiplication** if the endomorphism ring of E, $End_K(E)$, is strickly larger than $\mathbb{Z}$. We now utilize the elliptic curves defined over $\mathbb{C}$ as examples to illustrate the endomorphism rings, then show that all the elliptic curves defined over finite fields have complex multiplication.

We use the elliptic curve $E : y^2 = 4x^3 - 4x$ defined over $\mathbb{C}$ as example.

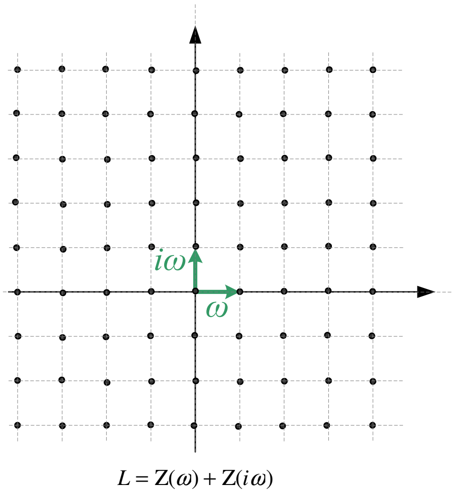


Figure 4.1: Square lattice $L = \mathbb{Z}\omega + \mathbb{Z}i\omega$

As we had proved, we can find a lattice $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ such that $E(\mathbb{C}) \simeq \mathbb{C}/L$. In this case, it can be computed that the lattice L can be written as $L = \mathbb{Z}\omega + \mathbb{Z}i\omega$ for a certain $\omega \in \mathbb{R}$. Figure 4.1 shows an example of this square lattice.

The square lattice was symmetic, i.e. $iL = L$. Considering the endomorphism $\alpha(x) = ix$ acts on the Weierstrass $\wp$-function

$$\begin{aligned}
\wp(iz) &= \frac{1}{(iz)^2} + \sum_{\omega \in L\setminus\{0\}} \left(\frac{1}{(iz-\omega)^2} - \frac{1}{\omega^2} \right) \\
&= \frac{1}{(iz)^2} + \sum_{i\omega \in L\setminus\{0\}} \left(\frac{1}{(iz-i\omega)^2} - \frac{1}{(i\omega)^2} \right) \\
&= -\wp(z), \\
\wp'(iz) &= i\wp'(z).
\end{aligned}$$

Hence, we have the corresponding endomorphism on the elliptic curve E given by

$$i(x,y) = (-x, iy)$$

i.e. we get the the corresponding map of the endomorphism between E and $\mathbb{C}/L$

$$\begin{array}{lrcl} \mathbb{C}/L: & z & \mapsto & iz \\ E(\mathbb{C}): & (x,y)=(\wp(z),\wp'(z)) & \mapsto & (\wp(iz),\wp'(iz))=(-x,iy) \end{array}$$

It shows that given $\alpha=a+bi\in\mathbb{Z}[i]$ and $(x,y)\in E(\mathbb{C})$, where $\mathbb{Z}[i]=\{a+bi|a,b\in\mathbb{Z}\}$, then α would be an endomorphism of E defined by

$$(x,y)\mapsto(a+bi)(x,y)=a(x)+b(-x,iy)$$

since point multiplication by integer a and b can be expressed by rational functions.

Therefore, in this cases,

$$\mathbb{Z}[i]\subseteq End_{\mathbb{C}}(E).$$

Figure 4.2 shows two examples of $End_{\mathbb{C}}(E)$, one is multiplication by integer and the other by i.

Now we deal with the endomorphism rings of the arbitrary elliptic curve over $\mathbb{C}$. We prove the following theorem.

Theorem 4.3. Let E be an elliptic curve defined over $\mathbb{C}$ and L be the lattice such that $E(\mathbb{C})\simeq\mathbb{C}/L$. Then

$$End_{\mathbb{C}}(E)\simeq\{\beta\in\mathbb{C}|\beta L\subseteq L\}.$$

Proof. Let E be an elliptic curve defined over $\mathbb{C}$ and $L=\mathbb{Z}\omega_1+\mathbb{Z}\omega_2$ be the corresponding lattice. To prove the theorem, we need to show the followings:

1. All endomorphisms of $E(\mathbb{C})$ can be expressed by β such that $\beta L\subseteq L$

2. All such β's define endomorphisms of $E(\mathbb{C})$

Here we start the proof.

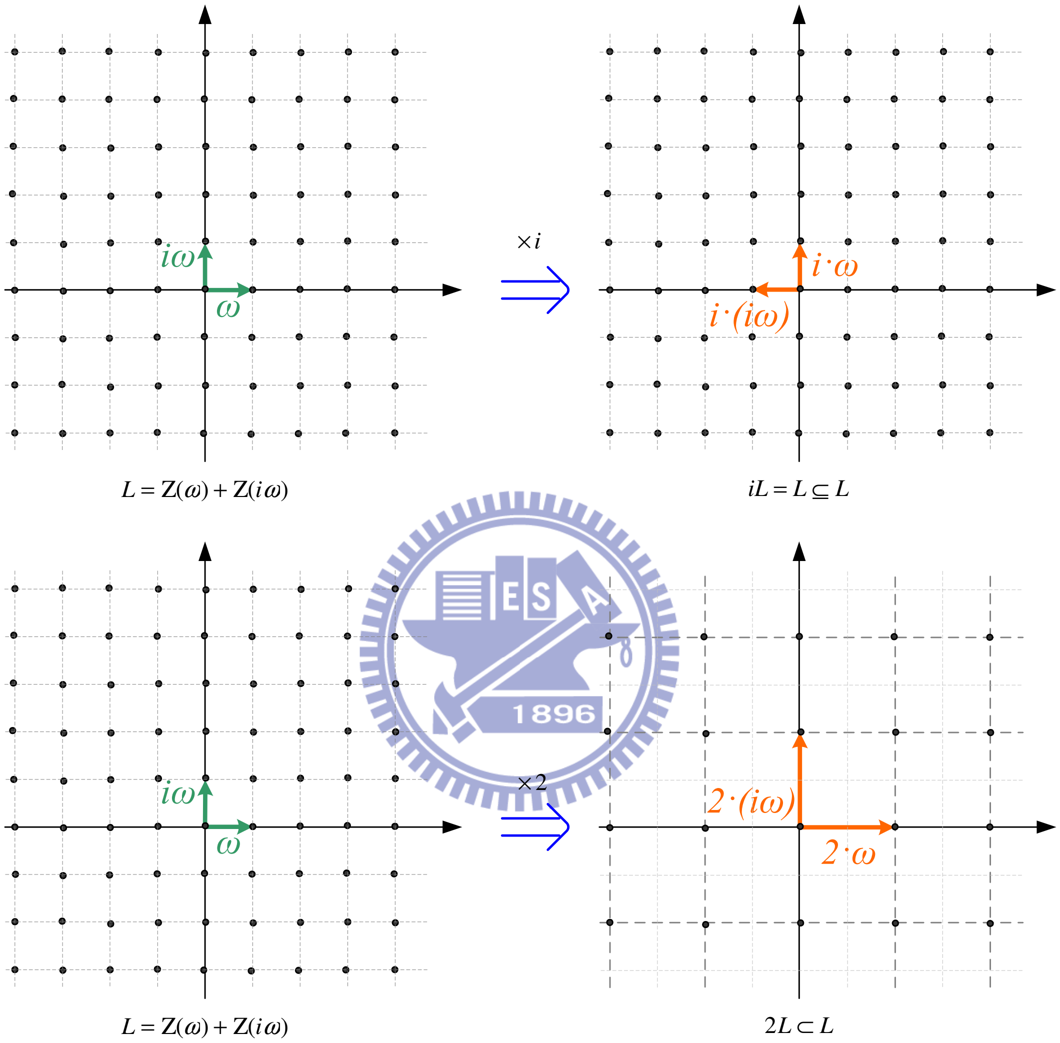


Figure 4.2: Examples of $End_{\mathbb{C}}(E) \simeq \{\beta \in \mathbb{C} | \beta L \subseteq L\}$

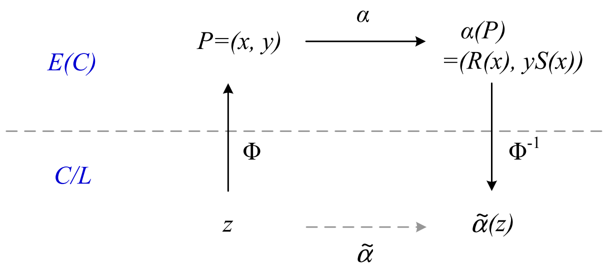


Figure 4.3: The illustration of the morphisms proved of Theorem 4.3 - (1)

1. Given an endomorphism α of $E\left(\mathbb{C}\right)$, by definition of the endomorphism, it maps a point $P = \left(x, y\right) \in E\left(\mathbb{C}\right)$ to $\alpha P = \alpha\left(x, y\right) \in E\left(\mathbb{C}\right)$ and can be expressed by rational functions

$$\alpha\left(x, y\right) = \left(R\left(x\right), yS\left(x\right)\right).$$

Since there exists an isomorphism Φ between $\mathbb{C}/L$ and $E\left(\mathbb{C}\right)$

$$\Phi : \ \mathbb{C}/L \longrightarrow E\left(\mathbb{C}\right), \Phi\left(z\right) = \left(\wp\left(z\right), \wp'\left(z\right)\right),$$

the map

$$\tilde{\alpha} = \Phi^{-1}\left(\alpha\left(\Phi\left(z\right)\right)\right)$$

would be an endomorphism of $\mathbb{C}/L$. Figure 4.3 illustrates the relations of these morphisms.

To show that $\tilde{\alpha}\left(z\right) = \beta z$ for some $\beta \in \mathbb{C}$, we focus on the action of the endomorphism applying on a sufficiently small area U near $z = 0$. Then we obtain the map from U to $\mathbb{C}$ such that

$$\tilde{\alpha}\left(z_1 + z_2\right) \equiv \tilde{\alpha}\left(z_1\right) + \tilde{\alpha}\left(z_2\right) \quad \text{mod } L, \quad \forall z_1, z_2 \in U$$

and we may assume that $\tilde{\alpha}\left(0\right) = 0$. By continuity, $\tilde{\alpha}\left(z\right) \to 0$ when $z \to 0$. If U is sufficiently small, we may assume that

$$\tilde{\alpha}\left(z_1+z_2\right)=\tilde{\alpha}\left(z_1\right)+\tilde{\alpha}\left(z_2\right), \quad \forall z_1, z_2 \in U.$$

Therefore, for $z \in U$,

$$\begin{aligned}
\tilde{\alpha}'(z) &= \lim_{h\to 0}\frac{\tilde{\alpha}(z+h)-\tilde{\alpha}(z)}{h} \\
&= \lim_{h\to 0}\frac{\tilde{\alpha}(z)+\tilde{\alpha}(h)-\tilde{\alpha}(z)}{h} \\
&= \lim_{h\to 0}\frac{\tilde{\alpha}(h)-\tilde{\alpha}(0)}{h} = \tilde{\alpha}'(0).
\end{aligned}$$

Let $\beta=\tilde{\alpha}'(0)$, since $\tilde{\alpha}'(z)=\beta, \forall z \in U$, we have $\tilde{\alpha}(z)=\beta z, \forall z \in U$.

Now let $z \in \mathbb{C}$ be arbitrary. Since there exists an integer n such that $z/n \in U$,

$$\tilde{\alpha}(z) \equiv n\tilde{\alpha}(z/n) = n(\beta z/n) = \beta z \mod L.$$

Hence, the endomorphism $\tilde{\alpha}$ is given by multiplication by β.

For the definition of homomorphsim, $\tilde{\alpha}(L) \subseteq L$, it follows that

$$\beta L \subseteq L.$$

2. Given $\beta \in \mathbb{C}$ satisfies $\beta L \subseteq L$, then multiplication by β is a homomorphism from $\mathbb{C}/L$ to $\mathbb{C}/L$. Therefore, the functions $\wp(\beta z)$ and $\wp'(\beta z)$ are doubly periodic with respect to L. By Theorem 2.50, there exists rational functions R and S such that

$$\wp(\beta z)=R(\wp(z)), \quad \wp'(\beta z)=\wp'(z)S(\wp(z)).$$

Hence, multiplication by β on $\mathbb{C}/L$ corresponds to the map on E:

$$(x,y) \mapsto (R(x), yS(x)).$$

$$\begin{tikzcd}
E(C) & \begin{array}{l} P=(\wp(z),\wp'(z)) \\ \quad =(x,y) \end{array} \arrow[r, dashed, "\alpha"] & \begin{array}{l} P'=(\wp(\beta z),\wp'(\beta z)) \\ \quad =(R(\wp(z)),\wp'(z)S(\wp(z))) \\ \quad =(R(x),yS(x)) \end{array} \\
C/L & z \arrow[u, "\Phi"'] \arrow[r, "\beta"'] & \beta z \arrow[u, "\Phi"']
\end{tikzcd}$$

Figure 4.4: The illustration of the morphisms proved of Theorem 4.3 - (2)

Again, we use Figure 4.4 to show the illustration of the relation between the morphisms proved in this part.

By proving the above, we link the endomorphism ring $End_{\mathbb{C}}(E)$ and the lattice L corresponding to $E(\mathbb{C})$ together. □

Theorem 4.3 shows that the endomorphism ring of an elliptic curve over $\mathbb{C}$ is related closely to the lattice it corresponds to. The next theorem gives us a precise structure of the endomorphism ring, $End_{\mathbb{C}}(E)$.

Theorem 4.4. Let E be an elliptic curve defined over $\mathbb{C}$. Then $End_{\mathbb{C}}(E)$ is isomorphic either to $\mathbb{Z}$ or to an order in an imaginary quadratic field.

Proof. Let $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ be the lattice corresponding to E. By Thoerem 4.3, let

$$R = End_{\mathbb{C}}(E) = \{\beta \in \mathbb{C} | \beta L \subseteq L\}.$$

Then we have $\mathbb{Z} \subset R$ and R is a ring since R is closed under the composition laws $+$ and $\times$.

Given $\beta \in R$, for $\{\omega_1, \omega_2\}$ is a basis of lattice L, then

$$\beta\omega_1 = j\omega_1 + k\omega_2, \quad \beta\omega_2 = m\omega_1 + n\omega_2, \quad j, k, m, n \in \mathbb{Z}$$
$$\Longrightarrow \begin{pmatrix} \beta - j & -k \\ -m & \beta - n \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = 0.$$

So the determinant of the matrix is 0,

$$\beta^2 - (j + n)\,\beta + (jn - km) = 0.$$

Hence, β lies in some quadratic field K and β is an algebraic integer ($\because\ j, k, m, n \in \mathbb{Z}$). We deal with field K in two cases.

1. Assume $\beta \in \mathbb{R}$.

   Then the equation above $\beta\omega_1 = j\omega_1 + k\omega_2$ (or $\beta\omega_2 = m\omega_1 + n\omega_2$) gives a dependence relation between ω_1 and ω_2 with real coefficients:

   $$\begin{aligned} &\beta\omega_1 = j\omega_1 + k\omega_2 &&\Rightarrow &&(\beta - j)\,\omega_1 = k\omega_2 \\ \text{or}\quad &\beta\omega_2 = m\omega_1 + n\omega_2 &&\Rightarrow &&m\omega_1 = (\beta - n)\,\omega_2 \end{aligned}$$

   Since ω_1 and ω_2 are linearly independent over $\mathbb{R}$, we have $\beta = j$ or $\beta = n$, means that $R \cap \mathbb{R} = \mathbb{Z}$.

2. Assume $\beta \in \mathbb{C}$ and $\beta \notin \mathbb{R}$. $\Rightarrow \beta \notin \mathbb{Z}$

   Then β is an algebraic integer in a quadratic field and for $\beta \notin \mathbb{R}$, K must be an imaginary quadratic field, denote K by $\mathbb{Q}\left(\sqrt{-d}\right)$. Let $\beta' \notin \mathbb{Z}$ be another element of R. By the same reason, $\beta' \in K' = \mathbb{Q}\left(\sqrt{-d'}\right)$ for some d'.

Since R is a ring, $\beta + \beta'$ must also be in R, implies that $K = K'$ and $R \subset K$. For all the elements of R are algebraic integers, we have

$$R \subseteq \mathcal{O}_K.$$

Therefore, the endomorphism ring $End_{\mathbb{C}}(E) = R$ is isomorphic either to $\mathbb{Z}$ or an order in an imaginary quadratic field. □

After studying the structure of the endomorphism ring of the elliptic curves defined over $\mathbb{C}$, next we discuss the endomorphism rings of elliptic curves defined over finite field $\mathbb{F}_q$.

Considering the Frobenius endomorphism ϕ_q on an elliptic curve defined over $\mathbb{F}_q$,

$$\phi_q : \begin{cases} E\left(\overline{\mathbb{F}_q}\right) & \longrightarrow & E\left(\overline{\mathbb{F}_q}\right) \\ (x, y) & \longmapsto & (x^q, y^q) \\ \infty & \longmapsto & \infty \end{cases}$$

By Corollary 2.46, the map $\phi_q^2 - t\phi_q + q$ is a zero map on elliptic curve E over $\mathbb{F}_q$, then ϕ_q would be a root of the polynomial

$$X^2 - tX + q = 0.$$

By the Hasse theorem (Theorem 2.43), the unique integer t satisfies $|t| \leqslant 2\sqrt{q}$. It can be shown that if $t = \pm 2\sqrt{q}$, then the endomorphism ring would be an order in a quaternion algebra. For our application and in pratical, we restrict the discussion on the case that $|t| < 2\sqrt{q}$. Since $|t| < 2\sqrt{q}$, the polynomial $X^2 - tX + q = 0$ would have only complex roots, therefore

$$\mathbb{Z} \neq \mathbb{Z}\left[\phi_q\right] \subseteq End\left(E\right).$$

From Theorem 4.4, then the endomorphism ring of an elliptic curve defined over finite field would be an order in an imaginary quadratic field. Observing the polynomial

$$X^2 - tX + q = 0,$$

the roots would lie in the imaginary quadratic field $\mathbb{Q}\left(\sqrt{t^2-4q}\right)$. Hence, for choosing the parameters t and q, we can then determine the imaginary quadratic field $K = \mathbb{Q}\left(\sqrt{-d}\right)$ such that

$$End\,(E) \subseteq \mathcal{O}_K.$$

This is an important result that allows us to choose the desired order first and then find the elliptic curve with the exactly order.

In this section, we link the relation of the order of an elliptic curve and the structure of its endomorphism ring. Following we show how to use the structure to find the desired elliptic curve.

4.3 Ideal Class Group

We have showed that the endormorphism ring of an elliptic curve is isomorphic to $\mathbb{Z}$ or to an order in an imaginary quadratic field in previous section. It can be proved that for an ordinary elliptic curve E defined over $\mathbb{F}_p$, the endomorphism ring $End\,(E)$ is an order in an imaginary quadratic field. To connect the endomorphism ring and the j-invariant of an elliptic curve together, we introduce the ideal class group in this section.

Definition 4.5. Let R be a ring, I is an ideal of R if it is a nonempty subset of R such that

- I is a subgroup of R with respect to the law $+$.

- for all $x \in R$ and all $y \in I$, $xy \in I$ and $yx \in I$.

We summarize some related definitions about ideal below.

- Prime ideal:

  An ideal $I \subsetneq R$ is prime if for all $x, y \in R$ with $xy \in I$, then $x \in I$ or $y \in I$.

- Maximal ideal:

  An ideal $I \subsetneq R$ is maximal if for any ideal J of R the inclusion $I \subset J$ implies $J = I$ or $J = R$.

- Finitely generated:

  An ideal I of a ring R is finitely generated if there are elements $a_1, \cdots, a_n$ such that every $x \in I$, we can write $x = x_1a_1 + \cdots + x_na_n$ with $x_1, \cdots, x_n \in R$.

- Principal ideal:

  An ideal I is principal if $I = aR$. And R is a principal ideal domain (PID) if it is an integral domain and if every ideal of R is principal.

Definition 4.6 (Fractional ideal)**.** Let K be a number field and let an order $\mathcal{O}$ be a Dedekind ring. A fractional ideal of K is a submodule of K over $\mathcal{O}$.

The Dedekind ring is defined as:

Definition 4.7 (Dedekind ring)**.** A Dedekind ring R is an integral domain satisfying the following properties.

(1) Every ideal of R is finitely generated.

(2) Every nonzero prime ideal of R is maximal.

(3) R is integrally closed in its quotient field

$$F = \{\alpha/\beta : \alpha, \beta \in R, \beta \neq 0\}.$$

From the definition, for a fractional ideal M of R, we have $\alpha M \subseteq R$ and αM is an integral ideal of R for some nonzero $\alpha \in R$. Hence for any fractional ideal of R, it can be expressed in the form $\alpha^{-1} I$, where I is an integral ideal of R.

Now we state the following lemma:

Lemma 4.8 (Group of fractional ideals)**.** If R is a Dedekind ring, then the set of all fractional ideals forms a multiplicative abelian group, denoted by $\mathfrak{F}(R)$. The set $\mathcal{P}(R)$ consisting of all principal fractional ideals of R is a subgroup of $\mathfrak{F}(R)$.

Then we can define the class group of an integral ring R.

Definition 4.9 (Class group)**.** Let R be a Dedekind ring. Then the quotient group $\mathfrak{F}(R)/\mathcal{P}(R)$ is called the class group of R, denoted by $\mathfrak{C}_R$. When $R = \mathcal{O}_K$, we write $\mathfrak{C}_K$.
We say that two fractional ideals are equivalent if they belong to the same coset of $\mathcal{P}(R)$ in $\mathfrak{F}(R)$. In other words, fractional ideals I, J are equivalent, denoted by $I \sim J$, provided that $\psi(I) = \psi(J)$ under the natural map $\psi : \mathfrak{F}(R) \mapsto \mathfrak{F}(R)/\mathcal{P}(R)$.

The cardinality of the class group $|\mathfrak{C}_K|$ is called the class number of $\mathcal{O}_K$, denoted by h_K. It can be proved that h_K is finite.

In our case, for an elliptic curve E, the endomorphism ring $End(E)$ will be an order R in an imaginary quadratic field $\mathbb{Q}\left(\sqrt{-d}\right)$. Let A_i be the representative of each equivalent class of $\mathfrak{C}_R$, then $j(A_i)$ are conjugates under the action of the Galois group of the ring class field over $\mathbb{Q}\left(\sqrt{-d}\right)$. And we will get the polynomial

$$H_D(x) = \prod_{i=1}^{h_D} (x - j(A_i))$$

is the Hilbert class polynomial. This will also be mentioned in the following sections.

4.4 j-invariant

We review the mathematical background related to j-invariant and link it to the CM-method in this section.

Recall that the definition of j-invariant is defined as a function of a complex number τ on the upper half plane of complex numbers. In Definition 2.59,

$$j(\tau) = 1728\frac{g_2^3}{\Delta} = 1728\frac{g_2^3}{g_2^3 - 27g_3^2}$$

Given a matrix $M \in SL_2(\mathbb{Z})$, the action on the upper half plane is

$$M\tau = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\tau + b}{c\tau + d}, \quad \forall \tau \in \mathcal{H}$$

We now proved Proposition 2.60:

Let $\tau \in \mathcal{H}$ and let matrix $M \in SL_2(\mathbb{Z})$, then

$$j(M\tau) = j\left(\frac{a\tau + b}{c\tau + d}\right) = j(\tau).$$

Proof. From the difinition of $j(\tau)$

$$j(\tau) = 1728\frac{g_2^3}{g_2^3 - 27g_3^2},$$

where

$$g_2 = g_2(\tau) = g_2(L_\tau) = 60G_4(L_\tau)$$

$$g_3 = g_3(\tau) = g_3(L_\tau) = 140G_6(L_\tau)$$

Observing the series $G_k\left(L_\tau\right) = G_k\left(\tau\right)$:

$$G_k\left(\tau\right) = \sum_{(m,n)\neq(0,0)} \frac{1}{\left(m\tau+n\right)^k}$$

$$\begin{aligned}
G_k\left(\frac{a\tau+b}{c\tau+d}\right) &= \sum_{(m,n)\neq(0,0)} \frac{1}{\left(m\left(\frac{a\tau+b}{c\tau+d}\right)+n\right)^k} \\
&= \left(c\tau+d\right)^k \sum_{(m,n)\neq(0,0)} \frac{1}{\left(m\left(a\tau+b\right)+n\left(c\tau+d\right)\right)^k} \\
&= \left(c\tau+d\right)^k \sum_{(m,n)\neq(0,0)} \frac{1}{\left(\left(ma+nc\right)\tau+\left(mb+nd\right)\right)^k}.
\end{aligned}$$

Since $\det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = 1$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix},$$

for

$$\left(m',n'\right) = \left(ma+nc, mb+nd\right) = \left(m,n\right)\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

we have

$$\left(m,n\right) = \left(m',n'\right)\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Hence there is a one-to-one mapping between $\left(m,n\right)$ and $\left(m',n'\right)$, so we can write

$$\begin{aligned}
G_k\left(\frac{a\tau+b}{c\tau+d}\right) &= \left(c\tau+d\right)^k \sum_{(m,n)\neq(0,0)} \frac{1}{\left(\left(ma+nc\right)\tau+\left(mb+nd\right)\right)^k} \\
&= \left(c\tau+d\right)^k \sum_{(m',n')\neq(0,0)} \frac{1}{\left(m'\tau+n'\right)^k} \\
&= \left(c\tau+d\right)^k G_k\left(\tau\right).
\end{aligned}$$

Therefore

$$g_2\left(\frac{a\tau+b}{c\tau+d}\right)=(c\tau+d)^4\,g_2(\tau)\,,\quad g_3\left(\frac{a\tau+b}{c\tau+d}\right)=(c\tau+d)^6\,g_3(\tau)$$

Put these terms into the definition of j, it follows that

$$\begin{aligned}j\left(\frac{a\tau+b}{c\tau+d}\right)&=1728\frac{g_2\left(\frac{a\tau+b}{c\tau+d}\right)^3}{g_2\left(\frac{a\tau+b}{c\tau+d}\right)^3-27g_3\left(\frac{a\tau+b}{c\tau+d}\right)^2}\\&=1728\frac{(c\tau+d)^{12}\,g_2(\tau)^3}{(c\tau+d)^{12}\left(g_2(\tau)^3-27g_3(\tau)^2\right)}\\&=j(\tau)\,.\end{aligned}$$

□

Hence, the j-function is a modular function. By the action on two special matrices in $SL_2(\mathbb{Z})$

$$M_1=\begin{pmatrix}1&1\\0&1\end{pmatrix},\quad M_2=\begin{pmatrix}0&-1\\1&0\end{pmatrix},$$

we have

$$j(\tau+1)=j(\tau)\,,\quad j\left(-\frac{1}{\tau}\right)=j(\tau)\,.$$

These two transformations generate a modular group and play important roles in proving Corollary 2.63:

If $z\in\mathbb{C}$, then there is exactly one $\tau\in\mathcal{F}$ such that $j(\tau)=z$.

It means that given a specific value z, we can find τ' such that

$$j(\tau')=z,$$

and for Proposition 2.60 and Proposition 2.62, by choosing appropriate $M\in SL_2(\mathbb{Z})$, we can find a transformation belonging to the modular group to find a unique τ in the fundamental domain such that

$$j(\tau) = j(M\tau') = j(\tau') = z, \quad \tau \in \mathcal{F}.$$

Hence, j-function is a one-to-one mapping from the fundamental domain to the entire complex plane. Since each value of j corresponds to the field of elliptic functions with periods 1 and τ, j-function is in a one-to-one relationship with isomorphism classes of elliptic curves.

Now we conclude the material discussed as below:

Theorem 4.10. Assume that E is defined over $\mathbb{C}$ and has complex multiplication. Let τ be its period. Then $\mathbb{Q}(\tau)$ is an imaginary quadratic field, $End_{\mathbb{Q}(\tau)}(E) = End_{\mathbb{C}}(E)$ is an order $\mathcal{O}_E$ in $\mathbb{Q}_\tau$ and the absolute invariant $j(\tau)$ is an algebraic integer that lies in the ring class field $H_{\mathcal{O}_E}$ over $\mathbb{Q}(\tau)$.

For our case, the $\mathcal{O}_E$ is the ring of integers of $\mathbb{Q}_\tau$. Then $H_{\mathcal{O}_E}$ is the Hilbert class field H of $\mathbb{Q}_\tau$. And there exists a monic polynomial with integer coefficients whose roots would be the j-invariants of the isomorphism classes of the elliptic curves. The monic integer polynomial, i.e. the minimal polynomial of the j-invariant, is the Hilbert class polynomial

$$H_D(x) = \prod_{i=1}^{h_D} (x - j(\tau_i)),$$

where d is the squarefree integer such that $\tau_i \in \mathbb{Q}\left(\sqrt{d}\right)$, h_D is the Hilbert class number, τ_i are the representatives of the elements of the class group of $\mathcal{O}_K$, and $j(\tau_i)$ are the j-invariants of corresponding τ_i value.

By Theorem 2.64, for an elliptic curve E over $\mathbb{C}$, there is a lattice L_τ such that $E(\mathbb{C}) \simeq \mathbb{C}/L_\tau$ and $j(E) = j(L_\tau) = j(\tau)$. Therefore, the j-invariants in above polynomial would be the j-invariants of the elliptic curve corresponding to τ_i. Since we have showed that j-function is a function that maps the fundamental domain $\mathcal{F}$ to entire complex plane, we can focus on the τ's in $\mathcal{F}$ for computing the Hilbert polynomial.

4.5 Hilbert Polynomial

To connect the elliptic curves over number fields and elliptic curves over finite field, we discuss the properties of Hilbert polynomial.

According to Theorem 4.10, restate the description of Hilbert polynomial first:

Corollary 4.11. Let $K = \mathbb{Q}\left(\sqrt{-d}\right)$ be an imaginary quadratic field with ring of integers $\mathcal{O}_K$. Let E be an elliptic curve with $End_{\mathbb{C}}(E) = \mathcal{O}_K$. Then the minimal polynomial of j_E is the Hilbert class polynomial

$$H_D(x) = \prod_{r=1}^{h_D} (x - j(\tau_i)),$$

where $j(\tau_i)$ is the j-invariant of the elliptic curve corresponding to τ_i, h_D is the Hilbert class number, and τ_i are representatives of the elements of the class group of $\mathcal{O}_K$.

We know that for a j-invariant $j(\tau)$, the minimal polynomial of $j(\tau)$ is the Hilbert polynomial. Since it can be proved that j-invariant is an algebraic integer, the Hilbert polynomial has integer coefficients. Therefore, by taking all the integer coefficients modulo a prime p, the Hilbert polynomial can be reduced to a polynomial $H_D(x)_p$ over $\mathbb{F}_p$.

$$\begin{aligned} H_D(x)_p &= \prod_{r=1}^{h_D} (x - j(\tau_i)) \pmod p \\ &= x^{h_D} + a_{h_D-1}x^{h_D-1} + \cdots + a_1 x + a_0, \end{aligned}$$

where $a_i \in \mathbb{F}_p$. Futhermore, if p does not divides d, the polynomial $H_D(x)_p$ would have simple roots in $\mathbb{F}_p$.

Let j_p be a root of the polynomial $H_D(x)_p$, then it is the reduction modulo p of one of the j-invariants $j(\tau_i)$. If j_p is contained in $\mathbb{F}_{p^k}$, for the $j(\tau_i)$ are conjugate, all the roots of $H_D(x)_p$ would be in $\mathbb{F}_{p^k}$.

As mentioned in beginning, if we have the j-invariant $j_p \in \mathbb{F}_p, j_p \neq 0, 1728$, then we can find the elliptic curve over $\mathbb{F}_p$ with invariant j_p by

$$y^2 = x^3 + \frac{3j_p}{1728 - j_p}x + \frac{2j_p}{1728 - j_p}.$$

Computing the Hilbert Polynomial

In order to find a root of Hilbert polynomial modulo p, we need to compute Hilbert polynomial first. For computing the polynomial, it needs to find all the τ_i's. Recall that each τ_i represents an element of the ideal class group of $\mathcal{O}_K$, we use the equivalence between the ideal classes of an algebraic number field with discriminant d and the equivalence classes of primitive, positive definite binary quadratic forms of discriminant d to find all τ_i's.

A binary quadratic form is a quadratic form in two variables. In the case of the ideal class group of function fields, it can be proved that there is exactly one reduced binary quadratic form in each equivalence class. The reduced binary quadratic form is defined as:

Definition 4.12. A quadratic form $ax^2 + bxy + cy^2$ is called a reduced binary quadratic form if it satisfies

- $|b| \leqslant a \leqslant c$
- $b \geqslant 0$ if $a = |b|$ or $a = c$
- $\gcd(a, b, c) = 1.$

Therefore, we search for all reduced binary quadratic forms of discriminant d to obtain all τ_i's. For each reduced binary quadratic form $ax^2 + bxy + cy^2$, it corresponds to the ideal $A = \mathbb{Z} + \mathbb{Z}\tau$ where

$$\tau = \frac{b + \sqrt{-d}}{2a}.$$

On the other hand, the conditions of the redeuced binary quadratic form make the corresponding τ belonging to the fundamental domain $\mathcal{F}$. Given a τ_i, one can compute $j(\tau_i)$ by following

Definition 4.13 (Dedekind's η-function)**.** Let τ be a complex number with positive imaginary part, i.e. $\tau \in \mathcal{H}$, define $q = e^{2\pi i \tau}$ and the η-function by

$$\eta(\tau) = q^{\frac{1}{24}} \prod_{n=1}^{\infty} (1 - q^n) = q^{\frac{1}{24}} \left(1 + \sum_{n \geqslant 1} (-1)^n \left(q^{n(3n-1)/2} + q^{n(3n+1)/2} \right) \right).$$

Let

$$\Delta(\tau) = \eta(\tau)^{24} = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = q \left(1 + \sum_{n \geqslant 1} (-1)^n \left(q^{n(3n-1)/2} + q^{n(3n+1)/2} \right) \right)^{24}$$

The $j(\tau)$ is related to $\Delta(\tau)$ by

$$h(\tau) = \frac{\Delta(2\tau)}{\Delta(\tau)}, \quad j(\tau) = \frac{(256h(\tau) + 1)^3}{h(\tau)}.$$

Since the computations are over $\mathbb{C}$, the results would be the approximate value for $j(\tau_i)$. By the fact that the coefficients of the Hilbert polynomial are all integers, we can obtain the actual polynomial by using sufficient precision.

4.6 Weber Polynomial

Since the coefficients of the Hilbert polynomial grow fast when the degree of the polynomial increases, the computation of the Hilbert polynomial was suggested to be taken in advance.

Another solution is to use other class invariant instead of j-invariant. Different class invariant leads different class polynomial. The Weber polynomial is used most. The Weber functions are defined as following, using the Dedekind's η-function (see Definition 4.13),

$$f(\tau) = \zeta_{48}^{-1}\frac{\eta((\tau+1)/2)}{\eta(\tau)}, \quad f_1(\tau) = \frac{\eta(\tau/2)}{\eta(\tau)}, \quad f_2(\tau) = \sqrt{2}\frac{\eta(2\tau)}{\eta(\tau)},$$

where $\zeta_n = e^{\frac{2\pi i}{n}}$, and

$$\gamma_2(\tau) = \frac{f(\tau)^{24} - 16}{f(\tau)^8}, \quad \gamma_3(\tau) = \frac{\left(f(\tau)^{24}+8\right)\left(f_1(\tau)^8 - f_2(\tau)^8\right)}{f(\tau)^8}.$$

For more details, refer to [2], [15]. The relation of these functions and the j-function are

$$\begin{aligned} j(\tau) &= \frac{\left(f(\tau)^{24}-16\right)^3}{f(\tau)^{24}} = \frac{\left(f_1(\tau)^{24}+16\right)^3}{f_1(\tau)^{24}} = \frac{\left(f_2(\tau)^{24}+16\right)^3}{f_2(\tau)^{24}} \\ &= \gamma_2(\tau)^3 = \gamma_3(\tau)^2 + 1728. \end{aligned}$$

Then the Weber polynomial $W_D(x)$ is defined as

$$W_D(x) = \prod_{i=1}^{h'}(x - \mu(\tau_i))$$

Atkin and Morain suggest a list of the choice $\mu(\tau_i)$ for different discriminant D in [2]:

- If $D \equiv 3 \pmod 6$, use $\mu(\tau) = \sqrt{-D}\gamma_3(\tau)$.
- If $D \equiv 7 \pmod 8$, use $\mu(\tau) = f(\tau)/\sqrt{2}$.
- If $D \equiv 3 \pmod 8$, use $\mu(\tau) = f(\tau)$.
- If $d \equiv \pm 2 \pmod 8$, use $\mu(\tau) = f_1(\tau)/\sqrt{2}$.
- If $d \equiv 5 \pmod 8$, use $\mu(\tau) = f(\tau)^4$.
- If $d \equiv 1 \pmod 8$, use $\mu(\tau) = f(\tau)^2/\sqrt{2}$.

where

$$d = \begin{cases} D, & \text{if } D \equiv 3 \pmod 4 \\ D/4, & \text{if } D \equiv 0 \pmod 4 \end{cases}$$

In the case when $D \equiv 3 \pmod 8$ and $D \not\equiv 3 \pmod 6$, the degree of Weber polynomial will be $3h_D$, h_D denotes the degree of the Hilbert polynomial. Therefore, it usually avoid to choose these values for D in practice.

4.7 Finding Roots of Polynomial over $\mathbb{F}_p$

After computing the Hilbert polynomial, next we want to find a root j_p in the finite field $\mathbb{F}_p$ to construct the corresponding elliptic curve. Before finding a root of the Hilbert polynomial modulo p, some criteria need to be satisfied when choosing the prime field p.

Assume the prime number p is decomposed in $\mathbb{Q}\left(\sqrt{-d}\right)$, by the class field theory of imaginary quadratic fields, we have following theorem.

Theorem 4.14. There is an integer $\pi \in \mathbb{Q}\left(\sqrt{-d}\right)$ such that $\pi\overline{\pi} = p$ and $|p + 1 - (\pi + \overline{\pi})|$ equals to $\#E\left(\mathbb{F}_p\right)$ or its twists.

From the theorem above, we have $\pi\overline{\pi} = p$ and $\pi + \overline{\pi} = \#E\left(\mathbb{F}_p\right) - (p + 1) = t$, then the minimal polynomial of π would be

$$x^2 - tx + p.$$

Recall the characteristic polynomial of Frobenius map ϕ_p

$$\phi_p^2 - t\phi_p + p,$$

where t is called the Frobenius trace. We can observe that in Theorem 4.14, the algebraic integer π is actually the Frobenius endomorphism acting on E_p or its twist modulo p.

Hence, we need to choose p which can be decomposed in $\mathcal{O}_K$. These primes would be the ones such that there are integer solutions to the norm equation

$$x^2 + dy^2 = \epsilon p, \quad \text{where } \epsilon = \begin{cases} 1 & \text{if } d \equiv 1, 2 \pmod 4 \\ 4 & \text{if } d \equiv 3 \pmod 4 \end{cases}.$$

From the equation above, we obtain that $-d$ must be a square modulo p. To find such a suitable prime p, one usually uses the Cornacchia's algorithm to get a solution.

Algorithm : Cornacchia's algorithm

INPUT: A squarefree integer $d > 0$ and a prime p such that the Legendre symbol $\left(\frac{-d}{p}\right) = 1$.

OUTPUT: $(x, y) \in \mathbb{Z}^2$ such that $x^2 + dy^2 = p$ if possible.

```
compute square root $a_0$ of $-d$ with $p/2 < a_0 < p$, i.e. $a_0^2 \equiv -d \pmod p$
$a \leftarrow p, \quad b \leftarrow a_0, \quad c \leftarrow \lfloor \sqrt{p} \rfloor$
while $b > c$ do
    $r \leftarrow a \pmod b, \quad a \leftarrow b, \quad b \leftarrow r$
if $d \nmid p - b^2$ or if $z = (p - b^2)/d$ is not a square, return ”no solution”
else return $(x, y) = (b, \sqrt{z})$
```

Choosing the prime p by the Cornacchia's algorithm, now we can factor the Hilbert polynomial in $\mathbb{F}_p$ to find roots $j_p \in \mathbb{F}_p$. We introduce the general way to find roots of a polynomial, then discuss the method to find roots of Hilbert polynomial.

For finding roots of a polynomial $f(x)$, it usually needs to make the polynomial squarefree first. Due to the characteristic of the field we deal with, we discuss this step in two cases.

(1) If the characteristic of the field is 0.

We can obtain the squarefree version of the polynomial $f(x)$ by computing

$$\frac{f(x)}{\gcd(f(x), f'(x))}.$$

(2) If the characteristic of the field is p.

Since a polynomial $f(x)$ satisfies $f'(x) = 0$ precisely when $f(x) = w(x)^p$ for some polynomial $w(x)$, we write $f(x) = v(x)\, w(x)^p$ (if $\deg(f(x)) < p$, then $w(x) = 1$). Then use the same process to deal with the $v(x)$.

After reducing the square part of the polynomial, we factor the polynomial such that

$$f(x) = f_1(x)\, f_2(x) \cdots f_m(x)$$

where $f_i(x)$ is the product of irreducible polynomials with degree i. For each $f_i(x)$, applying the Cantor-Zassenhaus algorithm to find individual factors. The Cantor-Zassenhaus algorithm can factor the polynomial with all irreducible factors having the same degree.

Focus on finding roots of reduced Hilbert polynomial modulo p, since $\deg\left(H_D(x)_p\right) < p$, reducing the square part can be done by computing $\frac{H_D(x)_p}{\gcd\left(H_D(x)_p, H'_D(x)_p\right)}$. For the roots we interest are those lie in ground field $\mathbb{F}_p$, we only process the polynomial $f_1(x)$, i.e. the product of the irreducible polynomials with degree 1.

We also can use the fact that $g(x) = x^p - x$ is the product of all irreducible polynomial of degree 1 in $\mathbb{F}_p$. The polynomial $f_1(x)$ then can be obtained by computing

$$f_1(x) = \gcd\left(H_D(x)_p, g(x)\right).$$

Finally, using the Cantor-Zassenhaus algorithm to find the roots in $\mathbb{F}_p$.

Algorithm : Cantor-Zassenhaus algorithm

INPUT: A polynomial $f(x)$ with all irreducible factors having the same degree. Assume $\deg(f(x)) = n$.

OUTPUT: All the factors of $f(x)$.

```
repeat
    select a random polynomial $r(x)$ with degree less than $n$
    if $\gcd(r(x), f(x)) \neq 1$, then return $r(x)$
    compute $s(x) = r(x)^{(p-1)/2} \pmod{f(x)}$
        then $\gcd(s(x) + 1, f(x))$ is a factor with probability $1 - 2^{-(n-1)}$
until factor $f(x)$ successful
```

4.8 Twist Curves

After finding the roots of the Hilbert polynomial (or transforming the roots of the Weber polynomial) in the finite field $\mathbb{F}_p$, we can compute the equations of the elliptic curves with the prescribed order by taking the roots as j-invariants of the curves. Since we set the discriminant $-D = t^2 - 4p$, the order of the curve we get might be

$$\#E(\mathbb{F}_p) = p + 1 - t \quad \text{or} \quad \#\tilde{E}(\mathbb{F}_p) = p + 1 + t.$$

The elliptic curve $\tilde{E}$ is called a twist of E. Here we introduce the twist curves.

Lemma 4.15. Let E be an elliptic curve defined over K. Assume the characteristic of K is prime to 6 and E is given by the simplified Weierstrass equation

$$E : y^2 = x^3 + Ax + B.$$

The j-invariant j_E depends only on the isomorphism class of E.

- $j_E = 0$ if and only if $A = 0$.
- $j_E = 1728$ if and only if $B = 0$.
- If $j_E \in K$ is not equal to $0, 1728$, then E is a quadratic twist of the elliptic curve

$$\tilde{E}_{j_E} : y^2 = x^3 + \frac{3j_E}{1728 - j_E}x + \frac{2j_E}{1728 - j_E}.$$

Corollary 4.16. Let E be an elliptic curve defined over K. Assume the characteristic of K is prime to 6 and E is given by the simplified Weierstrass equation

$$E : y^2 = x^3 + Ax + B.$$

- If $A = 0$, then for every $B' \in K^*$ the curve E is isomorphic to

$$E' : y^2 = x^3 + B' \quad \text{over} \quad K\left(\left(\frac{B}{B'}\right)^{1/6}\right).$$

- If $B = 0$, then for every $A' \in K^*$ the curve E is isomorphic to

$$E' : y^2 = x^3 + A'x \quad \text{over} \quad K\left(\left(\frac{A}{A'}\right)^{1/4}\right).$$

- If $AB \neq 0$, then for every $v \in K^*$ the curve E is isomorphic to

$$\tilde{E}_v : y^2 = x^3 + A'x + B' \quad \text{with} \quad A' = v^2 A,\ B' = v^3 B \quad \text{over} \quad K\left(\sqrt{v}\right).$$

The curves occuring in the Corollary above are called twist of E. In the last case, the curves $\tilde{E}_v$ are called quadratic twists of E. Note that E is isomorphic to $\tilde{E}_v$ over K if and only if v is a square in K^*.

In Corollary 4.16, by taking $v \in K^*$ a quadratic nonresidue, one can define the quadratic twist of E as

$$\tilde{E}_v : vy^2 = x^3 + Ax + B$$

by dividing by v^3 and transforming $y \mapsto y/v$ and $x \mapsto x/v$. Then it can be seen that both E and $\tilde{E}_v$ contain exactly two points (x, y_i) for each $x \in \mathbb{F}_p$. Hence we have the following proposition.

Proposition 4.17. Let E be a curve defined over $\mathbb{F}_p$ and let $\tilde{E}$ be the quadratic twist of E. Then

$$\#E\left(\mathbb{F}_p\right) + \#\tilde{E}\left(\mathbb{F}_p\right) = 2p + 2.$$

Hence, if $\#E\left(\mathbb{F}_p\right) = p + 1 - t$ then $\#\tilde{E}\left(\mathbb{F}_p\right) = p + 1 + t$. Therefore, if the order of the curve we get from the algorithm is not the one we want, then find a quadratic nonresidue v and the twist curve by v would be the actual curve with desired order.

Chapter 5

Experimental Result

In this chapter, we present our experimental results of implementing the CM method. The implementation refers to IEEE P1363 and the MIRACL [1] (Multiprecision Integer and Rational Arithmetic C/C++ Library) library is used. The computing environment is Intel Xeon E5520 processor with 2.27GHz, 4G RAM on FreeBSD 7.2 with the MIRACL library version 5.4.

5.1 Distribution of Computation Time

First of all, we analyze the computation time of each step in CM method. Considering the steps of the algorithm:

(1) Determine the desired parameters of the elliptic curve

$$\Rightarrow \quad \#E\left(\mathbb{F}_p\right), p, t$$

(2) Compute the discriminant

$$\Rightarrow \quad -D = t^2 - 4p$$

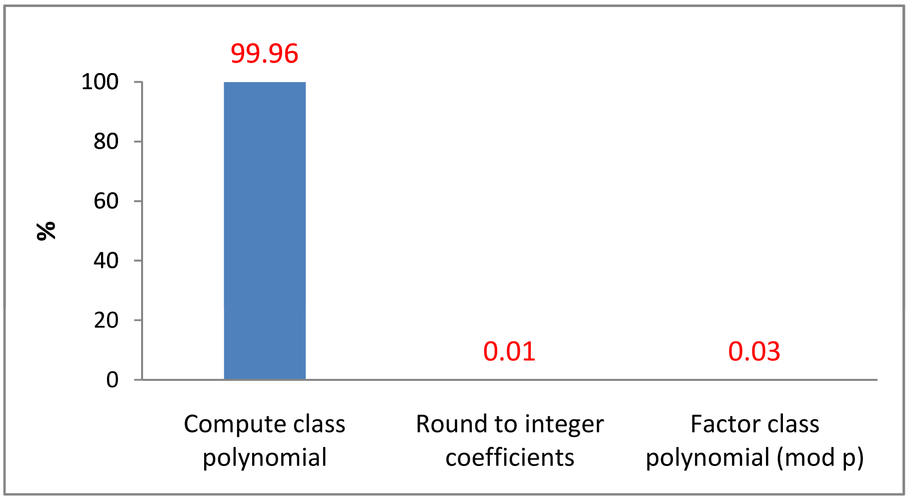


Figure 5.1: Proportion of computing time of each step

(3) Compute the class polynomial

$\Rightarrow$ H_D or W_D

(4) Factor the class polynomial and get all roots in $\mathbb{F}_p$

$\Rightarrow$ use Cantor-Zassenhaus algorithm

(5) Compute the desired elliptic curve equation

$\Rightarrow$ $y^2 = x^3 + \frac{3j}{1728-j}x + \frac{2j}{1728-j}$ or $y^2 = x^3 + \frac{3j}{1728-j}v^2x + \frac{2j}{1728-j}v^3$, for quadratic nonresidue v

Since the steps (1), (2), and (5) are computed by the simple equations, we ignore the time for computing these steps. By examining some examples, we observe that the computation of the class polynomial dominates the whole computing. Hence we focus on the results of computing the class polynomials in the following discussions. Figure 5.1 shows the proportion of computing time for each step.

	Hilbert polynomial	Weber polynomial
1 digit	1	1
2 digits	6	9
3 digits	37	70
4 digits	266	527
5 digits	457	3358
6 digits	–	19058
Total	767	23023

Table 5.1: Number of class polynomials computed

5.2 Computation of Class Polynomial

The discriminants we used in CM method are ranged from 2 to 6 digits. Table 5.1 is the number of actual computed discriminants. Although there has no known attacks for the small discriminants yet, it is suggeted that the discirminants used should have class number greater than 200 for the security consideration. Since lots of the discrminants with 6 digits satisfy the requirement, we also provide the observations focused on these discriminants.

Note: for simplifying the figures, we randomly select the data to restrict the number of points displayed under 1000.

The class polynomials most used in CM method are Hilbert polynomial and Weber polynomial. Figure 5.2a compares the computing time of each polynomials. The higher class number means more invariants to be computed and would take more time. therefore, we use the class number as x-axis. By scaling the y-axis to 0 to 1 second, this trend can be observed in Figure 5.2b.

Considering the fact that the coefficients of Hilbert polynomial would much lager than those of Weber polynomial, we use Weber polynomial instead of Hilbert polynomial in the following experiments.

5.2.1 Class Number Distribution

We observe the relation between the class numbers and the discriminants first. From some related researches, it is claimed that the class number will grow as $O\sqrt{|D|}$. Therefore, we plot Figure 5.3 to confirm the trend of the class number.

5.2.2 Precision of the Computation

In [7], [5], and [6], it mentioned the bound of bit precision required to compute the Hilbert and Weber polynomials. The bit precision required to compute the Hilbert polynomial is

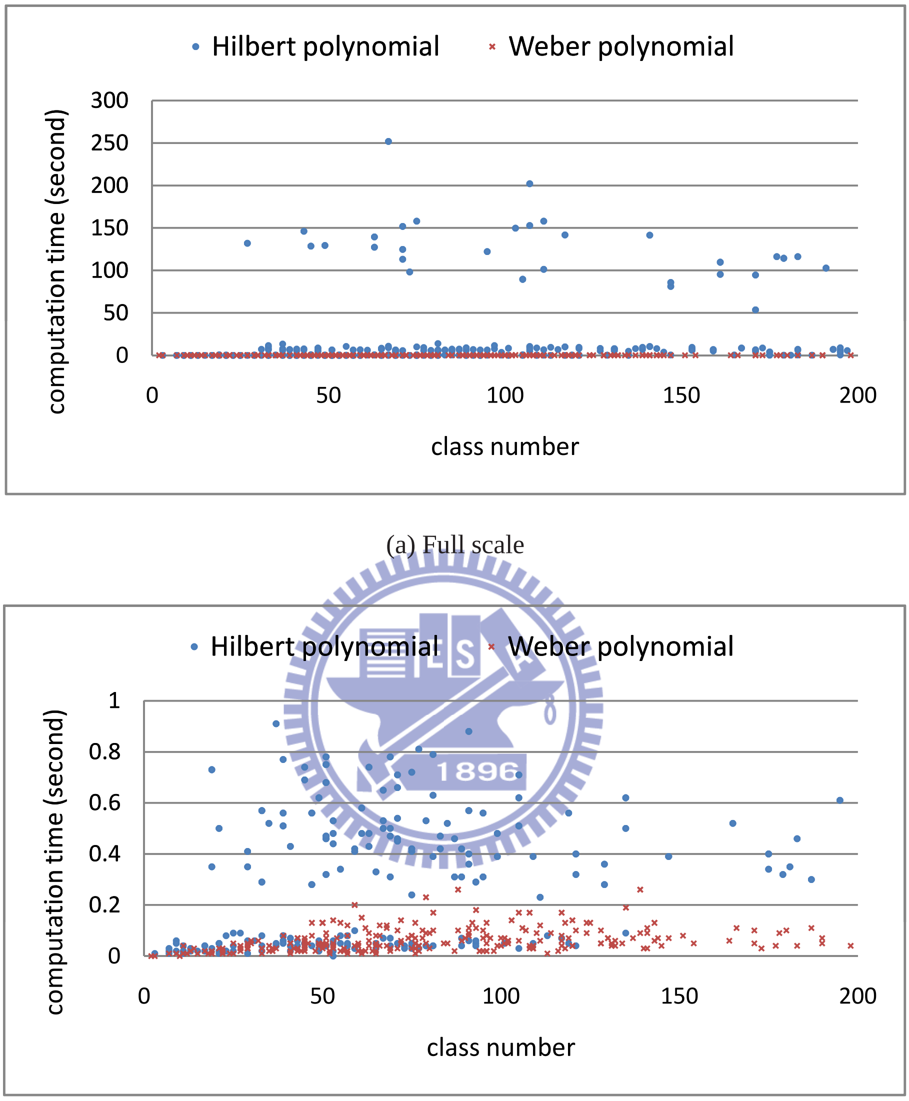
$$\text{H-Prec}\,(D) \approx \frac{\ln 10}{\ln 2}\left(\frac{h}{4}+5\right) + \frac{\pi\sqrt{D}}{\ln 2}\sum_{\tau}\frac{1}{a_\tau}$$

where the sum runs over the same values of τ as the computation of the class polynomial, i.e. runs over each reduced binary quadratic form (a, b, c). And the bit precision required to compute the Weber polynomial is

$$\text{W-Prec}\,(D) \approx c_1 h + \frac{\pi\sqrt{D}}{c_2 \ln 2}\sum_{\tau}\frac{1}{a_\tau} \tag{5.1}$$

where

$$c_1 = \begin{cases} 3 & \text{if } D \equiv 3 \pmod 8 \\ 1 & \text{if } D \not\equiv 3 \pmod 8 \end{cases}$$



(a) Full scale

(b) Scale to 0 – 1 second

Figure 5.2: Computing time of Hilbert and Weber polynomial

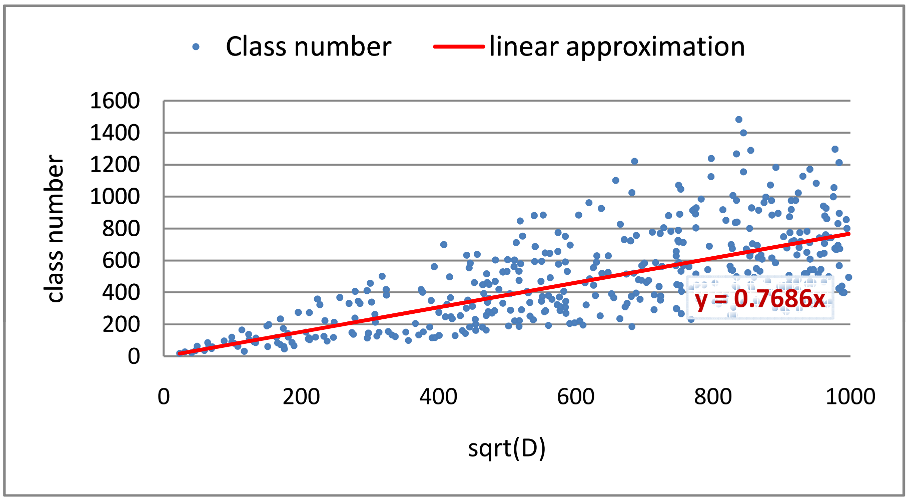


Figure 5.3: Trend of the class number

$$c_2 = \begin{cases} 24 & \text{if } D \equiv 3, 7 \text{ (mod 8) and } D \not\equiv 0 \text{ (mod 3)} \\ 8 & \text{if } D \equiv 3, 7 \text{ (mod 8) and } D \equiv 0 \text{ (mod 3)} \\ 6 & \text{if } D/4 \equiv 5 \text{ (mod 8) and } D \not\equiv 0 \text{ (mod 3)} \\ 2 & \text{if } D/4 \equiv 5 \text{ (mod 8) and } D \equiv 0 \text{ (mod 3)} \\ 12 & \text{if } D/4 \equiv 1, 2, 6 \text{ (mod 8) and } D \not\equiv 0 \text{ (mod 3)} \\ 4 & \text{if } D/4 \equiv 1, 2, 6 \text{ (mod 8) and } D \equiv 0 \text{ (mod 3)} \end{cases} .$$

And for the case $D \equiv 7 \pmod 8$, there exists a more accurate bound

$$\frac{\ln 10}{\ln 2}\left(\frac{\frac{h}{4} + 5 + \frac{\pi\sqrt{D}}{\ln 10}\sum_\tau \frac{1}{a_\tau}}{47} + 1\right).$$

We use the general bound in Equation 5.1 to estimate the bit precision required in our computation. In order to compare the accuracy of the bound, the implementation also reports the actual bits required of the maximal coefficient of the Weber polynomial. We plot the results in Figure 5.4.

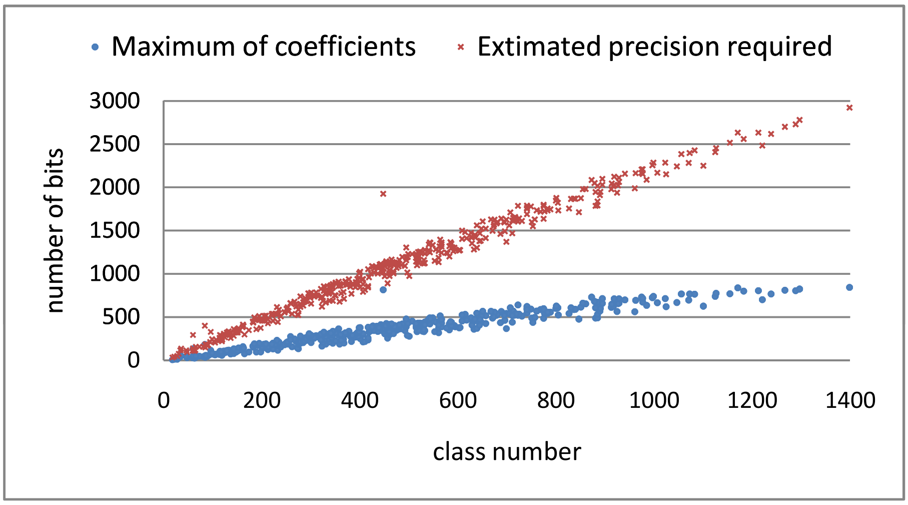


Figure 5.4: Estimated and actual precision required

5.2.3 Computation Time

In this section, we provide the results of the computation time which reflect the efficiency directly. First of all, the Figure 5.5 shows the computation time of all discriminants from 1 digit to 6 digits. Since the bits we use to compute are 1024, 2048, and 4096 bits, the results in Figure 5.5 are separated into three parts. To show that the relation between class number and the computing time is approximately linear, we also provide the result of each part in Figure 5.6a, Figure 5.6b, and Figure 5.6c.

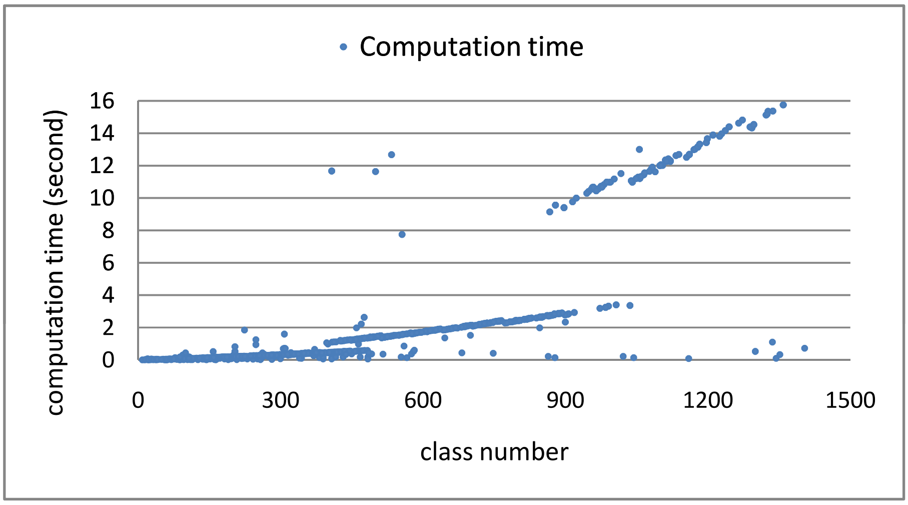
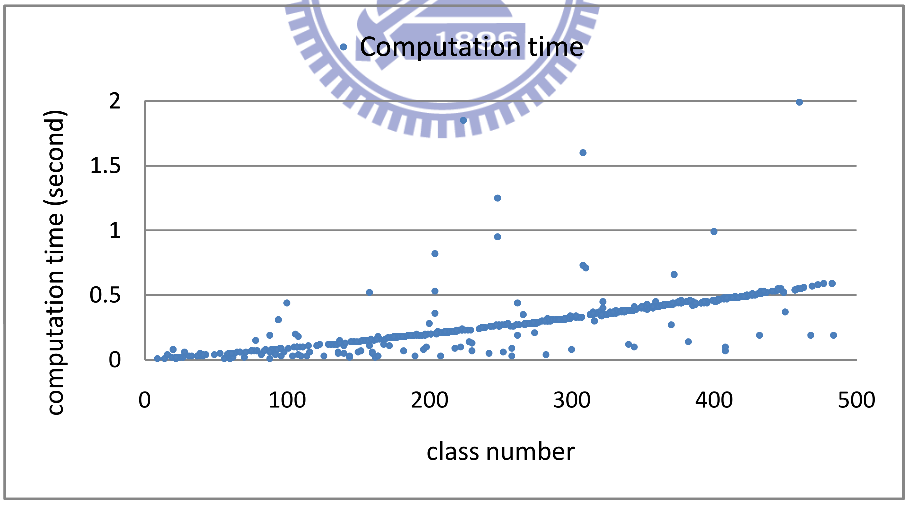
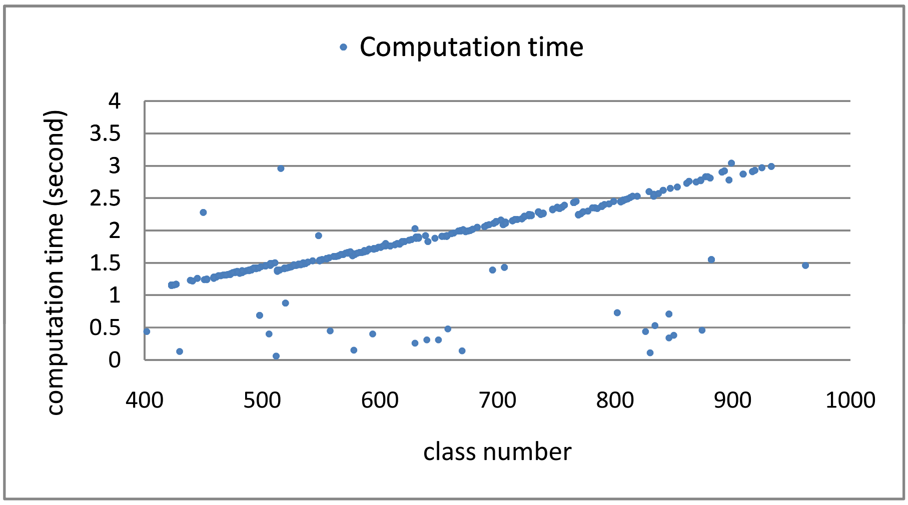


Figure 5.5: Computation time of Weber polynomial

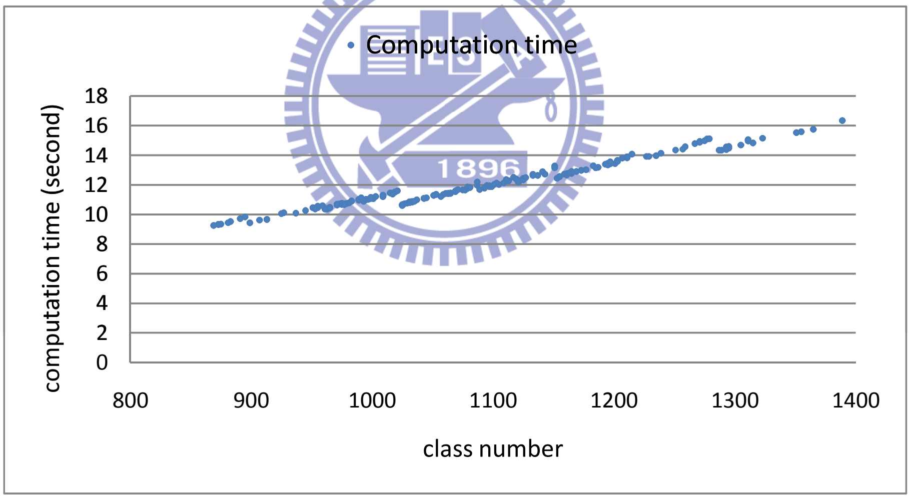


(a) 1024 bits used

Figure 5.6: Computation time of Weber polynomials - partitioned by precision



(b) 2048 bits used



(c) 4096 bits used

Figure 5.6: Computation time of Weber polynomials - partitioned by precision

Chapter 6

Conclusion & Future Work

We state the mathematical backgrounds and describe each step of the complex complication method in this thesis. For computing the class polynomial is one of the major part of CM method, we focus on the computation of the class polynomial, present the experimental results, and find some interesting differences between the prime and composite discriminants. It seems like that the computations of the Weber polynomials of composite discriminants have the chance to be more efficient. To confirm this effect, it should take more experiments and observe closely.

In our experiments, we compute the class polynomial of discriminants with at most 6 digits. Though the computation of class polynomial with more digits would take more time, there must exist more interesting properties to be discovered and may become the measurement of evaluating the discriminants.

Lots of researches related to computing the class polynomial are proposed nowadays. Andrew V. Sutherland achieve the record of computing the class polynomial with discirim-inant $D = 4058817012071$ and has clas number $h_D = 5000000$ in April, 2009 [12]. For solving the large space requirement of the polynomial, Andrew V. Sutherland proposed the computation using Chinese Remainder Theorem [13].

In the future, we will implement the algorithm with CRT to overcome the difficult of computing class polynomial with large digits. Besides, the researches of CM method on hyperelliptic curves with genus 2 are also ongoing.

Bibliography

[1] MIRACL, Multiprecision Integer and Rational Arithmetic C/C++ Library http://www.shamus.ie/.

[2] A. O. L. Atkin and F. Morain, “Elliptic Curves and Primality Proving,” *Mathematics of Computation*, no. 203, pp. 29–68, Jul 1993,
Also available as http://citeseer.ist.psu.edu/atkin93elliptic.html.

[3] R. M. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen, and F. Vercauteren, *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. CRC Press, 2006.

[4] I. F. Blake, G. Seroussi, and N. P. Smart, *Elliptic Curves in Cryptography*. Cambridge University Press, 1999.

[5] E. Konstantinou, Y. C. Stamatiou, and C. Zaroliagis, “On the Construction of Prime Order Elliptic Curves,” *Lecture Notes in Computer Science*, pp. 309–322, 2003.

[6] ——, “On the Use of Weber Polynomials in Elliptic Curve Cryptography,” *Lecture Notes in Computer Science*, pp. 335–349, 2004.

[7] G.-J. Lay and H. G. Zimmer, “Constructing Elliptic Curves with Given Group Order over Large Finite Fields,” *Lecture Notes in Computer Science*, pp. 250–263, 1994.

[8] A. Miyaji, M. Nakabayashi, and S. Takano, “New Explicit Conditions of Elliptic Curve Traces for FR-Reduction,” *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*, no. 84, pp. 1234–1243, May 2001.

[9] R. A. Mollin, *Algebraic Number Theory*. CRC Press, 1999.

[10] R. Schoof, “Elliptic Curves over Finite Fields and the Computation of Square Roots mod p,” *Mathematics of Computation*, no. 170, pp. 483–494, Apr 1985.

[11] ——, “Counting Points on Elliptic Curves over Finite Fields,” *Journal de théorie des nombres de Bordeaux*, no. 1, pp. 219–254, 1995,
Also available as http://citeseer.ist.psu.edu/schoof95counting.html.

[12] A. V. Sutherland, cM Record
http://www-math.mit.edu/ drew/CMRecords.html.

[13] ——, “Computing Hilbert Class Polynomials with the Chinese Remainder Theorem,” Available as http://arxiv.org/pdf/0903.2785.

[14] L. C. Washington, *Elliptic Curves: Number Theory and Cryptography*, 2nd ed. CRC Press, 2003.

[15] H. Weber, *Lehrbuch der Algebra, Volume I, II, III*, 3rd ed. AMS Chelsea Publishing, 1961.