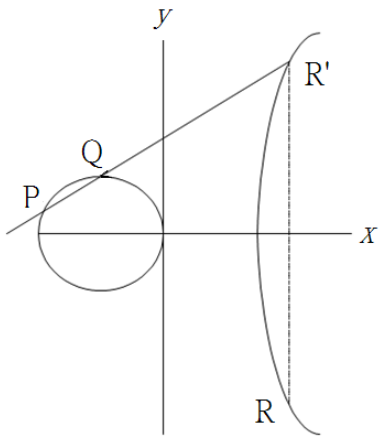
前言

過去 30 年，公開金鑰密碼學成為網際網路及其他形式通訊上為保護資訊安全的重要研究領域，同時也是金鑰管理與數位簽章的基礎。在金鑰管理方面，公開金鑰加密可用來保護通訊密鑰；在數位簽章方面，提供了認證資料來源與確認資料不被更改的功能。在 70 年代中期，第一代的公開金鑰演算法提供了接下來 20 年的資訊安全，最為著名的有：提供金鑰管理與認證 IP 的 IKE 與 IPSEC，提供網路通訊安全的 SSL/TLS。

公開金鑰技術為密碼學帶來了很大的變革，陸續有許多相關研究發展，而最近 20 年來，發展出更具有效率且安全性的密碼技術－橢圓曲線密碼學。這些密碼系統或數位簽章技術的安全性大多是建立在解一些數學問題的困難度之上。

在 1985 年，Koblitz 與 Miller 利用橢圓曲線的特性分別提出兩個著名的橢圓曲線密碼系統。雖然研究橢圓曲線密碼應用理論從 1985 年就已開始，但是與 RSA 及 ElGamal 比較起來，橢圓曲線密碼應用理論顯得比較令人難以了解。但是橢圓曲線密碼系統能帶來的好處，如較短的金鑰長度，仍使得橢圓曲線密碼學成為學術界越來越熱門的研究。



以二維實數平面上的橢圓曲線為例，我們可定義點與點加法。設 P、Q 為曲線上的兩個點，我們可以畫出一條直線通過這兩點(如果兩點相同，就做切線)，然後這條直線還會通過在曲線上的另外一點 R’，最後對著 R’做 x 軸的鏡射，得到的點 R 就定為 P+Q；此外，R 與 R’互為反元素，即一

個點的反元素為自身對 x 軸的鏡射；最後，定義單位元素∞，如此一來，橢圓曲線就形成一個加法群。設 E 為定義在有限體上的橢圓曲線，P 為曲線上一點，Q 在 P 所生成的子群中，則尋找一個整數 k 使得 Q = kP 就是橢圓曲線離散對數問題。橢圓曲線密碼系統的安全性就建立在橢圓曲線離散對數問題。

根據美國國家技術標準學會(NIST)之建議，現在的安全強度要求至少要同 RSA-2048。提高安全度的一種選擇是增加安全參數(更多位元數)的傳統公開金鑰系統；另一種選擇則是採用橢圓曲線密碼系統。

評斷公開金鑰密碼系統所需要之金鑰長度的方法之一是將他們與傳統加密演算法(即對稱式加密演算法－symmetric encryption algorithms，如 DES 及 AES 演算法)做比較，下表列出 NIST 所建議之金鑰長度：

Symmetric Key Size	**RSA and Diffie-Hellman Key Size**	**Elliptic Curve Key Size Prime Field / Binary Field**
80	1024	192 / 163
112	2048	224 / 233
128	3072	256 / 283
192	7680	384 / 409
256	15360	521 / 571

NIST 建議之金鑰長度(單位: bit)

以安全性來說，要達到與對稱式加密演算法一樣的安全度，橢圓曲線需要長度為對稱式加密演算法兩倍長的金鑰。使用 RSA 或 Diffie-Hellman 密碼系統保護 128 位元 AES 密鑰，依上表所建議應使用 3072 位元之金鑰－是目前在網際網路中所使用的三倍，而相對應的橢圓曲線密碼系統所需使用的金鑰只要 256 位元。如此便可發現，在增加相同強度安全性下，RSA 與 Diffie-Hellman 金鑰長度增加的速度，比橢圓曲線密碼系統所需增加的速度更為驚人。也就是說，橢圓曲線密碼系統每位元所提供之安全度比 RSA 或 Diffie-Hellman 密碼系統更佳。

另外，安全度不是橢圓曲線密碼學唯一有吸引力的特點。橢圓曲線密

碼系統在計算效率上比第一代公開密碼系統(如 RSA 和 Diffie-Hellman)更快速。雖然橢圓曲線上的運算比 RSA 或 Diffie-Hellman 所需之運算稍加複雜，但每位元所增加之安全強度可補償額外的運算時間。下表顯示在不同安全強度(相當於金鑰長度)下 Diffie-Hellman 與橢圓曲線運算比率：

Security Level (bits)	**Ratio of DH Cost : EC Cost**
80	3:1
112	6:1
128	10:1
192	32:1
256	64:1

雖然在橢圓曲線上的運算是較第一代公開密碼系統複雜的，但是得益於其較短的金鑰長度，因此整體運算速度依然可以快於第一代的公開密碼系統。另外，不同金鑰長度也直接影響到金鑰交換或數位簽章時所需通訊通道的負載程度，在 NIST 建議的金鑰位元數大致上相當於通道中需要傳送的位元數。故在受限制的通訊環境與計算能力，如無線通訊，或手機或 PDA 上的密碼系統實作，橢圓曲線提供了更好的公開金鑰演算法的選擇。

另外，在橢圓曲線上的 bilinear pairings，如 Weil pairing 與 Tate pairing (改進過後的 Eta pairing、Ate pairing 與 generalized Ate pairing)等，也造就了另一支 pairing-based 密碼系統，從 Boneh 與 Franklin 使用 pairing 提出的 identity-based 密碼系統開始，pairing-based 密碼系統也成為很重要的研究領域，許多的應用也相繼而生。

除了用以建構 identity-based 密碼系統外，雙線性配對還可應用至許多不同之密碼系統及領域，並可能因此觀察到新的性質，如存取控制[S02b]、金鑰協定[BMP04]、非互動式金鑰發佈[DE02]、憑證[CL04]、可證明之安全簽章[BMS03]、短簽章[BB04b]、群體簽章[BBS04]、具總和性及可驗證之加密簽章[BGLS03]、盲簽章或部分盲簽章[ZSS04]、Proxy 簽章[ZSL03]、具不可否認性質之簽章[ZSS03]、多人簽章[LWZ03]、有限制驗證者之簽章[CZK04]、有門檻之密碼系統[LHKKI04]、階層式密碼系統[TYW04]、可驗證之隨機函數[D02]、Strongly insulated encryption[BP02]、可抵抗不法攻擊

之加密演算法[DFKMY03]、不須憑證之PKC[AP03]、找出反叛者[MSK02]、身分認證系統[KKK02]、其他應用及密碼系統[AL03, SD03]等。

研究目的

在選擇橢圓曲線作為一個公開金鑰系統的基礎有許多安全上的考量。NIST 提供了一份安全的橢圓曲線列表，其中五條曲線是定義於二元體上的 Koblitz 橢圓曲線，五條是定義於相同二元體上的隨機橢圓曲線，另五條曲線是定義在質數體上的隨機橢圓曲線。這些橢圓曲線可保護相當於長度為 80、112、128、192 和 256 位元對稱式密碼算法的密鑰。

由於 NIST 建議，公開金鑰密碼系統需相當於 RSA-2048 之安全度，可用短金鑰之橢圓曲線密碼系統的協定標準化(ECDSA、ECMQV、ECIES 等)，所以未來公開金鑰密碼系統之走向勢必為橢圓曲線密碼系統，因此，選擇安全並運算具有一定效率的橢圓曲線，是建置一個實用的資訊安全系統的重要議題。

在公開金鑰密碼系統中，增加金鑰長度可以達到更高的安全等級，但相對地，也要付出更久的運算時間。因此，選擇安全且高效率的橢圓曲線，是建置實用資訊安全系統的重要議題。根據橢圓曲線密碼學的研究，一般破解離散對數的方法中，最有效的是 Pohlig-Hellman 攻擊法，而專門針對橢圓曲線離散對數問題的同構攻擊法(Isomorphism Attack)，包含 MOV 攻擊、FR 攻擊法，及針對 prime-field-anomalous 曲線的攻擊法，以及 Weil Descent 攻擊。綜合上述所有的攻擊法，我們要選擇一條定義在有限體上適用的橢圓曲線，必須滿足以下條件：

1. 橢圓曲線的點個數 $\#E(\mathbb{F}_q) = hr$，其中 r 為至少 160-bit 長的質數
2. $\#E(\mathbb{F}_q) \neq q$
3. $r \nmid q^d - 1$ for $d \in [1,20]$
4. 若 $q = p^m$，則 m 為質數

因此，在橢圓曲線密碼系統的應用上，為了避免密碼系統被攻破，求出有限體上橢圓曲線的有理點個數是很關鍵的，也就是點數計算問題(point counting problem)，如果用直觀的計算方式，如 Legendre 符號(Legendre

symbol)：

$$\#E(\mathbb{F}_q) = q + 1 + \sum_{x=0}^{q-1} \left(\frac{x^3 + ax + b}{q} \right)$$

這個方法需要指數次方 $2^{\log(q)}$ 的時間，可見，我們需要更強而有力的工具，有效率的解決這個問題。

且，從 pairing-based 密碼系統上的應用之多，可見得 pairing-based 所受之重視，但一般而言，pairing-based 密碼系統的計算量是非常大的，因此若是未能找到合適的橢圓曲線(pairing-friendly 橢圓曲線)，來當作 pairing 計算之基礎，在實作上是有困難度的，因此在近年來即有許多的學者研究如何找到 pairing-friendly 橢圓曲線，而這些方法都會用到複乘法。

文獻探討

現在，主要用以下三種技術來找尋適用於密碼系統的橢圓曲線：

1. 隨機曲線：隨機產生橢圓曲線的係數，並計算此曲線上點的個數，直到找到一條適合密碼系統的橢圓曲線。
2. 複乘法。
3. 子體曲線。

本年度計畫所著重的是第二種方法。由於 pairing 之計算量頗為複雜，因此若是無法找到適合之橢圓曲線，將會使得 pairing-based 密碼系統在實務上淪為不可行，眾多學者紛紛提出各式各樣的方法，尋找 pairing-friendly 橢圓曲線，即橢圓曲線具有以下特性：

1. 橢圓曲線 E 定義於質數體 $\mathbb{F}_q$ 上，其中 q 為質數
2. 橢圓曲線的點個數 $\#E(\mathbb{F}_q) = h \cdot r$，其中 $r > 2^{160}$ 為質數
3. 存在一個夠小的 embedding degree k 使得 $r \mid q^k - 1$
4. 存在一個夠小的 D 使得 $4q - t^2 = Dy^2$，其中 $\#E(\mathbb{F}_q) = q + 1 - t$，y 為整數

符合以上條件的橢圓曲線，其實是很稀疏的，因此必須有各種的策略來搜尋 pairing-friendly 橢圓曲線。自 2001 年以來，許多學者紛紛提出各種尋求

pairing-friendly 橢圓曲線的策略，在這些學者所提出來的方法中，大致上可分為兩種類型：一種是家族式的橢圓曲線(elliptic curves in families)，另一種則是非家族式的橢圓曲線(elliptic curves not in families)。

在此簡短的介紹尋找 pairing-friendly 橢圓曲線的演進，首先，由 Miyaji，Nakabayashi 及 Takano 針對 k=3、4、6 提出 MNT 橢圓曲線，2004 年 Galbraith、Mckee、Valenca 提出了散發的 Brezing-Weng 家族式橢圓曲線(sporadic families of Brezing-Weng curve)，2005 年 Brezing 及 Weng 提出 cyclotomic 家族橢圓曲線(cyclotomic families elliptic curve)，2006 年 Freeman 提出 Freeman 家族橢圓曲線(Freeman's families elliptic curve)。同年，Scott 及 Barret 提出了 Scott-Barreto 家族橢圓曲線(Scott-Barreto families elliptic curve)。

如果要找非家族式的橢圓曲線，通常只要使用學者所提的方法，就可以找到合適的橢圓曲線，但一般來說，這個方法能找到的曲線數量是很有限的。因此，本計畫將著重家族式橢圓曲線，在這類的方法中，先用多項式表示橢圓曲線參數，包含係數、定義的有限體等，然後可以代入不同的 x 值，而得到不同的 pairing-friendly 橢圓曲線，但是，通常使用目前學者所提的方法，尚不能很快找到合適的橢圓曲線，因為通常在家族式橢圓曲線的論文中，只是找到代表橢圓曲線的一組多項式，而並未提到該代入何值使得這些多項式真正能代表一個合適的橢圓曲線。

在找尋到適合的橢圓曲線參數後，需要用 CM 演算法求得真正橢圓曲線的係數 a 與 b，首先介紹，對於一個複數 τ，下列式子可以計算j(τ)：

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

$$\Delta(\tau) = q\left(1 + \sum_{n\geq 1}(-1)^n\left(q^{\frac{n(3n-1)}{2}} + q^{\frac{n(3n+1)}{2}}\right)\right)^{24}$$

$$h(\tau) = \frac{\Delta(2\tau)}{\Delta(\tau)}$$

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

而 CM 演算法的過程簡述如下：

1. 已經有適當的橢圓曲線參數 (N, a_p, p)，使得 $-Dy^2 = a_p^2 - 4p$，其中 D 不會太大
2. 找出所有的 (a, b, c) 符合以下條件：
   (1) a, b, c 為整數，且 $a > 0$
   (2) $\gcd(a, b, c) = 1$
   (3) $b^2 - 4ac = -D$
   (4) $-a < b \leq a$
   (5) $a \leq c$
   (6) 若 $a = c$，則 $b \geq 0$
3. 利用找出的 (a, b, c) 計算一多項式

$$P(X) = H_D(X) = \prod_{(a,b,c)} \left(X - j\left(\frac{-b + \sqrt{-D}}{2a} \right) \right)$$

   此多項式為整係數多項式
4. 將 $P(X)$ 看成是 $\mathbb{F}_p$ 上的一個多項式，在 $\mathbb{F}_p$ 中求解，求出來的解即為所求橢圓曲線之 j-invariant
5. 利用此解，建構出在 $\mathbb{F}_p$ 上的橢圓曲線。

$$E: Y^2 = X^3 - \frac{3j}{j - 1728}X + \frac{2j}{j - 1728}$$

   在質數體上，擁有相同 j-不變量的橢圓曲線可能是扭曲 (twist) 曲線，因此要檢查其點數為 $p + 1 - a_p$ 或 $p + 1 + a_p$
6. 如果是 $p + 1 + a_p$ 的情形，利用一個在 $\mathbb{F}_p$ 上沒有平方跟的元素 d，則

$$E: Y^2 = X^3 + d^2AX + d^3B$$

即為點數為 $p + 1 - a_p$ 之橢圓曲線

研究方法

在尋找 pairing-friendly 橢圓曲線中，最重要的一步驟就是 Complex Multiplication 方法的計算，在本年度中，我們充分了解此方法的代數理論，也了解此方法的相關改進，並試圖使用 Computer Science 背景，針對程式設計部分做改良，以期能更有效率的產生適用於 pairing-based 密碼系統的橢圓曲線。另一方面，我們也針對 pairing-based 密碼系統做一研究，了解 bilinear pairing 的原理與應用，並對現行多種 pairing-based 密碼系統之設計做一了解，找出能將 pairing 更加推廣與應用的方法。

結果與討論(含結論與建議)

We present our experimental results of implementing the CM method. The implementation refers to IEEE P1363 and the MIRACL (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.

1. 計算時間分布

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

(2) Compute the discriminant
$\Rightarrow \quad -D = t^2 - 4p$

(3) Compute the class polynomial
$\Rightarrow \quad H_D$ or W_D

(4) Factor the class polynomial and get all roots in $\mathbb{F}_p$
$\Rightarrow$ use Cantor-Zassenhaus algorithm

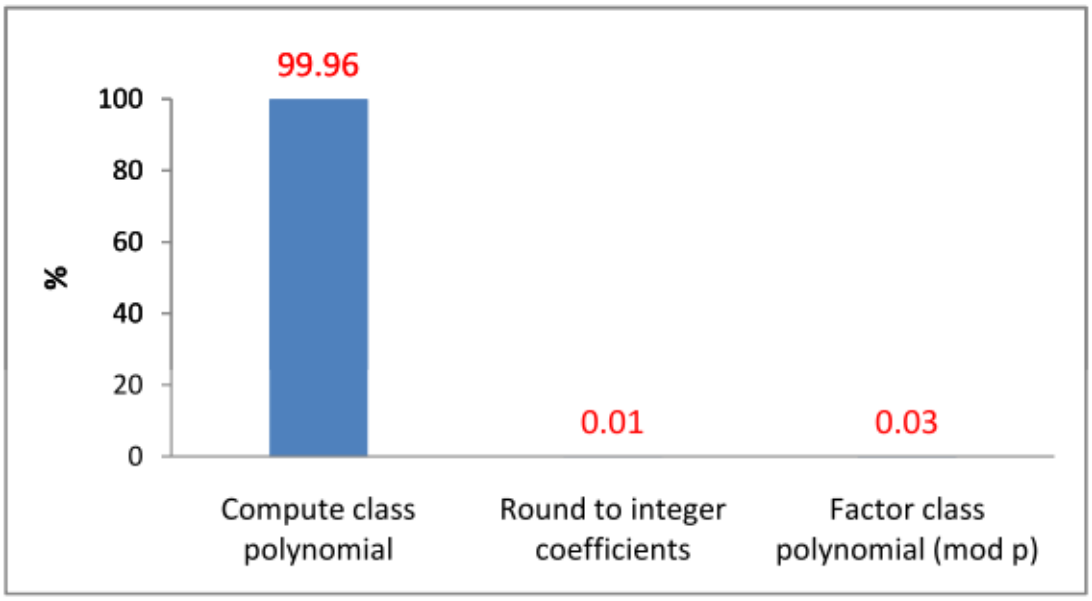


Figure 5.1: Proportion of computing time of each step

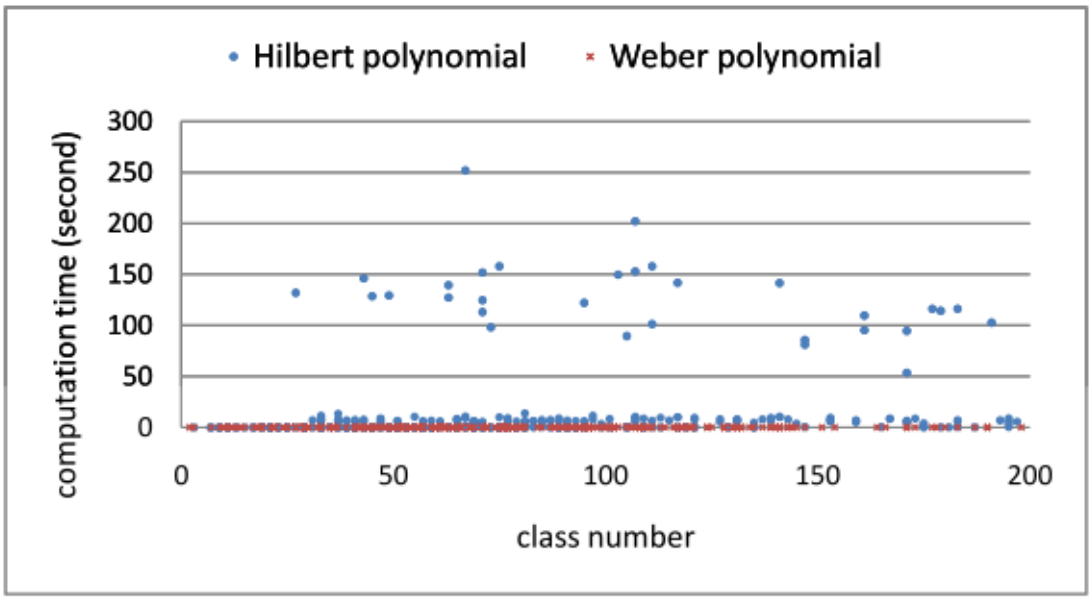
(5) Compute the desired elliptic curve equation
$\Rightarrow \quad y^2 = x^3 + \frac{3j}{1728-j}x + \frac{2j}{1728-j}$ or $y^2 = x^3 + \frac{3j}{1728-j}v^2x + \frac{2j}{1728-j}v^3$, for quadratic nonresidue v

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.

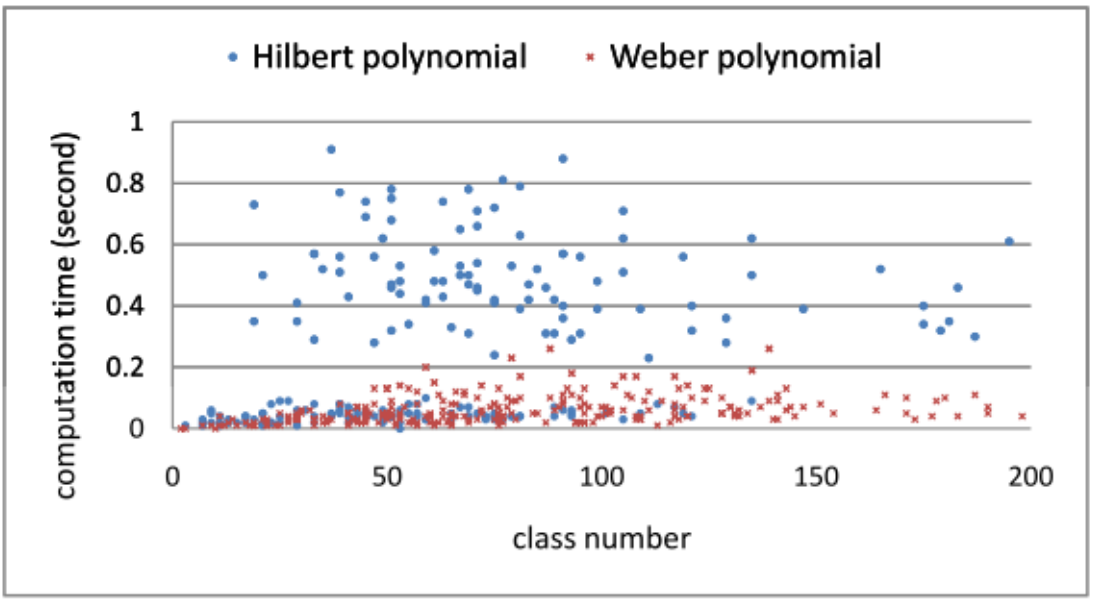
由上圖可知，花最多時間的步驟就是計算 class polynomial。

2. 計算 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



(a) Full scale



(b) Scale to 0 – 1 second

Figure 5.2: Computing time of Hilbert and Weber polynomial

digits satisfy the requirement, we also provide the observations focused on these discriminants.

	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

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.

2.1. Class Number 分布

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.

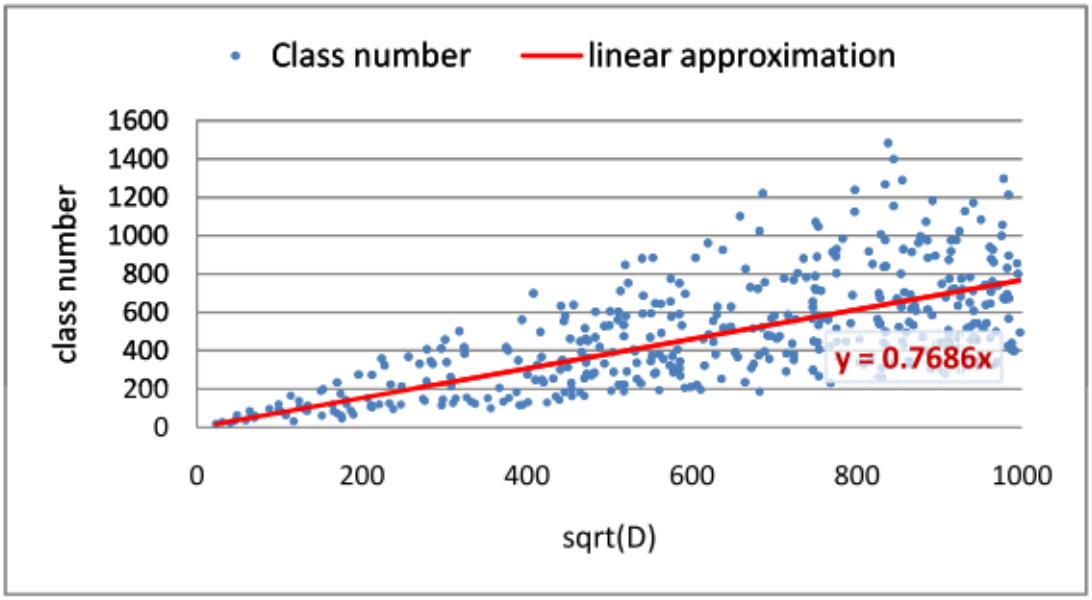


Figure 5.3: Trend of the class number

2.2. 計算精準度

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

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

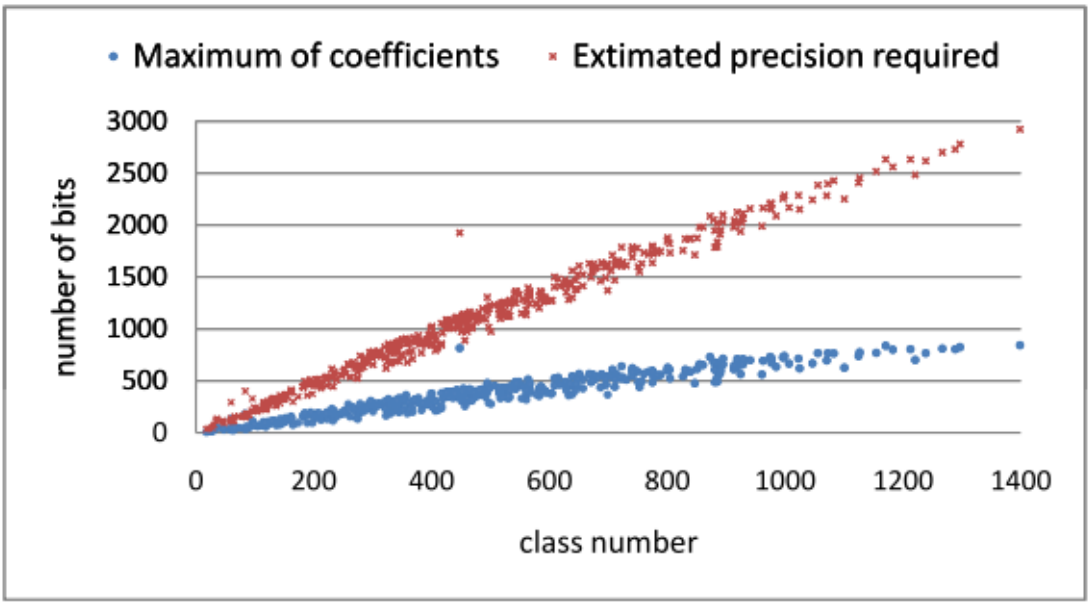


Figure 5.4: Estimated and actual precision required

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

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.

2.3. 計算時間

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.

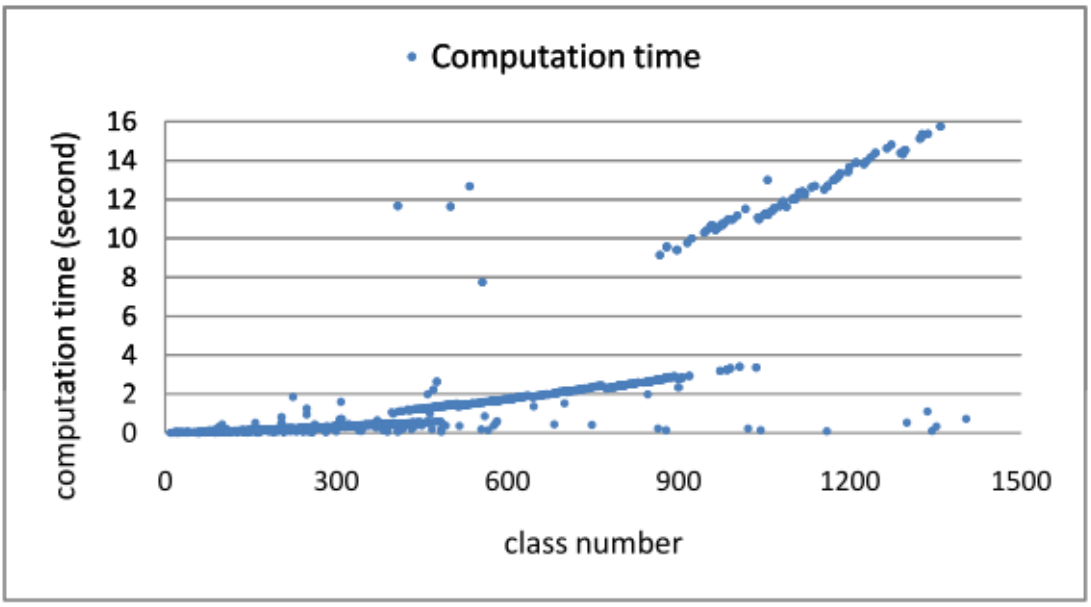
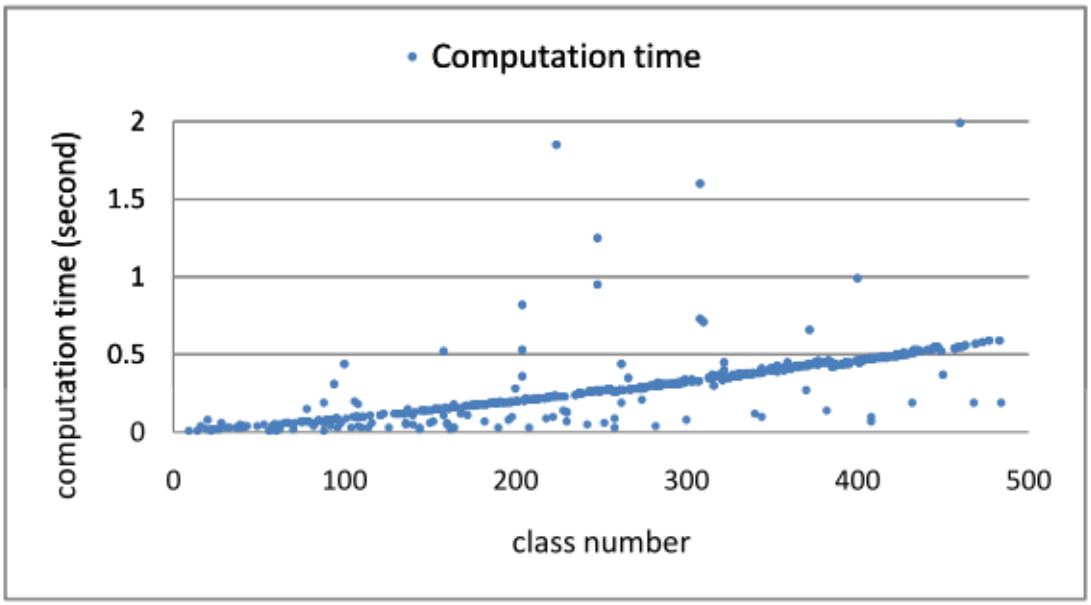
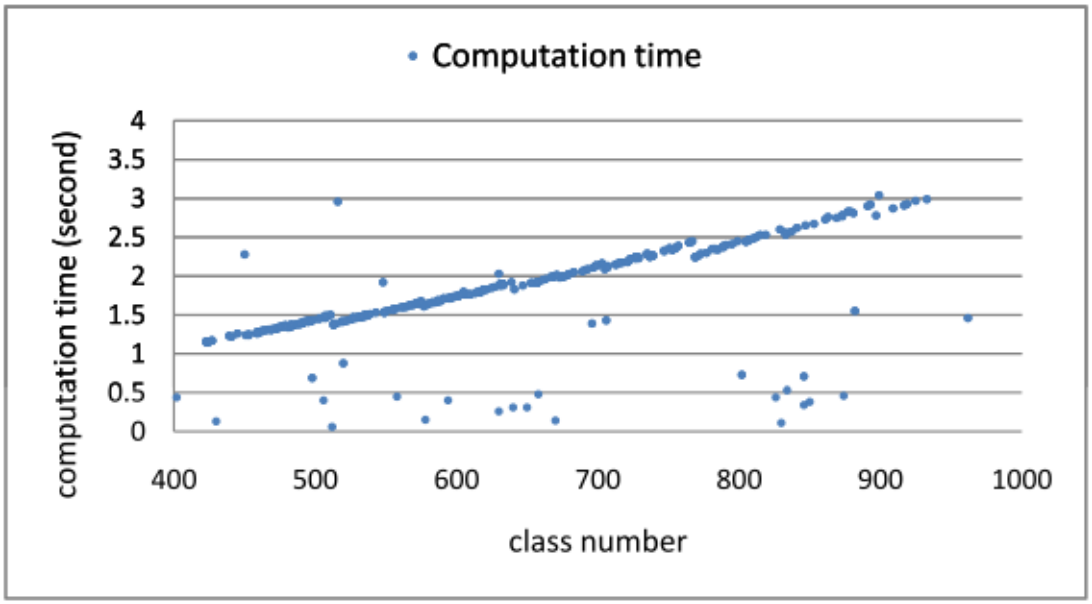


Figure 5.5: Computation time of Weber polynomial

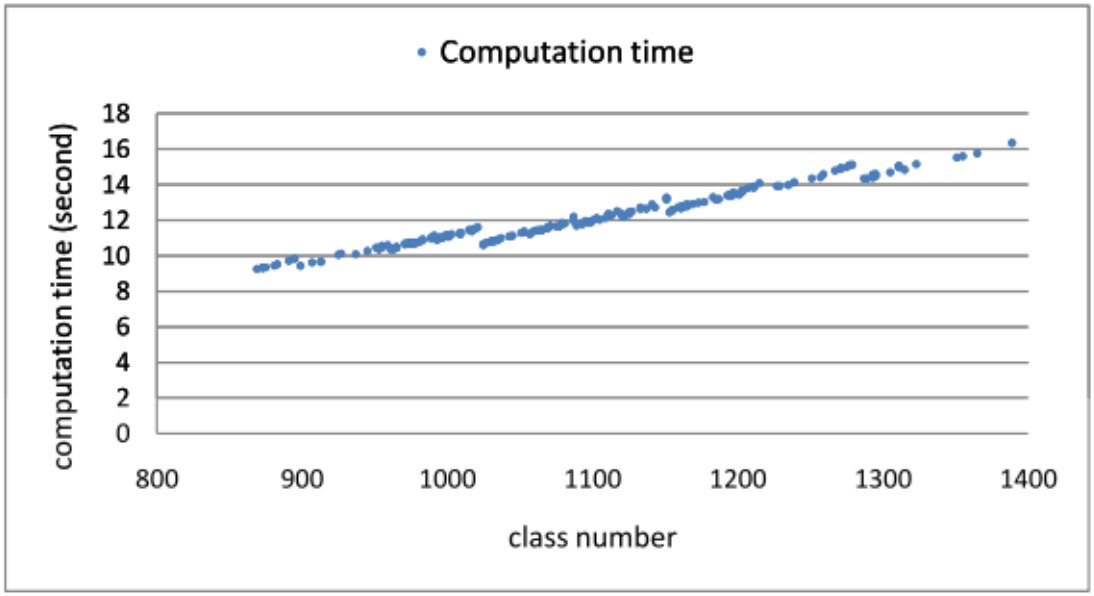


(a) 1024 bits used

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

結論與建議

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 discriminant D=4058817012071 and has class number

h_D=5000000 in April, 2009. For solving the large space requirement of the polynomial, Andrew V. Sutherland proposed the computation using Chinese Remainder Theorem.

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.

參考文獻

1. Elliptic curves over finite fields and the computation of square roots mod p. Schoof, R. Math Comp. 44, 483-494. (1985)
2. Counting points on elliptic curves over finite fields. Schoof, R. Journal de Theorie des Nombres de Bordeaux 7, 219-254. (1995)
3. On the computation of modular polynomials for elliptic curvess, Ian Blake, Janos Csirik, and Gadiel Seroussi, Hewlett-Packard Laboratories technical report, 1999.
4. D. Charles, K. Lauter, Computing modular polynomials. Lond. Math. Soc. J. Comput. Math. 8, 195–204(2005).
5. Isogeny cycles and the Schoof-Elkies-Atkin algorithm. J.-M. Conveignes, L. Dewaghe, F. Morain. L'Ecole Polytechnique, Laboratoire D'Informatique, CNRS, Palaiseau. August 1996.
6. Schoof's algorithm and isogeny cycles. J.-M. Conveignes, F. Morain. ANTS-1, 43-58. 1994.
7. Counting the number of point on elliptic curves over finite fields of characteristic greater than three. F. Lehmann, M. Maurer, V. Mueller, et al. ANTS-I, LNCS 877, 60-70. 1994.
8. Finding the eigenvalue in Elkies's Algorithm. M. Maurer, V. Mueller. Experimental Mathematics 10(2) 275-285. 2001.
9. Schoof-Elkies-Atkin 演算法的有效實現. 董軍武，胡磊，裴定一. Communications of the CCISA, Vol. 12, No. 2. April 2006.
10. Elliptic Curves in Cryptography. I. Blake, G. Seroussi, N. P. Smart. Cambridge University Press. 1999.
11. Counting the number of points on elliptic curves over finite fields: strategies and performances. Advances in Cryptology—EUROCRYPT '95 (LNCS 921), 79-94, 1995.
12. Efficient implementation of Schoof's algorithm. Advances in Cryptology—ASIACRYPT '98 (LCNS 1514), 66-79, 1998.
13. The canonical lift of an ordinary elliptic curve over a prime field and its point counting. T. Satoh. Journal of the Ramanujan Mathematical Society, 15, 247-270. 2000.
14. Guide to Elliptic Curve Cryptography, Darrel Hankerson, Alfred Menezes, Scott Vanstone. Springer-Verlag, 2004.
15. An improved algorithm for computing logarithms over GF(p) and its cryptographic significance. S. Pohlig, M. Hellman. IEEE Transactions on Information Theory, 24, 106-110. 1978.
16. Monte Carlo methods for index cimputation (mod p). J. Pollard.

Mathematics of Computation, 32, 918-924. 1978.
17. Use of elliptic curves in cryptography. V. Miller. Advances in Cryptology, CRYPTO ’85 (LNCS 218), 417-426. 1986.
18. On the discrete logarithm in the divisor class group of curves. H. Ruck. Mathematics of Computation, 68, 805-806. 1999.
19. Reducing elliptic curves logarithms to logarithms in a finite field. A. Menezes, T. Okamoto, S. Vanstone. IEEE Transactions on Information Theory, 39, 1639-1646. 1993.
20. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. G. Frey, H. Ruck. Mathematics of Computation, 62, 865-874. 1994.
21. Applications of arithmetical geometry to cryptographic constructions. G. Frey. Proceedings of the fifth international conference on finite fields and applications, 128-161. 2001.
22. Index calculus for Abelian varieties and the elliptic curve discrete logarithm problem. P. Gaudry. October, 2004.
23. Fast computation of canonical lifts of elliptic curves and its application to point counting. T. Satoh, B. Skjernaa, Y. Taguchi. Finite fields and their applications, 9, 89-101. 2003.
24. Elliptic curves and primality proving. A. Atkin, F. Morian. Mathematics of Computation, 61, 191-210. 1989.
25. Constructing elliptic curves with given group order over large finite fields. G. Lay, H. Zimmer. Algorithmic Number Theory—ANTS-I (LNCS 877), 250-263. 1994.
26. A comparison and a combination of SST and AGM algorithms for counting points of elliptic curves in characteristic 2. Advances of Cryptology—EUROCRYPT 2000 (LNCS 2501), 311-327. 2002.
27. The elliptic curve digital signature algorithm(ECDSA). D. Johnson, A. Menezes, S. Vanstone. International Journal of Information Security, 1, 36-63. 2001.
28. A study on the proposed Korean digital signature algorithm. Advances in Cryptology—ASIACRYPT ’98 (LNCS 1514), 175-186. 1998.
29. Minimizing the use of random oracles in authenticated encryption schemes. Information and Communications Security ’97 (LNCS 1334), 1-16. 1997.
30. ISO/IEC 18033-2. Information Technology—Security Technology—Encryption Algorithms—Part 2, Asymmetric Ciphers, draft 2002.

31. Authentication and authenticated key exchanges. W. Diffie, P. Van

Ooeschot, M. Wiener. Design, Codes and Cryptography, 2, 107-125. 1992.
32. An efficient protocol for authenticated key agreement. L. Law, A. Menezes, M. Qu, J. Solinas, S. Vanstone. Designs, Codes and Cryptography, 28, 119-134. 2003.
33. Die Berechnung der Punktanzahl elliptischer Kurven ueber endlichen Koerpern der Charackteristik groeber 3. Ph. D. thesis, Universitaet des Saarlandes, Saarbruechen, Germany. 1995.
34. Class number, a theory of factorization, and genera. D. Shanks. 415-420, Number Theory Institute, 1969.
35. On p-adic point counting algorithms for elliptic curves over finite fields. T. Satoh, In: C. Fieker, D. Kohel (Eds.), Algorithmic number theory, Proceeding of ANTS-5, 2002 (Sydney, Australia, July 2002), Lecture Notes in Computer Science, Vol. 2369, Springer, Berlin, 2002, pp. 43–66.
36. Fast computation of canonical lifts of elliptic curves and its application to point counting. Takakazu Satoh, Berit Skjernaa, Yuichiro Taguchi, Finite Fields and Their Applications, Volume 9, Issue 1, January 2003, Pages 89-101, ISSN 1071-5797, DOI: 10.1016/S1071-5797(02)00013-8.
37. Point counting on elliptic curves over binary fields. Marc Masdeu Sabate.
38. Finding secure curves with the Satoh-FGHalgorithm and an early abort strategy. Fouquet, M., Gaudry, P. and Harley, R., Advances in Cryptology - EUROCRYPT2001, Lecture Notes in Comput. Sci. 2045 (ed. Pfitzmann, B., Springer, 2001) 14–29.
39. MIRACL, Multiprecision Integer and Rational Arithmetic C/C++ Library http://www.shamus.ie/
40. Handbook of Elliptic and Hyperelliptic Curve Cryptography. R. M. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen, and F. Vercauteren. CRC Press, 2006.
41. On the Construction of Prime Order Elliptic Curves. E. Konstantinou, Y. C. Stamatiou, and C. Zaroliagis. Lecture Notes in Computer Scisnce, pp. 309—322, 2003.
42. On the Use of Weber Polynomials in Elliptic Curve Cryptography. Lecture Notes in Computer Science, pp. 335—349, 2004.
43. New Explicit Conditions of Elliptic Curve Traces for FR-Reduction. A. Miyaji, M. Nakabayashi, and S. Takano. IEICE TRANSACTIONS on Fundamentals of Electronics, Communications, and Computer Sciences, no. 84, pp. 1234—1243, May 2001.
44. Algebraic Number Theory. R. A. Mollin. CRC Press, 1999.
45. CM Record. A. V. Sutherland. http://www-math.mit.edu/drew/CMRecords.html

46. Computing Hilbert Class Polynomials with the Chinese Remainder Theorem. Available as http://arxiv.org/pdf/0903.2785
47. Elliptic Curves: Number Theory and Cryptography, 2nd ed. L. C. Washington. CRC Press, 2003.
48. Lehrbuch der Algebra, Volume I, II, III, 3rd ed. H. Weber. AMS Chelsea Publishing, 1961.

Chapter 3

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.

3.1 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 $Char\,(q) > 3$, 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

$$y^2 = x^3 + \frac{3j}{1728 - j}x + \frac{2j}{1728 - j}. \tag{3.1}$$

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

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 $j\,(E_{\mathbb{C}}) = j\,(\tau)$.

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

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

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 $j(E_{\mathbb{C}})$ is the Hilbert class polynomial

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

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 $j(A_i)$ 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 3.1 (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 $H_D(x) \pmod p$.

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 $End(E)$ and the Hilbert class field.

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

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

1. do
2. do
3. choose prime p of desired size
4. until $\epsilon p = x^2 + dy^2$ for some $x, y \in \mathbb{Z}$
5. Let $n_1 = p + 1 - \frac{2x}{\delta}, \quad n_2 = p + 1 + \frac{2x}{\delta}$
6. until n_1 or n_2 has a large prime factor l
7. find a root j_p of $H_D(x)$ (mod p)
8. compute the elliptic curve $E_j/\mathbb{F}_p$ by 3.1 and its twist $E'_j/\mathbb{F}_p$
9. do
10. find a point $P \in E_j(\mathbb{F}_p)$ and compute $Q = n_1 P$
11. if $Q = \infty$ and $n_2 P \neq \infty$, return p and E_j
12. else if $Q \neq \infty$, return p and E'_j

3.2 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 3.2 (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 $\mathcal{A}_1$.

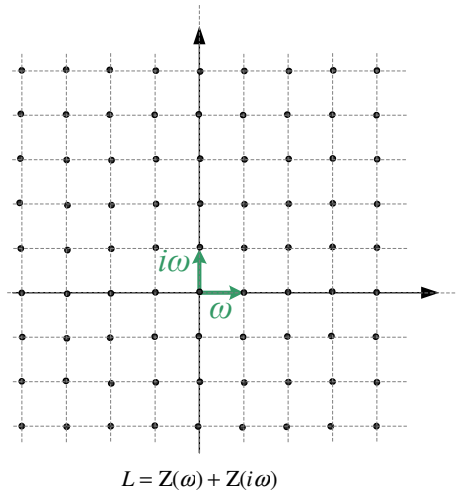


Figure 3.1: Square lattice $L = \mathbb{Z}\omega + \mathbb{Z}i\omega$

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.

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 3.1 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 $\mathbb{C}/L$

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

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 3.2 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 3.3. 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

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

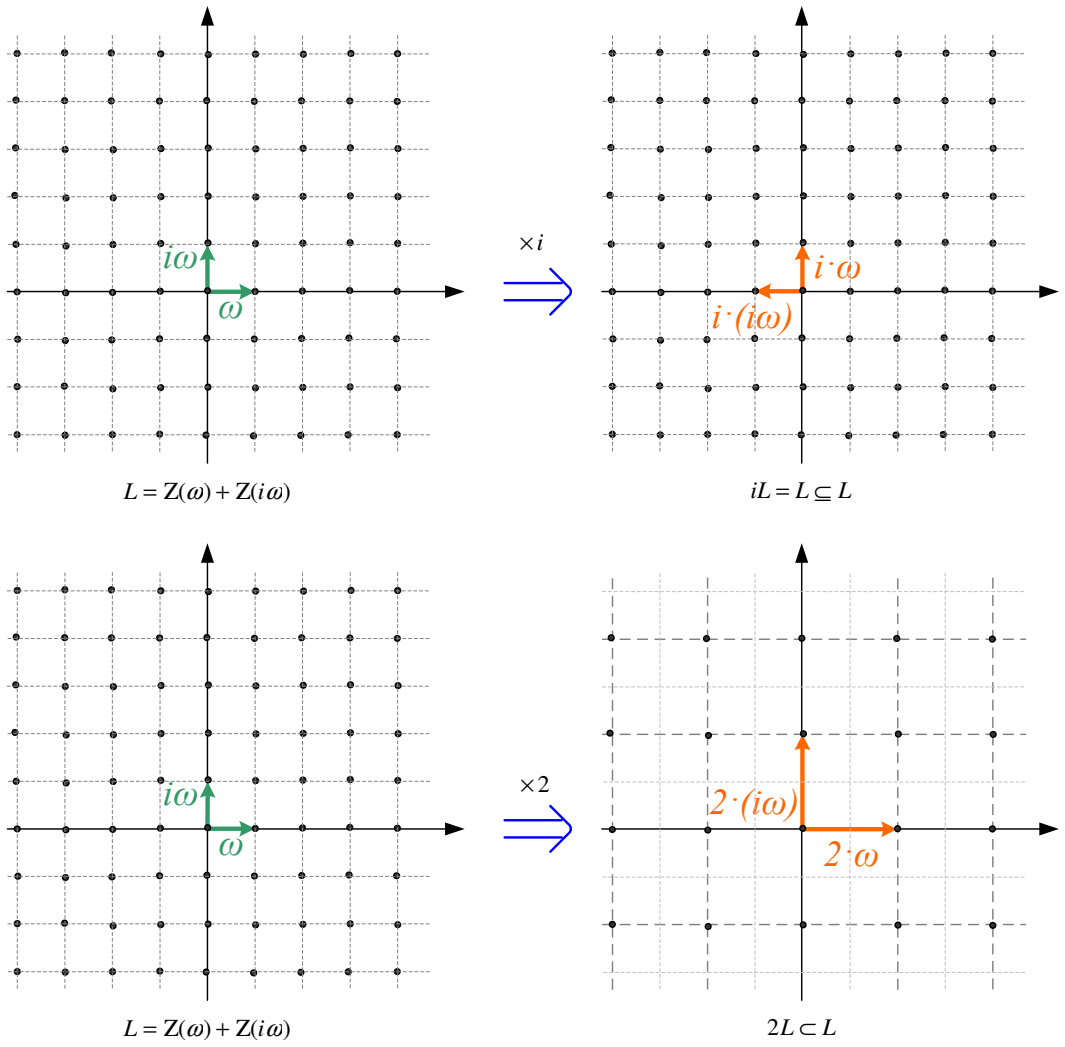


Figure 3.2: Examples of $End_{\mathbb{C}}(E) \simeq \{\beta \in \mathbb{C} | \beta L \subseteq L\}$

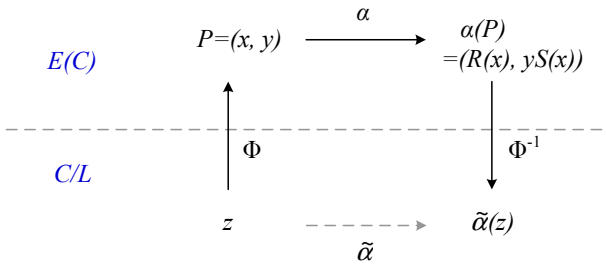


Figure 3.3: The illustration of the morphisms proved of Theorem 3.3 - (1)

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.

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

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

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

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

the map

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

would be an endomorphism of $\mathbb{C}/L$. Figure 3.3 illustrates the relations of these morphisms.

To show that $\tilde{\alpha}(z) = \beta z$ 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

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

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

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

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 **??**, 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:

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

Again, we use Figure 3.4 to show the illustration of the relation between the morphisms proved in this part.

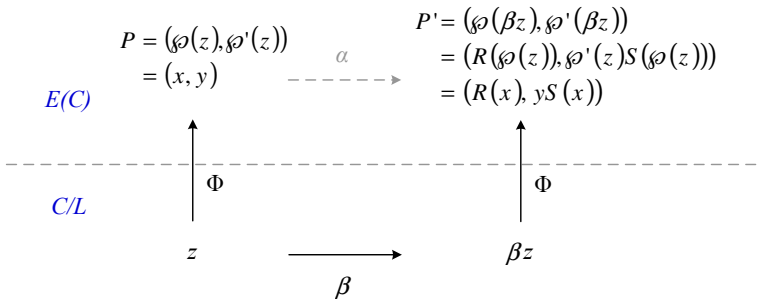


Figure 3.4: The illustration of the morphisms proved of Theorem 3.3 - (2)

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

Theorem 3.3 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 3.4. 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 3.3, 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:

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

   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

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

From Theorem 3.4, 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.

3.3 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 3.5. 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 3.6 (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 3.7 (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 3.8 (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 3.9 (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.

3.4 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 **??**,

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

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 **??**:

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 $G_k(L_\tau) = G_k(\tau)$:

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

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

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

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

we have

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

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

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

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

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

□

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 **??**:

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 **??** and Proposition **??**, 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 3.10. 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 $j\left(\tau_i\right)$ are the j-invariants of corresponding τ_i value.

By Theorem **??**, for an elliptic curve E over $\mathbb{C}$, there is a lattice L_τ such that $E\left(\mathbb{C}\right) \simeq \mathbb{C}/L_\tau$ and $j\left(E\right) = j\left(L_\tau\right) = j\left(\tau\right)$. 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.

3.5 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 3.10, restate the description of Hilbert polynomial first:

Corollary 3.11. 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 $End_{\mathbb{C}}\left(E\right) = \mathcal{O}_K$. Then the minimal polynomial of j_E is the Hilbert class polynomial

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

where $j\left(\tau_i\right)$ 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 $j\left(\tau\right)$, the minimal polynomial of $j\left(\tau\right)$ 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 $H_D\left(x\right)_p$ over $\mathbb{F}_p$.

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

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 3.12. 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 3.13 (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.

3.6 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 3.13),

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

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.

3.7 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 3.14. 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 3.14, 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.

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

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

3.8 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

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

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

Lemma 3.15. 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 3.16. 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 3.16, 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 3.17. 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.