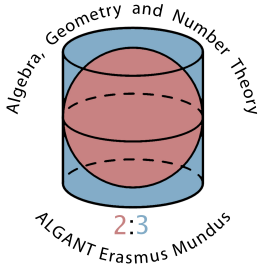


Applications of Complex Multiplication of Elliptic Curves

MASTER THESIS

Candidate:
Massimo CHENAL

Supervisor:
Prof. Jean-Marc COUVEIGNES

UNIVERSITÀ DEGLI STUDI DI PADOVA
Facoltà di Scienze MM. FF. NN.

UNIVERSITÉ BORDEAUX 1
U.F.R. Mathématiques et Informatique

Academic year 2011-2012

Introduction

Elliptic curves represent perhaps one of the most interesting points of contact between mathematical theory and real-world applications. Altough its fundamentals lie in the Algebraic Number Theory and Algebraic Geometry, elliptic curves theory finds many applications in Cryptography and communication security. This connection was first suggested independently by N. Koblitz and V.S. Miller in the late '80s, and many efforts have been made to study it thoroughly ever since.

The goal of this Master Thesis is to study the complex multiplication of elliptic curves and to consider some applications. We do this by first studying basic Hilbert class field theory; in parallel, we describe elliptic curves over a generic field k, and then we specialize to the cases $k = \mathbb{C}$ and $k = \mathbb{F}_p$. We next study the reduction of elliptic curves, we describe the so called Complex Multiplication method and finally we explain Schoof's algorithm for computing point on elliptic curves over finite fields. As an application, we see how to compute square roots modulo a prime p. Explicit algorithms and full-detailed examples are also given.

Thesis Plan

Complex Multiplication method (or CM-method, for short) exploit the so called Hilbert class polynomial, and in Chapter 1 we introduce all the tools we need to define it. Therefore we will describe modular forms and the j-function, and we provide an efficient method to compute the latter. After briefly recalling the basic facts we need from Algebraic Number Theory, we study quadratic forms with a particular emphasis on their relationship with orders in quadratic fields: it is this connection that provide us the algorithm we use to compute Hilbert class polynomials, as shown in Algorithm 3. The main result of Chapter 1, as well as one of the basis of the CM-method, is Theorem 1.5.12 which explore the reduction of the Hilbert class polynomial modulo a prime p and the splitting of p.

In Chapter 2 we introduce the protagonist of our thesis, i.e. elliptic curves. This is done in rather classical way: we define it as a non singular projective curve of genus 1 with a distinguished point, and we show that it can always been written in Weierstrass equation. After the necessary fundamental properties and definitions, we discuss the twists of elliptic curves and we exploit in more depth the ring of endomorphisms. Particular attention will be paid to classification of endomorphism rings.

After studying elliptic curves over a generic field k, it is time to specialize to the case $k = \mathbb{C}$ which will allow us to introduce the idea of complex multiplication; this is material of Chapter 3. We start by taking into account the field of elliptic functions, and we see that this is generated by the particular case of the Weierstrass function $\wp$ and its derivative $\wp'$. We study lattices and their j-invariant, and we see how to classify elliptic curves over the complex numbers. The main results are explained in the last two sections where we explore the structure of the endomorphism ring and the notion of complex multiplication.

The counterpart of the CM-method is based upon the theory of elliptic curves over finite fields: this is where Chapter 4 comes in. The most important arithmetic quantity associated to an elliptic curve defined over a finite field $\mathbb{F}_q$ is its number of rational points. After introducing the Frobenius map, we prove a theorem of Hasse that says that if $E/\mathbb{F}_q$ is an elliptic curve, then $E(\mathbb{F}_q)$ has approximately q points, with an error of no more than $2\sqrt{q}$. We then study the endomorphism ring of an elliptic curve defined over a finite field.

In Chapter 5 we use our previous results and explore the interaction between elliptic curves over finite fields and elliptic curves over $\mathbb{C}$. In particular, given an elliptic curve E over a number field K, we consider the operation of reducing E modulo a prime $\mathfrak{p}$ of $\mathcal{O}_K$ lying above a given rational prime p. A theorem of Deuring says that any elliptic curve over $\mathbb{F}_p$, and with a non-trivial endomorphism, can be considered as the reduction of some elliptic curve over a number field with the same endomorphism ring. As an application of these results, we consider the problem of finding an elliptic curve E over a finite field, such that ring of endomorphisms is given: this is the CM-method, which exploits all the results presented so far. We see also a method of building an elliptic curve over a finite field with a given number of rational points. For the sake of clarity, we provide full-detailed examples and explicit algorithms.

Time for applications of our results has come, and a particular important one is to find an efficient way to compute the number of points of an elliptic curve over a finite field: for instance, in elliptic curve cryptography it is important to know the number of points to judge the difficulty of solving the discrete logarithm problem in the group of points on an elliptic curve. Therefore, in Chapter 6 we present Schoof's deterministic algorithm that computes the number of points in polynomial time.

We end our thesis by showing how to build a deterministic algorithm that compute square roots modulo a prime p: this is an important problem in computational number theory. After considering the cases in which the problem is easily solved ($p \equiv 3, 5, 7 \pmod 8$), we study the hard case in which $p \equiv 1 \pmod 8$. This is a two-part task that use the CM-method as well as Schoof's algorithm.

The following diagram displays graphically the interaction between the topics presented in this thesis.

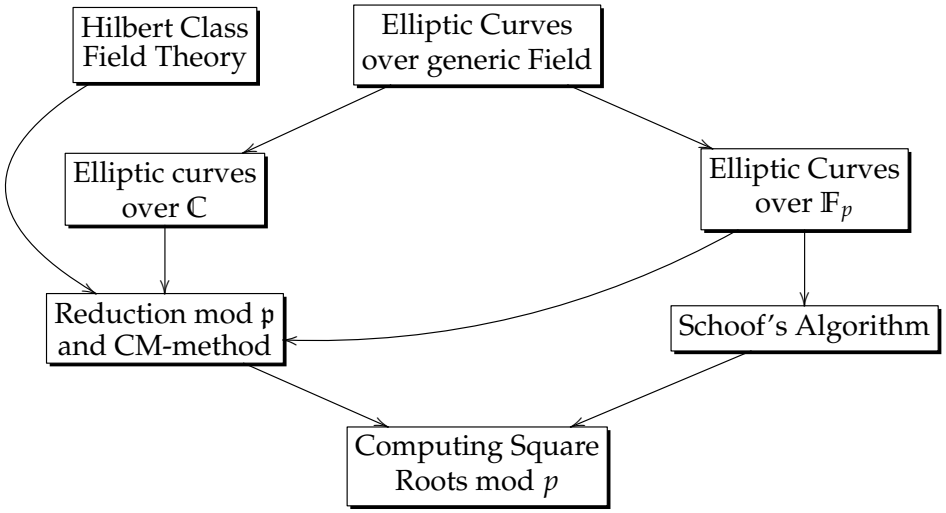


Figure 1: Master Thesis Plan

Contents

Introduction **i**

1 Fundamentals **1**
1.1 Modular Forms and j-function 1
1.2 Algebraic Number Theory 4
1.3 Quadratic Forms 10
1.4 Orders and Quadratic Forms 14
1.5 The Hilbert Class Field 15

2 The Geometry of Elliptic Curves **20**
2.1 Definition and First Properties 21
2.2 The Group Law 28
2.3 Getting The Weierstrass Equation 30
2.4 The Ring of Endomorphisms 31
2.5 Classification of Endomorphism Rings 34

3 Elliptic Curves over $\mathbb{C}$ **35**
3.1 Lattices and Bases 35
3.2 Elliptic Functions 36
3.3 The Weierstrass Function 38
3.4 The Field of Doubly Periodic Functions 41
3.5 The j-invariant of a Lattice 45
3.6 Quotients of $\mathbb{C}$ by Lattices 47
3.7 The Holomorphic Maps $\mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ 47
3.8 The Elliptic Curve $E(\Lambda)$ 48
3.9 Classification of Elliptic Curves over $\mathbb{C}$ 50
3.10 The Structure of the Endomorphism Ring 51
3.11 Complex Multiplication 53

4 Elliptic Curves Over Finite Fields **56**
4.1 The Frobenius Map 56
4.2 The Trace of the Frobenius Map 60
4.3 The Endomorphism Ring 64

5 Reduction modulo $\mathfrak{p}$ and CM method **67**
5.1 Reduction of an Elliptic Curve modulo p 67
5.2 A theorem of Deuring 68
5.3 The Complex Multiplication Method 72
5.4 Examples 74
5.5 Building the Hilbert Class Polynomial 76
5.6 CM Method - Alternative 84

6 Schoof's Algorithm **87**
6.1 Motivation 87
6.2 The Setup and the Naive Method 88
6.3 The Idea Behind the Algorithm 89
6.4 The Complexity 92
6.5 The Division Polynomials 93
6.6 Algorithm Implementation 95
6.7 Putting all Together 99
6.8 Improvements 99

7 Computing Square Roots in Finite Fields **101**
7.1 The First Case 102
7.2 The Second Case 102

A Appendix **106**
A.1 Algorithm for Fast Exponentiation 106

References **108**

CHAPTER 1

Fundamentals

Abstract

We start by recalling and discussing the tools that we will need later on: topics will cover modular forms, ramification theory, orders and quadratic forms. This will enable us to introduce the Hilbert class field and the Hilbert class polynomial, which will be useful in later chapters. Since this is just some preparing material for our main topics of elliptic curves and complex multiplication, proofs will be in general omitted and references will be given.

1.1 Modular Forms and j-function

We start by considering the special linear group $\mathrm{SL}_2(\mathbb{Z})$, that is the group of all 2×2 matrices with determinant 1 and integer coefficients

$$\mathrm{SL}_2(\mathbb{Z}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}$$

An element $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ of $\mathrm{SL}_2(\mathbb{Z})$ acts on a complex number z by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az + b}{cz + d}$$

Remark 1.1.1. The quotient $\Gamma := \mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$ is called the *modular group* (observe that $\{\pm I\}$ is the center of $\mathrm{SL}_2(\mathbb{Z})$). This is also referred to as $\mathrm{SL}_2(\mathbb{Z})$, the *special linear group*.

Let $\mathcal{H} := \{\alpha \in \mathbb{C} \mid \mathrm{Im}(\alpha) > 0\}$ be the upper half complex plane.

Definition 1.1.2. Let $k \in \mathbb{Z}$. A *modular form of weight* $2k$ is a function f meromorphic everywhere on $\mathcal{H} \cup \{\infty\}$, and such that $\forall z \in \mathcal{H}$, $\forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, we have

$$f(z) = (cz + d)^{-2k} f\left(\frac{az + b}{cz + d}\right)$$

If the form is holomorphic everywhere (which implies $k > 0$ for non-constant forms), we say that the form is *regular*.

A modular form of weight 0 is called a *modular function*.

In Chapter 3 we will introduce the notion of a lattice L and we will define its j-invariant $j(L)$.

1.1.1 The j-function

For our purposes, following [1], we anticipate some details here. Let $\tau \in \mathcal{H}$ and consider the lattice $L := \mathbb{Z} + \mathbb{Z}\tau := [1, \tau]$. Put

$$G_{2k}(L) = \sum_{(m,n)\neq(0,0)} \frac{1}{(m\tau + n)^{2k}}$$

for $k > 1$; in this case $G_{2k}(L)$ is a regular modular form of weight $2k$. We put

$$g_2(L) = 60G_4 \quad g_2(L) = 140G_6$$
$$\Delta = g_2^3 - 27g_3^2 \qquad j = 12^3 \frac{g_2^3}{\Delta}$$

g_2, g_3 and Δ are regular modular forms of weight 4,6 and 12 respectively. The *modular invariant* is defined to be j.

Remark 1.1.3. For $\tau \in \mathcal{H}$, we put $j(\tau) := j(L)$.

The main properties of the j-function are given by the following result [1, Proposition 3.1].

Proposition 1.1.4. *The j-function is a modular function, holomorphic in $\mathcal{H}$, and has a simple pole at infinity.*

It follows that $j(\tau)$ is invariant under $\mathrm{SL}_2(\mathbb{Z})$. Therefore we see that

$$j(\tau + 1) = j\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \tau\right) = j(\tau)$$

This implies that $j(\tau)$ is a holomorphic function in $q = q(\tau) = e^{2\pi i \tau}$, defined in the region $0 < |q| < 1$. Consequently, $j(\tau)$ has a Laurent expansion

$$j(\tau) = \sum_{-\infty}^{+\infty} c_n q^n$$

which is called the *q-expansion* of $j(\tau)$. The following theorem will be important in following chapters.

Theorem 1.1.5. *The q-expansion of $j(\tau)$ is given by*

$$j(\tau) = \frac{1}{q} + 744 + 196884q + \cdots = \frac{1}{q} + \sum_{n=0}^{\infty} c_n q^n \tag{1.1}$$

where $\tau \in \mathcal{H}$ and $c_n \in \mathbb{Z}\ \forall n >= 0$

Proof. See [4, §4.1]. □

Remark 1.1.6. In the future it will be of particular interest being able to compute efficiently the values of $j(\tau)$. For this purpose, we end this section on modular forms by describing a method of computing the complex values $j(\tau)$.

1.1.2 A method to compute $j(\tau)$

We will follow ideas from [3, §12.B]. There are basically two ways to compute $j(\tau)$, either by using the expansion 1.1, or by computing $j(\tau)$ in terms of the Dedekind η-function. This is a modular form defined by

$$\eta(\tau) = q^{1/24} \prod_{m=1}^{\infty} (1 - q^m)$$

where $q = e^{2\pi\tau}$. Since $0 < |q| < 1$, this product converges for any $\tau \in \mathcal{H}$. By Euler's identity we have

$$\prod_{m=1}^{\infty} (1 - q^m) = \sum_{m=-\infty}^{+\infty} q^{m(3m+1)/2}$$

this product can be expanded as follows

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

Now, the η-function satisfies the functional equations

$$\eta(\tau + 1) = \zeta_{24}\eta(\tau), \quad \eta(-\tau^{-1}) = \sqrt{-i\tau}\eta(\tau)$$

where ζ_{24} is the 24-th root of unity in $\mathbb{C}$. If we let $\Delta(\tau)$ be the discriminant of L, we have

$$\Delta(\tau) = (2\pi)^{12}\eta(\tau)^{24}$$

Therefore, we can compute $j(\tau)$ as

$$j(\tau) = \frac{(256f(\tau) + 1)^3}{f(\tau)}, \quad \text{where } f(\tau) := \frac{\Delta(2\tau)}{\Delta(\tau)} \tag{1.2}$$

1.2 Algebraic Number Theory

1.2.1 Basic tools

We quickly recall some basic notions from algebraic number theory. Further details and proofs can be found, for instance, in [3, §5].

We define a *number field* K to be a subfield of the complex numbers $\mathbb{C}$ for which $[K : \mathbb{Q}] < \infty$, where $[K : \mathbb{Q}]$ denotes the degree of K over $\mathbb{Q}$. Given such a field K, we let $\mathcal{O}_K$ denote the algebraic integers of K, i.e., the set of all $\alpha \in K$ which are roots of a monic integer polynomial. It is known that $\mathcal{O}_K$ is a subring of $\mathbb{C}$ whose field of fractions is K, and it is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$. We will often call $\mathcal{O}_K$ the *ring of integers* or the *number ring* of K.

If $\mathfrak{a}$ is a nonzero ideal of $\mathcal{O}_K$, then the quotient ring $\mathcal{O}_K/\mathfrak{a}$ is finite. Given a nonzero ideal $\mathfrak{a}$ of the number ring $\mathcal{O}_K$, its *norm* is defined to be $N(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$, which is of course finite.

In general, the rings $\mathcal{O}_K$ are not UFDs (unique factorization domains) but they are *Dedekind domains*:

Theorem 1.2.1. *Let $\mathcal{O}_K$ be the ring of integers in a number field K. Then $\mathcal{O}_K$ is a Dedekind domain, which means that*

(i) $\mathcal{O}_K$ is integrally closed in K, i.e. if $\alpha \in K$ satisfies a monic polynomial with coefficients in $\mathcal{O}_K$, then $\alpha \in \mathcal{O}_K$.

(ii) $\mathcal{O}_K$ is Noetherian, i.e., given any chain of ideals $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots$, there is an integer n such that $\mathfrak{a}_n = \mathfrak{a}_{n+1} = \cdots$

(iii) Every nonzero prime ideal of $\mathcal{O}_K$ is maximal.

The most important property of a Dedekind domain is that it has unique factorization at the level of ideals. More precisely, any nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$ can be written as a product

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$$

of prime ideals, and the decomposition is unique up to order. Furthermore, the $\mathfrak{p}_i$'s are exactly the prime ideals of $\mathcal{O}_K$ containing $\mathfrak{a}$.

When $\mathfrak{p}$ is a prime of K, the quotient ring $\mathcal{O}_K/\mathfrak{p}$ is a finite field by Theorem 1.2.1. This field is called the *residue field* of $\mathfrak{p}$.

Besides ideals of $\mathcal{O}_K$, we will also use *fractional ideals*, which are the nonzero finitely generated $\mathcal{O}_K$-submodules of K. Such an ideal can be written in the form $\alpha\mathfrak{a}$, where $\alpha \in K$ and $\mathfrak{a}$ is an ideal of $\mathcal{O}_K$. The basic properties of fractional ideals are given by the following

Proposition 1.2.2. *Let $\mathfrak{a}$ be a fractional $\mathcal{O}_K$-ideal.*

(i) $\mathfrak{a}$ is invertible, i.e., there is a fractional $\mathcal{O}_K$-ideal $\mathfrak{b}$ such that $\mathfrak{ab} = \mathcal{O}_K$. The ideal $\mathfrak{b}$ will be denoted $\mathfrak{a}^{-1}$.

(ii) $\mathfrak{a}$ can be written uniquely as a product $\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{r_i}$, where $r_i \in \mathbb{Z}$ and the $\mathfrak{p}_i$'s are distinct prime ideals of $\mathcal{O}_K$.

We will let I_K denote the set of all fractional ideals of K. I_K is closed under multiplication of ideals, and then part (i) of Proposition 1.2.2 shows that I_K is a group. A particular important subgroup of I_K is the subgroup P_K of principal fractional ideals, i.e., those of the form $\alpha\mathcal{O}_K$ for some $\alpha \in K^*$.

Definition 1.2.3. We define the *ideal class group* as the quotient $C(\mathcal{O}_K) := I_K/P_K$. Its cardinality $h = |C(\mathcal{O}_K)|$ is called the *class number*.

Remark 1.2.4. An important result is that $h < \infty$, i.e. $C(\mathcal{O}_K)$ is a finite group.

1.2.2 Ramification theory

We next consider *ramification*, which is concerned with the behaviour of primes in finite extensions. Suppose that K is a number field, and let L be a finite extension of K. If $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$, then $\mathfrak{p}\mathcal{O}_L$ is an ideal of $\mathcal{O}_L$, and hence has a prime factorization

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$$

where the $\mathfrak{P}_i$'s are the distinct primes of L containing $\mathfrak{p}$. The integer e_i, also written $e_{\mathfrak{P}_i|\mathfrak{p}}$, is called the *ramification index* of $\mathfrak{p}$ in $\mathfrak{P}_i$. Each prime $\mathfrak{P}_i$ containing $\mathfrak{p}$ also gives a residue field extension $\mathcal{O}_K/\mathfrak{p} \subset \mathcal{O}_L/\mathfrak{P}_i$, and its degree, written f_i or $f_{\mathfrak{P}_i|\mathfrak{p}}$, is the *inertial degree* of $\mathfrak{p}$ in $\mathfrak{P}_i$. The basic relation between the e_i's and f_i's is given by

$$\sum_{i=1}^{g} e_i f_i = [L : K] \tag{1.3}$$

In the above situation, we say that a prime $\mathfrak{p}$ of K *ramifies* in L if any of the ramification indices e_i are greater than 1. It can be proved that only a finite number of primes of K ramify in L.

If $K \subset L$ is a Galois extension, the above description can be simplified as follows:

Theorem 1.2.5. *Let $K \subset L$ be a Galois extension, and let $\mathfrak{p}$ be prime in K.*

(i) The Galois group $Gal(L/K)$ acts transitively on the primes of L containing $\mathfrak{p}$, i.e. if $\mathfrak{P}$ and $\mathfrak{P}'$ are primes of L containing $\mathfrak{p}$, then $\exists \sigma \in Gal(L/K)$ such that $\sigma(\mathfrak{P}) = \mathfrak{P}'$.

(ii) *The primes* $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ *of* L *containing* $\mathfrak{p}$ *all have the same ramification index* e *and the same inertial degree* f*, and the relation 1.3 becomes*

$$efg = [L : K]$$

Definition 1.2.6. Given a Galois extension $K \subset L$, an ideal $\mathfrak{p}$ of K *ramifies* if $e > 1$, and is *unramified* if $e = 1$. If $\mathfrak{p}$ satisfies the stronger condition $e = f = 1$, we say that $\mathfrak{p}$ *splits completely* in L. If $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$, we say that the prime $\mathfrak{P}$ lies *above* $\mathfrak{p}$.

A prime $\mathfrak{p}$ that splits completely is of course unramified, and in addition $\mathfrak{p}\mathcal{O}_L$ is the product of $[L : K]$ distinct primes, the maximum number allowed by Theorem 1.2.5. The extension L is determined uniquely by the primes of K that split completely in L.

The following proposition will help us decide when a prime is unramified or split completely in a Galois extension:

Proposition 1.2.7. *Let* $K \subset L$ *be a Galois extension, where* $L = K(\alpha)$ *for some* $\alpha \in \mathcal{O}_K$*. Let* $f(x)$ *be the monic minimal polynomial of* α *over* K*, so that* $f(x) \in \mathcal{O}_K$*. If* $\mathfrak{p}$ *is prime in* $\mathcal{O}_K$ *and* $f(x)$ *is separable modulo* $\mathfrak{p}$*, then*

(i) $\mathfrak{p}$ *is unramfied in* L

(ii) *If* $f(x) \equiv f_1(x) \cdots f_g(x)$ *mod* $\mathfrak{p}$*, where the* $f_i(x)$ *are distinct and irreducible modulo* $\mathfrak{p}$*, then* $\mathfrak{P}_i = \mathfrak{p}\mathcal{O}_L + f_i(\alpha)\mathcal{O}_L$ *is a prime ideal of* $\mathcal{O}_L$*,* $\mathfrak{P}_i \neq \mathfrak{P}_j$ *for* $i \neq j$*, and*

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_g$$

(splits completely). Furthermore, all of the $f_i(x)$ *have the same degree, which is the inertial degree* f*.*

(iii) $\mathfrak{p}$ *splits completely in* L *if and only if* $f(x) \equiv 0$ *mod* $\mathfrak{p}$ *has a solution in* $\mathcal{O}_K$*.*

1.2.3 Quadratic Fields

In our discussion, we will mostly consider field extensions of degree 2, called *quadratic extensions*. Such fields can be written uniquely in the form $K = \mathbb{Q}(\sqrt{N})$, where $N \neq 0, 1$ is a squarefree integer. The basic invariant of K is its *discriminant* d_K, which is defined to be

$$d_K = \begin{cases} N & \text{if } N \equiv 1 \bmod 4 \\ 4N & \text{otherwise} \end{cases}$$

Note that $d_K \equiv 0, 1 \bmod 4$ and $K = \mathbb{Q}(\sqrt{d_K})$, so that a quadratic field is determined by its discriminant.

We have

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{d_K + \sqrt{d_K}}{2}\right]$$

We now describe units and primes (ideals) of K: let's first consider units.

Quadratic fields can be either real ($d_K > 0$) or imaginary ($d_K < 0$), and the units $\mathcal{O}_K^*$ behave quite differently in the two cases.

$d_K < 0$ In the imaginary case, there are only finitely many units. The group of units $\mathcal{O}_K^*$ for $K = \mathbb{Q}(\sqrt{-3})$ and $K = \mathbb{Q}(i)$ are given, respectively, by $\{\pm 1, \pm\omega, \pm\omega^2\}$ and $\{\pm 1, \pm i\}$ (where $\omega = e^{2\pi/3}$). For all other imaginary quadratic fields it turns out that $\mathcal{O}_K^* = \{\pm 1\}$.

$d_K > 0$ Real quadratic fields always have infinitely many units, and determining them is related to Pell's equation and continued fractions. We shall not discuss this subject any further.

Remark 1.2.8. For future references, we collect these results in a compact form. Let $D < 0$ be a fundamental discriminant (Definition 1.4.1) and let $\mathcal{O}_K$ be the ring of integers $K = \mathbb{Q}(\sqrt{D})$ ($\mathcal{O}_K$ is the unique quadratic order of discriminant D). Then the group of units $\mathcal{O}_K^*$ has cardinality $\rho(D)$ given by

$$\rho(D) = \begin{cases} 2 & \text{if } D < -4 \\ 4 & \text{if } D = -4 \\ 6 & \text{if } D = -3 \end{cases}$$

and the group of units in $\mathcal{O}_K$ is equal to the $\rho(D)$-th roots of unity in K.

Before describing the primes of $\mathbb{O}_K$, we introduce the following notation: if $D \equiv 0, 1 \bmod 4$, then the *Kronecker symbol* is defined by

$$\left(\frac{D}{2}\right) = \begin{cases} 0 & \text{if } D \equiv 0 \bmod 4 \\ 1 & \text{if } D \equiv 1 \bmod 8 \\ -1 & \text{if } D \equiv 5 \bmod 8 \end{cases}$$

(if $p \neq 2$, the notation (d/p) is the usual Legendre symbol). We will most often apply this when $D = d_K$ is the discriminant of a quadratic field K. The following proposition tells us about the primes of quadratic fields:

Proposition 1.2.9. *Let K be a quadratic field of discriminant d_K, and let the non-trivial automorphism of K be denoted $\alpha \mapsto \alpha'$. Let p be prime in $\mathbb{Z}$.*

(i) If $(d_K/p) = 0$ (i.e. $p | d_K$), then $p\mathcal{O}_K$ ramifies as $p\mathcal{O}_K = \mathfrak{p}^2$ for some prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$

(ii) If $(d_K/p) = 1$ (i.e. the congruence $x^2 \equiv d_K \bmod p$ has a solution), then $p\mathcal{O}_K$ splits as the product of two distinct ideals in $\mathcal{O}_K$, i.e. $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$, where $\mathfrak{p} \neq \mathfrak{p}'$ are primes in $\mathcal{O}_K$.

(iii) If $(d_K/p) = -1$, then $p\mathcal{O}_K$ is inert, i.e. it is still a prime in $\mathcal{O}_K$.

Furthermore the primes in (i)-(iii) above give all nonzero primes of $\mathcal{O}_K$.

Remark 1.2.10. An important fact, as we shall see better in Theorem 1.5.12, is that the equation $p = N(\pi)$ has a solution in $\mathcal{O}_K$ if and only if (p) splits as the product of two principal ideals in K.

From this proposition, we get the following immediate corollary which tells us how primes of $\mathbb{Z}$ behave in a quadratic extension:

Corollary 1.2.11. *Let K be a quadratic field of discriminant d_K, and let p be an rational prime. Then:*

(i) p ramifies in K if and only if p divides d_K.

(ii) p splits completely in K if and only if $(d_K/p) = 1$.

We now consider in detail the way in which primes $p \in \mathbb{Z}$ split in quadratic fields. This will be useful when computing explicitly reduction of elliptic curves in Chapter 5, and in particular in Example 5.6.3. Let $K = \mathbb{Q}(\sqrt{d})$, d square-free, and consider the ring of integers $\mathcal{O}_K$. Then we have the following theorem

Theorem 1.2.12. *With notation as above, we have*

- *if $p \mid d$, then $p\mathcal{O}_K = (p, \sqrt{d})$*
- *if d is odd, then*

$$2\mathcal{O}_K = \begin{cases} (2, 1+\sqrt{d})^2 & \text{if } d \equiv 3 \pmod 4 \\ \left(2, \frac{1+\sqrt{d}}{2}\right)\left(2, \frac{1-\sqrt{d}}{2}\right) & \text{if } d \equiv 1 \pmod 8 \\ \text{prime} & \text{if } d \equiv 5 \pmod 8 \end{cases}$$

- *if p is odd and $p \nmid d$ then*

$$p\mathcal{O}_K = \begin{cases} (p, n+\sqrt{d})(p, n-\sqrt{d}) & \text{if } d \equiv n^2 \pmod p \\ \text{prime} & \text{if } d \text{ is not a square mod } p \end{cases}$$

1.2.4 Orders in Imaginary Quadratic Fields

What we have said for $\mathcal{O}_K$ can be extended in more generality to orders in a quadratic field K. But, unlike $\mathcal{O}_K$, an order $\mathcal{O}$ is usually not a Dedekind domain. A fact that will be important later is that, in the case of imaginary quadratic fields, there is a nice relation between ideals in orders and quadratic forms (to be defined later in Section 1.3). In particular, an order $\mathcal{O}$ has an ideal class group $C(\mathcal{O})$, and for any discriminant $D < 0$, the form class group $C(D)$ (Definition 1.4.3) is naturally isomorphic to $C(\mathcal{O})$ for a suitable order $\mathcal{O}$.

So an order $\mathcal{O}$ in a quadratic field K is defined to be a subset $\mathcal{O} \subset K$ such that it is a subring of K containing 1, it is a finitely generated $\mathbb{Z}$-module and contains a $\mathbb{Q}$-basis of K.

$\mathcal{O}$ is a free $\mathbb{Z}$-module of rank 2. The ring $\mathcal{O}_K$ is always an order in K, and for any order $\mathcal{O}$ of K, we have $\mathcal{O} \subset \mathcal{O}_K$, so that $\mathcal{O}_K$ is the *maximal order* of K. If we write $\mathcal{O}_K = [1, w_K]$, where $w_K = \frac{d_K + \sqrt{d_K}}{2}$ and d_K is the discriminant of K, then setting $f = [\mathcal{O}_K : \mathcal{O}]$ we have $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K = [1, w_K]$. The index $f = [\mathcal{O}_K : \mathcal{O}]$ is called the *conductor* of the order.

Remark 1.2.13. Let $\alpha \mapsto \alpha'$ be the non-trivial automorphism of K, and suppose that $\mathcal{O} = [\alpha, \beta]$. Then the *discriminant* of $\mathcal{O}$ is the number

$$D = \left(\det \begin{pmatrix} \alpha & \beta \\ \alpha' & \beta' \end{pmatrix} \right)^2$$

The discriminant is independent of the integral basis used, and if we compute D using the basis $\mathcal{O} = [1, fw_K]$ we obtain the formula

$$D = f^2 d_K$$

Thus the discriminant satisfies $D \equiv 0, 1 \bmod 4$.

Remark 1.2.14. We can define in a similar way the norm of an ideal, the proper and fractional ideals of an order, and the class group $C(\mathcal{O})$ of the order $\mathcal{O}$. For further details, see [3].

Remark 1.2.15. Sometimes it is useful to compute the class number $h(d_K)$ for a given discriminant d_K. This is not always easy to compute, and a number of tricks have been developed to estimate this. It is interesting to study how $h(d_K)$ grows as $|d_K|$ gets large. The best result is due to Siegel, who proved in 1935 that

$$\lim_{d_K \to -\infty} \frac{\log h(d_K)}{\log |d_K|} = \frac{1}{2} \tag{1.4}$$

This implies that, for all $\epsilon > 0$, there exists a constant $C(\epsilon)$ such that

$$h(d_K) > C(\epsilon) |d_K|^{(1/2)-\epsilon}$$

for all field discriminants $d_K < 0$.

We conclude this section with the following result.

Theorem 1.2.16. *(i) If K is an imaginary quadratic field of discriminant d_K, then*

$$h(d_K) = 1 \Leftrightarrow d_K = -3, -4, -7, -8, -11, -19, -43, -67, -163$$

(ii) If $D \equiv 0, 1$ mod 4, then

$$\begin{aligned} h(D) = 1 \Leftrightarrow D \quad = \quad & -3, -4, -7, -8, -11, -12, -16, \\ & -19, -27, -28, -43, -67, -163 \end{aligned}$$

1.3 Quadratic Forms

Definition 1.3.1. A *binary quadratic form* f is a function

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

where $a, b, c \in \mathbb{Z}$. We will denote it more briefly as $[a,b,c]$. We say that f is *primitive* if $gcd(a,b,c) = 1$; if moreover f satisfies the condition

$$|b| \leq a \leq c \text{ and } b \geq 0 \text{ whenever } |b| = a \text{ or } a = c \tag{1.5}$$

we say that f is *reduced*.

The *discriminant* of $[a,b,c]$ is given by $D := b^2 - 4ac$.

To each quadratic form $F = [a,b,c]$ we associate a matrix

$$M(F) := \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$$

This allows us to define an equivalence relation: two forms F and F' of the same discriminant are equivalent, and we write $F \sim F'$ if there exists $A \in \mathrm{SL}_2(\mathbb{Z})$ such that

$$M(F') = A^{-1}M(F)A$$

Remark 1.3.2. We will now define the reduced quadratic forms in an alternative way. This will enable us to compute the class number in quadratic orders by means of reduced quadratic forms.

Let $f(x,y) = ax^2 + bxy + cy^2$ be a quadratic form and denote by τ the root of $f(x,1)$ in the upper half plane $\mathcal{H} = \{\tau \in \mathbb{C} \mid \mathrm{Im}(\tau) > 0\}$, i.e.

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

Then the quadratic form $[a,b,c]$ is reduced if $\tau \in \mathcal{D}$, where $\mathcal{D}$ is the domain

$$\begin{aligned} \mathcal{D} : &= \mathcal{D}_1 \cup \mathcal{D}_2 \quad \text{with} \\ \mathcal{D}_1 &= \{\tau \in \mathcal{H} \mid \mathrm{Re}(\tau) \in [-\frac{1}{2}, \frac{1}{2}[, |\tau| > 1\} \\ \mathcal{D}_2 &= \{\tau \in \mathcal{H} \mid \mathrm{Re}(\tau) \in [-\frac{1}{2}, 0], |\tau| = 1\} \end{aligned}$$

Remark 1.3.3. As $\tau \in \mathcal{H}$, we see that $j(\tau)$ is well-defined. When the context is clear, we write $j([a,b,c])$ to mean $j\left(\frac{-b+\sqrt{D}}{2a}\right)$.

Definition 1.3.4. For any quadratic number $\tau \in \mathcal{H}$ we define the *discriminant* of τ as the discriminant of the unique primitive positive definite quadratic form $[a,b,c]$ such that τ is a root of $ax^2 + bx + c = 0$.

The equivalent definition of the reduced quadratic form enable us to consider the following proposition:

Proposition 1.3.5. *In every class of positive definite quadratic forms of discriminant $D < 0$ there exists exactly one reduced form.*

For the proof, see [2, §5.3]. We also have the following fact:

Fact 1.3.6. Let $f = [a, b, c]$ be a positive definite binary quadratic form of discriminant $D = b^2 - 4ac < 0$.

(i) If f is reduced, we have the inequality

$$a \leq \sqrt{\frac{|D|}{3}}$$

(ii) Conversely, if

$$a < \sqrt{\frac{|D|}{4}} \text{ and } -a < b \leq a$$

then f is reduced.

Proof. (i) If f is reduced, then

$$|D| = 4ac - b^2 \geq 4a^2 - a^2, \text{ which implies } a \leq \sqrt{\frac{|D|}{3}}$$

(ii) We have

$$c = \frac{b^2 + |D|}{4a} \geq \frac{|D|}{4a} > \frac{a^2}{a} = a$$

therefore f is reduced.

□

In the following section we will discuss the relationship between orders and quadratic forms. We set up the situation by considering the set $C(D)$ of reduced quadratic forms of discriminant D, and let $h(D) = |C(D)|$. Thanks to condition 1.5, we have that $h(D) < \infty$. The set $C(D)$ can be given the structure of an abelian group, under multiplication given by compostition of equivalence classes. The inverse of the class of $[a, b, c]$ in $C(D)$ is the class of $[a, -b, c]$.

Definition 1.3.7. A form is *ambiguous* if it has order 2.

An ambiguous binary quadratic form is one of $[a, 0, c]$, $[a, a, c]$, $[a, b, a]$.

Remark 1.3.8. We will see that $h(D) = h(\mathcal{O}_K)$ where $K = \mathbb{Q}(\sqrt{D})$. We deduce that when $D < 0$ the class number $h(D)$ of $\mathbb{Q}(\sqrt{D})$ can be obtained simply by counting reduced forms of discriminant D (since in that case all forms of discriminant D are primitive), using the inequalities $|b| \leq a \leq \sqrt{|D|/3}$. This leads to the following algorithm, that outputs the class number $h(D)$ of quadratic forms of fundamental discriminant $D < 0$. It will be useful when discussing an algorithm for building Hilbert class polynomials (see Algorithm 3).

Algorithm 1 Class number $h(D)$ for quadratic forms of fund. disc. $D < 0$

$h := 1$;
$b := D \pmod 2$;
$B := \lfloor \sqrt{|D|/3} \rfloor$;
repeat
  $q := (b^2 - D)/4$;
  $a := b$;
  if $a \leq 1$ **then**
    $a := 2$;
  end if
  repeat
    if $a \mid q$ **then**
      if $a = b$ or $a^2 = b$ or $b = 0$ **then**
        $h := h + 1$;
      else
        $h := h + 2$;
      end if
    end if
    $a := a + 1$;
  until $a^2 > q$
  $b := b + 2$;
until $b > B$
return h

The following algorithm determines all reduced forms for a fundamental discriminant $-D$.

Algorithm 2 Computing all reduced forms of fund. disc. $-D$

$r := \left\lfloor \sqrt{\frac{D}{3}} \right\rfloor$;
$b := D \pmod 2$;
while $b \leq r$ **do**
  $m := \frac{b^2+D}{4}$;
  for $a \mid m$ and $a \leq \lfloor \sqrt{m} \rfloor$ **do**
    $c := \frac{m}{a}$;
    if $b \leq a$ **then**
      if $b = a$ or $c = a$ **then**
        store $[a, b, c]$;
      else
        store $[a, \pm b, c]$;
      end if
    end if
  end for
  $b := b + 2$;
end while

1.4 Orders and Quadratic Forms

References: [3, §7.B]

Definition 1.4.1. An integer D is called a *fundamental discriminant* if one of the following statements holds

- $D \equiv 1 \pmod 4$ and D is square-free, or
- $D = 4m$, where $m \equiv 2 \pmod 4$ or $m \equiv 3 \pmod 4$ and m is square-free.

Remark 1.4.2. Unless otherwise noted, in this section we write D to mean a negative fundamental discriminant.

Definition 1.4.3. Let $C(D)$ be the set of the classes of primitive quadratic forms of discriminant D. We call such a set the *form class group*.

We relate now the ideal class group $C(\mathcal{O})$ of Definition 1.2.3 to the form class group $C(D)$ as follows.

Theorem 1.4.4. *Let $\mathcal{O}$ be the order of discriminant D in an imaginary quadratic field K.*

(i) If $f(x,y) = ax^2 + bxy + cy^2$ is a primitive positive definite quadratic form of discriminant D, then

$$[a, (-b + \sqrt{D})/2] := \{ma + n(-b + \sqrt{d_K})/2 : m, n \in \mathbb{Z}\}$$

is a proper ideal of $\mathcal{O}$.

(ii) The map sending $f(x,y)$ to $[a, (-b + \sqrt{D})/2]$ induces an isomorphism $C(D) \simeq C(\mathcal{O})$ between the form class group $C(D)$ and the ideal class group $C(\mathcal{O})$.

Hence the order of $C(\mathcal{O})$ is the class number $h(D)$.

(iii) A positive integer m is represented by a form $f(x,y)$ if and only if m is the norm $N(\mathfrak{a})$ of some ideal $\mathfrak{a}$ in the corresponding ideal class in $C(\mathcal{O})$ (recall that $N(\mathfrak{a} = |\mathcal{O}/\mathfrak{a}|)$).

Remark 1.4.5. Because of the isomorphism $C(D) \simeq C(\mathcal{O})$, we will sometimes write the class number as $h(\mathcal{O})$ instead of $h(D)$.

1.5 The Hilbert Class Field

References: [1] The Hilbert class field of a number field K is the maximal unramified Abelian extensions of K. Let's see what this means.

We start by saying that an extension $K \subset L$ is *Abelian* if it is Galois and $\mathrm{Gal}(L/K)$ is an Abelian group. Now, prime ideals of $\mathcal{O}_K$ are often called *finite primes* to distinguish them from the *infinite primes*, which are determined by the embeddings of K into $\mathbb{C}$. A *real infinite prime* is an embedding $\sigma : K \to \mathbb{R}$, while a *complex infinite prime* is a pair of complex conjugate embeddings $\sigma, \overline{\sigma} : K \to \mathbb{C}$, with $\sigma \neq \overline{\sigma}$. Given an extension $K \subset L$, an infinite prime σ of K *ramifies* in L provided that σ is real but it has an extension to L which is complex. An extension $K \subset L$ is *unramified* if it is unramified at all primes, finite or infinite.

Remark 1.5.1. This is a very strong restriction, and yet it may happen that a given field has unramified extensions of arbitrarily high degree. This is the case, for instance, of $K = \mathbb{Q}(\sqrt{-2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13})$.

The following Theorem lead the way to the definition of Hilbert class fields.

Theorem 1.5.2. *Given a number field K, there is a finite Galois extension L of K such that:*

(i) L is an unramified Abelian extension of K.

(ii) Any unramified Abelian extension of K lies in L.

Definition 1.5.3. The field L of Theorem 1.5.2 is called the *Hilbert class field* of K. It is the maximal unramified Abelian extension of K and is clearly unique.

For the Hilbert class field of K we use notation K_H. The following result [1, Theorem 3.1] relates the Hilbert class field to values of the j-function at points in the upper half complex plane $\mathcal{H}$. It serves also as introduction for the Hilbert class polynomial.

Theorem 1.5.4. *Let $K = \mathbb{Q}(\sqrt{D})$, where D is a negative fundamental discriminant. Then*

(i) The Hilbert class field of K can be obtained by adjoining as $K_H = K(j[a,b,c])$, where $[a,b,c] \in C(D)$ is any one of the reduced quadratic forms of discriminant D.

(ii) The minimal polynomial of the $j([a,b,c])$'s, denoted by $H_D(X)$, has integer coefficients:

$$H_D(X) = \prod_{[a,b,c] \in C(D)} (X - j([a,b,c])) \in \mathbb{Z}[X]$$

(iii) There is an isomorphism

$$\begin{array}{ccc} C(D) & \xrightarrow{\sim} & Gal(K_H/K) \\ f & \mapsto & \sigma_f \end{array}$$

The action of σ_f on j is given by

$$\sigma_f(j(\overline{f})) = j(f^{-1} \cdot \overline{f})$$

Definition 1.5.5. The minimal polynomial polynomial $H_D(X)$ is called the *Hilbert class polynomial*, and we refer to the equation $H_D(X) = 0$ as the *class equation*.

Remark 1.5.6. We observe explicitly that the Hilbert class field K_H is precisely the splitting field of the Hilbert class polynomial $H_D(X)$.

Thanks to the Remark 1.3.3, the class polynomial can be expressed as

$$H_D(X) = \prod_{[a,b,c] \in C(D)} \left(X - j\left(\frac{-b + \sqrt{D}}{2a} \right) \right) \in \mathbb{Z}[X]$$

Remark 1.5.7. It follows that, if $\tau \in \mathcal{H}$ is a quadratic imaginary number with discriminant D in K_H as in Definition 1.3.4, then $j(\tau)$ is an algebraic integer of degree exactly equal to $h(D)$, where $h(D)$ is the class number of the imaginary quadratic order of discriminant D. More precisely, the minimal polynomial of $j(\tau)$ over $\mathbb{Z}$ is the equation $\prod(X - j(\alpha)) = 0$, where α runs over the quadratic numbers associated to the reduced forms of discriminant D.

Note that $j(\tau)$ is indeed a root of this polynomial, since any quadratic form of discriminant D is equivalent to a reduced form, and since the j-function is $\mathrm{SL}_2(\mathbb{Z})$-invariant.

Remark 1.5.8. We will consider again in more detail Theorem 1.5.4 in Section 3.10, where we explore the connection with elliptic curves.

Remark 1.5.9. Sometimes it is useful to build explicitly the Hilbert class polynomial by approximating to the nearest integer the coefficients of the polynomial. The following result (discovered by Gross and Zagier in their paper *On singular moduli*, 1985) helps us to check if the polynomial we have found is the correct one.

Proposition 1.5.10. *The norm of j in $\mathbb{Q}(j)$, i.e. the constant term $H_D(0)$, is a cube of an integer in $\mathbb{Z}$.*

Remark 1.5.11. The class polynomial can in general be defined for any integer D that occurs as the discriminant of some order $\mathcal{O}$ in K. Then the class polynomial of $\mathcal{O}$ is

$$H_{\mathcal{O}} = \prod (X - j(\mathfrak{a}))$$

where the product is over representatives $\mathfrak{a}$ of each ideal class of $\mathcal{O}$. Since $\mathcal{O}$ is uniquely determined by its discriminant D, we will often write $H_D(X)$ instead of $H_{\mathcal{O}}(X)$.

We end this chapter with the following result [1, §2,§3] that describes the behaviour of certain rational primes in the Hilbert class field. It is of fundamental importance.

Theorem 1.5.12. *Let D be a negative fundamental discriminant, consider $K = \mathbb{Q}(\sqrt{D})$ and let K_H be the Hilbert class field of K. Then, if p is a rational prime, $p \nmid D$, the following statements are equivalent:*

(i) *p is a norm in K (i.e. the equation $p = N(\pi)$ has a solution in $\mathcal{O}_K$)*

(ii) *(p) splits completely in K_H.*

(iii) *p splits as the product of two distinct elements in $\mathcal{O}_K$.*

(iv) *$H_D(X)$ modulo p has only simple roots and they are all in $\mathbb{Z}/p\mathbb{Z}$.*

(v) *$4p = t^2 + s^2|D|$ has a solution in $x, y \in \mathbb{Z}$.*

1.5.1 The Artin Map

Now we are going to define the Artin symbol to link L to the ideal structure of $\mathcal{O}_K$.

Proposition 1.5.13. *Let $K \subset L$ be a Galois extension, and let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ which is unramified in L. If $\mathfrak{P}$ is a prime of $\mathcal{O}_L$ containing $\mathfrak{p}$, then there is a unique element $\sigma \in Gal(L/K)$ such that for all $\alpha \in \mathcal{O}_L$,*

$$\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \pmod{\mathfrak{P}}$$

where $N(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}|$ is the norm of $\mathfrak{p}$.

Definition 1.5.14. The unique element σ of Proposition 1.5.13 is called the *Artin symbol* and it is denoted $((L/K)/\mathfrak{P})$ since it depends on the prime $\mathfrak{P}$ of L.

Remark 1.5.15. The important property of the Artin symbol is that, for any $\alpha \in \mathcal{O}_L$, we have

$$\left(\frac{L/K}{\mathfrak{P}}\right)(\alpha) \equiv \alpha^{N(\mathfrak{p})} \pmod{\mathfrak{P}}$$

where $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$.

Corollary 1.5.16. *Let $K \subset L$ be a Galois extension, and let $\mathfrak{p}$ be an unramified prime of K. Given a prime $\mathfrak{P}$ of L containing $\mathfrak{p}$, we have:*

(i) If $\sigma \in Gal(L/K)$, then

$$\left(\frac{L/K}{\sigma(\mathfrak{P})}\right) = \sigma \left(\frac{L/K}{\mathfrak{P}}\right) \sigma^{-1}$$

(ii) The order of $((L/K)/\mathfrak{P})$ is the degree of inertia $f = f_{\mathfrak{P}|\mathfrak{p}}$.

(iii) $\mathfrak{p}$ splits completely in L if and only if $((L/K)/\mathfrak{P}) = 1$.

Remark 1.5.17. When $K \subset L$ is an abelian extension, the Artin symbol $((L/K)/\mathfrak{P})$ depends only on the underlying prime $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$. In fact, let $\mathfrak{P}'$ be another prime containing $\mathfrak{p}$. We have $\mathfrak{P}' = \sigma(\mathfrak{P})$ for some $\sigma \in \mathrm{Gal}(L/K)$. Then Corollary 1.5.16 implies that

$$\left(\frac{L/K}{\mathfrak{P}'}\right) = \left(\frac{L/K}{\sigma(\mathfrak{P})}\right) = \sigma \left(\frac{L/K}{\mathfrak{P}}\right) \sigma^{-1} = \left(\frac{L/K}{\mathfrak{P}}\right)$$

since $\mathrm{Gal}(L/K)$ is abelian. It follows that whenever $K \subset L$ is abelian, the Artin symbol can be written as $((L/K)/\mathfrak{p})$.

When $K \subset L$ is an unramified Abelian extension, things are especially nice because $((L/K)/\mathfrak{p})$ is defined for all primes $\mathfrak{p}$ of $\mathcal{O}_K$. Let I_K be the set of all fractional ideals of $\mathcal{O}_K$. We saw that any fractional ideal $\mathfrak{a} \in I_K$ has a prime factorization

$$\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{r_i}, \quad r_i \in \mathbb{Z}$$

We define the *Artin symbol* $((L/K)/\mathfrak{a})$ to be the product

$$\left(\frac{L/K}{\mathfrak{a}}\right) = \prod_{i=1}^{r} \left(\frac{L/K}{\mathfrak{p}_i}\right)^{r_i}$$

The Artin symbol thus defines a homomorphism, called the *Artin map*,

$$\left(\frac{L/K}{\cdot}\right) : I_K \to \mathrm{Gal}(L/K)$$

Notice that when $K \subset L$ is ramified, the Artin map is not defined on all of I_K.

The *Artin reciprocity theorem for the Hilbert class field* relates the Hilbert class field to the ideal class group $C(\mathcal{O}_K)$ as follows:

Theorem 1.5.18. *If L is the Hilbert class field of a number field K, then the Artin map*

$$\left(\frac{L/K}{\cdot}\right) : I_K \to Gal(L/K)$$

is surjective, and its kernel is exactly the subgroup P_K of principal fractional ideals. Thus the Artin map induces an isomorphism

$$C(\mathcal{O}_K) \xrightarrow{\sim} Gal(L/K)$$

The appearance of the class group $C(\mathcal{O}_K)$ explains why L is called a "class field".

If we apply Galois theory to Theorems 1.5.2 and 1.5.18, we get the following classification of unramified Abelian extensions of K:

Corollary 1.5.19. *Given a number field K, there is a one-to-one correspondence between unramified Abelian extensions M of K and subgroups H of the ideal class group $C(\mathcal{O}_K)$. Furthermore, if the extension $K \subset M$ corresponds to the subgroup $H \subset C(\mathcal{O}_K)$, then the Artin map induces an isomorphism*

$$C(\mathcal{O}_K)/H \xrightarrow{\sim} Gal(M/K)$$

This corollary is *class field theory for unramified Abelian extensions*, and it illustrates one of the main themes of class field theory: a certain class of extensions of K (unramified Abelian extensions) are classified in terms of data intrinsic to K (subgroups of the ideal class group).

Theorem 1.5.18 also allows us to characterize the primes of K which split completely in the Hilbert class field:

Corollary 1.5.20. *Let L be the Hilbert class field of a number field K, and let $\mathfrak{p}$ be a prime ideal of K. Then*

$$\mathfrak{p} \textit{ splits completely in } L \Leftrightarrow \mathfrak{p} \textit{ is a principal ideal.}$$

CHAPTER 2

The Geometry of Elliptic Curves

Abstract

Elliptic curves are curves of genus one having a specified base point. Our ultimate goal is to study the endomorphism ring of such curves, and analyze their points defined over finite fields. In order to do so, in this chapter we study the geometry of elliptic curves over an arbitrary algebraically closed field k, postponing to later chapters the specialization to the field of complex numbers $\mathbb{C}$ and to the finite fields $\mathbb{F}_q$, where $q = p^r$ is a prime power.

We start by looking at elliptic curves given by explicit polynomial equations called Weierstrass equations. Using these explicit equations, we show that the set of points of an elliptic curve forms an abelian group, and that the group law is given by rational functions. Then we use the Riemann-Roch theorem to study arbitrary elliptic curves and to show that every elliptic curve has a Weierstrass equation, so the results from the part in fact apply generally. In the remainder of the chapter we consider the maps between elliptic curves: in particular, since the points of an elliptic curve form a group, for each integer m there is a multiplication-by-m map from the curve to itself. This enable us to define the Endomorphism ring of an elliptic curve and to consider the so called *complex multiplication*, which will be of fundamental importance. We conclude by classifying endomorphism rings.

2.1 Definition and First Properties

An elliptic curve over a field k is a nonsingular complete curve of genus 1 with a distinguished point O. When char $k \neq 2, 3$, it can be written as a plane projective curve

$$Y^2Z = X^3 + aXZ^2 + bZ^3$$

with $4a^3 + 27b^2 \neq 0$, and every such equation defines an elliptic curve over k. The distinguished point is $(0 : 1 : 0)$.

Definition 2.1.1. An elliptic curve over k can be defined equivalently as:

(a) a nonsingular projective plane curve E over k of degree 3 together with a point $O \in E(k)$;

(b) a nonsingular projective curve E of genus 1 together with a point $O \in E(k)$.

(c) a nonsingular projective plane curve E over k of the form

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{2.1}$$

Definition 2.1.2. The equation 2.1 is said to be a *Weierstrass equation* for the elliptic curve E.

We will see in section 2.3 that, if we define an elliptic curve E as in (b), then it has indeed a Weierstrass equation 2.1: precisely, every such curve can be written as the locus in $\mathbb{P}^2$ of a cubic equation with only one point, the base point, on the line at ∞. Then, after X and Y are scaled appropriately, an elliptic curve has an equation of the form 2.1. Here $O = [0 : 1 : 0]$ is the base point and $a_1, \ldots, a_6 \in \overline{k}$.

Remark 2.1.3. In this section and in the next, we assume the fact that every elliptic curve as in (b) can be given a Weierstrass equation, and therefore we study the curves in such a form.

Proposition 2.1.4. *Let k be a field of characteristic $\neq 2, 3$. Every elliptic curve (E, O) is isomorphic to a curve of the form*

$$E(a, b) : Y^2Z = X^3 + aXZ^2 + bZ^3, \quad a, b \in k \tag{2.2}$$

pointed by $(0 : 1 : 0)$. Conversely, the curve $E(a, b)$ is nonsingular (and so, together with $(0 : 1 : 0)$ is an elliptic curve) if and only if $4a^3 + 27b^2 \neq 0$.

Proof. Let E be an elliptic curve over k, written in the Weierstrass form

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{2.3}$$

When k has characteristic $\neq 2, 3$, a change of variables

$$X' = X, \quad Y' = Y + \frac{a_1}{2}X, \quad Z' = Z$$

will eliminate the XYZ term in 2.3, and a change of variables

$$X' = X + \frac{a_2}{3}, \quad Y' = Y + \frac{a_3}{2}, \quad Z' = Z$$

will then eliminate the X^2 and Y terms. Thus we arrive at the equation:

$$Y^2Z = X^3 + aXZ^2 + bZ^3$$

The point $(0 : 1 : 0)$ is always nonsingular on $E(a, b)$, and the affine curve

$$Y^2 = X^3 + aX + b$$

is nonsingular if and only if $4a^3 + 27b^2 \neq 0$. □

2.1.1 The details

We see now the details. To ease notation, we write the Weierstrass equation for our elliptic curve using non-homogeneous coordinates $x = X/Z$ and $y = Y/Z$,

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

always remembering that there is an extra point $O = [0 : 1 : 0]$ out at infinity.

If $\mathrm{char}\bar{k} \neq 2$, then we can simplify the equation by completing the square. Thus the substitution

$$y \mapsto \frac{1}{2}(y - a_1x - a_3)$$

gives an equation of the form

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

where

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

We also define quantities

$$\begin{aligned}
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\
c_4 &= b_2^2 - 24b_4 \\
c_6 &= -b_2^3 + 36b_2b_4 - 216b_6 \\
\Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\
j &= c_4^3/\Delta \\
\omega &= \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y}
\end{aligned}$$

Simple computations show that

$$4b_8 = b_2b_6 - b_4^2, \qquad 1728\Delta = c_4^3 - c_6^2$$

If moreover $\mathrm{char}\bar{k} \neq 2, 3$, then the substitution

$$(x, y) \mapsto \left(\frac{x - 3b_2}{36}, \frac{y}{108}\right)$$

eliminates the x^2 term, yielding the simpler equation

$$E : y^2 = x^3 - 27c_4x - 54c_6$$

Definition 2.1.5. The quantity Δ is the *discriminant* of the Weierstrass equation, the quantity j is the j-invariant of the elliptic curve, and ω is the invariant differential associated to the Weierstrass equation.

Now, a natural question to ask is to what extent is the Weierstrass equation for an elliptic curve unique. Assuming that the line at infinity, i.e., the line $Z = 0$ in $\mathbb{P}^2$, is required to intersect E only at the one point $[0 : 1 : 0]$, we will see in section 2.3 that the only change of variables fixing $[0 : 1 : 0]$ and preserving the Weierstrass form of the equation is given by

$$x = u^2x' + r \quad \text{and} \quad y = u^3y' + u^2sx' + t$$

where $u, r, s, t \in \bar{k}$ and $u \neq 0$. If we perform this substitution and compute the a_i' coefficients and associated quantities for the new equation we obtain the following quantities:

$$\begin{aligned}
ua_1' &= a_1 + 2s & u^2a_2' &= a_2 - sa_1 + 3r - s^2 \\
u^4a_4' &= a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st & u^3a_3' &= a_3 + ra_1 + 2t \\
u^6a_6' &= a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1 & u^2b_2' &= b_2 + 12r \\
u^6b_6' &= b_6 + 2rb_4 + r^2b_2 + 4r^3 & u^4b_4' &= b_4 + rb_2 + 6r^2 \\
u^8b_8' &= b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4 & u^4c_4' &= c_4 \\
u^6c_6' &= c_6 & u^{12}\Delta' &= \Delta \\
j' &= j & u^{-1}\omega' &= \omega
\end{aligned}$$

It is now clear why the j-invariant has been so named; it is an invariant of the isomorphism class of the curve, and does not depend on the particular equation chosen. For algebraically closed fields, the converse is true, as we shall see in a moment.

Remark 2.1.6. We have seen that if $\mathrm{char}k \neq 2, 3$, then any elliptic curve over k has a particularly simple Weierstrass equation. In almost all what follows in this chapter, we continue to assume $\mathrm{char}k \neq 2, 3$.

Our elliptic curve has Weierstrass equation of the form

$$E : y^2 = x^3 + ax + b \tag{2.4}$$

and we consider

$$\Delta = -16(4a^3 + 27b^2) \quad \text{and} \quad j = -1728\frac{(4a)^3}{\Delta} \tag{2.5}$$

The only change of variables preserving this form of the equation is

$$x = u^2x' \quad \text{and} \quad y = u^3y'$$

for some $u \in \overline{k}^*$ and then

$$u^4a' = a, \quad u^6b' = b, \quad u^{12}\Delta' = \Delta$$

Remark 2.1.7. We will often write $E(a, b)$ as a shorthand notation for an elliptic curve with a Weierstrass equation given by 2.4.

Theorem 2.1.8. *Two elliptic curves $E(a, b)$ and $E(a', b')$ defined over k are isomorphic (over $\overline{k}$) if and only if there exists $c \in \overline{k}^*$ such that $a' = c^4a$ and $b' = c^6b$, the isomorphism being given by the map*

$$(x, y) \mapsto (c^2x, c^3y)$$

Proof. This follows directly from Proposition 2.3.1 □

Proposition 2.1.9. *(a) The curve given by a Weierstrass equation is nonsingular if and only if $\Delta \neq 0$.*

(b) Two elliptic curves are isomorphic over $\overline{k}$ if and only if they both have the same j-invariant.

(c) Let $j_0 \in \overline{k}$. There exists an elliptic curve defined over $k(j_0)$ whose j-invariant is equal to j_0.

Proof. (a) Let E be given by the Weierstrass equation

$$E : f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$$

We start by showing that the point at infinity is never singular. Thus we look at the curve in $\mathbb{P}^2$ with homogeneous equation

$$\begin{aligned} F(X, Y, Z) &= Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 \\ &= 0 \end{aligned}$$

and at the point $O = [0 : 1 : 0]$. Since

$$\frac{\partial F}{\partial Z}(O) = 1 \neq 0$$

we see that O is a nonsingular point of E.

Next suppose that E is singular, say at $P_0 = (x_0, y_0)$. The substitution

$$x = x' + x_0, \quad y = y' + y_0$$

leaves Δ and c_4 invariant, so without loss of generality we may assume that E is singular at $(0,0)$. Then

$$a_6 = f(0,0) = 0, \quad a_4 = \frac{\partial f}{\partial x}(0,0) = 0, \quad a_3 = \frac{\partial f}{\partial y}(0,0) = 0$$

so the equation for E takes the form

$$E : f(x,y) = y^2 + a_1xy - a_2x^2 - x^3 = 0$$

This equation has associated quantities

$$c_4 = (a_1^2 + 4a_2)^2 \quad \text{and} \quad \Delta = 0$$

Assume now E is nonsingular; we show that $\Delta \neq 0$. To simplify the computation, we assume that char$k \neq 2$ and consider a Weierstrass equation of the form

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

The curve E is singular if and only if there is a point $(x_0, y_0) \in E$ satisfying

$$2y_0 = 12x_0^2 + 2b_2x_0 + 2b_4 = 0$$

In other words, the singular points are exactly the points of the form $(x_0, 0)$ such that x_0 is a double root of the cubic polynomial $4x^3 + b_2x^2 + 2b_4x + b_6$. This polynomial has a double root if and only if its discriminant, which equals 16Δ, vanishes.

(a) If two elliptic curves are isomorphic, then the transformation formulas show that they have the same j-invariant. For the converse, we will assume that char$k \geq 5$. Let E and E' be elliptic curves with the same j-invariant, say with Weierstrass equations

$$\begin{aligned} E : y^2 &= x^3 + Ax + B \\ E' : y'^2 &= x'^3 + A'x' + B' \end{aligned}$$

Then the assumption that $j(E) = j(E')$ means that

$$\frac{(4A)^3}{4A^3 + 27B^2} = \frac{(4A')^3}{4A'^3 + 27B'^2}$$

which yields

$$A^3B'^2 = A'^3B^2$$

We look for an isomorphism of the form $(x,y) = (u^2x', u^3y')$ and consider three cases:

Case 1 . $A = 0$ (and $j = 0$). Then $B \neq 0$ since $\Delta \neq 0$, so $A' = 0$, and we obtain an isomorphism using $u = (B/B')^{1/6}$.

Case 2 . $B = 0$ (and $j = 1728$). Then $A \neq 0$, so $B' = 0$, and we take $u = (A/A')^{1/4}$.

Case 3 . $AB \neq 0$ (and $j \neq 0, 1728$). Then $A'B' \neq 0$, since if one of them were 0, then both of them would be 0, contradicting $\Delta' \neq 0$. Taking $u = (A/A')^{1/4}$ gives the desired isomorphism.

(c) Assume that $j_0 \neq 0, 1728$ and consider the curve

$$E : y^2 + xy = x^3 - \frac{36}{j_0 - 1728}x - \frac{1}{j_0 - 1728}$$

A direct computation yields

$$\Delta = \frac{j_0^3}{(j_0 - 1728)^3} \quad \text{and} \quad j = j_0$$

This gives the desired elliptic curve (in any characteristic) provided that $j_0 \neq 0, 1728$.

To complete the list, we use the two curves

$$\begin{aligned} &E : y^2 + y = x^3, && \Delta = -27, && j = 0 \\ &E : y^2 = x^3 + x, && \Delta = -64, && j = 1728 \end{aligned}$$

(Notice that if char$k = 2, 3$ we have $1728 = 0$, so even in these cases one of the two curves will be nonsingular and fill in the missing value of j).

□

Remark 2.1.10. We exhibit explicit equations for elliptic curves E over k with a given j-invariant $j(E) = j \in k$. Put $c = \frac{j}{j-1728}$; we have

$$\begin{aligned} &y^2 = x^3 + 1, && j = 0 \\ &y^2 = x^3 + x, && j = 1728 \\ &y^2 = x^3 - \frac{27}{4}cx - \frac{27}{4}c && j \neq 0, 1728 \end{aligned}$$

Remark 2.1.11. Two elliptic curves can have the same j-invariant and yet not be isomorphic over k. For example, if c is not a square in k, then

$$Y^2Z = X^3 + ac^2XZ^2 + bc^3Z^3$$

has the same j-invariant as $E(a, b)$, but it is not isomorphic to it.

2.1.2 Twists of Elliptic Curves

Definition 2.1.12. Let C/K be a smooth projective curve. The *isomorphism group* of C, denoted by $\mathrm{Isom}(C)$, is the group of $\overline{K}$-isomorphisms from C to itself. We denote the subgroup of $\mathrm{Isom}(C)$ consisting of isomorphisms defined over K by $\mathrm{Isom}_K(C)$.

Remark 2.1.13. The group that we are denoting by $\mathrm{Isom}(C)$ is usually called the *automorphism group* of C and denoted by $\mathrm{Aut}(C)$. However, if E is an elliptic curve, then we have defined $\mathrm{Aut}(E)$ to be the group of isomorphisms from E to E that take O to O. Thus $\mathrm{Aut}(E) \neq \mathrm{Isom}(E)$, since for example, the group $\mathrm{Isom}(E)$ contains translation maps $\tau_P : E \to E$.

Definition 2.1.14. A twist of C/K is a smooth curve C'/K that is isomorphic to C over $\overline{K}$. We treat two twists as equivalent if they are isomorphic over K. The set of twists of C/K, modulo K-isomorphism, is denoted by $\mathrm{Twist}(C/K)$.

Let E be an elliptic curve over a field K, with base point O. If $\mathrm{char}(K) \neq 2, 3$, then the elements of the group $\mathrm{Twist}((E,O)/K)$ can be described as follows:

Proposition 2.1.15. *Assume* $\mathrm{char}(K) \neq 2, 3$, *and let*

$$n = \begin{cases} 2 & \text{if } j(E) \neq 0, 1728 \\ 4 & \text{if } j(E) = 1728 \\ 6 & \text{if } j(E) = 0 \end{cases}$$

Then $\mathrm{Twist}((E,O)/K)$ *is canonically isomorphic to* $K^*/(K^*)^n$. *More precisely, choose a Weierstrass equation*

$$E : y^2 = x^3 + ax + b$$

for E/K, *and let* $D \in K^*$. *Then the elliptic curve* $E_D \in \mathrm{Twist}(E,O)/K)$ *corresponding to* $D (\mathrm{mod} (K^*)^n)$ *has Weierstrass equation*

$$\begin{aligned} &E_D : y^2 = x^3 + D^2ax + D^3b, && j(E) \neq 0, 1728, \\ &E_D : y^2 = x^3 + Dax, && j(E) = 1728, \\ &E_D : y^2 = x^3 + Db, && j(E) = 0, \end{aligned}$$

Proof. See [10, §X.5]. □

Corollary 2.1.16. *Define an equivalence relation on the set* $K \times K^*$ *by*

$$(j, D) \sim (j', D') \quad \text{if } j = j' \text{ and } D/D' \in (K^*)^{n(j)}$$

where $n(j) = 2$ (resp. 4, resp. 6) if $j \neq 0, 1728$ (resp. $j = 1728$, resp. $j = 0$). Then the K-isomorphism classes of elliptic curves E/K are in 1-1 correspondence with the elements of the quotient

$$\frac{K \times K^*}{\sim}$$

Remark 2.1.17. We will consider in later chapters elliptic curves over a finite field K, char$K \neq 2, 3$. In this case,

$$\frac{K^*}{(K^*)^2} \cong \frac{\mathbb{Z}}{2\mathbb{Z}}$$

In fact, K^* is cyclic and $\exists q \in K$ such that

$$\begin{aligned} K^* &= < q >= \frac{\mathbb{Z}}{(q-1)\mathbb{Z}} \\ (K^*)^2 &= < q >^2 = \frac{\mathbb{Z}}{\frac{q-1}{2}\mathbb{Z}} \end{aligned}$$

In this case, a twist of the curve

$$y^2 = x^3 + ax + b$$

is given by

$$y^2 = x^3 + ad^2x + bd^3$$

where d is not a quadratic residue in K.

2.2 The Group Law

The set of points on an elliptic curve can be given the structure of an abelian group, with a group law $\oplus$ that we are going to define. We will next give the formulas for the addition and doubling of points on the curve

$$E : Y^2Z = X^3 + aXZ^2 + bZ^3, \quad a, b \in k, \quad \Delta = 4a^3 + 27b^2 \neq 0$$

Let E be an elliptic curve given by a Weierstrass equation. Thus $E \subset \mathbb{P}^2$ consists of the points $P = (x, y)$ satisfying the Weierstrass equation, together with the point $O = [0 : 1 : 0]$ at infinity. Let $L \subset \mathbb{P}^2$ be a line. Then, since the equation has degree 3, the line L intersects E at exactly 3 points, say P, Q, R. Of course, if L is tangent to E, then P, Q, R need not be distinct. The fact that $L \cap E$, taken with multiplicities, consists of exactly 3 points is a special case of Bézout's theorem. However, since we give explicit formulas later in this section, there is no need to use a general theorem.

We define a composition law $\oplus$ on E by the following rule:

Composition Law Let $P, Q \in E$, let L be the line through P and Q (if $P = Q$, let L be the tangent line to E at P), and let R be the third point of intersection of L with E. Let L' be the line through R and O. Then L' intersects E at R, O, and a third point. We denote that third point by $P \oplus Q$.

Remark 2.2.1. The composition law makes E into an abelian group with identity element O. All verifications are easy except for the associativity. This is not difficult but quite time-consuming, so we refer the details to [7] or [10].

Notation. From here on, we drop the special symbol $\oplus$ and simply write $+$ and $-$ for the group operation on an elliptic curve E. For $m \in \mathbb{Z}$ and $P \in E$, we let

$$[m]P = P + \cdots p$$

with m terms if $m > 0$, and

$$[m]P = -P - \cdots - P$$

with $|m|$ terms if $m < 0$. Moreover, $[0]P = O$.

We now derive explicit formulas for the group operations on E. These will be useful in the description of Schoof's algorithm.

Theorem 2.2.2. *Let $E : y^2 = x^3 + ax + b$ be an elliptic curve. The inversion of a point (x_0, y_0) on E is the point $(x_0, -y_0)$, i.e. reflection in the x-axis.*

Let $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ be two points on E. Then the sum $P_1 \oplus P_2 =: (x_3, y_3)$ is given by

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 \\ y_3 &= \lambda(x_1 - x_3) - y_1 \end{aligned}$$

where

$$\lambda = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1} & \text{if } x_1 \neq x_2 \\ (3x_1^2 + a)(2y_1)^{-1} & \text{if } x_1 = x_2 \end{cases}$$

Proof. The theorem follows from direct manipulation of plane coordinates. This is not difficult but rather time consuming, and so we avoid the details here. We refer to [7]. □

Remark 2.2.3. We can define the morphisms

$$\begin{aligned} + : E \times E &\longrightarrow E & \qquad - : E &\longrightarrow E \\ (P_1, P_2) &\mapsto P_1 + P_2 & \qquad P &\mapsto -P \end{aligned}$$

2.3 Getting The Weierstrass Equation

Let E be a complete nonsingular curve of genus 1 over a field k and let $O \in E(k)$. As promised in the beginning of the chapter, we see now that E can be written in Weierstrass equation. According to the Riemann-Roch theorem (see [10, §II.5]), the rational functions on E having no poles except at O and having at worst a pole of order $m \geq 1$ at O, form a vector space of dimension m over k, i.e., $L(m[O])$ has dimension m for $m \geq 1$. The constant functions lie in $L([O])$, and according to the Riemann-Roch theorem, there are no other. Thus $\{1\}$ is a basis for $L([O])$.

Choose x so that $\{1, x\}$ is a basis for $L(2[O])$. Choose y so that $\{1, x, y\}$ is a basis for $L(3[O])$. Then $\{1, x, y, x^2\}$ is a basis for $L(4[O])$ - if it were linearly dependent, x^2 would have to be a linear combination of $1, x, y$, but then it could not have a quadruple pole at O. And $\{1, x, y, x^2, xy\}$ is a basis for $L(5[O])$ for a similar reason.

The subset $\{1, x, y, x^2, xy, x^3, y^2\}$ of $L(6[O])$ contains 7 elements, and so it must be linearly dependent: there exist $a_i \in k$ such that

$$a_0y^2 + a_1xy + a_3y = a_0'x^3 + a_2x^2 + a_4x + a_6$$

(as regular functions on $E/\{O\}$). Moreover, a_0 and a_0' must be nonzero, because the set with either x^3 or y^2 omitted is linearly independent, and so, after replacing y with a_0y/a_0' and x with a_0x/a_0' and multiplying through by $a_0'^2/a_0^3$, we can suppose both equal 1. The map $P \mapsto (x(P), y(P))$ sends $E/\{O\}$ onto the plane affine curve

$$C : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

The function x has a double pole at O and no other pole, and so it has only two zeros. Similarly, $x + c$ has two zeros for any $c \in k$ (counting multiplicities), and so the composite

$$E/\{O\} \to C \to \mathbb{A}^1, \quad P \mapsto (x(P), y(P)) \mapsto x(P)$$

has degree 2. Similarly, the composite

$$E/\{O\} \to C \to \mathbb{A}^1, \quad P \mapsto (x(P), y(P)) \mapsto y(P)$$

has degree 3. The degree of $E/\{O\}$ divides both 2 and 3, and therefore is l. If C were singular, it would have genus 0, which is impossible. Therefore C is nonsingular, and so the map is an isomorphism, and it extends to an isomorphism of E onto

$$\overline{C} : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

Proposition 2.3.1. *Let E be an elliptic curve defined over k. Any two Weierstrass equations for E in the form*

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

(where $a_i \in k$) are related by a linear change of variables of the form

$$X = u^2X' + t, \quad Y = u^3Y' + su^2X' + t$$

with $u \in k^*$ and $r, s, t \in k$.

Proof. Let $\{x, y\}$ and $\{x', y'\}$ be two sets of Weierstrass coordinate functions on E. Then x and x' have poles of order 2 at O, and y and y' have poles of order 3 at O. Hence $\{1, x\}$ and $\{1, x'\}$ are both bases for $\mathcal{L}(2[O])$, and similarly $\{1, x, y\}$ and $\{1, x', y'\}$ are both bases for $\mathcal{L}(3[O])$. Thus there are constants $u_1, u_2 \in k^*$ and $r, s_2, t \in k$ such that

$$x = u_1x' + r \quad \text{and} \quad y = u_2y' + s_2x' + t$$

Since both (x, y) and (x', y') satisfy Weierstrass equations in which the Y^2 and X^3 terms have coefficient 1, we have $u_1^3 = u_2^2$. Letting $u = u_2/u_1$ and $s = s_2/u^2$ puts the change of variables formula into the desired form. □

2.4 The Ring of Endomorphisms

Having examined in some detail the geometry of individual elliptic curves, we turn now to the study of the maps between curves. Since an elliptic curve has a distinguished zero point, it is natural to single out the maps that respect this property.

Definition 2.4.1. Let E_1 and E_2 be elliptic curves. An isogeny from E_1 to E_2 is a morphism

$$\phi : E_1 \to E_2$$

satisfying $\phi(O_1) = O_2$ (from now on we will indicate simply O without subfix. In fact, no confusion should arise). Two elliptic curves E_1 and E_2 are *isogenous* if there is an isogeny from E_1 to E_2 with $\phi(E_1) \neq \{O\}$.

We have that an isogeny satisfies either

$$\phi(E_1) = \{O\} \quad \text{or} \quad \phi(E_1) = E_2$$

Thus except for the zero isogeny defined by $[0](P) = O$ for all $P \in E$, every other isogeny is a finite map of curves.

Example 2.4.2. For each $m \in \mathbb{Z}$ we define the *multiplication-by-m isogeny*

$$[m] : E \to E$$

in the natural way. Thus if $m > 0$, then

$$[m](P) = P + P + \cdots + P$$

where the sum involve m terms. For $m < 0$, we set $[m](P) = [-m](-P)$, and we have already defined $[0](P) = O$. Thanks to Remark 2.2.3, an easy induction shows that $[m]$ is a morphism, hence an isogeny, since it clearly sends O to O.

Definition 2.4.3. Let E be an elliptic curve and let $m \in \mathbb{Z}$ with $m \geq 1$. The *m-torsion subgroup* of E is the set of points of E of order m:

$$E[m] = \{P \in E \mid [m]P = O\}$$

The *torsion subgroup* of E, denoted by E_{tors}, is the set of points of finite order

$$E_{\text{tors}} = \bigcup_{m=1}^{\infty} E[m]$$

If E is defined over a field k, then $E_{\text{tors}}(k)$ denotes the points of finite order in $E(k)$.

The most important fact about the multiplication-by-m map is that it has degree m^2, from which one can deduce the structure of the finite group $E[m]$.

Aside 2.4.4. We briefly recall the definition of degree of a map between curves C_1, C_2 over a field K. Let $\phi : C_1 \to C_2$ be a non-constant rational map defined over K. Then composition with ϕ induces an injection of function fields fixing K

$$\begin{aligned} \phi^* : K(C_2) &\to K(C_1) \\ \phi^* f &= f\phi \end{aligned}$$

where $K(C)$ is the function field of C over K.

Definition 2.4.5. Let $\phi : C_1 \to C_2$ be a map of curves defined over K. If ϕ is constant, we define the *degree* of ϕ to be 0. Otherwise we say that ϕ is a *finite map* and we define its *degree* to be

$$\deg \phi = [K(C_1) : \phi^* K(C_2)]$$

We say that ϕ is *separable, inseparable* or *purely inseparable* if the field extension $K(C_1)/\phi^* K(C_2)$ has the corresponding property, and we denote the separable and inseparable degrees of the extension by $\deg_s \phi$ or $\deg_i \phi$ respectively.

We now prove the following result, which is not only interesting on its own but will also be fundamental in the discussion of the Tate module of Section 4.2.

Proposition 2.4.6. *Let $E/\mathbb{C}$ be an elliptic curve over the field of complex numbers, and let $m \geq 1$ be an integer.*

(a) There is an isomorphism

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

(b) The multiplication-by-m map $[m] : E \to E$ has degree m^2

Proof. It will be easy after we will discuss elliptic curves over $k = \mathbb{C}$. So we postpone the proof to Proposition 3.9.4, where we will provide full details. □

We introduce now an object that will be fundamental to our following discussion. It will lead the way to introduce the idea of *complex multiplication*.

Definition 2.4.7. The *Endomorphism Ring* of an elliptic curve E over a field k is defined to be

$$\mathrm{End}_k(E) = \{\text{isogenies } \phi : E \to E \text{over } k\}$$

It is a ring with multiplication and addition given respectively

$$(\phi\psi)(P) = \phi(\psi(P)), \quad (\phi + \psi)(P) = \phi(P) + \psi(P)$$

where ϕ and ϕ are elements of $\mathrm{End}_k(E)$ and P is a point on E. When E is defined over k , we will write sometimes $\mathrm{End}(E)$ to denote $\mathrm{End}_{\bar{k}}(E)$.

Remark 2.4.8. The maps $[m]$ of example 2.4.2 are elements of $\mathrm{End}(E)$, and we get an injection $\mathbb{Z} \hookrightarrow \mathrm{End}(E)$.

Most of the time, these maps are the only elements, in which case $\mathrm{End}(E) \cong \mathbb{Z}$ because the maps are distinct. But if $\mathrm{End}(E)$ is strictly larger than $\mathbb{Z}$, then we say that E has *complex multiplication*.

2.5 Classification of Endomorphism Rings

In the future it will be useful to dispose of a good criterion for classify endomorphism rings: given the elliptic curve E, we want now to characterize which rings may occur as the endomorphism ring of E. To set up the situation, we use the following definitions.

Definition 2.5.1. Let $\mathcal{K}$ be a (not necessarily commutative) $\mathbb{Q}$-algebra that is finitely generated over $\mathbb{Q}$. An *order* $\mathcal{R}$ of $\mathcal{K}$ is a subring of $\mathcal{K}$ that is finitely generated as a $\mathbb{Z}$-module and satisfies $\mathcal{R} \otimes \mathbb{Q} = \mathcal{K}$.

Example 2.5.2. Let $\mathcal{K}$ be an imaginary quadratic field and let $\mathcal{O}_{\mathcal{K}}$ be its ring of integers. Then for each integer $f \geq 1$, the ring $\mathbb{Z} + f\mathcal{O}$ is an order of $\mathcal{K}$. In fact, these are all of the orders of $\mathcal{K}$.

Definition 2.5.3. A *quaternion algebra* is an algebra of the form

$$\mathcal{K} = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta$$

whose multiplication satisfies

$$\alpha^2, \beta^2 \in \mathbb{Q}, \quad \alpha^2, \beta^2 < 0, \quad \beta\alpha = -\alpha\beta$$

We have the following result.

Theorem 2.5.4. *The endomorphism ring of an elliptic curve E over a field k is one of the following:*

1. *the integers $\mathbb{Z}$;*
2. *an order in an imaginary quadratic field;*
3. *an order in a quaternion algebra.*

If $\operatorname{char} k = 0$, then only the first two cases are possible.

If k is a finite field $\mathbb{F}_q$, then $\operatorname{End}(E)$ is always bigger than $\mathbb{Z}$ (see Theorem 4.3.1).

Proof. We will prove this for $k = \mathbb{C}$ in the Theorem 3.10.3. For other cases, see [10, §III.9]. □

CHAPTER 3

Elliptic Curves over $\mathbb{C}$

Abstract

In this chapter we explore the theory of elliptic curves over the field of complex numbers $\mathbb{C}$. After defining a lattice, we will introduce the elliptic curves which are meromorphic functions having two $\mathbb{R}$-linearly independent periods. A particularly important elliptic function is the so called Weierstrass $\wp$-function: in fact, the field of elliptic functions is generated over $\mathbb{C}$ by $\wp$ and $\wp'$. We will next introduce the j-invariant of a lattice and see when the toruses $\mathbb{C}/\Lambda$, $\mathbb{C}/\Lambda'$ are isomorphic as Riemann surfaces (Λ, Λ' lattices). Finally, we see how one can associate an elliptic curve to a torus $\mathbb{C}/\Lambda$.

3.1 Lattices and Bases

Definition 3.1.1. Let $n \in \mathbb{N}_+$. Let $0 < r \leq n$ be an integer and consider $(\omega_1, \omega_2, \ldots, \omega_r)$, a free family of the $\mathbb{R}$-vector space $\mathbb{R}^n$. A *lattice* is every discrete subgroup $\Lambda \subset \mathbb{R}^n - \overline{0}$ is of the form

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 + \cdots + \mathbb{Z}\omega_r$$

The integer r is called the *rank* of the lattice.

We will be interested in lattices of rank 2, so they will have the form

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2, \qquad \text{for some } \omega_1, \omega_2 \in \mathbb{C}$$

If the basis the lattice Λ over $\mathbb{Z}$ is given by $\{\omega_1, \omega_2\}$, we also write $\Lambda = [\omega_1, \omega_2]$.

Remark 3.1.2. Since neither ω_1 nor ω_2 is a real multiple of the other, we can order them so that $\mathrm{Im}(\omega_1/\omega_2) > 0$, i.e. ω_1/ω_2 lies in the complex upper half-plane

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

3.2 Elliptic Functions

Let $\Lambda = [\omega_1, \omega_2]$ be a lattice.

Definition 3.2.1. The interior of any parallelogram with vertices $z_0, z_0 + \omega_1, z_0 + \omega_2, z_0 + \omega_1 + \omega_2$ is called a *fundamental domain* or *period parallelogram* D for Λ: it is the set

$$D := \{\alpha + t_1\omega_1 + t_2\omega_2, \quad 0 \leq t_i \leq 1\}$$

We usually choose z_0 so that D contain 0.

We want now define functions on $\mathbb{C}/\Lambda$; this amounts to giving a function on $\mathbb{C}$ such that

$$f(z + \omega) = f(z) \tag{3.1}$$

as functions on $\mathbb{C}$, for all $\omega \in \Lambda$. This condition is equivalent to require that f is *doubly periodic* for Λ.

Definition 3.2.2. If $\{\omega_1, \omega_2\}$ is a basis for Λ, then a function f on $\mathbb{C}$ is doubly periodic if

$$\begin{cases} f(z + \omega_1) = f(z) \\ f(z + \omega_2) = f(z) \end{cases}$$

Definition 3.2.3. An *elliptic function* f (with respect to Λ) is a meromorphic function on $\mathbb{C}$ which is Λ-doubly periodic.

Remark 3.2.4. An elliptic function which is entire (i.e. without poles) must be constant, because it can be viewed as a continuous function on $\mathbb{C}/\Lambda$, which is compact (homeomorphic to a torus), whence the function is bounded, and therefore constant.

We now study the doubly periodic meromorphic functions for a lattice Λ, and next we interpret these functions as meromorphic functions on the quotient Riemann surface $\mathbb{C}/\Lambda$. From now on, "doubly periodic" will mean "doubly periodic and meromorphic".

Theorem 3.2.5. *Let $f(z)$ be a doubly periodic function for Λ, not identically zero, and let D be a fundamental domain for Λ such that f has no zeros or poles on the boundary ∂D. Then*

(a) $\sum_{P \in D} Res_P(f) = 0$;
here the sum is over the points in D where f has a pole.

(b) $\sum_{P\in D} ord_P(f) = 0$*;*

(c) $\sum_{P\in D} ord(f)\cdot P \equiv 0 \ mod\ \Lambda$
in (b) and in (c) the sum are over the points where it has a zero or pole (and $ord_P(f)$ *is the order of the zero or the negative of the order of the pole).*

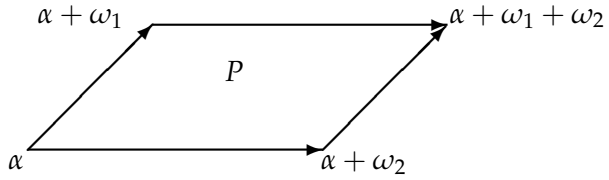
Each sum is finite.

Proof. We assume we know basic results in complex analysis, such as the residue or Liouville's theorem.

(a) According to the residue theorem,

$$\int_{\partial D} f(z)dz = 2\pi i \sum_{P\in D} \mathrm{Res}_P(f)$$

Since f is periodic, the integrals of it over opposite sides of D cancel, and so the integral is zero.



(b) f elliptic implies that f' and $\frac{f'}{f}$ are elliptic. We then apply the residue theorem to f'/f, noting that this is again doubly periodic and that $\mathrm{Res}_P(f'/f) = \mathrm{ord}_P(f)$:

$$0 = \int_{\partial D} \frac{f'}{f}(z)dz = 2\pi i \sum \text{Residues} = 2\pi i \sum \mathrm{ord}_P(f)$$

(c) We apply the residue theorem to $z\cdot f'(z)/f(z)$. This is no longer doubly periodic, but the integral of it around ∂D lies in Λ. Precisely, let $\{a_i\}$ be the singular point (zeros and poles) of f inside D, and let f have order m_i at a_i. We take integral

$$\int_{\partial D} z\frac{f'(z)}{f(z)}dz = 2\pi i \sum m_i a_i$$

because

$$\mathrm{res}_{a_i} z\frac{f'(z)}{f(z)} = m_i a_i$$

On the other hand, we compute the integral over the boundary of the parallelogram by taking it for two opposite sides at a time. One pair of such integrals is equal to

$$\int_{\alpha}^{\alpha+\omega_1} z\frac{f'(z)}{f(z)}dz - \int_{\alpha+\omega_2}^{\alpha+\omega_1+\omega_2} z\frac{f'(z)}{f(z)}dz$$

We change variables in the second integral, letting $u = z - \omega_2$. Both integrals are taken from α to $\alpha + \omega_1$, and after a cancellation, we get the value

$$-\omega_2 \int_{\alpha}^{\alpha+\omega_1} \frac{f'(u)}{f(u)} du = 2\pi i k \omega_2$$

for some integer k. The integral over the opposite sides is done in the same way. □

Remark 3.2.6. An elliptic function can be viewed as a meromorphic function on the torus $\mathbb{C}/\Lambda$, and part (a) of previous theorem can be interpreted as saying that the sum of the residues on the torus is equal to 0. Hence:

Corollary 3.2.7. *An elliptic function has at least two poles (counting multiplicities) on the torus.*

Proof. A holomorphic doubly periodic function is bounded on the closure of any fundamental domain (by compactness), and hence on the entire plane (by periodicity). It is therefore constant by Liouville's theorem. It is impossible for a doubly periodic function to have a single simple pole in a period parallelogram because, by (a) of the theorem, the residue at the pole would have to be zero there, and so the pole could not be simple. □

Part (c) means that the sum of orders of the singular points of f on the torus is equal to 0.

3.3 The Weierstrass Function

We now prove the existence of elliptic functions by writing some analytic expression. Our goal is to obtain the so called *Weierstrass function*

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda'} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right]$$

where the sum is taken over the set of all non-zero periods, denoted by Λ'. We have to show that this series converges uniformly on compact sets not including the lattice points. For bounded z, staying away from the lattice points, the expression in the brackets has the order of magnitude of $1/|\omega|^3$. Hence it suffices to prove

Lemma 3.3.1. *If $\lambda > 2$, then $\sum_{\omega \in L'} \frac{1}{|\omega|^\lambda}$ converges*

But let's start with order. Let Λ be a lattice in $\mathbb{C}$. The Riemann-Roch theorem applied to the quotient $\mathbb{C}/\Lambda$ proves the existence of nonconstant doubly periodic meromorphic functions for Λ, and - as we announces - we shall construct them explicitly for Λ. When G is a finite group acting on a

set S, it is easy to construct functions invariant under the action of G: take f to be any function $f : S \to \mathbb{C}$, and define

$$F(s) = \sum_{g \in G} f(gs)$$

then $F(g's) = \sum_{g \in G} f(g'gs) = F(s)$ because, as g runs over G, so does $g'g$; thus F is invariant, and all invariant functions are of this form. When G is not finite, one has to verify that the series converges - in fact, in order to be able to change the order of summation, one needs (at least) absolute convergence.

Recall some basic facts: let D be an open subset of G, and let $f_0, f_1, \ldots$ be a sequence of holomorphic functions on D. Recall from elementary Calculus that the series $\sum_n f_n$ is said to converge normally on a subset A of D if the series of positive terms $\sum_n \|f_n\|$ converges, where $\|f_n\| = \sup_{z \in A} |f_n(z)|$. The series $\sum_n f_n$ is then both uniformly convergent and absolutely convergent on A. When $f_0, f_1, \ldots$ is a sequence of meromorphic functions, the series is said to converges normally on A if, after a finite number of terms f_n have been removed, it becomes a normally convergent series of holomorphic functions. If a series $\sum_n f_n$ of meromorphic functions is normally convergent on compact subsets of D, then the sum f of the series is a meromorphic function on D; moreover, the series of derivatives converges normally on compact subsets of D, and its sum is the derivative of f.

Now let $\varphi(z)$ be a meromorphic function on $\mathbb{C}$ and write

$$\Phi(z) = \sum_{\omega \in \Lambda} \varphi(z + \omega)$$

Assume that as $|z| \to \infty$, $\varphi(z) \to 0$ so fast that the series for $\Phi(z)$ is normally convergent on compact subsets. Then $\Phi(z)$ is doubly periodic with respect to Λ, because replacing z by $z + \omega_0$ for some $\omega_0 \in \Lambda$ merely rearranges the terms in the sum.

To prove the normal convergence for the functions we are interested in (the Weierstrass Functions), we shall need the following result.

Lemma 3.3.2. *For any lattice Λ in G, the series $\sum_{\omega \in \Lambda - \{0\}} 1/|\omega|^3$ converges.*

Proof. Let ω_1, ω_2 be a basis for Λ, and, for each integer $n \geq 1$, consider the parallelogram

$$P(n) = \{a_1\omega_1 + a_2\omega_2 \mid a_1, a_2 \in \mathbb{R}, \max(|a_1|, |a_2|) = n\}$$

There are $8n$ points of Λ on $P(n)$, and the distance between 0 and any of them is at least kn, where k is the shortest distance from 0 to a point of

$P(1) \cap \Lambda$. Therefore, the contribution of the points on $P(n)$ to the sum is bounded by $8n/k^3n^3$, and so

$$\sum_{\omega \in \Lambda - \{0\}} \frac{1}{|\omega|^3} \leq \frac{8}{k^3} \sum_n \frac{1}{n^2} < \infty$$

□

We know from Corollary 3.2.7 that the simplest possible nonconstant doubly periodic function is one with a double pole at each point of Λ and no other poles. Suppose $f(z)$ is such a function. Then $f(z) - f(-z)$ is a doubly periodic function with no poles except perhaps simple ones at the points of Λ. Hence it must be constant, and since it is an odd function it must vanish. Thus $f(z)$ is even, and we can make it unique by imposing the normalization condition

$$f(Z) = z^{-2} + 0 + z^2 g(z)$$

with $g(z)$ holomorphic near $z = 0$. There is such a function, namely, the Weierstrass function $\wp(z)$, but we can't define it directly from $1/z^2$ by the method at the start of this subsection because $\sum_{\omega \in \Lambda} 1/(z+\omega)^2$ is not normally convergent. Instead, we define

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda - \{0\}} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right]$$

3.3.1 Summing up

The series expression for $\wp$ shows that it is meromorphic, with a double pole at each lattice point, and no other pole. Also, $\wp$ is even, i.e.

$$\wp(z) = \wp(-z)$$

(summing over the lattice points is the same as summing over their negatives).

We get $\wp'$ by differentiating term by term,

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

Note that $\wp'$ is clearly periodic, and is odd, i.e.

$$\wp'(-z) = -\wp'(z)$$

From its periodicity, we conclude that there is a constant C such that

$$\wp(z + \omega_1) = \wp(z) + C$$

Let $z = -\frac{\omega_1}{2}$ (not a pole of $\wp'$). We get

$$\wp\left(\frac{\omega_1}{2}\right) = \wp\left(-\frac{\omega_1}{2}\right) + C$$

and since $\wp$ is even, it follows that $C = 0$. Hence $\wp$ is itself periodic, something which we could not see immediately from its series expansion.

Proposition 3.3.3. *The two series $\wp(z)$ and $\wp'(z)$ converge normally on compact subsets of $\mathbb{C}$, and their sums $\wp$ and $\wp'$ are doubly periodic meromorphic functions on $\mathbb{C}$ with $\wp' = \frac{d\mathfrak{p}}{dz}$.*

Proof. Note that $\wp'(z) = \sum_{\omega\in\Lambda} \varphi(z)$, with $\varphi(z) = \frac{-2}{z^3} = \frac{d}{dz}(1/z^2)$ and that $\sum_{\omega\in\Lambda} \varphi(z+\omega)$ converges normally on any compact disk $|z| \leq r$ by comparison with $\sum \frac{1}{|\omega|^3}$. Thus, $\wp'(z)$ is a doubly periodic meromorphic function on $\mathbb{C}$ by the above remarks.

For $|z| \leq r$, and for all but the finitely many ω with $|\omega| \leq 2r$, we have that

$$\left|\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right| = \left|\frac{-z^2+2\omega z}{\omega^2(z-\omega)^2}\right| = \frac{z(2-\frac{z}{\omega})}{|\omega|^3|1-\frac{z}{\omega}|^2} \leq \frac{r^{5/2}}{|\omega^3|\cdot\frac{1}{4}} = \frac{10r}{|\omega|^3}$$

and so $\mathfrak{p}(z)$ also converges normally on the compact disk $|z| \leq r$. Because its derivative is doubly periodic, so also is $\wp$. □

3.4 The Field of Doubly Periodic Functions

Let Λ be a lattice in $\mathbb{C}$. The meromorphic functions on $\mathbb{C}$ form a field $M(\mathbb{C})$, and the doubly periodic functions form a subfield of $M(\mathbb{C})$, which we will determine in a moment. We shall see that there is a relation between $\wp$ and $\wp'$, namely

$$\wp'^2 = 4\wp^3 - g_2\wp - g_3 \tag{3.2}$$

where g_2, g_3 are to be determined.

Theorem 3.4.1. *The field of elliptic functions (with respect to the lattice Λ) is the subfield $\mathbb{C}(\wp, \wp')$ of $M(\mathbb{C})$ generated by $\wp$ and $\wp'$, i.e., every doubly periodic meromorphic function can be expressed as a rational function of $\wp$ and $\wp'$.*

Proof. If f is elliptic, we can write f as a sum of an even and an odd elliptic function as usual, namely

$$f(z) = \frac{f(z)+f(-z)}{2} + \frac{f(z)-f(-z)}{2}$$

If f is odd, then the product $f\wp'$ is even, so it will suffice to prove that $\mathbb{C}(\wp)$ is the field of even elliptic functions, i.e. if f is even, then f is a rational function of $\wp$.

Claim 3.4.2. Suppose that f is even and has a zero of order m at some point u. Then clearly f also has a zero of the same order at $-u$ because

$$f^{(k)}(u) = (-1)^k f^{(k)}(-u)$$

Similarly for poles.

If $u \equiv -u(\bmod \Lambda)$, then the above assertion holds in the strong sense, namely f has a zero (or pole) of even order at u.

Proof. First note that $u \equiv -u(\bmod \Lambda)$ is equivalent to

$$2u \equiv 0(\bmod \Lambda)$$

On the torus, there are exactly 4 points with this property, represented by

$$0, \frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2},$$

in a period parallelogram. If f is even, then f' is odd, i.e.

$$f'(u) = -f'(-u)$$

Since $u \equiv -u(\bmod \Lambda)$ and f' is periodic, it follows that $f'(u) = 0$, so that f has a zero of order at least 2 at u. If $u \not\equiv 0(\bmod \Lambda)$, then the above argument shows that the function

$$g(z) = \wp(z) - \wp(u)$$

has a zero of order at least 2 (hence exactly 2 by Theorem 3.2.5 and the fact that $\wp$ has only one pole of order 2 on the torus).

Then f/g is even, elliptic, holomorphic at u. If $f(u)/g(u) \neq 0$ then $\operatorname{ord}_u f = 2$. If $f(u)/g(u) = 0$ then f/g again has a zero of order at least 2 at u and we can repeat the argument. If $u \equiv 0(\bmod \Lambda)$ we use $g = \frac{1}{\wp}$ and argue similarly, thus proving that f has a zero of even order at u, and our claim is proved. □

Now we come back to the proof of the theorem. Let $u_i, i = 1, \ldots, r$ be a family of points containing one representative from each class $(u, -u)(\bmod \Lambda)$ where f has a zero or pole, other than the class of Λ itself. Let

$$m_i = \operatorname{ord}_{u_i} f \qquad \text{if} \qquad 2u_i \not\equiv 0(\bmod \Lambda),$$
$$m_i = \frac{1}{2}\operatorname{ord}_{u_i} f \qquad \text{if} \qquad 2u_i \equiv 0(\bmod \Lambda)$$

Our previous remarks show that for $a \in \mathbb{C}$, $a \not\equiv 0(\bmod \Lambda)$, the function $\wp(z) - \wp(a)$ has a zero of order 2 at a if and only if $2a \equiv 0(\bmod \Lambda)$, and has

distinct zeros of order 1 at a and $-a$ otherwise. Hence for all $z \not\equiv 0 (\bmod \Lambda)$ the function

$$\prod_{i=1}^{r} [\wp(z) - \wp(u_i)]^{m_i}$$

has the same order at z as f. This is also true at the origin because of Theorem 3.2.5 applied to f and the above product. The quotient of the above product by f is then an elliptic function without zero or pole, hence a constant, thereby proving Theorem 3.4.1. □

Next, we obtain the power series development of $\wp$ and $\wp'$ at the origin, form which we shall get the algebraic relation 3.2 holding between these two functions.

We compute the Laurent expansion of $\wp(z)$ near 0. Recall that for $|t| < 1$,

$$\frac{1}{1-t} = 1 + t + t^2 + \cdots$$

On differentiating this, we find that

$$\frac{1}{(1-t)^2} = \sum_{n \geq 1} n t^{n-1} = \sum_{n \geq 0} (n+1) t^n$$

Hence, for $|z| < |\omega|$,

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{1}{\omega^2} \left(\frac{1}{\left(1 - \frac{z}{\omega}\right)^2} - 1 \right) = \sum_{n \geq 1} (n+1) \frac{z^n}{\omega^{n+2}}$$

On putting this into the definition of $\wp(z)$ and changing the order of summation, we find that for $|z| < |\omega|$,

$$\begin{aligned} \wp(z) &= \frac{1}{z^2} + \sum_{\omega \in \Lambda'} \left[\frac{1}{\omega^2} \left(1 + \frac{z}{\omega} + \left(\frac{z}{\omega}\right)^2 + \cdots \right)^2 - \frac{1}{\omega^2} \right] \\ &= \frac{1}{z^2} + \sum_{\omega \in \Lambda'} \sum_{m=1}^{\infty} (m+1) \left(\frac{z}{\omega}\right)^m \frac{1}{\omega^2} \\ &= \frac{1}{z^2} + \sum_{m=1}^{\infty} c_m z^m \end{aligned}$$

where

$$c_m = \sum_{\omega \neq 0} \frac{m+1}{\omega^{m+2}}$$

Note that $c_m = 0$ if m is odd.

Using the notation

$$s_m(\Lambda) = s_m = \sum_{\omega \neq 0} \frac{1}{\omega^m} \tag{3.3}$$

we get the expansion

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty} (2n+1)s_{2n+2}(\Lambda)z^{2n} \tag{3.4}$$

from which we write down the first few terms explicitly

$$\wp(z) = \frac{1}{z^2} + 3s_4z^2 + 5s_6z^4 + \cdots$$

and differentiating term by term, we get

$$\wp'(z) = -\frac{2}{z^3} + 6s_4z + 20s_6z^3 + \cdots$$

Theorem 3.4.3. *Let* $g_2 = g_2(\Lambda) = 60s_4$ *and* $g_3 = g_3(\Lambda) = 140s_6$. *Then*

$$\wp'^2 = 4\wp^3 - g_2\wp - g_3 \tag{3.5}$$

Proof. We expand out the function

$$\varphi(z) = \wp'(z)^2 - 4\wp(z)^3 + g_2\wp(z) + g_3$$

at the origin, paying attention only to the polar term and the constant term. This is easily done, and one sees that there is enough cancellation so that these terms are 0, in other words, $\varphi(z)$ is an elliptic function without poles, and with a zero at the origin. Hence φ is identically zero, thereby proving our theorem. □

Remark 3.4.4. The preceding theorem shows that the points $(\wp(z), \wp'(z))$ lie on the curve defined by the equation

$$y^2 = 4x^3 - g_2x - g_3$$

The cubic polynomial on the right-hand side has a discriminant given by

$$\Delta = g_2^3 - 27g_3^2$$

We shall see in a moment that this discriminant does not vanish.

Let

$$e_i = \wp\left(\frac{\omega_i}{2}\right)$$

where $\Lambda = [\omega_1, \omega_2]$ and $\omega_3 = \omega_1 + \omega_2$. Then the function

$$h(z) = \wp(z) - e_i$$

has a zero at $\omega_i/2$, which is of even order so that $\wp'(\omega_i/2) = 0$ for $i = 1, 2, 3$ by previous remarks. Comparing zeros and poles, we conclude that

$$\wp'^2(z) = 4(\wp(z) - e_1)(\wp(z) - e_2)(\wp(z) - e_3)$$

Thus e_1, e_2, e_3 are the roots of $4x^3 - g_2x - g_3$. Furthermore, $\wp$ takes on the value e_i with multiplicity 2 and has only one pole of order 2 mod Λ, so that $e_i \neq e_j$ for $i \neq j$. This means that the three roots of the cubic polynomial are distinct, and therefore

$$\Delta = g_2^3 - 27g_3^2 \neq 0$$

3.5 The j-invariant of a Lattice

Elliptic functions depend on which lattice is being used, but sometimes different lattices can have basically the same elliptic functions. We say that two lattices L and L' are *homothetic* if there is a nonzero complex number $\lambda \in \mathbb{C} - \{0\}$ such that $L' = \lambda L$. Note that homothety is an equivalence relation. Homothety affects elliptic functions: if $f(z)$ is an elliptic function for L, then $f(\lambda z)$ is an elliptic function for λL. Furthermore, the $\wp$-function transforms as follows:

$$\wp(\lambda z; \lambda L) = \lambda^{-2}\wp(z; L)$$

Thus we would like to classify lattices up to homothety, and this is where the j-invariant comes in.

Definition 3.5.1. The j-invariant $j(L)$ of the lattice L is defined to be the complex number

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

Note that $j(L)$ is always defined since, as we have seen, $\Delta(L) \neq 0$.

Remark 3.5.2. The reason for the factor of 1728 is clear from Theorem 1.1.5: it is exactly the factor needed to guarantee that all of the coefficients of the q-expansion are integers without any common divisor.

The remarkable fact is that the j-invariant $j(L)$ characterizes the lattice L up to homothety:

Theorem 3.5.3. *If L and L' are lattices in $\mathbb{C}$, then $j(L) = j(L')$ if and only if L and L' are homothetic.*

Proof. It is easy to see that homothetic lattices have the same j-invariant. Namely, if $\lambda \in \mathbb{C}^*$, then the definition of $g_2(L)$ and $g_3(L)$ implies that

$$g_2(\lambda L) = \lambda^{-4}g_2(L) \tag{3.6}$$
$$g_3(\lambda L) = \lambda^{-6}g_3(L) \tag{3.7}$$

and $j(\lambda L) = j(L)$ follows easily.

Now suppose that L and L' are lattices such that $j(L) = j(L')$. We first claim that there is a complex number λ such that

$$g_2(L') = \lambda^{-4}g_2(L) \tag{3.8}$$
$$g_3(L') = \lambda^{-6}g_3(L) \tag{3.9}$$

When $g_2(L') \neq 0$ and $g_3(L') \neq 0$, we can pick a number λ such that

$$\lambda^4 = \frac{g_2(L)}{g_2(L')}$$

Since $j(L) = j(L')$, few computations show that

$$\lambda^6 = \pm \frac{g_3(L)}{g_3(L')}$$

Replacing λ by $i\lambda$ if necessary, we can assume that the above sign is $+$, and then 3.8 follows. The proof when $g_2(L') = 0$ or $g_3(L') = 0$ is similar.

In order to complete our proof, we state now the following Lemma; for the proof, see [3, §10.B].

Lemma 3.5.4. *Let $\wp(z)$ be the $\wp$-function for the lattice L, and let*

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty} (2n+1) s_{2n+2}(L) z^{2n}$$

be its Laurent expansion that we already have encountered in equation 3.4 (the function $s(\cdot)$ is defined in equation 3.3). Then, for $n \geq 1$, the coefficient $(2n+1)s_{2n+2}(L)$ of z^{2n} is a polynomial with rational coefficients, independent of L, in $g_2(L)$ and $g_3(L)$.

Now, suppose that we have lattices L and L' such that equation 3.8 holds for some constant λ. We claim that $L' = \lambda L$. To see this, first note that by equation 3.6, we have $g_2(L') = g_2(\lambda L)$ and $g_3(L') = g_3(\lambda L)$. Then the Lemma implies that $\wp(z; L')$ and $\wp(z; \lambda L)$ have the same Laurent expansion about 0, so that the two functions agree in a neighborhood of the origin, and hence $\wp(z; L') = \wp(z; \lambda L)$ everywhere. Since the lattice is the set of poles of the $\wp$-function, this proves that $L' = \lambda L$. □

Remark 3.5.5. Besides the notion of the j-invariant of a lattice, there is another way to think about the j-invariant which is useful when we study modular functions. Given a complex number τ in the upper half plane $\mathcal{H} = \{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\}$, we get the lattice $[1, \tau]$, and then the *j-function* $j(\tau)$ is defined by

$$j(\tau) = j([1, \tau])$$

The analytic properties of $j(\tau)$ play an important role in the theory of complex multiplication. An important fact is the following:

Fact 3.5.6. The j-function is surjective.

A complete proof of this impressive result is too long and far beyond the purposes of this thesis. We refer the proof to [3, §11.A].

3.6 Quotients of $\mathbb{C}$ by Lattices

Let Λ be a lattice in $\mathbb{C}$. Topologically the quotient $\mathbb{C}/\Lambda$ is isomorphic to $\mathbb{R}^2/\mathbb{Z}^2$, which is a one-holed torus. Write $\pi : \mathbb{C} \to \mathbb{C}/\Lambda$ for the quotient map. Then $\mathbb{C}/\Lambda$ can be given a complex structure for which a function $\varphi : U \to \mathbb{C}$ on an open subset U of $\mathbb{C}/\Lambda$ is holomorphic (resp. meromorphic) if and only if the composite $\varphi \circ \pi : \pi^{-1}(U) \to \mathbb{C}$ is holomorphic (resp. meromorphic) in the usual sense. It is the unique complex structure for which π is a local isomorphism of Riemann surfaces.

We shall see that, although any two quotients $\mathbb{C}/\Lambda$, $\mathbb{C}/\Lambda'$ are homeomorphic, they will be isomorphic as Riemann surfaces only if $\Lambda' = \alpha\Lambda$ for some $\alpha \in \mathbb{C}^\times$.

3.7 The Holomorphic Maps $\mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$

Let Λ and Λ' be lattices in $\mathbb{C}$. The map $\pi : \mathbb{C} \to \mathbb{C}/\Lambda$ realizes $\mathbb{C}$ as the universal covering space of $\mathbb{C}/\Lambda$. Since the same is true of $\pi' : \mathbb{C} \to \mathbb{C}/\Lambda'$, a continuous map $\varphi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ such that $\varphi(0) = 0$ will lift uniquely to a continuous map $\varphi : \tilde{\mathbb{C}} \to \mathbb{C}$ such that $\varphi(\tilde{0}) = 0$:

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\tilde{\varphi}} & \mathbb{C} \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi'} \\ \mathbb{C}/\Lambda & \xrightarrow[\varphi]{} & \mathbb{C}/\Lambda' \end{array}$$

Because π and π' are local isomorphisms of Riemann surfaces, the map go will be holomorphic if and only if $\tilde{\varphi}$ is holomorphic.

Proposition 3.7.1. *Let Λ and Λ' be lattices in $\mathbb{C}$. A complex number α such that $\alpha\Lambda \subset \Lambda'$ defines a holomorphic map*

$$[z] \mapsto [\alpha z] : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$$

sending 0 to 0, and every holomorphic map $\mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$ sending 0 to 0 is of this form (for a unique α).

Proof. It is obvious from the above remarks that α defines a holomorphic map $\mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$. Conversely, let $\varphi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ be a holomorphic map such that $\varphi(0) = 0$, and let φ be its unique lifting to a holomorphic map $\mathbb{C} \to \mathbb{C}$ sending 0 to 0. For any $\omega \in \Lambda$, the map $z \mapsto \tilde{\varphi}(z + \omega) - \tilde{\varphi}(z)$ is continuous and takes values in $\Lambda' \subset \mathbb{C}$; because $\mathbb{C}$ is connected and Λ' is discrete, it must be constant, and so its derivative is zero:

$$\tilde{\varphi}'(z + \omega) = \tilde{\varphi}'(z)$$

Therefore $\tilde{\varphi}(z)$ is doubly periodic. As it is holomorphic, it must be constant, say $\tilde{\varphi}(z) = \alpha$ for all z. On integrating, we find that $\tilde{\varphi}(z) = \alpha z + \beta$, and $\beta = \tilde{\varphi}(0) = 0$. □

From Proposition 3.7.1 we get immediately the following

Corollary 3.7.2. *The Riemann surfaces $\mathbb{C}/\Lambda$ and $\mathbb{C}/\Lambda'$ are isomorphic if and only if $\Lambda' = \alpha\Lambda$ for some $\alpha \in \mathbb{C}^\times$, i.e. if and only if Λ and Λ' are homothetic.*

Corollary 3.7.3. *Every holomorphic map $\mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ sending 0 to 0 is a homomorphism of groups.*

Proof. Clearly $[z] \mapsto [\alpha z]$ is a homomorphism of groups. □

The proposition shows that

$$\mathrm{Hom}(\mathbb{C}/\Lambda, \mathbb{C}/\Lambda') \simeq \{\alpha \in \mathbb{C} \mid \alpha\Lambda \subset \Lambda'\}$$

and the corollary shows that there is a one-to-one correspondence

$$\{\mathbb{C}/\Lambda\}/\approx \overset{1:1}{\leftrightarrow} \mathscr{L}/\mathbb{C}^\times$$

where $\mathscr{L}$ is the set of lattices in $\mathbb{C}$.

3.8 The Elliptic Curve $E(\Lambda)$

Remark 3.8.1. The Weierstrass equation 2.4 is very similar to the differential equation 3.5 for the Weierstrass $\wp$-function (in equation 2.4 set $y' = y/2$ and multiply by 4 to get a similar equation). This is no coincidence and we see why in Proposition 3.8.3.

Let Λ be a lattice in $\mathbb{C}$. As we already mentioned,

Lemma 3.8.2. *The polynomial $f(X) = 4X^3 - g_2(\Lambda)X - g_3(\Lambda)$ has distinct roots.*

Proof. The function $\wp'(z)$ is odd, so $\wp'(\omega_1/2) = -\wp'(-\omega_1/2)$, and doubly periodic, so $\wp'(\omega_1/2) = \wp'(-\omega_1/2)$. Thus, $\wp'(\omega_1/2) = 0$ and Theorem 3.4.3 shows that $\wp(\omega_1/2)$ is a root of $f(X)$. The same argument shows that $\wp(\omega_2/2)$ and $\wp((\omega_1+\omega_2)/2)$ are also roots of $f(X)$. It remains to prove that these three numbers are distinct.

The function $\wp(z) - \wp(\omega_1/2)$ has a zero at $\omega_1/2$, which must be a double zero because its derivative is also 0 there. Since $\wp(z) - \wp(\omega_1/2)$ has only one (double) pole in a fundamental domain D containing 0, Theorem 3.2.5 shows that $\omega_1/2$ is the only zero of $\wp(z) - \wp(\omega_1/2)$ in D, i.e., that $\wp(z)$ takes the value $\wp(\omega_1/2)$ only at $z = \omega_1/2$ within D. In particular, $\wp(\omega_1/2)$ is not equal to $\wp(\omega_2/2)$ or $\wp((\omega_1+\omega_2)/2)$. Similarly, $\wp(\omega_2/2)$ is not equal to $\wp((\omega_1+\omega_2)/2)$. □

From the lemma, we see that

$$E(\Lambda) : Y^2Z = 4X^3 - g_2(\Lambda)XZ^2 - g_3(\Lambda)Z^3$$

is an elliptic curve. Moreover we have $c^4 g_2(c\Lambda) = g_2(\Lambda)$ and $c^6 g_3(c\Lambda) = g_3(\Lambda)$ for any $c \in \mathbb{C}^\times$, and so $c\Lambda$ defines essentially the same elliptic curve as Λ.

For any elliptic curve

$$E : Y^2Z = X^3 + a_4XZ^2 + a_6Z^3$$

the closed subspace $E(\mathbb{C})$ of $\mathbb{P}^2(\mathbb{C})$ has a natural complex structure: for example, in a neighborhood of a point $P \in E(\mathbb{C})$ such that $y(P) \neq 0 \neq z(P)$, the function x/z provides a local coordinate.

Proposition 3.8.3. *The map*

$$\begin{array}{rcll} \psi : \mathbb{C}/\Lambda & \to & E(\Lambda)(\mathbb{C}) & \\ z & \mapsto & (\wp : \wp'(z) : 1), & z \neq 0 \\ 0 & \mapsto & (0 : 1 : 0) & \end{array}$$

is an isomorphism of Riemann surfaces.

Proof. It is certainly a well-defined map. The function $\wp(z) : \mathbb{C}/\Lambda \to \mathbb{P}^1(\mathbb{C})$ is $2 : l$ in a fundamental domain containing 0, except at the points $\frac{\omega_1}{2}, \frac{\omega_2}{2}$, where it is one-to-one. Therefore, $\wp$ realizes $\mathbb{C}/\Lambda$ as a covering of degree 2 of the Riemann sphere, and it is a local isomorphism except at the four listed points. Similarly, x/z realizes $E(\Lambda)(\mathbb{C})$ as a covering of degree 2 of the Riemann sphere, and it is a local isomorphism except at $(0 : 1 : 0)$ and the three points where $y = 0$. It follows that $\mathbb{C}/\Lambda \to E(\Lambda)(\mathbb{C})$ is an isomorphism outside the two sets of four points. A similar argument shows that it is a local isomorphism at the remaining four points. □

We show now that the map ψ of Proposition 3.8.3 is a homomorphism of groups.

Consider $\wp(z + z')$. For a fixed z', it is a doubly periodic function of z, and therefore it is a rational function of $\wp$ and $\wp'$. The next result exhibits the rational function.

Proposition 3.8.4. *The following formula holds:*

$$\wp(z + z') = \frac{1}{4}\left(\frac{\wp'(z) - \wp'(z')}{\wp(z) - \wp(z')}\right)^2 - \wp(z) - \wp(z')$$

Proof. Let $f(z)$ denote the difference of the left and the right sides. Its only possible poles (in a fundamental domain for Λ) are at 0 or $\pm z'$, and by examining the Laurent expansion of $f(z)$ near these points one sees that it has no pole at 0 or $-z'$, and at worst a simple pole at z'. Since it is doubly periodic, it must be constant, and since $f(0) = 0$, it must be identically zero. □

Corollary 3.8.5. *The map $z \mapsto (\wp(z) : \wp'(z) : 1) : \mathbb{C}/\Lambda \to E(\Lambda)$ is a homomorphism of groups.*

Proof. The above formula agrees with the formula for the x-coordinate of the sum of two points on $E(\Lambda)$: let $Y = mX + c$ be the line through the points $P = (x, y)$ and $P' = (x', y')$ on the curve $Y^2 = 4X^3 - g_4X - g_6$. Then the x, x', and $x(P + P')$ are the roots of the polynomial

$$(mX + c)^2 - 4X^3 + g_4X + g_6$$

and so

$$x(P + P') + x + x' = \frac{m^2}{4} = \frac{1}{4}\left(\frac{y - y'}{x - x'}\right)^2$$

□

3.9 Classification of Elliptic Curves over $\mathbb{C}$

We finally see that every elliptic curve E over $\mathbb{C}$ is isomorphic to $E(\Lambda)$ for some lattice Λ. In particular, we show that *every* elliptic curve over $\mathbb{C}$ arises from a *unique* Weierstrass $\wp$-function. More precisely, we have the following result:

Proposition 3.9.1 (Uniformization Theorem)**.** *Let E be an elliptic curve over $\mathbb{C}$ given by the Weierstrass equation*

$$y^2 = 4x^3 - g_2x - g_3 \tag{3.10}$$

where $g_2, g_3 \in \mathbb{C}$ and $g_2^3 - 27g_3^2 \neq 0$. Then there is a unique lattice $L \subset \mathbb{C}$ such that

$$\begin{aligned} g_2 &= g_2(L) \\ g_3 &= g_3(L) \end{aligned}$$

Proof. The existence of L follows from the surjectivity of the j-function (Fact 3.5.6) with simple considerations. The uniqueness follows from the from the proof of Theorem 3.5.3. □

Corollary 3.9.2. *Let $E/\mathbb{C}$ be an elliptic curve. There exists a lattice $\Lambda \subset \mathbb{C}$, unique up to homothety, and a complex analytic isomorphism*

$$\begin{aligned} \phi &: \mathbb{C}/\Lambda \to E(\mathbb{C}) \\ \phi(z) &= [\wp(z, \Lambda), \wp'(z, \Lambda), 1] \end{aligned}$$

Aside 3.9.3. We are now in position to prove Proposition 2.4.6.

Proposition 3.9.4. *Let $E/\mathbb{C}$ be an elliptic curve and let $m \geq 1$ be an integer.*

(a) *There is an isomorphism*

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

(b) *The multiplication-by-m map* $[m] : E \to E$ *has degree* m^2

Proof. (a) From Corollary 3.9.2, we know that $E(\mathbb{C})$ is isomorphic to $\mathbb{C}/\Lambda$ for some lattice $\Lambda \subset \mathbb{C}$. Hence

$$E[m] \cong \left(\frac{\mathbb{C}}{\Lambda}\right)[m] \cong \frac{\frac{1}{m}\Lambda}{\Lambda} \cong \left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^2$$

(b) Since $\mathrm{char}(\mathbb{C}) = 0$ and the map $[m]$ is unramified, the degree of $[m]$ is equal to the number of points in $E[m] = [m]^{-1}\{O\}$.

□

Proposition 3.9.1 is often called *uniformization theorem* for elliptic curves. It is a consequence of the properties of the j-function.

The mention of the j-function prompts our definition of the j-invariant: if an elliptic curve E over a field K is defined by the Weierstrass equation 3.10, then the *j-invariant* $j(E)$ is (as we saw already) the number

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

Remark 3.9.5. Observe that, if E is the elliptic curve over $\mathbb{C}$ corresponding to the lattice $L = [1, \tau]$, then $j(E) = j(\tau)$. Recall that, from Theorem 1.5.4 that $j(E)$ is an algebraic integer of degree exactly equal to $h(D)$, where D is the discriminant of τ, and that $H_D(X)$ is the minimal polynomial of $j(E)$.

3.10 The Structure of the Endomorphism Ring

Consider again the map ψ from Proposition 3.8.3 from the complex torus $\mathbb{C}/L$ to the projective plane

$$\begin{aligned} \psi : \mathbb{C}/L &\to E(\mathbb{C}) \\ z &\mapsto (\wp : \wp'(z) : 1), \quad z \neq 0 \\ 0 &\mapsto (0 : 1 : 0) \end{aligned}$$

We have just established the following fundamental identification:

Theorem 3.10.1. *Let L be a lattice in $\mathbb{C}$. Then the map ψ defines a bijection between $\mathbb{C}/L$ and the elliptic curve $E : y^2 = 4x^3 - g_2(L)x - g_3(L)$.*

The final theorem we will need about elliptic curves over $\mathbb{C}$ concerns the structure of the endomorphism ring.

Remark 3.10.2. We already described, in general, what are the endomorphism rings for an elliptic curve over a field k (see Theorem 2.5.4). We now prove it for $k = \mathbb{C}$.

Let $E/\mathbb{C}$ be an elliptic curve. We know that, if $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ for a lattice Λ, then

$$\mathrm{End}(E) \cong \{\alpha \in \mathbb{C} \mid \alpha\Lambda \subset \Lambda\}$$

Since Λ is unique up to homothety (a fact established in Corollary 3.7.2), this ring is independent of the choice of Λ. We use this description of $\mathrm{End}(E)$ to completely characterize the endomorphism rings that may occur.

Theorem 3.10.3. *Let $E/\mathbb{C}$ be an elliptic curve, and let ω_1 and ω_2 be generators for the lattice Λ associated to E by Corollary 3.9.2. Then exactly one of the following is true:*

(i) $\mathrm{End}(E) = \mathbb{Z}$

(ii) The field $\mathbb{Q}(\omega_2/\omega_1)$ is an imaginary quadratic extension of $\mathbb{Q}$, and $\mathrm{End}(E)$ is isomorphic to an order in $\mathbb{Q}(\omega_1/\omega_2)$.

Proof. Let $\tau = \omega_1/\omega_2$. Multiplying Λ by ω_1/ω_2 shows that Λ is homothetic to $\mathbb{Z} + \mathbb{Z}\tau$, so we may replace Λ by $\mathbb{Z} + \mathbb{Z}\tau$. Let

$$\mathcal{R} = \{\alpha \in \mathbb{C} \mid \alpha\Lambda \subset \Lambda\}$$

so $\mathcal{R} \cong \mathrm{End}(E)$. Then, for any $\alpha \in \mathcal{R}$, there are integers a, b, c, d such that

$$\alpha = a + b\tau \quad \text{and} \quad \alpha\tau = c + d\tau$$

Eliminating τ from these equations yields

$$\alpha^2 - (a+d)\alpha + ad - bc = 0$$

This proves that $\mathcal{R}$ is an integral extension of $\mathbb{Z}$.

Now suppose that $\mathcal{R} \neq \mathbb{Z}$ and choose some $\alpha \in \mathcal{R}/\mathbb{Z}$. Then, with notation as above, we have $b \neq 0$, so eliminating α gives a non-trivial equation

$$b\tau^2 - (a-d)\tau - c = 0$$

It follows that $\mathbb{Q}(\tau)$ is an imaginary quadratic extension of $\mathbb{Q}$ (note that $\tau \neq \mathbb{R}$). Finally, since $\mathcal{R} \subset \mathbb{Q}(\tau)$ and $\mathcal{R}$ is integral over $\mathbb{Z}$, it follows that $\mathcal{R}$ is an order in $\mathbb{Q}(\tau)$. □

Example 3.10.4. We exhibit some endomorphisms of elliptic curves not in $\mathbb{Z}$.

(a) Consider
$$E : Y^2Z = X^3 + aXZ^2$$
and let $i = \sqrt{-1} = 1^{\frac{1}{4}}$. Then $(x : y : z) \mapsto (-x : iy : z)$ is an endomorphism of E of order 4, and so $\mathrm{End}(E) = \mathbb{Z}[i]$. Note that E has j-invariant 1728.

(b) Consider
$$E : Y^2Z = X^3 + bZ^3$$
and let $\rho = e^{2\pi i/3} = 1^{\frac{1}{3}}$. Then $(x : y : z) \mapsto (\rho x : y : z)$ is an endomorphism of E of order 3 of E. In this case, E has j-invariant 0.

3.11 Complex Multiplication

We end this chapter by exploring in more detail the following connections, a topic we introduced in Theorem 1.5.4.

Let $K = \mathbb{Q}(\sqrt{D})$ be an imaginary quadratic field, let $\mathcal{O}_K$ be its ring of integers, and let $C(\mathcal{O}_K)$ be the ideal class group of $\mathcal{O}_K$.

Remark 3.11.1. If we fix an embedding $K \hookrightarrow \mathbb{C}$, then each ideal Λ of $\mathcal{O}_K$ is a lattice $\Lambda \subset \mathbb{C}$, so we may consider the elliptic curve $\mathbb{C}/\Lambda$.

From Proposition 3.7.1 we have
$$\mathrm{End}(\mathbb{C}/\Lambda) \cong \{\alpha \in \mathbb{C} \mid \alpha\Lambda \subset \Lambda\} = \mathcal{O}_K$$
Further, Corollary 3.7.2 says that up to isomorphism, the elliptic curve $\mathbb{C}/\Lambda$ depends only on the ideal class $[\Lambda] \in C(\mathcal{O}_K)$.

Conversely, suppose that $E/\mathbb{C}$ satisfies $\mathrm{End}(E) \cong \mathcal{O}_K$. Then Corollary 3.9.2 implies that $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ for a unique ideal class $[\Lambda] \in C(\mathcal{O}_K)$. We have proven the following result.

Proposition 3.11.2. *With notation as above, there is a 1-1 correspondence between ideal classes in $C(\mathcal{O}_K)$ and isomorphism classes of elliptic curves $E/\mathbb{C}$ with $\mathrm{End}(E) \cong \mathcal{O}_K$.*

Corollary 3.11.3. *(a) There are only finitely many isomorphism classes of elliptic curves $E/\mathbb{C}$ with $\mathrm{End}(E) \cong \mathcal{O}_K$.*

(b) Let $E/\mathbb{C}$ be an elliptic curve with $\mathrm{End}(E) \cong \mathcal{O}_K$. Then $j(E)$ is algebraic over $\mathbb{Q}$.

Proof. (a) Clear from Proposition 3.11.2, since $\mathcal{O}_K$ is finite.

(b) Let $\sigma \in \mathrm{Aut}(\mathbb{C}/\mathbb{Q})$. Then

$$\mathrm{End}(E^\sigma) \cong \mathrm{End}(E) \cong \mathcal{O}_K$$

It follows from (a) that $\{E^\sigma \mid \sigma \in \mathrm{Aut}(\mathbb{C}/\mathbb{Q})\}$ contains only finitely many isomorphism classes of elliptic curves. Since $j(E^\sigma) = j(E)^\sigma$, the set $\{j(E)^\sigma \mid \sigma \in \mathrm{Aut}(\mathbb{C}/\mathbb{Q})\}$ is finite. It follows that $j(E)$ is algebraic over $\mathbb{Q}$.

□

Actually, we can say quite a bit more about the j-invariant of an elliptic curve having complex multiplication. For $[\Lambda] \in C(\mathcal{O}_K)$, we denote the j-invariant of $\mathbb{C}/\Lambda$ by $j(\Lambda)$.

Theorem 3.11.4 (Weber, Feuter)**.** *Let $[\Lambda] \in C(\mathcal{O}_K)$.*

(a) $j(\Lambda)$ is an algebraic integer

(b) $[K(j(\Lambda)) : K] = [\mathbb{Q}(j(\Lambda)) : \mathbb{Q}] = |\mathcal{O}_K|$

(c) The field $K_H = K(j(\Lambda))$ is the maximal unramified abelian extension of K, i.e. K_H is the Hilbert class field of K.

(d) Let $\{\Lambda_1\}, \ldots, \{\Lambda_h\}$, be a complete set of representatives for $C(\mathcal{O}_K)$. Then $j(\Lambda_1), \ldots, j(\Lambda_h)$ is a complete set of Gal$(\overline{K}/K)$ conjugates for $j(\Lambda)$.

Proof. See [10, §C.11]. □

Example 3.11.5. Suppose that $E/\mathbb{Q}$ is an elliptic curve with complex multiplication, and suppose that $\mathrm{End}(E)$ is the full ring of integers $\mathcal{O}_K$ in the field $K = \mathrm{End}(E) \otimes \mathbb{Q}$. (Note that Theorem 3.10.3 tells us that K is imaginary quadratic). Since $j(E) \in \mathbb{Q}$ it follows from Theorem 3.11.4(c) that

$$K_H = K(j(E)) = K$$

and thus K has class number $h = 1$. Conversely, if $K/\mathbb{Q}$ is an imaginary quadratic field with class number $h = 1$, then Theorem 3.11.4(b),(c) implies that

$$j(\Lambda) \in \mathbb{Q} \quad \forall [\Lambda] \in C(\mathcal{O}_K)$$

For example, this is true for $\Lambda = \mathcal{O}_K$. Hence $\mathbb{C}/\Lambda$ is (analytically) isomorphic to an elliptic curve $E/\mathbb{Q}$ satisfying $j(E) = j(\Lambda)$ and $\mathrm{End}(E) \cong \mathbb{O}_K$.

We have seen in Theorem 1.2.16 that there are exactly 9 imaginary quadratic fields whose ring of integers has class number $h = 1$, hence there are only 9 possible j-invariants for elliptic curves E defined over $\mathbb{Q}$ for which $\mathrm{End}(E)$ is the full ring of integers in $\mathrm{End}(E) \otimes \mathbb{Q}$.

Let $[\Lambda] \in C(\mathcal{O}_K)$. Then Theorem 3.11.4 tells us that the Galois group $\mathrm{Gal}(K_H/K)$ acts on $K(j(\Lambda))$. This action can be described quite precisely in terms of the Artin map (recall definitions and properties of Section 1.5.1).

Theorem 3.11.6 (Hasse)**.** *Let $[\Lambda] \in C(\mathcal{O}_K)$ and let $K_H = K(j(\Lambda))$ be as in Theorem 3.11.4. For each prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, let $\phi_\mathfrak{p} \in Gal(K_H/K)$ be the Frobenius element corresponding to $\mathfrak{p}$. Suppose that there is an elliptic curve with j-invariant $j(\Lambda)$ defined over K_H that has good reduction at all primes of K_H lying over $\mathfrak{p}$. Then*

$$j(\Lambda)^{\phi_\mathfrak{p}} = j(\Lambda \cdot \mathfrak{p}^{-1})$$

where $\Lambda \cdot \mathfrak{p}^{-1}$ is the usual product of fractional ideals in K.

We shall see explicitly in Chapter 5 how to build the class polynomial.

CHAPTER 4

Elliptic Curves Over Finite Fields

Abstract

In this chapter we specialize to the study of elliptic curves defined over a finite field $k = \mathbb{F}_q$. The most important arithmetic quantity associated to an elliptic curve defined over a finite field $\mathbb{F}_q$ is its number of rational points. After introducing the Frobenius map, we prove a theorem of Hasse that says that if $E/\mathbb{F}_q$ is an elliptic curve, then $E(\mathbb{F}_q)$ has approximately q points, with an error of no more than $2\sqrt{q}$. We then study the endomorphism ring of an elliptic curve defined over a finite field. We let q be a power of a prime p, $\mathbb{F}_q$ a finite field with q elements, and $\overline{\mathbb{F}}_q$ an algebraic closure of $\mathbb{F}_q$.

4.1 The Frobenius Map

We start by introducing the Frobenius morphism. Let K be a field of characteristic $p > 0$, let $q = p^r$. Recall that the Frobenius map

$$\begin{array}{ccc} K & \to & K \\ x & \mapsto & x^p \end{array}$$

is an isomorphism of K. Let E/K be the elliptic curve $E : y^2 = x^3 + ax + b$ defined over K given by a Weierstrass equation. We define the curve $E^{(q)}/K$ by raising the coefficients of the equation for E to the q^{th} power

$$E^{(q)} : y^2 = x^3 + a^q x + b^q$$

We define then the Frobenius morphism ϕ_q

$$\begin{array}{ccc} \phi_q : E & \to & E^{(q)} \\ (x, y) & \mapsto & (x^q, y^q) \end{array}$$

Since $E^{(q)}$ is the zero locus of a Weierstrass equation, it will be an elliptic curve provided that its equation is nonsingular. Writing everything out in terms of Weierstrass coefficients and using the fact that the q^{th}-power map $K \to K$ is a homomorphism, it is clear that

$$\Delta(E^{(q)}) = \Delta(E)^q \quad \text{and} \quad j(E^{(q)}) = j(E)^q$$

In particular, the equation for $E^{(q)}$ is nonsingular.

Now suppose that $\mathbb{F}_q$ is a finite field with q elements. Then the q^{th}-power map on K is the identity, so $E^{(q)} = E$ and ϕ_q is an endomorphism of E, called the Frobenius endomorphism. In fact, more is true. Recall that an isogeny is a map between elliptic curves that sends O to O, the distinguished point. We have the following

Fact 4.1.1. ϕ_q is an isogeny.

The set of points fixed by ϕ_q is exactly the finite group $E(\mathbb{F}_q)$. This fact lies at the heart of Hasse's proof of the estimate for $\#E(\mathbb{F}_q)$ that we shall see in a moment.

Aside 4.1.2. Before going any further, we recall some basic facts of maps between elliptic curves. We need them to prove Hasse's theorem, but in order not to burden the discussion too much, we omit the proofs and refer them to [10, §III].

Let C_1/K and C_2/K be curves and let $\phi : C_1 \to C_2$ be a non-constant rational map defined over K. Recall the definitions we gave in the paragraph Aside 2.4.4. We shall need the following results.

Proposition 4.1.3. *Let $f : E_1 \to E_2$ be a non-zero isogeny of elliptic curves. Then*

$$\ker f = f^{-1}(O)$$

is a finite group. Moreover, if f is separable, then f is unramified, $\#\ker f = \deg f$ (and $\overline{K}(E_1)$ is a Galois extension of $f^*\overline{K}(E_2)$).

Proposition 4.1.4. *Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$ of characteristic p, let $\phi : E \to E$ be the q-th power Frobenius morphism, and let $m, n \in \mathbb{Z}$. Then the map*

$$m + n\phi : E \to E$$

is separable if and only if $p \nmid m$. In particular, the map $1 - \phi$ is separable.

Remark 4.1.5. We have $\deg \phi_q = q$.

In order to prove Hasse's theorem we need a last definition and result (see [10, §III.6]).

Definition 4.1.6. Let A be an abelian group. A function

$$d : A \to \mathbb{R}$$

is a *quadratic form* if it satisfies the following conditions:

(i) $d(\alpha) = d(-\alpha)$ for all $\alpha \in A$

(ii) The pairing

$$A \times A \to \mathbb{R}, \quad (\alpha, \beta) \mapsto d(\alpha + \beta) - d(\alpha) - d(\beta)$$

is bilinear.

A quadratic form d is *positive definite* if it further satisfies:

(iii) $d(\alpha) \geq 0$ for all $\alpha \in A$

(iv) $d(\alpha) = 0$ if and only if $\alpha = 0$.

Fact 4.1.7. Let E_1 and E_2 be elliptic curves. The degree map

$$\deg : \mathrm{Hom}(E_1, E_2) \to \mathbb{Z}$$

is a positive definite quadratic form.

4.1.1 Number of Rational Points

Let $E/\mathbb{F}_q$ be an elliptic curve defined over a finite field. We wish to estimate the number of points in $E(\mathbb{F}_q)$, or equivalently, one more than the number of solutions to the equation

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

with $(x, y) \in \mathbb{F}_q^2$.

Remark 4.1.8. Since each value of x yields at most two values for y, a trivial upper bound is

$$\#E(\mathbb{F}_q) \leq 2q + 1$$

However, since a "random1y chosen"" quadratic equation has a 50% chance of being solvable in $\mathbb{F}_q$, we expect that the right order of magnitude should be q, rather than $2q$.

Next result, conjectured by E. Artin and proved by Hasse, shows that this heuristic reasoning is correct. We start with the following lemma, which is a version of the Cauchy-Schwarz inequality.

Lemma 4.1.9. *Let A be an abelian group, and let*

$$d : A \to \mathbb{Z}$$

be a positive definite quadratic form. Then

$$\mid d(\psi - \phi) - d(\phi) - d(\psi) \mid \leq 2\sqrt{d(\phi)d(\psi)}$$

for all $\psi, \phi \in A$.

Proof. For $\psi, \phi \in A$, let

$$L(\psi, \phi) = d(\psi - \phi) - d(\phi) - d(\psi)$$

be the bilinear form associated to the quadratic form d. Since d is positive definite, we have for all $m, n \in \mathbb{Z}$,

$$0 \leq d(m\psi - n\phi) = m^2 d(\psi) + mnL(\psi, \phi) + n^2 d(\phi).$$

1n particular, taking

$$m = -L(\psi, \phi) \quad \text{and} \quad n = 2d(\psi)$$

yields

$$0 \leq d(\psi)(4d(\psi)d(\phi) - L(\psi, \phi)^2).$$

This gives the desired inequality, provided that $\psi \neq 0$, while for $\psi = 0$ the original inequality is trivial. □

We are now ready to state and prove Hasse's theorem.

Theorem 4.1.10 (Hasse)**.** *Let $E/\mathbb{F}_q$ be an elliptic curve defined over a finite field. Then*

$$\mid \#E(\mathbb{F}_q) - q - 1 \mid \leq 2\sqrt{q}$$

Proof. Choose a Weierstrass equation for E with coefficients in $\mathbb{F}_q$, and let

$$\begin{array}{rcl} \phi : E & \to & E, \\ (x, y) & \mapsto & (x^q, y^q) \end{array}$$

be the q^{th}-power Frobenius morphism. Since the Galois group $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ is generated by the q^{th}-power map on $\overline{F}_q$, we see that for any point $P \in E(\overline{\mathbb{F}}_q)$,

$$P \in E(\mathbb{F}_q) \Leftrightarrow \phi(P) = P$$

Thus

$$E(\mathbb{F}_q) = \ker(1 - \phi)$$

so using Proposition 4.1.4 and Proposition 4.1.3, we find that

$$\#E(\mathbb{F}_q) = \#\ker(1-\phi) = \deg(1-\phi)$$

In this passage, we stress the importance of knowing that the map $1-\phi$ is separable. Since the degree map on $\mathrm{End}(E)$ is a positive definite quadratic form (see Fact 4.1.7) and since $\deg\phi = q$, Lemma 4.1.9 gives the desired result. □

Remark 4.1.11. Hasse's theorem gives a bound for the number of points in $E(\mathbb{F}_q)$, but it does not provide a practical algorithm for computing $\#E(\mathbb{F}_q)$ when q is large. That's where Schoof's algorithm comes in, by computing deterministically $\#E(\mathbb{F}_q)$ in polynomial time $O(\log^{8+o(1)} q)$ elementary operations (or $O(\log^{5+o(1)} q)$, if we use fast exponentiation arithmetic).

Remark 4.1.12. Let $E/\mathbb{F}_q$ be an elliptic curve, and let $P, Q \in E(\mathbb{F}_q)$ be points such that Q is in the subgroup generated by P. The elliptic curve discrete logarithm problem (ECDLP) asks for an integer m satisfying $Q = [m]P$. If q is small, we can compute $P, [2]P, [3]P, \ldots$ until we find Q, but for large values of q it is quite difficult to find m. This has led people to create public key cryptosystems based on the difficulty of solving the ECDLP.

4.2 The Trace of the Frobenius Map

We want now to state and prove Theorem 4.2.5, which involves the trace of the Frobenius map. It is of fundamental importance in our task to compute the cardinality $\#E(\mathbb{F}_q)$. We prepare the proof by collecting the following facts and propositions involving the so-called Tate module.

Also in this case, a complete and accurate treatment of the theory related to Tate modules would dramatically increase the volume of the present work, so for practical reasons we limit ourselves to deal with the strictly necessary. For all the details, we consider reading [10, §III and §IV].

4.2.1 The Tate Module

Let E/K be an elliptic curve and consider an integer $m \geq 2$ prime to $\mathrm{char}(K)$ if $\mathrm{char}(K) > 0$. As we have seen in Proposition 3.9.4, we have

$$E[m] \cong \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}$$

the isomorphism being one between abstract groups. However, the group $E[m]$ comes equipped with considerably more structure than an abstract group. For example, each element σ of the Galois group $\mathrm{Gal}(\overline{K}/K)$ acts on $E[m]$, since if $[m]P = O$, then

$$[m](P^\sigma) = ([m]P)^\sigma = O^\sigma = O$$

We thus obtain a representation

$$\mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(E[m]) \cong \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$$

where the latter isomorphism involves choosing a basis for $E[m]$. Individually, for each m, these representations are not completely satisfactory, since it is generally easier to deal with representations whose matrices have coefficients in a ring of characteristic 0. We are going to fit together these mod m representations for varying m in order to create a characteristic 0 representation. To do this, we mimic the inverse limit construction of the l-adic integers $\mathbb{Z}_l$ from the finite groups $\mathbb{Z}/l^n\mathbb{Z}$.

Definition 4.2.1. Let E be an elliptic curve and let $l \in \mathbb{Z}$ be a prime. The (l-adic) *Tate module* of E is the group

$$T_l(E) := \varprojlim_n E[l^n]$$

the inverse limit being taken with respect to the natural maps

$$E[l^{n+1}] \xrightarrow{[l]} E[l^n]$$

Remark 4.2.2. Since each $E[l^n]$ is a $\mathbb{Z}/l^n\mathbb{Z}$-module, we see that the Tate module has a natural structure as a $\mathbb{Z}_l$-module. Further, since the multiplication-by-l maps are surjective, the inverse limit topology on $T_l(E)$ is equivalent to the l-adic topology that it gains by being a $\mathbb{Z}_l$-module.

Remark 4.2.3. The Tate module is a useful tool for studying isogenies. Let

$$\phi : E_1 \to E_2$$

be an isogeny of elliptic curves. Then ϕ induces maps

$$\phi : E_1[l^n] \to E_2[l^n]$$

and hence it induces a $\mathbb{Z}_l$-linear map

$$\phi_l : T_l(E_1) \to T_l(E_2)$$

We thus obtain a natural homomorphism

$$\mathrm{Hom}(E_1, E_2) \to \mathrm{Hom}(T_l(E_1), T_l(E_2))$$

Further, if $E_1 = E_2 = E$, then the map

$$\mathrm{End}(E) \to \mathrm{End}(T_l(E))$$

is even a homomorphism of rings.

Now, For each integer $n \geq 1$, let $\mathbb{F}_{q^n}$ be the extension of $\mathbb{F}_q$ of degree n, so $\#\mathbb{F}_{q^n} = q^n$. Let l be a prime different from $p = \text{char}(\mathbb{F}_q)$. Having in mind the representation

$$\begin{array}{rcl} \text{End}(E) & \to & \text{End}(T_l(E)) \\ \psi & \mapsto & \psi_l \end{array}$$

choose a $\mathbb{Z}$-basis for $T_l(E)$: we can write ψ_l as a 2×2 matrix and compute its determinant $\det(\psi_l) \in \mathbb{Z}_l$ and trace $\text{tr}(\psi_l) \in \mathbb{Z}_l$. We need the following

Proposition 4.2.4. *Let $\psi \in End(E)$. Then*

$$det(\psi_l) = deg(\psi)$$

and

$$tr(\psi_l) = 1 + deg(\psi) - deg(1 - \psi)$$

In particular $det(\psi_l)$ and $tr(\psi_l)$ are in $\mathbb{Z}$ and are independent of l.

Proof. See [10, §III.8]. □

By applying this proposition to an elliptic curve over a finite field, we are finally in the position to prove Theorem 4.2.5. This enables us to compute the number of points and to deduce an important property of the Frobenius endomorphism.

4.2.2 The Theorem

Theorem 4.2.5. *Let $E/\mathbb{F}_q$ be an elliptic curve, let*

$$\begin{array}{rcl} \phi : E & \to & E \\ (x, y) & \mapsto & (x^q, y^q) \end{array}$$

be the q^{th}-power Frobenius endomorphism, and let

$$a = q + 1 - \#E(\mathbb{F}_q)$$

(a) Let $\alpha, \beta \in \mathbb{C}$ be the roots of the polynomial $T^2 - aT + q$. Then α, β are complex conjugates satisfying $|\alpha| = |\beta| = \sqrt{q}$, and for every $n \geq 1$,

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

(b) The Frobenius endomorphism satisfies

$$\phi^2 - a\phi + q = 0$$

in $End(E)$

Proof. We already observed in the proof of Hasse's theorem that

$$\#E(\mathbb{F}_q) = \deg(1-\phi)$$

By Proposition 4.2.4 we can compute

$$\begin{aligned} \det(\phi_l) &= \deg(\phi) = q, \\ \operatorname{tr}(\phi_l) &= 1 + \deg(\phi) - \deg(1-\phi) = 1 + q - \#E(\mathbb{F}_q) = a \end{aligned}$$

Hence the characteristic polynomial of ϕ_l is

$$\det(T-\phi_l) = T^2 - \operatorname{tr}(\phi_l)T + \det(\phi_l) = T^2 - aT + q$$

(a) Since the characteristic polynomial of ϕ_l has coefficients in $\mathbb{Z}$, we can factor it over $\mathbb{C}$ as

$$\det(T-\phi_l) = T^2 - aT + q = (T-\alpha)(T-\beta)$$

For every rational number $m/n \in \mathbb{Q}$ we have

$$\det\left(\frac{m}{n} - \phi_l\right) = \frac{\det(m-n\phi_l)}{n^2} = \frac{\deg(m-n\phi)}{n^2} \geq 0$$

Thus the quadratic polynomial $\det(T-\phi_l) = T^2 - aT + q \in \mathbb{Z}[T]$ is nonnegative for all $T \in \mathbb{R}$, so either it has complex conjugate roots or it has a double root. In either case we have $|\alpha| = |\beta|$, and then from

$$\alpha\beta = \det\phi_l = \deg\phi = q$$

we deduce that

$$|\alpha| = |\beta| = \sqrt{q}$$

This gives the first part of (a).

Similarly, for each integer $n \geq 1$, the $(q^n)^{\text{th}}$-power Frobenius endomorphism satisfies

$$\#E(\mathbb{F}_{q^n}) = \deg(1-\phi^n)$$

It follows that the characteristic polynomial of ϕ_l^n is given by

$$\det(T-\phi_l^n) = (T-\alpha^n)(T-\beta^n)$$

(To see this, put ϕ_l into Jordan normal form, so it is upper triangular with α and β on the diagonal). In particular,

$$\begin{aligned} \#E(\mathbb{F}_q) &= \deg(1-\phi^n) \\ &= \det(1-\phi_l^n) \qquad \text{from Proposition 4.2.4} \\ &= 1 - \alpha^n - \beta^n + q^n \end{aligned}$$

(b) The Cayley-Hamilton theorem[(1)] tells us that ϕ_l satisfies its characteristic polynomial, so $\phi_l^2 - a\phi_l + q = 0$. Applying Proposition 4.2.4 gives

$$\deg(\phi^2 - a\phi + q) = \det(\phi_l^2 - a\phi_l + q) = \det(0) = 0$$

so $\phi^2 - a\phi + q$ is the zero map in $\mathrm{End}(E)$.

□

Remark 4.2.6. Let $E/\mathbb{F}_q$ be an elliptic curve. The quantity

$$a = q + 1 - \#E(\mathbb{F}_q)$$

is called the trace of Frobenius, because one can see that it is equal to the trace of the q-power Frobenius map considered as a linear transformation of $T_l(E)$. Thus if ϕ denotes the q-power Frobenius map, then Proposition 4.2.4 gives

$$\mathrm{tr}(\phi_l) = 1 + \deg(\phi) - \deg(1 - \phi) = 1 + q - \#E(\mathbb{F}_q) = a.$$

4.3 The Endomorphism Ring

We want now to describe the endomorphism ring of elliptic curves over finite fields $\mathbb{F}_q$. We already saw in the Theorem 2.5.4 what happens for a general field k. If $\mathrm{char}\, k = q$ is prime, we have the following theorem.

Theorem 4.3.1. *If E is an elliptic curve over $\mathbb{F}_q$, then $End_{\overline{\mathbb{F}}_q}(E)$ is either*

(i) an order in an imaginary quadratic field, or

(ii) an order in a quaternion algebra.

Remark 4.3.2. In particular, for elliptic curves over a finite field K, $\mathrm{End}_{\overline{K}}(E)$ is always bigger than $\mathbb{Z}$.

Definition 4.3.3. In case (i), we say that E is *ordinary*, or that E has Hasse invariant 1. In case (ii), we say that E is *supersingular*, or that E has Hasse invariant 0.

For the proof of this result, see [10, §V.3].

For completeness, we report here a shortened version of [10, Theorem V.3.1]:

[(1)] Every square matrix over a commutative ring satisfies its own characteristic equation.

Theorem 4.3.4. *Let K be a field of characteristic p, and let E/K be an elliptic curve. For each integer $r \geq 1$, let*

$$\phi_r : E \to E^{(p^r)}$$

be the p^r-power Frobenius map.

(a) The following are equivalent:

(i) $E[p^r] = 0$ for one (all) $r \geq 1$

(ii) $End(E)$ is an order in a quaternion algebra

(b) If the equivalent conditions in (a) do not hold, then $E[p^r] = \mathbb{Z}/p^r\mathbb{Z}$ for all $r \geq 1$. If further $j(E) \in \overline{\mathbb{F}}_p$, then $End(E)$ is an order of a quadratic imaginary field.

We end this chapter by providing explicit equations for elliptic curves over a finite field with given endomorphism ring. Recall Proposition 2.1.15, and let $p \in \mathbb{Z}$ be a prime that splits in $\mathcal{O}_K$. Call $\rho(D)$ the number of roots of unity in the quadratic order of discriminant D; so $\rho(D) = 2$ if $D < -4$, $\rho(-4) = 4$ and $\rho(-3) = 6$. We have

Proposition 4.3.5. *There exist exactly $\rho(D) := \#\mathcal{O}_K^\times$ twists of elliptic curves modulo p with complex multiplication by $\mathcal{O}_K$, the quadratic order of discriminant D. These correspond to the factorizations $p = (\zeta\pi)(\overline{\zeta\pi})$, where ζ runs over all $\rho(D)$-roots of unity (in particular, $\zeta = \pm 1$ if $D < -4$).*

We now determine, in each case, the explicit equation of elliptic curves E modulo p with complex multiplication by an order in a quadratic number field $K = \mathbb{Q}(\sqrt{D})$, where p splits as a product of two elements. We suppose that p, D are given.

Since p splits in the order of discriminant D, we have $\rho(D) \mid p-1$. Now let

$$A := \{g \in \mathbb{Z}/p\mathbb{Z} \text{ such that } g^{(p-1)/q} \neq 1 \text{ for each prime } q \mid \rho(D)\}$$

We have

$$\#A = \begin{cases} \frac{p-1}{3} & \text{if } D = -3 \\ \frac{p-1}{2} & \text{otherwise} \end{cases}$$

Choose a value $g \in A$. We distinguish three cases:

$D = -3$ The six isomorphism classes of elliptic curves with complex multiplication by the order of discriminant $D = -3$ are given by the affine equations

$$y^2 = x^3 - g^k, \quad 0 \leq k \leq 5$$

$D = -4$ The four isomorphism classes of elliptic curves with complex multiplication by the order of discriminant $D = -4$ are given by the affine equations

$$y^2 = x^3 - g^k x, \quad 0 \leq k \leq 3$$

$D < -4$ Set

$$c = \frac{j}{j - 1728},$$

where is the j-invariant which corresponds to the order of discriminant D. Then the two isomorphism classes of elliptic curves with given j-invariant and with complex multiplication by the order of discriminant D can be given by the affine equations

$$\begin{aligned} y^2 &= x^3 + 3cx + 2c \\ y^2 &= x^3 + 3ca^2x + 2ca^3 \end{aligned} \tag{4.1}$$

where $a \in \mathbb{F}_p$, a not a square. For what we have said, one of these curves will have $p + 1 - t$ rational points, and the other will have $p + 1t$ rational points.

CHAPTER 5

Reduction modulo $\mathfrak{p}$ and CM method

Abstract

In this chapter we explore the interaction between elliptic curves over finite fields and elliptic curves over $\mathbb{C}$. In particular, given an elliptic curve E over a number field K, we consider the operation of *reducing E modulo* a prime $\mathfrak{p}$ of $\mathcal{O}_K$ lying above a given rational prime p. A theorem of Deuring says that any elliptic curve over $\mathbb{F}_p$, and with a non-trivial endomorphism, can be considered as the reduction of some elliptic curve over a number field with the same endomorphism ring.

As an application of these results, we consider the problem of finding an elliptic curve E over a finite field, such that $\mathrm{End}(E)$ is given. We refer to this problem as the *Complex Multiplication method* (or CM method, for short). We see also a method of building an elliptic curve over a finite field with a given number of rational points.

5.1 Reduction of an Elliptic Curve modulo p

We start with the simple case of reducing an elliptic curve whose coefficients are in $\mathbb{Q}$. Consider an elliptic curve in projective coordinates

$$E : Y^2Z = X^3 + aXZ^2 + bZ^3$$

where $a, b \in \mathbb{Q}$, $\Delta = 4a^3 + 27b^2 \neq 0$. After a change of variables $X \mapsto X/c^2$, $Y \mapsto Y/C^3$, $Z \mapsto Z$, we may suppose that the coefficients a, b lie in $\mathbb{Z}$, and so we may look at them modulo p to obtain a curve $\overline{E}$ over the field $\mathbb{F}_q := \mathbb{Z}/q\mathbb{Z}$.

Suppose for simplicity that char $k \neq 2, 3$. The reduced curve

$$\overline{E} : Y^2Z = X^3 + \overline{a}XZ^2 + \overline{b}Z^3$$

may be singular or not. We are interested only in the case in which $\overline{E}$ is again an elliptic curve over $\mathbb{F}_q$. This happens if $q \neq 2$ and q does not divide Δ: we say that the reduction is *good*. For a point $P = (x : y : z)$ on E, we can choose a representative (x, y, z) for P with $x, y, z \in \mathbb{Z}$ and having no common factor, and then $\overline{P} := (\overline{x} : \overline{y} : \overline{z})$ is a well-defined point on E. Since $(0 : 1 : 0)$ reduces to $(0 : 1 : 0)$ and lines reduce to lines, the map $E(\mathbb{Q}) \to \overline{E}(\mathbb{F}_q)$ is a homomorphism.

If the reduction is *bad*, i.e. $\Delta \equiv 0 \bmod q$, then the curve is singular and can be cuspidal or nodal. We will not consider these cases.

5.2 A theorem of Deuring

We see now what happens more in general. Let K be a number field and consider the elliptic curve

$$E : y^2 = x^3 + ax + b$$

where $a, b \in K$. We are interested in the operation of *reducing E modulo a prime* $\mathfrak{p}$ of $\mathcal{O}_K$ lying above p, i.e. such that $\mathfrak{p} \cap \mathbb{Z} = p$. This cannot be done in general, but suppose that a, b can be written in the form α/β, where $\alpha, \beta \in \mathcal{O}_K$ and $\beta \notin \mathfrak{p}$. Then we can define the images $\overline{a}, \overline{b}$ in the finite field $\mathbb{F}_\mathfrak{p} := \mathcal{O}_K/\mathfrak{p}$. If in addition we have

$$\Delta = -16(4\overline{a}^3 + 27\overline{b}^2) \neq 0 \in \mathcal{O}_K/\mathfrak{p}$$

then

$$\overline{E} : y^2 = x^3 + \overline{a}x + \overline{b}$$

defines an elliptic curve of $\mathcal{O}_K/\mathfrak{p}$, and we say that E has a *good reduction* modulo $\mathfrak{p}$, or that $\mathfrak{p}$ is a *prime of good reduction*.

In the 1940s, Deuring developed a theory concerning the reduction of elliptic curves. While the full statements of Deuring's results is beyond the scope of this thesis, we will state without proof in Theorem 5.2.3 a result that defines the behaviour of the endomorphism ring of an elliptic curve under reduction modulo a prime: full statements and proofs can be found in [4, §13.4]. We start by defining the *non-degenerate* reduction.

5.2.1 Non-degenerate Reduction

Let A be a local ring without zero divisors, and with maximal ideal $\mathfrak{m}$. Consider an elliptic curve E defined to be an absolutely integral smooth equation

$$f(X, Y, Z) = 0$$

in projective space and with coefficients in A.

Definition 5.2.1. The elliptic curve E is said to have *non-degenerate reduction modulo* $\mathfrak{m}$ if, when we reduce f mod $\mathfrak{m}$ we obtain again an absolutely integral equation, defining again a smooth curve denoted by $\overline{E}$.

Remark 5.2.2. If the curve is defined by a Weierstrass equation

$$y^2 = 4x^3 - g_2x - g_3$$

with $g_2, g_3 \in A$, and $\mathrm{char}(A/\mathfrak{m}) \neq 2, 3$, then non-degenerate reduction means that the discriminant Δ is a unit in A.

We are now ready for the following Theorem.

Theorem 5.2.3. *[Deuring Reduction Theorem] Let E be an elliptic curve over a number field, with $End E \cong \mathcal{O}$, where $\mathcal{O}$ is an order in an imaginary quadratic field K. Let $\mathfrak{P}$ be a place of $\overline{\mathbb{Q}}$ over a prime number p, where E has non-degenerate reduction $\overline{E}$. Suppose that p splits completely in K, let c be the conductor of $\mathcal{O}$ and write $c = p^r c_0$, where $p \nmid c_0$. Then*

(i) $End(\overline{E}) = \mathbb{Z} + c_0\mathcal{O}_K$ is the order in K with conductor c_0.

(ii) If $p \nmid c$, then we have an isomorphism

$$\begin{aligned} End(E) &\longrightarrow End(\overline{E}) && (5.1)\\ \lambda &\mapsto \overline{\lambda} && (5.2) \end{aligned}$$

When E has complex multiplication and good reduction, Deuring discovered a relation between the complex multiplication of E and the number of points in $\overline{E}(\mathcal{O}_K/\mathfrak{p})$. We will present a version of this result that concerns only elliptic curves over the prime field $\mathbb{F}_p$.

To set up the situation, let $\mathcal{O}$ be an order in an imaginary quadratic field K, and let L be the ring class field of $\mathcal{O}$. Let p be a prime in $\mathbb{Z}$ which splits completely in L, p does not divide the conductor of $\mathcal{O}$, and we will fix a prime $\mathfrak{P}$ of L lying above p, so that $\mathcal{O}_L/\mathfrak{P} \simeq \mathbb{F}_p$. Finally, let E be an elliptic curve over L which has good reduction at $\mathfrak{P}$. With these hypotheses, the reduction $\overline{E}$ is an elliptic curve over $\mathbb{F}_p$. Then we have the following

Theorem 5.2.4. *Let $\mathcal{O}$, L, p and $\mathfrak{P}$ be as above, and let E be an elliptic curve over L with $End_{\mathbb{C}}(E) = \mathcal{O}$. If E has good reduction modulo $\mathfrak{P}$, then there is $\pi \in \mathcal{O}$ such that $p = \pi\overline{\pi}$ and*

$$|\overline{E}(\mathbb{F}_p)| = p + 1 - (\pi + \overline{\pi})$$

Furthermore, $End_{\overline{F}_p}(\overline{E}) = \mathcal{O}$, and every elliptic curve over $\mathbb{F}_p$ with endomorphism ring (over $\overline{\mathbb{F}}_p$) equal to $\mathcal{O}$ arises in this way.

Proof. Theorem 5.2.3 says that reduction induces an isomorphism

$$\mathrm{End}_{\mathbb{C}} \xrightarrow{\simeq} \mathrm{End}_{\overline{\mathbb{F}}_p}(\overline{E})$$

that preserves degrees. It follows that there is some $\pi \in \mathrm{End}_{\mathbb{C}}(E)$ corresponding to the Frobenius endomorphism $F_p \in \mathrm{End}_{\overline{\mathbb{F}}_p}(\overline{E})$ under reduction modulo p. Since the reduction preserves degrees, we have

$$\deg(\pi) = \deg(F_p) = p$$

Over the complex numbers, we know that the degree of $\pi \in \mathcal{O} = \mathrm{End}_{\mathbb{C}}(E)$ is just its norm, so that $N(\pi) = p$. Thus we can write $p = \pi\overline{\pi}$ in $\mathcal{O}$, i.e. p splits as the product of two elements in $\mathcal{O}$.

Now, look at the group of rational points $E(\mathbb{F}_p)$. We know that the Frobenius endomorpishm F_p acts trivially on points in $\mathbb{F}_p$. In other words, $P \in E(\mathbb{F}_p)$ if and only if $F_p(P) = P$. Recall from the proof of Hasse theorem that

$$|E(\mathbb{F}_p)| = |\ker(1 - F_p)| = \deg(1 - F_p)$$

Since the reduction map preserves degrees, it follows that

$$\begin{aligned} \deg(1 - F_p) &= \deg(1 - \pi) = N(1 - \pi) = (1 - \pi)(1 - \overline{\pi}) \\ &= p + 1 - (\pi + \overline{\pi}) \end{aligned}$$

since $p = \pi\overline{\pi}$. This proves the desired formula.

For a proof of the final part of the theorem, see [4, §13, Theorems 13 and 14]. □

We can restate our theorem in terms of an order $\mathcal{O}_D$ with given discriminant D:

Theorem 5.2.5. *Let E be an elliptic curve with complex multiplication by an imaginary quadratic order $\mathcal{O}_D$ of discriminant D, and let p be a prime number that splits into a product of two prime elements in $\mathcal{O}_D$. Then, there exists $\pi \in \mathcal{O}_D$ such that $p = \pi\overline{\pi}$ and*

$$|\overline{E}(\mathbb{F}_p)| = p + 1 - t$$

where $t = \pi + \overline{\pi}$.

Remark 5.2.6. We remark explicitly that not all π do the job: if we consider a unit $u \in \mathcal{O}_D^{\times}$, then $N(u\pi) = N(\pi) = p$, but in general $u\pi + \overline{u\pi} \neq \pi + \overline{\pi}$. In the case $D < -4$, we know that $\mathcal{O}_D^{\times} = \{\pm 1\}$; this implies that an incorrect choice of π gives an opposite value of t in Theorem 5.2.5.

Remark 5.2.7. If the prime p of Theorem 5.2.5 is inert, i.e. if $\left(\frac{D}{p}\right) = -1$, then $t = 0$, so that

$$|\overline{E}(\mathbb{F}_p)| = p + 1$$

We end this section with the following

Theorem 5.2.8 (Deuring Lifting Theorem)**.** *Let E_0 be an elliptic curve in characteristic p, with an endomorphism f_0 which is not trivial. Then there exists an elliptic curve E defined over a number field, an endomorphism f of E, and a non-degenerate reduction of E at a place $\mathfrak{P}$ lying above p, such that we have an isomorphism*

$$\begin{array}{ccc} E_0 & \xrightarrow{\simeq} & \overline{E} \\ f_0 & \mapsto & \overline{f} \end{array}$$

5.3 The Complex Multiplication Method

We want to solve the following

Problem 5.3.1. Let $\mathcal{O}$ be an imaginary quadratic order, and let $p = \mathfrak{p}\overline{\mathfrak{p}}$ be a split prime in $\mathcal{O}$. We want to construct an elliptic curve $\overline{E}$ over a finite field $\mathbb{F}_q$, $q = p^k$, such that $\mathrm{End}(\overline{E}) = \mathcal{O}$.

Remark 5.3.2. Problem 5.3.1 can be easily solved if we content ourselves to have an analytic model for the curves, instead of an algebraic one. Precisely, we start from an invertible ideal Λ of $\mathcal{O}$. Since we regard $\mathcal{O}$ as a subring of the field $\mathbb{C}$ of complex numbers, following Remark 3.11.1 we can see $\Lambda \subset \mathcal{O}$ as a lattice in $\mathbb{C}$ of dimension 2.

The quotient $T = \mathbb{C}/\Lambda$ is a complex torus such that $\mathrm{End}(T) = \mathcal{O}$. We pick an ideal in every class in the class group $C(\mathcal{O})$ and consider the h associated tori ($h = |C(\mathcal{O})|$).

Any torus of dimension 2 having $\mathcal{O}$ as endomorphism ring is isomorphic to exactly one of these h tori: this completely solves the problem of constructing all elliptic curves with complex multiplication by $\mathcal{O}$ except that we have an analytic model for these curves, and we would like to have an algebraic model also. This is possible since - as we know very well - any complex torus can be given the structure of an algebraic curve using Weierstrass functions. This is the algebraic model which is of interest to us.

We split Problem 5.3.1 into two sub-problems:

(1) construct an elliptic curve E over $\mathbb{C}$ such that $\mathrm{End}_{\mathbb{C}}(E) = \mathcal{O}$;

(2) reduce the curve E modulo $\mathfrak{p}$.

Sub-problem (2) is straightforward from what we saw early in this chapter. So let us focus on and give an overview of the solution to sub-problem (1). We use all the results obtained so far in this thesis.

Let $D < 0$ be an imaginary quadratic discriminant, and let $\mathcal{O} := \mathcal{O}_D = [1, \frac{D+\sqrt{D}}{2}]_{\mathbb{Z}}$ be the (not necessarily maximal) order of discriminant D in $K = \mathbb{Q}(\sqrt{D})$. Let $h = |C(\mathcal{O}_D)|$ be the ideal class number of $\mathcal{O}_D$.

We know - by a result of Siegel, see the estimate 1.4 - that

$$\frac{\log h}{\log|D|} \to \frac{1}{2}, \quad \text{as } |D| \to +\infty$$

so that $|D| \in O(h^{2\epsilon})$ and $h \in O(|D|^{1/2+\epsilon})$ for any $\epsilon > 0$.

By Proposition 3.11.2, we know that there are h isomorphism classes of elliptic curves over $\mathbb{C}$ having complex multiplication by $\mathcal{O}_D$, i.e. curves with $\mathcal{O}_D$ as endomorphism ring. Namely, let

$$j : \mathcal{H} = \{\tau \in \mathbb{C} \mid \mathrm{Im}(\tau) > 0\} \to \mathbb{C}$$

the absolute modular invariant (see Section 1.1). We know from Theorem 1.4.4 that there is an isomorphism between the ideal class group $C(\mathcal{O}_D)$ and the form class group $C(D)$ of primitive quadratic forms of discriminant D (Definition 1.4.3). So consider the reduced quadratic forms

$$[A_i, B_i, C_i] = A_i X^2 + B_i X + C_i$$

of discriminant $D = B_i^2 - 4A_iC_i$, representing the ideal classes of $\mathcal{O}_D$. Let $\tau_i := \frac{-B_i+\sqrt{D}}{2A_i}$ run through the roots in $\mathcal{H}$ of the reduced quadratic forms $[A_i, B_i, C_i]$ (recall Remark 1.3.3).

By Remark 1.1.3, the j-invariant of the elliptic curves are given by $j(\tau_i)$. Moreover, by Theorem 3.11.4, these $j(\tau_i)$ are algebraic integers and they generate the ring class field K_D for $\mathcal{O}_D$, the Galois extension of K such that

$$\mathrm{Gal}(K_D, K) \cong C(\mathcal{O}_D)$$

where the isomorphism is given by the Artin map; see Theorem 1.5.18. Thanks to Theorem 1.5.4, the minimal polynomial of the $j(\tau_i)$ over K

$$H_D(X) = \prod_{i=1}^{h}(X - j(\tau_i)) \in \mathbb{Z}[X]$$

has coefficients in $\mathbb{Z}$. In the special case that D is a fundamental discriminant (Definition 1.4.1), the ring class field K_D is the Hilbert class field of K.

Collecting our results, we have h elliptic curves (with abuse of notation, since we should talk about isomorphism classes of elliptic curves) $E_1, \ldots, E_h$, all defined over the Hilbert class field and having endomorphism ring isomorphic to $\mathcal{O}_D$. For every such curve E_l and for every prime p that splits in $\mathcal{O}_D$, we may reduce E_l modulo a prime ideal lying above p. We obtain an ordinary elliptic curve defined over a finite extension $\mathbb{F}_q$ of $\mathbb{F}_p$.

Namely, suppose p splits in $\mathcal{O}_D$ as $p = \mathfrak{p}\overline{\mathfrak{p}}$ (and $p \nmid D$, so p is unramified in K_D), and let

$$k := \min\{n \in \mathbb{Z}_{>0} \mid \mathfrak{p}^n \text{ is principal}\} \tag{5.3}$$

Let $q = p^k$; this is equivalent to ask that $4q = U^2 + DV^2$ with $U, V \in \mathbb{Z}$. Places of the Hilbert class field above $\mathfrak{p}$ have inertia degree equal to k, so reducing E_l modulo such a place produces an elliptic curve $E_l \pmod p$ over the finite field $\mathbb{F}_q$ with q elements.

By Deuring's reduction and lifting theorems these h curves are precisely the elliptic curves over $\mathbb{F}_q$ with complex multiplication by $\mathcal{O}_D$. They may be obtained as follows: compute the class polynomial $H_D \in \mathbb{Z}[X]$ and reduce it modulo p. It splits completely over $\mathbb{F}_q$, and each of its roots is the j-invariant of an elliptic curve over $\mathbb{F}_q$ with the desired endomorphism ring.

Remark 5.3.3. Call $\overline{E}_l := E_l \pmod p$. The Frobenius element F, seen as an element of $\mathcal{O}$, is a generator for the principal ideal $\mathfrak{p}^k$.

5.4 Examples

We give now a couple of full-detailed examples of this method.

Example 5.4.1. Let $D = -2$ and consider the quadratic imaginary field $K = \mathbb{Q}(\sqrt{-2})$. For the basic theory seen in Section 1.2.3, the discriminant is $d_K = -8$ and the ring of integers is $\mathcal{O}_K = \mathbb{Z}[\sqrt{-2}] = \mathbb{Z} + \mathbb{Z}\sqrt{-2}$.

By Theorem 1.2.16, we know that the class number of $\mathcal{O}_K$ is $h = 1$, i.e. $\mathcal{O}_K$ is a PID. So there is a unique (isomorphism class of) elliptic curve E such that $\mathrm{End}(E) = \mathcal{O}_K$. Since a $\mathbb{Z}$-basis for the lattice $\mathcal{O}_K$ is $\{1, \sqrt{-2}\}$, following the reasoning in Section 1.1.1 we take $\tau = \sqrt{-2} \in \mathcal{H}$. According to Theorem 1.5.4, the Hilbert class polynomial $H_D(X) = X - j(\tau)$ has coefficients in $\mathbb{Z}$, i.e. $j(\tau) \in \mathbb{Z}$.

Let $q = \exp(2\pi i \tau)$. According to Theorem 1.1 we have

$$j(\tau) = \frac{1}{q} + 744 + 196,884q + 21,493,760q^2 + \cdots$$

By numerically evaluating the first four terms of $j(\tau)$, we get

$$j(\tau) \approx 7999.997$$

Therefore $j := j(\tau) = 8000$. Since $j \neq 0, 1728$, Remark 2.1.10 tells us that an elliptic curve with j-invariant $j(\tau)$ is

$$y^2 = x^3 - \frac{27}{4}\frac{125}{98}x - \frac{27}{4}\frac{125}{98}$$

By Proposition 2.1.15, we can choose $1/18 \in K^*$ and consider the elliptic curve with equation

$$E : y^2 = x^3 - \frac{5^3}{4704}x - \frac{5^3}{84672}$$

obtained by multiplying the linear factor by 18^{-2} and the constant factor by 18^{-3}. Now, let $p \in \mathbb{Z}$ be a prime that splits in $\mathcal{O}_K$ as $p = \mathfrak{p}\bar{\mathfrak{p}}$. We want to reduce the curve E over $\mathbb{F}_q$, where $q = p^k$ and k as in condition 5.3. Recalling Proposition 1.2.9, p splits in $\mathcal{O}_K$ if $(d_K/p) = 1$. Take $p = 17$; we have

$$d_K \equiv -8 \equiv 9 \equiv 3^2 \pmod{17}$$

and so $p = 17$ splits in $\mathcal{O}_K$. We now find $\mathfrak{p}$: by Theorem 1.2.12 we have

$$17 = (17, n + \sqrt{-2})(17, n - \sqrt{-2})$$

where n is such that $-2 \equiv n^2 \pmod{17}$. Now, -2 is indeed a quadratic residue modulo 17 since, by elementary properties of Legendre symbol,

$$\left(\frac{-2}{17}\right) = \left(\frac{-1}{17}\right)\left(\frac{2}{17}\right) = (-1)^{\frac{17-1}{2}}(-1)^{\frac{17^2-1}{8}} = 1$$

By a direct computation, we find that $-2 \equiv 7^2 \pmod{17}$ and therefore $\mathfrak{p} = (17, \sqrt{-2} - 7)$.

We want now to find k such that $\mathfrak{p}^k$ is principal; but since $\mathcal{O}_K$ is a PID, we have $k = 1$. Therefore, reduction of E is possible in $\mathbb{F}_{17}$; by standard techniques[(1)] we find a generator of $\mathfrak{p}$ and we can write $\mathfrak{p} = (3 + 2\sqrt{-2})$.

We finally reduce E modulo 17: we have

$$4704 \equiv -5 \pmod{17}, \quad 84672 \equiv -5 \pmod{17}$$

and since

$$\frac{5^3}{5} = 5^2 \equiv 8 \pmod{17}$$

we have

$$\overline{E} : y^2 = x^3 + 8x + 8$$

which is the desired equation.

Remark 5.4.2. Observe that sometimes it is useful to obtain also the equation of the twisted curve of $\overline{E}$ (see Remark 2.1.17 for the details). To find such an equation we look for a non-quadratic residue modulo 17, for example 3. In fact we have

$$\left(\frac{3}{17}\right) = \left(\frac{17}{3}\right)(-1)^{\frac{3-1}{2}\frac{17-1}{2}} = \left(\frac{2}{3}\right) = (-1)^{\frac{3^2-1}{8}} = -1$$

So we have

$$\begin{aligned} 8 \cdot 3^2 &= 72 \equiv 4 \pmod{17} \\ 8 \cdot 3^3 &= 216 \equiv 12 \pmod{17} \end{aligned}$$

and so we have the twisted curve

$$\overline{E}_2 : y^2 = x^3 + 4x + 12$$

Remark 5.4.3. The main step in the CM method is the construction of the Hilbert class polynomial of the imaginary quadratic order of discriminant D. In Example 5.4.1, this was easy to compute since the class number was $h = 1$. When $h > 1$ things are more complicated.

We will see in Example 5.5.6 a situation in which $h = 3$; but before is better to say a (not so) few words on how one can determine efficiently the Hilbert class polynomial.

(1) Gauss reduction algorithm for lattices of dimension 2.

5.5 Building the Hilbert Class Polynomial

We follow the ideas in [1] by showing how to effectively construct the Hilbert class polynomial $H_D(X)$. By Theorem 1.5.4 we know that

$$H_D(X) = \prod_{[a,b,c]\in C(D)} \left(X - j\left(\frac{-b + i\sqrt{d}}{2a} \right) \right) \tag{5.4}$$

where $C(D)$ is the set of all reduced quadratic forms of discriminant D, and we have set and $d = |D|$. We know that $\deg H_D(X) = h := h(D)$, the class number.

Now, a simple way to build $H_D(X)$ is to compute, for all reduced forms of discriminant D, a numerical value of the corresponding j. If we work with enough precision, we are then able to recover $H_D(X)$ given by equation 5.4: in fact, by Theorem 1.5.4 we know that $H_D(X)$ has integer coefficients, so it is enough to carry out computations in such a way that the absolute error of each coefficient is within a value of 0.5 at most. Another key-point observation that allows us to double-check the correctness of our result is that, by Proposition 1.5.10, $H_D(0)$ is a cube of a rational integer.

Remark 5.5.1. Instead of computing the value $j([a,b,c])$ for all reduced quadratic forms of discriminant D, the present remark allows us to halve the computation. If $[a,b,c]$ is an ambiguous form, i.e. if $b = 0$ or $a = b$ or $a = c$, then $j([a,b,c])$ is easily seen to be a real number (in any case $b^2 - 4ac < 0$). If on the other hand $[a,b,c]$ is non-ambiguous, then we have $j([a,-b,c]) = \overline{j([a,b,c])}$ (conjugation in $\mathbb{C}$).

Now, if $H_D(x) = 0$ for some x, then also $H_D(\overline{x}) = 0$. Hence we can halve the computation this way:

- $[a,b,c]$ ambiguous $\longrightarrow$ we adjoin a factor $X - j([a,b,c])$
- $[a,b,c]$ non ambiguous $\longrightarrow$ we adjoin a factor

$$(X - j([a,b,c]))\left(X - \overline{j([a,b,c])}\right) = X^2 - 2\mathrm{Re}\left(j([a,b,c])\right)X + |j([a,b,c])|^2$$

To achieve the accuracy we need to carry out computations, we need to make some a priori estimate on the size of the coefficients of $H_D(X)$, that we shall see in a moment. For further references, see [1, §7]. The first step is to evaluate $j(\tau)$ as fast as possible: in order to do this, we recall formula 1.2 of Section 1.1.2 which express $j(\tau)$ in terms of the Dirichlet function $\eta(\tau)$. We have a good convergence of the q-expansion for η, so it is convenient to directly apply this formula to compute a numerical value of $j(\tau)$. Now, the heart of the computation is the evaluation of $\eta(\tau)$, so we have to study

the optimal choice of the parameters and see how many terms have to be included for a desired precision, we look at the truncated series

$$\eta_M(\tau) = q^{1/24}\left(1 + \sum_{m=1}^{M}(-1)^m(q^{m(3m-1)/2} + q^{m(3m+1)/2})\right) \tag{5.5}$$

where M is a positive integer and $q = \exp(2\pi i\tau)$. We look for an upper bound on the error resulting on the computation of this truncates series instead of $\eta(\tau)$: for this it is useful the following Lemma.

Lemma 5.5.2. *Let $q = e^{2\pi i\tau} = \rho e^{i\theta}$, where τ is a complex number in the upper half plane $\mathcal{H}$ such that $0 < |q| < \frac{1}{2}$. Then if M is a positive integer,*

$$|\eta(\tau) - \eta_M(\tau)| \leq 6\rho^{3M^2/2}$$

Proof. Let $q = \rho e^{i\theta} = \rho(\cos(\theta) + i\sin(\theta))$ and assume that $0 < |q| < 1$. For ease of computation it is better to work with the series inside the expression 5.5. Therefore we define

$$\begin{aligned} f(q) &= \sum_{m=1}^{\infty}(-1)^m(q^{m(3m-1)/2} + q^{m(3m+1)/2}) \\ f_M(q) &= \sum_{m=1}^{M}(-1)^m(q^{m(3m-1)/2} + q^{m(3m+1)/2}) \end{aligned}$$

Now, let $R(q)$ and $R_N(q)$ be the real parts of $f(q)$ and $f_N(q)$ respectively, and let

$$E(q) = R(\rho) - R(q)$$
$$E_M(q) = R_M(\rho) - R_M(q)$$

We have that $E(q)$ is an alternating series with positive real coefficients. Let $A_m := m(3m-1)/2$ and $B_m := m(3m+1)/2$; we have

$$\begin{aligned} |E(q) - E_N(q)| &= \sum_{m=M+1}^{\infty}(-1)^m(\rho^{A_m}(1-\cos(\theta A_m)) + \rho^{B_m}(1-\cos(\theta B_m))) \\ &\leq \rho^{A_m}(1-\cos(\theta A_m)) + \rho^{B_m}(1-\cos(\theta B_m))\ |_{m=M+1} \\ &\leq 2(\rho^{(M+1)(3M+2)/2} + \rho^{(M+1)(3M+4)/2}) \\ &= 2\epsilon_{M+1} \end{aligned}$$

Now we can estimate

$$\begin{aligned} |R(q) - R_M(q)| &= |(R(q) - R(\rho)) + (R_M(\rho) - R_M(q)) + (R(\rho) - R_M(\rho))| \\ &= |(E_M(q) - E(q)) + (R(\rho) - R_M(\rho))| \\ &\leq 3\epsilon_{M+1} \end{aligned}$$

We proceed analogously for the imaginary parts. Therefore, $|f(\tau) - f_N(\tau)| \leq 6\epsilon_{N+1}$. Looking at the term ϵ_m, it is not hard to see that $\epsilon_m \leq \rho^{3(m-1)^2/2}$ if we require $\rho < 1/4$ and $m \geq 5$. Then we get the desired formula observing that $|q^{1/24}| < 1$. □

Put $\tau = \frac{-b+i\sqrt{d}}{2a}$. By the identity $q = \exp(2\pi i\tau) = \rho\exp(i\theta)$ seen in Lemma 5.5.2, we obtain

$$\rho = \exp(-\pi\sqrt{d}/a), \quad \theta = -\pi b/a$$

By the q-expansion of j given by equation 1.1, we get the estimate

$$|j(\tau)| = O(q^{-1}) = O(\exp(\pi\sqrt{d}/a)) \tag{5.6}$$

We deduce an upper bound B on the size of the coefficients of $H_D(X)$: the constant term $H_D(0)$ is equal to the product of all values $j(\tau)$

$$H_D(0) = \prod_{[a,b,c]\in C(D)} j\left(\frac{-b+i\sqrt{d}}{2a}\right)$$

and so, by the estimate 5.6 we have

$$H_D(0) \approx \exp(\pi\sqrt{d}\sum_{[a,b,c]}\frac{1}{a})$$

In order to get a bound for all the coefficients, we multiply this by the middle binomial coefficient (which is the largest) and hence obtain

$$B = \binom{h}{\lfloor h/2\rfloor}\exp\left(\pi\sqrt{d}\sum_{[a,b,c]}\frac{1}{a}\right)$$

Aside 5.5.3. We would like to provide an estimate of $\log(B)$. By [5, §XVI.4] we know that

$$\log h \sim \log(\sqrt{d}), \quad \text{for } d \to \infty$$

So for any $\epsilon \in \mathbb{R}_+$ we have

$$d^{1/2-\epsilon} \leq h \leq d^{1/2+\epsilon}$$

for d big enough, or better $A_\epsilon d^{1/2-\epsilon} \leq h \leq B_\epsilon d^{1/2+\epsilon}$.

We now proceed to give an upper and a lower bound for $\log B$.

Lower bound By Fact 1.3.6(i), we have that $a \leq \sqrt{d/3}$ and so

$$\sum\frac{1}{a} \geq h\sqrt{\frac{3}{d}} \sim \sqrt{3}h$$

Therefore $\exists c > 1$ constant such that $\log B > c\sqrt{d}$, for d large enough.

Upper bound We estimate $\sum \frac{1}{a}$: following ideas from [6, §5.10], we have that there are not too many a's which are small. This is because

$$\#\{\text{reduced forms}[a,b] \text{ such that } a \text{ is fixed}\} \leq \tau(a)$$

where $\tau(a)$ is the number of positive divisors of a. So we have

$$\sum \frac{1}{a} \leq \sum_{a=1}^{d} \frac{\tau(a)}{a} = \\ = \sum_{a=1}^{d} \left(\sum_{v=1}^{a} \tau(v) \right) \left(\frac{1}{a} - \frac{1}{a+1} \right) + \frac{1}{d+1} \sum_{a=1}^{d} \tau(a)$$

By a known result in Analytic Number Theory we have

$$\sum_{a=1}^{d} \tau(a) = d\log d + (2\gamma - 1)d + O(\sqrt{d})$$

where γ is the Euler's gamma. By limiting ourselves to the estimate $d\log d$ we have

$$\int_{a=1}^{d} \frac{\log a}{a} da = \frac{(\log d)^2}{2} < \log d.$$

It follows that

$$\sum \frac{1}{a} = O(\log d)^2$$

Now, the middle binomial coefficient is smaller than the sum of all the binomial coefficients, i.e.

$$\binom{h}{\lfloor h/2 \rfloor} \leq 2^h$$

Therefore

$$B \leq 2^h \exp(\Theta \pi \sqrt{d} (\log d)^2)$$

for some constant Θ, and finally we get

$$\log B = O(\sqrt{d}(\log d)^2) = O(h(\log h)^2)$$

By taking the base 10 logarithm of this bound B, we get the required decimal precision: the number of digits we need to consider in our computations is given by

$$\text{Prec}(D) = \left\lceil \frac{\log \binom{h}{\lfloor h/2 \rfloor} + \pi\sqrt{d}}{\log 10} \sum_{[a,b,c]} \frac{1}{a} \right\rceil + v_0 \tag{5.7}$$

where v_0 is a positive constant that takes into account the rounding error and the error made in our estimate of $|j(\tau)|$; typically one considers $v_0 = 10$.

Now we want to determine M in equation 5.5 such that it approximates $\eta(\tau)$ with the desired accuracy. In order to do so, we apply Lemma 5.5.2. The hypothesis hold: if $[a, b, c]$ is a reduced form of negative discriminant D then

$$d = 4ac - b^2 \geq 4a^2 - a^2$$

which implies that $a \leq \sqrt{d/3}$. Hence

$$\rho = \exp(-\pi\sqrt{d}/a) \leq \exp(-\pi\sqrt{3}) \approx 4.33 \times 10^{-3} < 1/2$$

so we can apply Lemma 5.5.2. We obtain M by solving the following equation

$$\log_{10}(6\rho^{3M^2/2}) = \mathrm{Prec}(D)$$

Simple algebra says that

$$M = \left\lceil \sqrt{a\frac{2}{3}\frac{\mathrm{Prec}(D)\log 10 + \log 6}{\pi\sqrt{d}}} \right\rceil \tag{5.8}$$

Then to calculate an accurate numerical value of $j(\tau)$ we compute $\eta_M(\tau)$ by equation 5.5 and apply the result to equation 1.2: in order to do so we need to compute $\Delta(\tau)$ and $\Delta(2\tau)$. In general, $\Delta(k\tau)$ is obtained by computing $\eta_M(q^k)$ to the order M, obtained by replacing a with a/k in equation 5.8.

We now show an algorithm that computes the Hilbert class polynomial; with these remarks in mind, this procedure runs through all positive a, b such that $b \leq a \leq \sqrt{d/3}$ and a divides $\frac{b^2-D}{4}$, and constructs a polynomial whose roots are the j-invariants associated with the reduced forms $[a, b, \frac{b^2-D}{4a}]$. The algorithm is closely related to Algorithm 1.

Remark 5.5.4. Since b is even if and only if D is even, we can reduce the number of iterations by initially checking the parity of D.

Algorithm 3 Computing Hilbert Class Polynomial

$H_D := 1$;
$b := |D| \pmod 2$;
$B := \lfloor \sqrt{|D|/3} \rfloor$;
while $b \leq B$ **do**
  $t := \frac{b^2 - D}{4}$;
  $a := \max(1, b)$;
  while $a^2 \leq t$ **do**
    if $a \mid t$ **then**
      $j := j((-b + \sqrt{D})/(2a))$;
      if $a = b$ or $a^2 = t$ or $b = 0$ **then**
        $H_D := H_D \cdot (X - j)$;
      else
        $H_D := H_D \cdot (X^2 - 2\mathrm{Re}(j)X + |j|^2)$;
      end if
    end if
    $a := a + 1$;
  end while
  $b := b + 2$;
end while
Round coefficients of H_D to the nearest integer;
return $H_D \pmod p$;

5.5.1 Examples - continued

Example 5.5.5. Let $D = -23$ and consider the quadratic imaginary field $K = \mathbb{Q}(\sqrt{-23})$. It is easy to see (otherwise just run Algorithm 1) that the class number is $h(-23) = 3$, and therefore there are 3 reduced quadratic forms $[a, b, c]$ of discriminant -23. The condition $|b| \leq a \leq \sqrt{-D/3}$ tells us that $a = 1, 2$. Easy computations then show that the 3 forms are

$$f_1 = [1, 1, 6], \quad f_2 = [2, 1, 3], \quad f_3 = [2, -1, 3]$$

Call τ_1, τ_2, τ_3 the corresponding τ-values. We have $\binom{h}{\lfloor h/2 \rfloor} = 3$, and therefore

$$\text{Prec}(-23) = \left\lceil \frac{\log 3 + \pi\sqrt{23}}{\log 10}(1 + \frac{1}{2} + \frac{1}{2}) \right\rceil + 10 = 25$$

In order to get this level of precision we must compute $\eta_{M_i}(\tau_i)$ to order M_i corresponding to τ_i, $i = 1, 2, 3$. Precisely,

$$\begin{aligned} M_1 &= \left\lceil \sqrt{\frac{2}{3}\frac{25\log 10 + \log 6}{\pi\sqrt{23}}} \right\rceil = 2 \\ M_2 = M_3 &= \left\lceil \sqrt{\frac{4}{3}\frac{25\log 10 + \log 6}{\pi\sqrt{23}}} \right\rceil = 3 \end{aligned}$$

We want to compute

$$H_{-23}(X) = (X - j(\tau_1))(X - j(\tau_2))(X - j(\tau_3))$$

By writing a few lines code with any programming language, we can compute in sequence

$$\eta_{M_i}(\tau_i), \quad \Delta(\tau_i), \quad \Delta(2\tau_i), \quad f(\tau_i)$$

and finally we get a numerical approximation of $j(\tau_i)$ (observe that $\Delta(2\tau_i)$ can be computed noting that changing τ into 2τ changes q into q^2).

After taking real parts and rounding to the nearest integer we get

$$H_{-23}(X) = X^3 + 3,491,750X^2 - 5,151,296,875X + 12,771,880,859,375$$

which is the desired result. We can double-check our computations observing that $H_{-23}(0)$ is indeed the cube of a rational integer:

$$23,375^3 = 12,771,880,859,375$$

We apply these results to give an example of the CM method when the class number is $h > 1$.

Example 5.5.6. Let $D = -23$ and consider the quadratic imaginary field $K = \mathbb{Q}\sqrt{-23}$. The discriminant of the field is $d_K \equiv -23 \equiv 1 \pmod 4$, and therefore the ring of integers is $\mathcal{O}_K = \mathbb{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{-23}]$. We want to find an elliptic curve over a finite field with this ring of integers as its endomorphisms ring. By the considerations made in Section 5.3, we have to find a prime p that splits in $\mathcal{O}_K$ as $p = \mathfrak{p}\overline{\mathfrak{p}}$, $\mathfrak{p} \in \mathcal{O}_K$. Then we compute $H_{-23}(X) \pmod p$: it splits completely over $\mathbb{F}_q$, $q = p^r$, and each of its roots are the j-invariant of an elliptic curve over $\mathbb{F}_q$ with the desired ring of endomorphisms.

In our case we can consider $p = 59$. In fact, having in mind the equivalence given by Theorem 1.5.12, we can write

$$4 \cdot 59 = 12^2 + 23 \cdot 2^2$$

Reducing modulo 59 the Hilbert polynomial obtained in Example 5.5.5, we obtain

$$H_{-23}(X) \equiv X^3 + 12X^2 + 28X + 33 \pmod{59}$$

Theorem 1.5.12 allows us to split it into linear factors:

$$H_{-23}(X) \equiv (X - 20)(X - 42)(X - 44) \pmod{59}$$

Take for instance $j_0 = 20$. We apply the formula given by Remark 2.1.10. Take $c = \frac{j_0}{j_0 - 1728}$ and we have

$$\overline{E} : y^2 = x^3 - \frac{27}{4}cx - \frac{27}{4}c \quad \text{in } \mathbb{F}_{59}$$

Computing in $\mathbb{Z}/59\mathbb{Z}$ we get

$$c = 20 \cdot (-1728)^{-1} = 20 \cdot 20 = 46$$

$$(-27) \cdot 4^{-1} = 32 \cdot 15 = 8$$

and since $8 \cdot 46 = 14$ we obtain

$$\overline{E} : y^2 = x^3 + 14x + 14$$

which is a curve over $\mathbb{F}_{59}$ with the desired endomorphism ring.

Even if it is not of interest in this example, we compute explicitly also a twist of this curve. Take $r = 29 \in \mathbb{F}_{59}$ (which is not a square). Then by Proposition 2.1.15 we have the twisted curve

$$\tilde{\overline{E}} : y^2 = x^3 + 33x + 13$$

5.6 CM Method - Alternative

With the same tools already developed, we can devise a method to build elliptic curves over a finite field with a given number of points. This is very similar to the CM method. In fact we use the Deuring Lifting Theorem that allows us to consider every elliptic curve over $\mathbb{F}_p$ as the reduction of some elliptic curve over a number field K with the same endomorphism ring. Our task is to construct a curve having exactly N rational points over $\mathbb{F}_p$, with p given prime number. Of course, N is required to belong to the Hasse interval, i.e. $p+1-2\sqrt{p} \leq N \leq p+1+2\sqrt{p}$.

Suppose we have found the imaginary quadratic field K of fundamental discriminant D where p splits as the product of two elements. If we look at elliptic curves over K with complex multiplication by the full ring of integers $\mathcal{O}_K$ in K then we are able to apply Theorem 5.2.5 which immediately gives us the desired cardinality over $\mathbb{F}_p$. To find such a field K we choose a fundamental discriminant $D < 0$ such that $4p = t^2 + s^2|D|$ has a solution for $t = p+1-N$ and s any integer. Finding a suitable discriminant D for the prime p is easy: set $t = p+1-N$ and then

$$D = \frac{t^2 - 4p}{s^2} = \frac{(p+1-N)^2 - 4p}{s^2}$$

and we look for s such that s^2 divides (t^2-4p) and $D<0$ is fundamental and small as possible. Then, by Theorem 1.5.12 (p) splits into two distinct ideals in K as $p = \pi\overline{\pi}$, with $\pi \in \mathcal{O}_K$. If we next find the equation of an elliptic curve E over $\mathbb{C}$ with $\mathrm{End}_{\mathbb{C}}(E) \simeq \mathcal{O}_K$ then by Theorem 5.2.5 the reduction of E modulo p will give us a curve with $p+1-t = N$ rational points over $\mathbb{F}_p$. To get such a curve we proceed as usual by means of the Hilbert class polynomial.

Remark 5.6.1. In the case $D < -4$, in the reduction process we obtain one elliptic curve $\overline{E} \pmod{p}$. By Remark 5.2.6 we have

$$\#\overline{E}(\mathbb{F}_p) = p+1 \pm t$$

If $\#\overline{E}(\mathbb{F}_p) = p+1-t$ we are done. Otherwise we twist the curve with the known formulas (cf. Proposition 2.1.15) and get the curve with the desired number of points. To see whether we wrote down the right curve, we can pick a random point on the curve and see if it is annihilated by N.

We can sum up the CM method for a known number of points:

Input prime p, number of points N.

Output elliptic curve $\overline{E}/\mathbb{F}_p$ such that $\#\overline{E}(\mathbb{F}_p) = N$.

1. Set $t := p + 1 - N$;
2. Determine D (fund. discriminant) such that $4p = t^2 + s^2|D|$, $s \in \mathbb{Z}$;
3. Build $H_D(X)$;
4. Find j_0 such that $H_D(j_0) \equiv 0 \pmod{p}$;
5. Write the equation of an elliptic curve $\overline{E}/\mathbb{F}_p$ with invariant j_0;
6. Pick randomly a point $P \in \overline{E}$
7. If $[N]P \neq O$, the desired curve is the twist $\tilde{\overline{E}}$.
8. If $[N]P = O$, $\overline{E}$ is *likely to be* the desired curve. To be sure, let $N' := p + 1 + t$ and compute $[N']P$. If $[N']P \neq O$ then $\overline{E}$ is the desired curve, otherwise we unfortunately pick a point annihilated by both N, N' and we must repeat step 6 with a different point Q.

Remark 5.6.2. The bad case in point 8. may happen only if the GCD is $(N, N') \neq 1$.

Example 5.6.3. We want to build an elliptic curve over the field $\mathbb{F}_{17}$ with $N = 24$ points. Observe that 24 lies in the Hasse interval of possible cardinalities $[\lceil 17+1-2\sqrt{17}\rceil, \lfloor 17+1+2\sqrt{17}\rfloor] = [10, 26]$. Set $t = 17+1-24 = -6$. We look for a fundamental discriminant D such that

$$D = \frac{t^2 - 4p}{s^2} = \frac{-2^5}{s^2}$$

In order to have D as small as possible we are forced to choose $s = 2$, and so $D = -8$. The quadratic field having -8 as discriminant is $K = \mathbb{Q}(\sqrt{-2})$, and $\mathcal{O}_K = \mathbb{Z}[\sqrt{-2}]$. Following Example 5.4.1 we find that the elliptic curve over $\mathbb{F}_{17}$ with complex multiplication given by $\mathcal{O}_K$ is

$$\overline{E}_1 : y^2 = x^3 + 8x + 8$$

and the twisted curve is

$$\overline{E}_2 : y^2 = x^3 + 4x + 12$$

In Example 5.4.1 we found that $p = \mathfrak{p}\bar{\mathfrak{p}}$, where $\mathfrak{p} = (3 + 2\sqrt{-2})$. We know that one of the $\overline{E}_i$ has Frobenius endomorphism corresponding to $\mathfrak{p}$, and

the other one has Frobenius endomorphism corresponding to $-\mathfrak{p}$ (as $p = (\pm\mathfrak{p})(\pm\overline{\mathfrak{p}})$, see Proposition 4.3.5). The one with Frobenius $\mathfrak{p}$ has cardinality the norm of $\mathfrak{p} - 1$:

$$\begin{aligned} p + 1 - t &= \mathfrak{p}\overline{\mathfrak{p}} + 1 - (\mathfrak{p} + \overline{\mathfrak{p}}) = (\mathfrak{p} - 1)(\overline{\mathfrak{p}} - 1) \\ &= N(\mathfrak{p} - 1) = N(2 + 2\sqrt{-2}) = 12 \end{aligned}$$

and the other has cardinality the norm of $\mathfrak{p} + 1$:

$$\begin{aligned} p + 1 + t &= \mathfrak{p}\overline{\mathfrak{p}} + 1 + (\mathfrak{p} + \overline{\mathfrak{p}}) = (\mathfrak{p} + 1)(\overline{\mathfrak{p}} + 1) \\ &= N(\mathfrak{p} + 1) = N(4 + 2\sqrt{-2}) = 24 \end{aligned}$$

Pick a random point on $\overline{E}_1$, say $P = (10, 3)$. Computer calculations tell us that $\mathrm{ord}_{\overline{E}_1} P = 24$. Therefore

$$\begin{aligned} \#\overline{E}_1(\mathbb{F}_{17}) &= 24 \\ \#\overline{E}_2(\mathbb{F}_{17}) &= 12 \end{aligned}$$

CHAPTER 6

Schoof's Algorithm

Abstract

In this chapter we will present Schoof's deterministic algorithm to compute the number of $\mathbb{F}_q$-points of an elliptic curve that is defined over a finite field $\mathbb{F}_q$ and which is given by a Weierstrass equation. The algorithm takes - as we shall see - $O(\log^{8+o(1)} q)$ elementary operations (bit operations). If we use fast exponentiation arithmetic, the total cost will be reduced to $O(\log^{5+o(1)} q)$.

6.1 Motivation

Let E be an elliptic curve defined over a finite field $\mathbb{F}_p$. For many applications, it is important to have an efficient way to compute the number of points in $E(\mathbb{F}_p)$, where p has usually many decimal digits. For instance, in elliptic curve cryptography it is important to know the number of points to judge the difficulty of solving the discrete logarithm problem in the group of points on an elliptic curve.

So it is a major problem to study an efficient way of computing $\#E(\mathbb{F}_p)$ for large primes. Before 1985, approaches to counting points on elliptic curves such as the naive one (which we will consider in a moment) and baby-step giant-step algorithms were not practical and had an exponential running time. In 1985, René Schoof from university of Amsterdam published, in his paper [8], an efficient way to determine $\#E(\mathbb{F}_p)$. It was a theoretical breakthrough, as it was the first deterministic polynomial time algorithm for counting points on elliptic curves.

In the 1990's, Elkies and Atkies improved Schoof's algorithm by studying elliptic curves over $\mathbb{C}$. The so called Schoof-Elkies-Atkin (SEA) algorithm can deal the problem of computing $\#E(\mathbb{F}_p)$, where p has hundreds of digits, see [9].

6.2 The Setup and the Naive Method

Let $p \neq 2, 3$ be a prime and let E be an elliptic curve over $\mathbb{F}_p$ given by a Weierstrass equation

$$y^2 = x^3 + Ax + B \tag{6.1}$$

for some $A, B \in \mathbb{F}_p$. The curve is not singular, so $4A^3 + 27B^2 \not\equiv 0 \pmod{p}$. We know that the set $E(\mathbb{F}_p)$ of rational points of E consists of the solutions $(a, b) \in \mathbb{F}_p^2$ satisfying the curve equation and the point at infinity O. Using the group law on elliptic curves restricted to this set we know that this set $E(\mathbb{F}_p)$ forms an abelian group, with O acting as the zero element. The number of points in $E(\mathbb{F}_p)$ with given X-coordinate $x \in \mathbb{F}_p$ is 0, 1 or 2.

Let $\left(\frac{\cdot}{p}\right)$ denote the usual quadratic symbol[(1)]. There are

$$1 + \left(\frac{x^3 + Ax + B}{p}\right)$$

rational points on E with X-coordinate equal to x. For a discussion involving the complexity of Legendre symbol, see Appendix A.1. Including the point at infinity, the set of rational points $E(\mathbb{F}_p)$ of E therefore has cardinality

$$\#E(\mathbb{F}_p) = 1 + \sum_{x \in \mathbb{F}_p} \left(1 + \left(\frac{x^3 + Ax + B}{p}\right)\right)$$

The 1 in this equation stands for the point at infinity $O = [0 : 1 : 0]$. If we group altogheter the ones in the previous equation, we get

$$\#E(\mathbb{F}_p) = 1 + \sum_{x \in \mathbb{F}_p} \left(1 + \left(\frac{x^3 + Ax + B}{p}\right)\right) = 1 + p + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + Ax + B}{p}\right)$$

Remark 6.2.1. The same argument holds if we consider a finite field $\mathbb{F}_q$ with $q = p^r$, where $p \neq 2, 3$ is prime and $r \in \mathbb{N}$ (and we use Jacobi's symbol instead of Legendre's).

[(1)] Recall that an integer a is a quadratic residue modulo p if it is congruent to a perfect square modulo p and is a quadratic nonresidue modulo p otherwise. The Legendre symbol is defined as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \text{ if } a \text{ is a quadratic residue modulo } p \text{ and } a \not\equiv 0 \pmod{p} \\ -1 \text{ if } a \text{ is a quadratic non-residue modulo } p \\ 0 \text{ if } a \equiv 0 \pmod{p}. \end{cases}$$

Remark 6.2.2. We deduce a first trivial bound $\#E(\mathbb{F}_p) \leq 2p+1$ (see Remark 4.1.8). We can use this equation to compute the number of points in $E(\mathbb{F}_p)$: we then have to compute p Legendre symbols. Now, every Legendre symbol is computed using fast exponentiation, and therefore by the result in Appendix A.1, the total running time is $O(q\log^3 q)$ if we use the elementary multiplication algorithm.

So this naive counting algorithm is not polynomial time: the size of the result is the number of digits in $\#E(\mathbb{F}_q)$ and this is $\leq \log_{10}(3q+1)+1$. An efficient counting algorithm should run in time polynomial in $\log q$, and this is the case of Schoof's algorithm.

6.3 The Idea Behind the Algorithm

To set up the situation, let $E/\mathbb{F}_q$ be an elliptic curve defined over a finite field $\mathbb{F}_q$, where $q = p^r$ for $p \neq 2,3$ a prime and r an integer ≥ 1, and consider its Weierstrass equation

$$y^2 = f(x) := x^3 + Ax + B$$

with $A, B \in \mathbb{F}_q$. Hasse's theorem 4.1.10 says that

$$\#E(\mathbb{F}_q) = q + 1 - t \tag{6.2}$$

with

$$|t| \leq 2\sqrt{q} \tag{6.3}$$

We start by quickly describing the ideas behind Schoof's Algorithm, which computes $\#E(\mathbb{F}_q)$ in polynomial time, i.e., it computes $\#E(\mathbb{F}_q)$ in $O(\log^c q)$ steps, where c is fixed, independent of q. Its approach is to compute the cardinality $\#E(\mathbb{F}_q)$ by making use of Hasse's theorem on elliptic curves along with the Chinese remainder theorem and division polynomials.

Hasse's theorem simplifies our problem by narrowing down $\#E(\mathbb{F}_q)$ to a finite (even if large) set of possibilities. We want to compute the value t as seen in equation 6.2: it is enough to compute t modulo N where $N > 4\sqrt{q}$. While there is no efficient way to compute $t \pmod N$ directly for general N, it is possible to compute $t \pmod l$ for l a small prime, rather efficiently. We choose $S = \{l_1, l_2, ..., l_r\}$ to be a set of distinct primes such that $\prod l_i = N > 4\sqrt{q}$. Given $t \pmod{l_i}$ for all $l_i \in S$, the Chinese remainder theorem allows us to compute $t \pmod N$.

Now, in order to compute $t \pmod l$ for a prime $l \neq p$, we make use of the theory of the Frobenius endomorphism ϕ and division polynomials. Note that considering primes $l \neq p$ is no loss since we can always pick a

bigger prime to take its place to ensure the product is big enough. Let

$$\begin{aligned} \phi : E(\overline{\mathbb{F}}_q) &\to E(\overline{\mathbb{F}}_q) \\ (x,y) &\to (x^q, y^q) \end{aligned}$$

be the q-power Frobenius map, so Theorem 4.2.5(b) tells us that

$$\phi^2 - t\phi + q = 0 \tag{6.4}$$

in $\mathrm{End}(E)$. In particular, if $P \in E(\mathbb{F}_q)[l]$ (the group of l-torsion points, see Definition 2.4.3), then

$$\phi^2(P) - [t]\phi(P) + [q]P = O$$

so if we write $P = (x,y)$ (we assume that $P \neq O$), then

$$(x^{q^2}, y^{q^2}) - [t](x^q, y^q) + [q](x,y) = O$$

One could try to compute these points (x^{q^2}, y^{q^2}), (x^q, y^q) and $[q](x,y)$ as functions in the coordinate ring $\mathbb{F}_p[x,y]/(y^2 - f(x))$ of E and the search for a value of t which satisfies the equation. However, the degrees get very large and this approach is hopeless.

A key observation is that, since the point $P = (x,y)$ is chosen to have order l, we have $[q]P = [\overline{q}]P$, where $\overline{q}$ is the unique integer such that $q \equiv \overline{q} \pmod{l}$, $0 \leq \overline{q} < l$.

Now, note that $\phi(O) = O$ and that for any integer r we have $r\phi(P) = \phi(rP)$. Thus $\phi(P)$ will have the same order as P: since $P = (x,y) \in E[l]$, we have also $\phi(P) \in E[l]$ and so $[t](x^q, y^q) = [\bar{t}](x^q, y^q)$, where $t \equiv \bar{t} \pmod{l}$ with $0 \leq \bar{t} < l$. Hence we have reduced our problem to solving the equation

$$(x^{q^2}, y^{q^2}) + [\bar{q}](x,y) \equiv [\bar{t}](x^q, y^q) \tag{6.5}$$

Remark 6.3.1. We can compute the trace t of the Frobenius endomorphism modulo l by checking which of the relations

$$(\phi^2 - \bar{t}\phi + q)P = 0$$

hold on $E[l]$.

Remark 6.3.2. For ease of notation, when the context is clear we will often write mP instead of $[m]P$ for the multiplication-by-m map.

Remark 6.3.3. Of course, we don't know the value of $\bar{t}$, so for each integer n between 0 and l we compute $[n](x^q, y^q)$ for a point $(x,y) \in E[l]/\{O\}$ and check to see whether it satisfies

$$[n](x^q, y^q) = (x^{q^2}, y^{q^2}) + [q](x,y)$$

However, the individual points in $E[l]$ tend to be defined over large extension fields of $\mathbb{F}_q$, so we instead work with all of the l-torsion points simultaneously. To do this, we use the division polynomial (Definition 6.5.2)

$$\psi_l(x) \in \mathbb{F}_q[x]$$

whose roots are the x-coordinates of the nonzero l-torsion points of E. (For simplicity, we assume that $l \neq 2$.) This division polynomial has degree $\frac{1}{2}(l^2-1)$ and is easily computed using the recurrence described in Definition 6.5.2. We then perform all computations in the quotient ring

$$R_l = \mathbb{F}_q[x,y] / \left(\psi_l(x), y^2 - f(x)\right)$$

Thus anytime we have a nonlinear power of y, we replace y^2 with $f(x)$, and anytime we have a power x^d with $d \geq \frac{1}{2}(l^2-1)$, we divide by $\psi_l(x)$ and take the remainder. In this way we never have to work with polynomials of degree greater than $\frac{1}{2}(l^2-3)$.

Our goal is to compute the value of $t \pmod{l}$ for enough primes l to determine t. Hasse's theorem says that $|t| \leq 2\sqrt{q}$, so it suffices to use all primes $l \leq l_{\max}$ such that

$$\prod_{l \leq l_{\max}} l \geq 4\sqrt{q} \tag{6.6}$$

The preceding discussion is the idea behind the following algorithm which computes $\#E(\mathbb{F}_q)$.

Algorithm 4 Schoof's Algorithm

$A := 1$;
$l := 3$;
while $A < 4\sqrt{q}$ **do**
  for $n = 0, \ldots, l-1$ **do**
    if $(x^{q^2}, y^{q^2}) + [q](x,y) = [n](x^q, y^q)$ in the ring R_l **then**
      Break out the loop;
    end if
  end for
  $A = l \cdot A$;
  $n_l = n$;
  $l :=$ next largest prime;
end while
Use the Chinese remainder theorem to find an integer a satisfying $a \equiv n_l \pmod{l}$ for all the stored values of n_l;
return $\#E(\mathbb{F}_q) = q + 1 - a$

Even before going to the detailed description of Schoof's algorithm, we can discuss its complexity already.

6.4 The Complexity

We prove that the running time of Schoof's algorithm is $O(\log^8 q)$. We begin by verifying three claims, having in mind the pseudo-code algorithm 4.

(a) The largest prime l used by the algorithm satisfies $l \leq O(\log q)$.

By classical results in analytic number theory, we know that the prime number theorem implies the statement

$$\lim_{X\to\infty} \frac{1}{X} \sum_{l\leq X, l\text{prime}} \log l = 1$$

Hence $\prod_{l\leq X} l \approx e^X$, so in order to make the product larger than $4\sqrt{q}$, it suffices to take $X \approx \frac{1}{2}\log(16q)$.

(b) Multiplication in the ring R_l can be done in $O(l^4\log^2 q)$ bit operations.

Elements of the ring R_l are polynomials of degree $O(l^2)$. Multiplication of two such polynomials and reduction modulo $\psi_l(x)$ takes $O(l^4)$ elementary operations (additions and multiplications) in the field $\mathbb{F}_q$. Similarly, multiplication in $\mathbb{F}_q$ takes $O(\log^2 q)$ bit operations. So basic operations in R_l take $O(l^4\log^2 q)$ bit operations.

Remark 6.4.1. A bit operation is a basic computer operation on one or two bits. Examples of bit operations include addition, multiplication, and, or, xor, and complement. Observe that, if we use fast exponentiation methods, we can reduce multiplication in R_l to $O((l^2\log q)^{1+\epsilon})$ bit operations, at the cost of a larger big-O constant.

(c) It takes $O(\log q)$ ring operations in R_l to reduce $x^q, y^q, x^{q^2}, y^{q^2}$ in the ring R_l.

In general, the square-and-multiply algorithm (see [10, §XI.1]) allows us to compute powers x^n and y^n using $O(\log n)$ multiplications in R_l. We note that this computation is done only once, and then the points

$$(x^{q^2}, y^{q^2}) + [q \bmod l](x, y) \quad \text{and} \quad (x^q, y^q)$$

are computed and stored for use in step (4) of Schoof's algorithm.

We now use (a), (b), and (c) to estimate the running time of Schoof's algorithm. From (a), we need to use only primes l that are less than $O(\log q)$. There are $O(\log q/\log\log q)$ such primes, so that is how many times the A-loop, steps (2)-(9), is executed. Then, each time we go through the A-loop, the n loop, steps (3)-(5), is executed $l = O(\log q)$ times.

Further, since $l = O(\log q)$, claim (b) says that basic operations in R_l take $O(\log^6 q)$ bit operations. The value of $[n](x^q, y^q)$ in step (4) can be computed in $O(1)$ operations in R_l from the previous value $[n-1](x^q, y^q)$, or we can be inefficient and compute it in $O(\log n) = O(\log l) = O(\log \log q)$ R_l-operations using the double-and-add algorithm.

Hence the total number of bit operations required by Schoof's algorithm is

$$A \text{ loop} \cdot n \text{ loop} \cdot \text{bit operations per } R_l \text{ operation}$$

i.e.

$$O(\log q) \cdot O(\log q) \cdot O(\log^6 q) = O(\log^8 q)$$

bit operations.

This completes the proof that Schoof's algorithm computes $\#E(\mathbb{F}_q)$ in polynomial time.

Remark 6.4.2. If we use fast arithmetic methods, we have that the total cost of Schoof algorithm is actually

$$T = O(\log^{5+o(1)} q)$$

The memory space used by the algorithm is

$$M = \log^3 q$$

because we need to store the division polynomials ψ_l. They have degree $(l^2-1)/2$ and coefficients in $\mathbb{F}_q$.

6.5 The Division Polynomials

Remark 6.5.1. From now on, we will just consider the problem of computing $\#E(\mathbb{F}_q)$ for q prime. In fact we have seen in Theorem 4.2.5(a) how one can easily compute $\#E(\mathbb{F}_q)$, with $q = p^r$, once $\#E(\mathbb{F}_p)$ is known.

Schoof idea to compute easily t modulo primes l relies on the introduction of the so called *division polynomials* ψ_n for the curve E. By their very definition, these polynomials ψ_n cancel exactly on n-torsion points. Let $E[n] = \{P \in E(\overline{\mathbb{F}}_p) \mid nP = 0\}$. We want to define $\psi_n := \psi_n(x, y) \in \mathbb{F}_q[x, y]$ in such a way that

$$\psi_n(x, y) = 0 \Leftrightarrow (x, y) \in E[n]$$

Definition 6.5.2. These polynomials are defined recursively as follows for $n \in \mathbb{Z}_{\geq -1}$.

$$\begin{aligned}
\psi_{-1}(x,y) &= -1, \psi_0(x,y) = 0, \psi_1(x,y) = 1, \psi_2(x,y) = 2y, \\
\psi_3(x,y) &= 3x^4 + 6Ax^2 + 12Bx - A^2, \\
\psi_4(x,y) &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3), \\
\psi_{2n}(x,y) &= \psi_n(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2)/2y \quad (n \in \mathbb{Z}_{\geq 1}), \\
\psi_{2n+1}(x,y) &= \psi_{n+2}\psi_n^3 - \psi_{n+1}^3\psi_{n-1} \qquad (n \in \mathbb{Z}_{\geq 1}).
\end{aligned}$$

For practical reasons, we now define the polynomials $f_n(x) \in \mathbb{F}_q[x]$ as follows. First we eliminate all y^2-terms from ψ_n: using the elliptic curve equation we can replace y^2 with $x^3 + Ax + B$. More generally we can replace y^{2k} with $(x^3 + Ax + B)^k$. This allows us to express the division polynomials as elements $\psi_n'(x,y)$ of $\mathbb{F}_q[x]$ or $y\mathbb{F}_q[x]$.

$$f_n(x) = \psi_n'(x,y) \quad \text{if } n \text{ is odd}, \tag{6.7}$$
$$f_n(x) = \psi_n'(x,y)/y \text{ if } n \text{ is even}. \tag{6.8}$$

These polynomials, by definition, also have the property that $f_n(x) = 0$ if and only if x is the x-coordinate of a point of order n. From the recursive formulas for ψ_n given above, one easily deduces that

$$\begin{aligned}
\deg f_n &= \frac{1}{2}(n^2 - 1) \text{ if } n \text{ is odd}, q \nmid n, \\
\deg f_n &= \frac{1}{2}(n^2 - 4) \text{ if } n \text{ is even}, q \nmid n
\end{aligned}$$

Proposition 6.5.3. *Let $P = (x,y) \in E(\overline{\mathbb{F}}_q)$ with $P \notin E[2]$ and let $n \in \mathbb{Z}_{\geq -1}$; then*

$$nP = 0 \Leftrightarrow f_n(x) = 0 \tag{6.9}$$

Proof. See Lang, *Elliptic curves: diophantine analysis*. □

Proposition 6.5.4. *Let $P = (x,y) \in E(\overline{\mathbb{F}}_q)$; let $n \in \mathbb{Z}_{\geq 1}$ with $nP \neq 0$; then*

$$nP = \left(x - \frac{\psi_{n-1}\psi_{n+1}}{\psi_n^2}, \frac{\psi_{n+1}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2}{4y\psi_n^3} \right) \tag{6.10}$$

(By ψ_k we mean $\psi_k(x,y)$).

Proof. See Lang, *Elliptic curves: diophantine analysis*. □

These explicit formulas will enable us to do the computations on l-torsion points of $E(\overline{\mathbb{F}}_q)$ that we need in our algorithm.

6.6 Algorithm Implementation

We are now ready to see the algorithm in detail. After computing a number L for which condition 6.6 holds and after making a list of the polynomials f_n (for $n \in [1, L]$), our second step is to compute $t \pmod{l}$ for different primes $l \leq L$. For the case of $l = 2$ we devise an *ad hoc* procedure, so we consider this case first. For $l > 2$ we will proceed differently, by mean of the Frobenius endomorphism and the division polynomials.

6.6.1 The case $l = 2$

Let $l = 2$. As usual, assume q is odd. Then we have

$$\#E(\mathbb{F}_q) = q + 1 - t \equiv t \bmod 2$$

Now, by Lagrange's and Sylow's theorems, $\#E(\mathbb{F}_q)$ is even if and only if there exists a subgroup of order 2. So in particular

$$t \equiv 0 \bmod 2 \Leftrightarrow \exists P \in E(\mathbb{F}_q) \text{ such that } 2P = O$$

Now, by definition of addition in the group, any element of order 2 must be of the form $P = (x_0, 0)$. Therefore, $t \equiv 0 \bmod 2$ if and only if the polynomial $x^3 + Ax + B$ has a root $x_0 \in \mathbb{F}_q$. Thanks to a basic result in algebra, this is true if and only if $\gcd(x^q - x, x^3 + Ax + B) \neq 1$. To sum up,

$$t \equiv \begin{cases} 1 (\bmod 2) & \text{if } \gcd(x^q - x, x^3 + Ax + B) = 1 \\ 0 (\bmod 2) & \text{if } \gcd(x^q - x, x^3 + Ax + B) \neq 1 \end{cases}$$

6.6.2 The case $l > 2$

We now proceed to see the part of the algorithm in which the computation modulo primes $l \neq 2$ is made explicit. Recall equation 6.5:

$$(x^{q^2}, y^{q^2}) + q(x, y) \equiv \tau(x^q, y^q)$$

where we called $\tau := \bar{t}$. By the Remark 6.3.1, we can compute $t \pmod{l}$ by checking which of the relations

$$\phi_l^2 + q = \tau \phi_l \quad (\tau \in \mathbb{Z}/l\mathbb{Z}) \tag{6.11}$$

holds on $E[l]$. These tests can be effected by computations with polynomials in $\mathbb{F}_q[X, Y]$: let l be a prime not equal to 2 or p and let $P = (x, y) \in E[l]$ not equal to 0. By Proposition 6.5.4 the relation 6.11 holds for (x, y) if and

only if

$$(x^{q^2}, y^{q^2}) + \left(x - \frac{\psi_{q-1}\psi_{q+1}}{\psi_q^2}, \frac{\psi_{q+2}\psi_{q-1}^2 - \psi_{q-2}\psi_{q+1}^2}{4y\psi_q^3}\right) =$$
$$= \begin{cases} 0 & \text{if } \tau \equiv 0 \ (\bmod\ l), \\ \left(x^q - \left(\frac{\psi_{\tau-1}\psi_{\tau+1}}{\psi_\tau^2}\right)^q, \left(\frac{\psi_{\tau+2}\psi_{\tau-1}^2 - \psi_{\tau-2}\psi_{\tau+1}^2}{4y\psi_\tau^3}\right)^q\right) & \text{otherwise} \end{cases} \tag{6.12}$$

(By ψ_k we denote $\psi_k(x, y)$ as before). By Proposition 6.5.3 the point $P = (x, y)$ is in $E[l]$ if and only if $\psi_l(x, y)$ or, equivalently, $f_l(x) = 0$. Using formula 6.1 and the addition formulas of Theorem 2.2.2, the relation 6.12 can be transformed into relations of the form

$$H_1(x) = 0 \text{ and } H_2(x) = 0$$

for some polynomials in $\mathbb{F}_q[X]$. This comes from the fact that $P = (x, y)$ satisfies 6.12 if and only if $-P = (x, -y)$ does. The final test boils down to testing whether

$$H_1 \equiv 0 \pmod{f_l} \text{ and } H_2 \equiv 0 \pmod{f_l} \tag{6.13}$$

in $\mathbb{F}_q[X]$.This test is done for every $\tau \in \mathbb{Z}/l\mathbb{Z}$, until a value of τ is encountered for which 6.6.2 holds; then we have that $t \equiv \tau \ (\bmod\ l)$. Note that testing 6.11 is equivalent to testing whether $\phi_l^2 + k = \tau\phi_l$, holds on $E[l]$, where $k \equiv q \pmod{l}$ and $1 \leq k < l$.

We will use now formula 6.12; since we use the addition formulas of Theorem 2.2.2 to evaluate 6.12, we distinguish the cases where the points are distinct or not: first test whether there is a nonzero point $P = (x, y)$ in $E[l]$ for which $\phi_l^2 P = \pm kP$ holds. Here $k \equiv q \pmod{l}$ and $1 \leq k < l$. So we must test Whether

$$x^{q^2} = x - \frac{\psi_{k-1}\psi_{k+1}}{\psi_k^2}(x, y)$$

holds or, using $f_m(X)$ rather than $\psi_m(X, Y)$

$$x^{q^2} = \begin{cases} x - \frac{f_{k-1}(x)f_{k+1}(x)}{f_k^2(x)(x^3+Ax+B)} & \text{if } k \text{ is even} \\ x - \frac{f_{k-1}(x)f_{k+1}(x)(x^3+Ax+B)}{f_k^2(x)} & \text{if } k \text{ is odd} \end{cases}$$

Note that the denominators in the above expressions do not vanish on $E[l]$. In order to simplify notation, put

$$g_k(x) := \begin{cases} (x^{q^2} - x)f_k^2(x)(x^3 + ax + b) + f_{k-1}(x)f_{k+1}(x) & k \text{ even} \\ (x^{q^2} - x)f_k^2(x) + f_{k-1}(x)f_{k+1}(x)(x^3 + ax + b) & k \text{ odd} \end{cases}$$

We find that

$$\phi_l^2 P = \pm kP \text{ if and only if } g_k(x) = 0$$

and we can test whether a point like P exists in $E[l]$ by computing $\gcd(g_k(x), f_l(x))$. We have two cases:

Case 1 If $\gcd(g_k(x), f_l(x)) \neq 1$, we have that a point P exists in $E[l]$ with $\phi_l^2 P = \pm qP$.

Case 2 If $\gcd(g_k(x), f_l(x)) = 1$, we have that $\tau \neq 0$ in 6.11, and we test equation 6.5 for various values of τ. In testing 6.11 for these values we can, when adding $\phi_l^2(x, y)$ and $q(x, y)$, apply the version of the addition formulas where the two points have distinct X-coordinates.

We now discuss the two cases in detail. *Case 1*. This is the case where for some nonzero $P \in E[l]$ we have that $\phi_l^2 P = \pm qP$. We'll see that, in this case, $t \in \{0, -2w, +2w\}$, where $w^2 \equiv q \pmod{l}$. If $\phi_l^2 P = -qP$, for some nonzero P, we have by 6.4 that $t\phi_l P = 0$, whence, since $\phi_l P \neq 0$, that $t \equiv 0 \pmod{l}$. If $\phi_l^2 P = qP$ for some nonzero P, we have by 6.4 that

$$(2q - t\phi_l)P = 0 \quad \text{and} \quad \phi_l P = \frac{2P}{t} P$$

(Note that $t \not\equiv 0 \pmod{l}$ since $l \neq 2, p$). From this, by squaring both sides, we deduce that $4q^2 = t^2\phi_l^2 = t^2 q$, i.e. $t^2 \equiv 4q \pmod{l}$. Therefore, q is a quadratic residue. Let $w \in \mathbb{Z}$ with $0 < w < l$ denote a square root of $q \pmod{l}$; this number may be computed by successively trying $1, 2, \ldots$. Once w is found, we have $4w^2 = t^2$, so that $t = \pm 2w$. Now

$$(\phi_l - w)(\phi_l + w) = \phi_l^2 - q = 0 \quad \text{so } \phi_l P = \pm wP$$

and therefore the eigenvalues of ϕ_l acting on $E[l]$ are w and $-w$. We can decide Case l by the following computations.

If $(\frac{q}{l}) = -1$ we clearly have that $t \equiv 0 \pmod{l}$; if not, we compute w, a square root of $q \pmod{l}$ with $0 < w < l$ and we test whether w or $-w$ is an eigenvalue of ϕ_l; if this is not the ease, we conclude that $t \equiv 0 \pmod{l}$ and if indeed a nonzero point P exists with $\phi_l P = \pm wP$, we test whether either $\phi_l P = wP$ or $\phi_l P = -wP$ holds. In the first case we have $t \equiv 2w \pmod{l}$; in the second case, $t \equiv -2w \pmod{l}$. Put

$$h_w(x) := \begin{cases} (x^q - x) f_w^2(x)(x^3 + ax + b) + f_{w-1}(x) f_{w+1}(x) & w \text{ even} \\ (x^q - x) f_w^2(x) + f_{w-1}(x) f_{w+1}(x)(x^3 + ax + b) & w \text{ odd} \end{cases}$$

Computing explicitly, with $w^2 \equiv q \pmod{l}$, we have that

- if $\gcd(h_w(x), f_l(x)) = 1$, we have $\phi_l^2 P = -qP$ so that $t \equiv 0 \pmod{l}$;

- if $\gcd(h_w(x), f_l(x)) \neq 1$, then $t \equiv \pm 2w \pmod{l}$ and we test the y-coordinate of $\phi_l P = \pm wP$ to determine the sign, like follows.

So suppose we know that $\phi_l P = \pm wP$: we need test the y-coordinate of $\phi_l P = wP$. Equation 6.10 gives for the y-coordinate,

$$y^q \equiv \frac{\psi_{w+2}\psi_{w-1}^2 - \psi_{w-2}\psi_{w+1}^2}{4y\psi_w^3} (\text{mod } \psi_l, q)$$

Put

$$r_w := \begin{cases} 4(y^2)^{(q+3)/2} f_w^3(x) - f_{w+2}(x) f_{w-1}^2 + f_{w-2}(x) f_{w+1}^2(x) & w \text{ even} \\ 4(y^2)^{(q-1)/2} f_w^3(x) - f_{w+2}(x) f_{w-1}^2 + f_{w-2}(x) f_{w+1}^2(x) & w \text{ odd} \end{cases}$$

where, as usual, $y^2 = x^3 + ax + b$. Notice that $r_w(x)$ is also a polynomial in x only since all exponents of y are even.

- If $\gcd(r_w(x), f_l(x)) = 1$ then there is no $P \in E[l]$ for which $\phi_l P = wP$, so $t \equiv -2w \pmod{l}$
- If $\gcd(r_w(x), f_l(x)) \neq 1$ such a point exists and $t \equiv 2w \pmod{l}$.

Case 2. This is the case where $\phi_l^2 P \neq \pm qP$ for any $P \in E[l]$. In this case we will test which of the relations 6.11 holds with $\tau \in \mathbb{Z}/l\mathbb{Z}^\times$. We have with $P = (x, y)$ and $k \equiv q \pmod{l}$ and $0 < k < l$, that

$$\phi_l^2 P + qP = \left(-x^{q^2} - x + \frac{\psi_{k-1}\psi_{k+1}}{\psi_k^2} + \lambda^2, y^{q^2} - \lambda \left(-2x^{q^2} - x + \frac{\psi_{k-1}\psi_{k+1}}{\psi_k^2} + \lambda^2 \right) \right),$$

where

$$\lambda = \frac{\psi_{k+2}\psi_{k-1}^2 - \psi_{k-2}\psi_{k+1}^2 - 4y^{q^2+1}\psi_k^3}{4\psi_k y((x - x^{q^2})\psi_k^2 - \psi_{k-1}\psi_{k+1})}$$

Note that the denominator of λ does not vanish on $E[l]$ since ψ_k has no zeros on $E[l]$ and since we are in Case 2. Let $\tau \in \mathbb{Z}$ with $0 < \tau < l$; we have

$$\tau\phi_l P = \left(x^q - \left(\frac{\psi_{\tau+1}\psi_{\tau-1}}{\psi_\tau^2} \right)^q, \left(\frac{\psi_{\tau+2}\psi_{\tau-1}^2 - \psi_{\tau-2}\psi_{\tau+1}^2}{4y\psi_\tau^3} \right)^q \right)$$

In a way analogous to the computations above one can test, by computations in $\mathbb{F}_q[X]$, which of the relations 6.11 holds by trying $\tau = 1, \ldots, l-1$. The computations involve evaluating polynomials modulo $f_l(X)$ and testing whether they are zero $f_l(X)$. We do not give all the details here, since they are quite long, but it is not difficult to fill in the details. Long story short, testing whether $\phi_l^2 + q = \tau\phi_l$, holds on $E[l]$ boils down to testing whether

$$((\psi_{k-1}\psi_{k+1} - \psi_k^2(X^{q^2} + X^q + X))\beta^2 + \psi_k^2\alpha^2)\psi_\tau^{2q} + \psi_{\tau-1}^q\psi_{\tau+1}^q\beta^2\psi_k^2$$

and

$$4Y^q\psi_\tau^{3q}(\alpha((2X^{q^2}+X)\beta^2\psi_k^2-\psi_{k-1}\psi_{k+1}\beta^2+\psi_k^2\alpha^2)-Y^{q^2}\beta^3\psi_k^2)+ \\ -\beta^3\psi_k^2(\psi_{\tau+2}\psi_{\tau-1}^2-\psi_{\tau-2}\psi_{\tau+1}^2)^q \tag{6.14}$$

are zero mod $f_l(x)$. Here

$$\alpha=\psi_{k+2}\psi_{k-1}^2-\psi_{k-2}\psi_{k+1}^2-4Y^{q^2+1}\psi_k^3$$

and

$$\beta=((X-X^{q^2})\psi_k^2-\psi_{k-1}\psi_{k+1})4Y\psi_k$$

By the expressions 6.14 we understand the polynomials in $\mathbb{F}_q$ one gets after eliminating Y using 6.14 and, if necessary, by dividing the expressions by Y. The result is a polynomial in $\mathbb{F}_q[X]$.

This completes the description of the second step of the algorithm.

6.7 Putting all Together

To sum up, the steps of the algorithm are

Step 1 Compute a number L for which condition 6.6 holds and of making a list of the polynomials f_n for $n=1,2,\ldots,L$.

Step 2 Computation of $t \pmod l$ for every prime $l \leq L$ not equal to p.

Step 3 Computation of t from the values of t mod l obtained using the Chinese Remainder Theorem and the estimate 6.3

Remark 6.7.1. Step 3 is straightforward. This completes the description of the algorithm.

6.8 Improvements

In the 1990s, Noam Elkies, followed by A. O. L. Atkin, devised improvements to Schoof's basic algorithm by restricting the set of primes $S=\{l_1,\ldots,l_s\}$ considered before to primes of a certain kind. These came to be called Elkies primes and Atkin primes respectively. A prime l is called an Elkies prime if the characteristic equation: $\phi^2-t\phi+q=0$ splits over $\mathbb{F}_l$, while an Atkin prime is a prime that is not an Elkies prime. Atkin showed how to combine information obtained from the Atkin primes with the information obtained from Elkies primes to produce an efficient algorithm, which came to be known as the Schoof-Elkies-Atkin (SEA) algorithm. The first problem to address is to determine whether a given prime is Elkies or Atkin. In order to do so, we make use of modular polynomials, which come

from the study of modular forms and an interpretation of elliptic curves over the complex numbers as lattices. Once we have determined which case we are in, instead of using division polynomials, we proceed by working modulo the modular polynomials f_l which have a lower degree than the corresponding division polynomial ψ_l (degree $O(l)$ rather than $O(l^2)$). This results in a further reduction in the running time, giving us an algorithm more efficient than Schoof's, with complexity $O(\log^6 q)$ for standard arithmetic and $O(\log^4 q)$ using fast exponentiation techniques.

CHAPTER 7

Computing Square Roots in Finite Fields

Abstract

An important problem in computational number theory is the computation of square roots modulo a prime p. As an application of Schoof's results, we give an algorithm to compute the square root of $x \in \mathbb{Z} \bmod p$, whenever x is a square mod p. This algorithm is deterministic and for fixed $x \in \mathbb{Z}$ it takes $O(\log^8 p)$ elementary operations; here the O-symbol depends on x; in general, the algorithm takes $O((|x|^{1/2+\epsilon}\log p)^8)$ elementary operations for any $\epsilon > 0$. If we apply fast multiplication techniques, the algorithm will take $O((|x|^{1/2}\log p)^{5+\epsilon})$ elementary operations for any $\epsilon > 0$.

Let p be an odd prime number, and suppose that $\left(\frac{a}{p}\right) = 1$. Then by definition, there exists an x such that $x^2 \equiv a \pmod{p}$. Our task is to find such a square x. A brute force search would take time $O(p)$ and, even for p moderately large, this is of course not practical. We need a faster algorithm to do this. We distinguish two cases:

1. $p \equiv 3, 5, 7 \pmod 8$ (easy)
2. $p \equiv 1 \pmod 8$ (hard)

7.1 The First Case

7.1.1 $p \equiv 3 \pmod 4$

There is an easy solution which comes to mind that works for half of the primes p, i.e. primes $p \equiv 3 \pmod 4$. In this case a solution is given by

$$x = a^{(p+1)/4} \pmod p$$

Indeed, since a is a quadratic residue, we have $a^{(p-1)/2} \pmod p$, hence

$$x^2 \equiv a^{(p+1)/2} \equiv a \cdot a^{(p-1)/2} \equiv a \pmod p$$

as claimed.

7.1.2 $p \equiv 5 \pmod 8$

A less trivial solution works for half of the remaining primes, i.e. primes $p \equiv 5 \pmod 8$. Since we have $a^{(p-1)/2} \equiv 1 \pmod p$ and since $\mathbb{F}_p$ is a field, we must have

$$a^{(p-1)/4} \equiv \pm 1 \pmod p$$

Now, if the sign is $+$, we can easily check as above that

$$x = a^{(p+3)/8} \pmod p$$

is a solution. Otherwise, using $p \equiv 5 \pmod 8$, we know that $2^{(p-1)/2} \equiv -1 \pmod p$. Then one can check that

$$x = 2a \cdot (4a)^{(p-5)/8} \pmod p$$

is a solution.

7.2 The Second Case

The only remaining case is $p \equiv 1 \pmod 8$. For this, we will devise a deterministic algorithm that computes a square root of $d \in \mathbb{Z}$ modulo p. This is a direct application of Schoof's algorithm for counting rational points on elliptic curves over finite fields.

Remark 7.2.1. This approach, even if it does solve the problem in a deterministic way, is not actually of practical use since it depends very badly on the size $|d|$: the algorithm works in fact in polynomial time in $|d| \log p$.

Remark 7.2.2. This approach works in general for primes $p \equiv 1 \pmod 4$, not just $p \equiv 1 \pmod 8$.

Let p be a rational prime, and let $d \in \mathbb{Z}$ be a quadratic residue modulo p. We want to compute $\sqrt{d} \pmod{p}$. We may assume $d < 0$: in fact if $d > 0$ we can compute $\sqrt{-1}$ and then we obtain $\sqrt{-d}$. Let $K = \mathbb{Q}(\sqrt{d})$ and consider the ring of integers $\mathcal{O}_K$. By the results of Section 5.3 we can construct an elliptic curve E over $\mathbb{F}_p$ if p splits in $\mathcal{O}_K$, and by Schoof's algorithm we can compute $\#E(\mathbb{F}_p)$ in deterministic polynomial time in $\log p$. Write

$$\#E(\mathbb{F}_p) = p + 1 - t$$

By schoof's algorithm we can deduce the value t and therefore we obtain the equation of the characteristic polynomial

$$P(X) = X^2 - tX + p$$

Remark that t is the trace of the Frobenius map ϕ:

$$t = \mathrm{Tr}(\phi)$$

Now, consider the ring $\mathbb{Z}[\phi]$; we have of course $\mathbb{Z}[\phi] \subseteq \mathcal{O}_K$. Moreover, p splits in $\mathbb{Z}[\phi]$ since $P(X)$ has two distinct roots, t and 0 modulo p. We deduce a ring homomorphism

$$\begin{array}{rcl} \Psi_p : \mathbb{Z}[\phi] & \to & \mathbb{Z}/p\mathbb{Z} \\ \phi & \mapsto & t \end{array}$$

Now, $\sqrt{d} \in \mathcal{O}_K$; there are two cases to consider.

Case 1 $\sqrt{d} \in \mathbb{Z}[\phi]$. We can write

$$\sqrt{d} = a + b\phi$$

and look for integers $a, b \in \mathbb{Z}$. We deduce

$$\sqrt{d} = a + bt \pmod{p}$$

i.e. $\Psi_p(\sqrt{d}) = a + bt$.

Case 2 $\sqrt{d} \notin \mathbb{Z}[\phi]$. Therefore $\mathbb{Z}[\phi] \subsetneq \mathcal{O}_K$ and we can consider the conductor

$$\theta := [\mathcal{O}_K : \mathbb{Z}[\phi]] \neq 1$$

Recall that θ is prime to p if and only if $t \equiv 0 \pmod{p}$. From Remark 1.2.13 we have

$$\Delta_\phi = \theta^2 \Delta$$

where Δ, Δ_ϕ are the discriminant of $\mathcal{O}_K$ and $\mathbb{Z}[\phi]$, respectively. Now, Δ_ϕ is the discriminant of the characteristic equation and so $\Delta_\phi = t^2 - 4p$. Therefore

$$\theta^2 = \frac{t^2 - 4p}{\Delta}$$

Now, $\theta\sqrt{d} \in \mathbb{Z}[\phi]$ and so we can write

$$\theta\sqrt{d} = a + b\phi$$

with $a, b \in \mathbb{Z}$ and we deduce

$$\sqrt{d} = \frac{a + bt}{\theta} \pmod{p}$$

Example 7.2.3. Take $d = -2$, $p = 11$. We have $K = \mathbb{Q}(\sqrt{-2})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-2}]$, $\Delta = -8$. By Example 5.4.1, an elliptic curve having ring of endomorphism given by $\mathcal{O}_K$ is

$$E : y^2 = x^3 - \frac{5^3}{4704}x - \frac{5^3}{84672}$$

We want to reduce it modulo 11. This is possible since 11 splits in $\mathcal{O}_K$:

$$\Delta = -8 \equiv 3 \equiv 5^2 \pmod{11}$$

Now,

$$4704 \equiv -4 \pmod{11}, \quad 84672 \equiv 5 \pmod{11}$$

and since $-5^3 \equiv -4 \pmod{1}1$, we have

$$\begin{aligned} \frac{-5^3}{4704} &\equiv 1 \pmod{11} \\ \frac{-5^3}{84672} &\equiv -5^2 \equiv 8 \pmod{11} \end{aligned}$$

So we obtain the curve over $\mathbb{F}_{11}$

$$\overline{E} : y^2 = x^3 + x + 8$$

By Schoof's algorithm, we get

$$\#\overline{E}(\mathbb{F}_{11}) = 6 = 11 + 1 - t$$

so $t = \mathrm{Tr}(\phi) = 6$. The characteristic polynomial is

$$P(X) = X^2 - 6X + 11$$

and so $\Delta_\phi = t^2 - 4p = -8$. Therefore $\theta = 1$, $\mathbb{Z}[\phi] = \mathcal{O}_K$ and so $\sqrt{-2} \in \mathbb{Z}[\phi]$.

We want to find two integers $a, b \in \mathbb{Z}$ such that $a + b\phi = \sqrt{-2}$. By a trace reasoning, we have

$$0 = \mathrm{Tr}(\sqrt{-2}) = \mathrm{Tr}(a + b\phi) = 2a + bt = 2a + 6b$$

We find $a = -3b$ and $-3b + b\phi = \sqrt{-2}$. Now, by a norm reasoning we get

$$\begin{aligned} 2 &= N(\sqrt{-2}) = N(b(\phi - 3)) = b^2(\phi - 3)(\overline{\phi} - 3) = \\ &= b^2(p + 9 - 3t) = 2b^2 \end{aligned}$$

So $b^2 = 1$; take $b = 1$, $a = -3$. We have $\sqrt{-2} = -3 + \phi$. By applying the ring homomorphism Ψ_p to this identity we obtain

$$\Psi_p(-3 + \phi) = -3 + t = 3$$

which is a square root of -2 modulo 11.

APPENDIX A

Appendix

A.1 Algorithm for Fast Exponentiation

A very important problem is exponentiation: given a mod N with $a \in [0, N[$ and an integer $e \geq 1$, compute a^e mod N.

Computing a^e and then reducing modulo N is not a good idea because a^e might be very large. Another option would be to set $a_1 = a$ and compute

$$a_k := (a_{k-1} \times a)\%N$$

for $2 \leq k \leq e$. This requires $e-1$ multiplications and $e-1$ Euclidean divisions, and most important we never deal with integers bigger than N^2. The complexity of this method is thus $c \times e \times \log^2 N$, where c is a positive constant, using elementary school algorithms. However, we can do much better: we write the expansion of e in base 2

$$e = \sum_{k=0}^{K} \epsilon_k 2^k$$

and we set $b_0 = a$, $b_k = b_{k-1}^2 \% N$ for $1 \leq k \leq K$. We then notice that

$$a^e \equiv \prod_{k=0}^{K} b_k^{\epsilon_k} \bmod N$$

So we can compute $a^e \% N$ at the expense of $c \log e$ multiplications and Euclidean divisions between integers $\leq N^2$. The total number of elementary operations is thus $c \log e \log^2 N$ with this method. The algorithm above is called fast exponentiation and it makes sense in any group.

A first interesting consequence is that for p an odd prime and a an integer such that $1 \leq a \leq p-1$, we can compute the Legendre symbol

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

at the expense of $c\log^3 p$ elementary operations using elementary multiplication. If we use quasi-linear integer multiplication the running time is $(\log p)^{2+o(1)}$. So testing quadratic residues is achieved in polynomial deterministic time.

Bibliography

[1] A.O.L. Atkin and F. Morain. Elliptic curves and primality proving. *Mathematics of Computation*, 61 (203):29–68, 1993.

[2] Henri Cohen. *A Course in Computational Algebraic Number Theory*. Springer GTM 138, 1993.

[3] D.A. Cox. *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*. Wiley, 1989.

[4] Serge Lang. *Elliptic Functions, 2nd Edition*. Springer GTM 112, 1987.

[5] Serge Lang. *Algbraic Number Theory - Second Edition*. Springer GTM 110, 1994.

[6] A.K. Lenstra and H.W. Jr. Lenstra. Algorithms in number theory. *Handbook of theoretical computer science*, A:673–715, 1990.

[7] J.S. Milne. *Elliptic Curves*. BookSurge Publishers, 2006.

[8] René Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Mathematics of Computation*, 44 (170):483–494, 1985.

[9] René Schoof. Counting points on elliiptic curves over finte fields. *Journal de Théorie des Nombres de Bordeaux*, 7:219–254, 1995.

[10] Joseph H. Silverman. *The Arithmetic of Elliptic Curves, 2nd Edition*. Springer GTM 106, 2009.