Universidad Nacional de
Educación a Distancia

Máster en Matemáticas Avanzadas

Master's Thesis

Algorithms for the Construction of Elliptic Curves with Given Cardinality

Author:
Francesc Sebé

Supervisor:
Milagros Izquierdo

2012-13 Course

Abstract

The objective of this thesis has been the implementation and comparison of two algorithms for generating an elliptic curve over a finite field with a given cardinality. The first one was proposed by Atkin and Morain in 1993 as part of their widely known primality test. The second one comes from a technical report by Agashe, Lauter and Venkatesan (2001). Both proposals are based on the construction of the *Hilbert class polynomial* modulo a prime number and the obtention of the j*-invariant* of the required elliptic curve as one of its roots. Prior to the implementation of those algorithms, a study on their mathematical background has been carried out. The two algorithms have been implemented in Sage, which is an open source software aimed to the implementation of mathematical algorithms. In the performed experiments, the first method has clearly outperformed the second one, in terms of running time.

Acknowledgments

I sincerely acknowledge Milagros Izquierdo for her guidance. Her advice, help, comments and suggestions have been fundamental for a proper development of this thesis.

I also thank the support and love provided by my wife Glòria and our son Oriol.

Nomenclature

Symbols

$\mathbb{Z}$	set of integer numbers
$\mathbb{Z}_n$	set of integer numbers modulo n
$\mathbb{Q}$	set of rational numbers
$\overline{\mathbb{Q}}$	algebraic closure of $\mathbb{Q}$
$\mathbb{R}$	set of real numbers
$\mathbb{C}$	set of complex numbers
$U(A)$	unities of ring A
$\langle x_1, \ldots, x_n \rangle$	ideal generated by $x_1, \ldots, x_n$
$A[X_1, \ldots, X_n]$	ring of polynomials in n variables $X_1, \ldots, X_n$ and coefficients in A
E/K	field extension E of K
$[E : K]$	degree of E/K
$P(\alpha, K)$	minimum polynomial of α over K
$K(\alpha)$	field generated by α over K
$G(E : K)$	automorphism group of E/K
$\Delta[\alpha_1, \ldots, \alpha_n]$	discriminant of the basis $\{\alpha_1, \ldots, \alpha_n\}$
$\mathfrak{O}_K$	ring of integers of number field K
I_K	fractional ideals of K
P_K	principal fractional ideals of K
$C(\mathfrak{O}_K)$	ideal class group of $\mathfrak{O}_K$
$\mathcal{O}$	order
d_K	discriminant of number field K
$C(D)$	form class group of discriminant D
$\mathbb{P}^1$	projective line
$\mathbb{P}^2(\mathbb{C})$	complex projective plane
$[x, y, z]$	homogeneous coordinates of a projective point
$L(D)$	linear space associated with divisor D
$[\omega_1, \omega_2]$	lattice generated by ω_1 and ω_2
$\wp(z; L)$	Weierstrass $\wp$-function of lattice L
$j(L)$	j-invariant of lattice L
$H_D(X)$	Hilbert class polynomial of discriminant D
$E(K)$	points of elliptic curve E over K

List of Figures

List of Tables

Contents

Introduction

Elliptic functions were deeply studied in the 19th century by very relevant mathematicians such as Abel, Jacobi and Weierstrass. From the so-called Weierstrass $\wp$-function and some properties involving its derivative, it could be seen that elliptic functions are tightly related with elliptic (genus 1 complex) curves defined over the complex numbers. Elliptic curves defined over finite fields were also studied. For instance, in 1933, Hasse [11] presented a very important result which bounds the number of points such a curve can have.

In the early 70s, the possibility to apply algebraic geometry to the construction of error-correcting codes was discovered [10]. Goppa published several papers about the construction of codes from algebraic lines and algebraic curves defined over a finite field.

Later, during the mid-80s, several applications of elliptic curves defined over finite fields were found. In 1985, Koblitz [14] and Miller [17] independently proposed the use of elliptic curves in public key cryptography. The advantage of elliptic curve cryptography comes from the fact that no sub-exponential time algorithm is known for solving the *elliptic curve discrete logarithm problem*. As a consequence, 160 bits long public keys are enough for obtaining the same level of security than that provided by 1024 bits RSA keys, so that elliptic curve cryptography can be implemented at a lower cost. Some years later, other ways to use elliptic curves in cryptography appeared. For instance, in 2001, Boneh and Franklin [3] suggested the use of the Weil pairing over elliptic curves as a way to implement the so-called *identity-based encryption*. Cryptographic protocols based on the use of elliptic curve cryptography have been proposed in different areas such as: smart cards, RFID tags, vehicular ad-hoc networks and electronic voting, among many others.

In a paper published in 1987 (the idea was announced two years before), Lenstra presented the *elliptic curve factorization method* [15], a sub-exponential running time algorithm for factoring integers. Nowadays, this algorithm is the third-fastest known general purpose factoring algorithm while it is still considered the best one for integers with a not too large prime divisor.

In 1986, Goldwasser and Kilian [9] propose the use of elliptic curves for *primality testing*, *i.e.* proving that a given (very large) integer is prime. That algorithm works by performing several stages in which random elliptic curves are generated until one with a specific cardinality is found. In 1993, Atkin and Morain [2] enhance that algorithm by replacing the random search with an

algorithm for building elliptic curves with a required cardinality.

The construction of elliptic curves with an appropriate cardinality is also of great interest in cryptography. This is because the Pohlig-Hellman algorithm [19] solves the discrete logarithm problem in a temporal cost that depends on the largest prime dividing the order of the group the problem is defined in. Hence, the security of discrete logarithm-based cryptography on elliptic curves is given by the size of the largest prime factor dividing the cardinality of a curve. As a consequence, algorithms to obtain elliptic curves whose cardinality is divisible by a large prime factor are required.

More recently, hyperelliptic curves [16] (genus ≥ 2) have also been used in the design of factorization algorithms and public key cryptography.

This thesis surveys the theory of complex multiplication on elliptic curves and its application to the construction of elliptic curves defined over a finite field with a given cardinality. Two algorithms have been implemented, tested and compared. The first one was published in 1993 in a paper by Atkin and Morain [2] as a part of a primality testing algorithm. The second one corresponds to a proposal by Agashe, Lauter and Venkatesan [1] published in a technical report in 2001. The underlying theory of both algorithms comes from complex elliptic curves and complex multiplication. The resulting curves are obtained from the roots of the so-called *Hilbert class polynomial* modulo a prime. The two studied algorithms differ in the technique employed for constructing such polynomial.

This thesis is composed of seven chapters:

Chapter 1: The first chapter summarizes important concepts from group, ring and field theory together with some elemental aspects about polynomials. Its content is required for understanding the remaining parts of the thesis.

Chapter 2: This second chapter is about number fields. Algebraic extensions of the rational numbers appear in the study of complex multiplication on elliptic curves, which is the underlying theory over which the two algorithms implemented in this Master's thesis hold. Important concepts such as *discriminant*, *ideal ramification* and *Hilbert class field* are given.

Chapter 3: This chapter is an introduction to quadratic forms and the composition operation which permits them to be endowed with an Abelian group structure. A known isomorphism between the *form class group* and the *ideal class group* of the ring of integers of an imaginary quadratic field concludes the chapter.

Chapter 4: Here, several concepts about complex algebraic curves and algebraic geometry are introduced. The possibility to associate the *closed points* of the projective line or an algebraic curve with *valuation rings* is explained. Other important concepts included are: *divisor*, *function field of a curve*, *genus* and the *Riemann-Roch theorem*.

Chapter 5: This chapter presents the so-called *complex multiplication* theory. This theory, initially focused on elliptic curves defined over complex numbers also embraces elliptic curves defined over finite fields and is the core of the two algorithms implemented in this thesis. The most relevant content presented in this chapter includes: *lattice*, *homotheticity*, *j-invariant*, *elliptic curve*, *complex multiplication* and its relation with the cardinality of elliptic curves defined over a finite field.

Chapter 6: This chapter is devoted to the implementation (in Sage) of Atkin-Morain's and Agashe-Lauter-Venkatesan's algorithms for constructing elliptic curves with a given cardinality. Results regarding the time needed to construct such curves are included.

Chapter 7: The last part of the thesis includes a comparison of both methods and some concluding remarks.

The two analyzed algorithms (and some parts of the studied background) have been implemented in Sage [20]. Sage is an open source mathematics software that combines various software packages into a common interface. The author has chosen Sage because it provides the data types and related procedures required in this Master's thesis: arbitrary precision real and complex numbers, finite fields, polynomials, quadratic forms and elliptic curves (including cardinality computation).

Chapter 1

Elementary concepts

This chapter provides the elementary background required for understanding the remaining parts that compose this work. It has been divided into four sections where basic concepts about *groups*, *rings*, *polynomials* and *fields* are presented. The content of this chapter has been extracted mainly from [5], [8], [18] and [23].

1.1 Groups

A group is an algebraic structure consisting of a non-empty set and a binary internal operation that satisfies a certain set of conditions. As we will see in Chapter 5, the points of an elliptic curve can be endowed with such a structure. When the elliptic curve is defined over a finite field, its group structure has applications in cryptography.

Other groups that are relevant for this Master's thesis are: the automorphism group of a field extension (Section 1.4), the ideal class group (Section 2.2) and the form class group (Section 3.2).

Definition 1 (Group)
A *group* is a non empty set G endowed with a binary operation

$$G \times G \to G : (a, b) \mapsto ab$$

satisfying:

1. The operation is associative, $(ab)c = a(bc)$, for each $a, b, c \in G$.
2. There exists an *identity element* u such that $ua = a = au$, for each $a \in G$.
3. For each element $a \in G$, there exists $x \in G$ such that $ax = u = xa$. The element x is the *inverse* of a and it is denoted a^{-1}.

Definition 2 (Abelian group)
A group G is said to be *Abelian* if $ab = ba$ for each pair $a, b \in G$.

Example 1
The set of integers $\mathbb{Z}$ with the addition operation has an Abelian group structure.

Example 2
Excluding zero, the set of integers modulo a prime p, $\mathbb{Z}_p^* = \{1, \ldots, p-1\}$ with multiplication has an Abelian group structure.

Definition 3 (Group homomorphism)
A mapping $f : G \to G'$ between two groups G, G' is a *group homomorphism* if,

$$f(ab) = f(a)f(b), \quad \forall a, b \in G.$$

A group homomorphism $f : G \to G'$ further inducing a bijection between G and G' is said to be an *isomorphism*.

Example 3
Let $\mathbb{R}^+ = \{x \in \mathbb{R} : x > 0\}$. Given $g \in \mathbb{R}^+$, the map

$$f : \mathbb{R} \to \mathbb{R}^+ : x \mapsto f(x) = g^x$$

is an homomorphism between $\mathbb{R}$ with the addition operation and $\mathbb{R}^+$ with the product operation. This is easy to check since, given $a, b \in \mathbb{R}$,

$$f(a+b) = g^{a+b} = g^a g^b = f(a)f(b).$$

Further, if $g \neq 1$, f is an isomorphism because f induces a bijection between $\mathbb{R}$ and $\mathbb{R}^+$.

1.2 Rings

Rings are a fundamental algebraic structure in the study of complex multiplication on elliptic curves. For instance, the so called *endomorphism ring* of ordinary elliptic curves (see Chapter 5) is part of that theory.

Other rings that are relevant for this Master's thesis are: the ring of integers of a number field (Section 2.1) and the valuation rings associated to algebraic curves (Chapter 4).

Definition 4 (Ring)
A *ring* is a set A with an addition $(+)$ and a product $(\cdot)$ operations satisfying:

1. A is a commutative group under addition.

2. A is associative under multiplication. That is, given $x, y, z \in A$,

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z.$$

3. A is distributive over addition. That is, given $x, y, z \in A$,

$$(x + y) \cdot z = x \cdot z + y \cdot z \qquad \text{and} \qquad z \cdot (x + y) = z \cdot x + z \cdot y.$$

The identity element of addition is usually denoted 0_A or simply 0. A ring is said to be *unitary* if the product operation has an identity element in $A^* = A\backslash\{0\}$. This identity element is denoted 1_A or simply 1. A ring whose product operation is commutative ($x \cdot y = y \cdot x$, for each pair $x, y \in A$) is said to be a *commutative ring*.

From now on, the $\cdot$ symbol will be suppressed from those expressions where it is not strictly necessary. For instance, we will write xy instead of $x \cdot y$.

Example 4
The set of integers $\mathbb{Z}$ with the usual addition and product operations is a ring.

Example 5
The set of integers modulo an integer n, $\mathbb{Z}_n$, is a ring.

Definition 5 (Unity)
Given a ring A, $x \in A$ is a *unity* if there exists some $y \in A$ satisfying,

$$xy = yx = 1.$$

The element y is called the *inverse* of x and it is denoted x^{-1}. The set of unities of A is denoted $U(A)$.

Example 6
In the ring $\mathbb{Z}_{15}$, the element 2 is a unity and $2^{-1} = 8$. This is so because,

$$2 \cdot 8 \equiv 1 \pmod{15}.$$

It is easy to see that the unities in $\mathbb{Z}_{15}$ are precisely those $x \in \mathbb{Z}_{15}$ satisfying $\gcd(x, 15) = 1$, hence,

$$U(\mathbb{Z}_{15}) = \{x \in \mathbb{Z}_{15} \ : \ \gcd(x, 15) = 1\}.$$

Definition 6 (Field)
A ring A whose elements in A^* are all invertible is called a *field*.

More details about fields are given in Section 1.4.

Example 7
If p is prime, all the elements in $\mathbb{Z}_p^* = \{1, \ldots, p-1\}$ are invertible. Let us take an integer $x \in \mathbb{Z}_p^*$. Since p is prime and $1 \leq x < p$, then $\gcd(x, p) = 1$. From Bezout's identity, there exist two integers $a, b \in \mathbb{Z}$ satisfying,

$$1 = ax + bp.$$

Hence,

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

and $a \pmod{p}$ is the inverse of x in $\mathbb{Z}_p$. Hence, $U(\mathbb{Z}_p) = \mathbb{Z}_p^*$ and $\mathbb{Z}_p$ is a field provided that p is prime.

Definition 7 (Divisor of zero)
Given a ring A, $x \in A^*$ is a *divisor of zero* if there exists some $y \in A^*$ satisfying,

$$xy = 0.$$

Definition 8 (Integral domain)
An *integral domain* (or simply a *domain*) is a commutative ring without divisors of zero.

Example 8
The ring $\mathbb{Z}_{15}$ is not an integral domain. We can easily check 3 is a divisor of zero because

$$3 \cdot 5 \equiv 0 \pmod{15}.$$

Example 9
If p is prime, $\mathbb{Z}_p$ is an integral domain. Let us take an integer $x \in \mathbb{Z}_p^* = \{1, \ldots, p-1\}$. If x were a divisor of zero, there would exist $y \in \mathbb{Z}_p^*$ satisfying,

$$xy \equiv 0 \pmod{p},$$

in which case,

$$xy = kp, \qquad k \in \mathbb{Z}.$$

Since neither x nor y are zero, $k \neq 0$. Then, x or y must be divisible by p which is not possible because both $x, y < p$.

Definition 9 (Ideal)
Let A be a commutative and unitary ring. An *ideal* is a subset $\mathfrak{a} \subset A$ satisfying:

1. $\mathfrak{a}$ is a subgroup of A under addition.
2. Given $x \in \mathfrak{a}$ and $a \in A$, the product $xa \in \mathfrak{a}$.

Being $\mathfrak{a}$ a subgroup under addition requires $0 \in \mathfrak{a}$. The subset $\{0\}$ is an ideal referred to as the *trivial ideal*. When $\mathfrak{a} \neq A$, $\mathfrak{a}$ is said to be a *proper ideal*. An ideal $\mathfrak{a}$ is proper if and only if $1 \notin \mathfrak{a}$.

Example 10
A field K does not have proper ideals. Let $\mathfrak{a} \neq \{0\}$ be an ideal of K, and let $x \neq 1 \in \mathfrak{a}$. Since all the elements of K are invertible, then $x^{-1} \in K$ and from the definition of ideal $1 = xx^{-1} \in \mathfrak{a}$ so that $\mathfrak{a} = K$. Hence the only ideals of a field K are the trivial one and K itself.

Definition 10 (Ideal generated from a set)
Let A be a commutative and unitary ring, and let L be a subset of A. We define the *ideal generated by* L as the minimal ideal of A containing all the elements of L.

If $L = \{x_1, \ldots, x_r\}$ is a finite set, we say that the ideal $\mathfrak{a}$ generated by L is *finitely generated* and we denote it (following [23]) as $\mathfrak{a} = \langle x_1, \ldots, x_r \rangle$. In this case,

$$\mathfrak{a} = \left\{ \sum_{k=1}^{r} a_k x_k : a_1, \ldots, a_r \in A \right\}.$$

An ideal $\mathfrak{a}$ that can be generated by one element, $\mathfrak{a} = \langle x_1 \rangle$ is said to be *principal* and,

$$\mathfrak{a} = \{ax_1 : a \in A\} = Ax_1.$$

A ring whose ideals are all principal is called a *principal ideal domain* (PID).

Example 11
In the ring of integers $\mathbb{Z}$, let $\mathfrak{a} = \langle 3, 5 \rangle$. Note that $(-3) \cdot 3 + 2 \cdot 5 = 1 \in \mathfrak{a}$. From the definition of ideal, if $1 \in \mathfrak{a}$, then for each $a \in \mathbb{Z}$, $1 \cdot a \in \mathfrak{a}$, hence $\mathfrak{a} = \mathbb{Z}$. The ideal $\mathfrak{a}$ can be expressed as $\mathfrak{a} = \langle 1 \rangle$ so that it is principal. The integers is a principal ideal domain since it can be proven that

$$\langle x_1, \ldots, x_r \rangle = \langle \gcd(x_1, \ldots, x_r) \rangle .$$

Definition 11 (Addition and product of ideals)
Let A be a commutative and unitary ring, and let $\mathfrak{a}, \mathfrak{b} \subseteq A$ be two ideals:

- $\mathfrak{a} + \mathfrak{b}$ is the ideal whose elements are of the form $x + y$, with $x \in \mathfrak{a}$ and $y \in \mathfrak{b}$.
- $\mathfrak{a} \cdot \mathfrak{b}$ is the ideal whose elements are of the form $x_1 y_1 + \ldots + x_r y_r$, with $x_1, \ldots, x_r \in \mathfrak{a}$ and $y_1, \ldots, y_r \in \mathfrak{b}$, being $r \geq 1$.

Remark 1
We have just seen that ideals can be multiplied. Hence, we can ask ourselves about the reverse operation, *i.e.* factorization. As we will see in Section 2.2, this question will lead us to the definition of a key concept for this Master's thesis: the *Hilbert class field*.

Definition 12 (Maximal ideal)
Let A be a commutative and unitary ring, and let $\mathfrak{a} \subseteq A$ be an ideal. The ideal $\mathfrak{a}$ is said to be *maximal* if the following two equivalent conditions are satisfied,

1. The quotient $A/\mathfrak{a}$ is a field.

2. $\mathfrak{a}$ is a proper ideal and no other proper ideal strictly contains it.

Definition 13 (Prime ideal)
Let A be a commutative and unitary ring, and let $\mathfrak{a} \subseteq A$ be an ideal. The ideal $\mathfrak{a}$ is said to be *prime* if the following two equivalent conditions are satisfied,

1. The quotient $A/\mathfrak{a}$ is an integral domain.

2. $\mathfrak{a}$ is a proper ideal and given $x, y \in A$, if $xy \in \mathfrak{a}$ then $x \in \mathfrak{a}$ or $y \in \mathfrak{a}$.

Lemma 1. *A maximal ideal is always prime.*

The reverse of the previous lemma is not true in general.

Example 12
In $\mathbb{Z}$, the ideal $\mathfrak{a} = \langle 7 \rangle = 7 \cdot \mathbb{Z}$ is maximal. This is because, $\mathbb{Z}/\mathfrak{a} = \mathbb{Z}/7\mathbb{Z} \approx \mathbb{Z}_7$ is a field. From the previous lemma, I is also prime.

Example 13
In $\mathbb{Z}$, the ideal $\mathfrak{a} = \langle 6 \rangle$ is not prime because $2, 3 \notin \mathfrak{a}$ but $2 \cdot 3 = 6 \in \mathfrak{a}$.

Definition 14 (Local ring)
A ring is said to be a *local ring* if it has a unique maximal ideal.

Example 14
The set of integers $\mathbb{Z}$ is not a local ring since it has several maximal ideals such as $\langle 2 \rangle$ or $\langle 3 \rangle$, for instance.

Example 15
Let d be a prime integer and let $c \in \mathbb{Q}$. The rational number c can be expressed in the form

$$c = d^k \frac{m}{n},$$

where k, m, n are integers with $n > 0$ and $d \nmid m$, $d \nmid n$. Here we can define the mapping

$$v : \mathbb{Q}\backslash\{0\} \to \mathbb{Z} : c \mapsto k.$$

The set $R = \{c \in \mathbb{Q}\backslash\{0\} \ : \ v(c) \geq 0\} \cup \{0\}$ is a (discrete valuation) ring having a unique maximal ideal given by $\mathfrak{m} = \{c \in \mathbb{Q}\backslash\{0\} \ : \ v(c) > 0\} \cup \{0\}$. Hence, R is a local ring. More details are given in Definition 17.

Definition 15 (Noetherian ring)
A domain D is *Noetherian* if every ideal in D is finitely generated.

Example 16
A principal ideal domain, like $\mathbb{Z}$, is always a Noetherian ring.

Proposition 1. *The following conditions are equivalent for an integral domain D:*

1. *D is Noetherian.*
2. *D satisfies the* ascending path condition*. That is, given an ascending chaing of ideals:*
$$\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \ldots \subseteq \mathfrak{a}_n \subseteq \ldots$$
there exists some N for which $\mathfrak{a}_n = \mathfrak{a}_N$ for all $n \geq N$.
3. *D satisfies the* maximal condition*: every non-empty set of ideals has a maximal element (an element which is not properly contained in every other element).*

Definition 16 (Artinian ring)
A domain D is *Artinian* if for every chain of ideals:

$$\mathfrak{a}_0 \supseteq \mathfrak{a}_1 \supseteq \ldots \supseteq \mathfrak{a}_n \supseteq \ldots$$

there exists some N for which $\mathfrak{a}_n = \mathfrak{a}_N$ for all $n \geq N$.

Example 17
The integers $\mathbb{Z}$ are not an Artinian ring. We can consider the chain of ideals

$$\langle 2 \rangle \supseteq \left\langle 2^2 \right\rangle \supseteq \left\langle 2^3 \right\rangle \supseteq \ldots \supseteq \langle 2^n \rangle \supseteq \ldots.$$

This chain has an infinite amount of different ideals.

Definition 17 (Discrete valuation)
A *discrete valuation* of a field K is a mapping $v : K^* \to \mathbb{Z}$ such that for all $x, y \in K^*$, we have,

1. $v(xy) = v(x) + v(y)$,
2. $v(x + y) \geq \min(v(x), v(y))$.

The set consisting of 0 and all $x \in K^*$ such that $v(x) \geq 0$ is the *discrete valuation ring* associated to v. A valuation ring is a local ring whose unique maximal ideal is composed of 0 together with all $x \in K^*$ such that $v(x) > 0$. As we will see in Chapter 4, valuation rings are used in the study of algebraic curves.

Example 18
The mapping $v : \mathbb{Q}\backslash\{0\} \to \mathbb{Z}$ in Example 15 is a discrete valuation of $\mathbb{Q}$.

Example 19
Let $a \in \mathbb{F}_{q^m}$, $m \geq 1$ and let $f = \frac{p(X)}{q(X)}$ be a rational function in $\mathbb{F}_q(X)$. We can represent f as

$$f = \frac{r(X)}{s(X)}(X-a)^e$$

so that $r, s, (X-a)$ are coprime polynomials in $\mathbb{F}_{q^m}[X]$. Here we can define the valuation $v_a(f) = e$. In this particular example, the valuation ring (also called a *place*) of v_a is the set

$$R = \left\{ f = \frac{p(X)}{q(X)} \in \mathbb{F}_{q^m}(X) \quad : q(a) \neq 0 \right\},$$

and the maximal ideal of R is

$$\mathfrak{m} = \left\{ f = \frac{p(X)}{q(X)} \in \mathbb{F}_{q^m}(X) \quad : \quad q(a) \neq 0, \quad p(a) = 0 \right\}.$$

Definition 18 (Ring homomorphism)
A *ring homomorphism* between two rings A,B is a function $f : A \to B$ satisfying,

1. $f(x+y) = f(x) + f(y), \quad x, y \in A,$
2. $f(xy) = f(x)f(y), \quad x, y \in A,$
3. $f(1_A) = 1_B.$

The *kernel* of a ring homomorphism $f : A \to B$ is the ideal defined as

$$\ker f = \{x \in A : \ f(x) = 0\}.$$

Definition 19 (Ring homomorphism types)
Let $f : A \to B$ be a ring homomorphism. We say that:

1. f is an *epimorphism*, if it is exhaustive,
2. f is a *monomorphism*, if it is injective,
3. f is an *isomorphism*, if there exists an homomorphism $g : B \to A$ so that

$$g \circ f = Id_A \qquad \text{and} \qquad f \circ g = Id_B.$$

Definition 20 (Module)
Let R be a ring. An R-module is an additive Abelian group M, together with an operation $R \times M \to M$ such that for all $r, s \in R$ and $x, y \in M$, we have:

1. $r(x + y) = rx + ry$,
2. $(r + s)x = rx + sx$,
3. $(rs)x = r(sx)$,
4. $1_R \cdot x = x$.

Example 20
The Gauss integers $\mathbb{Z}[i] = \{m+n\sqrt{-1} \ : \ m, n \in \mathbb{Z}\}$ with the addition operation have a $\mathbb{Z}$-module structure.

1.3 Polynomials

The algorithms implemented in this Master's thesis ([1] and [2]) permit to obtain an elliptic curve defined over a finite field with a given amount of points (elliptic curves are explained in Chapters 4 and 5). As we will see in Chapter 6, the elliptic curves with the required cardinality are obtained after computing the roots of a certain polynomial. Some basic definitions about polynomials are next given in this section. A wider introduction to polynomials can be found in [8].

Definition 21 (Polynomial)
A *polynomial* in n variables $X_1, \ldots, X_n$ and coefficients in a commutative and unitary ring A is an expression of the form:

$$f = \sum_{v=(v_1,\ldots,v_n)} a_v X_1^{v_1} \cdots X_n^{v_n},$$

where the coefficients $a_v \in A$ are all zero except for a finite amount.

Example 21
The expression $f = X^3Y^2 - 4X^2 + 3Y$ is a polynomial in two variables X, Y and coefficients in $\mathbb{Z}$.

Remark 2
Given a bivariate polynomial like the one in the previous example, the set of points (x, y) satisfying $f(x, y) = 0$ compose a *plane affine algebraic curve*. More details are given in Chapter 4.

Definition 22 (Degree of a polynomial)
The *degree* of a polynomial $f = \sum_{v=(v_1,\ldots,v_n)} a_v X_1^{v_1} \cdots X_n^{v_n}$ is defined as

$$\deg f = \max\{d \ : \ \exists\, a_v \neq 0, \text{ with } v_1 + \ldots + v_n = d\}.$$

Example 22
The degree of $f = X^3Y^2 - 4X^2 + 3Y$ is $\deg f = 5$.

Definition 23 (Homogeneous polynomial)
A nonzero polynomial $P(X_1, \ldots, X_n)$ in n variables is *homogeneous* of degree d if

$$P(\lambda X_1, \ldots, \lambda X_n) = \lambda^d P(X_1, \ldots, X_n).$$

for all λ.

Polynomials can be added and multiplied forming a ring.

Definition 24 (Polynomial addition and product)
Given two polynomials $f = \sum_v a_v X_1^{v_1} \cdots X_n^{v_n}$ and $g = \sum_v b_v X_1^{v_1} \cdots X_n^{v_n}$, their *addition* is given by

$$f + g = \sum_v (a_v + b_v) X_1^{v_1} \cdots X_n^{v_n},$$

and their *product* is

$$f \cdot g = \sum_v \left(\sum_{\lambda+\mu=v} a_\lambda b_\mu \right) X_1^{v_1} \cdots X_n^{v_n}.$$

Example 23
Let $f = X^3 + XY$ and $g = X^2 + Y$, then,

$$f + g = X^3 + X^2 + XY + Y,$$

and

$$f \cdot g = X^5 + 2X^3Y + XY^2.$$

Definition 25 (Polynomial ring)
Given a commutative and unitary ring A, the set of polynomials in n variables $X_1, \ldots, X_n$ and coefficients in A endowed with the addition and product operations is a commutative and unitary ring denoted as $A[X_1, \ldots, X_n]$.

Proposition 2. *The polynomial ring $A[X_1, \ldots, X_n]$ is an integral domain if and only if A is an integral domain.*

Since $A[X_1, \ldots, X_n]$ is a ring, some of its elements are invertible (unities). If A is an integral domain, it turns out that $U(A[X_1, \ldots, X_n]) = U(A)$.

Definition 26 (Irreducible polynomial)
A polynomial $f \in A[X_1, \ldots, X_n]$ is *irreducible* when it can not be expressed as a product of two (non-unity) polynomials $g, h \in A[X_1, \ldots, X_n]$.

Example 24
The polynomial $f = X^2 - Y^2$ is reducible because,

$$X^2 - Y^2 = (X + Y)(X - Y).$$

Example 25
The polynomial $f = X^5 + 5X^4 + 10X^3 + 20X + 10$ is irreducible in $\mathbb{Q}[X]$. This can be easily proven through Eisenstein's criterion [8, p.144].

Definition 27 (Polynomial evaluation)
Let A be a unitary and commutative ring and let $X_1, \ldots, X_n$ be n variables. Given a ring B having A as a subring and considering n elements $x_1, \ldots, x_n \in B$, we define the *evaluation* in $x_1, \ldots, x_n$ as the mapping $A[X_1, \ldots, X_n] \to B$ given by

$$f = \sum_v a_v X_1^{v_1} \ldots X_n^{v_n} \mapsto f(x_1, \ldots, x_n) = \sum_v a_v x_1^{v_1} \ldots x_n^{v_n}.$$

Definition 28 (Polynomial root)
A root of a polynomial $f \in A[X]$ is a number x satisfying $f(x) = 0$.

Example 26
Number 1 is a root of $f = X^3 - X^2 + X - 1$ defined in $\mathbb{Z}[X]$.

Example 27
The polynomial $f = X^2 + 2$ is irreducible in $\mathbb{Z}_5$. If it were reducible, it could be expressed as a product

$$f = (X - a)(X - b), \quad a, b \in \mathbb{Z}_5,$$

so that a would be a root of f. We can see f has no roots in $\mathbb{Z}_5$ by evaluating it in each element of $\mathbb{Z}_5$ and checking the result is not 0 in any case.

1.4 Fields

Fields are the basic algebraic structure over which algebraic curves (Chapter 4) are constructed. In this Master's thesis, we have focused on a particular type of algebraic curves, namely elliptic curves. The theory of number fields (Chapter 2), including the Hilbert class field, is fundamental for the study of complex multiplication on elliptic curves. This section provides a basic introduction to fields.

Definition 29 (Field)
A ring K is said to be a *field* when $K^* = K \backslash \{0\}$ is a group under the product operation.

The previous definition is equivalent to saying that a field is a unitary ring K such that $U(K) = K^*$. That is, all its non-zero elements are invertible (unities).

Fields whose product operation is commutative are said to be *commutative*.

Definition 30 (Finite field)
A field is said to be *finite* when its cardinality (or order) is finite.

Definition 31 (Field characteristic)
Given a field K, we consider the mapping:

$$\phi : \mathbb{Z}^+ \to K : n \mapsto \underbrace{1_K + \ldots + 1_K}_{n \text{ times}}.$$

If the previous mapping is injective, we say K has *characteristic* 0. Otherwise, let p be the smallest positive integer, other than 0, such that $\phi(p) = 0$. Then we say K has *characteristic* p.

The characteristic of a field K is either zero or a prime number. Note that the characteristic of a finite field can not be zero.

Example 28
The characteristic of $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ is 0.

Example 29
The characteristic of $\mathbb{Z}_p$, p prime, is p.

Definition 32 (Prime subfield)
Given a finite field K, the kernel of ϕ is an ideal $\langle p \rangle$ of $\mathbb{Z}$, being p a prime number. Hence, K has a subfield that is isomorphic to $\mathbb{Z}/\langle p \rangle \approx \mathbb{Z}_p$. This is the *prime subfield* of K.

In Section 1.2 a definition of ring homomorphism has been given together with an statement about its kernel being an ideal. Since a field does not have proper ideals, a homomorphism $f : K_1 \to K_2$ between two fields can only be the zero-map (when $\ker f = K_1$) or a monomorphism (when $\ker f = \{0\}$).

Definition 33 (Field extension)
Let K, E be fields. It is said that E is an *extension* of K, represented by E/K, when there exists a field monomorphism $j : K \to E$.

In such a case, K is isomorphic to $j(K)$ so that K can be identified with $j(K)$, a subfield of E.

Example 30
The complex numbers $\mathbb{C}$ are an extension of $\mathbb{R}$. In this case, a field monomorphism $j : \mathbb{R} \to \mathbb{C}$ is given by

$$j : \mathbb{R} \to \mathbb{C} : x \mapsto x.$$

Remark 3
Sometimes a *field monomorphism* is called an *embedding*. In the previous example, the real numbers $\mathbb{R}$ are embedded in $\mathbb{C}$ by j.

Definition 34 (Homomorphism)
A *homomorphism* from an extension E_1/K over E_2/K is a field homomorphism $\phi : E_1 \to E_2$ such that, when restricted to K, ϕ is an identity mapping from K to K.

When the previous homomorphism provides a bijection between E_1 and E_2 it is said to be an *isomorphism*. Moreover, if $E_1 = E_2$ we refer to it as an *automorphism*. The set of automorphisms of a field extension E/K, under the composition operation, has a group structure. This group is denoted by $G(E : K)$.

Example 31
If we consider the extension $\mathbb{C}/\mathbb{R}$, the conjugation mapping $z = x + iy$ to $\overline{z} = x - iy$ is an automorphism $\mathbb{C}/\mathbb{R} \to \mathbb{C}/\mathbb{R}$. The conjugation and the identity mappings compose the automorphism group $G(\mathbb{C} : \mathbb{R})$ which is isomorphic to $\mathbb{Z}_2$.

Proposition 3. *Let E/K be a field extension. Then E has a vector space structure over K.*

Example 32
Let us consider the extension $\mathbb{C}/\mathbb{R}$. It is known that a complex number $z \in \mathbb{C}$ is of the form $z = x + iy$, with $x, y \in \mathbb{R}$. Hence complex numbers have a vector space structure over $\mathbb{R}$ of dimension two and basis $\{1, i\}$.

Definition 35 (Degree of a field extension)
Let E/K be a field extension. The *degree*, denoted $[E : K]$, of such an extension is defined to be $\dim_K E$, when E is considered a vector space over K.

Let K be a finite field and let F be its prime subfield. Then K/F is a field extension and K has a vector space structure over F. Let p be the cardinality of F and $m = [K : F]$. Then the cardinality of K is p^m. Hence, any finite field has a prime-power cardinality. Moreover, any two finite fields with the same number of elements are know to be isomorphic. Let p be a prime and $m \geq 1$, the *unique* finite field having cardinality p^m is usually denoted $\mathbb{F}_{p^m}$.

Example 33
The extension $\mathbb{C}/\mathbb{R}$ has degree 2.

Example 34
Let us consider the polynomial $f = X^{p^2} - X$ defined over $\mathbb{Z}_p$. All the elements $\alpha \in \mathbb{F}_{p^2}$ satisfy that $x^{p^2} = x$, hence, each of the p^2 elements in $\mathbb{F}_{p^2}$ is a root of f. In this way, f can be expressed as

$$f = \prod_{\alpha \in \mathbb{F}_{p^2}} (X - \alpha),$$

and $\mathbb{F}_{p^2}$ is the *splitting field* of f. Generalizing this idea, any finite field $\mathbb{F}_{p^m}$ can be defined as the splitting field of polynomial $X^{p^m} - X$ defined over $\mathbb{Z}_p$.

Definition 36 (Finite extension)
A field extension whose degree is finite is said to be a *finite extension*.

Example 35
The extension $\mathbb{C}/\mathbb{R}$ is finite.

Definition 37 (Subextension)
Let E/K be a field extension. Then, L/K is a *subextension* of E/K if E is an extension of L.

A subextension of E/K is said to be *proper* if it is different from E/K and K/K.

Definition 38 (Subextension generated from a subset)
Let E/K be a field extension, and let $A = \{a_i \ : \ i \in I\} \subset E$ be non-empty. The *field generated* by A over K, denoted $K(A)$ is the smallest subfield of E containing both K and A. In this case we say that L is generated by A over K.

Definition 39 (Finitely generated extension)
A field extension L/K is *finitely generated* when L is generated over K by a finite set.

Definition 40 (Simple extension)
A field extension L/K is *simple* when L is generated over K by a set containing one element.

Example 36
Let us consider $\mathbb{R}/\mathbb{Q}$. We can take $A = \{\sqrt[3]{7}\} \subset \mathbb{R}$. Then $\mathbb{Q}(\sqrt[3]{7})/\mathbb{Q}$ is a simple field extension.

Let E/K be a simple field extension, that is, $E = K(\alpha)$ for some $\alpha \in E$. Let us consider the following homomorphism:

$$K[X] \to E \ : \ f \mapsto f(\alpha),$$

and let I be its kernel. We say that α is:

1. *Transcendental:* if $I = \{0\}$, that is, α is not root of any polynomial with coefficients in K.
2. *Algebraic:* if $f(\alpha) = 0$ for some non-null polynomial in $K[X]$.

When α is algebraic, by evaluating $X = \alpha$ we get an epimorphism

$$K[X] \to E,$$

whose kernel is generated by an irreducible polynomial f. By taking f to be monic, we get the following important definition.

Definition 41 (Minimum polynomial)
Let α be an algebraic element over a field K. We define the *minimum polynomial of α over K* as the unique monic irreducible polynomial in $K[X]$ having α as a root. Such a polynomial is denoted $P(\alpha, K)$.

Given a field extension E/K with $E = K(\alpha)$, the degree of $P(\alpha, K)$ coincides with the extension degree $[E : K]$. That is,

$$\deg P(\alpha, K) = [E : K].$$

Moreover, if $\deg P(\alpha, K) = n$ then $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis of E over K.

Example 37
The minimum polynomial $P(\sqrt[3]{7}, \mathbb{Q})$ is $X^3 - 7$. The elements of $\mathbb{Q}(\sqrt[3]{7})$ are of the form,

$$q_1 + q_2 \sqrt[3]{7} + q_3 (\sqrt[3]{7})^2, \quad q_1, q_2, q_3 \in \mathbb{Q}.$$

Example 38
A *cyclotomic field* is of the form $\mathbb{Q}(\zeta)$, with $\zeta = e^{2\pi i/m}$ (ζ is a primitive complex m-th root of unity). When m is an odd prime, the minimum polynomial of ζ over $\mathbb{Q}$ is

$$P(\zeta, \mathbb{Q}) = \frac{X^m - 1}{X - 1} = X^{m-1} + X^{m-2} + \ldots + X + 1.$$

Hence, $\mathbb{Q}(\zeta)/\mathbb{Q}$ is a degree $m - 1$ extension.

Example 39
We know from a previous example that $f = X^2 + 2$ is an irreducible polynomial

in $\mathbb{Z}_5$. Let α be a root of f (in some extension of $\mathbb{Z}_5$). Then $\mathbb{Z}_5(\alpha)/\mathbb{Z}_5$ is a degree 2 field extension. The field $\mathbb{Z}_5(\alpha)$ can be considered a dimension 2 vector space over $\mathbb{Z}_5$ so that its cardinality is 5^2. Hence, $\mathbb{Z}_5(\alpha)$ is isomorphic to $\mathbb{F}_{5^2}$. Its elements are of the form

$$m + n\alpha : \quad m, n \in \mathbb{Z}_5.$$

Theorem 1. *If E/K is a finite extension of fields of characteristic 0, then it is simple algebraic. That is, $E = L(\alpha)$ for some $\alpha \in E$. Such an element α is said to be a* primitive element *of the extension.*

Given a finite extension E/K, when it is simple, we have $E = K(\alpha)$ and there exists the minimum polynomial $P(\alpha, K)$. We know α is a root of $P(\alpha, K)$, but the minimum polynomial may have other roots in E. The amount of roots of $P(\alpha, K)$ is $[E : K]$ at most (the degree of $P(\alpha, K)$).

Let $\{\alpha, \alpha_2, \ldots, \alpha_r\} \subset E$ be the roots of $P(\alpha, K)$ in E. An automorphism $\phi : E/K \to E/K$ is determined by the value where α is mapped to by ϕ. Hence, the cardinality of the automorphism group $G(E : K)$ corresponds to the amount of different roots of $P(\alpha, K)$ in E.

Example 40
Let us consider $\mathbb{Q}(\sqrt[3]{7})/\mathbb{Q}$. The minimum polynomial of $\sqrt[3]{7}$ over $\mathbb{Q}$ is

$$P(\sqrt[3]{7}, \mathbb{Q}) = X^3 - 7.$$

This polynomial has only one root over $\mathbb{Q}(\sqrt[3]{7})$, namely $\sqrt[3]{7}$, but its has two other roots in $\mathbb{C}$. They are $\omega\sqrt[3]{7}$ and $\omega^2\sqrt[3]{7}$, being $\omega = e^{i\frac{2\pi}{3}}$, both of them falling outside $\mathbb{Q}(\sqrt[3]{7})$. Hence

$$G(\mathbb{Q}(\sqrt[3]{7}) : \mathbb{Q}) = \{Id\}.$$

Definition 42 (Galois extension)
A finite extension E/K is called a *Galois extension* when the cardinality of $G(E : K)$ is $[E : K]$.

Example 41
The extension $\mathbb{Q}(\sqrt[3]{7})/\mathbb{Q}$ is not a Galois extension.

Example 42
An extension of the form $\mathbb{Q}(\zeta)/\mathbb{Q}$, with $\zeta = e^{2\pi i/m}$, m an odd prime, is a Galois extension. The roots of its minimum polynomial

$$X^{m-1} + X^{m-2} + \ldots + X + 1$$

are ζ^k, for $k = 1, \ldots, (m-1)$, each of them falling in $\mathbb{Q}(\zeta)$.

Definition 43 (Abelian extension)
A Galois extension E/K whose automorphism group is Abelian is called an *Abelian extension.*

Example 43
The extension $\mathbb{Q}(e^{2\pi i/5})/\mathbb{Q}$ is a Galois extension. Moreover, its automorphism group has cardinality four, so that it is Abelian (see [5, Ex.2]). Hence, the extension is Abelian.

Definition 44 (Separable extension)
An algebraic extension E/K is *separable* when for every $\alpha \in E$, the minimum polynomial $P(\alpha, E)$ is separable (its roots are distinct).

We finish this chapter providing some examples of sets having a field structure.

Example 44
Let us consider an irreducible polynomial $f \in \mathbb{Q}[X]$ with $\deg f \geq 1$. Since f is irreducible, it has no roots in $\mathbb{Q}$ but it has at least one root $\alpha \in \mathbb{C}$. In this way, $\mathbb{Q}(\alpha)/\mathbb{Q}$ is a field extension of degree $\deg f$. The field $\mathbb{Q}(\alpha)$ is called a *number field*. More details about number fields are given in Chapter 2.

Example 45
An algebraic number is a number that is a root of a non-zero polynomial in one variable with rational coefficients. The set of algebraic numbers endowed with the usual addition and product operations has a field structure. This field is usually denoted $\overline{\mathbb{Q}}$. The field $\overline{\mathbb{Q}}$ is known to be the algebraic closure of $\mathbb{Q}$.

Example 46
Let $f \in \mathbb{C}[X, Y]$ be an irreducible polynomial, and consider the curve

$$C : f(x, y) = 0.$$

Any complex rational function

$$R(x, y) = P(x, y)/Q(x, y),$$

where P and Q are polynomials, is declared to be zero whenever P but not Q is divisible by f. We place in one class all the rational functions which differ by zero from a given one. This collection of equivalence classes is a field, which is an extension of the field of complex numbers. This is the *function field* of the curve C. More details will be given in Chapter 4.

Chapter 2

Number fields

Algebraic extensions of $\mathbb{Q}$ are fundamental in the study of complex multiplication on elliptic curves. This chapter provides a brief introduction to those aspects of number fields that are the required background for Chapter 5. For a complete account of number fields the reader is referred to [6] and [23].

2.1 Algebraic numbers

Definition 45 (Algebraic number)
A complex number is *algebraic* if it is the root of a non-zero polynomial with coefficients in $\mathbb{Q}$.

Example 47
Any number $\alpha \in \mathbb{Q}$ is algebraic because it is the root of the linear polynomial $X - \alpha$.

Example 48
Numbers $\sqrt{\frac{3}{2}}$, $\sqrt[4]{-5}$ are algebraic because they are a root of $X^2 - \frac{3}{2}$ and $X^4 + 5$, respectively.

The set $\overline{\mathbb{Q}}$ of algebraic numbers is a subfield of $\mathbb{C}$. Next we focus our attention on a particular type of subfields of $\overline{\mathbb{Q}}$.

Definition 46 (Number field)
A *number field* is a subfield K of $\mathbb{C}$ such that $[K : \mathbb{Q}]$ is finite.

Example 49
The set of algebraic numbers $\overline{\mathbb{Q}}$ is not a number field, since $[\overline{\mathbb{Q}} : \mathbb{Q}]$ is not finite.

From its definition, the elements of a number field are all algebraic so that

$K \subseteq \overline{\mathbb{Q}}$. A number field K is a finite extension of the rational numbers $\mathbb{Q}$, hence $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ for some finite set of algebraic numbers $\alpha_1, \ldots, \alpha_n$. Since $\mathbb{Q}$ has characteristic 0, Theorem 1 states that any number field K is a primitive extension of $\mathbb{Q}$. Hence, $K = \mathbb{Q}(\theta)$ for some algebraic number θ.

Next, we recall the concept of *monomorphism* (see Definition 19) and apply it to number fields. The following theorem (see [23]) is fundamental for defining the concept of *conjugates*, which are in turn the basis for a very important concept in number field theory: the *discriminant*.

Theorem 2. *Let $K = \mathbb{Q}(\theta)$ be a number field of degree n over $\mathbb{Q}$. Then there are exactly n distinct monomorphisms $\sigma_i : K \to \mathbb{C}$ $(i = 1, \ldots, n)$. The elements $\sigma_i(\theta) = \theta_i$ are the distinct zeros in $\mathbb{C}$ of the minimum polynomial of θ over $\mathbb{Q}$.*

Definition 47 (Conjugates)
Given a number field K, $[K : \mathbb{Q}] = n$, and $\alpha \in K$, the elements $\sigma_i(\alpha)$ for $i = 1, \ldots, n$ are called the K-*conjugates* of α.

Example 50
Let $K = \mathbb{Q}(\sqrt[3]{7})$ (see Example 40). The minimum polynomial of $\sqrt[3]{7}$ over $\mathbb{Q}$ is $X^3 - 7$. The roots over $\mathbb{C}$ of this polynomial are $\{\sqrt[3]{7}, \omega\sqrt[3]{7}, \omega^2\sqrt[3]{7}\}$, with $\omega = e^{\frac{2\pi i}{3}}$.

Hence, the K-conjugates of $3 + 2\sqrt[3]{7}$ are:

$$\sigma_1(3 + 2\sqrt[3]{7}) = 3 + 2\sqrt[3]{7}$$

$$\sigma_2(3 + 2\sqrt[3]{7}) = 3 + 2\omega\sqrt[3]{7}$$

$$\sigma_3(3 + 2\sqrt[3]{7}) = 3 + 2\omega^2\sqrt[3]{7}$$

This example shows that the K-conjugates of $\alpha \in K$ may not lie in K.

Definition 48 (Discriminant of a basis)
Let $K = \mathbb{Q}(\theta)$ be a degree n number field, and let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis of K as a vector space over $\mathbb{Q}$. We define the *discriminant* of this basis to be

$$\Delta[\alpha_1, \ldots, \alpha_n] = \{\det[\sigma_i(\alpha_j)]\}^2.$$

Example 51
Let $K = \mathbb{Q}(\sqrt[3]{7})$. We can take $\{1, \sqrt[3]{7}, (\sqrt[3]{7})^2\}$ as a basis of K over $\mathbb{Q}$. Let us compute the discriminant of this basis:

$$\begin{vmatrix} 1 & \sqrt[3]{7} & (\sqrt[3]{7})^2 \\ 1 & \omega\sqrt[3]{7} & \omega^2(\sqrt[3]{7})^2 \\ 1 & \omega^2\sqrt[3]{7} & \omega(\sqrt[3]{7})^2 \end{vmatrix}^2 = \big(7(3\omega^2 - 3\omega)\big)^2 = 7^2 \cdot 3^2 \cdot (\omega^2 - \omega)^2 = 7^2 \cdot 3^2 \cdot (-3) = -1323.$$

Example 52
Let $K = \mathbb{Q}(\sqrt{-15})$. The pair $\{1, \sqrt{-15}\}$ is a basis of K over $\mathbb{Q}$ so that we can compute its discriminant which is

$$\begin{vmatrix} 1 & \sqrt{-15} \\ 1 & -\sqrt{-15} \end{vmatrix}^2 = \left(-2\sqrt{-15}\right)^2 = -60.$$

Another basis of K over $\mathbb{Q}$ is given by $\{1, \frac{1+\sqrt{-15}}{2}\}$. The dicriminant of this basis is

$$\begin{vmatrix} 1 & \frac{1+\sqrt{-15}}{2} \\ 1 & \frac{1-\sqrt{-15}}{2} \end{vmatrix}^2 = \left(-\sqrt{-15}\right)^2 = -15.$$

This example shows that the discriminants of different basis of the same field extension do not necessarily agree. As we will see later, this is not the case for *integral basis*.

Definition 49 (Algebraic integer)
A complex number θ is an *algebraic integer* if there is a monic polynomial $p(T)$ with integer coefficients such that $p(\theta) = 0$.

Theorem 3. *The algebraic integers form a subring of the field of algebraic numbers.*

Let $\mathbf{B}$ be the set of algebraic integers. For any number field K we write

$$\mathfrak{O}_K = K \cap \mathbf{B}.$$

That is, $\mathfrak{O}_K$ is the set composed of the algebraic integers of K. The set $\mathfrak{O}_K$ is called the *ring of integers* of K. The ring $\mathfrak{O}_K$ will be denoted $\mathfrak{O}$ when the field K is clear from the context.

Example 53
We have that $\mathfrak{O}_{\mathbb{Q}} = \mathbb{Z}$. First of all, $\alpha \in \mathbb{Z}$ is a root of the monic polynomial with integer coefficients $X - \alpha$, hence, $\mathbb{Z} \subseteq \mathfrak{O}_{\mathbb{Q}}$.

Reversely, let us assume $\alpha = \frac{a}{b}$ is an algebraic integer in $\mathbb{Q}$. Then, its minimum polynomial in $\mathbb{Q}[X]$, $X - \frac{a}{b}$, must have integer coefficients, which happens only when b divides a, so that $\alpha \in \mathbb{Z}$, and $\mathfrak{O}_{\mathbb{Q}} \subseteq \mathbb{Z}$.

Proposition 4. *Let K be a number field.*

1. *$\mathfrak{O}_K$ is a subring of $\mathbb{C}$ whose field of fractions is K.*
2. *$\mathfrak{O}_K$ is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$.*

Definition 50 (Integral basis)
Let $\mathfrak{O}$ be the ring of integers of K. We say that $\{\alpha_1, \ldots, \alpha_s\}$ is an *integral basis* for K (or for $\mathfrak{O}$) if and only if $\alpha_i \in \mathfrak{O}, \forall i$, and every element of $\mathfrak{O}$ is uniquely expressible in the form

$$a_1\alpha_1 + \ldots + a_s\alpha_s,$$

for *rational integers* $a_1, \ldots, a_s$, *i.e.* $a_i \in \mathbb{Z}, \forall i$.

Definition 51 (Discriminant of a number field)
Let $\mathfrak{O}$ be the ring of integers of K. The *discriminant* of K is defined as the discriminant of any integral basis for $\mathfrak{O}$. This value does not depend on the choice of such a basis.

Example 54
Let $K = \mathbb{Q}(\sqrt[3]{7})$. We will ask Sage for an integral basis for K.

```
sage:  Q=PolynomialRing(QQ,'x')
sage:  x=Q.gen()
sage:  K.<t>=NumberField(x^3-7)
sage:  K.integral_basis()
[1, t, t^2]
```

The result states that, given a primitive element t of the extension $\mathbb{Q}(\sqrt[3]{7})/\mathbb{Q}$, then $\{1, t, t^2\}$ is an integral basis. In this way, taking $t = \sqrt[3]{7}$, we get that $\{1, \sqrt[3]{7}, (\sqrt[3]{7})^2\}$ is an integral basis. Its discriminant has been computed in Example 51 (being -1323) so that the discriminant of $\mathbb{Q}(\sqrt[3]{7})$ is -1323.

Definition 52 (Quadratic field)
A *quadratic field* is a number field K of degree 2 over $\mathbb{Q}$.

We know that $K = \mathbb{Q}(\theta)$ where θ is an algebraic integer. Since the degree of K is two, θ must be the root of an irreducible monic degree 2 polynomial

$$X^2 + aX + b, \qquad a, b \in \mathbb{Z}.$$

Thus,

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

If $a^2 - 4b = r^2 d$ with $r, d \in \mathbb{Z}$ and d is squarefree, then,

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

and we conclude that $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{d})$. Hence, quadratic fields are those of the form $\mathbb{Q}(\sqrt{d})$ for d a squarefree rational integer. The set $\{1, \sqrt{d}\}$ is a basis for

K so that the elements of $\mathbb{Q}(\sqrt{d})$ are of the form

$$r + s\sqrt{d}, \qquad r, s \in \mathbb{Q}.$$

Definition 53 (Real/Imaginary quadratic field)
If $d > 0$, the field K is said to be a *real quadratic field*. Otherwise ($d < 0$), we say that K is an *imaginary quadratic field*.

Let $\alpha = r + s\sqrt{d} \in \mathbb{Q}(\sqrt{d})$. Such a value can be expressed as $\alpha = \frac{a}{c} + \frac{b}{c}\sqrt{d}$, with $a, b, c \in \mathbb{Z}$, $c > 0$ and no prime divides all of a, b, c. Then, α is an integer if the coefficients of its minimum polyonomial $(X - \alpha)(X - \sigma_2(\alpha))$ are integers. That is,

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

$$= X^2 - \frac{2a}{c}X + \frac{a^2 - b^2 d}{c^2},$$

has integer coefficients, so that both $\frac{2a}{c}$ and $\frac{a^2 - b^2 d}{c^2}$ are integers.

If a and c have some common prime factor p, then $\frac{a^2 - b^2 d}{c^2}$ being an integer requires that p also divides b which contradicts our assumption that $\gcd(a, b, c) = 1$. Hence a and c are comprime and $\frac{2a}{c}$ can only be an integer if $c = 1$ or $c = 2$. In the former case, the minimum polynomial always has integer coefficients. If $c = 2$, both a and b must be odd and $\frac{a^2 - b^2 d}{4}$ is an integer if and only if

$$a^2 - b^2 d \equiv 0 \pmod 4.$$

If both a and b are squarefree, we have that $a^2 \equiv b^2 \equiv 1 \pmod 4$ and

$$0 \equiv a^2 - b^2 d \equiv 1 - d \pmod 4,$$

so that $d \equiv 1 \pmod 4$. In this way:

1. If $d \not\equiv 1 \pmod 4$ then $c = 1$ and the algebraic integers of $K = \mathbb{Q}(\sqrt{d})$ are of the form $a + b\sqrt{d}$. We conclude that $\{1, \sqrt{d}\}$ is an integral basis for $\mathfrak{O}_K$ and $\mathfrak{O}_K = \mathbb{Z}[\sqrt{d}]$.

2. If $d \equiv 1 \pmod 4$ then, we can have $c = 2$ so that $\{1, \frac{1}{2} + \frac{1}{2}\sqrt{d}\}$ is an integral basis for $\mathfrak{O}_K$ and $\mathfrak{O}_K = \mathbb{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{d}]$.

It is worth noting that, given $K = \mathbb{Q}(\sqrt{d})$, we can describe its ring of integers as

$$\mathfrak{O}_K = \mathbb{Z}[w_K], \qquad w_K = \frac{d + \sqrt{d}}{2}.$$

Let us now compute the discriminant of such integral basis (the discriminant of $\mathbb{Q}(\sqrt{d})$):

1. If $d \not\equiv 1 \pmod 4$,

$$\Delta[1, \sqrt{d}] = \begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix}^2 = (-2\sqrt{d})^2 = 4d.$$

2. If $d \equiv 1 \pmod 4$,

$$\Delta\left[1, \frac{1}{2} + \frac{1}{2}\sqrt{d}\right] = \begin{vmatrix} 1 & \frac{1}{2} + \frac{1}{2}\sqrt{d} \\ 1 & \frac{1}{2} - \frac{1}{2}\sqrt{d} \end{vmatrix}^2 = (-\sqrt{d})^2 = d.$$

Note that the discriminant of a quadratic number field satisfies either $d \equiv 0 \pmod 4$ (the former case above) or $d \equiv 1 \pmod 4$ (the latter case above).

Example 55
The number field $\mathbb{Q}(\sqrt{-15})$ is an imaginary quadratic field. Since $-15 \equiv 1 \pmod 4$, its discriminant is $d_{\mathbb{Q}(\sqrt{-15})} = -15$ and $\{1, \frac{1+\sqrt{-15}}{2}\}$ is a basis of its ring of integers $\mathfrak{O}_{\mathbb{Q}(\sqrt{-15})}$. Then,

$$\mathfrak{O}_{\mathbb{Q}(\sqrt{-15})} = \left\{ m + \left(\frac{1+\sqrt{-15}}{2}\right) n \ : \ m, n \in \mathbb{Z} \right\}.$$

Remark 4
Let us consider the polynomial $f = X^2 + 2$ defined in $\mathbb{Z}_5$ and let α be a root of f (in some extension of $\mathbb{Z}_5$). In Example 39 we saw that $\{1, \alpha\}$, is a basis of $\mathbb{F}_{5^2}$ over $\mathbb{Z}_5$. The discriminant of such a basis can be computed exactly in the same manner it is done for number fields:

$$\Delta[1, \alpha] = \begin{vmatrix} 1 & \alpha \\ 1 & -\alpha \end{vmatrix}^2 = (-2\alpha)^2 = 4\alpha^2 = 4 \cdot (-2) = 4 \cdot 3 = 2.$$

2.2 Ideals

Ideals in the ring of integers of a number field can be uniquely decomposed as a product of prime ideals. The way in which ideals factorize over extended fields will leads us to introduce the Hilbert class field, which is fundamental for the methods that have been implemented in this Master's thesis. Fractional ideals are also introduced in this section.

Theorem 4. *The ring of integers $\mathfrak{O}_K$ in a number field K is a Dedekin domain, which means that,*

1. *$\mathfrak{O}_K$ is integrally closed.*
2. *$\mathfrak{O}_K$ is Noetherian,* i.e.*, given any chain of ideals $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \ldots$, there is an integer n such that $\mathfrak{a}_n = \mathfrak{a}_{n+1} = \ldots$.*
3. *Every nonzero prime ideal of $\mathfrak{O}_K$ is maximal.*

Dedekin domains have a very important property: unique factorization for ideals. This is stated in the following corollary.

Corollary 1. *If K is a number field, then any nonzero ideal of $\mathfrak{O}_K$ 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 $\mathfrak{O}_K$ containing $\mathfrak{a}$.

Definition 54 (Ideal norm)
Let K be a number field, $\mathfrak{O}_K$ its ring of integers, and let $\mathfrak{a}$ be an ideal in $\mathfrak{O}_K$. The *norm* of $\mathfrak{a}$ is defined to be,

$$N(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|.$$

The ideal norm can also be seen as $N(\mathfrak{a}) = n$ when $\mathfrak{a}\overline{\mathfrak{a}} = \langle n \rangle$, with $n \in \mathbb{Z}$ and $\overline{\mathfrak{a}}$ denoting the complex conjugate of $\mathfrak{a}$.

The ring of integers of a number field is not always a principal ideal domain. Nevertheless, its ideals are either principal or generated by a two elements set.

Example 56 ([23], Exercise 5.2)
The ring of integers of $K = \mathbb{Q}(\sqrt{-5})$ is $\mathfrak{O}_K = \mathbb{Z}[\sqrt{-5}]$. Now we will show that, in $\mathbb{Z}[\sqrt{-5}]$, the ideal $\langle 2 \rangle$ decomposes into $\mathfrak{p}^2 = \langle 2 \rangle$ where $\mathfrak{p} = \langle 2, 1 + \sqrt{-5} \rangle$.

The elements in $\mathfrak{p}$ are of the form

$$2z_1 + z_2(1 + \sqrt{-5}), \quad z_1, z_2 \in \mathbb{Z}[\sqrt{-5}].$$

Hence, from the definition of product of ideals, the elements in $\mathfrak{p}^2$ are generated by adding elements of the form

$$(2z_1 + z_2(1 + \sqrt{-5}))(2z_3 + z_4(1 + \sqrt{-5})), \quad z_1, z_2, z_3, z_4 \in \mathbb{Z}[\sqrt{-5}]. \tag{2.1}$$

Operating, we get

$$4z_1z_3 + 2(1 + \sqrt{-5})(z_1z_4 + z_2z_3) + (-4 + 2\sqrt{-5})z_2z_4 =$$

$$= 2\left(2z_1z_3 + (1 + \sqrt{-5})(z_1z_4 + z_2z_3) + (-2 + \sqrt{-5})z_2z_4\right).$$

In this way, the elements in $\mathfrak{p}^2$ are an addition of numbers of the form $2(k_1 + k_2\sqrt{-5})$, with $k_1, k_2 \in \mathbb{Z}$ so that $\mathfrak{p}^2 \subseteq \langle 2 \rangle$.

So as to prove that $\mathfrak{p}^2 =< 2 >$ we will show that $2 \in \mathfrak{p}^2$. In equation 2.1 we can take $z_1 = 0, z_2 = 1, z_3 = 1, z_4 = -1$ and we get $6 \in \mathfrak{p}^2$. In a similar fashion, by taking $z_1 = 1, z_2 = 0, z_3 = 1, z_4 = 0$ we get $4 \in \mathfrak{p}^2$. And from the definition of ideal, if $4, 6 \in \mathfrak{p}^2$ then $2 = 6 - 4 \in \mathfrak{p}^2$, hence $\langle 2 \rangle \subseteq \mathfrak{p}^2$ and we conclude that $\mathfrak{p}^2 = \langle 2 \rangle$.

We can check it in Sage:

```
sage:  Q.<T>=PolynomialRing(QQ,'T')
sage:  K.<x>=NumberField(T^2+5)
sage:  I=K.ideal(2)
sage:  I.factor()
(Fractional ideal (2, x + 1))^2
```

Note that the ideal $\langle 2\rangle$ is principal while $\left\langle 2, 1+\sqrt{-5}\right\rangle$ is not. From some known results about ideal norms, it can be proven that $\left\langle 2, 1+\sqrt{-5}\right\rangle$ can not be principal.

Finally, we see that $N(\mathfrak{p}) = 2$ since $\overline{\mathfrak{p}} = \mathfrak{p}$ and $\mathfrak{p}^2 = \langle 2\rangle$. Note that

$$2 - (1+\sqrt{-5}) = 1 - \sqrt{-5} = \overline{1+\sqrt{-5}},$$

hence,

$$\overline{\left\langle 2, 1+\sqrt{-5}\right\rangle} = \left\langle 2, 1-\sqrt{-5}\right\rangle = \left\langle 2, 1+\sqrt{-5}\right\rangle.$$

If $\mathfrak{p}$ is a prime ideal in $\mathfrak{O}_K$ it can not be further factored in $\mathfrak{O}_K$. Nevertheless, that is not the case if we consider a finite extension L of K. If $\mathfrak{p}$ is an ideal of $\mathfrak{O}_K$ then $\mathfrak{p}\mathfrak{O}_L$ is and ideal of $\mathfrak{O}_L$ and can be uniquely be decomposed as a product of prime ideals,

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

We say that a prime ideal $\mathfrak{p}$ of $\mathfrak{O}_K$ ramifies in L if any of the *ramification indices* e_i are greater than 1.

Example 57
The ring of integers of $\mathbb{Q}$ is $\mathbb{Z}$. The ideal $\langle 2\rangle$ is prime in $\mathbb{Z}$, but as we have seen in the previous example, it ramifies in the ring of integers of $\mathbb{Q}(\sqrt{-5})$, namely, in $\mathbb{Z}[\sqrt{-5}]$ since,

$$\langle 2\rangle = \left\langle 2, 1+\sqrt{-5}\right\rangle^2.$$

On the other side, the ideal $\langle 3\rangle$ does not ramify in $\mathbb{Z}[\sqrt{-5}]$ since in this case,

$$\langle 3\rangle = \left\langle 3, 1+\sqrt{-5}\right\rangle \left\langle 3, 2+\sqrt{-5}\right\rangle.$$

We can check it in Sage:

```
sage:  Q.<T>=PolynomialRing(QQ,'T')
sage:  K.<x>=NumberField(T^2+5)
sage:  I=K.ideal(3)
sage:  I.factor()
(Fractional ideal (3, x + 1)) * (Fractional ideal (3, x + 2))
```

Definition 55 (Fractional ideal)
A *fractional ideal* is a nonzero finitely generated $\mathfrak{O}_K$-submodule 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 $\mathfrak{O}_K$.

Remark 5
Given a number field K, its ring of integers $\mathfrak{O}_K$ is a Dedekin domain and fractional ideals have unique factorization into prime ideals (the powers may be negative). Given a prime ideal $\mathfrak{p}$ and a fractional ideal $\mathfrak{a}$, the function $v_\mathfrak{p}(\mathfrak{a})$ that returns the power of $\mathfrak{p}$ that appears in the factorization of $\mathfrak{a}$ is a discrete valuation (see Definition 17). The discrete valuation $v_\mathfrak{p}(\mathfrak{a})$ tells us about the ramification of the prime $\mathfrak{p}$.

Example 58
Let us consider the following set:

$$I = \left\{ \frac{3}{2}m + \frac{3}{2}\sqrt{-5}n \;\; : \;\; m, n \in \mathbb{Z} \right\}.$$

This set can described as

$$\left\{ \frac{1}{2}3(m + \sqrt{-5}n) \;\; : \;\; m, n \in \mathbb{Z} \right\} = \left\{ \frac{1}{2}3z \;\; : \;\; z \in \mathbb{Z}[\sqrt{-5}] \right\} = \frac{1}{2}\langle 3 \rangle .$$

Since $\frac{1}{2} \in \mathbb{Q}(\sqrt{-5})$ and $\langle 3 \rangle$ is an ideal of its ring of integers we conclude $I \in I_{\mathbb{Q}(\sqrt{-5})}$.

The set of all fractional ideals of K is denoted by I_K. The set I_K is a group under multiplication of ideals. We distinguish the subgroup of I_K composed of principal fractional ideals and denote it by P_K. Now we can provide the following definition.

Definition 56 (Ideal class group)
Let K be a number field and let I_K and P_K be the set of fractional ideals and its subgroup of principal fractional ideals, respectively. The *ideal class group* $C(\mathfrak{O}_K)$ is defined to be the quotient I_K/P_K.

Remark 6
The ideal class group can also be defined by considering that two fractional ideals $A, B \subset K$ are equivalent when there exist $r, s \in K$ so that $rA = sB$. The ideal class group corresponds to the quotient set of that equivalence relation.

By defining the class product as the class of the product of two ideals, ideal classes have a group structure under multiplication whose identity element is the class of principal ideals (which contains $\mathfrak{O}_K$). It can be proven that the ideal class group is generated by ideals whose norm is less or equal than $\frac{2}{\pi}\sqrt{|D|}$, where D is the discriminant of the number field K.

Example 59
The ring of integers of $\mathbb{Q}$ is $\mathbb{Z}$ which is known to be a principal ideal domain. Hence all the ideals of $\mathbb{Z}$ are principal and so are the fractional ideals of $\mathbb{Q}$. Hence $I_{\mathbb{Q}} = P_{\mathbb{Q}}$ and the quotient $C(\mathfrak{O}_{\mathbb{Q}}) = I_{\mathbb{Q}}/P_{\mathbb{Q}}$ is isomorphic to $\{0\}$.

Example 60
In the ring of integers of $K = \mathbb{Q}(\sqrt{-5})$, the ideal $I = \left\langle 2, 1+\sqrt{-5} \right\rangle$ generates the ideal class group since its norm $N(I) = 2$ is not larger than $\frac{2}{\pi}\sqrt{20} \approx 2.84$. In this example, $C(\mathfrak{O}_K)$ is isomorphic to $\mathbb{Z}_2$ since, as we saw in Example 56, $I^2 = \langle 2 \rangle$ in $\mathbb{Z}[\sqrt{-5}]$.

Example 61
In the ring of integers of $K = \mathbb{Q}(\sqrt{-15})$, we have that

$$\langle 2 \rangle = \left\langle 2, \frac{1+\sqrt{-15}}{2} \right\rangle \left\langle 2, \frac{1-\sqrt{-15}}{2} \right\rangle.$$

In this example, $\langle 2 \rangle$ and $\mathfrak{O}_K$ are in the same ideal class since $\frac{1}{2}\langle 2 \rangle = \langle 1 \rangle = \mathfrak{O}_K$ which is the identity element of $C(\mathfrak{O}_K)$. Moreover, $\left\langle 2, \frac{1+\sqrt{-15}}{2} \right\rangle$ and $\left\langle 2, \frac{1-\sqrt{-15}}{2} \right\rangle$ are in the same class which we denote by J. Then, J^2 is the identity element of $C(\mathfrak{O}_K)$.

Theorem 5. *Given a number field K, there is a finite Galois extension L of K such that:*

1. *L is an unramified Abelian extension of K.*
2. *Any unramified Abelian extension of K lies in L.*

Definition 57 (Hilbert class field)
The field L of Theorem 5 is called the *Hilbert class field* of K.

Example 62
Let $K = \mathbb{Q}(\sqrt{-15})$. We will use Sage to compute the Hilbert class field L of K.

```
sage:  K.<t>=QuadraticField(-15)
sage:  L=K.hilbert_class_field('u')
sage:  L
Number Field in u with defining polynomial x^2 - x + 1 over
its base field
```

We can see $X^2 - X + 1$ is the minimum polynomial of L over K. Hence, the Hilbert class field L is a degree 2 extension of K and the automorphism group $G(L:K)$ is isomorphic to $\mathbb{Z}_2$.

Lemma 2. *Let L/K be a Galois extension, and let $\mathfrak{p}$ be a prime ideal of $\mathfrak{O}_K$ which is unramified in L. If $\mathfrak{P}$ is a prime ideal of $\mathfrak{O}_L$ containing $\mathfrak{p}$, then there is a unique element $\sigma \in G(L:K)$ such that for all $\alpha \in \mathfrak{O}_L$,*

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

where $N(\mathfrak{p}) = |\mathfrak{O}_K/\mathfrak{p}|$.

Definition 58 (Artin symbol)
Let L/K be a Galois extension and let $\mathfrak{P}$ be a prime ideal of $\mathfrak{O}_L$. The unique element σ related to $\mathfrak{O}_L$ of Lemma 2 is called the *Artin symbol* and is denoted by $((L/K)/\mathfrak{P})$.

Definition 59 (Artin map)
The Artin symbol defines a homomorphism, called the *Artin map*,

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

Next, Theorem 6 states that the Artin map provides and isomorphism between the ideal class group of a number field K and the automorphism group of L/K, being L the Hilbert class field of K. More details are given in [6].

Theorem 6. *If L is the Hilbert class field of a number field K, then the Artin map is surjective, and its kernel is the subgroup P_K of principal fractional ideals. Thus, the Artin map induces an isomorphism*

$$C(\mathfrak{O}_K) \sim G(L:K).$$

Proof sketch. By [6, Theorem 8.2] we have that given a number field K, an Abelian extension E/K, and a modulus $\mathfrak{m}$ (when K is purely imaginary, a modulus can be regarded simply as an ideal of $\mathfrak{O}_K$) divisible by all primes of K that ramify in E, then the Artin map $\Phi_{\mathfrak{m}}$ is surjective ($\Phi_{\mathfrak{m}}$ is the Artin map restricted to primes not dividing $\mathfrak{m}$). Since the Hilbert class field L is unramified, if we take $E = L$ then $\mathfrak{m} = 1$ and the Artin map $\left(\frac{L/K}{\cdot}\right)$ is surjective.

It is known that if L is the Hilbert class field of a number field K, and $\mathfrak{p}$ is a prime ideal of K, then $\mathfrak{p}$ splits completely in L if and only if $\mathfrak{p}$ is a principal ideal. It is also known that an ideal $\mathfrak{p}$ splits completely if and only if $((L/K)/\mathfrak{p}) = 1$. Hence, the kernel of the Artin map consists of the principal ideals of K, namely P_K.

We conclude that $G(L:K)$ is isomorphic to $C(\mathfrak{O}_K) = I_K/P_K$.

2.3 Orders in imaginary quadratic fields

As we will see in Section 5.2, orders in imaginary quadratic fields appear when studying lattice homotheticity and complex multiplication. Such orders are

briefly introduced in this section.

Definition 60 (Order in a quadratic field)
An *order* $\mathcal{O}$ in a quadratic field K is a subset $\mathcal{O} \subset K$ such that,

1. $\mathcal{O}$ is a subring of K containing 1.
2. $\mathcal{O}$ is a finitely generated $\mathbb{Z}$-module.
3. $\mathcal{O}$ contains a $\mathbb{Q}$-basis of K.

The ring of integers $\mathfrak{O}_K$ is an order in K and any order $\mathcal{O}$ of K satisfies $\mathcal{O} \subset \mathfrak{O}_K$, hence $\mathfrak{O}_K$ is the *maximal order* of K. The following lemma addresses how the orders of a quadratic field K are.

Lemma 3. *Let $\mathcal{O}$ be an order in a quadratic field K, then,*

$$\mathcal{O} = \mathbb{Z} + f\mathfrak{O}_K,$$

where $f = [\mathfrak{O}_K : \mathcal{O}]$ is the index of $\mathcal{O}$ in $\mathfrak{O}_K$. This value is referred to as the conductor *of the order.*

Example 63
The set

$$\mathcal{O} = \mathbb{Z} + 2\mathfrak{O}_{\mathbb{Q}(\sqrt{-15})} = \left\{m + (\sqrt{-15})n \quad : \quad m, n \in \mathbb{Z}\right\} = \mathbb{Z}\left[\sqrt{-15}\right]$$

is an order in $\mathbb{Q}(\sqrt{-15})$. Its conductor is 2.

Definition 61 (Discriminant of an order)
The *discriminant* of an order $\mathcal{O}$ in a quadratic field K is $D = f^2 d_K$, where f is the conductor and d_K is the discriminant of the field K.

Example 64
The discriminant of an order in a quadratic field is computed in the same manner as it was described in page 38. Since $\{1, \frac{1+\sqrt{-15}}{2}\}$ is a basis for $\mathfrak{O}_{\mathbb{Q}(\sqrt{-15})}$ (see Example 52) then, $\{1, \sqrt{-15}\}$ is basis for $\mathcal{O} = \mathbb{Z}+2\mathfrak{O}_{\mathbb{Q}(\sqrt{-15})}$ whose discriminant is

$$\begin{vmatrix} 1 & \sqrt{-15} \\ 1 & -\sqrt{-15} \end{vmatrix}^2 = (-2\sqrt{-15})^2 = 2^2(-15).$$

As expected, the result is of the form $f^2 d_K$ with $f = 2$ and $d_K = -15$ ($K = \mathbb{Q}(\sqrt{-15})$).

Since an order $\mathcal{O}$ has a ring structure, it can contain ideals.

Definition 62 (Proper ideal of an order)
Let $\mathcal{O}$ be an order in a quadratic field an let $\mathfrak{a}$ be an ideal of $\mathcal{O}$. The ideal $\mathfrak{a}$ is said to be *proper* when

$$\mathcal{O} = \{\beta \in K \quad : \quad \beta\mathfrak{a} \subset \mathfrak{a}\}.$$

Fractional ideals of an order are defined as a subset of K which is a nonzero finitely genereated $\mathcal{O}$-module. Hence, every fractional ideal is of the form $\alpha\mathfrak{a}$, where $\alpha \in K^*$ and $\mathfrak{a}$ is an $\mathcal{O}$-ideal.

Definition 63 (Ideal class group of an order)
Given an order $\mathcal{O}$, we denote $I(\mathcal{O})$ the set of proper fractional $\mathcal{O}$-ideals, and $P(\mathcal{O}) \subset I(\mathcal{O})$ the subset composed of those that are principal. The *ideal class group* of the order $\mathcal{O}$ is the quotient,

$$C(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O}).$$

Chapter 3

Quadratic forms

In this chapter we will see that there exists a particular type of quadratic forms that can be endowed with a group structure: the so called *form class group*. The importance of this group comes from the fact that it is isomorphic to the ideal class group of the ring of integers of an imaginary quadratic field (see Theorem 8). This isomorphism is the core of Atkin-Morain's method for constructing Hilbert class polynomials (Section 6.1). The concepts and results of this chapter have been extracted mainly from [4] and [6].

3.1 Basic concepts

Definition 64 (Binary quadratic form)
An *integral quadratic form* in two variables is an expression,

$$f(x,y) = ax^2 + bxy + cy^2, \qquad a,b,c \in \mathbb{Z}.$$

If coefficients a, b, c are relatively prime, $f(x,y)$ is said to be *primitive*. An integer m is *represented* by a form $f(x,y)$ if there exist two integers x', y' satisfying,

$$m = f(x', y').$$

If x', y' are relatively prime, we say that m is *properly represented* by $f(x,y)$. Two forms $f(x,y)$ and $g(x,y)$ are *properly equivalent* when,

$$f(x,y) = g(px+qy, rx+sy), \qquad p,q,r,s \in \mathbb{Z}, \;\; ps - qr = 1.$$

Example 65
Let us consider $f(x,y) = 34x^2 - 45xy + 15y^2$. This quadratic form is primitive since

$$\gcd(34, -45, 15) = 1.$$

We can see $f(x,y)$ properly represents 1 and 4 since, $1 = f(2,3)$ and $4 = f(1,2)$.

The integers $p = 2$, $q = 1$, $r = 3$ and $s = 2$ satisfy $ps - qr = 1$, and,

$$f(2x+y,3x+2y) = 34(4x^2+4xy+y^2)-45(6x^2+7xy+2y^2)+15(9x^2+12xy+4y^2) =$$

$$= x^2 + xy + 4y^2 = g(x,y).$$

Hence, $f(x,y)$ and $g(x,y)$ are properly equivalent. As a consequence, the sets of integers represented by both forms coincide. For instance, $g(x,y)$ also represents 1 and 4, since $1 = g(1,0)$ and $4 = g(0,1)$.

Definition 65 (Discriminant)
The *discriminant* of a quadratic form $f(x,y) = ax^2 + bxy + cy^2$ is defined to be,

$$D = b^2 - 4ac.$$

The discriminant is tightly related to proper equivalence in the sense that two properly equivalent quadratic forms have the same discriminant. The converse is not necessarily true.

Since $D = b^2 - 4ac$, we get $b^2 = D + 4ac$, and $b^2 \equiv D \pmod 4$. If $b \equiv 0, 2 \pmod 4$ then $D \equiv b^2 \equiv 0 \pmod 4$ while if $b \equiv 1, 3 \pmod 4$ then $D \equiv b^2 \equiv 1 \pmod 4$. Hence the discriminant of any quadratic form satisfies that,

$$D \equiv 0, 1 \pmod 4.$$

Given a form $f(x,y) = ax^2 + bxy + cy^2$, we can see that

$$4af(x,y) =$$

$$= 4a^2x^2 + 4abxy + 4acy^2 = 4a^2x^2 + 4abxy + (b^2y^2 - b^2y^2) + 4acy^2 =$$

$$= (4a^2x^2 + 4abxy + b^2y^2) - y^2(b^2 - 4ac) =$$

$$= (2ax + by)^2 - Dy^2.$$

Here we can distinguish two cases:

- $D > 0$: the quadratic form represents both positive and negative integers.
- $D < 0$: the quadratic form represents only positive integers (if $a > 0$) or only negative ones (if $a < 0$). In the former case $f(x,y)$ is *definite positive*.

Definition 66 (Reduced form)
A primitive positive definite form $f(x,y) = ax^2 + bxy + cy^2$ is said to be *reduced* if,

$$|b| \leq a \leq c, \text{ and } b \geq 0 \text{ if either } |b| = a \text{ or } a = c.$$

Theorem 7. *Every primitive positive definite form is properly equivalent to a unique reduced form.*

An algorithm for computing the reduced equivalent form is described in [4, Chap.5].

By considering the proper equivalence relation, primitive positive definite forms can be grouped into equivalence classes containing a unique reduced form each.

Example 66
Let $f(x,y) = 34x^2 - 45xy + 15y^2$ and $g(x,y) = x^2 + xy + 4y^2$.

We have seen that both forms are properly equivalent. It is easy to check that both forms have the same discriminant. In effect, the discriminant D of $f(x,y)$ is,

$$D = (-45)^2 - 4 \cdot 34 \cdot 15 = -15$$

while that of $g(x,y)$, D', is,

$$D' = 1^2 - 4 \cdot 1 \cdot 4 = -15.$$

Both quadratic forms are definite positive. Form g is reduced.

Next we will see that once the discriminant $D < 0$ has been fixed, the number $h(D)$ of equivalence classes of primitive positive definite forms of discriminant D is finite. The number $h(D)$ is the *class number*.

Let $f(x,y) = ax^2 + bxy + cy^2$ be a form of discriminant $D < 0$. If f is positive definite then $1 \leq a$ while if f is reduced then $b^2 \leq a^2$ and $a \leq c$, so that

$$-D = 4ac - b^2 \geq 4a^2 - a^2 = 3a^2.$$

In this way, $1 \leq a \leq \sqrt{(-D)/3}$. For a fixed $D < 0$, there are only finitely many integers a satisfying the previous inequality. A reduced form satisfies $|b| \leq a$ so that for each a the amount of such b values is also finite. Finally, given a pair a, b, there is at most one value for c satisfying $D = b^2 - 4ac$ (such an integer c may not exist). Hence, the number of reduced primitive positive forms having discriminant $D < 0$ is finite.

Example 67
There are two different reduced primitive positive forms of discriminant $D = -15$. They are:

$$x^2 + xy + 4y^2, \;\; 2x^2 + xy + 2y^2$$

We can check it in Sage:

```
sage:  BinaryQF_reduced_representatives(-15,primitive_only=True)
[x^2 + x*y + 4*y^2, 2*x^2 + x*y + 2*y^2]
```

Note that the number of forms obtained in this example coincides with the degree of the extension $L/\mathbb{Q}(\sqrt{-15})$ where L is the Hilbert class field of

$Q(\sqrt{-15})$ that was computed in Example 62 (p. 46). This is a particular example of an important statement resulting from Theorems 6 and 8 which is the basis of Atkin-Morain's method for generating elliptic curves with a given cardinality. That method is studied in Section 6.1.

Example 68
There are four different reduced primitive positive forms of discriminant $D = -56$. They are:

$$x^2 + 14y^2, \;\; 2x^2 + 7y^2, \;\; 3x^2 - 2xy + 5y^2, \;\; 3x^2 + 2xy + 5y^2$$

We can check it in Sage:

```
sage:  BinaryQF_reduced_representatives(-56,primitive_only=True)
[x^2 + 14*y^2, 2*x^2 + 7*y^2, 3*x^2 - 2*x*y + 5*y^2,
3*x^2 + 2*x*y + 5*y^2]
```

We got four quadratic forms. We can now check the degree of the extension $L/\mathbb{Q}(\sqrt{-56})$, where L is the Hilbert class field of $\mathbb{Q}(\sqrt{-56})$ is four:

```
sage:  K.<t>=QuadraticField(-56)
sage:  L=K.hilbert_class_field('u')
sage:  L
Number Field in u with defining polynomial x^4 + 2*x^3 + x^2 +
2*x + 1 over its base field
```

The set composed of quadratic form equivalence classes with discriminant D is denoted $C(D)$. We can take the unique reduced form in each class as a representative for that class. Next we will see that this set can be endowed with a group structure.

3.2 Form class group

Definition 67 (Quadratic form composition)
If $f(x, y)$ and $g(x, y)$ are primitive positive definite forms of discriminant D, a form $F(x, y)$ of the same type is their *composition* provided that

$$f(x, y)g(z, w) = F(B_1(x, y; z, w), B_2(x, y; z, w)),$$

where

$$B_i(x, y; z, w) = a_i xz + b_i xw + c_i yz + d_i yw, \quad i = 1, 2.$$

When the previous expressions satisfy

$$a_1b_2 - a_2b_1 = f(1,0), \qquad a_1c_2 - a_2c_1 = g(1,0)$$

the composition is said to be *direct*.

Lemma 4. *Assume that* $f(x,y) = ax^2+bxy+cy^2$ *and* $g(x,y) = a'x^2+b'xy+c'y^2$ *have discriminant* D *and satisfy* $\gcd(a, a', (b+b')/2) = 1$. *Then there is a unique integer* B *modulo* $2aa'$ *satisfying,*

$$\begin{aligned} B &\equiv b \pmod{2a} \\ B &\equiv b' \pmod{2a'} \\ B^2 &\equiv D \pmod{4aa'}. \end{aligned}$$

Definition 68 (Dirichlet composition)
Let $f(x,y) = ax^2+bxy+cy^2$ and $g(x,y) = a'x^2+b'xy+c'y^2$ be primitive positive definite forms of discriminant $D < 0$ which satisfy $gcd(a, a', (b+b')/2) = 1$. The *Dirichlet composition* of $f(x,y)$ and $g(x,y)$ is the form

$$F(x,y) = aa'x^2 + Bxy + \frac{B^2 - D}{4aa'}y^2,$$

where B is the integer determined by Lemma 4.

Let $D \equiv 0, 1 \pmod 4$ be a negative discriminant. The set $C(D)$ is finite and its cardinality is $h(D)$. The Dirichlet composition induces a well-defined binary operation on $C(D)$ which makes $C(D)$ into a finite Abelian group. The identity element of $C(D)$ is the class containing the form

$$x^2 - \frac{D}{4}y^2, \quad \text{if } D \equiv 0 \pmod 4,$$

$$x^2 + xy + \frac{1-D}{4}y^2, \quad \text{if } D \equiv 1 \pmod 4.$$

Example 69
Taking $D = -15$, we know that

$$C(-15) = \{x^2 + xy + 4y^2,\ \ 2x^2 + xy + 2y^2\}$$

The class of $x^2 + xy + 4y^2$ is the identity element of $C(-15)$ and the class of $2x^2 + xy + 2y^2$ must have order 2, hence $C(-15)$ is isomorphic to $\mathbb{Z}_2$.

Remark 7
Note that in Example 62 we concluded that the automorphism group of the extension $L/\mathbb{Q}(\sqrt{-15})$ being L the Hilbert class field of $\mathbb{Q}(\sqrt{-15})$ was also isomorphic to $\mathbb{Z}_2$. Theorem 6 together with the forthcoming Theorem 8 will serve us to state that both groups are *always* isomorphic. The Atkin-Morain [2] method implemented in Section 6.1 employs this isomorphism for constructing the Hilbert class polynomial from quadratic forms.

Remark 8
In Section 6.1 we will see how Atkin-Morain's method constructs a Hilbert class polynomial by making use of the elements in an appropiate form class group.

Example 70
Let us take $D = -56$. In this case,

$$C(-56) = \{x^2 + 14y^2,\ \ 2x^2 + 7y^2,\ \ 3x^2 - 2xy + 5y^2,\ \ 3x^2 + 2xy + 5y^2\}.$$

The class of $x^2 + 14y^2$ is the identity element of $C(-56)$. Let $f(x, y) = 2x^2 + 7y^2$ and $g(x, y) = 3x^2 - 2xy + 5y^2$. Now we will compute the composition of $f(x, y)$ and $g(x, y)$. In this example, the value $B = 4$ satisfies the conditions of Lemma 4:

$$4 \equiv 0 \pmod 4,$$
$$4 \equiv -2 \pmod 6,$$
$$16 \equiv -56 \pmod{24}.$$

Once B is know, we compute the Dirichlet composition of $f(x, y)$ and $g(x, y)$:

$$F(x, y) = 6x^2 + 4xy + 3y^2.$$

The obtained form F is not reduced since the coefficients $a = 6$ and $c = 3$ do not satisfy $a \leq c$. The integers $p = 0$, $q = -1$, $r = 1$ and $s = 1$ satisfy that $pr - qs = 1$ and

$$F(px + qy, rx + sy) = F(-y, x + y) = 3x^2 + 2xy + 5y^2.$$

In this way, the Dirichlet composition of the classes represented by $2x^2 + 7y^2$ and $3x^2 - 2xy + 5y^2$ generates as a result the class of $3x^2 + 2xy + 5y^2$.

We can check it in Sage:

```
sage:  f=BinaryQF([2,0,7])
sage:  g=BinaryQF([3,-2,5])
sage:  f*g
6*x^2 + 4*x*y + 3*y^2
sage:  (f*g).reduced_form()
3*x^2 + 2*x*y + 5*y^2
```

It could happen that two quadratic forms $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y) = a'x^2 + b'xy + c'y^2$ with the same discriminant $D < 0$ do not satisfy the condition of Lemma 4 ($\gcd(a, a', (b + b')/2) = 1$). In that case, prior to composing both forms, we would have to find a quadratic form $g'(x, y) = a''x^2 + b''xy + c''y^2$ properly equivalent to $g(x, y)$ satisfying $\gcd(a, a'') = 1$. Now, the forms $f(x, y)$ and $g'(x, y)$ meet the requirement of Lemma 4 so that they can

be composed. As a result we would obtain a quadratic form belonging to the class of the composition of $f(x,y)$ and $g(x,y)$. Such a quadratic form $g'(x,y)$ is guaranteed to exist.

Example 71
Let $f(x,y) = 3x^2 - 2xy + 5y^2$ and $g(x,y) = 3x^2 + 2xy + 5y^2$. These forms do not satisfy the condition of Lemma 4 since,

$$\gcd\left(3, 3, \frac{-2+2}{2}\right) = 3 \neq 1.$$

Nevertheless, we can take integers $p = 3$, $q = 5$, $r = 1$ and $s = 2$ which satisfy $ps - qr = 1$ and we can compute

$$g'(x,y) = g(3x + 5y, x + 2y) = 182x^2 + 140xy + 27y^2.$$

The form $g'(x,y)$ is properly equivalent to $g(x,y)$. The forms $f(x,y)$ and $g'(x,y)$ do satisfy the condition of Lemma 4. In this case, $B = 868$ and we can apply Dirichlet composition obtaining as a result,

$$546x^2 + 868xy + 345y^2.$$

This form is not reduced. Its reduced equivalent form is $x^2 + 14y^2$ which is a representative of the identity class in $C(-56)$. Hence, $f(x,y)$ and $g(x,y)$ are inverses of each other.

We can check it in Sage:

```
sage:  f=BinaryQF([3,-2,5])
sage:  g=BinaryQF([3,2,5])
sage:  (f*g).reduced_form()
x^2 + 14*y^2
```

Example 72
Let us consider again the group:

$$C(-56) = \{x^2 + 14y^2,\ \ 2x^2 + 7y^2,\ \ 3x^2 - 2xy + 5y^2,\ \ 3x^2 + 2xy + 5y^2\}.$$

This group is Abelian, hence it can be isomorphic to $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$. Let us check it.

We take the class of $f(x,y) = 3x^2 - 2xy + 5y^2$ and check its order:

$$f(x,y) * f(x,y) = 2x^2 + 7y^2.$$

We compute also,

$$f(x,y) * f(x,y) * f(x,y) = 3x^2 + 2xy + 5y^2.$$

Finally,

$$f(x,y) * f(x,y) * f(x,y) * f(x,y) = x^2 + 14y^2$$

Hence, $C(-56)$ has an order 4 element, so that it is isomorphic to $\mathbb{Z}_4$. We can check it in Sage:

```
sage:  f=BinaryQF([3,-2,5])
sage:  (f*f).reduced_form()
2*x^2 + 7*y^2
sage:  (f*f*f).reduced_form()
3*x^2 + 2*x*y + 5*y^2
sage:  (f*f*f*f).reduced_form()
x^2 + 14*y^2
```

3.3 Forms and ideals

This section is devoted to present Theorem 8 (see [6]) which is of great importance since it provides a method for generating the elements of the ideal class group of the ring of integers of an imaginary quadratic field of discriminant d_K from the elements of the form class group of the same discriminant.

Theorem 8. *Let K be an imaginary quadratic field of discriminant $d_K < 0$. Then,*

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

$$\left[a, \frac{-b+\sqrt{d_K}}{2}\right] = \left\{ma + n\frac{-b+\sqrt{d_K}}{2} \quad : \quad m,n \in \mathbb{Z}\right\}$$

   is an ideal of $\mathfrak{O}_K$.

2. *The map sending $f(x,y)$ to $\left[a, \frac{-b+\sqrt{d_K}}{2}\right]$ induces an isomorphism between the form class group $C(d_K)$ and the ideal class group $C(\mathfrak{O}_K)$.*

Proof sketch. Since $d_K < 0$, the polynomial $f(x,1) = ax^2 + bx + c$ has $\tau = \frac{-b+\sqrt{d}}{2a} \in \mathfrak{h}$ as a root and $\left[a, \frac{-b+\sqrt{d_K}}{2}\right] = [a, a\tau] = a[1,\tau]$ with $\tau \in K$ which is an ideal of $\mathfrak{O}_K$ [6, p.137].

By [6, p.138], we get that if $f(x,y)$ and $g(x,y)$ are two forms of the same discriminant and τ, τ' are their respective roots, then $f(x,y)$ and $g(x,y)$ are properly equivalent if and only if $[1,\tau] = \lambda[1,\tau']$ for some $\lambda \in K^*$. Hence, the map sending $f(x,y)$ to $a[1,\tau]$ induces an injection $C(D) \to C(\mathfrak{O}_K)$ which is known to be surjective. Moreover, the Dirichlet composition of $f(x,y)$ and $g(x,y)$ corresponds to the product of their corresponding ideal classes, so that $C(d_K)$ and $C(\mathfrak{O}_K)$ are isomorphic.

Example 73
Let us consider the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-15})$. Since $-15 \equiv 1 \pmod 4$, its discriminant is $d_K = -15$ and its ring of integers is $\mathfrak{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-15}}{2}\right]$.

We know from previous examples that the form class group of discriminant -15 has cardinality two, being $x^2 + xy + 4y^2$ and $2x^2 + xy + 2y^2$ the reduced forms representing each of the two equivalence classes in $C(-15)$.

Then, the ideal class representatives of $C(\mathfrak{O}_K)$ are given by

$$\left\{ \left[1, \frac{-1+\sqrt{-15}}{2}\right], \ \left[2, \frac{1+\sqrt{-15}}{2}\right] \right\}.$$

Note that, $\left[1, \frac{-1+\sqrt{-15}}{2}\right] = \left[1, \frac{1+\sqrt{-15}}{2}\right] = \mathbb{Z}\left[\frac{1+\sqrt{-15}}{2}\right] = \mathfrak{O}_K$ is the identity element of $C(\mathfrak{O}_K)$.

Remark 9
From theorems 6 and 8 we can conclude that the form class group $C(D)$ is isomorphic to the automorphism group $G(L : \mathbb{Q}(\sqrt{D}))$ with L being the Hilbert class field of $\mathbb{Q}(\sqrt{D})$.

Example 74
From Remark 9 and Example 69 we get that $G(L : \mathbb{Q}(\sqrt{-15}))$ is isomorphic to $\mathbb{Z}_2$, being L the Hilbert class field of $\mathbb{Q}(\sqrt{-15})$.

This was already stated in Example 62 due to the simplicity of this group.

Example 75
From Remark 9 and Example 72, $G(L' : \mathbb{Q}(\sqrt{-56}))$ is isomorphic to $\mathbb{Z}_4$, being L' the Hilbert class field of $\mathbb{Q}(\sqrt{-56})$.

Remark 10
The isomorphism commented in Remark 9 is of capital importance since it provides a method for constructing Hilbert class polynomials (as explained in Section 5.2). This is precisely what one of the steps of the Atkin-Morain method (implemented in Section 6.1) does.

Chapter 4

Algebraic curves

This chapter is composed of two sections. The first one provides an overview of complex algebraic affine and projective curves. The second one is an introduction to algebraic geometry. Their content comes mainly from [13] and [18].

4.1 Complex algebraic curves

This section presents some basic concepts about algebraic curves defined over the complex numbers together with the projective plane and some results involving complex projective algebraic curves of degree three. These curves are the core of the theory of complex multiplication, as we will see in Chapter 5. The reader is referred to [13] for more details.

Definition 69 (Complex algebraic curve in $\mathbb{C}^2$)
Let $P(X, Y)$ be a nonconstant polynomial with complex coefficients. The *complex algebraic curve* in $\mathbb{C}^2$ defined by P is

$$C = \{(x, y) \in \mathbb{C}^2 \ : \ P(x, y) = 0\}.$$

Example 76
The set $C = \{(x, y) \in \mathbb{C}^2 \ : \ x^2 - 3xy + 2y^2 = 0\}$ is a complex algebraic curve defined by $X^2 - 3XY + 2Y^2$.

Remark 11
If a polynomial $P(X, Y)$ factors as $P(X, Y) = Q(X, Y)R(X, Y)$, then the curve defined by P is the union of the curves defined by Q and R.

Definition 70 (Components of a curve)
Given a polynomial $P(X, Y)$, the curves defined by its irreducible factors are said to be the *components* of the curve defined by P.

Example 77
The curves $C_1 = \{(x, y) \in \mathbb{C}^2 \ : \ x - y = 0\}$ and $C_2 = \{(x, y) \in \mathbb{C}^2 \ : \ x - 2y = 0\}$ are the components of curve C in Example 76.

Definition 71 (Degree of a curve)
The *degree* of a curve C defined by $P(X, Y)$ is the degree of P.

Definition 72 (Singular point)
A point $(a, b) \in C$ is called a *singular point* of C if

$$\frac{\partial P}{\partial X}(a, b) = 0 = \frac{\partial P}{\partial Y}(a, b).$$

The curve C is called *nonsingular* if its set of singular points is empty.

Example 78
The point $(0, 0)$ is a singular point of $C = \{(x, y) \in \mathbb{C}^2 \ : \ x^2 - 3xy + 2y^2 = 0\}$. This is because $(0, 0) \in C$ and it is a zero of the two partial derivatives of $P = X^2 - 3XY + 2Y^2$:

$$\frac{\partial P}{\partial X} = 2X - 3Y \qquad \text{and} \qquad \frac{\partial P}{\partial Y} = -3X + 4Y.$$

Definition 73 (Complex projective plane)
The *complex projective plane* $\mathbb{P}^2(\mathbb{C})$ is the quotient of $\mathbb{C}^3 \backslash \{0\}$ under the equivalence relation

$$(x, y, z) \sim (\lambda x, \lambda y, \lambda z), \quad \lambda \in \mathbb{C}^*.$$

The equivalence class of a point (x, y, z) is denoted by $[x, y, z]$.

Let us now define the following subset of $\mathbb{P}^2(\mathbb{C})$:

$$U = \{[x, y, z] \in \mathbb{P}^2(\mathbb{C}) \ : \ z \neq 0\},$$

and consider the mapping $\phi : U \to \mathbb{C}^2$ defined as

$$\phi[x, y, z] \mapsto \left(\frac{x}{z}, \frac{y}{z}\right).$$

The mapping ϕ is a homeomorphism between U and $\mathbb{C}^2$, hence, $\mathbb{C}^2$ is embedded in $\mathbb{P}^2(\mathbb{C})$.

The points in the complement of U in $\mathbb{P}^2(\mathbb{C})$, *i.e.* $\{[x, y, z] \in \mathbb{P}^2(\mathbb{C}) \ : \ z = 0\}$ are the *points at infinity.*

Definition 74 (Complex projective curve in $\mathbb{P}^2(\mathbb{C})$)
Let $P(X, Y, Z)$ be a nonconstant homogeneous polynomial in three variables with complex coefficients. The *projective curve* $\tilde{C}$ defined by P is

$$\tilde{C} = \{[x, y, z] \in \mathbb{P}^2(\mathbb{C}) \ : \ P(x, y, z) = 0\}.$$

Remark 12
Given a projective curve $\tilde{C}$ in $\mathbb{P}^2(\mathbb{C})$ defined by an homogeneous polynomial $P(X,Y,Z)$ we can compute its intersection with $\mathbb{C}^2$ by considering its points $[x,y,z]$ satisfying $z \neq 0$. This intersection is a curve C defined by the polynomial in two variables $P(X,Y,1)$.

Remark 13
Let $Q(X,Y)$ be a polynomial of degree d given by,

$$Q(X,Y) = \sum_{r+s \leq d} a_{r,s} X^r Y^s$$

and let C be the affine curve defined by Q. The curve C is the intersection of $\mathbb{C}^2$ with the projective curve $\tilde{C}$ defined by the homogeneous polynomial

$$Z^d Q\left(\frac{X}{Z}, \frac{X}{Z}\right) = \sum_{r+s \leq d} a_{r,s} X^r Y^s Z^{d-r-s}.$$

Example 79
Let us consider the *affine* curve defined by polynomial

$$Q(X,Y) = Y^2 - 4X^3 + g_2 X + g_3,$$

that is,

$$C = \{(x,y) \in \mathbb{C} \times \mathbb{C} : y^2 = 4x^3 - g_2 x - g_3\}.$$

Now we can construct the *projective* curve $\tilde{C}$ from the polynomial

$$Z^3 Q\left(\frac{X}{Z}, \frac{Y}{Z}\right) = Y^2 Z - 4X^3 + g_2 X Z^2 + g_3 Z^3.$$

This curve is given by

$$\tilde{C} = \{[x,y,z] \in \mathbb{P}^2(\mathbb{C}) : y^2 z = 4x^3 - g_2 x z^2 - g_3 z^3\}.$$

We can identify the points $[x,y,z] \in \tilde{C}$ with $z \neq 0$ with the points $(x,y) \in C$ via the homeomorphism

$$\phi([x,y,z] = \left(\frac{x}{z}, \frac{y}{z}\right).$$

The curve $\tilde{C}$ has an additional *point at infinity* which is $[0,1,0]$.

Remark 14
In Section 5.3 we will see that the points of an elliptic curve can be endowed with an Abelian group structure in which the point at infinity is the identity element.

The next proposition is an important result regarding the topology of complex projective curves. It includes the definition of *genus*:

Proposition 5. *A nonsingular complex projective curve of degree d in $\mathbb{P}^2(\mathbb{C})$ is topologically a sphere with g handles, where the* genus g *satisfies the* degree-genus *formula*

$$g = \frac{1}{2}(d-1)(d-2).$$

Remark 15
The genus of a nonsingular *cubic* curve (its degree is $d = 3$) is $g = 1$. Hence, such curves are topologically a torus.

Prior to the end of this section, we focus our attention on a particular type of projective curves, which are those defined by a degree three polynomial. The following result [13, Ex. 3.11] is of great importance for Chapter 5 since it introduces the so called *Weierstrass equation* of an elliptic curve.

Proposition 6. *A nonsingular projective curve of degree three is equivalent under a projective transformation to one defined by*

$$Y^2Z = 4X^3 - g_2XZ^2 - g_3Z^3,$$

where $(g_2)^3 - 27(g_3)^2 \neq 0$.

4.2 Algebraic geometry

In this section, some basic concepts about algebraic geometry are introduced. The possibility to associate the *closed points* of the projective line or an algebraic curve with *valuation rings* is explained. For a complete account on algebraic geometry, the reader is referred to [18].

4.2.1 The projective line

We begin by recalling the concept of *valuation* previously introduced in Definition 17 for the particular case $G = \mathbb{Z}$, in which case it is called a *discrete valuation*.

Definition 75 (Valuation)
Let K be a field and let G be a totally ordered Abelian group. A *valuation* of K with values in G is a map $v : K^* \to G$ such that for all $x, y \in K$, $x, y \neq 0$, we have

1. $v(xy) = v(x) + v(y)$,
2. $v(x + y) \geq \min(v(x), v(y))$.

The set $R = \{x \in K \ : \ v(x) \geq 0\} \cup \{0\}$ is called a *valuation ring* of v and the subset $m = \{x \in k \ : \ v(x) > 0\} \cup \{0\}$ is the only maximal ideal of R, therefore (R, m) is a *local ring*. The quotient R/m, which is a field (m is maximal, see Definition 12), is called the *residue field*.

Next, some examples are given. The first one, was already given in Example 19 (p. 26).

Example 80
Let $a \in \mathbb{F}_{q^m}$, $m \geq 1$ and let $f = \frac{p(X)}{q(X)}$ be a rational function in $\mathbb{F}_q(X)$. We can represent f as

$$f = \frac{r(X)}{s(X)}(X - a)^e$$

so that $r, s, (X - a)$ are coprime polynomials in $\mathbb{F}_{q^m}[X]$. Here we can define the discrete valuation $v_a(f) = e$. In this particular example, the valuation ring (also called a *place*) of v_a is the set

$$R = \left\{ f = \frac{p(X)}{q(X)} \in \mathbb{F}_{q^m}(X) \quad : q(a) \neq 0 \right\},$$

and the maximal ideal of R is

$$m = \left\{ f = \frac{p(X)}{q(X)} \in \mathbb{F}_{q^m}(X) \quad : \quad q(a) \neq 0, \quad p(a) = 0 \right\}.$$

Example 81
Let $p(X) \in k[X]$ be an irreducible polynomial. We can define a discrete valuation associated to $p(X)$ as

$$v_p : k(X)^* \to \mathbb{Z}$$

$$f \mapsto e,$$

where f is represented as a quotient of polynomials

$$f = \frac{r(X)}{s(X)} p(X)^e$$

where r, s and p are relatively prime polynomials.

Example 82
If in the previous example we take $p(X) = X^2 + 3 \in \mathbb{Z}_5[X]$, then the associated valuation ring R can be described as

$$R = \left\{ \frac{r(X)}{s(X)} \ : \ r, s \in \mathbb{Z}_5[X], \ \ r, s \ \text{ coprime, and } \ (X^2 + 3) \nmid s \right\}.$$

Definition 76 (Closed points of the affine line)
Let $k = \mathbb{F}_q$ be a finite field. The monic irreducible polynomials in $k[X]$ of degree d in the indeterminate X will be called the *closed points of the affine line* $\mathbb{A}^1(k)$ *rational over* k *and of degree* d.

Definition 77 (Degree of a point)
If the closed point $P \in \mathbb{A}^1(k)$ corresponds to the polynomial $f(X)$ and $\deg f = d$, we will write

$$\deg P = \deg f = d.$$

Example 83
The degree 1 points of $\mathbb{A}^1(\mathbb{Z}_5)$ correspond to the degree 1 polynomials in $\mathbb{Z}_5[X]$. They are:

$$\{X,\ \ X+1,\ \ X+2,\ \ X+3,\ \ X+4\}.$$

The degree 2 points of $\mathbb{A}^1(\mathbb{Z}_5)$ are the irreducible degree 2 polynomials in $\mathbb{Z}_5[X]$. They are:

$$\{X^2+2,\ \ X^2+3,\ \ X^2+X+1,\ \ X^2+X+2,\ \ X^2+2X+3,\ \ X^2+2X+4,$$

$$X^2+3X+3,\ \ X^2+3X+4,\ \ X^2+4X+1,\ \ X^2+4X+2\}.$$

Next we will see that we can associate each closed point of the affine line with a discrete valuation ring. The following definition is possible since the ring of polynomials $k[X]$ is a unique factorization domain.

Next, for each closed point of $\mathbb{A}^1(k)$ we define the following discrete valuation that takes as input an element of the field of rational functions of k, *i.e.* $k(X)$.

Definition 78 (Valuation of a closed point of $\mathbb{A}^1(k)$)
Let $P \in \mathbb{A}^1(k)$ and let $p(X)$ be the monic irreducible polynomial corresponding to P. The valuation v_P is defined as in Example 81 considering the polynomial $p(X)$.

Example 84
Let us consider the closed point $P \in \mathbb{A}^1(\mathbb{Z}_5)$ corresponding to polynomial X^2+3. Next, let f be the following rational function in $\mathbb{Z}_5(X)$:

$$f = \frac{X^5+X^4+X^3+X^2+4X+4}{X^2+1}$$

In this case $v_P(f) = 2$ since,

$$f = \frac{(X+1)}{(X+2)(X+3)}(X^2+3)^2.$$

Definition 79 (Valuation ring of a closed point of $\mathbb{A}^1(k)$)
Let $P \in \mathbb{A}^1(k)$, the discrete valuation ring associated to P is

$$R_P = \{f \in k(X) \ : \ v_P(f) \geq 0\},$$

whose maximal ideal is

$$m_P = \{f \in k(X) \ : \ v_P(f) > 0\},$$

and the *residue class field* associated to P is R_P/m_P.

Example 85
If $P \in \mathbb{A}^1(\mathbb{Z}_5)$ corresponds to polynomial $X^2 + 3$, then the valuation ring R_P is, as we saw in Example 82:

$$R_P = \left\{ \frac{r(X)}{s(X)} \ : \ r, s \in \mathbb{Z}_5[X], \ \ r, s \ \text{ coprime, and } \ (X^2+3) \nmid s \right\},$$

the maximal ideal of R_P is

$$m_P = \left\{ \frac{r(X)}{s(X)} \ : \ r, s \in \mathbb{Z}_5[X], \ \ r, s \ \text{ coprime, and } \ (X^2+3) \mid r \right\},$$

and the corresponding residue class field is

$$k_P = R_P/m_P = \left\{ \frac{aX+b}{s(X)} \ : \ a, b \in \mathbb{Z}_5, \ \text{ and } \ (X^2+3) \nmid s \right\}.$$

Definition 80 (Projective line $\mathbb{P}^1(k)$)
The *projective line* $\mathbb{P}^1(k)$ is obtained by adding to the affine line $\mathbb{A}^1(k)$ a point at infinity. That is,

$$\mathbb{P}^1(k) = \mathbb{A}^1(k) \cup \{\infty\}.$$

Remark 16
The projective line $\mathbb{P}^1(\mathbb{R})$ is topologically equivalent to a circle.

Remark 17
The projective line $\mathbb{P}^1(\mathbb{C})$ is topologically equivalent to a sphere, known as the *Riemann sphere*.

Previously, we have associated a polynomial to each closed point of $\mathbb{A}^1(k)$. The projective line has an additional point at infinity. Next we will assign a rational function to it. More precisely,

$$p_\infty(X) = 1/X.$$

Definition 81 (Valuation of the point at infinity)
Let $f(X) = s(X)/r(X)$ be the quotient of two polynomials in $k[X]$. We define the valuation v_∞ as

$$v_\infty(f) = \deg r - \deg s.$$

The discrete valuation ring associated to ∞ is

$$R_\infty = \{f \in k(X) \ : \ v_\infty(f) \geq 0\}.$$

Example 86
Let us consider the point at infinity in $\mathbb{P}^1(\mathbb{Z}_5)$, and let

$$f = \frac{X^5 + X^4 + X^3 + X^2 + 4X + 4}{X^2 + 1}.$$

Then $v_\infty(f) = -3$.

Theorem 9. *The only discrete valuations of $k(X)$ are v_P where P is a monic irreducible polynomial in $k[X]$ and v_∞.*

From the previous theorem, if we consider a finite field k, the closed points on the projective line $\mathbb{P}^1(k)$, rational over k, correspond in a one-to-one manner to the discrete valuations of $k(X)$, the field of rational functions in the transcendental element T. Rational functions play a fundamental role in the theory of algebraic curves. As we will see next in Definition 84, employing divisors we will be able to associate a set of points of the projective line (valuation rings) to any given rational function.

Definition 82 (Divisor on the projective line)
A *divisor* on the projective line $\mathbb{P}^1(k)$ is a formal sum of points with integral coefficients. Hence, a divisor D is an expression of the form

$$D = \sum_P m_P P,$$

where the sum is over all closed points of $\mathbb{P}^1(k)$, and the integers m_P are all, except for a finite number, equal to 0.

Example 87
Let the closed points $P, Q \in \mathbb{P}^1(\mathbb{Z}_5)$ correspond to X^2+3 and $X+1$, respectively. Then,

$$D = 3P + 2Q$$

is a divisor on $\mathbb{P}^1(\mathbb{Z}_5)$.

Given two divisors D and D', we say that $D \geq D'$ if all the corresponding coefficients satisfy $m_P \geq n_P$.

Definition 83 (Degree of a divisor)
Let $D = \sum_P m_P P$ be a divisor on $\mathbb{P}^1(k)$. The *degree* of D is the integer

$$\deg D = \sum_P m_P \deg P.$$

Example 88
Let the closed points $P, Q \in \mathbb{P}^1(\mathbb{Z}_5)$ correspond to X^2+3 and $X+1$, respectively. If $D = 3P + 2Q$, then

$$\deg D = 3 \deg P + 2 \deg Q = 3 \cdot 2 + 2 \cdot 1 = 8.$$

Definition 84 (Divisor associated to a rational function)
Given a rational function $f \in k(X)$ we define the *divisor associated to* f as

$$(f) = \sum_P v_P(f) P.$$

Example 89
Let us consider the rational function $f = \frac{X^5+X^4+X^3+X^2+4X+4}{X^2+1}$ in $\mathbb{Z}_5(X)$. Since

$$f = \frac{(X^2+3)^2(X+1)}{(X+2)(X+3)},$$

then,

$$(f) = 2P + Q - R - T - 3\infty,$$

where P, Q, R, T are closed points corresponding to X^2+3, $X+1$, $X+2$, $X+3$, respectively.

Definition 85 (Principal divisor)
A divisor D which is of the form $D = (f)$ for some rational function f is called *principal*. The degree of a principal divisor is 0.

Definition 86 (Linear space associated with a divisor)
Let D be a divisor on $\mathbb{P}^1(k)$. The *linear space associated with* D is

$$L(D) = \{f \in k(T) \ : \ (f) + D \geq 0\} \cup \{0\}.$$

We define $l(D) = \dim_k L(D)$.

Theorem 10. *Let D be a divisor on $\mathbb{P}^1(k)$. We have $l(D) = \deg D + 1$.*

4.2.2 Algebraic curves

We have just seen how to associate the points of the projective line to valuation rings. In this section, we will do the same considering the points of an algebraic curve.

Definition 87 (Plane affine algebraic curve)
Let k be a field, and let f be a polynomial in $k[X, Y]$. A *plane affine algebraic curve* is given by:

$$C = \{(x, y) \in K^2 \ : \ f(x, y) = 0\}$$

where K is an algebraically closed extension of k.

Definition 88 (Coordinate ring of a curve)
Let f be a polynomial in $k[X, Y]$ which is absolutely irreducible (it remains irreducible over any finite extension of k). Under this condition, the curve

$$C : f(x, y) = 0$$

is connected. Let us denote by $\langle f \rangle$ the principal ideal in $k[X, Y]$ generated by f. The *coordinate ring* of the curve C is defined as

$$R = k[X, Y]/\langle f \rangle .$$

Definition 89 (Function field of a curve)
Let R be the coordinate ring of the curve C. The field of fractions of R is the *function field* $K = k(C)$ of the curve C.

Remark 18
An alternative definition (focused on complex numbers) of the function field of a curve was given in Example 46. We recall it here in a more general form. Let $f \in k[X, Y]$ be an irreducible polynomial, and consider the curve

$$C : f(x, y) = 0.$$

Any rational function

$$R(X, Y) = P(X, Y)/Q(X, Y),$$

where P and Q are polynomials, is declared to be zero whenever P but not Q is divisible by f. We place in one class all the rational functions which differ by zero from a given one. This collection of equivalence classes is a field. This is the *function field* of curve C.

Example 90
Let us consider the polynomial $f = Y^2 - Y - X^2 - 2$ defined over $\mathbb{Z}_5$, and let C be the curve defined by f. In the function field of C, the rational functions

$$R(X, Y) = 3X^2 + Y,$$

and

$$R'(X, Y) = 2X^2 + Y^2 - 2,$$

are in the same class.

The following definition is a generalization of Definition 76.

Definition 90 (Closed point of a curve)
A discrete valuation ring (R_v, m_v) of the function field $K = k(C)$ is called a *closed point* of C.

Definition 91 (Degree of a closed point)
Let $P_v = (R_v, m_v)$ be a closed point of curve C. If $k_v = R_v/m_v$ denotes the residue class field of P_v then we define the *degree* of P_v as

$$\deg(P_v) = [k_v : k].$$

Since the function field $K = k(C)$ of a curve is the field of fractions of the coordinate ring $k[X,Y]/\langle f\rangle$, any element $g \in K$ can be represented as a quotient

$$g = \frac{A(X,Y)}{B(X,Y)}, \qquad A, B \in k[X,Y].$$

Let $P = (\alpha, \beta)$ so that $f(\alpha, \beta) = 0$. With the point P we can associate the ring

$$R = \left\{ g \in K \ : \ g = \frac{A(X,Y)}{B(X,Y)},\ B(\alpha,\beta) = 0 \right\}$$

and

$$m = \left\{ g \in R \ : \ g = \frac{A(X,Y)}{B(X,Y)},\ A(\alpha,\beta) = 0 \right\}$$

If (α, β) is a simple (non-singular) point of C, then the pair (R, m) is a discrete valuation ring and $P_v = (R, m)$ is the closed point corresponding to $P = (\alpha, \beta)$.

Conversely, if $P_v = (R_v, m_v)$ is a closed point of degree one, the maximal ideal m_v as an ideal in $k[X,Y]/\langle f\rangle$ must be of the form $m_v = \langle X - \alpha, Y - \beta\rangle$, with $\alpha, \beta \in k$ and $f(\alpha, \beta) = 0$. When $P = (\alpha, \beta)$ is not a simple point, there may be several closed points on $k(C)$ corresponding to P.

Our objective is to view an algebraic curve C as a covering of the projective line $\mathbb{P}^1$. The following theorem addresses the extension of valuation rings in the function field of $\mathbb{P}^1$ to the function field of curve C.

Theorem 11. *Let K be the function field of a curve C, and let k be the field of constants. Let A be a subring of K containing k and m_A an ideal in A, such that, $m_A \neq A, \{0\}$. Then there exists a valuation ring B of K with maximal ideal m_B and satisfying $m_A \subset m_B \cap A$.*

Let K be the function field of a curve C defined over a field k, and let A be a valuation ring in K (a point of C) such that $k \subset A$, then $A \cap k(X)$ is a valuation ring of $k(X)$ so that it is a point of $\mathbb{P}^1(k)$.

Reversely, given a valuation ring in $k(X)$ (a point of $\mathbb{P}^1(k)$), Theorem 11 states that it can be extended to a valuation ring of K which is associated to a point of a curve C with function field K.

Example 91
Let us consider again the polynomial $f = Y^2 - Y - X^2 - 2$ defined over $\mathbb{Z}_5$, and let C be the curve defined by f. In $\mathbb{Z}_5$, the points of C are:

$$\{(0,2),(0,4),(2,3),(3,3)\}$$

Now, we extend $\mathbb{Z}_5$ by considering a root α of X^2+2, that is $\mathbb{Z}_5(\alpha)$. Here, the points of C are:

$$\{(0,2),(0,4),(1,2\alpha+3),(1,3\alpha+3),(2,3),(3,3),(4,2\alpha+3),(4,3\alpha+3),$$
$$(\alpha,0),(\alpha,1),(\alpha+2,2\alpha+4),(\alpha+2,3\alpha+2),(\alpha+3,2\alpha+2),(\alpha+3,3\alpha+4),$$
$$(2\alpha,\alpha+3),(2\alpha,4\alpha+3),(3\alpha,\alpha+3),(3\alpha,4\alpha+3),(4\alpha+2,2\alpha+2),(4\alpha+2,3\alpha+4),$$
$$(4\alpha+3,2\alpha+4),(4\alpha+3,3\alpha+2),(4\alpha,0),(4\alpha,1)\}$$

Definition 92 (Divisor on a curve)
A divisor on a curve C, rational over k, is a formal linear combination

$$D = \sum_P m_P P,$$

of closed points P with integral coefficients m_P all of which, except for a finite number, are zero. The set of all divisors on a curve C is denoted by $\mathrm{Div}(C)$. The *degree* of a divisor D is defined as

$$\deg D = \sum_P m_P \deg P.$$

Definition 93 (Divisor of a function and divisor of a differential)
The *divisor of a function* $f \in K(C)$ is

$$(f) = \sum_P \mathrm{ord}_P(f) P.$$

The *divisor of a differential* $\omega \in \Omega_C$ is

$$(\omega) = \sum_P \mathrm{ord}_P(\omega) P.$$

Definition 94 (Canonical class)
Let C be a curve, the *canonical class* is the set of divisors

$$W = \{(\omega) \in \mathrm{Div}(C) \ : \ \omega \in \Omega_C\}.$$

Definition 95 (Genus of a curve)
Let C be a curve and let $\omega \in \Omega_C$. Let $\deg \omega = 2g - 2$. We define the *genus* of C to be g.

This section is concluded with the statement of the Riemann-Roch theorem. The reader is referred to Definition 86 for a definition of function l.

Theorem 12. *Let D be a divisor on a curve C of genus g and $W = (\omega)$ the divisor of a differential. Then we have*

$$l(D) = \deg D + 1 - g + l(W - D).$$

Chapter 5

Elliptic complex curves

Elliptic curves defined over finite fields are widely used in cryptography and primality testing. In cryptography, we need elliptic curves with a cardinality divisible by a large prime, so that algorithms for finding such curves are required. In this thesis two algorithms for finding elliptic curves with a given cardinality have been studied. Both of them are based on computing the roots of the *Hilbert class polynomial* modulo a prime. The underlying theory of these methods comes from elliptic curves defined complex numbers. This chapter is an introduction to elliptic functions and complex multiplication. The last section is devoted to curves over finite fields. The reader is referred to [6] and [12] for a more detailed exposition.

5.1 Lattices

This section is devoted to the introduction of some basic concepts: *lattice*, *elliptic function* and *j-invariant*.

Definition 96 (Lattice)
We define a *lattice* as an additive subgroup L of $\mathbb{C}$ which is generated by two complex numbers ω_1 and ω_2 which are linearly independent over $\mathbb{R}$. It is denoted

$$L = [\omega_1, \omega_2] .$$

Example 92
The lattice $L = [3, i]$ is the following set of complex numbers:

$$L = \{3m + in : m, n \in \mathbb{Z}\} .$$

Definition 97 (Homothetic lattices)
Two lattices L and L' are said to be *homothetic* if there is a nonzero complex number λ such that $L' = \lambda L$. *Homotheticity* is an equivalence relation.

Example 93
Lattices $L = [2+i, 3-i]$ and $L' = [-1+2i, 1+3i]$ are homothetic since

$$L = \{(2+i)m + (3-i)n : m, n \in \mathbb{Z}\}$$

and by taking $\lambda = i$, we get

$$iL = \{(2+i)im + (3-i)in : m, n \in \mathbb{Z}\} =$$

$$= \{(-1+2i)m + (1+3i)n : m, n \in \mathbb{Z}\} = L'.$$

The generators of both lattices are shown graphically in Figure 5.1. The generators of homothetic lattices define parallelograms having the same shape (maybe at a different scale).

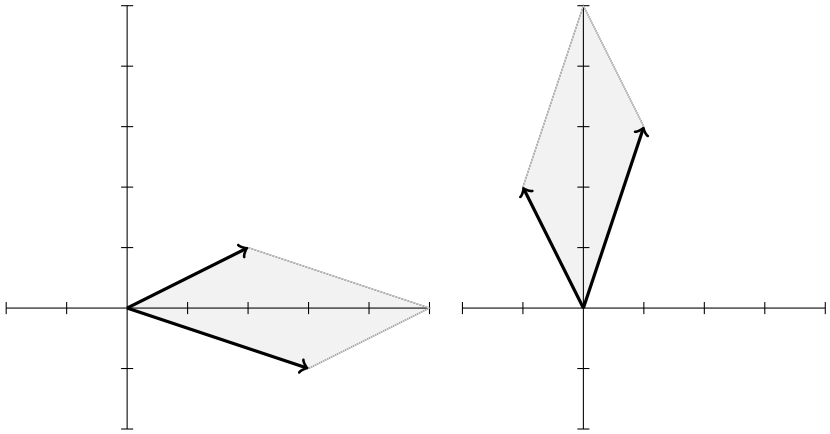

Figure 5.1: Generators of lattices L (left) and L' (right) plotted as vectors over $\mathbb{C}$ and the parallelograms they define.

Definition 98 (Elliptic function)
An *elliptic function* for a lattice L is a function $f(z)$ defined on $\mathbb{C}$, except for isolated singularities, which satisfies the following two conditions:

1. $f(z)$ is meromorphic on $\mathbb{C}$.
2. $f(z+\omega) = f(z)$ for all $\omega \in L$.

Definition 99 (Weierstrass $\wp$-function)
Given a lattice L and $z \in \mathbb{C} \backslash L$, we define the Weierstrass $\wp$-function as,

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

The function $\wp(z;L)$ is elliptic for L and has double poles at the points of L. When the lattice L is fixed, we will write $\wp(z)$ instead of $\wp(z;L)$.

The next theorem is of great importance since, as we will see in Section 5.3, it provides a way to relate lattices and algebraic curves defined over the complex numbers.

Theorem 13. *The Weierstrass function $\wp(z)$ satisfies the following differential equation*

$$\wp'(z)^2 = 4\wp^3(z) - g_2(L)\wp(z) - g_3(L),$$

where

$$g_2(L) = 60 \sum_{\omega \in L - \{0\}} \frac{1}{\omega^4},$$

and

$$g_3(L) = 140 \sum_{\omega \in L - \{0\}} \frac{1}{\omega^6}.$$

Next, we introduce the concept of j-invariant of a lattice. Its importance arises from the fact that it permits to determine whether two lattices are homothetic or not.

Definition 100 (j-invariant)
The *j-invariant* of a lattice L is defined as

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

Theorem 14. *Given two lattices L and L', then $j(L) = j(L')$ if and only if L and L' are homothetic.*

Given a lattice $L = [\omega_1, \omega_2]$, we can take $\lambda = \omega_1^{-1}$. Then,

$$L' = \lambda L = [1, \omega_1^{-1}\omega_2] = [1, \tau],$$

with $\tau \in \mathbb{C} \backslash \mathbb{R}$. In a similar manner, we can take $\lambda = \omega_2^{-1}$ and, in this case,

$$L'' = \lambda L = [\omega_1 \omega_2^{-1}, 1] = [1, \omega_1 \omega_2^{-1}] = [1, \tau^{-1}].$$

The lattices L,L' and L'' are homothetic and either τ or τ^{-1} is in the upper half plane $\mathfrak{h} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$. Hence, any lattice L is homothetic to a lattice of the form $[1, \tau]$ with $\tau \in \mathfrak{h}$. For such a τ value, we define

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

Example 94
The lattice $L = [2 + i, 3 - i]$ in Example 93 is homothetic to

$$(3 - i)^{-1} L = \left[\frac{2 + i}{3 - i}, 1\right] = \left[1, \frac{1}{2} + \frac{1}{2}i\right] = [1, \tau],$$

with $\tau = \frac{1}{2} + \frac{1}{2}i \in \mathfrak{h}$. The generators of the resulting lattice are shown graphically in Figure 5.2.

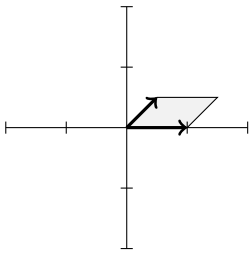

Figure 5.2: Generators of a lattice of the form $[1, \tau]$, with $\tau \in \mathfrak{h}$.

Let us now consider the *modular group* $SL(2, \mathbb{Z})$ composed of all the 2×2 matrices with coefficients in $\mathbb{Z}$ and determinant 1. Given $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{Z})$, the *action of* γ *on* $\tau \in \mathfrak{h}$ is defined as

$$\gamma\tau = \frac{a\tau + b}{c\tau + d}.$$

This action is well defined (an element $\tau \in \mathfrak{h}$ is mapped to $\mathfrak{h}$) and the lattices $[1, \tau]$ and $[1, \gamma\tau]$ are known to be homothetic. Further, two lattices $[1, \tau]$ and $[1, \tau']$ are homothetic if and only if there exists some $\gamma \in SL(2, \mathbb{Z})$ satisfying that $\tau' = \gamma\tau$ (see [6, p.221]).

Remark 19
From Theorem 14 and the previous explanation we conclude that given $\tau, \tau' \in \mathfrak{h}$, there exists $\gamma \in SL(\mathbb{Z}, 2)$ with $\gamma\tau = \tau'$ if and only if $j(\tau) = j(\tau')$.

Example 95 ([6], Exercise 10.17)
Let $\omega = e^{2\pi i/3}$, and let $L = [1, \omega]$. Now we will show that $g_2(L) = 0$ which implies that $j(\omega) = 0$.

The complex number ω can be represented as $\omega = \frac{-1}{2} + i\frac{\sqrt{3}}{2}$. Now we will show that $L' = \omega L = L$. We have that

$$L' = \omega L = \omega[1, \omega] = [\omega, \omega^2] = \left[\frac{-1}{2} + i\frac{\sqrt{3}}{2}, \frac{-1}{2} - i\frac{\sqrt{3}}{2}\right].$$

We will prove $L = L'$ by showing that the two generators of L, namely $1, \omega$ are in L' and the two generators of L', namely ω, ω^2 are in L. Since ω is a generator of both L and L' we simply have to prove that $1 \in L'$ and $\omega^2 \in L$. We can

easily see that $1 \in L'$ since:

$$1 = -\left(\frac{-1}{2} + i\frac{\sqrt{3}}{2}\right) - \left(\frac{-1}{2} - i\frac{\sqrt{3}}{2}\right) = (-1)\omega + (-1)\omega^2 \in L'.$$

In a similar way we can see $\omega^2 \in L$:

$$\omega^2 = \left(\frac{-1}{2} - i\frac{\sqrt{3}}{2}\right) = -1 - \left(\frac{-1}{2} + i\frac{\sqrt{3}}{2}\right) = (-1)1 + (-1)\omega \in L.$$

Once we have proven $L = L'$, we get

$$g_2(L) = g_2(L') = g_2(\omega L) = \frac{1}{\omega^4} g_2(L) = \omega^{-1} g_2(L).$$

Since $\omega^{-1} \neq 1$ we conclude $g_2(L) = 0$.

We can check it in Sage. The result is not exactly 0 due to roundoff inaccuracies.

```
sage:  elliptic_j((-1+i*sqrt(3))/2)
-1.03244741666549e-44 - 1.75569396057967e-47*I
```

The following Theorem (see [6, p.220]) is of great importance. One of its consequences is that the minimum polynomial of the j-invariant of a proper fractional ideal of an order in an imaginary quadratic field has integer coefficients. This theorem shows that a link between the theory of quadratic fields and the theory of elliptic functions does exist. More aspects of the relation between both theories will be presented in the next section.

Theorem 15. *Let $\mathcal{O}$ be an order in an imaginary quadratic field, and let $\mathfrak{a}$ be a proper fractional $\mathcal{O}$-ideal. Then $j(\mathfrak{a})$ is an algebraic integer of degree $h(\mathcal{O})$.*

Proof sketch. Let α be a proper $\mathcal{O}$-ideal which is primitive (it is not of the form $d\mathfrak{p}$ where $d > 1$ is an integer and $\mathfrak{p}$ is a proper $\mathcal{O}$-ideal). It is known that $\alpha\mathfrak{a}$ is a cyclic sublattice of $\mathfrak{a}$ of index $m = N(\alpha)$. Then,

$$0 = \Phi_m(j(\alpha\mathfrak{a}), j(\mathfrak{a})) = \Phi_m(j(\mathfrak{a}), j(\mathfrak{a})),$$

so that $j(a)$ is a root of $\Phi_m(X, X)$ which has integer coefficients ($\Phi_m(X, Y)$ is the m-th modular polynomial). Further, by taking α so that $m = N(\alpha)$ is not a perfect square (such an α always exists), the leading coefficient of $\Phi_m(X, X)$ is ± 1 so that $j(\mathfrak{a})$ is an algebraic integer. For more details, see [6].

Remark 20
The elements composing an ideal in an imaginary quadratic field can be considered as the elements of a lattice. This fact permits to associate a j-invariant to ideals which is precisely what has been done in the previous theorem.

5.2 Complex multiplication

The theory of complex multiplication provides a link between lattices and orders in imaginary quadratic fields. This section is a brief introduction to complex multiplication.

Theorem 16. *The Weierstrass function $\wp(z)$ satisfies the following addition law*

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

provided that $z, w \notin L$ and $z+w \notin L$.

Remark 21
The previous theorem is of great importance since, as we will see at the end of Section 5.3, it allows to endow the points of an elliptic curve with an addition operation that provides a group structure.

By means of some elementary calculus, we can see that,

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

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

From Theorem 13 we know that,

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

Now we derivate that expression with respect to z,

$$2\wp'(z)\wp''(z) = 12\wp^2(z)\wp'(z) - \frac{1}{2}g_2\wp'(z),$$

and we obtain,

$$\wp''(z) = 6\wp^2(z) - \frac{1}{2}g_2.$$

Finally, we obtain that,

$$\wp(2z) = -2\wp(z) + \frac{(12\wp(z)^2 - g_2)^2}{16(4\wp(z)^3 - g_2\wp(z) - g_3)}.$$

Hence, $\wp(2z)$ is a rational function in $\wp(z)$. By induction, one can show that for any positive integer n, $\wp(nz)$ is also a rational function in $\wp(z)$. The following theorem (see [6, p.209]) addresses for which complex numbers $\alpha \in \mathbb{C}$, $\wp(\alpha z)$ is a rational function in $\wp(z)$ and its relation with orders in imaginary fields.

Theorem 17. *Let L be a lattice, and let $\wp(z)$ be the $\wp$-function for L. Given $\alpha \in \mathbb{C} - \mathbb{Z}$, the following statements are equivalent:*

1. *$\wp(\alpha z)$ is a rational function in $\wp(z)$.*
2. *$\alpha L \subset L$.*
3. *There is an order $\mathcal{O}$ in an imaginary quadratic field K such that $\alpha \in \mathcal{O}$ and L is homothetic to a proper fractional $\mathcal{O}$-ideal.*

Remark 22
As a consequence of the previous theorem, if an elliptic function has multiplication by some $\alpha \in \mathbb{C}-\mathbb{Z}$, then it has multiplication by an order $\mathcal{O}$ in an imaginary quadratic field. Since the elements in $\mathcal{O}-\mathbb{Z}$ are not real, we talk about *complex multiplication*. Note that the inclusion $\alpha L \subset L$ is always satisfied when $\alpha \in \mathbb{Z}$.

Example 96
Let us consider the lattice $L = [2, i]$. This lattice does not have complex multiplication by $i = \sqrt{-1}$ since $1 \in iL = [-1, 2i] = [1, 2i]$ but $1 \notin L$, hence $iL \not\subset L$.

Example 97
Let us consider $L = [2, i]$ again. This lattice has complex multiplication by $2i$. This is because $2iL = [4i, -2] = [2, 4i] \subset [2, i] = L$.

As a consequence, L has complex multiplication by complex numbers in the set $\mathcal{O} = \{m + (2i)n \ : \ m, n \in \mathbb{Z}\}$. The set $\mathcal{O}$ is the order with conductor 2 in $\mathbb{Z}[i]$, *i.e.* the ring of integers of $\mathbb{Q}(i)$.

Given an order $\mathcal{O}$ in an imaginary quadratic field, it is known [6, Ex. 10.15] that two proper fractional $\mathcal{O}$-ideals are homothetic as lattices if and only if they determine the same class in the ideal class group $C(\mathcal{O})$. This consideration together with Theorem 17 permits to enunciate the following corollary.

Corollary 2. *Let $\mathcal{O}$ be an order in an imaginary quadratic field. Then there is a one-to-one correspondence between the ideal class group $C(\mathcal{O})$ and the homotheticity classes of lattices with $\mathcal{O}$ as their full ring of complex multiplication.*

The last part of this section presents some results relating the j-invariant of a lattice with Hilbert class fields.

Theorem 18. *Let $\mathcal{O}$ be an order in an imaginary quadratic field K, and let $\mathfrak{a}$ be a proper fractional $\mathcal{O}$-ideal. Then the j-invariant $j(\mathfrak{a})$ is an algebraic integer and $K(j(\mathfrak{a}))$ is the ring class field of the order $\mathcal{O}$.*

Corollary 3. *If K is an imaginary quadratic field, then $K(j(\mathfrak{O}_K))$ is the Hilbert class field of K.*

Given an order $\mathcal{O}$ in an imaginary quadratic field K, $H_{\mathcal{O}}(X)$ denotes the monic minimal polynomial of $j(\mathcal{O})$ over $\mathbb{Q}$. Since $j(\mathcal{O})$ is an algebraic integer, $H_{\mathcal{O}}(X)$ has integer coefficients. The equation $H_{\mathcal{O}}(X) = 0$ is called the *class equation*. When $\mathcal{O} = \mathfrak{O}_K$, for some imaginary quadratic field K, $H_{\mathcal{O}}(X)$ is called the *Hilbert class polynomial* (see Definition 57).

Since an order $\mathcal{O}$ is determined by its discriminant D, sometimes $H_D(X)$ is written instead of $H_{\mathcal{O}}(X)$.

Proposition 7. *Let $\mathcal{O}$ be an order in an imaginary quadratic field K, and let $\mathfrak{a}_i$, $i = 1, \ldots, h$ be the ideal class representatives. Then the class equation is given by the formula,*

$$H_{\mathcal{O}}(X) = \prod_{i=1}^{h} (X - j(\mathfrak{a}_i)).$$

Remark 23
This formula is employed by the methods implemented in Section 6 for constructing Hilbert class polynomials.

Example 98
Let $K = \mathbb{Q}(\sqrt{-15})$. From Example 73, we know the ideal class representatives of $C(\mathfrak{O}_K)$ are given by

$$\left\{ \left[1, \frac{-1+\sqrt{-15}}{2}\right], \ \left[2, \frac{-1+\sqrt{-15}}{2}\right] \right\}.$$

From the j-invariants j_1, j_2 of the lattices related to each class representative we will be able to compute the Hilbert class polynomial for the ring of integers of $K = \mathbb{Q}(\sqrt{-15})$ as,

$$H_{\mathfrak{O}_K}(X) = (X - j_1)(X - j_2).$$

Regarding $\left[1, \frac{-1+\sqrt{-15}}{2}\right]$, its j-invariant is $j\left(\frac{-1+\sqrt{-15}}{2}\right)$.

Regarding the ideal $\left[2, \frac{-1+\sqrt{-15}}{2}\right]$ when considered as a lattice, it is homothetic to $\left[1, \frac{-1+\sqrt{-15}}{4}\right]$, so that its j-invariant is $j\left(\frac{-1+\sqrt{-15}}{4}\right)$.

Both computations are shown next:

```
sage:  elliptic_j((-1+sqrt(-15))/2)
-191657.832862547 + 1.34167142884203e-10*I
```

```
sage:  elliptic_j((-1+sqrt(-15))/4)
632.832862547208 + 1.06470772211784e-13*I
```

Next we show the commands required to compute the Hilbert class polynomial for the ring of integers of $K = \mathbb{Q}(\sqrt{-15})$. As it can be seen, the obtained polynomial does not have integer coefficients due to the limited accuracy of computations. To solve it, we have rounded the coefficients of the obtained polynomial to their closest integers.

```
sage:  Q=PolynomialRing(QQ,'x')
sage:  x=Q.gen()
sage:  H=(x-elliptic_j((-1+sqrt(-15))/2)) *
(x-elliptic_j((-1+sqrt(-15))/4))
sage:  H
x^2 + (191025.000000000 - 1.34273611115879e-10*I)*x -
1.21287375000000e8 + 6.44999077307861e-8*I
sage:  HH=x^2 + int(H[1].real())*x + int(H[0].real())
sage:  HH
x^2 + 191025*x - 121287375
```

As a result, we have obtained that for $K = \mathbb{Q}(\sqrt{-15})$,

$$H_{\mathfrak{O}_K}(X) = X^2 + 191025X - 121287375.$$

Sage provides a procedure that generates the Hilbert class polynomial given the discriminant of K. We can use it to check our computations:

```
sage:  hilbert_class_polynomial(-15)
x^2 + 191025*x - 121287375
```

5.3 Elliptic curves over complex numbers

Theorem 13 states that the Weierstrass $\wp$-function satisfies a differential equation. That equation provides a link between lattices and a particular type of algebraic curves, *i.e.* elliptic curves.

Definition 101 (Elliptic curve over $\mathbb{C}$)
An *elliptic curve* E over $\mathbb{C}$ is an equation of the form

$$Y^2 = 4X^3 - g_2X - g_3,$$

where $g_2, g_3 \in \mathbb{C}$ and $\triangle = g_2^3 - 27g_3^2 \neq 0$.

Remark 24
Curves of this form were introduced in Example 79.

Remark 25
This equation is known as the *Weierstrass equation of* E. The condition $\triangle \neq 0$ is for ensuring the curve does not have singular points.

Definition 102 ($E(\mathbb{C})$)
Given an elliptic curve E over $\mathbb{C}$, we define $E(\mathbb{C})$ to be the set of solutions

$$E(\mathbb{C}) = \{(x, y) \in \mathbb{C} \times \mathbb{C} : y^2 = 4x^3 - g_2 x - g_3\} \cup \{\infty\}.$$

Remark 26
The extra point $\{\infty\}$ appears when the elliptic curve is considered in the projective space $\mathbb{P}^2(\mathbb{C})$ (see Section 4.1).

Let $L \subset \mathbb{C}$ be a lattice. Theorem 13 states that its $\wp(z)$-function satisfies

$$\wp'(z)^2 = 4\wp^3(z) - g_2(L)\wp(z) - g_3(L).$$

Hence, when $z \notin L$, the pair $(\wp(z), \wp'(z))$ satisifies the equation

$$Y^2 = 4X^3 - g_2(L)X - g_3(L).$$

This provides a well-defined mapping

$$(\mathbb{C} - L)/L \to E(\mathbb{C}) - \{\infty\}.$$

By sending $z \in L$ to ∞, we obtain a bijection,

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

We can see that the differential equation of the $\wp$-function of a lattice gives us an elliptic curve. The following proposition states that every elliptic curve over $\mathbb{C}$ arises from a unique $\wp$-function.

Proposition 8. *Let E be an elliptic curve over $\mathbb{C}$ given by equation*

$$Y^2 = 4X^3 - g_2 X - g_3, \quad g_2, g_3 \in \mathbb{C}, \quad g_2^3 - 27g_3^2 \neq 0,$$

then there is a unique lattice $L \subset \mathbb{C}$ such that,

$$g_2 = g_2(L), \;\; g_3 = g_3(L).$$

Since an elliptic curve E over $\mathbb{C}$ is uniquely related to a lattice L, we can define its j-invariant as $j(E) = j(L)$. More precisely,

Definition 103 (j-invariant)
Given an elliptic curve $E : Y^2 = 4X^3 - g_2X - g_3$, the *$j$-invariant* of E is defined to be the number

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

Definition 104 (Isomorphic elliptic curves)
Two elliptic curves $E : Y^2 = 4X^3 - g_2X - g_3$ and $E' : Y^2 = 4X^3 - g_2'X - g_3'$ are *isomorphic over* $\mathbb{C}$ if there is a nonzero $c \in \mathbb{C}$ such that

$$g_2' = c^4 g_2,$$
$$g_3' = c^6 g_3.$$

Let us consider a point $(x, y) \in E(\mathbb{C})$, *i.e.* it satifies the curve equation $y^2 = 4x^3 - g_2x - g_3$. Multiplying both sides of the equation by c^6 we get

$$c^6y^2 = 4c^6x^3 - g_2c^6x - c^6g_3$$

so that

$$(c^3y)^2 = 4(c^2x)^3 - (c^4g_2)(c^2x) - (c^6g_3)$$

and

$$(c^3y)^2 = 4(c^2x)^3 - g_2'(c^2x) - g_3'.$$

As a consequence, if $(x, y) \in E(\mathbb{C})$ then $(c^2x, c^3y) \in E'(K)$. The mapping sending (x, y) to (c^2x, c^3y) induces a bijection $E(\mathbb{C}) \approx E'(\mathbb{C})$.

Moreover, it is easy to check that two isomorphic elliptic curves E, E' satisfy that $j(E) = j(E')$.

The following proposition summarizes the relation between elliptic curve isomorphy, lattice homotheticity and equality of j-invariants.

Proposition 9. *Let E and E' be elliptic curves corresponding to lattices L and L' respectively. The following statements are equivalent:*

1. *E and E' are isomorphic over $\mathbb{C}$,*
2. *L and L' are homothetic,*
3. *$j(E) = j(E')$.*

Remark 27
From the previous theorem and Remark 19, we can state that two elliptic curves are isomorphic if and only if their corresponding lattices are related by the action of some $\gamma \in SL(2, \mathbb{Z})$.

Definition 105 (Endomorphism ring of an elliptic curve)
Let E be an elliptic curve over $\mathbb{C}$ that corresponds to the lattice L. We define

$$\mathrm{E}nd_{\mathbb{C}}(E) = \{\alpha \in \mathbb{C} \ : \ \alpha L \subset L\}.$$

Remark 28
$\mathrm{E}nd_{\mathbb{C}}(E)$ is a subring of $\mathbb{C}$ that includes $\mathbb{Z}$. We say that E has *complex multiplication* if $\mathbb{Z} \neq \mathrm{E}nd_{\mathbb{C}}(E)$. The curve E has complex multiplication if and only its corresponding lattice L does, in which case, $\mathrm{E}nd_{\mathbb{C}}(E)$ is an order $\mathcal{O}$ in an imaginary quadratic field.

From Theorem 16 we know the Weierstrass $\wp$-function satisfies an addition law. Next we will see that this can be translated into an addition operation over the points of an elliptic curve. This operation endows the points of an elliptic curve with an Abelian group structure. Moreover, the elliptic curve may be defined over any field K (not necessarily $\mathbb{C}$).

Definition 106 (Addition operation)
Let $E : Y^2 = 4X^3 - g_2X - g_3$ be an elliptic curve over K and let $P_1, P_2 \in E(K)$. The addition $P_1 + P_2 \in E(K)$ is defined as follows:

1. If $P_1 = \infty$ then $P_1 + P_2 = P_2$.
2. If $P_2 = \infty$ then $P_1 + P_2 = P_1$.
3. If $P_1, P_2 \neq \infty$ let $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$.
   (a) If $x_1 \neq x_2$, then $P_1 + P_2 = (x_3, y_3)$ with,
   $$x_3 = -x_1 - x_2 + \frac{1}{4}\left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2,$$
   $$y_3 = -y_1 - (x_3 - x_1)\left(\frac{y_1 - y_2}{x_1 - x_2}\right).$$
   (b) If $x_1 = x_2$ and $y_1 \neq y_2$ then $P_1 + P_2 = \infty$.
   (c) If $x_1 = x_2$ and $y_1 = y_2$, then $P_1 + P_2 = 2P_1 = (x_3, y_3)$ with,
   $$x_3 = -x_1 - x_2 - \frac{1}{16}\left(\frac{12x_1^2 - g_2}{y_1}\right)^2,$$
   $$y_3 = -y_1 - (x_3 - x_1)\left(\frac{12x_1 - g_2}{2y_1}\right).$$

Theorem 19. *If E is an elliptic curve over a field K, then $E(K)$ is a group under the binary operation defined above. The identity element is ∞.*

Remark 29
Given an elliptic curve $Y^2 = 4X^3 - g_2X - g_3$, defined over a field of characteristic different from 2 and 3, we can divide both sides of the equation by 4 obtaining
$$\left(\frac{Y}{2}\right)^2 = X^3 - \frac{g_2}{4}X - \frac{g_3}{4},$$

so that by replacing $\frac{Y}{2} \mapsto Y$, $-\frac{g_2}{4} \mapsto a$ and $-\frac{g_3}{4} \mapsto b$, we get

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

Elliptic curves given in this form are widely employed in the literature (the software Sage uses this form). The j-invariant of an elliptic curve E in this form is computed as,

$$j(E) = 1728\frac{4a^3}{4a^3 + 27b^2}.$$

Remark 30
A more general form for elliptic curves is given by the following expression [22, Chap.3]:

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

If the curve is defined over a field of characteristic different from 2, replacing $Y \mapsto \frac{1}{2}(Y - a_1X - a_3)$ gives an equation of the form

$$E : Y^2 = 4X^3 + b_2X^2 + 2b_4X + b_6,$$

with $b_2 = a_1^2 + 4a_2$, $b_4 = 2a_4 + a_1a_3$ and $b_6 = a_3^2 + 4a_6$. If further, the characteristic of the underlying field is different from 2 and 3, then replacing $X \mapsto \frac{X-3b_2}{36}$ and $Y \mapsto \frac{Y}{216}$ yields an equation of the form

$$E : Y^2 = X^3 - 27c_4X - 54c_6.$$

This form coincides with that given in Remark 29.

5.4 Elliptic curves over finite fields

Next, some results involving elliptic curves defined over a finite field $\mathbb{F}_q$ are presented. We will assume $\mathbb{F}_q$ has characteristic greater than 3, that is, $q = p^m$, $p > 3$.

A first consequence of defining elliptic curves over finite fields is that the set $E(\mathbb{F}_q)$ becomes finite. The following theorem due to Hasse [6, p.315] bounds such a cardinality.

Theorem 20. *If E is an elliptic curve over $\mathbb{F}_q$, then*

$$q + 1 - 2\sqrt{q} \leq |E(\mathbb{F}_q)| \leq q + 1 + 2\sqrt{q}.$$

Remark 31
In the construction of algebraic geometric codes over elliptic curves defined over $\mathbb{F}_q$, one is interested in finding curves with many rational points, *i.e.* curves whose cardinality is close to $q + 1 + 2\sqrt{q}$.

When elliptic curves are going to be used for discrete logarithm-based cryptography, one needs elliptic curves whose cardinality is divisible by a large prime.

Definition 107 (Trace)
Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$ so that $|E(\mathbb{F}_q)| = q+1-t$. The value t is known as the *trace* of Frobenius of curve E.

Example 99
Let us consider the elliptic curve $E : y^2 = 4x^3 - x - 1$. The set $E(\mathbb{Z}_{19})$ is

$$E(\mathbb{Z}_{19}) = \{(3,3),(3,16),(4,2),(4,17),(5,0),(8,5),(8,14),(11,7),\\ (11,12),(14,6),(14,13),(17,8),(17,11),\infty\}.$$

The cardinality is $|E(\mathbb{Z}_{19})| = 14$, and the trace of Frobenius is $t = 6$.

Remark 32
If the curve E in the previous example is considered over $\mathbb{F}_{19^2}$, by extending $\mathbb{Z}_{19}$ with a root α of $X^2 + 18X + 2$, the cardinality $|E(\mathbb{F}_{19^2})|$ is 364. For instance, the points $(\alpha + 17, 3), (\alpha + 17, 16)$ are in $E(\mathbb{F}_{19^2})$ but not in $E(\mathbb{Z}_{19})$.

Next, Theorem 21 addresses how the endomorphism ring of an elliptic curve defined over a finite field is.

Theorem 21. *If E is an elliptic curve over $\mathbb{F}_q$, then the endomorphism ring $End_{\overline{\mathbb{F}}_q}(E)$ is either:*

1. *An order in an imaginary quadratic field, in which case E is said to be* ordinary.

2. *An order in a quaternion algebra, in which case E is said to be* supersingular.

When elliptic curves are defined over a finite field, the j-invariant alone no longer determines whether two curves are isomorphic or not. The next proposition addresses this issue for ordinary curves (those whose trace $t \neq 0$).

Proposition 10. *Let E and E' be elliptic curves over $\mathbb{F}_p$. If E is ordinary, then E and E' are isomorphic over $\mathbb{F}_p$ if and only if $j(E) = j(E')$ and $|E(\mathbb{F}_p)| = |E'(\mathbb{F}_p)|$.*

Remark 33
The j-invariant of an elliptic curve defined over a finite field (of characteristic $\neq 2, 3$) given in Weierstrass form is computed using the same formula as for complex numbers.

Remark 34
When two elliptic curves E and E' defined over $\mathbb{F}_p$ satisfy $j(E) = j(E')$ but $|E(\mathbb{F}_p)| \neq |E'(\mathbb{F}_p)|$, then it is know that if $|E(\mathbb{F}_q)| = q + 1 - t_E$ and $|E'(\mathbb{F}_q)| = q + 1 - t_{E'}$ then $t_E + t_{E'} = 0$.

Remark 35
Given an ordinary elliptic curve E defined over $\mathbb{Z}_p$ with trace t, the endomorphism ring of E is known to be an order in the ring of integers of $\mathbb{Q}(\sqrt{D})$ with $D = t^2 - 4p$. Furthermore, if D is a *fundamental discriminant* (it is not divisible by any square of an odd prime) then the endomorphism ring of E is the ring of integers of $\mathbb{Q}(\sqrt{D})$.

We will focus our attention on ordinary curves. When defined over a prime field $\mathbb{F}_p$, such curves are easy to characterize. The following theorem characterizing supersingular curves serves to that end.

Theorem 22. *An elliptic curve E defined over $\mathbb{F}_p$, $p > 3$ is supersingular if and only if*

$$|E(\mathbb{F}_p)| = p + 1.$$

Ordinary elliptic curves over finite fields have, like elliptic curves over $\mathbb{C}$ with complex multiplication, an endomorphism ring that is an order in an imaginary quadratic field. Next we will see both types of curves are deeply related.

Definition 108 (Curves with good reduction)
Let K be a number field and let E be an elliptic curve

$$E : Y^2 = 4X^3 - g_2X - g_3, \qquad g_2, g_3 \in K.$$

Let $\mathfrak{p}$ be a prime ideal in $\mathfrak{O}_K$ and suppose that g_2, g_3 can be written in the form α/β, with $\alpha, \beta \in \mathfrak{O}_K$ and $\beta \notin \mathfrak{p}$. Defining $[g_2]$ and $[g_3]$ in $\mathfrak{O}_K/\mathfrak{p}$ we obtain that

$$\overline{E} : Y^2 = 4X^3 - [g_2]X - [g_3]$$

is an elliptic curve over the finite field $\mathfrak{O}_K/\mathfrak{p}$. We call $\overline{E}$ the *reduction* of E modulo $\mathfrak{p}$, and we say that E has *good reduction* modulo $\mathfrak{p}$.

Remark 36
As pointed out in [2, Section 4.2], an elliptic curve defined over $\mathbb{Z}_p$ can be described as the reduction modulo p of an elliptic curve $E(\mathbb{C})$ with complex multiplication by an order of a quadratic field. Let $D < 0$ be a fundamental discriminant and let $p \in \mathbb{Z}$ so that $4p = t^2 - Du^2$ for some integers u and t. If $H_D(X)$ is the Hilbert class polynomial of $\mathbb{Q}(\sqrt{D})$ then all the roots of $H_D(X) \pmod p$ lie in $\mathbb{Z}_p$ and they correspond to the j-invariant of elliptic curves defined over $\mathbb{Z}_p$ whose cardinality is either $p + 1 - t$ or $p + 1 + t$.

Remark 37
The previous remark is the basis of the methods implemented in Chapter 6. Both methods aim to construct polynomial $H_D(X) \pmod p$ and obtain elliptic curves with a required cardinality from its roots.

The Atkin-Morain method obtains $H_D(X) \pmod p$ by first computing the Hilbert class polynomial $H_D(X)$ from ideal class representatives of $C(\mathfrak{O}_K)$, $K =$

$\mathbb{Q}(\sqrt{D})$, using the formula indicated in Proposition 7. The required ideal class representatives are obtained making use of the bijection stated in Theorem 8 which permits to compute them from the classes composing the form class group of discriminant D, $C(D)$. The amount of such forms is finite as explained in Section 3.1. This method is explained in more detail in Section 6.1.

The Agashe-Lauter-Venkatesan method uses a different approach. The polynomial $H_D(X) \pmod p$ is computed using the Chinese Remainder Theorem from a set of polynomials $H_D(X) \pmod{p_i}$, being p_i primes of the form $4p_i = t_i^2 - D$. Each polynomial $H_D(X) \pmod{p_i}$ is computed taking into account that its roots are the j-invariants of elliptic curves in $\mathbb{Z}_{p_i}$ whose cardinality is either $p_i + 1 - t_i$ or $p_i + 1 + t_i$. This technique is explained in Section 6.2.

Chapter 6

Construction of elliptic curves with a given cardinality over a finite field

In this chapter the Atkin-Morain (Section 6.1) and the Agashe-Lauter-Ventakesan (Section 6.2) algorithms for finding an elliptic curve with a given cardinality (not necessarily maximal) are explained and analyzed in terms of running time. Each algorithm is first explained, next, a detailed example is provided and finally, some figures showing its running time are given. The two algorithms will be compared in Chapter 7.

6.1 Atkin-Morain's method

In [2], Atkin and Morain present a method, based on the theory of complex multiplication, for constructing an elliptic curve with a given cardinality. The method computes the Hilbert class polynomial $H_D(X)$ for a certain discriminant D and then reduces it modulo a prime p. The roots of the resulting polynomial provide the j-invariant of elliptic curves with the desired cardinality.

The algorithm takes as input a prime finite field $\mathbb{F}_p$ and the desired cardinality N for the curve to be constructed. From Theorem 20 we know the cardinality N should satisfy $N = p + 1 - t$ with $|t| \leq 2\sqrt{p}$.

For simplicity, the (negative) integer $D = t^2 - 4p$ is assumed to be a *fundamental discriminant* which is equivalent to requiring that it is not divisible by any square of an odd prime and satisfies $D \equiv 1 \pmod 4$ or $D \equiv 8, 12 \pmod{16}$.

6.1.1 Method steps

The algorithm is composed of the following steps:

1. Generate a list $\mathcal{L}$ containing all the primitive, reduced, positive definite binary quadratic forms of discriminant D.

   As explained in Section 3.1, the amount of such forms, denoted $h(D)$ (class number), is finite.

2. For each quadratic form $f_i = a_i x^2 + b_i xy + c_i y^2 \in \mathcal{L}$, compute the j-invariant
$$j_i = j\left(\frac{-b_i + \sqrt{D}}{2a_i}\right).$$

   Theorem 8 states there is a bijection between the forms in $\mathcal{L}$ and the elements that compose the ideal class group $C(\mathfrak{O}_K)$ with $K = \mathbb{Q}(\sqrt{D})$. More precisely, the form f_i generates the ideal
$$I_i = \left[a_i, \frac{-b_i + \sqrt{D}}{2}\right].$$

   The ideal I_i can be considered as a lattice which is homothetic (see Section 5.1) to lattice $a^{-1}I_i$ being
$$a_i^{-1} I_i = \left[1, \frac{-b_i + \sqrt{D}}{2a_i}\right].$$

   Since homothetic lattices have the same invariant,
$$j_i = j(I_i) = j(a_i^{-1} I_i) = j\left(\frac{-b_i + \sqrt{D}}{2a_i}\right).$$

   The j-invariants j_i are computed numerically so that the amount of precision becomes a crucial issue. In [2], it is stated that the largest coefficient of $H_D(X)$ is upperbounded by
$$B = \begin{pmatrix} h \\ \lfloor h/2 \rfloor \end{pmatrix} e^{\pi\sqrt{-D}\sum \frac{1}{a_i}}$$

   where the sum is taken over the integers a_i so that $a_i x^2 + b_i xy + c_i y^2 \in \mathcal{L}$. As a consequence, around $\log_2 B$ bits of precision are enough. In our implementation, $\lceil \log_2 B \rceil + 32$ bits of precision have been taken.

3. Compute the Hilbert class polynomial $H_D(X)$ as,
$$H_D(X) = \prod (X - j_i).$$

This step computes the Hilbert class polynomial $H_D(X)$ from the j-invariant of the lattices associated to the representatives of the ideal class group $C(\mathfrak{O}_K)$ (see Proposition 7). Due to roundoff inaccuracies, some coefficients of the computed polynomial may not be integer numbers. If this happens, the non-integer coefficients have to be rounded to their closest integer.

4. Find a root j of $H_D(X) \pmod p$ and compute the elliptic curve

$$E : y^2 = x^3 + 3kx + 2k,$$

where

$$k = \frac{j}{1728 - j}.$$

The cardinality $|E(\mathbb{Z}_p)|$ may either be $(p + 1 - t)$ (desired cardinality) or $(p+1+t)$. In the former case we are done, otherwise, we try with another root of $H_D(X) \pmod p$.

6.1.2 Detailed example

Next we will construct an elliptic curve over $\mathbb{Z}_{50021}$ of cardinality $N = 50467$. In this particular example, equation $N = p+1-t$ yields $t = 455$ and $D = t^2-4p = -2059$. The value D factors as $-2059 = -29 \cdot 71$ so that it is a fundamental discriminant. Computations have been carried out using 364 bits of precision.

1. In the first step, generate the list $\mathcal{L}$ containing all the primitive, reduced, positive definite binary quadratic forms of discriminant D.

   The quadratic forms composing $\mathcal{L}$ are shown in Table 6.1. As it can be seen, $\mathcal{L}$ contains eight quadratic forms, hence the class number $h(-2059) = 8$.

Form	Expression
f_1	$x^2 + xy + 515y^2$
f_2	$5x^2 - xy + 103y^2$
f_3	$5x^2 + xy + 103y^2$
f_4	$11x^2 - 3xy + 47y^2$
f_5	$11x^2 + 3xy + 47y^2$
f_6	$17x^2 - 7xy + 31y^2$
f_7	$17x^2 + 7xy + 31y^2$
f_8	$25x^2 + 21xy + 25y^2$

Table 6.1: Primitive, reduced, positive definite binary quadratic forms of discriminant $D = -2059$.

2. The second step is devoted to the computation of the j-invariants j_i of the lattices arising from the ideal class associated to each form f_i. As said

before, computations have been done employing 364 bits of precision. The results are shown (truncated) in Table 6.2.

j-invariant	Value	
j_1	$-8.132450466(\ldots)\cdot 10^{61}$	$-1.52000683(\ldots)\cdot 10^{-63}i$
j_2	$1.949853265(\ldots)\cdot 10^{12}$	$-1.416651320(\ldots)\cdot 10^{12}i$
j_3	$1.949853265(\ldots)\cdot 10^{12}$	$+1.416651320(\ldots)\cdot 10^{12}i$
j_4	$278940.314457048(\ldots)$	$-321054.961057362(\ldots)i$
j_5	$278940.314457048(\ldots)$	$+321054.961057362(\ldots)i$
j_6	$1954.81612413973(\ldots)$	$-4171.95604291573(\ldots)i$
j_7	$1954.81612413973(\ldots)$	$+4171.95604291573(\ldots)i$
j_8	$30.8936540456884(\ldots)$	$-3.6831015(\ldots)\cdot 10^{-117}i$

Table 6.2: j-invariants of the lattices associated to the representatives of the ideal class group $C(\mathfrak{O}_K)$, with $K=\mathbb{Q}(\sqrt{-2059})$.

3. Next, compute the Hilbert class polynomial

$$H_{-2059}(X)=\prod(X-j_i)\,,$$

which is a monic degree eight polynomial

$$H_{-2059}(X)=X^8+a_7X^7+a_6X^6+a_5X^5+a_4X^4+a_3X^3+a_2X^2+a_1X^1+a_0.$$

The values of the coefficients a_i are shown in Table 6.3.

a_7	8132450466169941169637006546375923632836825064114986736 1173504
a_6	−3171417476166593449477480202142006099622515215360868917697426072113428561 92
a_5	4724002964020315156143187259614324998239809746059904153 5420852938710380531261895396 5568
a_4	−2654044380264516409913225553944381907500162887963223842110408854199002950585596235165005250 56
a_3	8649819909224108953676771230198029757082859326272817089 7256449244680855228593363778346517782331392
a_2	−3423426700480862098802618969543352588354528788014336791506753490950703163470936987981159591961 0505221 12
a_1	1824291952089881900027334206261814738869090207478311873 5777531026554691610078856509268639648744741598658 56
a_0	−5603485668458992707841459135868602442730359202119169750185440315832341566967535164299356529615710947010150 4

Table 6.3: Coefficients of the Hilbert class polynomial $H_{-2059}(X)$.

4. Next, reduce the coefficients of $H_{-2059}(X)$ modulo 50021. The resulting polynomial is:

$$X^8 + 42643 \cdot X^7 + 33275 \cdot X^6 + 30118 \cdot X^5 + 47201 \cdot X^4$$

$$+38641 \cdot X^3 + 15977 \cdot X^2 + 1744 \cdot X + 2331.$$

In $\mathbb{Z}_{50021}$, the reduced polynomial has eight roots. They are:

$$\{48195, 42016, 39886, 34827, 14497, 13532, 11348, 3161\}.$$

By taking, for instance, the root $j = 42016$, one obtains the curve

$$y^2 = x^3 + 10138x + 12186$$

whose cardinality in $\mathbb{Z}_{50021}$ is precisely 50467, as desired.

6.1.3 Running time

Our implementation of Atkin-Morain's method has been tested on a computer with an Intel Xeon processor running at 3.16 GHz. The algorithm has been run so as to generate elliptic curves over $\mathbb{Z}_p$ being $p = 10000019$. Cardinalities $N = p + 1 - t$ associated to fundamental discriminants $D = t^2 - 4p$ have been chosen. Figure 6.1 shows the running time as a function of the absolute value of D, *i.e.* $|D|$. The values taken for D are between -32392 and -39983947. An irregular behaviour with a tendency to obtain larger running times for larger values of $|D|$ can be observed. The longest running time was obtained for $D = -37491020$ in which around 10 hours and a half were taken by the algorithm.

The results of the same experiments are depicted in Figure 6.2 but in this figure, the running time is represented as a function of the precision required for the j-invariants computation (step 2 in Section 6.1.1). A strong relation between arithmetic precision and running time can be observed.

6.2 Agashe-Lauter-Venkatesan's method

In [1], Agashe, Lauter and Ventakesan provide an alternative method for generating elliptic curves over a finite field $\mathbb{Z}_p$ with a desired cardinality. That proposal computes the Hilbert class polynomial $H_D(X)$ modulo a set of small primes and, after that, by using a modified version of the Chinese remainder theorem, $H_D(X) \pmod p$ is computed. Elliptic curves with the desired cardinality are obtained from the roots of $H_D(X) \pmod p$. When compared to [2], the method in [1] employs only arithmetic over the integers so that it is not necessary to consider accuracy issues as it happens when employing numerical methods over $\mathbb{C}$.

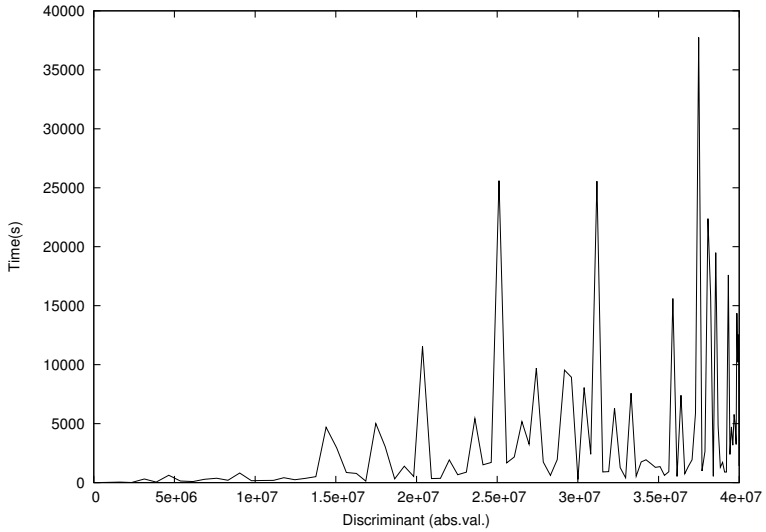

Figure 6.1: Running time of Atkin-Morain's method as a function of the absolute value of the discriminant D.

6.2.1 Method steps

As in Section 6.1, let $N = p+1-t$ be the desired cardinality and let $D = t^2 - 4p$ be a fundamental discriminant. The algorithm is as follows:

1. Compute the class number $h = H(D)$.

2. Generate a list $\mathcal{L}$ containing all the primitive, reduced, positive definite binary quadratic forms of discriminant D.

3. Compute
$$B = \left(\begin{array}{c} h \\ \lfloor h/2 \rfloor \end{array} \right) e^{\pi\sqrt{-D}\sum \frac{1}{a_i}}$$
where the sum in the above expression is taken over the integers a_i so that the quadratic form $a_i x^2 + b_i xy + c_i y^2 \in \mathcal{L}$.

   The value B is an upper bound for the size of the coefficients of the class polynomial.

4. Generate a collection of distinct primes $\{p_i\}$, each satisfying $4p_i = t_i^2 - D$, for some integer t_i. Generate enough primes p_i so that their product exceeds $2B$. Let $\mathcal{S}$ be a list containing all such primes.

5. For each $p_i \in \mathcal{S}$, let j run through all possible j-invariants over $\mathbb{Z}_{p_i}$ and store in a list S_i those j-invariants that correspond to a curve having $p_i + 1 - t_i$ or $p_i + 1 + t_i$ points. There are exactly h such j values.

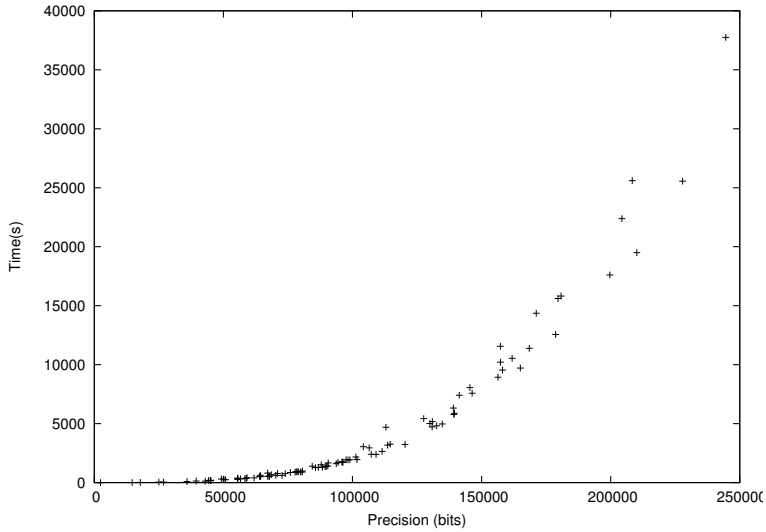

Figure 6.2: Running time of Atkin-Morain's method as a function of the precision (in bits) of the arithmetic computations over $\mathbb{C}$.

6. For each prime $p_i \in \mathcal{S}$, form the polynomial $H_D(X) \pmod{p_i}$ as,

$$H_D(X) \pmod{p_i} = \prod_{j_k \in \mathcal{S}_i} (X - j_k) \pmod{p_i}.$$

7. Using the modified chinese remainder theorem [1, Sec.5.], compute the coefficients of $H_D(X) \pmod{p}$ using the coefficients of $H_D(X) \pmod{p_i}$ for all $p_i \in \mathcal{S}$.

8. Obtain a curve with the required cardinality from a root of $H_D(X) \pmod{p}$ (like in Section 6.1).

6.2.2 Detailed example

Next, as it was done in Section 6.1.2, an elliptic curve over $\mathbb{Z}_{50021}$ of cardinality $N = 50467$ will be computed. Let us remember that, in this case, $D = t^2 - 4p = -2059$.

1. The first step is devoted to computing the class number, that is $h(-2059) = 8$.

2. The list $\mathcal{L}$ of quadratic forms is exactly the same obtained in Section 6.1.2.

3. Next, compute the upper bound B. In this example, the obtained value is:

$$B = \begin{array}{l} 343380993024870950094432889661828820697111779475657658 \\ 78216811022842329572888548075120820226820277383477126 47. \end{array}$$

4. The third step is devoted to constructing the list $\mathcal{S}$ of small primes. The constructed list is:

$$\mathcal{S} = \begin{array}{l} \{521, 557, 571, 587, 647, 787, 821, 857, 977, 1021, 1217, 1327, 1571, \\ 1637, 1847, 1997, 2237, 2677, 3167, 3271, 3821, 4297, 4421, 4547, \\ 4937, 6367, 6521, 7321, 7487, 8171, 8887, 9257, 12071\}. \end{array}$$

   The primes in $\mathcal{S}$ are of the form $4p_i = t_i^2 - D$. For instance,

$$4 \cdot 521 = 5^2 - (-2059).$$

5. Next, for each prime $p_i \in \mathcal{S}$, compute the j-invariants corresponding to curves defined over $\mathbb{Z}_{p_i}$ having either $p_i + 1 - t_i$ or $p_i + 1 + t_i$ points. The results are shown in Table 6.4.

6. After that, for each prime $p_i \in \mathcal{S}$, compute $H_D(X) \pmod{p_i}$. The generated polynomials are in Table 6.5.

7. Next, compute $H_D(X) \pmod{p}$. The resulting polynomial is:

$$X^8 + 42643 \cdot X^7 + 33275 \cdot X^6 + 30118 \cdot X^5 + 47201 \cdot X^4$$

$$+38641 \cdot X^3 + 15977 \cdot X^2 + 1744 \cdot X + 2331.$$

   As expected, this is exactly the same polynomial obtained in Section 6.1.2.

8. Finally, take a root j of $H_D(X) \pmod{p}$ corresponding to the j-invariant of some curve whose cardinality is 50467. That is the case for $j = 3161$ which generates the curve

$$y^2 = x^3 + 16573x + 42777.$$

6.2.3 Running time

Our implementation of Agashe-Lauter-Venkatesan's method has been tested on the same computer used in Section 6.1.3. In this case, curves over $\mathbb{Z}_p$ with $p = 10007$ have been generated. Several cardinalities have been chosen with the associated fundamental discriminants between -28 and -15692. The spent running time as a function of the absolute value of the discriminant is depicted in Figure 6.3. Similarly as it happened with Atkin-Morain's method, an irregular behaviour in which larger discriminants tend to produce a larger running time can be observed.

Although our experiments have generated curves over a quite small prime field ($p = 10007$), the observed running times are rather large. For instance, the execution on $D = -8699$ took almost 11 hours, while that on $D = -15692$

Prime p_i	j-invariants
521	108 115 133 144 174 369 384 438
557	2 14 61 116 307 441 470 517
571	20 154 156 170 216 356 365 485
587	15 110 192 201 277 328 485 543
647	168 175 296 349 365 401 534 642
787	46 71 203 224 239 569 595 784
821	61 80 92 356 363 467 722 725
857	242 298 422 449 607 762 764 810
977	39 342 439 509 537 607 623 759
1021	28 56 187 262 294 340 637 1003
1217	150 442 585 681 744 857 953 1216
1327	138 276 283 524 861 898 931 1028
1571	101 638 963 1118 1273 1322 1516 1568
1637	430 556 710 1052 1245 1269 1367 1449
1847	56 81 169 387 641 736 1213 1750
1997	234 344 688 938 1243 1328 1372 1476
2237	106 430 947 1288 1516 1563 1662 2206
2677	142 416 611 867 1481 1520 1522 2563
3167	388 504 682 1046 2127 2209 2235 3145
3271	515 770 1225 1519 1751 1897 2301 2960
3821	539 642 2214 2308 2393 2695 2815 3264
4297	631 2546 2923 3069 3113 3833 3914 4013
4421	192 591 1012 1383 3222 3846 4029 4315
4547	1037 2457 2654 3459 3524 3817 4423 4433
4937	446 583 1147 1247 2572 3156 4045 4329
6367	113 231 1335 1525 1564 4886 4938 5455
6521	98 176 780 1393 1760 1798 5341 6436
7321	357 1000 1764 3269 3482 3847 3937 4169
7487	1364 1969 3779 3894 5464 6768 6943 7010
8171	561 1130 2967 3156 3327 7424 7452 7728
8887	52 514 865 1365 3094 3283 3710 4318
9257	590 636 1850 2483 2643 3081 5276 6474
12071	1071 5549 5649 5897 6620 6810 8837 10304

Table 6.4: Table of primes p_i and the j-invariants for constructing $H_D(X) \pmod{p_i}$, being $D = -2059$.

Prime p_i	$H_D(X) \pmod{p_i}$
521	$X^8 + 219X^7 + 476X^6 + 37X^5 + 100X^4 + 235X^3 + 260X^2 + 199X + 159$
557	$X^8 + 300X^7 + 433X^6 + 450X^5 + 498X^4 + 262X^3 + 50X^2 + 367X + 139$
571	$X^8 + 362X^7 + 313X^6 + 6X^5 + 407X^4 + 497X^3 + 332X^2 + 522X + 429$
587	$X^8 + 197X^7 + 140X^6 + 121X^5 + 535X^4 + 508X^3 + 525X^2 + 572X + 14$
647	$X^8 + 305X^7 + 624X^6 + 106X^5 + 472X^4 + 72X^3 + 130X^2 + 194X + 483$
787	$X^8 + 417X^7 + 362X^6 + 53X^5 + 142X^4 + 258X^3 + 625X^2 + 421X + 161$
821	$X^8 + 418X^7 + 211X^6 + 606X^5 + 23X^4 + 229X^3 + 607X^2 + 184X + 417$
857	$X^8 + 788X^7 + 612X^6 + 277X^5 + 676X^4 + 672X^3 + 773X^2 + 532X + 314$
977	$X^8 + 53X^7 + 964X^6 + 850X^5 + 508X^4 + 633X^3 + 542X^2 + 574X + 609$
1021	$X^8 + 256X^7 + 636X^6 + 111X^5 + 276X^4 + 440X^3 + 402X^2 + 360X + 737$
1217	$X^8 + 457X^7 + 1048X^6 + 466X^5 + 960X^4 + 2X^3 + 779X^2 + 333X + 904$
1327	$X^8 + 369X^7 + 1132X^6 + 851X^5 + 851X^4 + 97X^3 + 792X^2 + 862X + 1216$
1571	$X^8 + 927X^7 + 1218X^6 + 913X^5 + 959X^4 + 1201X^3 + 265X^2 + 302X + 922$
1637	$X^8 + 107X^7 + 1214X^6 + 510X^5 + 1131X^4 + 947X^3 + 1004X^2 + 1037X + 900$
1847	$X^8 + 508X^7 + 421X^6 + 1447X^5 + 1788X^4 + 513X^3 + 155X^2 + 913X + 1451$
1997	$X^8 + 365X^7 + 94X^6 + 1458X^5 + 701X^4 + 696X^3 + 1663X^2 + 748X + 1664$
2237	$X^8 + 1467X^7 + 1329X^6 + 680X^5 + 1996X^4 + 188X^3 + 326X^2 + 1325X + 1718$
2677	$X^8 + 1586X^7 + 2182X^6 + 2522X^5 + 426X^4 + 890X^3 + 901X^2 + 128X + 1462$
3167	$X^8 + 332X^7 + 1558X^6 + 2500X^5 + 711X^4 + 2631X^3 + 2947X^2 + 1915X + 2898$
3271	$X^8 + 146X^7 + 2135X^6 + 2810X^5 + 3052X^4 + 801X^3 + 2061X^2 + 672X + 2750$
3821	$X^8 + 2235X^7 + 3621X^6 + 518X^5 + 2526X^4 + 1473X^3 + 2514X^2 + 3681X + 1367$
4297	$X^8 + 1740X^7 + 4006X^6 + 3198X^5 + 628X^4 + 1787X^3 + 4146X^2 + 1314X + 186$
4421	$X^8 + 3515X^7 + 1708X^6 + 2432X^5 + 3364X^4 + 19X^3 + 4363X^2 + 3299X + 1694$
4547	$X^8 + 1478X^7 + 557X^6 + 547X^5 + 4216X^4 + 4199X^3 + 931X^2 + 122X + 2603$
4937	$X^8 + 2223X^7 + 2283X^6 + 3633X^5 + 3014X^4 + 1441X^3 + 1038X^2 + 895X + 2929$
6367	$X^8 + 5421X^7 + 3063X^6 + 4934X^5 + 5408X^4 + 3086X^3 + 3209X^2 + 2378X + 4026$
6521	$X^8 + 1781X^7 + 3020X^6 + 4001X^5 + 6251X^4 + 4299X^3 + 4662X^2 + 3795X + 1481$
7321	$X^8 + 138X^7 + 40X^6 + 86X^5 + 4768X^4 + 5552X^3 + 2218X^2 + 5144X + 2932$
7487	$X^8 + 244X^7 + 1323X^6 + 2129X^5 + 2433X^4 + 6188X^3 + 4478X^2 + 3403X + 482$
8171	$X^8 + 7110X^7 + 5721X^6 + 442X^5 + 1707X^4 + 2076X^3 + 7975X^2 + 5261X + 5130$
8887	$X^8 + 573X^7 + 1259X^6 + 1137X^5 + 1257X^4 + 6273X^3 + 3973X^2 + 2349X + 1179$
9257	$X^8 + 4738X^7 + 1098X^6 + 7341X^5 + 1995X^4 + 4749X^3 + 6734X^2 + 4637X + 1513$
12071	$X^8 + 9618X^7 + 3291X^6 + 26X^5 + 4751X^4 + 4781X^3 + 8312X^2 + 3824X + 6102$

Table 6.5: Polynomials $H_D(X) \pmod{p_i}$, being $D = -2059$.

took more than 38 hours. Such a large running time is due to the elevated computational cost of Step 5. This step is run for each of the primes in the collection $\{p_i\}$ generated in Step 4. For each prime p_i, this step iterates $O(p_i)$ times with each iteration requiring the computation of the cardinality of an elliptic curve. The computational cost of the other steps is negligible.

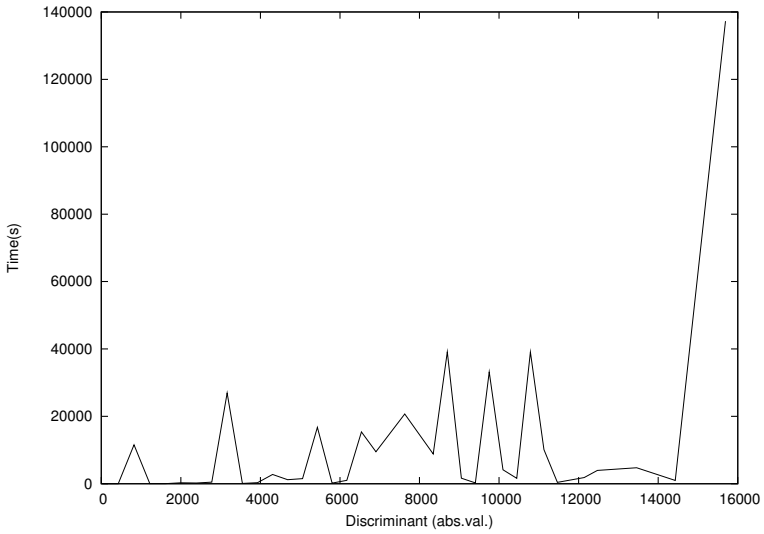

Figure 6.3: Running time of Agashe-Lauter-Venkatesan's method as a function of the absolute value of the discriminant D.

Again, we have depicted the spent running time as a function of the size of the largest coefficient of the Hilbert class polynomial $H_D(X)$. In this case, we observe again some tendency to obtain larger running times for larger polynomial coefficients, but the relation between both parameters looks more irregular.

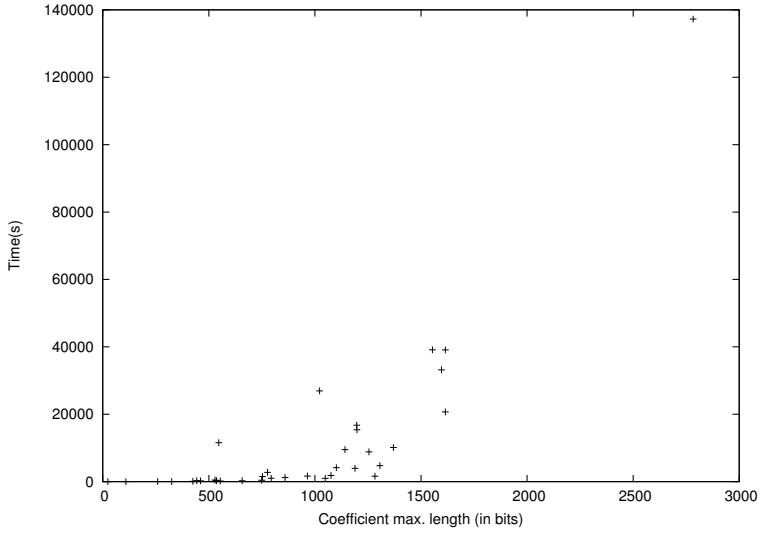

Figure 6.4: Running time of Agashe-Lauter-Venkatesan's method as a function of the size (in bits) of the largest coefficient of $H_D(X)$.

Chapter 7

Method comparison and conclusion

7.1 Method comparison

So as to compare the two implemented methods, some of the experiments carried out with Agashe-Lauter-Venkatesan's method in the previous chapter have been repeated using Atkin-Morain's method. The results are shown in Table 7.1 which shows that, according to our implementation, Atkin-Morain's method is much faster than Agashe-Lauter-Venkatesan's. As a particular example, the experiment on $D = -15692$ took around one second and a half with Atkin-Morain's whereas it took more than 38 hours with Agashe-Lauter-Venkatesan's. The running time of both methods grows very fast with the absolute value of discriminant D in such a way that both algorithms are only feasible for reduced values of $|D|$.

The cost of both algorithms depends on the largest coefficient of the Hilbert class polynomial $H_D(X)$, which is upperbounded by

$$B = \left(\begin{array}{c} h \\ \lfloor h/2 \rfloor \end{array} \right) e^{\pi\sqrt{-D}\sum \frac{1}{a_i}}$$

where the sum in the above expression is taken over the integers a_i such that the quadratic form $a_i x^2 + b_i xy + c_i y^2$ is primitive, reduced, positive definite of discriminant D (h is the class number $H(D)$). The required precision for complex number arithmetic of Atkin-Morain's algorithm, and the amount of small primes taken by Agashe-Lauter-Venkatesan's grow with B. Since B grows exponentially with $|D|$, both algorithms have a running time which is exponential with $|D|$.

In [1] it is stated that generating random curves until one with the required cardinality is found is asymptotically more efficient that complex multiplication methods. It is also pointed out that complex multiplication methods are better that random curve generation just in some situations, like when the curve is

Discriminant	Time (AM)	Time (ALV)
-3164	1.5	26939
-6172	1.18	1028
-8699	1.27	39134
-12472	1.38	3972
-15692	1.58	137282

Table 7.1: Comparison of the time spent (in seconds) by Atkin-Morain's (AM) and Agashe-Lauter-Venkatesan's (ALV) algorithms for some discriminants D.

defined over a large finite field yet the discriminant D is relatively small. The results obtained in this thesis agree with that statement.

7.2 Conclusion

The objective of this thesis has been the implementation of two algorithms for constructing elliptic curves with a given cardinality. Both algorithms are based on the theory of complex multiplication on elliptic curves. The thesis begins by reviewing some elementary mathematical background on groups, rings, fields and polynomials. After that, some chapters devoted to provide some more deep content on number fields, quadratic forms, algebraic curves, elliptic functions and complex multiplication have been provided. Finally, the two implemented algorithms have been explained together with a detailed example of each one, and results regarding their running time.

The obtained results show that algorithms based on the construction of the Hilbert class polynomial $H_D(X)$ are constrained by its exponentially (with $|D|$) large coefficients. As a consequence, the studied algorithms are only practical for generating elliptic curves with a relatively small complex multiplication discriminant, D.

The two studied algorithms have analogous (yet much more complicated) versions for constructing genus 2 curves with a given number of points on its Jacobian. The genus 2 version of Atkin-Morain's generates the *Igusa class polynomials* of a quartic (degree four) complex multiplication field K by evaluating the modular invariants of all the abelian varieties of dimension 2 with complex multiplication by K. Regarding Agashe-Lauter-Venkatesan's, its genus 2 generalization first computes the Igusa class polynomials modulo some small primes and later, the Igusa class polynomial is computed using the Chinese Remainder Theorem. Some additional difficulties like the need to compute the endomorphism ring of Jacobians of genus 2 curves have to be dealt with. The reader is referred to [7, 21] for more details.

Bibliography

[1] A. Agashe, K. Lauter, R. Venkatesan, "Constructing elliptic curves with a given number of points over a finite field", Technical Report, 2001. `http://arxiv.org/pdf/math/0111159v1.pdf`

[2] A.O.L. Atkin, F. Morain, "Elliptic curves and primality proving", Math. Comp. **61**, 1993.

[3] D. Boneh, M. Franklin, "Identity based encryption from the Weil pairing", Proc. of CRYPTO, 2001.

[4] J. Buchmann, U. Vollmer, "Binary quadratic forms. An algorithmic approach", Algorithms and Computation in Mathematics, **20**, Springer, 2007.

[5] E. Bujalance, J.J. Etayo, J.M. Gamboa, "Teoría elemental de grupos" (3a Ed.), Cuadernos de la UNED, 2002.

[6] D.A. Cox, "Primes of the form $x^2 + ny^2$. Fermat, class field theory, and complex multiplication", Wiley Interscience, 1989.

[7] K. Eisenträger, K. Lauter, "A CRT algorithm for constructing genus 2 curves over finite fields", Technical Report, 2007. `http://arxiv.org/pdf/math/0405305v2.pdf`

[8] J.M. Gamboa, J.M. Ruiz, "Anillos y cuerpos conmutativos", Cuadernos de la UNED, 2002.

[9] S. Goldwasser, J. Kilian, "Almost all primes can be quickly certified", Proc. 18th Annual ACM Symp. on Theory of Computing, 1986.

[10] V.D. Goppa, "A new class of linear error correcting codes", Problemy Peredachi Informatsii, 1970.

[11] H. Hasse, "Zur Theorie der abstrakten elliptischen Funktionenkörper. I, II & III", Crelle's Journal, **175**, 1936.

[12] G.A. Jones, D. Singerman, "Complex functions. An algebraic and geometric viewpoint", Cambridge University Press, 1987.

[13] F. Kirwan, "Complex algebraic curves", London Mathematical Society Student Texts, **23**, Cambride University Press, 1992.

[14] N. Koblitz, "Elliptic curve cryptosystems", Mathematics of Computation, **48**, 1987.

[15] H.W. Lenstra Jr., "Factoring integers with elliptic curves", Annals of Mathematics, **126**, 1987.

[16] A.J. Menezes, Y. Wu, R.J. Zuccherato, "An elementary introduction to hyperelliptic curves", Technical Report CORR 96-19, University of Waterloo, 1996.

[17] V. Miller, "Use of elliptic curves in cryptography", Proc. of CRYPTO 85, 1985.

[18] C.J. Moreno, "Algebraic curves over finite fields", Cambridge Tracts in Mathematics, **97**, Cambridge University Press, 1991.

[19] S. Pohlig, M. Hellman, "An improved algorithm for computing logarithms over GF(p) and its cryptographic significance", IEEE Transactions on Information Theory, **24**, 1978.

[20] Sage: Open source mathematics software (ver.5.9). `http://www.sagemath.org/`

[21] T. Shaska, L. Beshaj, "The arithmetic of genus two curves", Information Security, Coding Theory and Related Combinatorics, IOS Press, 2011.

[22] J.H. Silverman, "The arithmetic of elliptic curves", Graduate Texts in Mathematics, Springer-Verlag, 1986.

[23] I.N. Stewart, D.O. Tall, "Algebraic number theory", 2nd Ed, Chapman & Hall, 1987.