University of Trento

Department of Mathematics

PhD Thesis

Binary quadratic forms, elliptic curves and Schoof's algorithm

Author:
Federico Pintore
XXVII Cicle

Supervisors:
Prof. Michele Elia,
Prof. Massimiliano Sala

27 March 2015

Introduction

The hellenistic mathematician Diophantus of Alexandria (3rd century A.D.), in his major work "The Arithmetica" considered a number of indeterminate equations, providing numerical solutions to them. In the light of his seminal contribution, the equations with integral coefficients in two or more unknowns, for which only integral solutions are looked for, are said Diophantine equations. In the subsequent centuries, the study of Diophantine equations ("Diophantine geometry") remained an important area of mathematical researches (a significant example is the so called *Fermat's Last Theorem*). In 1900 Hilbert proposed the problem of finding an algorithm that decides the solvability of any given Diophantine equation as the tenth of his celebrated problems. Seventy years later, Juri V. Matijasevic proved that such an algorithm cannot exist. It is therefore necessary to develop algorithms that solve subclasses of Diophantine equations. The easiest Diophantine equations are linear and they can be solved using the Euclidean algorithm. Furthermore, univariate quadratic Diophantine equations can be solved using algorithms for extracting square roots. Thus, the first hardly solvable Diophantine equation is a bivariate quadratic, i.e. an equation of the form

$$ax^2 + bxy + cy^2 = m \qquad a, b, c, m \in \mathbb{Z}, \tag{1}$$

that Diophantus considedered in many of his problems [29, 5] and that is still source of interesting open questions [26, 57, 11].

The left expression in (1) is an integral binary quadratic form $Q(x, y)$, also denoted with the triplet (a, b, c), that in the following will be assumed to be primitive (with $gcd(a, b, c) = 1$). If equation (1) has a solution in relatively prime integers x and y, then we say that the quadratic form $Q(x, y)$ represents m. The problem of deciding whether equation (1) is solvable depends on the discriminant of $Q(x, y)$, which is the integer Δ defined as $b^2 - 4ac$, and was addressed by Lagrange [20, Lemma 2.6]. Even though Fermat, Euler and Lagrange worked on binary quadratic forms, the first who considerably expanded the theory of these objects was Gauss in [26]. Thanks to his theory, in which classes and composition of forms are studied in a systematic way, the attention was moved from specific quadratic forms to sets of quadratic forms and it became possible to restrict only to those cases where the constant term m in the equation (1) is a prime integer p [17, page 215].

The set of the quadratic forms with the same discriminant Δ is partitioned into a finite set, $C(\Delta)$, of h_Δ proper equivalence classes ($h_\Delta \in \mathbb{N}$) [44, Theorem 3.7, p.116] by the equivalence notion: two forms $Q_1(x, y)$ and $Q_2(x, y)$ are equivalent if integers r, s, t, and u exist such that $Q_1(x, y) = Q_2(rx + sy, tx + uy)$ and $ru - st = \pm 1$, and are properly equivalent if $ru - st = 1$ [26, §157]. All forms in a proper equivalence class represent the same integers and they are identified by some reduced form (A, B, C). A reduced form is a quadratic form (A, B, C) whose coefficients satisfy the conditions

$$\begin{array}{lllll} |B| \leq A \leq C & \text{and} & B \geq 0 \quad \text{when} \quad A = |B| \quad \text{or} \quad A = C & & \text{if} \;\; \Delta < 0 \\ 0 < B < \sqrt{\Delta} & \text{and} & \sqrt{\Delta} - B < 2\,|A| < \sqrt{\Delta} + B & & \text{if} \;\; \Delta > 0 \end{array} \tag{2}$$

If $\Delta < 0$, each proper equivalence class contains a single reduced form [45, Theorem 3.1]; if $\Delta > 0$, each proper equivalence class contains the same even number P_c of reduced forms [26], [57, p.111]. These capital results were proved by Gauss [26, art. 171 and art. 183] by means of two constructive demonstrations with the same structure: successive transformations of a starting form $f(x, y)$ create a sequence of forms, properly equivalent to $f(x, y)$, that ends with a reduced form. From these proofs one can deduce an algorithm that takes a quadratic form $f(x, y)$ as input and returns a reduced form $h(x, y)$ properly equivalent to $f(x, y)$, together with four integers r, s, t, u such that $f(rx + sy, tx + uy) = h(x, y)$. This algorithm is called *Gauss reduction algorithm*.

When p is represented by some quadratic form of discriminant Δ, it is possible [20, Lemma 2.6, p.25] to produce an integral binary quadratic form $g(x, y) = px^2 + b'xy + c'y^2$ of discriminant Δ that represents p. To accomplish this task is necessary to find a square root of Δ modulo p. According to [17, Theorem 5, p. 200], $g(x, y)$ and $g(x, -y)$ are the representatives of the only proper equivalence classes contained in $C(\Delta)$ made up by forms that represent p. When $\Delta < 0$, starting from $Q(x, y)$ and $g(x, y)$, one can solve equation (1) applying *Gauss reduction algorithm* to $Q(x, y)$, $g(x, y)$ and $g(x, -y)$. Equation (1) has a solution if and only if the reduced form properly equivalent to $Q(x, y)$ is equal to one of the reduced forms properly equivalent to $g(x, y)$ and $g(x, -y)$. When a solution exists, it could be computed using the integers that describe the transformation that sends $Q(x, y)$ into $g(x, y)$ or into $g(x, -y)$. When $\Delta > 0$, the same approach presents further difficulties. In Chapter 1 we will provide an algorithm, written in the language of the modern computer algebra software MAGMA, that, through *Gauss reduction algorithm*, solves equation (1) in the both cases $\Delta > 0$ and $\Delta < 0$. In particular, when the discriminant is positive, we use [10, Corollary 6.8.11] to enumerate all the reduced forms contained in the proper equivalence classes of $g(x, y)$ and $g(x, -y)$.

Now we assume that Δ is a fundamental discriminant, i.e.

$$\Delta = \begin{cases} d & \Delta \equiv 1 \pmod 4 \\ 4d & \Delta \equiv 0 \pmod 4 \end{cases}$$

with d squarefree integer. In this case, there is a natural correspondence between the quadratic forms with discriminant Δ and the *ideals* of the quadratic field $\mathbb{K} = \mathbb{Q}(\sqrt{d})$.

An element of $\mathbb{K}$ is an algebraic integer if it is a root of some univariate monic polynomial with integral coefficients [11, pag. 89]. The set $\mathcal{O}_{\mathbb{K}}$ of all the algebraic integers of $\mathbb{K}$ is a ring [11, Proposition 6.6] with $\mathbb{K}$ as field of fractions of $\mathcal{O}_{\mathbb{K}}$ [45, Lemma 1.4]. The ring $\mathcal{O}_{\mathbb{K}}$ is called the *ring of integers of* $\mathbb{K}$. None of the elements of $\mathbb{K} \setminus \mathcal{O}_{\mathbb{K}}$ is integral over $\mathcal{O}_{\mathbb{K}}$, i.e.

is a root of some univariate monic polynomial of $\mathcal{O}_{\mathbb{K}}[x]$. Furthermore, the ring of integers of $\mathbb{K}$ is Noetherian and such that each of its prime ideals is maximal. These properties make $\mathcal{O}_{\mathbb{K}}$ a Dedekind domain [20, Theorem 5.5]. More generally, the algebraic integers of every finite extensions of $\mathbb{Q}$ are a Dedekind domain.

Since every ideal of $\mathcal{O}_{\mathbb{K}}$ is a finitely generated $\mathcal{O}_{\mathbb{K}}$-module, it is natural to consider all the finitely generated $\mathcal{O}_{\mathbb{K}}$-module contained in $\mathbb{K}$. These are the *fractional ideals* of $\mathcal{O}_{\mathbb{K}}$ and they form a free abelian multiplicative group $I(\mathcal{O}_{\mathbb{K}})$ [39, Chapter 1]. Among all, we consider the subgroup of all those fractional ideals generated by a single element of positive norm [9, pag. 400]. The corresponding quotient group is denoted by $C^+(\mathcal{O}_{\mathbb{K}})$ and called the *narrow ideal class group of* $\mathcal{O}_{\mathbb{K}}$.

The connection between $C(\Delta)$ and $\mathbb{K}(\sqrt{d})$ is due to the existence of an isomporhism [17, Chapter 13] between $C(\Delta)$, endowed with the group structure by the composition of forms [11, Chapter 4], and $C^+(\mathcal{O}_{\mathbb{K}})$.

Thanks to the Class Field Theory, also the elliptic curves play a role in the relationship between quadratic forms and quadratic fields. The Hilbert class field $\mathbb{L}$ of the quadratic field $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ is a finite unramified field extension of $\mathbb{K}$ such that every non-principal ideal of $\mathbb{K}$ becomes principal in $\mathbb{L}$ [46, Theorem 4.18, p.189]. The field $\mathbb{L}$ is specified by a root α of an irreducible polynomial $h_{\mathbb{K}}(x) \in \mathbb{K}[x]$. It is called the *Hilbert class polynomial of* $\mathbb{L}$ and has degree h_Δ. In particular, when $d < 0$, $h_{\mathbb{K}}(x)$ always has integral coefficients. Given an elliptic curve $\mathbb{E}$ over $\mathbb{L}$ with complex multiplication $\mathcal{O}_{\mathbb{K}}$ [15, Chapter 7], and a prime ideal $\mathfrak{B}$ of $\mathcal{O}_{\mathbb{L}}$ containing the constant term of equation (1) (that we assume to be a prime integer p), we can then consider $\mathbb{E}$ modulo $\mathfrak{B}$ obtaining an elliptic curve $\overline{\mathbb{E}}$ over the finite field $\mathbb{F}_q$, with $q = p^n$ [1, Chapter 4]. When d is negative, by Deuring's results [47], there exists $\pi \in \mathcal{O}_{\mathbb{K}}$ such that $\left|\overline{\mathbb{E}}(\mathbb{F}_q)\right| = q + 1 - (\pi + \overline{\pi})$ and $q = \pi\overline{\pi}$, where $\overline{\pi}$ is the conjugate of π in $\mathbb{K}$ [11, pag. 92]. This gives a representation of q by the principal form $Q_0(x, y)$ of discriminant Δ [42, Cor. 2.4] which is defined as:

$$Q_0(x,y) = \begin{cases} (1, 0, -\Delta/4) & \Delta \equiv 0 \pmod 4 \\ (1, 1, -(\Delta-1)/4) & \Delta \equiv 1 \pmod 4 \end{cases} \tag{3}$$

In Chapter 3, we will prove a theorem that allows us to find a representantion of p by those reduced forms of discriminant Δ that represent p. So it supplies a method, alternative to that based on the *Gauss reduction algorithm*, to find in polynomial time complexity a representation of p. The proof of the theorem is done using the above mentioned connections between quadratic forms, quadratic fields and elliptic curves. When $h_\Delta \leq 3$, in the light of [2, Theorem 3.2], we use the factorization of $h_{\mathbb{K}}(x)$ modulo p to determine which of the h_Δ reduced form $Q_0(x, y), Q_1(x, y), \ldots, Q_{h_\Delta - 1}(x, y)$ of discriminant Δ (a representative to each proper equivalence class of $C(\Delta)$) represent p. So, for $h_\Delta = 1, 2, 3$ we will provide three algorithms (written in MAGMA language) to determine the $Q_i(x, y)$'s that represent p and the corresponding representation.

The polynomial complexity of the proposed algorithms is principally due to the Schoof's algorithm [50] to count the rational points of elliptic curves over finite fields. With an effective use of the Chinese remainder theorem and the division polynomials [58, Section 3.2], it computes the number of the rational points of an elliptic curve over a finite field $\mathbb{F}_q$

taking $O(\log^9 q)$ elementary operations. In Chapter 4 we will discuss the possible existence of a family of elliptic curves not taken into account by the Schoof's original paper.

Contents

Chapter 1

Integral binary quadratic forms

Our work arises from the problem of solving a quadratic Diophantine equation:

$$ax^2 + bxy + cy^2 = m \tag{1.1}$$

where a, b, c, m belongs to $\mathbb{Z}$. Solve a Diophantine equation means to find the integer values of the unknowns for which the equation is satisfied. We are interested only in solutions (x_0, y_0) of equation 1.1 such that $gcd(x_0, y_0) = 1$.
The left term of the equation is a binary quadratic form $f(x, y)$ with integral coefficients. We will consider only that cases where $f(x, y)$ is primitive, i.e. such that $gcd(a, b, c) = 1$. The research of the solutions of equation 1.1 is based on the theory of integral binary quadratic forms that owed its development to Lagrange, Gauss, Fermat and other great mathematicians. In particular, Gauss' contribution about composition of forms and reduced forms, permits to consider only those cases where m is a prime integer p and to deduce an algorithm to this kind of equations.
In the following sections we will recall some classical facts about binary quadratic forms in order to exhibit the mentioned algorithm. Even if quite all what we are going to see was yet contained in "Disquisitiones Arithmeticae" of Gauss ([26]), we will refer to several books of number theory, like [11], [20], [45], [38], [10].
We start introducing the notion of integral binary quadratic form and some related terminology, following part four of the Edmund Landau's book "Elementary number theory" [38].

1.1 An introduction to integral binary quadratic forms

An integral binary quadratic form $f(x, y)$ is an homogeneous polynomial of degree 2 of the ring $\mathbb{Z}[x, y]$:

$$f(x, y) = ax^2 + bxy + cy^2 \qquad a, b, c \in \mathbb{Z} \tag{1.2}$$

For simplicity, from now on, *integral binary quadratic form* will be only *quadratic form* or *form*, and $f(x, y) = ax^2 + bxy + cy^2$ will be denoted by (a, b, c). As we have said, in the following only primitive quadratic forms will be considered if not specified otherwise. So the term *primitive* will be omitted.

A quadratic form $f(x, y) = (a, b, c)$ **represents** an integer m if there exist two integers x_0, y_0 such that $f(x_0, y_0) = m$. If x_0 and y_0 are relatively prime we said that $f(x, y)$ **represents** m **properly** by x_0 and y_0. We also said that m **is (properly) represented by** $f(x, y)$ by the pair (x_0, y_0).

Definition 1.1. *Let $f(x, y) = (a, b, c)$ be a quadratic form. Its discriminant Δ is the integer defined as:*

$$\Delta = b^2 - 4ac$$

Here are enumerated some elementary observations about the discriminant:

1. Δ and b^2 are congruent modulo 4;
2. Δ is congruent to 0 modulo 4 if b is even while it is congruent to 1 modulo 4 if b is odd. Then Δ and b have the same parity;
3. the following relations hold:

$$4af(x, y) = (2ax + by)^2 + (4ac - b^2)y^2 = (2ax + by)^2 - \Delta y^2 \tag{1.3}$$

$$4cf(x, y) = (2cy + bx)^2 + (4ac - b^2)x^2 = (2cy + bx)^2 - \Delta x^2 \tag{1.4}$$

For every integer $\Delta \equiv 0, 1 \pmod 4$, there exists a quadratic form $Q_0(x, y)$ with Δ as discriminant. We have:

$$Q_0(x, y) = \left(1, 0, -\frac{\Delta}{4}\right) \qquad if\ \ \Delta \equiv 0 \pmod 4 \tag{1.5}$$

and

$$Q_0(x, y) = \left(1, 1, -\frac{\Delta - 1}{4}\right) \qquad if\ \ \Delta \equiv 1 \pmod 4 \tag{1.6}$$

The form $Q_0(x, y)$ is called the **principal form of discriminant** Δ.

1.2 Reducible, definite and indefinite quadratic forms

Given a quadratic form $f(x, y) = (a, b, c)$, we can ask about the types of integers that it represents:

1. does $f(x, y)$ represent 0 by a couple of integer not both zero?
2. does $f(x, y)$ represent integers of opposite sign?

To answer to these questions we follow [38]. The first query needs two preliminary lemmas.

Lemma 1.2. *Given a quadratic form $f(x,y) = (a,b,c)$ there exist four rational numbers $\alpha, \beta, \gamma, \delta$ such that $(\alpha x + \beta y)(\gamma x + \beta y) = f(x,y)$ if and only if $f(x,y)$ is reducible in $\mathbb{Z}[x,y]$*

Proof. One of the two implications is obvious. For the second one, we fix the following notation:

$$\alpha = \frac{\alpha'}{\alpha''} \qquad \beta = \frac{\beta'}{\beta''} \qquad \gamma = \frac{\gamma'}{\gamma''} \qquad \delta = \frac{\delta'}{\delta''}$$

with $\alpha', \alpha'', \beta', \beta'', \gamma', \gamma'', \delta', \delta''$ integers such that

$$gcd(\alpha', \alpha'') = gcd(\beta', \beta'') = gcd(\gamma', \gamma'') = gcd(\delta', \delta'') = 1$$

Let $\tilde{m}$ be the least common multiple of $\alpha'', \beta'', \gamma'', \delta''$. Then, setting $m = \tilde{m}^2$, we have

$$mf(x,y) = \tilde{m}(\alpha x + \beta y)\tilde{m}(\gamma x + \beta y) = (rx + sy)(tx + uy)$$

with $r, s, t, u \in \mathbb{Z}$.
If $gcd(m,r,s) > 1$, then

$$\frac{1}{gcd(m,r,s)} mf(x,y) = \left(\frac{r}{gcd(m,r,s)}x + \frac{s}{gcd(m,r,s)}y\right)(tx + uy)$$

with

$$gcd\left(m' = \frac{m}{gcd(m,r,s)}, r' = \frac{r}{gcd(m,r,s)}, s' = \frac{s}{gcd(m,r,s)}\right) = 1$$

So we can assume $gcd(m,r,s) = 1$ and, for analogy, $gcd(m,t,u) = 1$.
We want to show that $m = 1$. If m is not 1, it is divisible by a prime integer p and from

$$mf(x,y) = max^2 + mbxy + mcy^2 = (rx + sy)(tx + uy) = rtx^2 + (ru + st)xy + suy^2$$

we can deduce that p divides r or t (because it divides $ma = rt$). Suppose $p \mid r$. Since $(ru + st) = mb$, p divides s or t. If $p \mid s$, then $gcd(m,r,s) \geq p$; if p does not divide s but $p \mid t$ then $gcd(m,t,u) \geq p$. This is a contradiction that we find also if we suppose that $p|ma$ implies $p \mid t$. □

Lemma 1.3. *A quadratic form $f(x,y) = (a,b,c)$ is reducible in $\mathbb{Z}[x,y]$ if and only if its discriminant Δ is a perfect square.*

Proof. If $f(x,y) = (rx + sy)(tx + uy) = rtx^2 + (ru + st)xy + suy^2$ with $r, s, t, u \in \mathbb{Z}$, then we have

$$\Delta = (ru + st)^2 - 4rtsu = (ru - st)^2$$

On the other hand, if $\Delta = d^2$, from 1.3 it follows

$$4af(x,y) = (2ax + by)^2 - d^2y^2 = (2ax + (b+d)y)(2ax + (b-d)y)$$

If $a \neq 0$ then $f(x,y) = \frac{1}{4a}(2ax + (b+d)y)(2ax + (b-d)y)$ and $f(x,y)$ is reducible in $\mathbb{Z}[x,y]$ by Lemma 1.2. If $a = 0$ we simply have $f(x,y) = bxy + cy^2 = (bx + cy)y$. □

If the form $f(x,y) = (a,b,c)$ has discriminant Δ which is a perfect square we said that $f(x,y)$ is **reducible**.

Proposition 1.4. *A quadratic form $f(x,y) = (a,b,c)$ represents 0 by two integers not both zero if and only if its determinant is a perfect square.*

Proof. If $f(x,y)$ represents 0 by two integers x_0, y_0 not both zero, then $f(x_0,y_0) = ax_0^2 + bx_0y_0 + cy_0^2 = 0$ and

$$4af(x_0,y_0) = 0 = (2ax_0 + by_0)^2 - \Delta y_0^2 \Rightarrow \left(\frac{2ax_0 + by_0}{y_0}\right)^2 = \Delta$$

Observe that, if $y_0 = 0$ then $ax_0^2 = 0$ and $a = 0$. In this case $\Delta = b^2$.
Conversely, if $\Delta = d^2$ then $f(x,y) = (rx+sy)(tx+uy)$ with $r,s,t,u \in \mathbb{Z}$ by Lemma 1.2, hence $f(-s,r) = 0$, with r,s not both zero. □

Suppose that the form $f(x,y) = (a,b,c)$ of the Diophantine equation 1.1 is reducible in $\mathbb{Z}[x,y]$, i.e. $f(x,y) = (rx+sy)(tx+uy)$ for some $r,s,t,u \in \mathbb{Z}$. The considered equation has a solution in two relative prime integers x,y if and only if

$$\begin{cases} rx + sy = m_1 \\ tx + uy = m_2 \end{cases}$$

for some factors m_1, m_2 of m such that $m = m_1m_2$. Since the number of m's factors is finite, solve $(rx+sy)(tx+uy) = m$ means to determine the solution sets of a finite number of systems of linear equations. For what we have just seen, in the following we will consider only non-reduced quadratic forms.

The second of the questions about the integers represented by a fixed quadratic form $f(x,y)$ is answered by the following result:

Proposition 1.5. *Let $f(x,y) = (a,b,c)$ be a quadratic form of discriminant Δ.
If $\Delta > 0$, $f(x,y)$ represents both positive and negative integers. If Δ is negative, then $f(x,y)$ represents only non-negative integers when $a > 0$ and only non-positive integers when $a < 0$.*

Proof. If we suppose that Δ is positive then we have:

$$f(1,0) = a$$

$$f(b,-2a) = ab^2 - 2ab^2 + 4a^2c = a(4ac - b^2) = -a\Delta$$

so $f(x,y)$ represents integer of opposite sign (as long as a is non-zero, i.e. Δ is not a perfect square). If $\Delta < 0$, from $4af(x,y) = (2ax+by)^2 - \Delta y^2$ it follows that $4af(x,y)$ is non negative for every couple of integers x,y. □

The quadratic form $f(x, y) = (a, b, c)$ of discriminant Δ, with Δ not a perfect square, is said **indefinite** if $\Delta > 0$, **positive definite** if $\Delta < 0$ and $a > 0$, **negative definite** if $\Delta < 0$ and $a < 0$.

It is easy to observe that $-f(x, y)$ is positive definite if $f(x, y)$ is negative definite and vice versa. In the light of this remark, if the quadratic form of equation 1.1 has negative discriminant, we can assume that $f(x, y)$ is positive definite. Hence, from now on, we will consider only indefinite and positive definite forms.

1.3 Equivalence of forms

In this section we introduce transformations between quadratic forms that do not change the discriminant and the represented integers (see [11, pag. 5]). These transformations will enable us to simplify the study of equation 1.1.

Two quadratic forms $f(x, y) = (a_1, b_1, c_1)$ and $g(x, y) = (a_2, b_2, c_2)$ are said **equivalent**, and we will write $f(x, y) \sim g(x, y)$, if there exist four integers r, s, t, u such that

$$f(rx + sy, tx + uy) = g(x, y) \tag{1.7}$$

and

$$ru - st = \pm 1 \tag{1.8}$$

In particular, when $ru - st = 1$ the forms $f(x, y)$ and $g(x, y)$ are said **properly equivalent**, and we will write $f(x, y) \sim_p g(x, y)$, while they are said **improperly equivalent**, with the notation $f(x, y) \sim_{imp} g(x, y)$, if $ru - st = -1$.

When $f(x, y)$ and $f(rx + sy, tx + uy) = g(x, y)$ are equivalent, we say that $f(x, y)$ **goes in** $g(x, y)$ through the transformation

$$\begin{cases} x = rx + sy \\ y = tx + uy \end{cases}$$

that is described by the matrix

$$\begin{pmatrix} r & s \\ t & u \end{pmatrix}$$

We can observe that $rs - tu$ is the determinant of the matrix that describes the transformation. Furthermore we have:

$$f(rx + sy, tx + uy) = a_1(rx + sy)^2 + b_1(rx + sy)(tx + uy)xy + c_1(tx + uy)^2 =$$

$$= (a_1r^2 + b_1rt + c_1t^2)x^2 + (2a_1rs + b_1(st + ru) + 2c_1tu)xy + (a_1s^2 + b_1su + c_1u^2)y^2 =$$

$$= a_2x^2 + b_2xy + c_2y^2 = g(x, y)$$

and hence

$$\begin{cases} a_2 = a_1r^2 + b_1rt + c_1t^2 = f(r,t) \\ b_2 = 2a_1rs + b_1(st + ru) + 2c_1tu \\ c_2 = a_1s^2 + b_1su + c_1u^2 = f(s,u) \end{cases}$$

As we expect, the defined binary relation in the set of all integral binary quadratic forms is an equivalence relation.

Theorem 1.6. *The binary relation "being equivalent to" ("being properly equivalent to") is an equivalent relation in the set of all quadratic forms.*

Proof. Given a quadratic form $f(x,y)$, it is clear that it is (properly) equivalent with itself. In fact $f(x,y)$ goes in itself by the transformation described by the 2×2 identity matrix. For the transitivity, suppose that $f(x,y) = (a_1, b_1, c_1)$ goes in $g(x,y) = (a_2, b_2, c_2)$ by the transformation

$$\begin{cases} x = r_1x + s_1y \\ y = t_1x + u_1y \end{cases}$$

and that $g(x,y)$ goes in $h(x,y) = (a_3, b_3, c_3)$ substituting x with $r_2x + s_2y$ and y with $t_2x + u_2y$. So:

$$\begin{aligned} g(x,y) &= a_1(r_1x + s_1y)^2 + b_1(r_1x + s_1y)(t_1x + u_1y) + c_1(t_1x + u_1y)^2 \\ h(x,y) &= a_1(r_1(r_2x + s_2y) + s_1(t_2x + u_2y))^2 + \\ &\quad + b_1(r_1(r_2x + s_2y) + s_1(t_2x + u_2y))(t_1(r_2x + s_2y) + u_1(t_2x + u_2y)) + \\ &\quad + c_1(t_1(r_2x + s_2y) + u_1(t_2x + u_2y))^2 = a_1((r_1r_2 + s_1t_2)x + (r_1s_2 + s_1u_2)y) + \\ &\quad + b_1((r_1r_2 + s_1t_2)x + (r_1s_2 + s_1u_2)y)((t_1r_2 + u_1t_2)x + (t_1s_2 + u_1u_2)y) + \\ &\quad + c_1((t_1r_2 + u_1t_2)x + (t_1s_2 + u_1u_2)y)^2 \end{aligned} \tag{1.9}$$

Therefore $f(x,y)$ is equivalent to $h(x,y)$ since $f(r_3x + s_3y, t_3x + u_3y) = h(x,y)$ with

$$\begin{pmatrix} r_3 & s_3 \\ t_3 & u_3 \end{pmatrix} = \begin{pmatrix} r_1 & s_1 \\ t_1 & u_1 \end{pmatrix} \begin{pmatrix} r_2 & s_2 \\ t_2 & u_2 \end{pmatrix}$$

The determinant of the matrix on the left is equal to the product of the determinants of the matrix on the right and so it is equal to ±1 (is equal to 1 if $f(x,y) \sim_p h(x,y)$ and $g(x,y) \sim_p h(x,y)$ or $f(x,y) \sim_{imp} g(x,y)$ and $g(x,y) \sim_{imp} h(x,y)$).

It remains to prove the simmetry of the binary relations. Assume that $f(x,y) = (a_1, b_1, c_1)$ goes on $g(x,y) = (a_2, b_2, c_2)$ by the transformation

$$\begin{cases} x = rx + sy \\ y = tx + uy \end{cases}$$

with $ru - st = \pm 1$. Since

$$\begin{pmatrix} r & s \\ t & u \end{pmatrix}^{-1} = (ru - st)\begin{pmatrix} u & -s \\ -t & r \end{pmatrix}$$

Using 1.9, from $g(x,y) = f(rx+sy, tx+uy)$ it follows that $g(x,y)$ goes in $f(x,y)$ by the transformation described by the matrix

$$(ru-st)\begin{pmatrix} u & -s \\ -t & r \end{pmatrix}$$

which has determinant $ru - st$ since $(ru-st)^2 = 1$. □

It is clear that the binary relation "be proper equivalent to" is contained in the binary relation "be equivalent to". Proving the transitivity of these binary relations, we have seen that, if two forms $f(x,y)$ and $h(x,y)$ are improperly equivalent to a form $g(x,y)$, then $f(,y)$ and $h(x,y)$ are properly equivalent.

1.4 Invariants of equivalent forms

We now want to see which properties have in common two equivalent quadratic forms $f(x,y) = (a_1, b_1, c_1)$, $g(x,y) = f(rx+sy, tx+uy) = (a_2, b_2, c_2)$.

Equivalent quadratic forms have the same discriminant

If Δ_1, Δ_2 are the discriminants of $f(x,y)$ and $g(x,y)$ respectively, then:

$$\Delta_2 = b_2^2 - 4a_2c_2 = (2a_1rs + b_1(st+ru) + 2c_1tu)^2 - 4(a_1r^2 + b_1rt + c_1t^2)(a_1s^2 + b_1su + c_1u^2) =$$

$$= (b_1^2 - 4a_1c_1)(ru-st)^2 = \Delta_1$$

Equivalent quadratic forms represent the same integers

If $f(x,y)$ represents an integer m , there exist $x_0, y_0 \in \mathbb{Z}$ such that $f(x_0,y_0) = m$. Therefore, we have $g(\pm(ux_0 - sy_0), \pm(-tx_0 + ry_0)) = f(x_0,y_0) = m$ for the simmetry of the equivalence relation. The sign of $ux_0 - sy_0$ and $-tx_0 + ry_0$ is $+$ when $f(x,y)$ and $g(x,y)$ are properly equivalent, is $-$ when $f(x,y)$ and $g(x,y)$ are improperly equivalent.

Equivalent quadratic forms properly represent the same integers

Let m be an integer such that $f(x_0,y_0) = m$, with $gcd(x_0,y_0) = 1$. Then $g(\pm(ux_0 - sy_0), \pm(-tx_0 + ry_0)) = f(x_0,y_0) = m$. Suppose that the greatest common divisor ℓ of $ux_0 - sy_0$ and $-tx_0 + ry_0$ is greater than 1. Since

$$\pm(r(ux_0 - sy_0) + s(-tx_0 + ry_0)) = x_0$$

$$\pm(t(ux_0 - sy_0) + u(-tx_0 + ry_0)) = y_0$$

ℓ divides both x_0 and y_0. This is a contradiction.

If $g(x, y)$ is primitive, $f(x, y)$ is primitive too

Suppose $gcd(a_1, b_1, c_1) = \ell > 1$. Then, from

$$\begin{cases} a_2 = a_1r^2 + b_1rt + c_1t^2 \\ b_2 = 2a_1rs + b_1(st + ru) + 2c_1tu \\ c_2 = a_1s^2 + b_1su + c_1u^2 \end{cases}$$

it follows that ℓ divides a_2, b_2, c_2. This is a contradiction.

If $f(x, y)$ is positive definite (respectively negative definite, indefinite) then $g(x, y)$ is positive definite (negative definite, idenfinite)

If $f(x, y)$ is indefinite, $g(x, y)$ is indefinite too since these two forms have the same discriminant. If $f(x, y)$ is positive definite, then $a_2 = f(r, t)$ is positive and then also $g(x, y)$ is positive definite.

1.5 Some results about the representation of integers

The aim of this section is to discuss some aspects of the representation of integers by quadratic forms. To begin with, for a quadratic form $f(x, y)$ of discriminant Δ one can ask if there exists a necessary and sufficient condition so that an integer m is represented by $f(x, y)$. The answer is contained in a result due to Lagrange (see [20, Lemma 2.3]).

Proposition 1.7. *A quadratic form $f(x, y) = (a, b, c)$ properly represents an integer m if and only if it is properly equivalent to a form $g(x, y) = (m, b', c')$, where b', c' are suitable integers.*

Proof. Suppose that $f(x, y)$ represents m properly. Then there exist two coprime integers, r and s, such that $f(r, s) = m$. For the Bézout identity, we can find $t, u \in \mathbb{Z}$ such that

$$ru - st = 1$$

Hence:

$$f(rx + ty, sx + uy) = f(r, s)x^2 + (2ars + b(st + ru) + 2ctu)xy + f(t, u)y^2 = (m, b', c')$$

On the other hand, if $f(x, y)$ is properly equivalent to (m, b', c'), since (m, b', c') represents properly m, the same holds for $f(x, y)$. □

The last proposition could be used to solve a weaker problem ([20, Lemma 2.5]): decide if an integer m could be properly represented by some quadratic forms having a fixed discriminant Δ.

Proposition 1.8. *Let Δ be an integer such that $\Delta \equiv 0, 1 \pmod 4$. If $m \in \mathbb{Z}$ is odd and $gcd(\Delta, m) = 1$ then m is properly represented by a quadratic form of discriminant Δ if and only if Δ is a square modulo m.*

Proof. Suppose that $f(x, y) = (a, b, c)$ is a quadratic form of discriminant Δ which properly represents m. By Proposition 1.7, we can assume $a = m$. Hence:

$$\Delta = b^2 - 4mc \quad \Rightarrow \quad \Delta \equiv b^2 \pmod m$$

Vice versa, suppose that Δ is a quadratic residue modulo m. Then there exists $b \in \mathbb{Z}$ such that $\Delta \equiv b^2 \pmod m$. We can assume that Δ and b have the same parity. In fact, if it is not the case, $m + b$ would have the same parity of Δ and $b + m \equiv b \pmod m$. This implies that $\Delta - b^2$ is divisible by 4 and hence $4m|\Delta - b^2$, since m is odd. Then there exists $c \in \mathbb{Z}$ such that $\Delta - b^2 = 4mc$. The quadratic form $f(x, y) = (m, b, c)$ has discriminant $b^2 - 4mc = \Delta$ and it represents properly m. Furthermore, it is primitive since $gcd(m, b) = 1$ (if $gcd(m, b)$ is greater than 1 it divides Δ too, contradicting the hypothesis $gcd(m, \Delta) = 1$). □

Corollary 1.9. *Let n be an integer and $p \in \mathbb{Z}$ an odd prime that doesn't divide n. Then p is properly represented by a quadratic form of discriminant $4n$ if and only if $(n/p) = 1$.*

Proof. Using Proposition 1.8, since $gcd(4n, p) = 1$, we have that p is properly represented by a primitive quadratic form of discriminant $4n$ if and only if $(4n/p) = 1$. But, for the properties of the Legendre Symbol, we have:

$$(4n/p) = (n/p)$$

□

If $\Delta \in \mathbb{Z}$ is a discriminant, i.e $\Delta \equiv 0, 1 \pmod 4$, it is a quadratic residue modulo an odd integer m, coprime with Δ, if and only if it is a quadratic residue modulo any prime factor of m. For the sake of completeness, we report the proof of this result, obtained by adapting Proposition 5.1.1 of [32].

Proposition 1.10. *Let $\Delta \in \mathbb{Z}$ be such that $\Delta \equiv 0, 1 \pmod 4$. If m is an odd integer coprime with Δ, then Δ is a quadratic residue modulo $m = p_1^{e_1} \cdots p_s^{e_s}$ (with $p_1, \dots, p_s$ distinct odd primes and $e_1, \dots, e_s \in \mathbb{N}$) if and only if Δ is a quadratic residue modulo modulo p_i, for every $i \in \{1, \dots, s\}$.*

Proof. If x is an integer such that $x^2 \equiv \Delta \pmod m$, clearly $x^2 \equiv \Delta \pmod{p_i^{e_i}}$ for every $i \in \{1, \dots, s\}$. In order to prove the reverse implication, we claim that the congruence $y^2 \equiv \Delta \pmod{p_i^\ell}$, with $i \in \{1, \dots, s\}$, is solvable for every non-zero natural number ℓ if $y^2 \equiv \Delta \pmod{p_i}$ is solvable. We proceed by induction on ℓ. Suppose that y_0 is a solution of the congruence $y^2 \equiv \Delta \pmod{p_i^\ell}$ with ℓ natural number grater than 1. Setting $y_1 = y_0 + bp_i^\ell$, with $b \in \mathbb{Z}$, we have

$$y_1^2 = y_0^2 + b^2 p_i^{2\ell} + 2by_0 p_i^\ell \equiv y_0^2 + 2by_0 p_i^\ell \pmod{p_i^{\ell+1}}$$

since $2\ell > \ell + 1$. If we choose b such that

$$2by_0 \equiv \frac{\Delta - y_0^2}{p_i^\ell} \pmod{p_i}$$

for this value of b we would have

$$2by_0 - \frac{\Delta - y_0^2}{p_i^\ell} = rp_i \quad r \in \mathbb{Z} \qquad \Rightarrow \qquad 2by_0p_i^\ell - (\Delta - y_0^2) = rp_i^{\ell+1}$$

and then

$$y_1^2 \equiv y_0^2 + 2by_0p_i^\ell \equiv y_0^2 + (\Delta - y_0^2) = \Delta \pmod{p_i^{\ell+1}}$$

Such a b exists because $\Delta \not\equiv 0 \pmod{p_i}$ and $\Delta \equiv y_0^2 \pmod{p_i}$, so $2y_0 \not\equiv 0 \pmod{p_i}$. Now suppose that $z_1, \dots, z_s \in \mathbb{Z}$ are such that $(z_i)^2 \equiv \Delta \pmod{p_i}$ for every i in $\{1, \dots, s\}$. Hence we have $(x_i)^2 \equiv \Delta \pmod{p_i^{\ell_i}}$ for some $x_i \in \mathbb{Z}$. Using the Chinese remainder theorem, we can find $x \in \mathbb{Z}$ such that $x \equiv x_i \pmod{p_i^{\ell_i}}$ for every $i \in \{1, \dots, s\}$. So $x^2 \equiv \Delta \pmod{p_i^{\ell_i}}$ and hence $x^2 \equiv \Delta \pmod{m}$. In fact, $x^2 - \Delta$ is divisible by $p_1^{e_1}$, i.e. $x^2 - \Delta = hp_1^{e_1}$ for some $h \in \mathbb{Z}$, is divisible by $p_2^{e_2}$, and $p_2^{e_2}|h$ since $p_1 \neq p_2$ and so on. □

In the light of Proposition 1.8, last result says that an odd integer m is represented by some quadratic form of discriminant Δ, with $gcd(\Delta, m) = 1$, if and only if all the prime factors of m are represented by some form of discriminant Δ. On the other hand, if p is an odd prime integer, coprime with Δ and represented by some quadratic form $f(x, y)$ of discriminant Δ, the following Proposition (see [17, pag. 200]) says that the only quadratic forms of discriminant Δ that represent p are those properly or improperly equivalent to $f(x, y)$.

Proposition 1.11. *Let $f(x, y)$, $g(x, y)$ be two quadratic forms with the same discriminant Δ. If the odd prime p is represented by both $f(x, y)$ and $g(x, y)$ we have $f(x, y) \sim_p g(x, y)$ or $f(x, y) \sim_{imp} g(x, y)$.*

Proof. By Proposition 1.7 and equation 1.9, we can assume $f(x, y) = (p, b_1, c_1)$ and $g(x, y) = (p, b_2, c_2)$. Then, from

$$\Delta = b_1^2 - 4pc_1 = b_2^2 - 4pc_2$$

it follows $b_1^2 \equiv b_2^2 \pmod{p}$. So $b_1 \equiv b_2 \pmod{p}$ or $b_1 \equiv -b_2 \pmod{p}$. Since b_1 and b_2 have the same parity of Δ, we have:

$$b_2 = \pm b_1 + 2\ell p \tag{1.10}$$

with $\ell \in \mathbb{Z}$, because p is odd. If $b_2 = b_1 + 2\ell p$, the form $f(x + \ell y, y) = (p, 2p\ell + b_1, f(\ell, 1))$ is equal to $g(x, y)$ and properly equivalent to $f(x, y)$; if $b_2 = b_1 - 2\ell p$, the form $f(x + \ell y, -y) = (p, -b_1 + 2\ell p, f(-\ell, 1))$ is equal to $g(x, y)$ and improperly equivalent to $f(x, y)$. □

1.6 Composition of forms

In this section we introduce a multiplication between forms of a fixed discriminant: the composition of forms. This binary operation was discovered by Gauss and published in his “Disquisitiones Arithmeticae" (see [26, art. 234]). The starting point is the following definition ([20, pag. 47]):

Definition 1.12. *Let $f(x, y)$ and $g(x, y)$ be two quadratic forms of discriminant Δ. A third binary quadratic form $F(x, y)$ is a composition of $f(x, y)$ and $g(x, y)$ if:*

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

where

$$B_i(x, y, w, z) = d_i xw + e_i xz + \ell_i yw + n_i yz \qquad d_i, e_i, \ell_i, n_i \in \mathbb{Z}$$

with $i \in \{1, 2\}$. Furthermore, if

$$\begin{cases} f(1, 0) = d_1e_2 - d_2e_1 \\ g(1, 0) = d_1\ell_2 - d_2\ell_1 \end{cases}$$

we will say that $F(x, y)$ is a direct composition of $f(x, y)$ and $g(x, y)$.

If $f(x, y)$ represents an integer m_1, i.e. $f(x_0, y_0) = m_1$ for some $x_0, y_0 \in \mathbb{Z}$, and $g(x, y)$ represents an integer m_2, i.e. $g(w_0, z_0) = m_2$ for some $w_0, z_0 \in \mathbb{Z}$, then a composition $F(x, y)$ of $f(x, y)$ and $g(x, y)$ represents m_1m_2:

$$F(B_1(x_0, y_0, w_0, z_0), B_2(x_0, y_0, w_0, z_0)) = f(x_0, y_0)g(w_0, z_0) = m_1m_2$$

The main result of Gauss's theory of composition of forms, is that the direct composition makes $C(\Delta)$, with $\Delta \in \mathbb{Z}$ such that it is not a perfect square and $\Delta \equiv 0, 1 \pmod 4$, an abelian group. The existence of the group structure is easier to prove using the rule to compose forms, based on the united forms, introduced by Dirichlet. If not specified otherwise, a reference for the rest of the section is [20, § 3].

Definition 1.13. *Two quadratic forms $f(x, y) = (a_1, b_1, c_1)$ and $g(x, y) = (a_2, b_2, c_2)$, with the same discriminant Δ, are said united if:*

$$gcd\left(a_1, a_2, \frac{b_1 + b_2}{2}\right) = 1$$

We observe that $(b_1 + b_2)/2$ is an integer since b_1 and b_2 have the same parity of Δ.

In order to use the united forms to specify a method to compose forms we need two lemmas.

Lemma 1.14. *Let $a_1, b_1, \dots, a_r, b_r, m$ be integers such that $gcd(a_1, \dots, a_r, m) = 1$. Then the system of linear congruences*

$$\begin{cases} a_1 x \equiv b_1 & \pmod{m} \\ \cdots & \\ a_r x \equiv b_r & \pmod{m} \end{cases}$$

has a unique solution modulo m if

$$a_i b_j \equiv a_j b_i \pmod{m}$$

for every $i, j \in \{1, \dots, r\}$.

Proof. For the Bézout identity, there exist $r+1$ integers $\ell_1, \dots, \ell_r, \ell$ such that

$$\ell_1 a_1 + \cdots + \ell_r a_r + \ell m = 1$$

For a j in $\{1, \dots, r\}$ we have:

$$-\ell m b_j = -b_j + \ell_1 a_1 b_j + \cdots + \ell_r a_r b_j$$

If $a_i b_j \equiv a_j b_i \pmod{m}$ for every $i, j \in \{1, \dots, r\}$, then

$$-b_j + \ell_1 a_1 b_j + \cdots + \ell_r a_r b_j \equiv -b_j + (\ell_1 b_1 + \cdots + \ell_r b_r) a_j \equiv 0 \pmod{m}$$

Setting $x = \ell_1 b_1 + \cdots + \ell_r b_r$ we have

$$a_j x \equiv b_j \pmod{m}$$

It remains to prove the uniqueness, modulo m, of the solution. Let x' be a second solution of the system. Hence:

$$a_j x \equiv a_j x' \pmod{m} \qquad \forall j \in \{1, \dots, r\}$$

The set $\mathcal{L}$ composed by the a_j's that are non-zero modulo m is not empty. Hence $m' = gcd(x - x', m)$ is greater than 1 and $m = m'm''$. If $a_j \in \mathcal{L}$, then $m'' | a_j$ and $gcd(a_1, \dots, a_r, m) \geq m''$. Hence $m'' = 1$ and $gcd(x - x', m) = m$. That means $x \equiv x' \pmod{m}$. □

Lemma 1.15. *Let $f(x, y) = (a_1, b_1, c_1)$ and $g(x, y) = (a_2, b_2, c_2)$ be two united forms of discriminant Δ. Then there exist two integers B, C, with B unique modulo $2a_1a_2$, such that:*

$$\begin{cases} B \equiv b_1 & \pmod{2a_1} \\ B \equiv b_2 & \pmod{2a_2} \\ B^2 \equiv \Delta & \pmod{4a_1a_2} \end{cases}$$

and $f(x, y)$, $g(x, y)$ properly equivalent to $(a_1, B, a_2C), (a_2, B, a_1C)$ respectively.

Proof. If an integer B satisfies the first two congruences of the system, then $B - b_1 = 2a_1h$ and $B - b_2 = 2a_2k$ for some $h, k \in \mathbb{Z}$. Hence $(B - b_1)(B - b_2) = 4a_1a_2hk$ and

$$B^2 - (b_1 + b_2)B + b_1b_2 = (B - b_1)(B - b_2) \equiv 0 \pmod{4a_1a_2}$$

So we have:

$$B^2 \equiv \Delta \pmod{4a_1a_2} \Leftrightarrow (b_1 + b_2)B - b_1b_2 \equiv \Delta \pmod{4a_1a_2} \Leftrightarrow$$

$$\Leftrightarrow \frac{b_1 + b_2}{2}B \equiv \frac{\Delta + b_1b_2}{2} \pmod{2a_1a_2}$$

with $b_1 + b_2$ and $\Delta + b_1b_2$ even since b_1 and b_2 have the same parity of Δ. Hence, the starting system is equivalent to:

$$\begin{cases} B \equiv b_1 & \pmod{2a_1} \\ B \equiv b_2 & \pmod{2a_2} \\ \frac{b_1+b_2}{2}B \equiv \frac{\Delta+b_1b_2}{2} & \pmod{2a_1a_2} \end{cases}$$

Furthermore we can observe that:

$$B \equiv b_1 \pmod{2a_1} \Leftrightarrow a_2B \equiv a_2b_1 \pmod{2a_1a_2}$$

Applying the same to the second congruence, we obtain a new equivalent system:

$$\begin{cases} a_2B \equiv a_2b_1 & \pmod{2a_1a_2} \\ a_1B \equiv a_1b_2 & \pmod{2a_1a_2} \\ \frac{b_1+b_2}{2}B \equiv \frac{\Delta+b_1b_2}{2} & \pmod{2a_1a_2} \end{cases}$$

Since we are assuming that $f(x, y)$ and $g(x, y)$ are united, then:

$$gcd\left(a_1, a_2, \frac{b_1 + b_2}{2}, 2a_1a_2\right) = 1$$

and we can apply Lemma 1.14. In fact we can observe that:

- $a_2(a_1b_2) = a_1(a_2b_1)$;
- since $a_2\Delta \equiv a_2b_1^2 \pmod{2a_1a_2}$, we have

$$a_2(b_1b_2 + \Delta)/2 \equiv (a_2b_1^2 + a_2b_1b_2)/2 = (b_1 + b_2)a_2b_1/2 \pmod{2a_1a_2}$$

- since $a_1\Delta \equiv a_1b_2^2 \pmod{2a_1a_2}$, we have

$$a_1(b_1b_2 + \Delta)/2 \equiv (a_1b_2^2 + a_1b_1b_2)/2 = (b_1 + b_2)a_1b_2/2 \pmod{2a_1a_2}$$

So the system has a solution B unique modulo $2a_1a_2$. Since $B = b_1 + 2a_1s$ for some $s \in \mathbb{Z}$, we have that $f(x + sy, y) = (a_1, B, a_2C)$ where:

$$C = \frac{B^2 - \Delta}{4a_1a_2} \in \mathbb{Z}$$

In the same way, from $B = b_2 + 2a_2s'$ for some $s' \in \mathbb{Z}$ we obtain $g(x+s'y, y) = (a_2, B, a_1C)$. □

The **Dirichlet composition** $f(x, y) \circ g(x, y)$ of two united forms $f(x, y) = (a_1, b_1, c_1)$, $g(x, y) = (a_2, b_2, c_2)$ of discriminant Δ, is defined as the quadratic form

$$F(x, y) = f(x, y) \circ g(x, y) = \left(a_1a_2, B, \frac{B^2 - \Delta}{4a_1a_2} = C\right)$$

where B and C are the integers of Lemma 1.15.
The quadratic form $F(x, y) = f(x, y) \circ g(x, y)$ has the following properties:

1. *$F(x, y)$ has the same discriminant of $f(x, y)$ and $g(x, y)$.* In fact $B^2 - 4a_1a_2(\frac{B^2-\Delta}{4a_1a_2})$ is equal to Δ;

2. *If Δ is negative and $f(x, y)$, $g(x, y)$ are both positive definite, then $F(x, y)$ is positive definite.* We have $a_1a_2 > 0$ since, for hypothesis, both a_1 and a_2 are positive;

3. *$F(x, y)$ is primitive if $f(x, y)$ and $g(x, y)$ are primitive.* Suppose that the prime integer $p > 1$ divides a_1a_2, B and C. Then we can assume that it divides a_1 and so (a_1, B, a_2C) is not primitive. This is a contradiction since $f(x, y)$ is properly equivalent to (a_1, B, a_2C) by Lemma 1.15;

4. *If B' is another solution of the system of Lemma 1.15, then the quadratic form $F'(x, y) = (a_1a_2, B', (\Delta - B'^2)/4a_1a_2)$ is properly equivalent to $F(x, y)$.* We are looking for four integers r, s, t, u such that $ru - st = 1$ and $F(rx + sy, tx + uy) = F'(x, y)$. Let us fix $r = u = 1$ and $t = 0$. Since $B \equiv B' \pmod{2a_1a_2}$, there exists $\ell \in \mathbb{Z}$ such that $B' = B + 2a_1a_2\ell$. Setting $s = \ell$ we have

$$2a_1a_2rs + B(ru + st) + 2\frac{B^2 - \Delta}{4a_1a_2}tu = 2a_1a_2s + B = B'$$

   From $F(r, t) = a_1a_2$ it follows $F(rx + sy, tx + uy) = F'(x, y)$ because $F(x, y)$ and $F'(x, y)$ have the same discriminant Δ;

5. *$F(x, y) = f(x, y) \circ g(x, y)$ is a direct composition of $f(x, y)$ and $g(x, y)$.*
   By Lemma 1.15, $f(x, y)$ is properly equivalent to the form $f_1(x, y) = (a_1, B, a_2C)$ while $g(x, y)$ is properly equivalent to $g_1(x, y) = (a_2, B, a_1C)$. By a direct computation one can easily prove that:

$$f_1(x, y)g_1(w, z) = F(xw - Cyz, a_1xz + a_2yw + Byz) \tag{1.11}$$

From the proof of Lemma 1.15 we know that:

$$f_1(x,y) = f(x+sy,y) \quad ; \quad g_1(w,z) = g(w+s'z,z)$$

with $s, s' \in \mathbb{Z}$. Hence

$$f(x,y) = f_1(x-sy,y) = a_1(x-sy)^2 + B(x-sy)y + a_2Cy^2$$

$$g(w,z) = g_1(w-s'z,z) = a_2(w-s'z)^2 + B(w-s'z)z + a_1Cz^2$$

From this follows:

$$f(x,y)g(w,z) = f_1(x-sy,y)g_1(w-s'z,z) =$$

$$= F((x-sy)(w-s'z) - Cyz, a_1(x-sy)z + a_2(w-s'z)y + Byz) =$$

$$= F(xw - s'xz - syw + (ss'-C)yz, a_1xz + a_2yw + (-a_1s - a_2s' + B)yz)$$

Following the notation of Definition 1.12 we have $d_1 = 1$, $d_2 = 0$, $e_1 = -s'$, $e_2 = a_1$, $\ell_1 = -s$, $\ell_2 = a_2$, $n_1 = ss' - C$, $n_2 = -a_1s - a_2s' + B$ and therefore:

$$d_1e_2 - d_2e_1 = a_1 = f(1,0)$$

$$d_1\ell_2 - d_2\ell_1 = a_2 = g(1,0)$$

If $f(x,y)$ and $g(x,y)$ are two united forms of discriminant Δ, we define:

$$[f(x,y)] \circ [g(x,y)] = [F(x,y)] \tag{1.12}$$

where $F(x,y)$ is the Dirichlet composition of $f(x,y)$ and $g(x,y)$. For the properties seen above $[F(x,y)]$ belongs to $C(\Delta)$. We ask ourself if in this fashion we can compose any two elements of $C(\Delta)$. That question is answered by the following result [45, Lemma 3.1].

Proposition 1.16. *If $f(x,y) = (a,b,c)$ is a primitive quadratic form and m an integer, then $f(x,y)$ represents properly a positive integer relatively prime with m.*

Proof. Let $m = p_1^{r_1}p_2^{r_2}\cdots p_s^{r_s}$ be the prime factor decomposition of m. We can define:

$$A = \{p_1, \ldots, p_s\}$$

$$A_1 = \{p \in A : p \mid a \wedge p \mid c\}$$

$$A_2 = \{p \in A : p \mid a \wedge p \nmid c\}$$

$$A_3 = \{p \in A : p \nmid a \wedge p \mid c\}$$

$$A_4 = \{p \in A : p \nmid a \wedge p \nmid c\}$$

Clearly A_1, A_2, A_3, A_4 are pairwise disjoint and such that their union is A. Let P, Q, R, S be the integers obtained multiplying, respectively, the elements of A_1, A_2, A_3, A_4. We want to show that $f(Q,RS) = aQ^2 + bQRS + c(RS)^2 = \ell$ is relatively prime with m. We observe

that $gcd(\ell, m) \neq 1$ if and only if there exists a prime integer p that divides ℓ and m. So it is sufficient to show that every element of A does not divide ℓ.
If $p \in A_1$, it divides aQ^2 and $c(RS)^2$. But it does not divide b (since f is primitive) and Q, R, S for construction. Therefore $p \nmid \ell$.
If $p \in A_2$, it divides aQ^2 and $b(QRS)$. But it does not divide c and P, R, S for construction. Therefore $p \nmid \ell$.
If $p \in A_3$, it divides $c(RS)^2$ and $bQRS$. But it does not divide a and P, Q, S for construction. Therefore $p \nmid aQ^2$.
If $p \in A_4$, it divides $bQRS$ and $c(RS)^2$ for construction. But it does not divide a and P, Q, R. Therefore $p \nmid aQ^2$.

We can assume Q coprime with RS because a divisor of ℓ is still coprime with m. When the discriminant $\Delta = b^2 - 4ac$ of the form $f(x, y)$ is negative, then ℓ is positive. Now suppose that Δ is positive and ℓ is negative. Considering the form $g(x, y) = (\ell, b', c')$, properly equivalent to $f(x, y)$, if we set $x_0 = b'mt + 1$, $y_0 = -2\ell mt$, with t non-zero integer, we can deduce that:

$$g(x_0, y_0) = \ell(1 - \Delta m^2 t^2)$$

is a positive integer. Furthermore, $g(x_0, y_0)$ is coprime with m because $gcd(\ell, m) = 1$.
If $b' \neq 0$, we can choose $t = 2\ell b'$ obtaining

$$x_0 = 2(b')^2 \ell m + 1 \quad , \qquad y_0 = -4b'\ell^2 m$$

with x_0 and y_0 coprime. If $b' = 0$, then $x_0 = 1$, $y_0 = -2\ell mt$ and

$$g(x_0, y_0) = \ell + 4c'\ell^2 m^2 t^2 = \ell(1 + 4c'\ell m^2 t^2)$$

that is positive since $\Delta = -4c'\ell > 0$. □

Lemma 1.17. *Let $f(x, y) = (a, b, c)$ and $g(x, y) = (a', b', c')$ be two primitive quadratic forms with the same discriminant Δ. Then there exists a third quadratic form $h(x, y)$, properly equivalent to $g(x, y)$, such that $f(x, y)$ and $h(x, y)$ are united.*

Proof. By Proposition 1.16 $g(x, y)$ represents properly an integer ℓ relatively prime with a. Hence $g(x, y)$ is properly equivalent to $h(x, y) = (\ell, b'', c'')$. Therefore the two forms $f(x, y)$ and $h(x, y)$ are united since from $gcd(a, \ell) = 1$ follows $gcd(a, \ell, (b + b'')/2) = 1$. □

The last Proposition shows that a pair of proper equivalence classes of $C(\Delta)$ could always be composed. Now we want to verify that the binary operation introduced in $C(\Delta)$ is well defined. In order to prove it, following [57, § 10], we use an equivalent condition to ascertain if two quadratic forms are properly equivalent.

Lemma 1.18. *Let $f(x, y) = (a_1, b_1, c_1)$ and $g(x, y) = (a_2, b_2, c_2)$ be two primitive quadratic forms with the same discriminant Δ. They are properly equivalent if and only if there exist $r, t \in \mathbb{Z}$ such that:*

$$\begin{cases} f(r, t) = a_2 \\ 2a_1 r + (b_1 + b_2)t \equiv 0 \pmod{2a_2} \\ (b_1 - b_2)r + 2c_1 t \equiv 0 \pmod{2a_2} \end{cases}$$

Proof. If $f(x,y)$ is properly equivalent to $g(x,y)$ there exist four integers r,s,t,u such that $f(r,t)=a_2$ and

$$\begin{cases} ru-ts=1 \\ (b_1r+2c_1t)u+(b_1t+2a_1r)s=b_2 \end{cases}$$

The last system could be written in matrix notation as:

$$\begin{pmatrix} r & -t \\ b_1r+2c_1t & b_1t+2a_1r \end{pmatrix}\begin{pmatrix} u \\ s \end{pmatrix}=\begin{pmatrix} 1 \\ b_2 \end{pmatrix}$$

The determinant of the 2x2 matrix is:

$$r(b_1t+2a_1r)+t(b_1r+2c_1t)=2(a_1r^2+b_1rt+c_1t^2)=2a_2$$

which is non-zero since we are considering irreducible forms. Therefore:

$$2a_2\begin{pmatrix} u \\ s \end{pmatrix}=\begin{pmatrix} b_1t+2a_1r & t \\ -b_1r-2c_1t & r \end{pmatrix}\begin{pmatrix} 1 \\ b_2 \end{pmatrix}$$

that means

$$\begin{cases} 2a_2u=b_1t+2a_1r+tb_2=(b_1+b_2)t+2a_1r \\ 2a_2s=-b_1r-2c_1t+rb_2=(b_2-b_1)r-2c_1t \end{cases}$$

and the necessary condition is proved. Proceeding in the reverse way we easily arrive to the sufficient condition using the fact that two quadratic forms are equal if they have the same discriminant and the same first two coefficients. □

Proposition 1.19. *Let $f(x,y)=(a_1,b_1,c_1)$ and $g(x,y)=(a_2,b_2,c_2)$ be two united forms. Suppose that also $f'(x,y)=(a_3,b_3,c_3)$ and $g'(x,y)=(a_4,b_4,c_4)$ are united and such that $f(x,y)$ is properly equivalent to $f'(x,y)$, $g(x,y)$ is properly equivalent to $g'(x,y)$. Then $f(x,y)\circ g(x,y)$ is properly equivalent to $f'(x,y)\circ g'(x,y)$.*

Proof. By Lemma 1.15 there exist $B,C,B',C'\in\mathbb{Z}$ such that:

$$\begin{aligned} f(x,y) &\sim_p (a_1,B,a_2C) \\ g(x,y) &\sim_p (a_2,B,a_1C) \\ f'(x,y) &\sim_p (a_3,B',a_4C') \\ g'(x,y) &\sim_p (a_4,B',a_3C') \end{aligned} \tag{1.13}$$

so, by Lemma 1.18, we can find $r,t,r',t'\in\mathbb{Z}$ for which:

$$\begin{cases} a_1r^2+Brt+a_2Ct^2=a_3 \\ 2a_1r+(B+B')t\equiv 0 \pmod{2a_3} \\ (B-B')r+2a_2Ct\equiv 0 \pmod{2a_3} \end{cases}$$

$$\begin{cases} a_2r'^2 + Br't' + a_1Ct'^2 = a_4 \\ 2a_2r' + (B+B')t' \equiv 0 & \pmod{2a_4} \\ (B-B')r' + 2a_1Ct' \equiv 0 & \pmod{2a_4} \end{cases}$$

Using the same lemma, we want to find two integers R and T such that:

$$\begin{cases} a_1a_2R^2 + BR + CT^2 = a_3a_4 \\ 2a_1a_2R + (B+B')T \equiv 0 & \pmod{2a_3a_4} \\ (B-B')R + 2CT \equiv 0 & \pmod{2a_3a_4} \end{cases}$$

Since (a_1, B, a_2C) represents a_3 and (a_2, B, a_1C) represents a_4, using equation 1.11 we can set

$$\begin{cases} R = rr' - Ctt' \\ T = a_1rt' + a_2tr' + Btt' \end{cases}$$

Furthermore we know that

$$\begin{cases} a_1r + \frac{B+B'}{2}t \equiv 0 & \pmod{a_3} \\ a_2r' + \frac{B+B'}{2}t' \equiv 0 & \pmod{a_4} \end{cases}$$

and then

$$2\left(a_1r + \frac{B+B'}{2}t\right)\left(a_2r' + \frac{B+B'}{2}t'\right) \equiv 0 \pmod{2a_3a_4}$$

Replacing B'^2 with $B^2 - 4a_1a_2C + 4a_3a_4C'$, a direct computation shows that

$$2a_1a_2R + (B+B')T \equiv 2\left(a_1r + \frac{B+B'}{2}t\right)\left(a_2r' + \frac{B+B'}{2}t'\right) \equiv 0 \pmod{2a_3a_4} \quad (1.14)$$

So R and T satisfy also the second congruence of the last system. To prove that R and T satisfy the third congruence, we use four relations that could be easily obtained by a direct computation:

$$2a_1\left(\frac{B-B'}{2}R + CT\right) \equiv 2\left(a_1r + \frac{B+B'}{2}t\right)\left(\frac{B-B'}{2}r' + a_1Ct'\right) \equiv 0 \pmod{2a_3a_4}$$

$$2a_2\left(\frac{B-B'}{2}R + CT\right) \equiv 2\left(\frac{B-B'}{2}r + a_2Ct\right)\left(a_2r' + \frac{B+B'}{2}t'\right) \equiv 0 \pmod{2a_3a_4}$$

$$(B-B')\left(\frac{B-B'}{2}R + CT\right) \equiv 2\left(\frac{B-B'}{2}r + a_2Ct\right)\left(\frac{B-B'}{2}r' + a_1Ct'\right) \equiv 0 \pmod{2a_3a_4}$$

$$(B+B')\left(\frac{B-B'}{2}R + CT\right) \equiv 2C\left(a_1r + \frac{B+B'}{2}t\right)\left(a_2r' + \frac{B+B'}{2}t'\right) \equiv 0 \pmod{2a_3a_4}$$

From the last two congruences, follows

$$2B\left(\frac{B-B'}{2}R + CT\right) \equiv 0 \pmod{2a_3a_4}$$

If $(B-B')R/2+CT \equiv 0 \pmod{2a_3a_4}$ then R and T clearly satisfy the third congruence of the system. On the other hand, if $gcd((B-B')R/2+CT, 2a_3a_4) < 2a_3a_4$, then $gcd(2a_1, 2a_2, 2B, 2a_2a_3)$ must be greater than 1. But

$$gcd(2a_1, 2a_2, 2B, a_3a_4) = 2gcd(a_1, a_2, B, a_3a_4) = 2$$

since (a_1, B, a_2C) is a primitive form. Then:

$$\frac{B-B'}{2}R + CT \equiv 0 \pmod{a_3a_4}$$

and we have done also in this case.

□

Now we are ready to state and prove the main theorem about the composition of forms.

Theorem 1.20. *Let $C(\Delta)$ be the set of the proper equivalence classes of the primitive quadratic forms of discriminant Δ. The composition of elements of $C(\Delta)$ induced by the Dirichlet composition of forms is a binary operation in $C(\Delta)$ that gives to $C(\Delta)$ the structure of an abelian group. The proper equivalence class that contains the principal form of discriminant Δ is the identity element and the inverse of a proper equivalence class $[(a,b,c)]$ is $[(a,-b,c)]$.*

The abelian group $C(\Delta)$ is called **form class group of discriminant** Δ or, more simply, **class group of discriminant** Δ.

Proof. By Lemma 1.17, we can always compose two proper equivalence classes that belong to $C(\Delta)$. Composing them we obtain another element of $C(\Delta)$ thanks to the properties of the Dirichlet composition between quadratic forms. Hence the composition of elements of $C(\Delta)$ is a binary operation in $C(\Delta)$. Its properties are showed in the following lines.

Commutativity
Given two united forms, $f(x,y) = (a_1, b_1, c_1)$ and $g(x,y) = (a_2, b_2, c_2)$, it is clear that the integer B of Lemma 1.15 does not depend on which order we consider $f(x,y)$ and $g(x,y)$. The same holds for $F(x,y) = f(x,y) \circ g(x,y)$.

Identity element
If $\Delta \equiv 0 \pmod 4$, the principal form of discriminated Δ is $Q_0(x,y) = x^2 - (\Delta/4)y^2$. Consider a generic element $[(a,b,c)]$ of $C(\Delta)$. It is obvious that $Q_0(x,y)$ and (a,b,c) are united. Since:

$$\begin{cases} b \equiv b & \pmod{2a} \\ b \equiv 0 & \pmod{2} \\ b^2 \equiv \Delta & \pmod{4a} \end{cases}$$

the Dirichlet composition of (a,b,c) and $Q_0(x,y)$ is:

$$\left(a, b, \frac{b^2-\Delta}{4a}\right) = (a,b,c)$$

On the other hand, if $\Delta \equiv 1 \pmod 4$ the principal form is $Q_0(x,y) = (1, 1, -(\Delta-1)/4)$. Given a generic primitive quadratic form $f(x,y) = (a,b,c)$ of discriminant Δ, it is clearly united with $Q_0(x,y)$. Furthermore, we have

$$\begin{cases} b \equiv b & \pmod{2a} \\ b \equiv 1 & \pmod 2 \\ b^2 \equiv \Delta & \pmod{4a} \end{cases}$$

since b is odd. Therefore the Dirichlet composition of $f(x,y)$ and $Q_0(x,y)$ is:

$$\left(a, b, \frac{b^2-\Delta}{4a}\right) = (a,b,c)$$

Inverse of an element
Let $[f(x,y)]$ be a generic element of $C(\Delta)$, with $f(x,y) = (a,b,c)$. The quadratic form $g(x,y) = (c,b,a)$ is primitive, of discriminant Δ and positive definite if $f(x,y)$ is positive definite. Since:

$$gcd\left(a, c, \frac{b+b}{2}\right) = 1$$

$f(x,y)$ and $g(x,y)$ are united. From:

$$\begin{cases} b \equiv b & \pmod{2a} \\ b \equiv b & \pmod{2c} \\ b^2 \equiv \Delta & \pmod{4ac} \end{cases}$$

we have that $f(x,y) \circ g(x,y) = (ac, b, (b^2-\Delta)/4ac) = (ac, b, 1)$ that is properly equivalent to $(1, -b, ac)$. We want to show that every primitive quadratic form $f'(x,y) = (1, b', c')$ of discriminant Δ is properly equivalent to the principal form of discriminant Δ. If $\Delta \equiv 0 \pmod 4$, the principal form is $Q_0(x,y) = (1, 0, -\Delta/4)$. Setting $r = u = 1$, $t = 0$ and s such that $b' = -2s$, we obtain $f'(rx+sy, tx+uy) = (1, 0, -\Delta/4)$ since

$$2rs + b'(st+ru) + 2c'tu = 2s + b' = 0$$

If $\Delta \equiv 1 \pmod 4$ the principal form is $Q_0(x,y) = (1, 1, -(\Delta-1)/4)$. As before, we can set $r = u = 1$, $t = 0$ and s such that $b' = -2s+1$. Then $f'(rx+sy, tx+uy) = (1, 1, -(\Delta-1)/4)$ since

$$2rs + b'(st+ru) + 2c'tu = 2s + b' = 1$$

Finally, the form $g(x,y) = (c,b,a)$ is properly equivalent to $(a, -b, c)$:

$$g(-y, x) = (a, -b, c)$$

Associativity

Consider three proper equivalence classes contained in $C(\Delta)$. Let $f(x,y) = (a_1, b_1, c_1)$ be a form contained in the first proper equivalence class. Then, using Lemma 1.16, we can choose $g(x,y) = (a_2, b_2, c_2)$ in the second proper equivalence class such that $gcd(2a_1, a_2) = 1$ and $h(x,y) = (a_3, b_3, c_3)$ in the third proper equivalence class such that $gcd(a_3, 2a_1a_2) = 1$. This implies

$$gcd(a_1, a_2) = gcd(a_2, a_3) = gcd(a_1, a_3) = 1$$

We have $f(x,y) \circ g(x,y) = (a_1a_2, B, C)$ with B solution of the system:

$$\begin{cases} B \equiv b_1 & \pmod{2a_1} \\ B \equiv b_2 & \pmod{2a_2} \\ B^2 \equiv \Delta & \pmod{4a_1a_2} \end{cases}$$

and $(f(x,y) \circ g(x,y)) \circ h(x,y) = (a_1a_2a_3, B', C')$ with B' such that

$$\begin{cases} B' \equiv B & \pmod{2a_1a_2} \\ B' \equiv b_3 & \pmod{2a_3} \\ (B')^2 \equiv \Delta & \pmod{4a_1a_2a_3} \end{cases}$$

On the other hand, $g(x,y) \circ h(x,y) = (a_2a_3, N, L)$ with N solution of the system

$$\begin{cases} N \equiv b_2 & \pmod{2a_2} \\ N \equiv b_3 & \pmod{2a_3} \\ N^2 \equiv \Delta & \pmod{4a_2a_3} \end{cases}$$

and $f(x,y) \circ (g(x,y) \circ h(x,y)) = (a_1a_2a_3, N', L')$ with N' such that

$$\begin{cases} N' \equiv b_1 & \pmod{2a_1} \\ N' \equiv N & \pmod{2a_2a_3} \\ (N')^2 \equiv \Delta & \pmod{4a_1a_2a_3} \end{cases}$$

From this follows that

$$\begin{cases} B' \equiv b_1 & \pmod{2a_1} \\ B' \equiv b_2 & \pmod{a_2} \\ B' \equiv b_3 & \pmod{a_3} \end{cases}$$

and

$$\begin{cases} N' \equiv b_1 & \pmod{2a_1} \\ N' \equiv b_2 & \pmod{a_2} \\ N' \equiv b_3 & \pmod{a_3} \end{cases}$$

For the Chinese Remainder Theorem we have $B' \equiv N' \pmod{2a_1a_2a_3}$ since $gcd(2a_1, a_2, a_3) = 1$ (this explains why we constructed $f(x,y)$, $g(x,y)$ and $h(x,y)$ in that way). Hence $f(x,y) \circ (g(x,y) \circ h(x,y))$ is properly equivalent to $(f(x,y) \circ g(x,y)) \circ h(x,y)$ for the properties of the Dirichlet composition of forms. □

We end this section mentioning the composition of forms defined in the book “A course in computational algebraic number theory” of Henry Cohen [15, Definition 5.4.6]. It is more general than the Dirichlet composition and in order to compose it is not necessary to solve a quadratic congruence as in Lemma 1.15.

1.7 Factoring

When the prime factorization of the integer m is known, using the composition of binary quadratic forms it is possible to solve equation (1.1) solving a finite number of Diophantine equations of the type

$$ax^2 + bxy + cy^2 = p \tag{1.15}$$

with p prime integer (see [37]). This allows us to consider only the Diophantine equations of the same type of (1.15).

Even if it is not possible to assert that solving $ax^2 + bxy + cy^2 = m$ always implies the factorization of m, there are some special cases in which this is true.
Let $(1, b, c)$ be a quadratic form of discriminant $\Delta = b^2 - 4c < -4$ and let m be an odd integer. Assume that two representations of m by $(1, b, c)$ are known, i.e. $m = x_1^2 + bx_1y_1 + cy_1^2 = x_2^2 + bx_2y_2 + cy_2^2$, with the condition $|y_1| \neq |y_2|$. Setting $u_1 = x_1 + \frac{b}{2}y_1$ and $u_2 = x_2 + \frac{b}{2}y_2$, the two expressions for m can be rewritten as

$$\begin{aligned} m &= (x_1 + \tfrac{b}{2}y_1)^2 + \tfrac{4c-b^2}{4}y_1^2 = u_1^2 + \tfrac{4c-b^2}{4}y_1^2 \\ m &= (x_2 + \tfrac{b}{2}y_2)^2 + \tfrac{4c-b^2}{4}y_2^2 = u_2^2 + \tfrac{4c-b^2}{4}y_2^2 \end{aligned}$$

Subtracting the second equation multiplied by y_1^2 from the first multiplied by y_2^2, we obtain

$$m(y_2^2 - y_1^2) = u_1^2y_2^2 - u_2^2y_1^2 = (u_1y_2 - u_2y_1)(u_1y_2 + u_2y_1)$$

an expression showing that the last product is zero modulo m if
i) $u_1y_2 - u_2y_1 = 0 \pmod{m}$, or
ii) $u_1y_2 + u_2y_1 = 0 \pmod{m}$, or
iii) some factors of m divide $(u_1y_2 - u_2y_1)$ and the remaining factors divide $(u_1y_2 + u_2y_1)$.
The first two hypotheses are excluded because of the Cauchy-Schwarz inequality, that applied to the vectors $(u_1, \pm y_1)$ and (y_2, u_2) implies

$$(u_1y_2 \pm y_1u_2)^2 \leq (u_1^2 + y_1^2)(u_2^2 + y_2^2) \quad \Rightarrow \quad |u_1y_2 \pm y_1u_2| \leq \sqrt{(u_1^2 + y_1^2)(u_2^2 + y_2^2)}$$

If m divides $u_1y_2 - u_2y_1$, then $m \leq |u_1y_2 - u_2y_1|$, thus

$$m \leq \sqrt{(u_1^2 + y_1^2)(u_2^2 + y_2^2)}$$

however m is trivially larger than $u_1^2 + y_1^2$ and $u_2^2 + y_2^2$ if $\Delta < -4$, therefore m is larger than $\sqrt{(u_1^2 + y_1^2)(u_2^2 + y_2^2)}$. The contradiction proves that m cannot divide $u_1y_2 - u_2y_1$, and similar argument shows that m cannot divide $u_1y_2 + u_2y_1$. In conclusion some non trivial factors of m are in common with $(u_1y_2 - u_2y_1)$ and some with $(u_1y_2 + u_2y_1)$, thus suitable greatest common divisor computations yield two proper factors of m.

1.8 Reduced forms

The goal of this section is to determine a canonical representative for each proper equivaqence class of quadratic forms with discriminant Δ. Following the terminology of [20], we say that a quadratic form $f(x, y) = (a, b, c)$ is **reduced** when

$$\begin{array}{lll} |b| \leq a \leq c \quad \text{and} \quad b \geq 0 \quad \text{if} \quad a = |b| \quad \text{or} \quad a = c & \text{if} \quad \Delta < 0 \\ 0 < b < \sqrt{\Delta} \quad \text{and} \quad \sqrt{\Delta} - b < 2\,|a| < \sqrt{\Delta} + b & \text{if} \quad \Delta > 0 \end{array} \tag{1.16}$$

Example. *Let $Q_0(x, y)$ be the principal form of discriminant Δ:*

$$Q_0(x, y) = \begin{cases} (1, 0, -\Delta/4) & \Delta \equiv 0 \pmod 4 \\ (1, 1, (1-\Delta)/4) & \Delta \equiv 1 \pmod 4 \end{cases}$$

When Δ is negative, Q_0 is reduced in both cases since $\Delta \equiv 0, 1 \pmod 4$ implies $\Delta \leq -3$. Now suppose that $Q_0(x, y)$ is indefinite. When $\Delta \equiv 0 \pmod 4$, the principal form $Q_0(x, y)$ is not reduced (in a reduced indefinite form b must be positive); when $\Delta \equiv 1 \pmod 4$, we have $0 < b < \sqrt{\Delta}$ (Δ is greater then 3 since it is not a perfect square) but $2\,|a| = 2$ is less than or equal to $\sqrt{\Delta} - 1$ for $\Delta \geq 9$.

The number of reduced forms contained in any element of $C(\Delta)$ is finite, both for $\Delta < 0$ and $\Delta > 0$. To prove it we refer to pages 13,21 and 22 of [11]. We start considering positive definite forms.

Lemma 1.21. *If $f(x, y) = (a, b, c)$ is a reduced positive definite quadratic form of discriminant Δ then:*

$$|b| \leq \sqrt{-\frac{\Delta}{3}}$$

Proof. From conditions 1.16 we can observe that:

$$4b^2 \leq 4ac = b^2 - \Delta \quad \Leftrightarrow \quad 3b^2 \leq -\Delta \quad \Leftrightarrow \quad b^2 \leq -\frac{\Delta}{3}$$

and then the lemma follows. □

Proposition 1.22. *If Δ is a negative integer such that $\Delta \equiv 0, 1 \pmod 4$, then there exist only a finite number of reduced positive definite forms of discriminant Δ.*

Proof. Let $f(x, y)$ be a reduced positive definite form of discriminant Δ. By Lemma 1.21, b belongs to a finite set. Furthermore, since

$$\frac{b^2 - \Delta}{4} = ac$$

we can consider the prime factorization of $(b^2 - \Delta)/4$:

$$\frac{b^2 - \Delta}{4} = p_1 p_2 \cdots p_r$$

The set $\{p_1, \dots, p_r\}$ admits a partition in two non-empty subsets such that the product of the elements of one is equal to a and the product of the elements of the other is c. Since the power set of $\{p_1, \dots, p_r\}$ is finite, both a and c lie in a finite set. □

As for the cases of negative discriminant, we need a preliminary lemma also when we consider indefinite forms.

Lemma 1.23. *If $f(x, y) = (a, b, c)$ be is an indefinite reduced binary form of discriminant Δ, then $ac < 0$ and*

$$\sqrt{\Delta} - b < 2\,|c| < \sqrt{\Delta} + b$$

Proof. Since $b < \sqrt{\Delta}$, we have that $b^2 - \Delta = 4ac < 0$ so that a and c are of opposite signs. This means $-4ac = (2\,|a|)(2\,|c|)$ and then

$$(\sqrt{\Delta} - b)(\sqrt{\Delta} + b) = (2\,|a|)(2\,|c|)$$

Since $\sqrt{\Delta} - b < 2\,|a| < \sqrt{\Delta} + b$, if we suppose $2\,|c| \geq \sqrt{\Delta} + b$ we would have $-4ac > \Delta - b^2$ and, simmetrically, $2\,|c| \leq \sqrt{\Delta} - b$ would imply $-4ac < \Delta - b^2$ contradicting $\Delta - b^2 = 4ac$. □

Proposition 1.24. *The number of indefinite reduced forms of discriminant $\Delta > 0$ is finite.*

Proof. Let $f(x, y) = (a, b, c)$ a reduced form of positive discriminant Δ. For the definition of reduced form, b lies in a finite set. The same is true for a and, in the light of Lemma 1.23, for c too. □

Every proper equivalence class of $C(\Delta)$ contains at least a reduced form. This important result was firstly proved by Gauss in his "Disquisitiones Arithmeticae" ([26]) considering initially the case $\Delta < 0$ (art. 171) and then the case $\Delta > 0$ (art. 183). Both the proofs are constructive and with the same structure: successive transformations of a starting form $f(x, y)$ create a sequence of forms, properly equivalent to $f(x, y)$, that ends with a reduced form. From these proofs an algorithm is deduced that takes a form $f(x, y)$ in input and returns a reduced form properly equivalent to $f(x, y)$. This algorithm is called *Gauss reduction algorithm.* To describe theme we will refer to [10, §5 and §6] since the terminology used by the authors allows them to estimate the number of steps necessary to finish the algorithm.

Theorem 1.25. *Every positive definite quadratic form $f(x, y) = (a, b, c)$ is properly equivalent to a reduced form.*

Proof. Given a quadratic form $f(x, y) = (a, b, c)$, if we substitute x by $x + s(f)y$, with $s(f) \in \mathbb{Z}$, we obtain the form $(a, 2as(f) + b, f(s(f), 1))$ which is properly equivalent to $f(x, y)$ since the matrix

$$\begin{pmatrix} 1 & s(f) \\ 0 & 1 \end{pmatrix}$$

has determinant equal to 1. We want to find $s(f) \in \mathbb{Z}$ such that

$$|2as(f) + b| \leq |2as' + b| \tag{1.17}$$

for every other integer s'. If we define $\left[\frac{-b}{2a}\right]$ as the unique integer such that

$$-\frac{1}{2} \leq -\frac{b}{2a} - \left[\frac{-b}{2a}\right] < \frac{1}{2}$$

and we set $s(f) = \left[\frac{-b}{2a}\right]$, we have:

$$-a \leq -b - 2as(f) < a \quad \Leftrightarrow \quad -a < b + 2as(f) \leq a$$

Since s is the nearest integer to $-b/2a$, given any $s' \in \mathbb{Z}$ we obtain

$$\left|\frac{-b}{2a} - s(f)\right| \leq \left|\frac{-b}{2a} - s'\right| \quad \Leftrightarrow \quad \left|\frac{b + 2as(f)}{2a}\right| \leq \left|\frac{b + 2as'}{2a}\right| \quad \Leftrightarrow \quad |b + 2as(f)| \leq |b + 2as'|$$

so $s(f) = \left[\frac{-b}{2a}\right]$ satisfies condition 1.17. Furthermore, from $4af(x, y) = (2ax + by)^2 - \Delta y^2$ it follows $f(s(f), 1) = \frac{(2as(f)+b)^2-\Delta}{4a}$ and

$$\frac{(2as(f) + b)^2 - \Delta}{4a} = f(s(f), 1) \leq f(s', 1) = \frac{(2as' + b)^2 - \Delta}{4a}$$

for every integer s'. The form $f(x + s(f)y, y)$ is called the **normalization** of $f(x, y)$ (**normalize** $f(x, y)$ means replace $f(x, y)$ by its normalization).

To prove the theorem, we transform $f(x, y)$ in forms properly equivalent to it until we find a reduced form. The first step of this procedure consists in replacing $f(x, y)$ by its normalization $f_0(x, y) = (a_0, b_0, c_0)$. After this, we iteratively apply what is called the **reduction step**: we substitute $f_0(x, y)$ with the normalization $f_1(x, y) = (a_1, b_1, c_1)$ of the form $(c_0, -b_0, a_0) = f_0(-y, x)$. We repeat this step until we find a reduced form. This will be properly equivalent to $f(x, y)$ for the transitivity of the equivalence relation.
The described procedure ends in a finite number of iterations. Suppose that it is not true and denote by $f_i(x, y) = (a_i, b_i, c_i)$ the form obtained after the ith reduction step. In this case, the sequence $(a_i)_{i \geq 0}$ is strictly decreasing. In fact, given a natural number i, the form $f_i(x, y) = (a_i, b_i, c_i)$ is such that

$$-a_i < b_i \leq a_i$$

and so a_i must be greater than c_i. If a_i would be less than or equal to c_i, $f_i(x, y)$ would be reduced or such that $a_i = c_i$ and $b_i < 0$, so $f_{i+1}(x, y)$ would be reduced ($f_{i+1}(x, y)$ is the normalization of $f_i'(x, y) = (a_i, -b_i, c_i)$ because $s(f_i')$ is zero). Since $a_{i+1} = c_i$, it follows $a_{i+1} < a_i$.
All the elements of the infinite sequence $(a_i)_{i \geq 0}$ are less than or equal to a (since $a_0 = a$) and properly represented by $f(x, y)$ (a_i is properly represented by $f_i(x, y)$ which is properly

equivalent to $f(x,y)$ for every $i \in \mathbb{N}$). This is a contradiction since there are only finitely many integers which are less than a and which are represented by $f(x,y)$. In fact, if $f(x_0,y_0) \leq \ell$, with $\ell, x_0, y_0 \in \mathbb{Z}$, from equations 1.3 and 1.4 we obtain:

$$f(x_0,y_0) = \frac{(2ax_0+by_0)^2}{4a} - \frac{\Delta}{4a}y_0^2 \quad , \quad f(x_0,y_0) = \frac{(2cx_0+by_0)^2}{4c} - \frac{\Delta}{4c}x_0^2$$

Hence, $f(x_0,y_0) \leq \ell$ implies $x_0^2 \leq -(4c\ell/\Delta)$ and $y_0^2 \leq -(4a\ell/\Delta)$. □

The proof for the case $\Delta < 0$ is analogous, but a bit more complicated, with respect to the proof seen above for positive definite forms. Before proving that every indefinite form is properly equivalent to a reduced form, we give the definition of indefinite normal form and of normalization of an indefinite form.

Definition 1.26. *An indefinite binary quadratic form $f(x,y) = (a,b,c)$ of discriminant Δ is said normal if:*

$$-|a| < b \leq |a| \quad \text{if} \quad |a| \geq \sqrt{\Delta} \tag{1.18}$$

$$\sqrt{\Delta} - 2|a| < b < \sqrt{\Delta} \quad \text{if} \quad |a| < \sqrt{\Delta} \tag{1.19}$$

Given an indefinite form $f(x,y) = (a,b,c)$ of discriminant Δ, if we define $\left\lfloor (\sqrt{\Delta}-b)/2|a| \right\rfloor$ as the unique integer such that

$$0 \leq (\sqrt{\Delta}-b)/2|a| - \left\lfloor (\sqrt{\Delta}-b)/2|a| \right\rfloor < 1 \tag{1.20}$$

and we set

$$s(f) = \begin{cases} sign(a)\left[\frac{-b}{2|a|}\right] & |a| \geq \sqrt{\Delta} \\ \\ sign(a)\left\lfloor \frac{\sqrt{\Delta}-b}{2|a|} \right\rfloor & |a| < \sqrt{\Delta} \end{cases}$$

the form $f(x+s(f)y, y) = (a, b+2as(f), f(s(f),1))$ is properly equivalent to $f(x,y)$ and normal.
In fact, if $|a| \geq \sqrt{\Delta}$, from the relation

$$-\frac{1}{2} \leq -\frac{b}{2|a|} - \left[\frac{-b}{2|a|}\right] < \frac{1}{2}$$

we obtain

$$-|a| \leq -b - 2|a|\left[\frac{-b}{2|a|}\right] < |a| \quad \Leftrightarrow \quad -|a| < b + 2as(f) \leq |a| \tag{1.21}$$

On the other hand, if $|a| < \sqrt{\Delta}$ from 1.20 (with the first inequality proper since Δ is a perfect square if $(\sqrt{\Delta}-b)/2|a| \in \mathbb{Z}$) we can deduce:

$$-\sqrt{\Delta} < -b - 2|a|\left\lfloor \frac{\sqrt{\Delta}-b}{2|a|} \right\rfloor < 2|a| - \sqrt{\Delta} \quad \Leftrightarrow \quad \sqrt{\Delta} - 2|a| < b + 2as(f) < \sqrt{\Delta} \tag{1.22}$$

The form $f(x+s(f)y,y)$ is called the **normalization** of the indefinite form $f(x,y)$ (**normalize** $f(x,y)$ means substitute $f(x,y)$ by its normalization).

Lemma 1.27. *Let $f(x,y)=(a,b,c)$ be and indefinite form of discriminant Δ. If $f(x,y)$ is normal and $|a|\le\sqrt{\Delta}/2$, then $f(x,y)$ is reduced.*

Proof. The hypothesis $|a|\le\sqrt{\Delta}/2$ implies $|a|<\sqrt{\Delta}$ because Δ is non-zero. Then $f(x,y)$ normal means

$$\left|\sqrt{\Delta}-2|a|\right|=\sqrt{\Delta}-2|a|<b<\sqrt{\Delta}$$

So $0<b<\sqrt{\Delta}$ and

$$\left|\sqrt{\Delta}-2|a|\right|<b \quad\Leftrightarrow\quad -b<2|a|-\sqrt{\Delta}<b \quad\Leftrightarrow\quad \sqrt{\Delta}-b<2|a|<\sqrt{\Delta}+b$$

hence $f(x,y)$ is reduced. □

Theorem 1.28. *Every indefinite form $f(x,y)=(a,b,c)$ is properly equivalent to a reduced form.*

Proof. Let Δ be the discriminant of $f(x,y)$. To prove the theorem, we transform $f(x,y)$ in forms properly equivalent to it until we find a reduced form. The first step of this procedure consists in replacing $f(x,y)$ by its normalization $f_0(x,y)=(a_0,b_0,c_0)$. After this, we iteratively apply the **reduction step** for indefinite forms: we substitute $f_0(x,y)$ with the normalization $f_1(x,y)=(a_1,b_1,c_1)$ of the form $(c_0,-b_0,a_0)=f_0(-y,x)$. We repeat this step until we find a reduced form. This will be properly equivalent to $f(x,y)$ for the transitivity of the equivalence relation.
To prove that the described procedure ends in a finite number of iterations we claim that, given the quadratic form $f_i(x,y)=(a_i,b_i,c_i)$ obtained after the ith reduction step, we have:

1. $|c_i|\le|a_i|/4$ if $|a_i|\ge\sqrt{\Delta}$;
2. $f_{i+1}(x,y)$ is reduced if $|a_i|<\sqrt{\Delta}$.

For the first point, since $f(x,y)$ is normal and $|a_i|\ge\sqrt{\Delta}$, we have $a_i^2\ge\Delta$ and $a_i^2\ge b_i^2$. So:

$$|c_i|=\begin{cases}\frac{\Delta-b_i^2}{4|a_i|} & \Delta\ge b_i^2\\[2ex] \frac{b_i^2-\Delta}{4|a_i|} & \Delta<b_i^2\end{cases}$$

and in both cases we obtain $|c_i|\le a_i^2/4|a_i|=|a_i|/4$.
For the second point, $|c_i|\le\sqrt{\Delta}/2$, by Lemma 1.27 $f_{i+1}(x,y)$ is reduced. Hence consider $|c_i|>\sqrt{\Delta}/2$. Being $f(x,y)$ normal, we have:

$$-\sqrt{\Delta}<\sqrt{\Delta}-2|a_i|<b_i<\sqrt{\Delta} \tag{1.23}$$

from which we deduce $|b_i| < \sqrt{\Delta}$ and

$$0 < \sqrt{\Delta} - b_i < 2\,|a_i| \quad , \qquad \sqrt{\Delta} + b_i > 0 \tag{1.24}$$

This means that $(\sqrt{\Delta} - b_i)(\sqrt{\Delta} + b_i) = -4a_ic_i$ is positive and then

$$\frac{\sqrt{\Delta} + b_i}{2\,|c_i|} = \frac{2\,|a_i|}{\sqrt{\Delta} - b_i} > 1 \quad \Rightarrow \quad \sqrt{\Delta} > -b_i + 2\,|c_i| \tag{1.25}$$

Being $|b_i| < \sqrt{\Delta}$, $|c_i|$ can not be greater than or equal to $\sqrt{\Delta}$ otherwise we would have $2\,|c_i| - b_i > \sqrt{\Delta}$. So

$$|c_i| < \sqrt{\Delta} \tag{1.26}$$

On the other hand, $|b_i| < \sqrt{\Delta}$ and $|c_i| > \sqrt{\Delta}/2$ imply

$$-\,b_i + 2\,|c_i| > 2\,|c_i| - \sqrt{\Delta} = \left|\sqrt{\Delta} - 2\,|c_i|\right| \tag{1.27}$$

Now consider the normalization of $f_i'(x,y) = (c_i, -b_i, a_i)$. It has:

$$s(f_i') = sign(c_i)\left\lfloor \frac{\sqrt{\Delta} + b_i}{2\,|c_i|} \right\rfloor = sign(c_i)$$

because $(\sqrt{\Delta} + b_i)/2\,|c_i| > 1$ for equation 1.25 and $\sqrt{\Delta} + b_i < 4\,|c_i|$ for equation 1.27. Hence$f_{i+1}(x,y)$ is $(c_i, -b_i + 2\,|c_i|\,, a_i - sign(c_i)b_i + c_i)$. This form is reduced since $0 < -b_i + 2\,|c_i| < \sqrt{\Delta}$ and $\sqrt{\Delta} + b_i - 2\,|c_i| < 2\,|c_i| < \sqrt{\Delta} - b_i + 2\,|c_i|$.

Now we can conclude: given $f_i(x,y)$ we have that $f_{i+1}(x,y)$ is reduced or $|a_{i+1}| = |c_i|$ is less than or equal to $|a_i|/4$. So, after a finite number of steps, we find $j \in \mathbb{N}$ such that $|a_j| < \sqrt{\Delta}$, that means $f_{j+1}(x,y)$ reduced.

□

When Δ is a positive discriminant, a proper equivalence form of $C(\Delta)$ could contain more than one reduced form. On the other hand, when we Δ is negative, every element of $C(\Delta)$ contains a **unique** reduced form. To prove these results, we provide an example and a Theorem, for which we refer to [48, Theorem 4.2].

Example. *Let $f(x,y) = (-1,5,1)$ and $g(x,y) = (1,5,-1)$ two quadratic forms of discriminant $\Delta = 29$. Both the forms are reduced and $f(-y, x+5y) = g(x,y)$, i.e. $f(x,y)$ and $g(x,y)$ are properly equivalent.*

Theorem 1.29. *If two reduced positive definite forms, $f(x,y) = (a_1,b_1,c_1)$ and $g(x,y) = (a_2,b_2,c_2)$, are properly equivalent, then they are equal.*

Proof. If x_0 and y_0 are two coprime integers, then $f(x_0, y_0) \geq a_1$, i.e. a_1 is the minimum integer represented by $f(x, y)$. In fact we have:

$$f(x_0, y_0) = a_1 x_0^2 + b_1 x_0 y_0 + c_1 y_0^2 \geq a_1 x_0^2 \geq a_1 \quad \text{if } \ 0 < |x_0| \leq |y_0|$$
$$f(x_0, y_0) = a_1 x_0^2 + b_1 x_0 y_0 + c_1 y_0^2 \geq c_1 y_0^2 \geq a_1 \quad \text{if } \ 0 < |y_0| \leq |x_0|$$
$$f(x_0, 0) = a_1 x_0^2 \geq a_1$$
$$f(0, y_0) = c_1 y_0^2 \geq c_1 \geq a_1$$

Since $f(x, y)$ and $g(x, y)$ are properly equivalent, there exist $r, s, t, u \in \mathbb{Z}$ such that $f(rx + sy, tx + uy) = g(x, y)$ and $ru - st = 1$. Properly equivalent forms represents properly the same integers, then $a_1 = a_2$.

Now we want to show that $f(x_0, y_0) = a_1$, with x_0 and y_0 coprime integers, implies $x_0 = \pm 1$ and $y_0 = 0$. From this we will deduce $b_1 = b_2$.

Case 1: $a_1 < c_1$
If $y_0 = 0$, we have $f(x_0, 0) = a_1 x_0^2$ that implies $x_0 = \pm 1$. On the other hand, $f(0, y_0) = c_1 y_0^2 > a_1$. Now assume that x_0 and y_0 are both non-zero. When $0 < |x_0| \leq |y_0|$ we have $f(x_0, y_0) > a_1 x_0^2 \geq a_1$ since $|b_1 x_0 y_0| < c_1 y_0^2$; when $0 < |y_0| \leq |x_0|$ we have $f(x_0, y_0) \geq c_1 y_0^2 \geq c_1 > a_1$ since $|b_1 x_0 y_0| < a_1 x_0^2$. Hence, from $f(r, t) = a_1$, we deduce $r = \pm 1$ and $t = 0$. Since $ru - st = 1$, we have $b_2 = 2a_1 rs + b_1(st + ru) + 2c_1 tu = \pm 2a_1 s + b_1$. Being $f(x, y)$ and $g(x, y)$ reduced, b_2 satisfies the inequality $|b_2| \leq a_2 = a_1$. If $s = 0$, we obtain $b_2 = b_1$; if $s \neq 0$, $|\pm 2a_1 s + b_1|$ is greater than or equal to a_1 and could be equal only when $(\pm 2a_1 s)b_1 < 0$ (if $b_1 = 0$ we must have $s = 0$) and $|s| = 1$, $|b_1| = a_1$. In this case we have $|b_2| = |b_1| = a_1$ and hence $b_2 = b_1$ (for conditions 1.16, b_1 and b_2 must be both positive).

Case 2: $a_1 = c_1$
If x_0 and y_0 are non-zero and with, for example, $|x_0| < |y_0|$, $|x_0 y_0|$ is less than x_0^2 and $f(x_0, y_0) > a_1 y_0^2 \geq a_1$. If x_0 and y_0 are both non-zero, $|x_0|$ could be equal to $|y_0|$ only when $(x_0, y_0) \in \{(1, 1), (-1, 1), (1, -1), (-1, -1)\}$. If $(x_0 = \pm 1, y_0 = \pm 1)$, we have $b_1 = -a_1$ that is impossible since b_1 must be positive when $a_1 = c_1$; if $(x_0, y_0) = (1, -1)$ or $(x_0, y_0) = 1$ we have $b_1 = a_1$ and the only possibilities is $f(x, y) = (1, 1, 1)$. Using Lemma 1.22, it is easy to see that $(1, 1, 1)$ is the only reduced form of discriminant -3 and in this case the theorem is proved. Hence $f(r, t) = a_1$ implies $r = \pm 1$, $t = 0$ or $r = 0$, $t = \pm 1$.
If $r = \pm 1$ and $t = 0$, we have $b_2 = \pm 2a_1 s + b_1$ and we proceed as in the case $a_1 < c_1$; if $r = 0$ and $t = \pm 1$, we have $b_2 = 2a_1 rs + b_1(st + ru) + 2c_1 tu = -b_1 \pm 2a_1 u$ and also in this case what we have see at the end of the case $a_1 < c_1$.

We conclude observing that from $a_1 = a_2$ and $b_1 = b_2$ it follows $c_1 = c_2$:

$$c_1 = \frac{(b_1)^2 - \Delta}{4a_1} = \frac{(b_2)^2 - \Delta}{4a_2} = c_2$$

□

Combining Theorems 1.22 and 1.24 with Theorems 1.25 and 1.28 we can deduce one of the most important result about the integral binary quadratic forms:

Theorem 1.30. *Let $\Delta \in \mathbb{Z}$ be such that it is not a perfect square and $\Delta \equiv 0, 1 \pmod 4$. Then the set $C(\Delta)$ has finite cardinality.*

The finite cardinality of the set $C(\Delta)$ is denoted by h_Δ and is called the **class number of the discriminant** Δ.

In the light of the results presented in this section, in order to solve equation (1) the following two problems will be principally of concern

Problem 1: Let $Q_i(x, y)$, $i = 0, \dots, h_\Delta - 1$, be a set of h_Δ reduced quadratic forms of discriminant Δ, one representative for each proper equivalence class. Given a prime p such that $(\Delta/p) = 1$, decide which are the forms representing it.

Problem 2: Knowing that a quadratic form $Q(x, y)$ represents p, find a representation.

In the following, we will refer to these problems as **representation problems** for the discriminant Δ and the prime integer p.

1.9 Solving $ax^2 + bxy + cy^2 = p$ with Gauss reduction algorithm

In this section we want to show how Gauss reduction algorithm allows to solve a quadratic Diophantine equation $ax^2 + bxy + cy^2 = p$, with $a, b, c, p \in \mathbb{Z}$ and p prime (equation 1.1 with $m = p$). Our goal is to provide an algorithm, written in MAGMA language, that takes a, b, c, p and returns a solution of equation 1.1.
We start assuming that:

- the discriminant $\Delta = b^2 - 4ac$ of the integral binary quadratic form $f(x, y) = (a, b, c)$ is not a perfect square;
- p is an odd prime that does not divide Δ.

In the light of Proposition 1.8, a necessary condition for Equation 1.1 to be solvable is that Δ is a quadratic residue modulo p. If $(\Delta/p) = 1$ then, by Proposition 1.11, there exist only two elements $[Q(x, y)]$, $[Q'(x, y)]$ of $C(\Delta)$ such that the forms contained in them represent p. Then, equation 1.1 has a solution if and only if $f(x, y)$ lies in one of these two proper equivalence classes. Since the proof of Proposition 1.7 is constructive, we are able to determine $Q(x, y)$ and $Q'(x, y)$. We provide here the function of MAGMA, named “Lagrange”, that from Δ (for easy notation, it will be denoted by D) and p outputs $Q(x, y) = (q_1, q_2, q_3)$.

```
function Lagrange (p, D)
Zp:=Integers(p);               /* ring of integers modulo p */
D1:=Zp!D;                      /* consider D in Zp */
l,q2:=IsSquare(D1);            /* function IsSquare returns true if D1 is a
                                  quadratic residue modulo p, false otherwise.
                                  If D1 is a quadratic residue,
                                  a root is also returned (we put it in q2) */
Z:=Integers();                 /* ring of integers */
q2:=Z!q2;                      /* q2 is regarded as an integer */
if (((D-q2) mod 2) eq 1) then  /* a control of the parity of D-q2 */
   q2:=-q2+p;
end if;
q3:=-((D-q2^2)/(4*p));         /* for \textsc{magma}, q3 is a rational number */
q3:=Z!q3;                       /* q3 is regarded as an integer */
return p,q2,q3;
end function;
```

For the computational complexity of the above function, the issue is to find a square root modulo p working with polynomial complexity in p. The equation $x^2 \equiv \Delta \pmod{p}$ is easily solved when $p \equiv 3 \pmod{4}$, while, when $p \equiv 1 \pmod{4}$ and $p \not\equiv 1 \pmod{16}$, it is solvable in polynomial complexity using Schoof algorithm for counting the number of points on elliptic curves over finite fields [50, Proposition 4.2]. Otherwise, the complexity is $O((|x|^{1/2+\epsilon} \log p)^9)$ which may not be polynomial.

Once we have obtained $Q(x,y)$ we can compute also $Q'(x,y)$ since $Q'(x,y) = (q_1, -q_2, q_3)$. To establish if $f(x,y)$ lies in one of the two proper equivalence classes $[Q(x,y)]$, $[Q'(x,y)]$ of $C(\Delta)$, the strategy is to find a representative reduced form for each of the classes $[f(x,y)]$, $[Q(x,y]$, $[Q'(x,y)]$ by the Gauss reduction algorithm. This algorithm is the procedure to obtain a reduced form properly equivalent to a given quadratic form provided by Gauss to prove Theorem 1.25 and Theorem 1.28. An implementation of Gauss reduction algorithm is here provided in MAGMA language. We observe that the function "Gauss", together with the coefficients of a reduced form $g(x,y)$ properly equivalent to the input form $f(x,y)$, returns $r,s,t,u \in \mathbb{Z}$ such that $f(rx+sy, tx+uy) = g(x,y)$.

```
function Equivalence  (a, b, c)  /* Input: coefficients of a form (a,b,c)
                                    Output: coefficients of the properly
                                    equivalent form (c,-b,a) */
return c,-b,a;
end function;

function Normalization (a,b,c)   /* Input: coefficients of a positive
                                    definite form f(x,y)=(a,b,c);
                                    Output: coefficients of the normalization
                                    of (a,b,c) and the integer sf used for the
                                    transformation */

   D:=b^2-4*a*c;                 /* D is the discriminant of the form (a,b,c) */
   if (D lt 0) then
      sf:=(-b)/(2*a);            /* sf is the unique integer such that -b/2a - s is
                                    greater than or equal to -0.5 and less than 0.5.
                                    \textsc{magma} does not supply a function to
    compute
                                                         such sf so we construct it */
      if ( (sf lt 0) and (Truncate(sf)-sf eq 0.5)) then
         sf:=Truncate(sf);                              /* Truncate(sf) returns the
                                                                integral part of sf */
      else
         sf:=Round(sf);             /* Round(sf) returns the integer nearest
                                       to sf. In the case of a tie, it returns
                                       i+1 if sf=i+0.5 and i-1 if sf=i-0.5 */
      end if;
   else
      if (Abs(a) lt Sqrt(D)) then   /* Abs(a) returns the absolute
                                       value of a;  Sqrt(D) is the
                                       square root of D.
                                       When (a,b,c) is indefinite, the
                                       integer used to transform the
                                       form in its normalization as two
                                       expressions  */
         sf:=Sign(a)*Floor((Sqrt(D)-b)/(2*Abs(a)));
                                    /* Sign(a) returns $1$ if a is positive, -1 if a
                                       is negative; Floor(q) is the largest integer
                                       less than or equal to the rational number q */
      else
         sf:=(-b)/(2*Abs(a));
         if ( (sf lt 0) and (Truncate(sf)-sf eq 0.5)) then
            sf:=Truncate(sf);
         else
            sf:=Round(sf);
         end if;
         sf:=Sign(a)*sf;
      end if;
   end if;
   w:=b;                            /* the value of b is saved in w */
   b:=2*a*sf+b;                     /* the normalization of (a,b,c) is the
                                       form (a,b+2*a*sf,a*sf^2+b*sf+c) */
   c:=a*sf^2+w*sf+c;
return a,b,c,sf;
end function;

function Gauss (a,b,c)              /* Input: coefficients of the form f(x,y)=(a,b,c)
                                       Output: coefficients of a reduced form properly
                                       equivalent to (a,b,c) and the integers
                                       r,s,t,u of the transformation that send (a,b,c)
                                       in the reduced form */
   r:=1;  s:=0; t:=1; u:=1;  /* the 2x2 matrix that describes the transformations of
                               (a,b,c) is initially set as the identity matrix */
   D:=b^2-4*a*c;             /* D is the discriminant of (a,b,c) */
   if (D lt 0) then          /* Case D<0 */
      a,b,c,sf:=Normalization(a,b,c);  /* zero step */
      s:=r*sf+s; u:=t*sf+u;  /*the transformation matrix is multiplied by (1,sf;0,1)*/
      while ((a gt c) or (a eq c and b lt 0)) do /* we repeat the reduction
                                                    step until we find a reduced
                                                    form: if (a,b,c) is a normal
                                                    form it is not  reduced if and
                                                    only if a>c or a=c and b<0 */
         a,b,c:=Equivalence(a,b,c);
         a,b,c,sf:=Normalization(a,b,c);
         w:=r; z:=t;                          /* r is saved in w and t is saved in z*/
         r:=s; ; t:=u; s:=s*sf-w; u:=u*sf-z;  /* the transformation matrix is
                                                 multiplied by (0,-1;1,sf) */
      end while;
   else                                       /* Case D>0 */
      a,b,c,sf:=Normalization(a,b,c);         /* zero step */
      s:=r*sf+s; u:=t*sf+u;  /*the transformation matrix is multiplied by (1,sf;0,1)*/
      while ((b in [1..Floor(D)] eq false) or
             (2*Abs(a) in [Ceiling(Sqrt(D)-b)..Floor(Sqrt(D)+b)] eq false)) do
             /* The condition to be an indefinite reduced form is different from
               the condition to be a positive definite reduced form */
         a,b,c:=Equivalence(a,b,c);
         a,b,c,sf:=Normalization(a,b,c);
         w:=r; z:=t;                          /* r is saved in w and t is saved in z*/
         r:=s; ; t:=u; s:=s*sf-w; u:=u*sf-z;  /* the transformation matrix is
                                                 multiplied by (0,-1;1,sf) */
      end while;
   end if;
return a,b,c,r,s,t,u;
end function;
```

The number of reduction steps performed by function "Gauss" is at most $\left\lfloor log_2(a/\sqrt{|\Delta|})\right\rfloor + 2$ when applied to a positive definite form $f(x,y) = (a,b,c)$ (see [10, Theorem 5.5.4]) and is at most $\frac{1}{2}\left\lfloor log_2(a/\sqrt{\Delta})\right\rfloor + 2$ when applied to a form $f(x,y) = (a,b,c)$ with positive discriminant [10, Theorem 6.5.3].

We can now propose an algorithm to solve equation 1.1 when $\Delta = b^2 - 4ac$ is not a perfect square and $(\Delta/p) = 1$. The idea is to reduce (a,b,c), $Q(x,y)$ and $Q'(x,y) = Q(x,-y)$ obtaining the forms (a_1,b_1,c_1), (a_2,b_2,c_2), (a_3,b_3,c_3) respectively. When $\Delta < 0$, if (a_1,b_1,c_1) is different from (a_2,b_2,c_2) and (a_3,b_3,c_3), the equation 1.1 has no solution. If, for example, (a_1,b_1,c_1) is equal to (a_2,b_2,c_2), then by function "Gauss" we know the integers r_1,s_1,t_1,u_1 and r_2,s_2,t_2,u_2 such that:

$$a(r_1x + s_1y)^2 + b(r_1x + s_1y)(t_1x + u_1y) + c(t_1x + u_1y)^2 = (a_1,b_1,c_1) \tag{1.28}$$

$$Q(r_2x + s_2y, t_2x + u_2y) = (a_2,b_2,c_2) \tag{1.29}$$

Therefore, from:

$$\begin{pmatrix} r & s \\ t & u \end{pmatrix} = \begin{pmatrix} r_1 & s_1 \\ t_1 & u_1 \end{pmatrix} \begin{pmatrix} u_2 & -s_2 \\ -t_2 & r_2 \end{pmatrix}$$

we can deduce $a(rx+sy)^2 + b(rx+sy)(tx+uy) + c(tx+uy)^2 = Q(x,y)$ and so

$$ar^2 + brt + ct^2 = Q(1,0) = p$$

If $\Delta > 0$, each proper equivalence class contains the same even number P_c, usually greater than 2, of reduced forms [26], [57, p.111]. P_c is a number strictly connected with the period of the continuous fraction development of $\sqrt{\Delta}$, period that, in some singular cases, depends on the form of Δ [52]; for example, the minimum value 2 of P_c occurs when $\Delta = \ell^2 + 1$, i.e. when the period of the continuous fraction for $\sqrt{\Delta}$ is 1, and the value 4 of P_c occurs when $\Delta = \ell^2 - 1$. The maximum value of P_c may be of order $O(\Delta^{1/2} \log \Delta)$ [31, p.329,p.337].
So, when $f(x, y)$ is indefinite, it could happen that (a, b, c) lies in one of the two proper equivalence classes $[Q(x, y)]$, $[Q'(x, y)]$ even if (a_1, b_1, c_1) is different from (a_2, b_2, c_2) and (a_3, b_3, c_3). So we need to find all the reduced forms contained in $[Q(x, y)]$ and $[Q'(x, y)]$. To obtain the reduced forms of $[Q(x, y)]$, in the light of [10, Corollary 6.8.11], we start *normalizing* (a_2, b_2, c_2). Then we *normalize* the new form and so on until we find again (a_2, b_2, c_2). To each of the reduced forms obtained in this way, we apply the same procedure seen for the case $\Delta < 0$.

```
function Diophantine (a,b,c,p)           /* Input: coefficients of the equation 1.1
                                            Output: a solution, if it exists, of
                                            the equation 1.1 */
   D:=b^2-4*a*c;
   q1,q2,q3:=Lagrange(p, D);
   if (D lt 0) then
      a1,b1,c1,r1,s1,t1,u1:=Gauss(a,b,c);
      a2,b2,c2,r2,s2,t2,u2:=Gauss(q1,q2,q3);
      a3,b3,c3,r3,s3,t3,u3:=Gauss(q1,-q2,q3);
      if ((a1 eq a2) and (b1 eq b2) and (c1 eq c2)) then
         r:=r1*u2-s1*t2;   s:= -r1*s2+s1*r2;
         t:=t1*u2-u1*t2;   u:=-s2*t1+u1*r2;
         x:=r;   y:=t;
         printf "%o=%o(%o)^2+%o(%o)(%o)+%o(%o)^2",p,a,x,b,x,y,c,y;
      elif ((a1 eq a3) and (b1 eq b3) and (c1 eq c3)) then
         r:=r1*u3-s1*t3;   s:= -r1*s3+s1*r3;   t:=t1*u3-u1*t3;   u:=-s3*t1+u1*r3;
         x:=r;
         y:=t;
         printf "%o=%o(%o)^2+%o(%o)(%o)+%o(%o)^2",p,a,x,b,x,y,c,y;
      else
         printf "No solutions";
      end if;
   else
      x:=0; y:=0;
      a1,b1,c1,r1,s1,t1,u1:=Gauss(a,b,c);
      a2,b2,c2,r2,s2,t2,u2:=Gauss(q1,q2,q3);
      a3,b3,c3,r3,s3,t3,u3:=Gauss(q1,q2,q3);
      while ((a3 ne a2) and (b3 ne b2) and (c3 ne c2)) do
         if ((a1 eq a3) and (b1 eq b3) and (c1 eq c3)) then
            r:=r1*u3-s1*t3;   s:= -r1*s3+s1*r3;   t:=t1*u3-u1*t3;   u:=-s3*t1+u1*r3;
            x:=r;
            y:=t;
            printf "%o=%o(%o)^2+%o(%o)(%o)+%o(%o)^2",p,a,x,b,x,y,c,y;
            break;
         end if;
         a3,b3,c3:=Equivalence(a3,b3,c3);
         a3,b3,c3,sf:=Normalization(a3,b3,c3);
         w:=r3; z:=t3;                     /* r is saved in w and t is saved in z*/
         r3:=s3; ; t3:=u3; s3:=s3*sf-w; u3:=u3*sf-z;  /* the transformation matrix is
                                                          multiplied by (0,-1;1,sf) */
      end while;
      a2,b2,c2,r2,s2,t2,u2:=Gauss(q1,-q2,q3);
      a3,b3,c3,r3,s3,t3,u3:=Gauss(q1,-q2,q3);
      while ((a3 ne a2) and (b3 ne b2) and (c3 ne c2)) do
         if ((a1 eq a3) and (b1 eq b3) and (c1 eq c3)) then
            r:=r1*u3-s1*t3;   s:= -r1*s3+s1*r3;   t:=t1*u3-u1*t3;   u:=-s3*t1+u1*r3;
            x:=r;
            y:=t;
            printf "%o=%o(%o)^2+%o(%o)(%o)+%o(%o)^2",p,a,x,b,x,y,c,y;
            break;
         end if;
         a3,b3,c3:=Equivalence(a3,b3,c3);
         a3,b3,c3,sf:=Normalization(a3,b3,c3);
         w:=r3; z:=t3;                     /* r is saved in w and t is saved in z*/
         r3:=s3; ; t3:=u3; s3:=s3*sf-w; u3:=u3*sf-z;  /* the transformation matrix is
                                                          multiplied by (0,-1;1,sf) */
      end while;
      if ((x eq 0) and (y eq 0)) then
         printf "No solutions";
      end if;
end if;
return x,y;
end function;
```

Chapter 2

Ideals and quadratic forms

In Section 8 of the previous chapter, we have introduced the form class group of the binary quadratic forms with a fixed discriminant. The aim of this chapter is to create a bridge between the quadratic forms and the ideals of a quadratic field, i.e. a two dimensional field extension of $\mathbb{Q}$. Such a field contains a subring, known as the ring of integers, which turns out to be a Dedekind ring. This property allows to give to the fractional ideals of the field a group structure, the narrow ideal class group, isomorphic to the form class group of the quadratic forms having the discriminant of the field. The matters recalled in the following are classic and they can be founded in several books of algebraic number theory. For the sake of easy reference, we report and prove all the intermediate results that bring to the isomorphism. We refer to [39], [33], [45], [20] for more detailed discussions.

2.1 Dedekind rings

Let R be an integral domain with $\mathbb{K}$ as field of fractions. Recalling that R could be seen as a subring of $\mathbb{K}$, an element $\alpha \in \mathbb{K}$ is said **integral over** R if it is a root of some monic polynomial $f(x) \in R[x]$. The set of all elements of $\mathbb{K}$ that are integral over R is called the **integral closure of** R **in** $\mathbb{K}$. When $\alpha \in \mathbb{K}$ integral over R implies $\alpha \in R$ we say that R is **integrally closed** [39, Chap. 1].

Definition 2.1. *A Dedekind ring R is an integral domain such that [45, Def. 1.23]:*

1. *it is Noetherian, i.e. does not exist an infinite ascending chain $I_1 \subsetneq \cdots \subsetneq I_s \subsetneq \dots$ of ideals of R;*

2. *every non-zero prime ideal is maximal;*

3. *it is integrally closed.*

Throughout this section, R will denote a Dedekind ring with field of fractions $\mathbb{K}$.

It is useful to see an equivalent definition ([39, pag. 4]) of integral element over R.

Lemma 2.2. *An element α of the field of fractions $\in \mathbb{K}$ of an integral domain R is integral over R if and only if there exists a non-zero finitely generated R-submodule M of $\mathbb{K}$ such that $xM \subset M$.*

Proof. It is evident that $\mathbb{K}$ is an R-module (the scalar multiplication is simply the product in $\mathbb{K}$). If $\alpha \in \mathbb{K}$ is integral over R, then $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$ for some elements $a_1, \ldots, a_{n-1}$ of R. Hence the R-module M generated by $1, \alpha, \ldots, \alpha^{n-1}$ is such that $\alpha M \subset M$ (since $\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_0$).
Vice versa, let $M = \langle \alpha_1, \ldots, \alpha_n \rangle$ be a finitely generated R-submodule of $\mathbb{K}$ such that $\alpha M \subset M$ for $\alpha \in \mathbb{K}$. Then:

$$\alpha\alpha_1 = a_{11}\alpha_1 + \cdots + a_{1n}\alpha_n, \qquad \ldots \qquad, \alpha\alpha_n = a_{n1}\alpha_1 + \cdots + a_{nn}\alpha_n \tag{2.1}$$

with the a_{ij}'s elements of R. The matrix:

$$\begin{pmatrix} \alpha - a_{11} & \ldots & -a_{1n} \\ & \ldots & \\ -a_{n1} & \ldots & \alpha - a_{nn} \end{pmatrix}$$

is singular since the endomorphism of $\mathbb{K}^n$ that it defines is not injective (the non-zero vector $(\alpha_1, \ldots, \alpha_n)$ is mapped into the zero vector). Its determinant could be seen as a monic polynomial of $R[x]$ evaluated in α (it is monic since the biggest power of α is obtained multiplying the elements of the diagonal). This proves that α is integral over R. □

In a Dedekind ring every non-zero ideal could be uniquely written as a product of prime ideals of the ring. We need some preliminary results before proving it. From now to the end of the section we follow [39].

Lemma 2.3. *Let B be a Noetherian ring. Then every ideal of B is finitely generated and contains a product of prime ideals of B.*

Proof. Let I be an ideal of B. If $I = \{0\}$ it is obviously finitely generated. Suppose that I is non-zero and not finitely generated. Given one of its non-zero elements a_1, there exists $a_2 \in I \setminus \langle a_1 \rangle$. Proceeding in this way we create an ascendent infinite chain of ideals:

$$\langle a_1 \rangle \subsetneq \langle a_1, a_2 \rangle \subsetneq \cdots \subsetneq \langle a_1, \ldots, a_\ell \rangle \ldots \tag{2.2}$$

This is a contradiction because B is Noetherian.
Now suppose that I does not contain a product of prime ideals of B. We can assume that I is maximal with respect to this property. Obviously, I is not prime and hence there exist two elements $b_1, b_2 \in B \setminus I$ such that b_1b_2 belongs to I. We define:

$$J_1 = Bb_1 + I, \qquad J_2 = Bb_2 + I \tag{2.3}$$

Since B is a ring with unit, J_1 and J_2 strictly contain I. Hence, both J_1 and J_2 contain a product of prime ideals of B. But J_1J_2 is contained in I, so I contain a product of prime ideals. This is a contradiction that proves the lemma. □

Given a Dedekind ring R with field of fractions $\mathbb{K}$, we are interested in the non-zero finitely generated R-submodules of $\mathbb{K}$: they are called **fractional ideals of** R. If a fractional ideal $\mathfrak{M}$ of R is contained in R then it is an ideal of R; vice versa, if I is an ideal of R it is a finitely generated R-submodule of $\mathbb{K}$ since R is Noetherian.
Let $\mathfrak{M}$ and $\mathfrak{N}$ be two fractionals ideals of R. We define $\mathfrak{M}\mathfrak{N}$ as the set:

$$\mathfrak{M}\mathfrak{N} = \{\sum_{i=1}^{\ell} m_i n_i \mid \ell \in \mathbb{N}, m_i \in \mathfrak{M}, n_i \in \mathfrak{N}\} \tag{2.4}$$

The next elementary properties of fractional ideals will be useful in the following.

Lemma 2.4. *Given three fractional ideals $\mathfrak{M}$, $\mathfrak{N}$ and $\mathfrak{F}$ of a Dedekind ring R with field of fractions $\mathbb{K}$ we have that:*

1. *$\mathfrak{M}\mathfrak{N}$ is a fractional ideal of R;*

2. *$\mathfrak{M}\mathfrak{N} = \mathfrak{N}\mathfrak{M}$;*

3. *$(\mathfrak{M}\mathfrak{N})\mathfrak{F} = \mathfrak{M}(\mathfrak{N}\mathfrak{F})$.*

Proof. From (2.4) points 2 and 3 follow easily.
For the first point, observe that $\mathfrak{M}\mathfrak{N}$ is an additive group, closed under multiplication by elements of R. Therefore it is an R-submodule of $\mathbb{K}$. If $\alpha_1, \dots, \alpha_\ell$ and $\beta_1, \dots, \beta_s$ are the generators of $\mathfrak{M}$ and $\mathfrak{N}$ respectively, then $\mathfrak{M}\mathfrak{N}$ is generated by $\alpha_i\beta_j$ with $i \in \{1, \dots, \ell\}$ and $j \in \{1, \dots, s\}$.
□

Lemma 2.5. *If $\mathfrak{M}$ is a fractional ideal of a Dedekind ring R with field of fractions $\mathbb{K}$, then the set*

$$\mathfrak{M}^{-1} = \{\alpha \in \mathbb{K} \mid \alpha\mathfrak{M} \subset R\}$$

is a fractional ideal of R.

Proof. As before, we observe that $\mathfrak{M}^{-1}$ contains 0, it is closed under addition, contains the opposite of any of its elements, is closed under multiplication by elements of R. Therefore $\mathfrak{M}^{-1}$ is an R-submodule of $\mathbb{K}$. Suppose that η is a non-zero element of $\mathfrak{M}$. Then $\mathfrak{M}^{-1}\eta$ is an ideal of R , hence it is finitely generated since R is Noetherian. Now it is clear that $\mathfrak{M}^{-1}$ is finitely generated (by the generators of $\mathfrak{M}^{-1}\eta$ multiplied by η^{-1}). □

Given a non zero element γ of the field of fractions $\mathbb{K}$ of a Dedekind ring R, we have that $R\gamma$ is a fractional ideal of R. We call **principal** this kind of fractional ideals of R. Observe that, for $\alpha \in \mathbb{K}$, we have $\alpha R\gamma \subset R$ if and only if $\alpha\gamma \in R$ (R is a ring with unit). Therefore

$$(R\gamma)^{-1} = R\gamma^{-1} \tag{2.5}$$

and

$$(R\gamma)^{-1}R\gamma = R\gamma^{-1}R\gamma = R \tag{2.6}$$

Definition 2.6. *A fractional ideal $\mathfrak{M}$ of a Dedekind ring R is invertible if $\mathfrak{M}\mathfrak{M}^{-1} \subset R$, with $\mathfrak{M}^{-1}$ defined as in Lemma 2.5.*

As we have seen, all the principal fractional ideals of a Dedekind ring R are invertible.

Proposition 2.7. *A non-zero ideal I of a Dedekind ring R with field of fractions $\mathbb{K}$ is an invertible fractional ideal of R.*

Proof. We start assuming that I is a maximal ideal of R. Obviously I^{-1} contains R: we want to prove that such inclusion is proper.
Given a non-zero element $a \in I$, using Lemma 2.3 we can choose a minimal s such that there exist s prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ of R with $\mathfrak{p}_1 \cdots \mathfrak{p}_s$ contained in Ra. We can assume that $\mathfrak{p}_1$ is contained in I (if we suppose that all the prime ideals $\mathfrak{p}_1, \cdots, \mathfrak{p}_s$ contain an element that do not belong to I then their product could not belong to I because it is a prime ideal). Since $\mathfrak{p}_1$ is maximal by the hypothesis on R, then $I = \mathfrak{p}_1$. For the minimality of s, $\mathfrak{p}_2 \cdots \mathfrak{p}_s$ is not contained in Ra and hence there exists $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_s$ such that $b \notin Ra$. But $b\mathfrak{p}_1 = bI \subset Ra$ and $a^{-1}bI \subset R$. Therefore $a^{-1}b$ is an element of I^{-1} that do not belong to R. This proves that R is properly contained in I^{-1}.
Since $1 \in I^{-1}$, then $I \subset I(I^{-1}) \subset R$. Now observe that $I(I^{-1})$ is an ideal of R (it is a fractional ideal contained in R). Since $1 \in I^{-1}$, it contains I. For the maximality of I it follows that $I(I^{-1}) = I$ or $I(I^{-1}) = R$. The first possibility implies that the elements of I^{-1} send I in I. Since I is a finitely generated R-module, the elements of I^{-1} would be integral over R (Lemma 2.2). This is impossible because I^{-1} is bigger than R and R is integrally closed. So $I(I^{-1}) = R$.
Now let I be a generic non-zero ideal of R. Suppose that the proposition is false. Since R is Noetherian, we can suppose that I is a maximal ideal with respect to this property. For the first part of the proof, I could not be a maximal ideal. Hence $I \subset \mathfrak{p}$ for some maximal ideal $\mathfrak{p}$ ([40, pag. 93]).
We have:

$$I \subset I\mathfrak{p}^{-1} \subset I(I^{-1}) \subset R$$

Since I is a finitely generated R-module we could not have $I\mathfrak{p}^{-1} \subset I$ because R is integrally closed and $\mathfrak{p}^{-1}$ contains properly R (see the previous case). But $I\mathfrak{p}^{-1}$ is an ideal in R (it is a fractional ideal contained in R since $\mathfrak{p}^{-1} \subset I^{-1}$). Therefore, for the maximality of I, $I\mathfrak{p}^{-1}$ is invertible with $(I\mathfrak{p}^{-1})^{-1} = J^{-1}$. This is a contradiction: $I\mathfrak{p}^{-1}J^{-1} = R$ implies I invertible with $I^{-1} = \mathfrak{p}^{-1}J^{-1}$ (if $\alpha I \subset R$, with $\alpha \in \mathbb{K}$, then $\alpha I\mathfrak{p}^{-1}J^{-1} \subset \mathfrak{p}^{-1}J^{-1}$, $xR \subset \mathfrak{p}^{-1}I^{-1}$). □

Now, we are ready to prove the mentioned result about the ideals of a Dedekind ring.

Theorem 2.8. *Every non-zero ideal I of a Dedekind ring R with field of fractions $\mathbb{K}$ could be uniquely factored as a product of prime ideals of R.*

Proof. Suppose that there exists a non-zero ideal I of R that could not be written as a product of prime ideals of R. Since R is a Noetherian, we can assume that I is maximal with respect to this property. Obviously, I is not prime and then is properly contained in some prime ideal $\mathfrak{p}$ of R (see [40, pag. 93]). So $I\mathfrak{p}^{-1}$ is contained in R and contains I (since

$\mathfrak{p}^{-1}$ contains the unit). From the proof of Proposition 2.7, we know that $\mathfrak{p}^{-1}$ properly contains R and then $\mathfrak{p}^{-1}I$ could not be contained in I, otherwise the elements of $\mathfrak{p}^{-1}$ would be integral over R, contradicting the hypothesis that R is integrally closed. Hence:

$$I \subsetneq \mathfrak{p}^{-1}I \tag{2.7}$$

and, for the maximality of I, we can write

$$\mathfrak{p}^{-1}I = \mathfrak{p}_1 \cdots \mathfrak{p}_s \tag{2.8}$$

with $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ prime ideals of R. Therefore, from Proposition 2.7, it follows:

$$I = \mathfrak{p}\mathfrak{p}_1 \cdots \mathfrak{p}_s \tag{2.9}$$

that is a contradiction. This ends the proof of the existence of a prime factorization. Now, for the uniqueness of the factorization of a non-zero ideal I of R, suppose that:

$$I = \mathfrak{q}_1 \cdots \mathfrak{q}_n = \mathfrak{q}'_1 \cdots \mathfrak{q}'_\ell \tag{2.10}$$

with $\mathfrak{q}_1, \ldots, \mathfrak{q}_n, \mathfrak{q}'_1, \ldots, \mathfrak{q}'_\ell$ prime ideals of R. Observe that $\mathfrak{q}_1 \cdots \mathfrak{q}_n \subset \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$. Therefore, $\mathfrak{q}'_1 \cdots \mathfrak{q}'_\ell$ is contained in $\mathfrak{q}_1$ and then one of the $\mathfrak{q}'_j$ is contained in $\mathfrak{q}_1$. From the maximality of $\mathfrak{q}'_j$ it follows $\mathfrak{q}'_j = \mathfrak{q}_1$. Less then renumbering, we can assume $j = 1$. Proceeding in this fashion, we obtain the equality of the two factorization. In fact, we can not arrive to $\mathfrak{q}_h \cdots \mathfrak{q}_n = R$, since this means R contained in a prime ideal. □

A similar theorem holds also for the fractional ideals of a Dedekind ring.

Theorem 2.9. *Let $\mathfrak{M}$ be a fractional ideal of a Dedekind ring R with field of fractions $\mathbb{K}$. It can be uniquely factored as the product of integral powers of prime ideals of R, i.e.*

$$\mathfrak{M} = \mathfrak{p}_1^{\ell_1} \cdots \mathfrak{p}_n^{\ell_n}$$

where $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are prime ideals of R and $\ell_1, \ldots, \ell_n$ are, not necessarily positive, integers.

Proof. Let $\alpha_1, \ldots, \alpha_r$ be the generators of $\mathfrak{M}$. Since they are elements of $\mathbb{K}$, we have:

$$\alpha_i = a_i/b_i$$

where a_i and b_i belong to R, with b_i non-zero. If we put $b = (b_1 \cdots b_r) \in R$ we obtain that

$$\alpha_i b = (a_i/b_i)(b_1 \cdots b_r) \in R$$

for every $i \in \{1, \ldots, r\}$. Hence, $\mathfrak{M}b \subset R$ is an ideal of R. By Theorem 2.8, we have:

$$Rb = \prod \mathfrak{q}_j^{\ell_j}, \qquad \mathfrak{M}b = \prod \mathfrak{p}_h^{\ell'_h}$$

whit $\mathfrak{q}_j$ and $\mathfrak{p}_h$ prime ideals of R and ℓ_j, ℓ'_h positive integers. We can observe that:

$$\prod \mathfrak{p}_h^{\ell'_h} = \mathfrak{M}b = (\mathfrak{M}R)b = \mathfrak{M}Rb = \mathfrak{M} \prod \mathfrak{q}_j^{\ell_j}$$

By Proposition 2.7, we can deduce:

$$\mathfrak{M} = \prod \mathfrak{p}_h^{\ell'_h} \prod \mathfrak{q}_j^{-\ell_j}$$

This ends the proof of the existence of the factorization. It remains the uniqueness. Assume that:

$$\mathfrak{M} = \prod \mathfrak{p}_h^{\ell_h} \prod \mathfrak{q}_j^{-\ell'_j} = \prod \mathfrak{r}_v^{s_v} \prod \mathfrak{s}_u^{-s'_u}$$

with $\mathfrak{p}_h, \mathfrak{q}_j, \mathfrak{r}_v, \mathfrak{s}_u$ prime ideals of R and $\ell_h, \ell'_j, s_v, s'_u$ positive integers. We can assume that all the $\mathfrak{p}_h$'s and $\mathfrak{q}_j$'s are distinct; the same could be done for all the $\mathfrak{r}_v$'s and $\mathfrak{s}_u$'s. Since the multiplication of a fractional ideal of R by R does not change the fractional ideal, we deduce:

$$\prod \mathfrak{p}_h^{\ell_h} \prod \mathfrak{s}_u^{s'_u} = \prod \mathfrak{q}_j^{\ell'_j} \prod \mathfrak{r}_v^{s_v}$$

Both the terms of the relation are ideals of R. Hence, from Proposition 2.8 and the hypothesis that all the $\mathfrak{p}_h$'s and $\mathfrak{q}_j$'s are distinct and all the $\mathfrak{r}_v$'s and $\mathfrak{s}_u$'s are distinct, the result follows. □

Denote by $I(R)$ the set of all the fractional ideals of a Dedekind ring R. We have already defined a product in $I(R)$ which is commutative and associative (Proposition 2.4). Furthermore:

- $I(R)$ has R as identity: it belongs to $I(R)$ and $R\mathfrak{M} = \mathfrak{M}$ for every fractional ideal $\mathfrak{M}$ of R.
- every fractional ideal $\mathfrak{M}$ of R has an inverse. By Theorem 2.8 we have

  $$\mathfrak{M} = \mathfrak{p}_1^{\ell_1} \cdots \mathfrak{p}_n^{\ell_n}$$

  where $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are prime ideals of R and $\ell_1, \ldots, \ell_n$ are integers, hence

  $$\mathfrak{M}\mathfrak{p}_1^{-\ell_1} \cdots \mathfrak{p}_n^{-\ell_n} = R$$

  by Proposition 2.7
- every element of $I(R)$ could be written uniquely as a product of integral powers of prime ideals of R.

It follows that $I(R)$ is a free abelian group respect to the defined product: it will be called **ideal group of** R. An important subgroup of $I(R)$ is the subset composed by the principal fractional ideals, that is denoted by $P(R)$. It is easy to observe that: the identity R is contained in $P(R)$; the inverse of a principal fractional ideal $R\gamma$, with γ in the field of fractions $\mathbb{K}$ of R, is the principal fractional ideal $R\gamma^{-1}$; the product of two principal fractional ideals $R\gamma_1$, $R\gamma_2$ is $R\gamma_1\gamma_2$. The quotient group

$$C(R) = I(R)/P(R) \tag{2.11}$$

is called the **ideal class group of** R.

When R is a principal ideal domain, we have $I(R) = P(R)$ and hence $C(R) = \{1\}$. So $C(R)$ may be taken as a measure of how far R is from being a principal ideal domain.

2.2 Finite field extensions

In the rest of our work, the finite field extensions will assume an important role. In particular, we will concern with finite field extensions of the field $\mathbb{Q}$. For this reason we dedicate this section to briefly recall some results that will be used in next sections. For more details we refer to [9].

In the whole section $\mathbb{K}$ denotes a finite field extension, of degree n, of the field $\mathbb{F}$ with $\{\omega_1, \ldots, \omega_n\}$ as a basis.

Given $\alpha \in \mathbb{K}$, the map

$$\begin{array}{rccc} \varphi_\alpha : & \mathbb{K} & \rightarrow & \mathbb{K} \\ & \xi & \mapsto & \alpha\xi \end{array}$$

is a linear map because

1. $\alpha(a\xi) = a(\alpha\xi)$ for every $\xi \in \mathbb{K}$, $a \in \mathbb{F}$;

2. $\alpha(\xi_1 + \xi_2) = \alpha\xi_1 + \alpha\xi_2$ for every $\xi_1, \xi_2 \in \mathbb{K}$.

For $i \in \{1, \ldots, n\}$ we have $\alpha\omega_i = \sum_{j=1}^n a_{ij}\omega_j$ and the matrix associated to φ_α with respect to the fixed basis is $A = (a_{ij})$. If we change the basis, we obtain a matrix similar to A, so with the same determinant and trace. The determinant $det(A)$ is called the **norm of** α and is denoted by $N_{\mathbb{K}/\mathbb{F}}(\alpha)$ and the trace of A is called the **trace of** α and denoted by $Sp_{\mathbb{K}/\mathbb{F}}(\alpha)$.
The **characteristic polynomial of** α **over** $\mathbb{F}$ is the characteristic polynomial of φ_α, i.e. $det(A - xId)$, and it does not depend on the basis that we have fixed. Such polynomial has leading coefficient equal to 1 or -1 and has α as root (because $(A - \alpha Id)(\omega_1, \ldots, \omega_n)^t$ is equal to the zero-vector and then the matrix is singular).
If β is another element of $\mathbb{K}$, $\varphi_{\alpha\beta} = \varphi_\alpha \circ \varphi_\beta$. If the matrices associated to φ_α and φ_β with respect to $\{\omega_1, \ldots, \omega_n\}$ are A and B respectively, then AB is the matrix associated to $\varphi_{\alpha\beta}$ with respect the same fixed basis. From the properties of the determinant it follows that $N_{\mathbb{K}/\mathbb{F}}(\alpha\beta) = N_{\mathbb{K}/\mathbb{F}}(\alpha)N_{\mathbb{K}/\mathbb{F}}(\beta)$.

We say that $\mathbb{K}$ is a separable over $\mathbb{F}$ if the linear map

$$\begin{array}{rccc} Sp_{\mathbb{K}/\mathbb{F}} : & \mathbb{K} & \rightarrow & \mathbb{F} \\ & \alpha & \mapsto & Sp_{\mathbb{K}/\mathbb{F}}(\alpha) \end{array}$$

is not identically zero. Since $\varphi_1 = Id(\mathbb{K})$, then $Sp(1)_{\mathbb{K}/\mathbb{F}} = n$.
So, if $\mathbb{F}$ has characteristic 0 or n is not a multiple of $char(\mathbb{F})$, then $\mathbb{K}$ is always separable over $\mathbb{F}$.
Now consider the square matrix, of order n and with entries in $\mathbb{F}$, defined as

$$S = (s_{ij}) = (Sp_{\mathbb{K}/\mathbb{F}}(\omega_i\omega_j))$$

Its determinant is called **discriminant of the basis** $\{\omega_1, \ldots, \omega_n\}$ and is denoted by $D(\omega_1, \ldots, \omega_n)$. We want to show that, if $\mathbb{K}$ is separable over $\mathbb{F}$, then S is not singular. Suppose that $det(S) = 0$. Therefore there exist $c_1, \ldots, c_n \in \mathbb{F}$, not all zero, such that:

$$\sum_{j=1}^{n} c_j Sp_{\mathbb{K}/\mathbb{F}}(\omega_i \omega_j) = 0 \qquad \forall i \in \{1, \ldots, n\}$$

since the columns of the matrix are linearly dependent over $\mathbb{F}$.
If we put $\gamma = c_1\omega_1 + \cdots + c_n\omega_n$, last relation is equivalent to the following:

$$Sp_{\mathbb{K}/\mathbb{F}}(\omega_i \gamma) = 0 \qquad \forall i \in \{1, \ldots, n\}$$

since $Sp_{\mathbb{K}/\mathbb{F}}$ is a linear map. In the light of the linear independence of $\omega_1, \ldots, \omega_n$ over $\mathbb{F}$, we can observe that also $\gamma\omega_1, \ldots, \gamma\omega_n$ are linearly independent over $\mathbb{F}$ becuase γ is non-zero. Hence, given a generic element ξ of $\mathbb{K}$, then $\xi = a_1\gamma\omega_1 + \cdots + \gamma a_n\omega_n$ with $a_1 \ldots, a_n$ elements of $\mathbb{F}$. Therefore from the linearity of $Sp_{\mathbb{K}/\mathbb{F}}$ it follows $Sp_{\mathbb{K}/\mathbb{F}}(\xi) = 0$. This contradicts the separability of $\mathbb{K}$.

If we suppose $\mathbb{K}$ separable over $\mathbb{F}$, given $b_1, \ldots, b_n \in \mathbb{F}$ there exists a unique element $\alpha \in \mathbb{K}$ such that $Sp_{\mathbb{K}/\mathbb{F}}(\omega_i \alpha) = b_i$ for $i \in \{1, \ldots, n\}$ (if we put $\alpha = x_1\omega_1 + \cdots + x_n\omega_n$ and we impose $Sp_{\mathbb{K}/\mathbb{F}}(\omega_i\alpha) = b_i$ for $i \in \{1, \ldots, n\}$ we obtain a linear system with matrix S. But S is not singular and hence, the system has a unique solution in $\mathbb{F}$). In particular we can find n elements $\omega_1^*, \ldots, \omega_n^* \in \mathbb{K}$ such that $Sp_{\mathbb{K}/\mathbb{F}}(\omega_i\omega_j^*) = \delta_{ij}$. These elements are linearly independent over $\mathbb{F}$ since, from $e_1\omega_1^* + \cdots + e_n\omega_n^* = 0$ ($e_i \in \mathbb{F}$), multiplyng by ω_i and applying $Sp_{\mathbb{K}/\mathbb{F}}$, it follows $e_i = 0$ for every $i \in \{1, \ldots, n\}$. Therefore $\{\omega_1^*, \ldots, \omega_n^*\}$ is a basis for $\mathbb{K}$, called the **dual basis of** $\{\omega_1, \ldots, \omega_n\}$. Finally, if $\alpha = a_1\omega_1 + \cdots + a_n\omega_n$ is an element of $\mathbb{K}$ then

$$a_i = Sp_{\mathbb{K}/\mathbb{F}}(\alpha\omega_i^*) \tag{2.12}$$

2.3 The ring of integers of a number field

For all the section, $\mathbb{K}$ will denote a number field, i.e. a finite field extension of the field of rational numbers:

$$n = [\mathbb{K} : \mathbb{Q}]$$

The field $\mathbb{K}$ contains a subring, denoted by $\mathcal{O}_{\mathbb{K}}$, such that:

1. its field of fractions is $\mathbb{K}$;

2. it is a Dedekind ring.

The subring $\mathcal{O}_{\mathbb{K}}$ could be introduced in several ways: we take as model what is done in the book *Number theory* by Borevich and Shafarevich [9]. We start with the notion of algebraic integer.

Definition 2.10. *An element α of the number field $\mathbb{K}$ is an algebraic number if it is a root of some polynomial $f \in \mathbb{Z}[x]$; α is an algebraic integer if it is a root of some monic polynomial $f \in \mathbb{Z}[x]$.*

The set $\mathcal{O}_{\mathbb{K}}$ composed by all the algebraic integers of the number field $\mathbb{K}$ is called the **ring of integers of** $\mathbb{K}$. The rest of this section is devoted to the proof of the properties of $\mathcal{O}_{\mathbb{K}}$. We will do it using orders.

Any number field $\mathbb{K}$ is a $\mathbb{Z}$-module. We denote by M a finitely generated $\mathbb{Z}$-submodule of $\mathbb{K}$. If $\mu_1, \dots, \mu_m$ are its generators, then:

$$M = \{a_1\mu_1 + \cdots + a_m\mu_m \mid a_i, \dots, a_m \in \mathbb{Z}\}$$

For simplicity, we will write $M = [\mu_1, \dots, \mu_m]$. Two $\mathbb{Z}$-submodules of $\mathbb{K}$, M_1 and M_2, are said similar if there exists a non-zero $\alpha \in \mathbb{K}$ such that $M_1 = \alpha M_2$. We can observe that $\alpha M_2 = [\alpha\mu_1, \dots, \alpha\mu_m]$ if $M_2 = [\mu_1, \dots, \mu_m]$.

Definition 2.11. *A finitely generated $\mathbb{Z}$-submodule of a number field $\mathbb{K}$ is said full if it contains a basis of the $\mathbb{Q}$-vector space $\mathbb{K}$; non-full in the other case.*

A system of generators $\mu_1, \dots, \mu_m$ of the finitely generated $\mathbb{Z}$-submodules M of $\mathbb{K}$ is a **basis** for M if $\mu_1, \dots, \mu_m$ are linearly independent over $\mathbb{Z}$. Therefore, every element μ of the M is uniquely written as a linear combination, with integral coefficients, of the elements of the basis.

The structure of a finitely generated $\mathbb{Z}$-module M in a number field $\mathbb{K}$ could be investigated using the abelian groups. Let G be an additive abelian group. It is **finitely generated** if there exist $g_1, \dots, g_m \in G$ such that every element g of G is of the form $c_1g_1 + \cdots + c_mg_m$ where $c_1, \dots, c_m$ are integers. In this case $g_1, \dots, g_m$ will be called a **finite system of generators for** G. A finite system of generators $g_1, \dots, g_m$ of G is a **basis** if $c_1g_1 + \cdots + c_mg_m = 0$ implies $c_1 = \cdots = c_m = 0$ (when it happens $g_1, \dots, g_m$ are said linearly independent over $\mathbb{Z}$). The order of $g \in G$ is the least positive integer ℓ such that $\ell g = 0$. If such integer does not exist, g is said of **infinite order**.

Proposition 2.12. *Let G be an additive abelian group without elements of finite order. If it is finitely generated, then it admits a basis.*

Proof. Let $g_1, \dots, g_m$ be a finite system of generators for G. If we substitute g_i with $g_i + \ell g_j$, where $i \neq j$ and $\ell \in \mathbb{Z}$, we obtain another finite system of generators for G. In fact, given $g \in G$, we have:

$$g = c_1g_1 + \cdots + c_mg_m = c_1g_1 + \cdots + (c_j - \ell c_i)g_j + \cdots + c_i(g_i + \ell g_j) + \cdots + c_mg_m$$

with $c_1, \dots, c_m \in \mathbb{Z}$. Suppose that $g_1, \dots, g_m$ are not linearly independent over $\mathbb{Z}$. Given $b_1g_1 + \cdots + b_mg_m = 0$ with $b_1, \dots, b_m \in \mathbb{Z}$ not all zero, assume that b_1 is the minimum (in

absolute value) of the non-zero b_i's. We would like that all the other b_i's would be divisible by b_1 because g_1 would be a linear combination of $g_2, \dots, g_m$ (we use the fact that G has not elements of finite order). On the other hand, if (for example) b_2 is not divisible by b_1, then $b_2 = qb_1 + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < b_1$. Then we can put $b_2' = b_2 - qb_1 = r$ and substitute g_1 with $g_1 + qg_2$. We obtain a new system of generators to which apply the same process (they remain linearly dependent over $\mathbb{Z}$ because b_1 and b_2' are non-zero). If we do not find the desired situation, iterating the procedure, at each step we decrease the non-zero coefficient with minimum absolute. Then, after a finite number of steps the non-zero coefficient with minimum absolute value becomes zero. But this is impossible since the new non-zero coefficient with minimum absolute value is the rest r of the euclidian division performed above.
So, if $g_1, \dots, g_m$ are not linearly independent over $\mathbb{Z}$ we can decrease the number of generators until we find a basis. It happens every time since at most remains only a generator: it is linearly independent over $\mathbb{Z}$ since it is of infinite order. □

It is easy to observe that a finitely generated $\mathbb{Z}$-submodule M of a number field $\mathbb{K}$ is an abelian additive group, finitely generated and without elements of finite order (a field does not have zero divisors). Its generators are also generators for the abelian group. Hence **every finitely generated $\mathbb{Z}$-submodule M of $\mathbb{K}$ admits a basis**.
The cardinality of a basis of M is equal to the maximal number s of linearly independent (over $\mathbb{Q}$) vectors of $\mathbb{K}$. In fact, since vectors linearly independent over $\mathbb{Z}$ are also linearly independent over $\mathbb{Q}$, we have that the cardinality m of a basis is less or equal to s. These two natural numbers must be equal: suppose that $\nu_1, \dots, \nu_s$ are elements of M linearly independent over $\mathbb{Q}$ and $\mu_1, \dots, \mu_m$ form a basis for M, with $s > m$. Therefore $a_1\nu_1 + \dots + a_s\nu_s = 0$ ($a_i \in \mathbb{Q}$) not necessarily implies $a_1 = \dots = a_r = 0$ (to the relation corresponds a linear system with variables $a_1, \dots, a_s$ and coefficient matrix of order $m \times s$ with entries in $\mathbb{Q}$: every linear application from $\mathbb{Q}^s$ to $\mathbb{Q}^m$ is obviously non-injective. Therefore all the basis of M have the same cardinality that is called **rank of** M and it is denoted by $rank(M)$.
Obviously, $rank(M) = [\mathbb{K} : \mathbb{Q}]$ if and only if M is full. Furthermore, a set of generators of M must have a cardinality greater or equal to $rank(M)$ for the proof of Theorem 2.12.

Theorem 2.13. *Let G be an abelian additive group, finitely generated and without elements of finite order. Then, if N is a non-zero subgroup of M, it has a finite system of generators and hence a basis. Furthermore, for any basis $\{g_1, \dots, g_m\}$ of G there exists a basis of N of the form:*

$$\begin{aligned} \eta_1 &= c_{11}g_1 + \dots + c_{1m}g_m \\ \eta_2 &= c_{22}g_2 + \dots + c_{2m}g_m \\ &\dots \\ \eta_n &= c_{nn}g_n + \dots + c_{nm}g_m \end{aligned} \tag{2.13}$$

where the c_{ij} are integers with $c_{ii} > 0$ and $n \leq m$.

Proof. We will prove the theorem by induction on the cardinality m of a basis of G.
If $m = 1$, the non-zero element g_1 generates G. Let ℓ be the smallest positive integer such that $\ell g_1 \in N$. Given an element $\ell' g_1 \in N$, with ℓ' positive integer, we have $\ell' = q\ell + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < \ell$. Since $\ell' g_1 - q\ell g_1 = (\ell' - q\ell)g_1 = rg_1$ belongs to N, we must have $r = 0$, otherwise the minimality of ℓ will be contradicted. So N is generated by ℓg_1. It is a basis for N since G does not have elements of finite order.
Now suppose $m > 1$. Let β a non-zero element of N. Then $\beta = c_1 g_1 + \cdots + c_m g_m$ where the integers $c_1, \ldots, c_m$ are not all zero. For simplicity, assume $c_1 > 0$ (if necessary we can consider $-\beta$). From the existence of β, it follows that we can consider, among all the elements of N, an element $\eta_1 = c_{11} g_1 + \cdots + c_{1m} g_m$, with $c_{11}, \ldots, c_{1m} \in \mathbb{Z}$ in which the positive coefficient of g_1 is the smallest. Then c_1 is divisible by c_{11}. Indeed, if $c_1 = c'' c_{11} + c'$ with $C', C'' \in \mathbb{Z}$ and $0 \leq c' < c_{11}$, then $\beta - q\eta_1$ belongs to N and has c'' as coefficient of g_1. If $c'' \neq 0$ we contradict the minimality of c_{11}. Therefore $\beta - q\eta_1 = e_2 g_2 + \cdots + e_m g_m$ with $e_2, \ldots, e_g \in \mathbb{Z}$.
Let G_0 be the subgroup of G generated by $g_2, \ldots, g_m$ (they form a basis of the subgroup). Then $G_0 \cap N$ is a non-zer subgroup of G_0 (otherwise η_1 would generate N) and we can use the induction hypothesis on G_0. So $G_0 \cap N$ has a basis of the type:

$$\begin{aligned} \eta_2 &= c_{22} g_2 + \cdots + c_{2m} g_m \\ \eta_3 &= c_{33} g_3 + \cdots + c_{3m} g_m \\ &\cdots \\ \eta_n &= c_{nn} g_n + \cdots + c_{nm} g_m \end{aligned} \tag{2.14}$$

where the c_{ij}'s are integers with $c_{ii} > 0$ and n is less than or equal to m. We claim that N is generated by $\eta_1, \ldots, \eta_n$. Let $\alpha = b_1 g_1 + \cdots + b_m g_m$, with $b_1, \ldots, b_m \in \mathbb{Z}$, an arbitrary element of N. Since c_{11} divides b_1 (even if $b_1 = 0$), we have:

$$\alpha - t\eta_1 \in G_0 \cap N$$

for a suitable $t \in \mathbb{Z}$, and therefore:

$$\alpha - t\eta_1 = t_2\eta_2 + \cdots + t_n\eta_n \quad \Rightarrow \alpha = t\eta_1 + t_2\eta_2 + \cdots + t_n\eta_n$$

for $t, t_2, \ldots, t_n \in \mathbb{Z}$, i.e. $\eta_1, \ldots, \eta_n$ generate N.
From the linear independence of $g_1, \cdots, g_m$ and for the form of $\eta_1, \ldots, \eta_n$ it follows the linear independence of $\eta_1, \cdots, \eta_n$. □

Corollary 2.14. *Let M be a finitely generated $\mathbb{Z}$-submodule of a number field $\mathbb{K}$. Then every additive subgroup N of M is a finitely generated $\mathbb{Z}$-submodule of M and hence of $\mathbb{K}$.*

Proof. M is an abelian additive group without elements of finite order. Therefore, if N is a subgroup of M, it is finitely generated and with a basis for the previous theorem. Then N is a finitely generated $\mathbb{Z}$-submodule of $\mathbb{K}$. □

Definition 2.15. *Let M be a full finitely generated $\mathbb{Z}$-submodule of a number field $\mathbb{K}$. A coefficient of M is an element $\alpha \in \mathbb{K}$ such that $\alpha M \subset M$.*

The set $\mathbb{D}_M$ composed by all the coefficients of M is a subring of $\mathbb{K}$ (it is clearly an additive subgroup, it is closed under multiplication and contains the unit). $\mathbb{D}_M$ is called the **ring of coefficients of** M. Observe that, if $\{\mu_1, \dots, \mu_n\}$ is a basis for M, then $\alpha \in \mathbb{K}$ belongs to $\mathbb{D}_M$ if and only if $\alpha\mu_1, \dots, \alpha\mu_n$ belong to M. One implication is clear; vice versa, for every $\beta \in M$ we have:

$$\alpha\beta = \alpha(b_1\mu_1 + \cdots + b_n\mu_n) = b_1\alpha\mu_1 + \cdots b_n\alpha\mu_n \in M$$

with $b_1, \dots, b_n \in \mathbb{Z}$, because M is an additive group.

Proposition 2.16. *Let M be a full finitely generated $\mathbb{Z}$-submodule of a number field $\mathbb{K}$. Then also $\mathbb{D}_M$ is full finitely generated $\mathbb{Z}$-submodule of $\mathbb{K}$.*

Proof. Let γ be a non-zero element of M. For the definition of $\mathbb{D}_M$ we have $\gamma\mathbb{D}_M \subset M$ with $\gamma\mathbb{D}_M$ additive subgroup of M (since also $\mathbb{D}_M$ is an additive group). For 2.14, $\gamma\mathbb{D}_M$ is a finitely generated $\mathbb{Z}$-submodule of $\mathbb{K}$ and then same holds for $\mathbb{D}_M = \gamma^{-1}\gamma\mathbb{D}_M$.
Let α be a non zero element of $\mathbb{K}$ and $\{\mu_1, \dots, \mu_n\}$ a basis for M and therefore for $\mathbb{K}$. We denote by a the common denominator of the rationals a_{ij}, with $i, j \in \{1, \dots, n\}$, such that:

$$\alpha\mu_i = a_{i1}\mu_1 + \cdots + a_{in}\mu_n$$

It follows that $a\alpha\mu_i \in M$, for every $i \in \{1, \dots, n\}$, and $a\alpha$ belongs to $\mathbb{D}_M$. Furthermore, if $\{\alpha_1, \dots, \alpha_n\}$ is a basis for $\mathbb{K}$, then $a_1\alpha_1, \dots, a_n\alpha_n$ belong to $\mathbb{D}_M$ for some non-zero integers $a_1, \dots, a_n$. Obviously, $a_1\alpha_1, \dots, a_n\alpha_n$ are linearly independent over $\mathbb{Q}$ so $\mathbb{D}_M$ is full. □

Definition 2.17. *A full finitely generated $\mathbb{Z}$-submodule M of a number field $\mathbb{K}$ is an order of $\mathbb{K}$ if it is a ring.*

From the above definition, it follows that the ring of coefficients $\mathbb{D}_M$ of a full finitely generated $\mathbb{Z}$-submodule $M \subset \mathbb{K}$ is an order. Vice versa, if $\mathbb{D}$ is an order of $\mathbb{K}$ then it is the ring of coefficients of itself (because $1 \in \mathbb{D}$ and $\alpha\mathbb{D} \subset \mathbb{D}$ implies $\alpha \in \mathbb{D}$).

Lemma 2.18. *Let M be a finitely generated full $\mathbb{Z}$-submodule of a number field $\mathbb{K}$. If γ is a non-zero element of $\mathbb{K}$, then $\mathbb{D}_M = \mathbb{D}_{\gamma M}$. Furthermore, M is similar to a full $\mathbb{Z}$-submodule of $\mathbb{K}$ contained in $\mathbb{D}_M$.*

Proof. An element $\alpha \in \mathbb{K}$ belongs to $\mathbb{D}_M$ if $\alpha\beta \in M$ for every $\beta \in M$. This is equivalent to the condition $\alpha\gamma\beta \in \gamma M$ for every $\beta \in M$ (we use the fact that γ as an inverse in $\mathbb{K}$ since it is non-zero). Hence $\mathbb{D}_M = \mathbb{D}_{\gamma M}$.
Let $\{\mu_1, \dots, \mu_n\}$ be a basis for M and $\{\eta_1, \dots, \eta_n\}$ be a basis for $\mathbb{D}_M$. For $i \in \{1, \dots, n\}$, we have $\mu_i = \sum_{j=1}^{n} b_{ij}\eta_j$, with $b_{ij} \in \mathbb{Q}$ (observe that $\eta_1, \dots, \eta_n$ form a basis for $\mathbb{K}$). Denote with b the common denominator of the rationals $b_{11}, \dots, b_{nn}$. Then $b\mu_i$ belongs to $\mathbb{D}_M$. So bM is a full finitely generated $\mathbb{Z}$-submodule of $\mathbb{K}$ ($b\mu_1, \dots, b\mu_n$ are linearly independent over $\mathbb{Q}$) and a subset of $\mathbb{D}_M$. □

Lemma 2.19. *Let $\mathbb{D}$ be an order in a number field $\mathbb{K}$. An element $\alpha \in \mathbb{D}$ has characteristic polynomial and minimal polynomial over $\mathbb{Q}$ with integral coefficients. In particular its norm $N_{\mathbb{K}/\mathbb{Q}}(\alpha)$ and its trace $Sp_{\mathbb{K}/\mathbb{Q}}(\alpha)$ are integers.*

Proof. Let $\mathbb{D}$ be the ring of coefficients of the full finitely generated $\mathbb{Z}$-submodule M with basis $\{\mu_1, \dots, \mu_n\}$ (for example, M could be $\mathbb{D}$ itself). If $\alpha \in \mathbb{D}$ then $\alpha\mu_i$, with $i \in \{1, \dots, n\}$, belongs to M and then the matrix $A = (a_{ij})$ associated to φ_α with respect to the basis $\{\mu_1, \dots, \mu_n\}$ of $\mathbb{K}$ has integral entries. It follows that $det(A)$ and $trace(A)$ are also integers. Furthermore, the characteristic polynomial of α over $\mathbb{Q}$ has integral coefficients and then α is an algebraic integer. It remains to prove that α has minimal polynomial over $\mathbb{Q}$ with integral coefficients.
Let $p(x) \in \mathbb{Q}[x]$ be the minimal polynomial of α over $\mathbb{Q}$ and let $g(x) \in \mathbb{Z}[x]$ a monic polynomial having α as root. It follows that:

$$g(x) = p(x) \cdot h(x)$$

with $h(x) \in \mathbb{Q}[x]$. Suppose that $p(x)$ does not belong to $\mathbb{Z}[x]$. So one of its coefficients is a rational number a/b with $a, b \in \mathbb{Z}$ and $gcd(a, b) = 1$ and $\langle b \rangle \neq 1$. Let $p \neq 1$ be a prime integer that divides b and suppose that p^i is the biggest power of p that divides some denominator of the $p(x)$'s coefficients. Similarly, let p^j be the biggest power of p that divides some denominator of the $h(x)$'s coefficients. Then:

$$p^{i+j}g(x) = p^{i+j}h(x)p(x) = (p^j h(x))(p^i p(x))$$

Now consider $p^{i+j}g(x)$ and $(p^j h(x))(p^i p(x))$ in $\mathbb{Z}_p$: the left term has all the coefficients equal to zero modulo p. Let x^s be the biggest monomial of $p(x)$ such that the denominator b_1 of its coefficient a_1/b_1 is divisible by p^i; let x^r be the biggest monomial of $h(x)$ such that the denominator b_2 of its coefficient a_2/b_2 is divisible by p^j. Hence the coefficient of x^{r+s} in $(p^j h(x))(p^i p(x))$ is:

$$p^{i+j}(\frac{a_1}{b_1}\frac{a_2}{b_2} + \frac{a_3}{b_3} + \dots + \frac{a_e}{b_e})$$

with $a_3/b_3, \dots, a_e/b_e \in \mathbb{Q}$. This coefficient is non-zero modulo p since the numerator of $p^{i+j}(a_1a_2/b_1b_2)$ is not divisible by p while $p^{i+j}(a3/b_3 + \dots + a_e/b_e)$ is zero in $\mathbb{Z}_p$. This is a contradiction. □

We denote by $\mathcal{O}_\mathbb{K}$ the set of all the elements of a number field $\mathbb{K}$ such that their minimal polynomial over $\mathbb{Q}$ have integral coefficients. From the last lemma it follows that $\mathcal{O}_\mathbb{K}$ contains every order of $\mathbb{K}$.

Lemma 2.20. *Let $\mathbb{K}$ be a number field. If $\alpha \in \mathcal{O}_\mathbb{K}$ and its minimal polynomial over $\mathbb{Q}$ is*

$$x^m + c_{m-1}x^{m-1} \dots + c_1x + c_0 \in \mathbb{Z}[x]$$

then the finitely generated $\mathbb{Z}$-submodule $M = \{1, \alpha, \dots, \alpha^{m-1}\}$ of $\mathbb{K}$ is a ring.

Proof. For the distributivity of the product in $\mathbb{K}$ it is sufficient to prove that α^ℓ belongs to M for every positive integer ℓ. We proceed by induction on ℓ. For $\ell \leq m-1$ this is clearly true and the same holds if $\ell = m$ (because $\alpha^m = -c_{m-1}\alpha^{m-1} - \dots - c_1\alpha - c_0 \in M$). Finally, if $\ell > m$, for inductive hypothesis we have $\alpha^\ell = \alpha\alpha^{\ell-1} = \alpha(a_0 + a_1\alpha + \dots + a_{m-1}\alpha^{m-1})$ for some $a_0, \dots, a_{m-1} \in \mathbb{Z}$ and hence α^ℓ belongs to M. □

Lemma 2.21. *Let $\mathbb{D}$ be an order in a number field $\mathbb{K}$ and α an element of $\mathcal{O}_{\mathbb{K}}$. Then the ring $\mathbb{D}[\alpha] = \{f(\alpha) \mid f \in \mathbb{D}[x]\}$ is an order in $\mathbb{K}$.*

Proof. It is obvious that $\mathbb{D}[\alpha]$ is a ring in $\mathbb{K}$ (0,1 belong to $\mathbb{K}$; it is closed under addition and multiplication and it contains the opposite of each of its elements). Since $\mathbb{D} \subset \mathbb{D}[\alpha]$, $\mathbb{D}[\alpha]$ contains a basis of $\mathbb{K}$, i.e. n linearly independent elements over the rationals numbers. It remains to show that $\mathbb{D}[\alpha]$ is a finitely generated $\mathbb{Z}$-submodule of $\mathbb{K}$. Let $\{\omega_1, \dots, \omega_n\}$ be a basis for $\mathbb{D}$. If m is the degree of the minimal polynomial of α over $\mathbb{Q}$, for the proof of the Lemma 2.20 we have that $\alpha^\ell = a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1}$, with $a_0, \dots, a_{m-1} \in \mathbb{Z}$, for every positive integer ℓ. We can conclude that $\mathbb{D}[\alpha]$ is a $\mathbb{Z}$-submodule of $\mathbb{K}$ generated by the elements $\omega_1, \omega_1\alpha, \dots, \omega_1\alpha^{m-1}, \dots, \omega_n, \omega_n\alpha, \dots, \omega_n\alpha^{m-1}$. □

Corollary 2.22. *Let $\mathbb{D}$ be an order in a number field $\mathbb{K}$ and $\alpha_1, \dots, \alpha_r$ elements of $\mathcal{O}_{\mathbb{K}}$. Then the ring $\mathbb{D}[\alpha_1, \dots, \alpha_r] = \{f(\alpha_1, \dots, \alpha_r) \mid f \in \mathbb{D}[x_1, \dots, x_r]\}$ is an order in $\mathbb{K}$.*

Proof. It follows from Lemma 2.21 since we can proceed by induction on r using the fact $\mathbb{D}[\alpha_1 \dots, \alpha_{r-1}, \alpha_r] = \mathbb{D}[\alpha_1, \dots, \alpha_{r-1}][\alpha_r]$ □

Theorem 2.23. *Let $\mathbb{K}$ be a number field. The set $\mathcal{O}_{\mathbb{K}}$ of all the elements of $\mathbb{K}$ whose minimal polynomials over $\mathbb{Q}$ have integral coefficients is the maximal order in $\mathbb{K}$, i.e. it contains every order of $\mathbb{K}$ and is not properly contained in an another order of $\mathbb{K}$.*

Proof. Let $\mathbb{D}$ be an order in $\mathbb{K}$ (it exists: we can consider the full $\mathbb{Z}$-submodule of $\mathbb{K}$ generated by a basis of $\mathbb{K}$ and then take its ring of coefficients). Fix two elements α, β of $\mathcal{O}_{\mathbb{K}}$. Since $\mathbb{D}[\alpha, \beta]$ is an order in $\mathbb{K}$ for Corollary 2.22, than it is contained in $\mathcal{O}_{\mathbb{K}}$ (Lemma 2.19). So $\alpha - \beta$ and $\alpha\beta$ belong to $\mathbb{D}[\alpha, \beta]$ and then to $\mathcal{O}_{\mathbb{K}}$. This proves that $\mathcal{O}_{\mathbb{K}}$ is a ring. It contains a basis of $\mathbb{K}$ because the order $\mathbb{D}$, which is contained in $\mathcal{O}_{\mathbb{K}}$ by Lemma 2.19, does. It remains to show that $\mathcal{O}_{\mathbb{K}}$ is a finitely generated $\mathbb{Z}$-submodule of $\mathbb{K}$.
Since $char(\mathbb{Q}) = 0$ and $\mathbb{K}$ is a finite extension of $\mathbb{Q}$, then $\mathbb{K}$ is a separable extension of $\mathbb{Q}$. Given a basis $\{\omega_1, \dots, \omega_n\}$ for $\mathbb{D}$ we can consider the dual basis $\{\omega_1^*, \dots, \omega_n^*\}$. We want to show that the full $\mathbb{Z}$-submodule $\mathbb{D}^*$ of $\mathbb{K}$ generated by $\omega_1^*, \dots, \omega_n^*$ contains $\mathcal{O}_{\mathbb{K}}$.
Let α be any element of the ring $\mathcal{O}_{\mathbb{K}}$. Then $\alpha = c_1\omega_1^* + \cdots + c_n\omega_n^*$ with $c_1, \dots, c_n$ rational numbers. For $i \in \{1, \dots, n\}$ we have $Sp_{\mathbb{K}/\mathbb{Q}}(\omega_i\alpha) = c_i$ and $\omega_i\alpha$ is obviously an element of the order $\mathbb{D}[\alpha]$. But $\mathbb{D}[\alpha]$ is an order and then the trace of $\omega_i\alpha$ is an integer, so $c_1, \dots, c_n$ are integers. Thus $\mathcal{O}_{\mathbb{K}} \subset \mathbb{D}^*$. Since $\mathcal{O}_{\mathbb{K}}$ is an additive group, we have that it is a finitely generated $\mathbb{Z}$-submodule of $\mathbb{K}$ by Lemma 2.14. Its maximality follows from 2.19. □

The maximal order $\mathcal{O}_{\mathbb{K}}$ of a number field $\mathbb{K}$ is the ring of integers of $\mathbb{K}$ defined at the beginning of the section: the algebraic integers of $\mathbb{K}$ are all and only the elements of $\mathbb{K}$ with minimal polynomials over $\mathbb{Q}$ with integral coefficients.

The next step is to show that the ring of integers $\mathcal{O}_{\mathbb{K}}$ of a number field $\mathbb{K}$ has $\mathbb{K}$ as field of fractions (see Lemma 1.4 and Corollary 1.16 of [45]).

Proposition 2.24. *Let $\mathbb{K}$ be a number field. Then its ring of integers $\mathcal{O}_{\mathbb{K}}$ has $\mathbb{K}$ as field of fractions.*

Proof. Since $\mathcal{O}_{\mathbb{K}}$ is a subring of the field $\mathbb{K}$, it is an integral domain. Let $Q(\mathcal{O}_{\mathbb{K}})$ be its field of fractions and consider the map:

$$\begin{array}{rccc} \varphi : & Q(\mathcal{O}_{\mathbb{K}}) & \to & \mathbb{K} \\ & [(\alpha, \beta)] & \mapsto & \alpha\beta^{-1} \end{array}$$

First of all, φ is well defined because if (α, β) and (α', β') are in the same equivalence class of the domain, then $\alpha\beta' = \beta\alpha'$ and:

$$\alpha = \beta\alpha'(\beta')^{-1} \Rightarrow \alpha\beta^{-1} = \varphi([(\alpha, \beta)]) = \alpha'(\beta')^{-1} = \varphi([(\alpha', \beta')])$$

We want to show that φ is a field isomorphism. If $[(\alpha_1, \beta_2)]$, $[(\alpha_2, \beta_2)]$ are two elements of $Q(\mathcal{O}_{\mathbb{K}})$ then we have:

$$\begin{aligned} &\varphi([(\alpha_1, \beta_1)] + [(\alpha_2, \beta_2)]) = \varphi([(\alpha_1\beta_2 + \alpha_2\beta_1, \beta_1\beta_2)]) = (\alpha_1\beta_2 + \alpha_2\beta_1)(\beta_1\beta_2)^{-1} = \\ &\alpha_1\beta_1^{-1} + \alpha_2\beta_2^{-1} = \varphi([(\alpha_1, \beta_1)]) + \varphi([(\alpha_2, \beta_2)]) \end{aligned} \tag{2.15}$$

$$\begin{aligned} &\varphi([(\alpha_1, \beta_1)][(\alpha_2, \beta_2)]) = \varphi([(\alpha_1\alpha_2, \beta_1\beta_2)]) = \alpha_1\alpha_2(\beta_1\beta_2)^{-1} = (\alpha_1\beta_1^{-1})(\alpha_2\beta_2^{-1}) = \\ &\varphi([(\alpha_1, \beta_1)])\varphi([(\alpha_2, \beta_2)]) \end{aligned} \tag{2.16}$$

and $\varphi([(1, 1)]) = 1$. It remains to prove that φ is a bijection. For the injectivity, if $[(\alpha_1, \beta_1)]$ and $[(\alpha_2, \beta_2)]$ have the same image, then:

$$\alpha_1\beta_1^{-1} = \alpha_2\beta_2^{-1} \Rightarrow \alpha_1 = \alpha_2\beta_1\beta_2^{-1} \Rightarrow \alpha_1\beta_2 = \alpha_2\beta_1 \Rightarrow [(\alpha_1, \beta_1)] = [(\alpha_2, \beta_2)]$$

Furthermore, every element γ of $\mathbb{K}$ is a fraction of elements of $\mathcal{O}_{\mathbb{K}}$. In fact, γ is an algebraic over $\mathbb{Q}$ since $\mathbb{K}$ is a finite field extension of $\mathbb{Q}$. Hence, there exists a monic polynomial $f(x) \in \mathbb{Q}[x]$ such that:

$$f(\gamma) = a_0 + a_1\gamma + \cdots + a_{d-1}\gamma^{d-1} + \gamma^d = 0$$

with $a_0, \ldots, a_{d-1}$ rational numbers. Let ℓ be the least common multiple of the denominators of the rational numbers $a_0, \ldots, a_{d-1}$. So:

$$(\ell\gamma)^d + (\ell a_{d-1})(\ell\gamma)^{d-1} + \cdots + (\ell^{d-1}a_1)(\ell\gamma) + \ell^d a_0 = 0$$

It follows that $\alpha = \ell\gamma$ is an algebraic integer and therefore $\gamma = \alpha/\ell$ where $\alpha \in \mathcal{O}_{\mathbb{K}}$ and $\ell \in \mathbb{Z} \subset \mathcal{O}_{\mathbb{K}}$. This concludes the proof. □

Before prove that the ring of integers $\mathcal{O}_{\mathbb{K}}$ of a number field $\mathbb{K}$ is a Dedekind ring we need one more preliminary results that will be used even in the following. For the next two propositions we refer to [20, Exercixe 5.1],

Proposition 2.25. *Let $\mathcal{O}_{\mathbb{K}}$ the ring of integers of a number field $\mathbb{K}$ and I a non-zero ideal of $\mathcal{O}_{\mathbb{K}}$. Then the quotient ring $\mathcal{O}_{\mathbb{K}}/I$ is finite.*

Proof. Every non-zero ideal I of $\mathcal{O}_{\mathbb{K}}$ contains an integer ℓ. In fact, if α is a non-zero element of I then there exists a monic polynomial $p(x) \in \mathbb{Z}[x]$ such that $p(\alpha) = 0$:

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{m-1} + \alpha^m = 0$$

with $a_0, a_1, \cdots, a_{m-1} \in \mathbb{Z}$. Since I is an ideal and $\mathcal{O}_{\mathbb{K}}$ contains $\mathbb{Z}$, then $a_0 = -a_1\alpha - \cdots - a_{n-1}\alpha^{m-1} - \alpha^m$ belongs to I. We consider the ideal of $\mathcal{O}_{\mathbb{K}}$ generated by ℓ: it is contained in I. Therefore we can define the following map:

$$\begin{array}{rccc} \varphi: & \mathcal{O}_{\mathbb{K}}/\langle\ell\rangle & \to & \mathcal{O}_{\mathbb{K}}/I \\ & [\beta]_{\langle\ell\rangle} & \mapsto & [\beta]_I \end{array}$$

that is well defined because if two elements of $\mathcal{O}_{\mathbb{K}}$ are equivalent modulo $\langle\ell\rangle$ then they are equivalent modulo I too. Obviously the map is surjective and hence, if the domain is finite, then $\mathcal{O}_{\mathbb{K}}/I$ must be finite too. Given $\beta \in \mathcal{O}_{\mathbb{K}}$ we have $\gamma = b_1\omega_1 + \cdots + b_n\omega_n$, where $b_1, \ldots, b_n$ are integers and $\{\omega_1, \ldots, \omega_n\}$ is a basis for $\mathcal{O}_{\mathbb{K}}$ as order of $\mathbb{K}$. Then:

$$[\beta]_{\langle\ell\rangle} = [b_1\omega_1 + \cdots + b_n\omega_n]_{\langle\ell\rangle} = [b_1]_{\langle\ell\rangle}[\omega_1]_{\langle\ell\rangle} + \cdots + [b_n]_{\langle\ell\rangle}[\omega_n]_{\langle\ell\rangle}$$

If two integers are congruent modulo ℓ then they are in the same equivalence class modulo $\langle\ell\rangle$ and then

$$\{[b_1]_{\langle\ell\rangle}, \cdots, [b_n]_{\langle\ell\rangle}\} \subseteq \{[0]_{\langle\ell\rangle}, [1]_{\langle\ell\rangle}, \ldots, [\ell-1]_{\langle\ell\rangle}\}$$

So the cardinality of the domain is less than or equal to ℓ^n. □

The finite cardinality of $\mathcal{O}_{\mathbb{K}}/I$, where I is a non-zero ideal of the ring of integers of a number field $\mathbb{K}$ is called **norm of** I and is denote by $N(I)$. Now we are able to show that $\mathcal{O}_{\mathbb{K}}$ is a Dedekind ring.

Proposition 2.26. *Let $\mathcal{O}_{\mathbb{K}}$ be the ring of integers of a number field $\mathbb{K}$. Then:*

1. *$\mathcal{O}_{\mathbb{K}}$ is Noetherian;*
2. *every nonzero prime ideal of $\mathcal{O}_{\mathbb{K}}$ is maximal;*
3. *$\mathcal{O}_{\mathbb{K}}$ is integrally closed (i.e. if $\gamma \in \mathbb{K}$ is a root of a monic polynomial with coefficients in $\mathcal{O}_{\mathbb{K}}$ then γ belongs to $\mathcal{O}_{\mathbb{K}}$).*

Proof. 1) Suppose that there exists an infinite chain $I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_h \subsetneq \cdots$ of ideals of $\mathcal{O}_{\mathbb{K}}$. Given $\alpha \in \mathcal{O}_{\mathbb{K}}$ we have $[\alpha]_{I_h} \subseteq [\alpha]_{I_{h+1}}$ for every natural number h. Hence

$$N(I_h) \geq N(I_{h+1})$$

Since I_h is properly contained in I_{h+1}, then $\mathcal{O}_{\mathbb{K}}$ has at least two elements, one in $I_{h+1} \setminus I_h$ and one in I_h, equivalent modulo I_{h+1} and not equivalent modulo I_h. Therefore

$$N(I_h) \gneq N(I_{h+1})$$

This is a contradiction, because in the sequence

$$N(I_1) \gneqq N(I_2) \gneqq \cdots \gneqq N(I_h) \gneqq \cdots$$

every norm is greater then 0 and then the chain could not be infinite. Hence $\mathcal{O}_{\mathbb{K}}$ is Noetherian.
2)Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_{\mathbb{K}}$. Since $\mathcal{O}_{\mathbb{K}}$ is an integral domain, the quotient ring $\mathcal{O}_{\mathbb{K}}/\mathfrak{p}$ is an integral domain. But every finite integral domain is a field and then $\mathfrak{p}$ is a maximal ideal.
3) Let $\gamma \in \mathbb{K}$ be integral over $\mathcal{O}_{\mathbb{K}}$, i.e. γ is a root of a monic polynomial $f(x) \in \mathcal{O}_{\mathbb{K}}[x]$. All the elements of $\mathcal{O}_{\mathbb{K}}$ are, by definition, integral over $\mathbb{Z}$. We want to show that γ is integral over $\mathbb{Z}$ (we refer to [39, pag. 5]). For hypothesis there exist $\alpha_0, \alpha_1, \ldots, \alpha_{m-1} \in \mathcal{O}_{\mathbb{K}}$ such that

$$\gamma^m + \alpha_{m-1}\gamma^{m-1} + \cdots + \alpha_1\gamma + \alpha_0 = f(\gamma) = 0$$

with m natural number. This implies that $\mathcal{O}_{\mathbb{K}}[\gamma] = \{g(\gamma) \mid g(x) \in \mathcal{O}_{\mathbb{K}}[x]\}$ is an $\mathcal{O}_{\mathbb{K}}$-module finitely generated. In fact, it is an additive subgroup of $\mathbb{K}$ and it is closed under multiplication by elements of $\mathcal{O}_{\mathbb{K}}$. Furthermore, from $\gamma^m = -\alpha_{m-1}\gamma^{m-1} - \cdots - \alpha_1\gamma - \alpha_0$, we can proceed by induction over the power of γ to show that every positive power of γ is a linear combination, with coefficients in $\mathcal{O}_{\mathbb{K}}$, of $1, \gamma, \ldots, \gamma^{m-1}$. Hence $\mathcal{O}_{\mathbb{K}}[\gamma]$ is generated by $1, \gamma, \ldots, \gamma^{m-1}$.
Following the same ideas, we have that $\mathbb{Z}[\alpha_0, \ldots, \alpha_{m-1}] = \{g(\alpha_0, \ldots, \alpha_{m-1}) \mid g(y_0, \ldots, y_{m-1}) \in \mathbb{Z}[y_0, \ldots, y_{m-1}]\}$ is a $\mathbb{Z}$-module and a subring of $\mathbb{K}$. Since $\alpha_0, \ldots, \alpha_{m-1}$ are integral over $\mathbb{Z}$, every power of α_j is a linear combination (with integral coefficients) of a finite number of powers of α_j. This means that $\mathbb{Z}[\alpha_0, \ldots, \alpha_{m-1}]$ is finitely generated. Obviously, γ is integral over $\mathbb{Z}[\alpha_0, \ldots, \alpha_{m-1}]$ and then $\mathbb{Z}[\alpha_0, \ldots, \alpha_{m-1}][\gamma]$ is a finitely generated $\mathbb{Z}[\alpha_0, \ldots, \alpha_{m-1}]$-module (use what we have said for γ integral over $\mathcal{O}_{\mathbb{K}}$). From $\mathbb{Z}[\alpha_0, \ldots, \alpha_{m-1}][\gamma] = \mathbb{Z}[\alpha_0, \ldots, \alpha_{m-1}, \gamma]$ it follows that $\mathbb{Z}[\alpha_0, \ldots, \alpha_{m-1}, \gamma]$ is finitely generated.
To end the proof, we show that all the elements of $\mathbb{Z}[\alpha_0, \ldots, \alpha_{m-1}, \gamma]$ are integral over $\mathbb{Z}$. Suppose that $\mu_1, \ldots, \mu_l$ generate $\mathbb{Z}[\alpha_0, \ldots, \alpha_{m-1}, \gamma]$ and let ϵ be an element of the module. Since $\mathbb{Z}[\alpha_0, \ldots, \alpha_{m-1}, \gamma]$ is a ring, $\epsilon\mu_1, \ldots, \epsilon\mu_l$ belongs to it and so we have:

$$\epsilon\mu_i = \sum_{j=1}^{l} c_{ij}\mu_j \Leftrightarrow \sum_{j=1}^{l}(\epsilon\delta_{ij} - c_{ij})\mu_j = 0 \qquad j \in \{1, \ldots, l\}$$

with $c_{ij} \in \mathbb{Z}$. The square matrix $(\epsilon\delta_{ij} - c_{ij})$ is singular (since sends $(\mu_1, \ldots, \mu_l)^t$ in the zero vector). In particular its determinant could be seen as a product of polynomials of $\mathbb{Z}[x]$ evaluated in ϵ. We obtain a monic polynomial (since the term of maximum degree is obtained multiplying the elements of the principal diagonal, which are monic) of $\mathbb{Z}[x]$ that evaluated in ϵ is 0. This proves that ϵ, and hence γ, are integral over $\mathbb{Z}$. So $\gamma \in \mathcal{O}_{\mathbb{K}}$.

□

2.4 Quadratic Fields

In this section with $\mathbb{K}$ we will denote a *quadratic field*, i.e. an extension of degree 2 of the field of rational numbers. Our aim is to characterize the quadratic fields and their ring of integers. For the following results, definitions and terminology we refer to Chapter 6 of [11].

Theorem 2.27. *All and only the quadratic fields $\mathbb{K}$ are that of the form $\mathbb{Q}(\sqrt{d})$ with $d \neq 1$ squarefree integer (i.e the square of each integer different from ± 1 does not divide d). Furthermore, $\{1, \sqrt{d}\}$ is a basis for $\mathbb{Q}(\sqrt{d})$.*

Proof. First consider $\mathbb{Q}(\sqrt{d}) = \{f(\sqrt{d}) \mid f(x) \in \mathbb{Q}[x]\}$ with $d \neq 1$ square free integer. To prove that $\mathbb{Q}(\sqrt{d})$ is a field, we consider the minimal polynomial $p(x) = x^2 - d \in \mathbb{Z}[x]$ of $\sqrt{d}$ over $\mathbb{Q}$. Given some $\alpha = f(\sqrt{d}) \in \mathbb{Q}(\sqrt{d})$, from the irreducibility of $p(x)$ over $\mathbb{Q}[x]$ it follows that there exist $g_1(x), g_2(x) \in \mathbb{Q}[x]$ such that $1 = f(x)g_1(x) + p(x)g_2(x)$. Hence $\alpha g_1(\sqrt{d}) = 1$ and α as an inverse in $\mathbb{Q}(\sqrt{d})$. Now is evident that $\mathbb{Q}(\sqrt{d})$ is a $\mathbb{Q}$-vector space. It is generated by 1 and $\sqrt{d}$: given $(\sqrt{d})^\ell$, with $\ell \in \mathbb{N}$, we can prove by induction on ℓ that $(\sqrt{d})^\ell = q_1 + q_2\sqrt{d}$ for suitable $q_1, q_2 \in \mathbb{Q}$. Furthermore, 1 and $\sqrt{d}$ are independent over $\mathbb{Q}$ since the minimal polynomial $p(x)$ of α has degree 2. Hence $\{1, \sqrt{d}\}$ is a basis of the quadratic field $\mathbb{Q}(\sqrt{d})$.
Now consider a quadratic field $\mathbb{K}$. An element β of $\mathbb{K} \setminus \mathbb{Q}$ is algebraic over $\mathbb{Q}$. Let $p(x) \in \mathbb{Q}[x]$, of degree n, be the minimal polynomial of β over $\mathbb{Q}$. Since $\beta \notin \mathbb{Q}$, we have $n > 1$. The set $\mathbb{Q}(\beta)$ is a $\mathbb{Q}$-vector space that has $\{1, \beta, \dots, \beta^{n-1}\}$ as a basis. In fact $1, \beta, \dots, \beta^{n-1}$ are linearly independent over $\mathbb{Q}$ for the definition of minimal polynomial and they generate $\mathbb{Q}(\beta)$ (since $p(\beta) = 0$, $\beta^n = -q_{n-1}\beta^{n-1} - \cdots - q_1\beta - q_0$ with $q_i \in \mathbb{Q}$ and so we can prove, by induction on the exponent $l \in \mathbb{N}$, that every power β^l could be written as linear combination of $1, \beta, \dots, \beta^{n-1}$ with rational coefficients).
But $\mathbb{Q}(\beta)$ is also a field:

- it is closed under product;
- $\mathbb{Q}(\beta)$ contains the inverse of each non-zero element. Given $\alpha = f(\beta) \in \mathbb{Q}(\sqrt{\beta})$, since $p(x)$ is irreducible over $\mathbb{Q}$, there exist two polynomials $g_1(x), g_2(x) \in \mathbb{Q}[x]$ such that $f(x)g_1(x) + p(x)g_2(x) = 1$. Hence $f(\beta)g_1(\beta) = 1$ and α has an inverse in $\mathbb{Q}(\sqrt{d})$.

Then we have $[\mathbb{Q}(\beta) : \mathbb{Q}] = n$ and, from $[\mathbb{K} : \mathbb{Q}(\beta)][\mathbb{Q}(\beta) : \mathbb{Q}] = 2$, it follows that $n = 2$. So $[\mathbb{K} : \mathbb{Q}(\beta)] = 1$, i.e. $\mathbb{K} = \mathbb{Q}(\beta)$.
We can now observe that β is a root of $ax^2 + bx + c \in \mathbb{Z}[x]$ for suitable $a, b, c \in \mathbb{Z}$. So we have:

$$\beta = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} = \frac{-b \pm e\sqrt{d}}{2a} = \frac{-b + e\sqrt{d}}{2a}$$

where $b^2 - 4ac = e^2 d$, with d squarefree integer, and the sign of $\pm\sqrt{b^2 - 4ac}$ absorbed by e. Obviously $d \neq 1$ and $e \neq 0$ since $\beta \in \mathbb{K} \setminus \mathbb{Q}$. So:

$$\mathbb{K} = \{q_1 + q_2 \frac{-b + e\sqrt{d}}{2} \mid q_1, q_2 \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{d}) \tag{2.17}$$

□

If $\mathbb{Q}(\sqrt{d_1})$ and $\mathbb{Q}(\sqrt{d_2})$ are two equal quadratic fields, with d_1 and d_2 squarefree integers different from 1, then:

$$\sqrt{d_2} = \frac{a_1}{b_1} + \frac{a_2}{b_2}\sqrt{d_1} \Rightarrow d_2 + \left(\frac{a_1}{b_1}y\right)^2 - \left(\frac{a_2}{b_2}\right)^2 d_1 - 2\frac{a_1}{b_1}\sqrt{d_2} = 0$$

with $a_1/b_1, a_2/b_2 \in \mathbb{Q}$. Since 1 and $\sqrt{d_2}$ are linearly independent over $\mathbb{Q}$ we have:

$$\begin{cases} d_2 + \left(\frac{a_1}{b_1}\right)^2 - \left(\frac{a_2}{b_2}\right)^2 d_1 = 0 \\ -2\frac{a_1}{b_1} = 0 \end{cases}$$

and from this follows that

$$\begin{cases} a_1 = 0 \\ (b_2)^2 d_2 = (a_2)^2 d_1 \end{cases}$$

Therefore, since $(b_2)^2$ divides d_1 ($gcd(a_2, b_2) = 1$) and $(a_2)^2$ divides d_2 we have $(a_2)^2 = (b_2)^2 = 1$ and $d_1 = d_2$.

Given a quadratic field $\mathbb{K}$, the unique squarefree integer $d \neq 1$ such that $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, is called the **radicand of** $\mathbb{K}$.

Definition 2.28. *Let $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, with $d \neq 1$ squarefree integer, be a quadratic field. The discriminant of $\mathbb{K}$, denoted by Δ, is defined as:*

$$\Delta = \begin{cases} d & d \equiv 1 \pmod 4 \\ 4d & d \equiv 2, 3 \pmod 4 \end{cases}$$

We observe that $\mathbb{K} = \mathbb{Q}(\sqrt{\Delta})$. When $d \equiv 1 \pmod 4$ this is obvious; in the other case we have $\sqrt{\Delta} = 2\sqrt{d}$. Clearly $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(2\sqrt{d})$.

In the light of Theorem 2.27, we can compute the norm $N_{\mathbb{K}/\mathbb{Q}}(\alpha)$ and the trace $Sp_{\mathbb{K}/\mathbb{Q}}(\alpha)$ of an element α of a quadratic field $\mathbb{K} = \mathbb{Q}(\sqrt{d})$. We consider $\{1, \sqrt{d}\}$ as basis of $\mathbb{K}$. We write $\alpha = q_1 + q_2\sqrt{d}$, where q_1 and q_2 are rational numbers. The matrix that corresponds to the linear map $\varphi_\alpha : \mathbb{K} \to \mathbb{K}$ respect to the fixed basis is:

$$\begin{pmatrix} q_1 & q_2 d \\ q_2 & q_1 \end{pmatrix}$$

The determinant $q_1^2 - (q_2^2)d$ and the trace $2q_1$ of the matrix are the norm $N_{\mathbb{K}/\mathbb{Q}}(\alpha)$ and the trace $Sp_{\mathbb{K}/\mathbb{Q}}(\alpha)$ respectively.
If we denote by $\overline{\alpha}$ what we called the **conjugate of** α:

$$\overline{\alpha} = q_1 - q_2\sqrt{d} \tag{2.18}$$

we have:

$$N_{\mathbb{K}/\mathbb{Q}}(\alpha) = q_1^2 - (q_2^2)d = \alpha\overline{\alpha} \tag{2.19}$$

$$Sp_{\mathbb{K}/\mathbb{Q}}(\alpha) = 2q_1 = \alpha + \overline{\alpha} \tag{2.20}$$

Theorem 2.29. *An element α of a quadratic field $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ is an algebraic integer if and only if $N_{\mathbb{K}/\mathbb{Q}}(\alpha)$ and $Sp_{\mathbb{K}/\mathbb{Q}}(\alpha)$ belong to $\mathbb{Z}$.*

Proof. Suppose that $\alpha \in \mathbb{K}$ has integral norm and integral trace. If $\alpha \in \mathbb{Z}$, it is obviously an algebraic integers. If α belongs to $\mathbb{K} \setminus \mathbb{Z}$, for the proof of Theorem 2.27, its minimal polynomial $p(x) \in \mathbb{Q}[x]$ over $\mathbb{Q}$ has degree 2. So:

$$\alpha^2 + \frac{a_1}{b_1}x + \frac{a_2}{b_2} = 0 \tag{2.21}$$

with $a_1/b_1, a_2/b_2 \in \mathbb{Q}$. Writing $\alpha = q_1 + q_2\sqrt{d}$ for suitable rational numbers q_1, q_2, it is immediate to verify that also $\overline{\alpha}$ is a root of $p(x)$. Since $\overline{\alpha} \neq \alpha$ we have:

$$p(x) = (x - \alpha)(x - \overline{\alpha}) = x^2 - (\alpha + \overline{\alpha})x + \alpha\overline{\alpha} = x^2 - Sp_{\mathbb{K}/\mathbb{Q}}(\alpha)x + N_{\mathbb{K}/\mathbb{Q}}(\alpha) \tag{2.22}$$

Hence $p(x)$ has integral coefficients and α is an algebraic integer.
Vice versa, suppose that α is an algebraic integer. If α belong to $\mathbb{Z}$, its norm and trace obviously are integers. When $\alpha \in \mathbb{K} \setminus \mathbb{Z}$, from the previous case we know that its minimal polynomial $p(x)$ over $\mathbb{Q}$ is equal to:

$$p(x) = x^2 - Sp_{\mathbb{K}/\mathbb{Q}}(\alpha)x + N_{\mathbb{K}/\mathbb{Q}}(\alpha) \tag{2.23}$$

But, by definition of algebraic integer, $p(x)$ lies in $\mathbb{Z}[x]$ and so $N_{\mathbb{K}/\mathbb{Q}}(\alpha), Sp_{\mathbb{K}/\mathbb{Q}}(\alpha) \in \mathbb{Z}$. □

Proposition 2.30. *Let $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ be a quadratic field. The ring of integers $\mathcal{O}_{\mathbb{K}}$ of $\mathbb{K}$ is $\{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ if $d \equiv 2, 3 \pmod 4$ and it is $\{\frac{a+b\sqrt{d}}{2} \mid a, b \in \mathbb{Z} \wedge a \equiv b \pmod 4\}$ if $d \equiv 1 \pmod 4$.*

Proof. The quadratic field $\mathbb{K}$ is equal to the set

$$S = \left\{ \frac{a + b\sqrt{d}}{2} \mid a, b \in \mathbb{Q} \right\}$$

since $\mathbb{K}$ is generated by 1 and $\sqrt{d}$. In the light of 2.19 and 2.20, for an element $\nu = (a + b\sqrt{d})/2$ of the quadratic field we have:

$$N_{\mathbb{K}/\mathbb{Q}}\left(\frac{a + b\sqrt{d}}{2}\right) = \frac{a^2 - b^2 d}{4} \quad , \quad Sp_{\mathbb{K}/\mathbb{Q}}\left(\frac{a + b\sqrt{d}}{2}\right) = a \tag{2.24}$$

We want to show that ν belongs to $\mathcal{O}_{\mathbb{K}}$ if and only if a, b are integers and

$$\begin{cases} a \equiv b \pmod 2 & d \equiv 1 \pmod 4 \\ a \equiv b \equiv 0 \pmod 2 & d \equiv 2, 3 \pmod 4 \end{cases}$$

If a, b are integers with the above property, then $N_{\mathbb{K}/\mathbb{Q}}(\nu)$ and $Sp_{\mathbb{K}/\mathbb{Q}}(\nu)$ belong to $\mathbb{Z}$ and then, in the light of Theorem 2.29, ν is an algebraic integer. This proves the sufficient condition.
Vice versa, if ν is an algebraic integer then $a, \frac{a^2-b^2d}{4} \in \mathbb{Z}$ and also b^2d is an integer, since

$$a^2 - 4\frac{a^2-b^2d}{4} = b^2d$$

Furthermore, $a^2 - b^2d$ must be zero modulo 4. This forces $a \equiv b \pmod 2$ when d is congruent to 1 modulo 4 and $a \equiv b \equiv 0 \pmod 2$ when $d \equiv 2, 3 \pmod 4$. □

Corollary 2.31. *Let $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ be a quadratic field of discriminant Δ.*
Define ω as:

$$\omega = \begin{cases} \frac{1+\sqrt{\Delta}}{2} = \frac{1+\sqrt{d}}{2} & \Delta \equiv 1 \pmod 4 \\ \sqrt{\frac{\Delta}{4}} = \sqrt{d} & \Delta \equiv 0 \pmod 4 \end{cases}$$

Then we have that:

$$\mathcal{O}_{\mathbb{K}} = [1, \omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$$

Proof. When $d \equiv 2, 3 \pmod 4$, we have $\Delta = 4d$, $\omega = \sqrt{\Delta/4} = \sqrt{d}$ and $\mathcal{O}_{\mathbb{K}} = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$. Hence the result is clear. Suppose that $d \equiv 1 \pmod 4$. Then $\Delta = d$, $\omega = (1+\sqrt{d})/2$ and $\mathcal{O}_{\mathbb{K}} = \{(a + b\sqrt{d})/2 \mid a, b \in \mathbb{Z} \wedge a \equiv b \pmod 2\}$. It is evident that $[1, \omega] \subset \mathcal{O}_{\mathbb{K}}$. Vice versa, if $(a + b\sqrt{d})/2$ belongs to $\mathcal{O}_{\mathbb{K}}$ then:

$$\frac{a + b\sqrt{d}}{2} = \frac{a-b}{2} + b\left(\frac{1+\sqrt{d}}{2}\right) \in [1, \omega]$$

since a, b are two integers with the same parity. □

Given a quadratic field $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, we have that $\{1, \omega\}$ generates the maximal order $\mathcal{O}_{\mathbb{K}}$ of $\mathbb{K}$. Furthermore, 1 and ω are linearly independent over $\mathbb{Q}$ (since the same holds for 1 and $\sqrt{d}$) and hence over $\mathbb{Z}$. So $\{1, \omega\}$ is a basis of the maximal order $\mathcal{O}_{\mathbb{K}}$ and it is called **integral basis of $\mathcal{O}_{\mathbb{K}}$**.

2.5 Ideals of a quadratic field

A non-zero ideal I of the ring of integers $\mathcal{O}_{\mathbb{K}}$ of a quadratic field $\mathbb{K}$ is a $\mathbb{Z}$-submodule of $\mathcal{O}_{\mathbb{K}}$. For Corollary 2.13, I is finitely generated. In particular, I is an order in $\mathbb{K}$:

Proposition 2.32. *Let $\mathbb{K}$ be a quadratic field and I a non-zero ideal of $\mathcal{O}_{\mathbb{K}}$. Then I contains a basis of the $\mathbb{Q}$-vector space $\mathbb{K}$.*

Proof. Let $\{\alpha_1, \alpha_2\}$ be a basis of $\mathbb{K}$. From the proof of Proposition 2.24 follows:

$$\alpha_1 = \frac{\gamma_1}{\ell_1} \quad ; \qquad \alpha_2 = \frac{\gamma_2}{\ell_2} \tag{2.25}$$

with $\gamma_1, \gamma_2 \in \mathcal{O}_{\mathbb{K}}$ and $\ell_1, \ell_2 \in \mathbb{Z}$. Furthermore, we know that I contains at least a non-zero integer ℓ (see the prof of Proposition 2.25). Hence $\ell\ell_1\alpha_1$, $\ell\ell_2\alpha_2$ are contained in I and they form a basis for $\mathbb{K}$ since $\ell\ell_1$ and $\ell\ell_2$ are non-zero. □

Following [11, Chapter 6], we are going to show, by means of several smaller propositions, that a non-zero ideal I of $\mathcal{O}_{\mathbb{K}}$, with $\mathbb{K}$ quadratic field, has a unique basis, as order, of the form $\{a, b + g\omega\}$ where $a, b, g \in \mathbb{Z}$, a is positive, $0 \leq b < a$, $0 < g \leq a$ and g divides both a and b.

Theorem 2.33. *Every non-zero ideal I of the ring of integers $\mathcal{O}_{\mathbb{K}}$ of a quadratic field $\mathbb{K}$ admits, as order, a basis $\{a, b + g\omega\}$ with $a, b, g \in \mathbb{Z}$, a positive, $0 \leq b < a$ and $0 < g \leq a$.*

Proof. Given a basis $\{\alpha_1, \alpha_2\}$ of the order I, we have:

$$\alpha_1 = a_1 + b_1\omega \quad ; \quad \alpha_2 = a_2 + b_2\omega \qquad a_1, b_1, a_2, b_2 \in \mathbb{Z}$$

We already seen (proof of Proposition 2.12), that if we substitute α_1 with $\alpha_1 + t\alpha_2$ ($t \in \mathbb{Z}$) we obtain a new basis for I; the same holds if we substitute α_2 with $\alpha_2 + t\alpha_1$ with $t \in \mathbb{Z}$. In the light of the Euclidean Algorithm to find the greatest common divisor of two integers, we proceed in this way:

1. $b_2 = q_1 b_1 + r_1$ with $q_1, r_1 \in \mathbb{Z}$ and $0 \leq r_1 < b_1$. So:

   $$\alpha_2' = \alpha_2 - q_1\alpha_1 = (a_2 - q_1 a_1) + (b_2 - q_1 b_1)\omega = (a_2 - q_1 a_1) + r_1\omega$$

   If $r_1 = 0$ then $b_1 = gcd(b_1, b_2)$, if $r_1 \neq 0$ we go further;

2. $b_1 = q_2 r_1 + r_2$ with $q_2, r_2 \in \mathbb{Z}$ and $0 \leq r_2 < r_1$. Therefore

   $$\alpha_1' = \alpha_1 - q_2\alpha_2' = (a_1 - q_2(a_2 - q_1 a_1)) + (b_1 - q_2 r_1)\omega = (a_1 - q_2(a_2 - q_1 a_1)) + r_2\omega$$

   If $r_2 \neq 0$ we return to the first step.

After a finite number of steps, we obtain a basis for I of the form $\{a, b + g\omega\}$ where a, b, g are integers and $g > 0$ is the greatest common divisor of b_1 and b_2. We can assume b_1 and b_2 positive since we can change the signs of α_1 and α_2. For the same reason we can assume $a > 0$. We can also divide b by a obtaining $b = qa + r$, with $q, r \in \mathbb{Z}$ such that $0 \leq r < a$, and a new basis $\{a, b + g\omega - qa\} = \{a, r + g\omega\}$. So, in the basis $\{a, b + g\omega\}$ we suppose $0 \leq b < a$.

Now, $a\omega$ belongs to I, so $a\omega = a\ell_1 + (b + g\omega)\ell_2$, for suitable integers ℓ_1, ℓ_2. For the linear independence of 1 and ω over $\mathbb{Z}$, we have $a = g\ell_2$ and hence $0 < g \leq a$. This completes the proof.

□

Proposition 2.34. *Let I be a non-zero ideal of the ring of integers $\mathcal{O}_{\mathbb{K}}$ of a quadratic field $\mathbb{K}$ and $\{a, b+g\omega\}$ a basis of the order I, with $a, b, g \in \mathbb{Z}$, a positive, $0 \leq b < a$ and $0 < g \leq a$. Then every integer m that belongs to I is a multiple of a. In particular a divides $N_{\mathbb{K}/\mathbb{Q}}(b+g\omega)$.*

Proof. If the integer m belongs to I, it could be uniquely written as a linear combination, with integral coefficients, of the elements of the basis $\{a, b+g\omega\}$:

$$m = a\ell_1 + \ell_2(b+g\omega) \Rightarrow (a\ell_1 + b\ell_2 - m) + g\ell_2\omega = 0 \qquad \ell_1, \ell_2 \in \mathbb{Z}$$

Since 1 and ω are linearly independent over $\mathbb{Z}$ it follows $\ell_2 = 0$ (g is non-zero). This implies $m = a\ell_1$. So m is a multiple of a.
Now, it is easy to observe that $\overline{b+g\omega} = b + g\overline{\omega}$. Since $\overline{\omega}$ belongs to the ring $\mathcal{O}_{\mathbb{K}}$ (see Proposition 2.30), then also $b+g\overline{\omega}$ belongs to $\mathcal{O}_{\mathbb{K}}$ and the integer $N_{\mathbb{K}/\mathbb{Q}}(b+g\omega) = (b+g\omega)(b+g\overline{\omega})$ is an element of I. So a divides $N_{\mathbb{K}/\mathbb{Q}}(b+g\omega)$. □

Proposition 2.35. *Every non-zero ideal I of the ring of integers $\mathcal{O}_{\mathbb{K}}$ of a quadratic field $\mathbb{K}$ admits a unique basis $\{a, b+g\omega\}$, as order, with $a, b, g \in \mathbb{Z}$, a positive, $0 \leq b < a$ and $0 < g \leq a$.*

Proof. For the existence of the basis we refer to Proposition 2.33. For the uniqueness, suppose that $\{a', b'+g'\omega\}$ is another basis of I that respects the conditions of the claim. Since a divides a' and vice versa, we have $a = a'$. Furthermore, $b' + g'\omega = a\ell_1 + (b+g\omega)\ell_2$ for suitable integers ℓ_1, ℓ_2 and, since 1 and ω are linearly independent over $\mathbb{Z}$, we have that g divides g'. Analogously we can obtain that g is a multiple of g' and so $g = g'$. Using $b' + g\omega = a\ell_1 + (b+g\omega)\ell_2$, it follows $b' - b = a\ell_1$ since ℓ_2 must be 1. But b and b' are both less then a, so ℓ_1 must be zero. □

Theorem 2.36. *Every non-zero ideal I of the ring of integers $\mathcal{O}_{\mathbb{K}}$ of a quadratic field $\mathbb{K}$ admits, as order, a unique basis $\{a, b+g\omega\}$ with $a, b, g \in \mathbb{Z}$, a positive, $0 \leq b < a$, $0 < g \leq a$ and such that g divides both a and b.*

Proof. In the light of the previous proposition, I admits a unique basis $\{a, b+g\omega\}$ with $a, b, g \in \mathbb{Z}$, a positive, $0 \leq b < a$, $0 < g \leq a$. We have to prove only that, for this basis, g divides a and b. Let m be the greatest common divisor of a and g. For the Bézout identity, there exist two integers ℓ_1, ℓ_2 such that $a\ell_1 + g\ell_2 = m$. From:

$$a\ell_1\omega \in I \quad \Rightarrow \quad a\ell_1\omega + (b+g\omega)\ell_2 = m\omega + b\ell_2 = ar + s(b+g\omega) \tag{2.26}$$

(with r, s suitable integers) it follows that $m = sg$, i.e. g divides a.
On the other hand, since $\omega^2 = \ell_1' + \ell_2'\omega$ for $\ell_1', \ell_2' \in \mathbb{Z}$, we have:

$$(b+g\omega)\omega \in I \quad \Rightarrow \quad b\omega + g(\ell_1' + \ell_2'\omega) = g\ell_1' + (b+g\ell_2')\omega = ar' + s'(b+g\omega) \tag{2.27}$$

with r', s' integers. Hence $gs' = b + g\ell_2'$. Hence g divides b. □

The basis $\{a, b+g\omega\}$ of the non-zero ideal $I \subset \mathcal{O}_{\mathbb{K}}$ of the previous Theorem is called **canonical basis of** I. This basis is the one that we have find, starting from a generic basis $\{\alpha_1, \alpha_2\}$ of I, in the proof of Theorem 2.33. Using the canonical basis we can easily compute the norm of I. The results proved in the last part of the section follow [42].

Theorem 2.37. *Let I be a non-zero ideal of the ring of integers $\mathcal{O}_{\mathbb{K}}$ of a quadratic field $\mathbb{K}$. If $\{a, b+g\omega\}$ is its canonical basis, then $N(I) = ag$.*

Proof. We want to show that the set $\mathcal{T} = \{r + s\omega \mid 0 \leq r < a, 0 \leq s < g\}$ contains exactly one representative for each class of $\mathcal{O}_{\mathbb{K}}/I$. Let $\ell_1 + \ell_2\omega$, with $\ell_1, \ell_2 \in \mathbb{Z}$, be an element of $\mathcal{O}_{\mathbb{K}}$. Dividing ℓ_2 by g we obtain $\ell_2 = q_1 g + r_1$ with $q_1, r_1 \in \mathbb{Z}$ and $0 \leq r_1 < g$. We have:

$$\ell_1 + \ell_2\omega - q_1(b + g\omega) = \ell_1 - q_1 b + r_1\omega \tag{2.28}$$

and hence $\ell_1 + \ell_2\omega \equiv \ell_1' + r_1\omega \pmod{I}$ since $q_1(b+g\omega)$ belongs to I. Now divide ℓ_1' by a: $\ell_1' = q_2 a + r_2$ with $q_2, r_2 \in \mathbb{Z}$ and $0 \leq r_2 < a$. Then $\ell_1' + r_1\omega \equiv r_2 + r_1\omega \pmod{I}$ with $r_2 + r_1\omega \in \mathcal{T}$.

Now, suppose that the elements $r + s\omega, r' + s'\omega$ of $\mathcal{T}$ are equivalent modulo I. Then $r - r' + (s - s')\omega$ belongs to I and $s - s'$ is divisible by g. This implies $s = s'$ and $r - r'$ multiple of a. So $r = r'$ and $r + s\omega = r' + s'\omega$. □

If $\{a, b+g\omega\}$ is the canonical basis of a non-zero ideal $I \subset \mathcal{O}_{\mathbb{K}}$, with $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ quadratic field of discriminant Δ, setting $\alpha_1 = a$ and $\alpha_2 = b + g\omega$ we have:

$$\left|\frac{\overline{\alpha_1}\alpha_2 - \alpha_1\overline{\alpha_2}}{\sqrt{\Delta}}\right| = \left|\frac{ag(\omega - \overline{\omega})}{\sqrt{\Delta}}\right| \tag{2.29}$$

In the light of Corollary 2.31, we can compute:

$$\omega - \overline{\omega} = \begin{cases} \frac{1+\sqrt{\Delta}}{2} - \frac{1-\sqrt{\Delta}}{2} = \sqrt{\Delta} & \Delta \equiv 1 \pmod{4} \\ \sqrt{\frac{\Delta}{4}} + \sqrt{\frac{\Delta}{4}} = \sqrt{\Delta} & \Delta \equiv 0 \pmod{4} \end{cases}$$

So:

$$\left|\frac{\overline{\alpha_1}\alpha_2 - \alpha_1\overline{\alpha_2}}{\sqrt{\Delta}}\right| = |ag| = ag = N(I) \tag{2.30}$$

Now suppose that $\{\alpha_1, \alpha_2\}$ is a generic basis of the order I. We have:

$$\alpha_1 = a_1 + b_1\omega \quad ; \qquad \alpha_2 = a_2 + b_2\omega \qquad a_1, b_1, a_2, b_2 \in \mathbb{Z}$$

from which follows

$$\left|\frac{\overline{\alpha_1}\alpha_2 - \alpha_1\overline{\alpha_2}}{\sqrt{\Delta}}\right| = \left|\frac{(a_1b_2 - a_2b_1)(\omega - \overline{\omega})}{\sqrt{\Delta}}\right| = |a_1b_2 - a_2b_1| \tag{2.31}$$

If we substitute α_1 with $\alpha_1' = \alpha_1 + t\alpha_2$ ($t \in \mathbb{Z}$) as in the proof of Theorem 2.33 we obtain that:

$$\left|\frac{(\overline{\alpha_1} + t\overline{\alpha_2})\alpha_2 - (\alpha_1 + t\alpha_2)\overline{\alpha_2}}{\sqrt{\Delta}}\right| = \left|\frac{\overline{\alpha_1}\alpha_2 - \alpha_1\overline{\alpha_2}}{\sqrt{\Delta}}\right| \tag{2.32}$$

The same holds if we substitute α_2 with $\alpha_2' = \alpha_2 + t\alpha_1$ ($t \in \mathbb{Z}$) and if we change the signs of α_1 and α_2. With elementary transformations of this type, from $\{\alpha_1, \alpha_2\}$ we arrive to the canonical basis. This implies:

$$\left| \frac{\overline{\alpha_1}\alpha_2 - \alpha_1\overline{\alpha_2}}{\sqrt{\Delta}} \right| = N(I) \tag{2.33}$$

A second way to compute the norm of a non-zero ideal I of $\mathcal{O}_{\mathbb{K}}$, with $\mathbb{K}$ a quadratic field, uses the conjugates of the elements of $\mathbb{K}$. Define $\overline{I}$ as:

$$\overline{I} = \{\overline{\alpha} \mid \alpha \in I\} \tag{2.34}$$

It is easy to observe that:

- $\overline{I}$ contains 0;
- if $\overline{\alpha_1}$ and $\overline{\alpha}_2$ belong to $\overline{I}$ then $\overline{\alpha_1} + \overline{\alpha_2} = \overline{\alpha_1 + \alpha_2}$ belongs to $\overline{I}$;
- if $\overline{\alpha} \in \overline{I}$ then $-\overline{\alpha} = \overline{-\alpha}$;
- if β belongs to $\mathcal{O}_{\mathbb{K}}$ and $\overline{\alpha} \in \overline{I}$, we have $\overline{\overline{\beta}\alpha} = \beta\overline{\alpha} \in \overline{I}$

since the map

$$\begin{array}{ccc} \mathbb{K} & \to & \mathbb{K} \\ \alpha & \mapsto & \overline{\alpha} \end{array}$$

is an involution, linear over $\mathbb{Q}$ and such that the conjugate of the product of two elements is the product of the conjugates. Hence, $\overline{I}$ is a non-zero ideal of $\mathcal{O}_{\mathbb{K}}$.

Proposition 2.38. *Let $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ be a quadratic field. If I is a non-zero ideal of $\mathcal{O}_{\mathbb{K}}$, then $I\overline{I}$ is a principal ideal generated by an integer.*

Proof. Let $\{\alpha_1, \alpha_2\}$ be a basis of the order I. It is obvious that $I = \langle \alpha_1, \alpha_2 \rangle$ and $\overline{I} = \langle \overline{\alpha_1}, \overline{\alpha_2} \rangle$. Therefore:

$$I\overline{I} = \langle \alpha_1\overline{\alpha_1}, \alpha_1\overline{\alpha_2}, \overline{\alpha_1}\alpha_2, \alpha_2\overline{\alpha_2} \rangle = \langle N_{\mathbb{K}/\mathbb{Q}}(\alpha_1), \alpha_1\overline{\alpha_2}, \overline{\alpha_1}\alpha_2, N_{\mathbb{K}/\mathbb{Q}}(\alpha_2) \rangle \tag{2.35}$$

Consider the ideal of $\mathcal{O}_{\mathbb{K}}$ generated by $N_{\mathbb{K}/\mathbb{Q}}(\alpha_1), Sp_{\mathbb{K}/\mathbb{Q}}(\alpha_1\overline{\alpha_2}), N_{\mathbb{K}/\mathbb{Q}}(\alpha_2)$, that are integers by Theorem 2.29. If $f \in \mathbb{N}$ is their greatest common divisors, then

$$\langle f \rangle \subset \langle N_{\mathbb{K}/\mathbb{Q}}(\alpha_1), Sp_{\mathbb{K}/\mathbb{Q}}(\alpha_1\overline{\alpha_2}), N_{\mathbb{K}/\mathbb{Q}}(\alpha_2) \rangle$$

for the Bézout identity. Actually, the equality holds, since f divides each of the three generators.
If we define $\gamma = \alpha_1\overline{\alpha_2}/f$, we have $\overline{\gamma} = \overline{\alpha_1}\alpha_2/f$ and

$$N_{\mathbb{K}/\mathbb{Q}}(\gamma) = \frac{N_{\mathbb{K}/\mathbb{Q}}(\alpha_1)N_{\mathbb{K}/\mathbb{Q}}(\alpha_2)}{f^2} \quad ; \quad Sp_{\mathbb{K}/\mathbb{Q}}(\gamma) = \frac{Sp_{\mathbb{K}/\mathbb{Q}}(\alpha_1\overline{\alpha_2})}{f} \tag{2.36}$$

for the linearity of the map $Sp_{\mathbb{K}/\mathbb{Q}}$. This implies that γ belongs to $\mathcal{O}_{\mathbb{K}}$ and then f divides both $\alpha_1\overline{\alpha_2}$ and $\overline{\alpha_1}\alpha_2$. Then:

$$I\overline{I} = \langle f \rangle \langle \frac{N_{\mathbb{K}/\mathbb{Q}}(\alpha_1)}{f}, \frac{\alpha_1\overline{\alpha_2}}{f}, \frac{\overline{\alpha_1}\alpha_2}{f}, \frac{N_{\mathbb{K}/\mathbb{Q}}(\alpha_2)}{f} \rangle \tag{2.37}$$

Observing that $\frac{N_{\mathbb{K}/\mathbb{Q}}(\alpha_1)}{f}, \frac{Sp_{\mathbb{K}/\mathbb{Q}}(\alpha_1\overline{\alpha_2})}{f}, \frac{N_{\mathbb{K}/\mathbb{Q}}(\alpha_2)}{f}$ are relative prime and $\frac{Sp_{\mathbb{K}/\mathbb{Q}}(\alpha_1\overline{\alpha_2})}{f} = \frac{\alpha_1\overline{\alpha_2}}{f} + \frac{\overline{\alpha_1}\alpha_2}{f}$, for the Bézout identity we obtain $I\overline{I} = \langle f \rangle$. □

Lemma 2.39. *If a rational number is an algebraic integer, then it belongs to $\mathbb{Z}$ ([11, Proposition 6.4]).*

Proof. Every integer is an algebraic integer. Vice versa, suppose that the algebraic integer (a/b) belongs to $\mathbb{Q}\setminus\mathbb{Z}$ (i.e. $gcd(a,b) = 1$ and $|b| \neq 1$). There exist $c_0, c_1, \ldots, c_{m-1} \in \mathbb{Z}$ such that:

$$\left(\frac{a}{b}\right)^m + c_{m-1}\left(\frac{a}{b}\right)^{m-1} + \cdots + c_0 = 0 \tag{2.38}$$

If we multiply both terms by b^m we obtain:

$$a^m + c_{m-1}a^{m-1}b + \cdots + c_1 a b^{m-1} + c_0 b^m = 0 \tag{2.39}$$

that implies $b|a^m$. This is a contradiction because for hypothesis a and b are coprime. □

Theorem 2.40. *Let I be a non-zero ideal of $\mathcal{O}_{\mathbb{K}}$, with $\mathbb{K}$ quadratic field $\mathbb{K}$. Then $I\overline{I}$ is a principal ideal generated by an integer f such that $|f| = N(I)$.*

Proof. Let $\{a, g(b' + \omega)\}$ be the canonical basis of I. We have seen that $N(I) = ag$ and that $I\overline{I}$ is principal, generated by an integer f. We want to show that $|f| = ag$. We have:

$$I\overline{I} = \langle a^2, ag(b' + \overline{\omega}), ag(b' + \omega), g^2 N_{\mathbb{K}/\mathbb{Q}}(b' + \omega)\rangle \tag{2.40}$$

We observe that $g(b'+\omega)(b'+\overline{\omega})$ belongs to I. But $g(b'+\omega)(b'+\overline{\omega})$ is equal to $gN_{\mathbb{K}/\mathbb{Q}}(b'+\omega)$ that lies in $I \cap \mathbb{Z}$. So it is divisible by a and we have:

$$I\overline{I} = \langle ag \rangle \langle c, (b' + \overline{\omega}), (b' + \omega), \frac{1}{c} N_{\mathbb{K}/\mathbb{Q}}(b' + \omega)\rangle = \langle ag \rangle J \tag{2.41}$$

with J non-zero ideal of $\mathcal{O}_{\mathbb{K}}$. Using the properties of the ideal group $I(\mathcal{O}_{\mathbb{K}})$, we obtain $\langle f/ag \rangle = J$. So J is a principal ideal and $\tilde{f} = f/ag$ is an integer since it is an algebraic integer (see Lemma 2.39). Obviously $\tilde{f}$ must divide every element of J. In particular there exist ℓ_1, ℓ_2 such that $b' + \omega = \tilde{f}(a\ell_1 + \ell_2 g(b' + \omega))$. So we have $\tilde{f}\ell_2 g = 1$ and hence $\tilde{f} = \pm 1$. Now we can conclude: $f = \pm ag$. □

The last theorem allows to obtain two important properties of the ideal norm:

Theorem 2.41. *Let $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ be a quadratic field. Then:*

1. *if I_1 and I_2 are non-zero ideals of $\mathcal{O}_{\mathbb{K}}$, then $N(I_1 I_2) = N(I_1)N(I_2)$;*

2. if α is a non zero element of $\mathcal{O}_{\mathbb{K}}$, then $N(\mathcal{O}_{\mathbb{K}}\alpha) = \left|N_{\mathbb{K}/\mathbb{Q}}(\alpha)\right|$.

Proof. 1) From Theorem 2.40, we know than $N(I_1 I_2)$ is the absolute value of the integral generator of the principal ideal $I_1 I_2 \overline{I_1 I_2}$. Since the conjugate of a product of elements of $\mathbb{K}$ is the product of the conjugates, the ideal $\overline{I_1 I_2}$ is equal to $(\overline{I_1})(\overline{I_2})$. Hence:

$$I_1 I_2 \overline{I_1 I_2} = I_1 \overline{I_1} I_2 \overline{I_2} = \mathcal{O}_{\mathbb{K}} f_1 f_2 \tag{2.42}$$

with $|f_1| = N(I_1)$ and $|f_2| = N(I_2)$. So $N(I_1 I_2) = |f_1 f_2| = N(I_1)N(I_2)$.
2) Given the principal ideal $I = \mathcal{O}_{\mathbb{K}}\alpha$ we have:

$$I\overline{I} = \mathcal{O}_{\mathbb{K}}\alpha\overline{\alpha} = \mathcal{O}_{\mathbb{K}} N_{\mathbb{K}/\mathbb{Q}}(\alpha) \tag{2.43}$$

and $N(I) = \left|N_{\mathbb{K}/\mathbb{Q}}(\alpha)\right|$. □

2.6 Narrow ideal class group and form class group

Let $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ be a quadratic field. We consider the ideal group $I(\mathcal{O}_{\mathbb{K}})$ of the Dedekind ring $\mathcal{O}_{\mathbb{K}}$. The principal fractional ideals of $\mathcal{O}_{\mathbb{K}}$ form a subgroup $P(\mathcal{O}_{\mathbb{K}})$. We can define a subset $P^+(\mathcal{O}_{\mathbb{K}})$ of $P(\mathcal{O}_{\mathbb{K}})$ composed by the principal fractional ideals of $\mathcal{O}_{\mathbb{K}}$ generated by elements of positive norm. Obviously the set contains $\mathcal{O}_{\mathbb{K}}$, the identity of the multiplication. For the multiplicativity of the norm, this set is also closed under multiplication and contains the inverse of each of its elements. So it is a subgroup. We call **narrow ideal class group** the quotient group $C^+(\mathcal{O}_{\mathbb{K}}) = I(\mathcal{O}_{\mathbb{K}})/P^+(\mathcal{O}_{\mathbb{K}})$. Two fractional ideals of $\mathcal{O}_{\mathbb{K}}$ that lie in the same equivalence class of $C^+(\mathcal{O}_{\mathbb{K}})$ are said **narrowly equivalent**.
When d is negative, the norm of any non-zero element of $\mathbb{K}$ is positive and then $P^+(\mathcal{O}_{\mathbb{K}}) = P(\mathcal{O}_{\mathbb{K}})$. When d is positive, the norm of the elements of $\mathbb{K}$ could be positive or negative. Let ϵ be a unit of $\mathcal{O}_{\mathbb{K}}$, i.e. an element of the Dedekind ring that has inverse in $\mathcal{O}_{\mathbb{K}}$, and $\gamma\mathcal{O}_{\mathbb{K}}$ a principal fractional ideal. Then it is easy to observe that $\gamma\mathcal{O}_{\mathbb{K}} = \gamma\epsilon\mathcal{O}_{\mathbb{K}}$. If there exists a unit of norm -1, every principal fractional ideal is generated by some element of $\mathbb{K}$ of positive norm. Hence, also in this case we have the equality:

$$P(\mathcal{O}_{\mathbb{K}}) = P^+(\mathcal{O}_{\mathbb{K}})$$

When such a unit does not exist, an equivalence class $[I] \in C(\mathcal{O}_{\mathbb{K}})$ of the ideal class group contains two classes of equivalence of $C^+(\mathcal{O}_{\mathbb{K}})$: one of the fractional ideals of the form γI with $\gamma \in \mathbb{K}$ of positive norm and one the fractional ideal of the form γI with $\gamma \in \mathbb{K}$ of negative norm.

If the quadratic field $\mathbb{K}$ has discriminant Δ then the narrow ideal class group $C^+(\mathcal{O}_{\mathbb{K}})$ and the form class group $C(\Delta)$ are isomorphic. This allows to define the **class number** $h_{\mathbb{K}}$ of $\mathbb{K}$: it is the finite cardinality of $C^+(\mathcal{O}_{\mathbb{K}})$, equal to h_Δ. In particular, the following result holds ([11, Theorem 6.20]):

Theorem 2.42. *Let $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ be a quadratic field of discriminant Δ. Given an equivalence class of $C^+(\mathcal{O}_\mathbb{K})$ and a non-zero ideal I of $\mathcal{O}_\mathbb{K}$ contained in it, if $\{\alpha_1, \alpha_2\}$ is a basis of I (as order) with $\overline{\alpha_1}\alpha_2 - \alpha_1\overline{\alpha_2}$ positive integer or positive imaginary then*

$$f(x, y) = \frac{(\alpha_1 x + \alpha_2 y)(\overline{\alpha_1} x + \overline{\alpha_2} y)}{N(I)} \tag{2.44}$$

is a binary quadratic form of discriminant Δ. The form f is positive defined if $\Delta < 0$. This correspondence naturally induces an isomorphism Ψ between the narrow ideal class group $C^+(\mathcal{O}_\mathbb{K})$ and the form class group $C(\Delta)$.

The rest of the section will be devoted to the proof of this fundamental result. First of all, we have to show that the map Ψ from $C^+(\mathcal{O}_\mathbb{K})$ to $C(\Delta)$ naturally induced by the correspondence between ideals and quadratic forms is well defined.

We start observing that every fractional ideal J of $\mathbb{K}$ is narrowly equivalent to a non-zero ideal I of $\mathcal{O}_\mathbb{K}$. If J is principal and generated by an element of positive norm, it is narrowly equivalent to $\mathcal{O}_\mathbb{K}$. If J is generated, as $\mathcal{O}_\mathbb{K}$-module, by the elements $\eta_1, \dots, \eta_r$ of $\mathbb{K}$, then for the proof of Proposition 2.24 we have $\eta_i = \alpha_i/\ell_i$, with $\alpha_i \in \mathcal{O}_\mathbb{K}$ and $\ell_i \in \mathbb{Z}$, for every $i \in \{1, \dots, r\}$. Setting $\ell = \ell_1 \cdots \ell_r$, we have that the product of the fractional ideal generated by ℓ and J is a non-zero ideal I of $\mathcal{O}_\mathbb{K}$, that is narrowly equivalent to J.

The second step is verifing that $f(x, y)$ is a binary quadratic form of discriminant Δ. We observe that:

$$f(x, y) = \frac{(\alpha_1 x + \alpha_2 y)(\overline{\alpha_1} x + \overline{\alpha_2} y)}{N(I)} =$$

$$= \frac{N_{\mathbb{K}/\mathbb{Q}}(\alpha_1)x^2 + (N_{\mathbb{K}/\mathbb{Q}}(\alpha_1 + \alpha_2) - N_{\mathbb{K}/\mathbb{Q}}(\alpha_1) - N_{\mathbb{K}/\mathbb{Q}}(\alpha_2))xy + N_{\mathbb{K}/\mathbb{Q}}(\alpha_2)y^2}{N(I)}$$

Since $N(I)$ divides the norm of any element of I (Theorem 2.40), $f(x, y)$ belongs to $\mathbb{Z}[x, y]$. Furthermore, we have that:

$$\left| \frac{\overline{\alpha_1}\alpha_2 - \alpha_1\overline{\alpha_2}}{\sqrt{\Delta}} \right| = \frac{\overline{\alpha_1}\alpha_2 - \alpha_1\overline{\alpha_2}}{\sqrt{\Delta}} = N(I) \tag{2.45}$$

for the hypothesis on the basis and for 2.33. Hence, the discriminant of $f(x, y)$ becomes:

$$\frac{1}{N(I)^2}((\alpha_1\overline{\alpha_2} + \overline{\alpha_1}\alpha_2)^2 - 4\alpha_1\overline{\alpha_1}\alpha_2\overline{\alpha_2}) = \frac{1}{N(I)^2}(\overline{\alpha_1}\alpha_2 - \alpha_1\overline{\alpha_2})^2 = \frac{1}{N(I)^2}N(I)^2\Delta = \Delta$$

It is clear that $f(x, y)$ is primitive: every binary quadratic form (a, b, c) of discriminant Δ is primitive. In fact, if a prime $p \in \mathbb{Z}$ divides a, b and c then Δ is a multiple of p^2. But Δ is squarefree, so p could be only 1 or -1.
If Δ is negative, the norm of any element of the quadratic field is positive. Hence the coefficient of x^2 in $f(x, y)$ is positive and $f(x, y)$ is positive definite.

To be sure that Ψ is well defined it remains to prove that the image does not depend on the basis of I and on the non-zero ideal of $\mathcal{O}_{\mathbb{K}}$ chosen as representative of the class. Let $\{\alpha_1, \alpha_2\}$ and $\{\beta_1, \beta_2\}$ be two basis of the ideal $I \subset \mathcal{O}_{\mathbb{K}}$ seen as order of $\mathbb{K}$. We have:

$$\begin{pmatrix}\alpha_1\\ \alpha_2\end{pmatrix} = \begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}\begin{pmatrix}\beta_1\\ \beta_2\end{pmatrix} \tag{2.46}$$

with $a_{ij} \in \mathbb{Z}$. Vice versa:

$$\begin{pmatrix}\beta_1\\ \beta_2\end{pmatrix} = \begin{pmatrix}b_{11} & b_{12}\\ b_{21} & b_{22}\end{pmatrix}\begin{pmatrix}\alpha_1\\ \alpha_2\end{pmatrix} \tag{2.47}$$

where the b_{ij}'s ar integers. Since every element of I could be uniquely written as a linear combination, with integral coefficients, of the elements of a basis, we have that the product of the matrices $A = (a_{ij})$ and $B = (b_{ij})$ must be the identity matrix. So

$$det(A) = det(B) = \pm 1$$

If we suppose that $\overline{\alpha_1}\alpha_2 - \alpha_1\overline{\alpha_2}$ and $\overline{\beta_1}\beta_2 - \beta_1\overline{\beta_2}$ are positive integers or positive imaginary (as requested by the claim of the theorem) then we obtain that $det(A)$ and $det(B)$ must be equal to 1 since

$$\overline{\alpha_1}\alpha_2 - \alpha_1\overline{\alpha_2} = (a_{11}a_{22} - a_{12}a_{21})(\overline{\beta_1}\beta_2 - \beta_1\overline{\beta_2})$$

Using 2.47 and 2.44 we obtain that the form that corresponds to I using the basis $\{\beta_1, \beta_2\}$ is properly equivalent to the form associated to I using the basis $\{\alpha_1, \alpha_2\}$: the transformation matrix is precisely the transpose of B.

Now suppose that I and J are two narrowly equivalent non-zero ideals of $\mathcal{O}_{\mathbb{K}}$. Then, there exists $\gamma \in \mathbb{K}$, of positive norm, such that $\gamma I = J$. Hence, if $\{\alpha_1, \alpha_2\}$ is a basis of the order I, with $\overline{\alpha_1}\alpha_2 - \alpha_1\overline{\alpha_2}$ positive integer or positive imaginary, we have that J is generated, as $\mathbb{Z}$-module, by $\gamma\alpha_1$ and $\gamma\alpha_2$. They form a basis of the order J and $\overline{\gamma\alpha_1}\gamma\alpha_2 - \gamma\alpha_1\overline{\gamma\alpha_2}$ is a positive integer or a positive imaginary, since γ has positive norm. The quadratic form that correspond to J respect to the basis $\{\gamma\alpha_1, \gamma\alpha_2\}$ is:

$$\frac{(\gamma\alpha_1\overline{\gamma\alpha_1})x^2 + (\gamma\alpha_1\overline{\gamma\alpha_2} + \overline{\gamma\alpha_1}\gamma\alpha_2)xy + (\gamma\alpha_2\overline{\gamma\alpha_2})y^2}{N(J)} \tag{2.48}$$

Observing that $N(J) = \gamma\overline{\gamma}N(I)$ (Theorem 2.41) we can easily deduce the equality with the form corresponding to I respect to the basis $\{\alpha_1, \alpha_2\}$.

The next step is to demonstrate that Ψ is bijective. We refer to [31, Theorem 13.1] for the surjectivity and to [**?**, pag. 192] for the injectivity. We start proving that every quadratic form (a, b, c) of discriminant Δ corresponds to some non-zero ideal of $\mathcal{O}_{\mathbb{K}}$. Consider the $\mathbb{Z}$-module I generated by a and $\frac{b+\sqrt{\Delta}}{2}$. Since $\Delta \equiv b \pmod 2$, the module is contained in $\mathcal{O}_{\mathbb{K}}$ by Proposition 2.30. In particular we have:

$$\frac{b+\sqrt{\Delta}}{2} = \begin{cases} \frac{b-1}{2} + \omega & d \equiv 1 \pmod 4 \\ \frac{b}{2} + \omega & d \equiv 2, 3 \pmod 4 \end{cases}$$

From the linear independence of ω and 1 over $\mathbb{Z}$ it follows that a and $\frac{b+\sqrt{\Delta}}{2}$ form a basis for I. To show that I is an ideal of $\mathcal{O}_{\mathbb{K}}$ it is sufficient to show that ω multiplied by the generators of I gives two elements of I. We have:

$$a\omega = \begin{cases} a(\frac{1-b}{2}) + a(\frac{b-1}{2} + \omega) & d \equiv 1 \pmod 4 \\ a(-\frac{b}{2}) + a(\frac{b}{2} + \omega) & d \equiv 2, 3 \pmod 4 \end{cases}$$

and

$$\left(\frac{b+\sqrt{\Delta}}{2}\right)\omega = \begin{cases} (\frac{1+b}{2})(\frac{b-1}{2} + \omega) + \frac{d-b^2}{4} = (\frac{1+b}{2})(\frac{b-1}{2} + \omega) - ac & d \equiv 1 \pmod 4 \\ \frac{b}{2}(\frac{b}{2} + \omega) + d - \frac{b^2}{4} = \frac{b}{2}(\frac{b}{2} + \omega) - ac & d \equiv 2, 3 \pmod 4 \end{cases}$$

since $\Delta = b^2 - 4ac$. If a is positive, the norm of I is:

$$N(I) = \left|\left(a\frac{b+\sqrt{\Delta}}{2} - a\frac{b-\sqrt{\Delta}}{2}\right)/\sqrt{\Delta}\right| = \left|\left(a\sqrt{\Delta}\right)/\sqrt{\Delta}\right| = a \tag{2.49}$$

and then its correspondent quadratic form is:

$$\frac{(ax + \frac{b+\sqrt{\Delta}}{2}y)(ax + \frac{b-\sqrt{\Delta}}{2}y)}{a} = ax^2 + bxy + cy^2 \tag{2.50}$$

If a is negative the form (a, b, c) is indefinite, so Δ is positive. Consider the ideal $I' = \langle\sqrt{\Delta}\rangle I$ which has $\{a\sqrt{\Delta}, \frac{b\sqrt{\Delta}+\Delta}{2}\}$ as a basis. The norm of I' is:

$$\left|\left(-a\sqrt{\Delta}\frac{b\sqrt{\Delta}+\Delta}{2} - a\sqrt{\Delta}\frac{-b\sqrt{\Delta}+\Delta}{2}\right)/\sqrt{\Delta}\right| = \left|(-a\Delta\sqrt{\Delta})/\sqrt{\Delta}\right| = -a\Delta \tag{2.51}$$

and the quadratic form associated to I' is:

$$\frac{(a\sqrt{\Delta}x + \frac{b\sqrt{\Delta}+\Delta}{2}y)(-a\sqrt{\Delta}x + \frac{-b\sqrt{\Delta}+\Delta}{2}y)}{-a\Delta} = ax^2 + bxy + cy^2 \tag{2.52}$$

This proves the surjectivity of Ψ.
For the injectivity, if to two non-zero ideals I, J of $\mathcal{O}_{\mathbb{K}}$ of basis (as orders) $\{\alpha_1, \alpha_2\}$ and $\{\beta_1, \beta_2\}$ respectively, correspond properly equivalent forms $f(x, y)$, $g(x, y)$, we want to prove that I and J are narrowly equivalent. We have:

$$f(x, y) = \frac{(\alpha_1 x + \alpha_2 y)(\overline{\alpha_1}x + \overline{\alpha_2}y)}{N(I)} \quad ; \quad g(x, y) = \frac{(\beta_1 x + \beta_2 y)(\overline{\beta_1}x + \overline{\beta_2}y)}{N(J)} \tag{2.53}$$

For hypothesis there exist four integers r, s, t, u such that $f(rx + sy, tx + uy) = g(x, y)$ and $ru - st = 1$. So:

$$\frac{(\beta_1 x + \beta_2 y)(\overline{\beta_1}x + \overline{\beta_2}y)}{N(J)} =$$

$$= \frac{((r\alpha_1 + t\alpha_2)x + (s\alpha_1 + u\alpha_2)y)((r\overline{\alpha_1} + t\overline{\alpha_2})x + (s\overline{\alpha_1} + u\overline{\alpha_2}y)}{N(I)} \tag{2.54}$$

Since $g(x,1)$ has at most two roots in $\mathbb{K}$, we have that $-(s\alpha_1 + u\alpha_2)/(r\alpha_1 + t\alpha_2)$ is equal to $-\beta_2/\beta_1$ or to $-\overline{\beta_2}/\overline{\beta_1}$. Hence there exists a non-zero element γ of $\mathbb{K}$ such that

$$r\alpha_1 + t\alpha_2 = \gamma\beta_1 \quad , \qquad s\alpha_1 + \alpha_2 = \gamma\beta_2 \tag{2.55}$$

or

$$r\alpha_1 + t\alpha_2 = \gamma\overline{\beta_1} \quad , \qquad s\alpha_1 + \alpha_2 = \gamma\overline{\beta_2} \tag{2.56}$$

Substituting these relations in the equality 2.54, in both cases we obtain:

$$\gamma\overline{\gamma} = \frac{N(I)}{N(J)} > 0 \tag{2.57}$$

But this implies that only 2.55 holds, for the other equalities we have a contradiction:

$$\overline{\gamma}\beta_1\gamma\overline{\beta_2} - \gamma\overline{\beta_1}\overline{\gamma}\beta_2 = -\gamma\overline{\gamma}(\overline{\beta_1}\beta_2 - \beta_1\overline{\beta_2}) = (ru - st)(\overline{\alpha_1}\alpha_2 - \alpha_1\overline{\alpha_2}) \tag{2.58}$$

since we suppose that for the basis $\{\alpha_1, \alpha_2\}$ and $\{\beta_1, \beta_2\}$ hold the conditions of the claim. From $ru - st = 1$ it follows that $\{\gamma\beta_1, \gamma\beta_2\}$ is a new basis for the order I. So $I = [\gamma\beta_1, \gamma\beta_2]$ and then

$$I = (\gamma\mathcal{O}_{\mathbb{K}})J \tag{2.59}$$

with $\gamma \in \mathbb{K}$ of positive norm. This means that I and J are narrowly equivalent.

Finally, we want to show that Ψ is a group homomorphism [17, Chapter 13]. We start proving that Ψ sends the identity of $C^+(\mathcal{O}_{\mathbb{K}})$ in the identity of $C(\Delta)$. The identity of $C^+(\mathcal{O}_{\mathbb{K}})$ contains the maximal order $\mathcal{O}_{\mathbb{K}}$ of $\mathbb{K}$. Its canonical basis is $\{1, \omega\}$ (see Theorem 2.36). Since $N(\mathcal{O}_{\mathbb{K}}) = 1$, the form associated to $\mathcal{O}_{\mathbb{K}}$ is:

$$x^2 + (\omega + \overline{\omega})xy + \omega\overline{\omega}y^2 \tag{2.60}$$

When $\Delta \equiv 1 \pmod 4$ we have $\omega + \overline{\omega} = 1$ and $\omega\overline{\omega} = (1 - \Delta)/4$. So the obtained form is the principal form of discriminant Δ (see 1.6). When $\Delta \equiv 0 \pmod 4$, we have $\omega + \overline{\omega} = 0$ and $\omega\overline{\omega} = (-\Delta)/4$. Even in this case, the computed form is the principal form of discriminant Δ (see 1.5).

In order to prove that Ψ respects the product, we consider two non-zero ideals of $\mathcal{O}_{\mathbb{K}}$, I_1 and I_2, to which correspond, respectively, the quadratic forms $f_1(x,y)$ and $f_2(x,y)$. The form $f_1(x,y)$ represents properly some positive integer both for positive and negative discriminant Δ. By Propositions 1.7 and Proposition 1.16, there exist two forms (a_1, b_1, c_1), (a_2, b_2, c_2), properly equivalent to $f_1(x,y)$ and $f_2(x,y)$ respectively, with a_1, a_2 coprime positive integers. If their Dirichlet composition is the form (a_1a_2, B, C), with $C = (B^2 - \Delta)/4a_1a_2$, by Lemma 1.15 we have that $f_1(x,y)$ is properly equivalent to the form $Q_1(x,y) = (a_1, B, a_2C)$ and $f_2(x,y)$ is properly equivalent to the form $Q_2(x,y) =$

(a_2, B, a_1C). Using what we have seen about the surjectivity of Ψ, we can deduce that $J_1 = [a_1, (B+\sqrt{\Delta})/2]$ and $J_2 = [a_2, (B+\sqrt{\Delta})/2]$ are two non-zero ideals of $\mathcal{O}_{\mathbb{K}}$ to which correspond the forms $Q_1(x,y)$ and $Q_2(x,y)$ respectively. Furthermore, for the injectivity of Ψ we have that I_1 is narrowly equivalent to J_1 and that I_2 is narrowly equivalent to J_2. The algebraic integer $\lambda = (B+\sqrt{\Delta})/2$ is such that:

$$\lambda^2 = \frac{B^2}{4} + \frac{\Delta}{4} + \frac{B\sqrt{\Delta}}{2} \quad , \quad B\lambda - a_1a_2C = \frac{B^2}{2} + \frac{B\sqrt{\Delta}}{2} - a_1a_2C = \frac{B^2}{4} + \frac{\Delta}{4} + \frac{B\sqrt{\Delta}}{2} \tag{2.61}$$

that means

$$\lambda^2 = B\lambda - a_1a_2C \tag{2.62}$$

Given $\alpha_1 = a_1x_1 + \lambda y_1 \in J_1$ and $\alpha_2 = a_2x_2 + \lambda y_2 \in J_2$, with $x_1, x_2, y_1y_2 \in \mathbb{Z}$, using relation 2.62 we obtain:

$$\alpha_1\alpha_2 = a_1a_2(x_1x_2 - Cy_1y_2) + \lambda(a_1x_1y_2 + a_2x_2y_1 + By_1y_2)$$

and so, setting $x_3 = x_1x_2 - Cy_1y_2$, $y_3 = a_1x_1y_2 + a_2x_2y_1 + By_1y_2$, we can write

$$\alpha_1\alpha_2 = a_1a_2x_3 + \lambda y_3 \qquad x_3, y_3 \in \mathbb{Z}$$

So J_1J_2 is contained in the $\mathbb{Z}$-module $M = [a_1a_2, \lambda]$ generated by a_1a_2 and λ. On the other hand M is contained in J_1J_2. In fact, J_1J_2 contains a_1a_2, $a_1\lambda$, $a_2\lambda$ and so $\lambda \in J_1J_2$ (we can use the Bézout identity since a_1 and a_2 are relatively prime). So $J_1J_2 = [a_1a_2, \lambda]$. Obviously, a_1a_2 and λ are linearly independent over $\mathbb{Z}$, so they form a basis for M. Since $a_1a_2\lambda - a_1a_2\overline{\lambda}$ is equal to $a_1a_2\sqrt{\Delta}$ with $a_1a_2 > 0$, the ideal J_1J_2 has norm a_1a_2 for equation 2.33. So, the quadratic forms that corresponds to J_1J_2 is:

$$\frac{(a_1a_2x + \lambda y)(a_1a_2x + \overline{\lambda}y)}{a_1a_2} = \frac{(a_1a_2)^2x^2 + a_1a_2(\lambda + \overline{\lambda})xy + \lambda\overline{\lambda}y^2}{a_1a_2} = a_1a_2x^2 + Bxy + Cy^2$$

that is the Dirichlet composition of $Q_1(x,y)$ and $Q_2(x,y)$.
In conclusion, Ψ maps the product $[I_1][I_2] \in C^+(\mathcal{O}_{\mathbb{K}})$ in $\Psi([I_1]) \circ \Psi([I_2])$.

Chapter 3

Solving representation problems via elliptic curves

In Chapter 1 we have seen a way, based only on the theory of integral binary quadratic forms, to solve the representation problems for an odd prime p and a discriminant Δ when Δ is not a perfect square.
If we suppose that Δ is the discriminant of a quadratic field $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, in the view of the correspondence between the form class group $C(\Delta)$ and the narrow ideal class group $C^+(\mathcal{O}_\mathbb{K})$ seen in Theorem 2.42, a suitable use of the Class field theory and the elliptic curves over a finite fields leads to our alternative method to solve representation problems. This method concerns the cases of negative fundamental discriminant Δ and of small class number. Before starting the description of the method, we summarize few results, not mentioned in the previous chapters, about the tools we are going to use. The first step is the introduction of the notion of Hilbert class field of a number field. For the terminology used in the next section we refer to [20].

3.1 Hilbert class field

Let $\mathbb{L}$ be a finite extension of a number field $\mathbb{K}$.
Given a non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_\mathbb{K}$, by Theorem 2.8 we have that :

$$\mathfrak{p}\mathcal{O}_\mathbb{L} = \mathfrak{B}_1^{e_1} \cdots \mathfrak{B}_g^{e_g}$$

where $\mathfrak{B}_1, \dots, \mathfrak{B}_g$ are distinct non-zero prime ideals of $\mathcal{O}_\mathbb{L}$ containing $\mathfrak{p}\mathcal{O}_\mathbb{L}$ and $e_1, \dots, e_g$ are positive integers. We say that $\mathfrak{p}$ **ramifies in** $\mathbb{L}$ if at least one of the e_i's is bigger than one; $\mathfrak{p}$ **is unramified in** $\mathbb{L}$ if $e_1 = \cdots = e_g = 1$.

Usually a prime ideal of $\mathcal{O}_\mathbb{K}$ is called **finite prime ideal of** $\mathbb{K}$. This name is due to a second type of prime ideals of $\mathbb{K}$: the infinite prime ideals. A **real infinite prime ideal of** $\mathbb{K}$ is a field homomorphism $\sigma : \mathbb{K} \to \mathbb{R}$; a **complex infinite prime ideal of** $\mathbb{K}$ is a pair of complex conjugated field homomorphisms $\sigma, \overline{\sigma} : \mathbb{K} \to \mathbb{C}$ with $\sigma \neq \overline{\sigma}$ (σ and $\overline{\sigma}$ could

be equal: this happens in the case that $Im(\sigma) \subset \mathbb{R}$).
Given an infinite prime ideal σ of $\mathbb{K}$, we say that σ **ramifies in** $\mathbb{L}$ if it is real and there exists a complex infinite prime ideal $\tilde{\sigma}$ of $\mathbb{L}$ such that $\tilde{\sigma}_{|\mathbb{K}} = \sigma$. Otherwise, we said that σ **is unramified in** $\mathbb{L}$.

Definition 3.1. *A finite extension* $\mathbb{L}$ *of a number field* $\mathbb{K}$ *is said unramified if each prime ideal of* $\mathbb{K}$*, finite or infinite, is unramified in* $\mathbb{L}$*.*

It could happen that a given number field has unramified extensions of arbitrarily high degree. But if we ask for unramified abelian extensions, there is a maximal one:

Theorem 3.2. *Given a number field* $\mathbb{K}$ *there exists a finite Galois extension* $\mathbb{L}$ *of* $\mathbb{K}$ *such that:*

1. $\mathbb{L}$ *is an abelian and unramified extension of* $\mathbb{K}$ *(abelian means that the Galois group* $Gal(\mathbb{L}/\mathbb{K})$ *is abelian);*

2. *any unramified, abelian, Galois finite extension of* $\mathbb{K}$ *is contained in* $\mathbb{L}$*.*

Proof. See [20, §8]. □

The extension $\mathbb{L}$ of the last theorem is called **Hilbert class field of the number field** $\mathbb{K}$. The next lines will be devoted to show the properties of the degree $[\mathbb{L} : \mathbb{K}]$ when $\mathbb{K}$ is an **imaginary quadratic field** $\mathbb{Q}(\sqrt{d})$, i.e. d is negative.

Lemma 3.3. *Let* $\mathbb{K} \subset \mathbb{L}$ *be two number fields, with* $\mathbb{L}$ *Galois extension of* $\mathbb{K}$*, and let* $\mathfrak{p}$ *be a non-zero prime ideal of* $\mathcal{O}_{\mathbb{K}}$ *that is unramified in* $\mathbb{L}$*. If* $\mathfrak{B}$ *is a non-zero prime ideal of* $\mathcal{O}_{\mathbb{L}}$ *containing* $\mathfrak{p}$ *there exists a unique automorphism* $\sigma \in Gal(\mathbb{L}/\mathbb{K})$ *such that* $\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \pmod{\mathfrak{B}}$ *for all* $\alpha \in \mathcal{O}_{\mathbb{L}}$*, where* $N(\mathfrak{p})$ *is the norm* $|\mathcal{O}_{\mathbb{K}}/\mathfrak{p}|$*.*

Proof. See [20, Lemma 5.19] □

This lemma holds for every non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_{\mathbb{K}}$ when $\mathbb{L}$ is the Hilbert class field of $\mathbb{K}$. The unique automorphism σ is called the **Artin Symbol** and it is denoted by $\left(\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{B}}\right)$.

Consider a non-zero prime ideal $\mathfrak{p}$ of the ring of integers $\mathcal{O}_{\mathbb{K}}$ of a number field $\mathbb{K}$. Given a finite extension $\mathbb{L}$ of $\mathbb{K}$ and a non-zero prime ideal $\mathfrak{B}$ of $\mathcal{O}_{\mathbb{L}}$ that contains $\mathfrak{p}$, the map

$$\begin{array}{rccc} \varphi: & \mathcal{O}_{\mathbb{K}}/\mathfrak{p} & \to & \mathcal{O}_{\mathbb{L}}/\mathfrak{B} \\ & [\xi]_{\mathfrak{p}} & \mapsto & [\xi]_{\mathfrak{B}} \end{array}$$

is an homomorphism of fields. In fact, it is well defined ($\mathfrak{B}$ contains $\mathfrak{p}$ and so two elements of $\mathcal{O}_{\mathbb{K}}$ equivalent modulo $\mathfrak{p}$ are also equivalent modulo $\mathfrak{B}$) and clearly respects sum and product. Therefore $Im(\varphi)$ is a subfield of $\mathcal{O}_{\mathbb{L}}/\mathfrak{B}$, so $\mathcal{O}_{\mathbb{K}}/\mathfrak{p}$ could be regarded as subfield of the finite field $\mathcal{O}_{\mathbb{L}}/\mathfrak{B}$. The natural number $f_{\mathfrak{B}|\mathfrak{p}} = [\mathcal{O}_{\mathbb{L}}/\mathfrak{B} : \mathcal{O}_{\mathbb{K}}/\mathfrak{p}]$ is called **inertial degree of** $\mathfrak{p}$ **in** $\mathfrak{B}$.

Corollary 3.4. *Let $\mathbb{K} \subset \mathbb{L}$ be two number fields, with $\mathbb{L}$ Galois extension of $\mathbb{K}$ and $\mathfrak{p}$ prime ideal of $\mathcal{O}_{\mathbb{K}}$ unramified in $\mathbb{L}$. If $\mathfrak{B}$ is a prime ideal of $\mathcal{O}_{\mathbb{L}}$ containing $\mathfrak{p}$ then:*

1. *if $\sigma \in Gal(\mathbb{L}/\mathbb{K})$ then $\left(\frac{\mathbb{L}/\mathbb{K}}{\sigma(\mathfrak{B})}\right) = \sigma \left(\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{B}}\right) \sigma^{-1}$;*

2. *the order of $\left(\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{B}}\right)$ in $Gal(\mathbb{L}/\mathbb{K})$ is $f_{\mathfrak{B}|\mathfrak{p}} = [\mathcal{O}_{\mathbb{L}}/\mathfrak{B} : \mathcal{O}_{\mathbb{K}}/\mathfrak{p}]$.*

Proof. See [20, Corollary 5.21] □

Suppose that the Galois extension $\mathbb{L}$ of $\mathbb{K}$ is abelian. Fixed a non-zero prime ideal $\mathfrak{p} \subset \mathcal{O}_{\mathbb{K}}$ unramified in $\mathbb{L}$, $Gal(\mathbb{L}/\mathbb{K})$ acts transitively on the prime ideals of $\mathcal{O}_{\mathbb{L}}$ containing $\mathfrak{p}$ [20, Theorem 5.9]. So, given two prime ideals of $\mathcal{O}_{\mathbb{L}}$ containing $\mathfrak{p}$, $\mathfrak{B}$ and $\mathfrak{B}'$, there exists $\sigma \in Gal(\mathbb{L}/\mathbb{K})$ such that $\mathfrak{B}' = \sigma(\mathfrak{B})$. Then, for point 1 of the last Corollary and the hypothesis of abelianity, we have:

$$\left(\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{B}'}\right) = \left(\frac{\mathbb{L}/\mathbb{K}}{\sigma(\mathfrak{B})}\right) = \sigma \left(\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{B}}\right) \sigma^{-1} = \left(\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{B}}\right) \tag{3.1}$$

In this case, the Artin Symbol could be written as $\left(\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{p}}\right)$, since it does not depend on $\mathfrak{B}$ but only on $\mathfrak{p}$. Furthermore, from point 2 of the last Corollary and the equality $\left(\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{B}}\right) = \left(\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{B}'}\right)$ it follows $f_{\mathfrak{B}/\mathfrak{p}} = f_{\mathfrak{B}'/\mathfrak{p}}$, i.e. the inertial degree of $\mathfrak{p}$ over a prime ideal $\mathfrak{B}$ of $\mathcal{O}_{\mathbb{L}}$ containing it does not depend of $\mathfrak{B}$ but its the same natural number, that we will denote by $f_{\mathfrak{p}}$, for every $\mathfrak{B}$.
The observations of the above lines hold when $\mathbb{L}$ is the Hilbert class field of $\mathbb{K}$.

When $\mathbb{L}$ is an abelian extension of $\mathbb{K}$, we can define the Artin symbol for every fractional ideal of $\mathcal{O}_{\mathbb{K}}$. Let $I(\mathcal{O}_{\mathbb{K}})$ be the ideal group of $\mathcal{O}_{\mathbb{K}}$ and $\mathfrak{a}$ one of its elements. By Theorem 2.9 we have:

$$\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{r_i}$$

where the $\mathfrak{p}_i$'s are distinct prime ideals of $\mathcal{O}_{\mathbb{K}}$ and $r_i \in \mathbb{Z}$. The Artin symbol for $\mathfrak{a}$ is:

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

This allows to introduce the **Artin map**:

$$\begin{array}{cccc} \left(\frac{\mathbb{L}/\mathbb{K}}{\cdot}\right): & I(\mathcal{O}_{\mathbb{K}}) & \to & Gal(\mathbb{L}/\mathbb{K}) \\ & \mathfrak{a} & \mapsto & \left(\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{a}}\right) \end{array}$$

where $\left(\frac{\mathbb{L}/\mathbb{K}}{\mathcal{O}_{\mathbb{K}}}\right) = Id_{\mathbb{L}}$ for convention. It is clear that the Artin map is an homomorphism of groups (it respect the product: the prime factors decomposition of a fractional ideal is unique).

Artin reciprocity theorem for the Hilbert class field. *Let $\mathbb{L}$ be the Hilbert class field of a number field $\mathbb{K}$. The Artin Map $\left(\frac{\mathbb{L}/\mathbb{K}}{\cdot}\right)$ is surjective and its kernel is $P(\mathcal{O}_{\mathbb{K}})$. Thus the Artin map induces an isomorphism between $Gal(\mathbb{L}/\mathbb{K})$ and the ideal class group $C(\mathcal{O}_{\mathbb{K}})$.*

Proof. See [20, §8]. □

The second part of the Artin reciprocity theorem follows from the first isomorphism theorem for groups. In particular the isomorphism is:

$$\begin{array}{rccc} \varphi: & C(\mathcal{O}_{\mathbb{K}}) & \rightarrow & Gal(\mathbb{L}/\mathbb{K}) \\ & [\mathfrak{a}] & \mapsto & \left(\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{a}}\right) \end{array}$$

Assuming that $\mathbb{L}$ is the Hilbert class field of a number field $\mathbb{K}$, we can deduce that:

- given a non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_{\mathbb{K}}$ and a prime ideal $\mathfrak{B}$ of $\mathcal{O}_{\mathbb{L}}$ containing $\mathfrak{p}$, the inertial degree $f_{\mathfrak{p}}$ is equal to the order of $((\mathbb{L}/\mathbb{K})/\mathfrak{p})$ in $Gal(\mathbb{L}/\mathbb{K})$ and then to the order of $[\mathfrak{p}]$ in $C(\mathcal{O}_{\mathbb{K}})$;

- when $\mathbb{K}$ is an imaginary quadratic field $\mathbb{Q}(\sqrt{d})$, i.e. d is negative, $C(\mathcal{O}_{\mathbb{K}})$ is equal to $C^{+}(\mathcal{O}_{\mathbb{K}})$. Then, by Theorem 2.42, we have that $C(\Delta)$, with Δ discriminant of $\mathbb{K}$, is isomorphic to $Gal(\mathbb{L}/\mathbb{K})$. Hence the degree of $\mathbb{L}$ over $\mathbb{K}$ is the class number $h_{\mathbb{K}}$ of $\mathbb{K}$ (see Section 2.6). In fact, the Hilbert class field of $\mathbb{K}$ is a finite Galois extension, i.e. $[\mathbb{L} : \mathbb{K}] = |Gal(\mathbb{L}/\mathbb{K})|$.

Since $\mathbb{K}$ and $\mathbb{Q}$ have both characteristic 0, the Hilbert class field $\mathbb{L}$ of $\mathbb{K}$ is separable over $\mathbb{K}$ and over $\mathbb{Q}$ ([19, Proposition 5.3.7]). So we can apply the primitive element theorem ([19, Theorem 5.4.1]) to deduce that:

- $\mathbb{L} = \mathbb{Q}(\alpha)$ for some $\alpha \in \mathbb{L}$. The minimal polynomial over $\mathbb{Q}$ of α will be denoted by $H_{\mathbb{K}}(x)$;

- there exists $\gamma \in \mathbb{L}$ such that $\mathbb{L} = \mathbb{K}(\gamma)$. The minimal polynomial of γ over $\mathbb{K}$ will be denoted by $h_{\mathbb{K}}(x)$ and called **Hilbert class polynomial of** $\mathbb{K}$. In particular, if $\mathbb{K}$ is an imaginary quadratic field, $h_{\mathbb{K}}(x)$ has degree $h_{\mathbb{K}}$ and integral coefficients [20, Proposition 5.29].

Furthermore, for the **Principal Ideal Theorem** (see [14, p.157]), every ideal I of $\mathcal{O}_{\mathbb{K}}$ is principal in $\mathcal{O}_{\mathbb{L}}$, i.e. $I\mathcal{O}_{\mathbb{L}}$ is a principal ideal of the ring of integers $\mathcal{O}_{\mathbb{L}}$.

Finally, given a prime ideal $\mathfrak{p}$ of $\mathcal{O}_{\mathbb{K}}$ and its prime factorization $\mathfrak{B}_1^{e_1} \cdots \mathfrak{B}_g^{e_g}$ in $\mathcal{O}_{\mathbb{L}}$, we have $e_1 = \cdots = e_g = 1$ since $\mathbb{L}$ is an unramified extension of $\mathbb{K}$. If we denote by $f_{\mathfrak{p}}$ the inertial degree of $\mathfrak{p}$ in $\mathfrak{B}_i$ (recall that the inertial degree depends only on $\mathfrak{p}$), from [20, Theorem 5.8] it follows that $f_{\mathfrak{p}}g = [\mathbb{L} : \mathbb{K}]$ and hence $g = [\mathbb{L} : \mathbb{K}]/f_{\mathfrak{p}}$. As observed before, $f_{\mathfrak{p}}$ is the order of $[\mathfrak{p}]$ in $C(\mathcal{O}_{\mathbb{K}})$.

3.2 Elliptic curves with $\mathcal{O}_{\mathbb{K}}$ as endomorphism ring

Let $\mathbb{L}$ be a number field. The equation of an elliptic curve $\mathbb{E}(\mathbb{L} \mid j_0)$, defined over $\mathbb{L}$ and of j-invariant $j_0 \in \mathbb{L} \setminus \{0, 1728\}$, is [58, pag. 47]:

$$y^2 = x^3 + \frac{3j_0}{1728 - j_0}x + \frac{2j_0}{1728 - j_0} \tag{3.2}$$

The elliptic curve defined over $\mathbb{L}$ with j-invariant 0 has equation

$$y^2 = x^3 + 1 \tag{3.3}$$

while the elliptic curve defined over $\mathbb{L}$ with $j_0 = 1728$ has equation

$$y^2 = x^3 + x \tag{3.4}$$

In the last two cases the coefficients of the equations belong to $\mathbb{Q}$.

Assume that $\mathfrak{B}$ is a non-zero prime ideal of $\mathcal{O}_{\mathbb{L}}$. Since the field of fractions of $\mathcal{O}_{\mathbb{L}}$ is $\mathbb{L}$ (see Proposition 2.24), the coefficients of $\mathbb{E}(\mathbb{L} \mid j_0)$ are fractions of elements of $\mathcal{O}_{\mathbb{L}}$. If their denominators do not belong to $\mathfrak{B}$, then we can consider the equivalence classes of the coefficients of $\mathbb{E}$ in the finite field $\mathcal{O}_{\mathbb{L}}/\mathfrak{B}$. In this way we obtain a cubic curve $\overline{\mathbb{E}}$ defined over a finite field. If it is non-singular, then it is an elliptic curve and in the literature ([20, pag. 317]) it is called **reduction of $\mathbb{E}$ modulo $\mathfrak{B}$** and it is also said that $\mathbb{E}$ has **good reduction modulo $\mathfrak{B}$**.
Adapting Deuring's results we can deduce the following Theorem [47].

Theorem 3.5. *Let $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ be an imaginary quadratic field (i.e. d is negative), $\mathcal{O}_{\mathbb{K}}$ its ring of integers and $\mathbb{L}$ its Hilbert class field. Given a prime integer p and a prime ideal $\mathfrak{B}$ of $\mathcal{O}_{\mathbb{L}}$ that contains p, we have $\mathcal{O}_{\mathbb{L}}/\mathfrak{B} = \mathbb{F}_{p^f}$ with $f \in \mathbb{N}$. If $\mathbb{E}(\mathbb{L} \mid j_0)$ is an elliptic curve that has good reduction modulo $\mathfrak{B}$ and endomorphism ring $End_{\mathbb{C}}(\mathbb{E})$ equal to $\mathcal{O}_{\mathbb{K}}$, there exists $\pi \in \mathcal{O}_{\mathbb{K}}$ such that:*

- $p^f = \pi\overline{\pi}$;
- $\left|\overline{\mathbb{E}}(\mathbb{F}_{p^f})\right| = p^f + 1 - (\pi + \overline{\pi})$.

where $\overline{\pi}$ is the conjugate of π in $\mathbb{K}$.

The natural number f of the theorem is the inertial degree of the prime ideal $\langle p \rangle$ of $\mathbb{Z}$ over $\mathfrak{B}$, i.e. $f = [\mathcal{O}_{\mathbb{L}}/\mathfrak{B} : \mathbb{Z}/\langle p \rangle]$. In fact, $\mathfrak{B} \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$ so it contains only one prime integer. By hypothesis $\mathfrak{B}$ lies over p, hence the unique prime integer contained in $\mathfrak{B}$ is p. Therefore, the cardinality of $\mathcal{O}_{\mathbb{L}}/\mathfrak{B}$ is p^f since one of its basis (as $\mathbb{Z}/\langle p \rangle$-vector space) has f elements and the field of scalars has p elements. So we have p^f different linear combinations.

The elliptic curves $\mathbb{E}(\mathbb{L} \mid j_0)$ having $\mathcal{O}_{\mathbb{K}}$ as endomorphism ring, with $\mathbb{L}$ Hilbert class field of the imaginary quadratic field $\mathbb{K}$, are all and only those with j_0 root of the Hilbert class polynomial $h_{\mathbb{K}}(x)$ (see [47, Theorem 6.10]).

Via Theorem 3.5 it is possible to set a correspondence between elliptic curves and binary quadratic forms. Let $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ be the imaginary quadratic field of the theorem, with $d < 0$ square-free integer. We recall how the discriminant Δ of $\mathbb{K}$ was defined (Definition 2.28):

$$\Delta = \begin{cases} d & d \equiv 1 \pmod 4 \\ 4d & d \equiv 2, 3 \pmod 4 \end{cases}$$

Furthermore the ring of integers $\mathcal{O}_{\mathbb{K}}$ is the order $[1, \omega]$ (Corollary 2.31) where:

$$\omega = \begin{cases} \frac{1+\sqrt{\Delta}}{2} = \frac{1+\sqrt{d}}{2} & \Delta \equiv 1 \pmod 4 \\ \\ \sqrt{\frac{\Delta}{4}} = \sqrt{d} & \Delta \equiv 0 \pmod 4 \end{cases}$$

First consider the case $d \equiv 1 \pmod 4$. The algebraic integer π of Theorem 3.5 is:

$$\pi = u + v\omega = u + v\frac{1+\sqrt{d}}{2}$$

for suitable $u, v \in \mathbb{Z}$. So we have that:

$$p^f = \pi\overline{\pi} = \left(u + v\frac{1+\sqrt{d}}{2}\right)\left(u + v\frac{1-\sqrt{d}}{2}\right) =$$

$$= (u)^2 + uv + \frac{1-d}{4}(v)^2 = (u)^2 + uv + \frac{1-\Delta}{4}(v)^2 \tag{3.5}$$

What we have shown is that $p^f = \pi\overline{\pi}$ is actually a representation of p^f via the principal form (1.6) of discriminant Δ.
Similarly, if $d \equiv 2, 3 \pmod 4$, the $\pi \in \mathcal{O}_{\mathbb{K}}$ of Theorem 3.5 is:

$$\pi = u + v\omega = u + v\sqrt{d}$$

for suitable $u, v \in \mathbb{Z}$. Hence:

$$p^f = \pi\overline{\pi} = \left(u + v\sqrt{d}\right)\left(u - v\sqrt{d}\right) =$$

$$= (u)^2 - d(v)^2 = (u)^2 - \frac{\Delta}{4}(v)^2 \tag{3.6}$$

Also in this case $p^f = \pi\overline{\pi}$ is a representation of p^f via the principal form (1.5) of discriminant Δ.

3.3 Main theorem

The connection between binary quadratic forms and elliptic curves introduced in the previous section provides the setting necessary to describe a method, alternative to that viewed in Chapter 1, for solving the representantion problems when the discriminant Δ is negative, fundamental and such that the class number h_Δ is less than or equal to 3.

A discriminant Δ is said **fundamental** if Δ is a squarefree integer when $\Delta \equiv 1 \pmod 4$, and in this case Δ is denoted by d, or of the form $4d$, where d is a squarefree integer such that $d \equiv 2, 3 \pmod 4$, when $\Delta \equiv 0 \pmod 4$. The hypothesis that Δ is negative and fundamental guarantees that Δ is the discriminant of an imaginary quadratic field, in particular it is the discriminant of $\mathbb{K} = \mathbb{Q}(\sqrt{d})$. We denote by $\mathbb{L}$ the Hilbert class field of $\mathbb{K}$ and by $h_{\mathbb{K}}(x) \in \mathbb{Z}[x]$ the corresponding Hilbert class polynomial.

Consider an odd prime integer p for which holds $(\Delta/p) = 1$ and suppose that h_Δ reduced quadratic forms $Q_0(x, y), Q_1(x, y), \ldots, Q_{h_\Delta - 1}(x, y)$, a representative for each proper equivalence class, are known, where $Q_0(x, y)$ is the principal form.

The theorem that follows allows to find a representation of p once we know which reduced forms represent p. The context is the one described in the previous lines.

Main Theorem - Theorem 3.6. *The ideal $p\mathcal{O}_{\mathbb{K}}$, generated in $\mathcal{O}_{\mathbb{K}}$ by the prime integer p, is equal to the product of two distinct conjugates prime ideals of $\mathcal{O}_{\mathbb{K}}$, $\mathfrak{p}$ and $\overline{\mathfrak{p}}$, and p is properly represented by a reduced form $Q_i(x, y)$ of discriminant Δ. If $f_{\mathfrak{p}}$ is the order of $[\mathfrak{p}]$ in $C^+(\mathcal{O}_{\mathbb{K}})$, four representations $Q_0(u, v) = q = p^{f_{\mathfrak{p}}}$ are obtained from*

$$\pm (u_1, v_1) = \begin{cases} \pm \left(\frac{a_q - v}{2} \, , \, \sqrt{\frac{4q - a_q^2}{-\Delta}} \right) & \Delta \equiv 1 \pmod 4 \\ \\ \pm \left(\frac{a_q}{2} \, , \, \sqrt{\frac{4q - a_q^2}{-\Delta}} \right) & \Delta \equiv 0 \pmod 4 \end{cases} \tag{3.7}$$

$$\pm (u_2, v_2) = \begin{cases} \pm \left(\frac{a_q + v}{2} \, , \, -\sqrt{\frac{4q - a_q^2}{-\Delta}} \right) & \Delta \equiv 1 \pmod 4 \\ \\ \pm \left(\frac{a_q}{2} \, , \, -\sqrt{\frac{4q - a_q^2}{-\Delta}} \right) & \Delta \equiv 0 \pmod 4 \end{cases} \tag{3.8}$$

where $N_q = q + 1 - a_q$ is the number of rational points of $\overline{\mathbb{E}}$, the reduction, modulo a prime ideal $\mathfrak{B}$ of $\mathcal{O}_{\mathbb{L}}$ containing $\mathfrak{p}$, of the elliptic curve $\mathbb{E}(\mathbb{L} \mid \jmath_0)$, with $\jmath_0$ a root of $h_{\mathbb{K}}(x)$. Furthermore, if $f_{\mathfrak{p}} \neq 1$ then p is properly represented by a non principal reduced form $Q_i(x, y)$, i.e. there exist two coprime integers x_0, y_0 such that $Q_i(x_0, y_0) = p$. These x_0 and y_0 are found as a solution of one of the Diophantine systems

$$\begin{cases} e_1(x, y) = \pm u_1 \\ e_2(x, y) = \pm v_1 \end{cases} \begin{cases} e_1(x, y) = \pm u_2 \\ e_2(x, y) = \pm v_2 \end{cases} \tag{3.9}$$

of two homogeneus equations in x and y of degree $f_{\mathfrak{p}}$.

Proof. The existence of $i \in \{0, \dots, h_{\mathbb{K}} - 1\}$ such that $Q_i(x, y)$ properly represents p follows from the hypothesis $(\Delta/p) = 1$ and Theorem 1.8. Also the factorization $\mathfrak{p}\overline{\mathfrak{p}}$, with $\mathfrak{p} \neq \overline{\mathfrak{p}}$, of the principal ideal $p\mathcal{O}_{\mathbb{K}}$ is a standard fact (for a proof see [20, Proposition 5.16] or [42, Theorem 2.19]).

The prime integer p is represented by the principal form $Q_0(x, y)$ if and only if $\mathfrak{p}$ is a principal ideal of $\mathcal{O}_{\mathbb{K}}$. If $\mathfrak{p} = \langle \pi \rangle$ then $p\mathcal{O}_{\mathbb{K}} = \langle \pi\overline{\pi} \rangle$, with $\pi\overline{\pi} \in \mathbb{Z}$. Hence, for the group structure of $I(\mathcal{O}_{\mathbb{K}})$, we obtain $\langle p/\pi\overline{\pi} \rangle = \langle \pi\overline{\pi}/p \rangle = \mathcal{O}_{\mathbb{K}}$. In the light of Lemma 2.39, we can deduce $p = \pi\overline{\pi}$ that means p properly represented by $Q_0(x, y)$. Vice versa, if $p = \pi\overline{\pi}$, then $p\mathcal{O}_{\mathbb{K}} = \langle \pi \rangle\langle \overline{\pi} \rangle$. From the uniqueness of the prime factorization of $p\mathcal{O}_{\mathbb{K}}$ it follows $\mathfrak{p} = \langle \pi \rangle$.

In order to prove our theorem, we take a prime ideal $\mathfrak{B}$ of $\mathcal{O}_{\mathbb{L}}$ that contains $\mathfrak{p}$ and an elliptic curve $\mathbb{E}(\mathbb{L} \mid j_0)$ where j_0 is a root of the Hilbert class polynomial $h_{\mathbb{K}}(x)$. As we have seen in Section 2, the cardinality of $\mathcal{O}_{\mathbb{L}}/\mathfrak{B}$ is p^f, where f is the inertial degree of $\langle p \rangle \subset \mathbb{Z}$ in $\mathfrak{B}$. But f coincides with the inertial degree of $\mathfrak{p}$ in $\mathfrak{B}$. For [39, pag. 24] we have that the inertial degree of $\langle p \rangle \subset \mathbb{Z}$ in $\mathfrak{B}$ is equal to the product of the inertial degree of $\mathfrak{p}$ in $\mathfrak{B}$ and the inertial degree of $\langle p \rangle \subset \mathbb{Z}$ in $\mathfrak{p}$. Applying [20, Theorem 5.9] it follows that the inertial degree of $\langle p \rangle \subset \mathbb{Z}$ in $\mathfrak{p}$ is one (we have $e = 1$, $g = 2$ and, from $egf = 2$, $f = 1$). So f is the inertial degree $f_{\mathfrak{p}}$ of $\mathfrak{p}$ in $\mathfrak{B}$ and it is equal to the order of $[\mathfrak{p}]$ in $C(\mathcal{O}_{\mathbb{K}})$, i.e. $f = f_{\mathfrak{p}}$.

The reduction of $\mathbb{E}$ modulo $\mathfrak{B}$ leads to an elliptic curve $\overline{\mathbb{E}}$ defined over the finite field $\mathbb{F}_q$, with $q = p^{f_{\mathfrak{p}}}$. The number N_q of rational points of $\overline{\mathbb{E}}$ could be computed in polynomial time complexity using the Schoof algorithm (see [50] or next chapter) and, by Theorem 3.5, there exists $\pi = u + \omega v \in \mathcal{O}_{\mathbb{K}}$, with $u, v \in \mathbb{Z}$, such that:

$$q = \pi\overline{\pi} \tag{3.10}$$

$$N_q = q + 1 - (\pi + \bar{\pi}) = q + 1 - a_q \tag{3.11}$$

The sum $a_q = \pi + \bar{\pi}$, considered together with the relation $\pi\overline{\pi} = q$ allows to obtain π from N_q and q. In fact, we have:

$$a_q = \pi + \overline{\pi} = (u + \omega v) + (u + \overline{\omega} v) = 2u + (\omega + \overline{\omega})v \tag{3.12}$$

$$q = (u + \omega v)(u + \overline{\omega} v) = u^2 + (\omega + \overline{\omega})uv + \omega\overline{\omega}v^2 \tag{3.13}$$

and then it follows that:

$$\begin{aligned} 4q - a_q^2 = 4u^2 + 4(\omega + \overline{\omega})uv + 4\omega\overline{\omega}v^2 - 4u^2 - 4(\omega + \overline{\omega})uv - (\omega + \overline{\omega})^2v^2 = \\ = -(\omega - \overline{\omega})^2v^2 \end{aligned} \tag{3.14}$$

Hence, from the definition of ω we have:

$$\omega - \overline{\omega} = \begin{cases} \frac{1+\sqrt{\Delta}}{2} - \frac{1-\sqrt{\Delta}}{2} = \sqrt{\Delta} & \Delta \equiv 1 \pmod 4 \\ \\ \sqrt{\frac{\Delta}{4}} + \sqrt{\frac{\Delta}{4}} = \sqrt{\Delta} & \Delta \equiv 0 \pmod 4 \end{cases}$$

and then

$$v = \pm\sqrt{\frac{4q - a_q^2}{-\Delta}} \tag{3.15}$$

Furthermore, from

$$\omega + \overline{\omega} = \begin{cases} \frac{1+\sqrt{\Delta}}{2} + \frac{1-\sqrt{\Delta}}{2} = 1 & \Delta \equiv 1 \pmod 4 \\ \\ \sqrt{\frac{\Delta}{4}} - \sqrt{\frac{\Delta}{4}} = 0 & \Delta \equiv 0 \pmod 4 \end{cases}$$

and the observation that $f(-x,-y) = f(x,y)$ for every quadratic form we can deduce that (u,v) could be one of the following four pairs:

$$\pm(u_1, v_1) = \begin{cases} \pm\left(\frac{a_q - v}{2}\ ,\ \sqrt{\frac{4q-a_q^2}{-\Delta}}\right) & \Delta \equiv 1 \pmod 4 \\ \\ \pm\left(\frac{a_q}{2}\ ,\ \sqrt{\frac{4q-a_q^2}{-\Delta}}\right) & \Delta \equiv 0 \pmod 4 \end{cases} \tag{3.16}$$

$$\pm(u_2, v_2) = \begin{cases} \pm\left(\frac{a_q + v}{2}\ ,\ -\sqrt{\frac{4q-a_q^2}{-\Delta}}\right) & \Delta \equiv 1 \pmod 4 \\ \\ \pm\left(\frac{a_q}{2}\ ,\ -\sqrt{\frac{4q-a_q^2}{-\Delta}}\right) & \Delta \equiv 0 \pmod 4 \end{cases} \tag{3.17}$$

If $\mathfrak{p}$ is a principal ideal, then $q = p$ and u, v are two integers such that $p = \pi\overline{\pi} = Q_0(u,v)$, i.e. we have found a proper representation of p by the principal form $Q_0(x,y)$.
If $\mathfrak{p}$ is not principal, p is properly represented by a non-principal reduced form $Q_i(x,y)$. We can consider the ideal $\mathfrak{I}_{a_i} = \langle a_i, b_i + \omega\rangle$, with $a_i, b_i \in \mathbb{Z}$, such that:

$$Q_i(x,y) = \frac{N_{\mathbb{K}/\mathbb{Q}}(a_i x + (b_i + \omega)y)}{N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{I}_{a_i})} \tag{3.18}$$

Now we observe that the element

$$\frac{N_{\mathbb{K}/\mathbb{Q}}(a_i x + (b_i + \omega)y)^{f_\mathfrak{p}}}{(N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{I}_{a_i}))^{f_\mathfrak{p}}} \tag{3.19}$$

of $\mathbb{K}$ (with $x, y \in \mathbb{Z}$), that is equal to

$$\frac{N_{\mathbb{K}/\mathbb{Q}}((a_i x + (b_i + \omega)y)^{f_\mathfrak{p}})}{(N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{I}_{a_i}^{f_\mathfrak{p}}))} \tag{3.20}$$

for the multiplicativity of the norm both for elements of $\mathbb{K}$ and ideals of $\mathcal{O}_\mathbb{K}$ (Theorem 2.41), is the norm of an algebraic integer

$$\frac{(a_i x + (b_i + \omega)y)^{f_\mathfrak{p}}}{\pi_{a_i}} \tag{3.21}$$

where π_{a_i} is the generator of $\mathfrak{I}_{a_i}^{f_\mathfrak{p}}$.
So we can impose

$$\pi = u + \omega v = \frac{(a_i x + (b_i + \omega)y)^{f_\mathfrak{p}}}{\pi_{a_i}} \tag{3.22}$$

and, from the linear independence of 1 and ω over $\mathbb{Z}$, we obtain the following Diophantine systems in x, y

$$\begin{cases} e_1(x,y) = u \\ e_2(x,y) = v \end{cases} \tag{3.23}$$

where the polynomials $e_1(x,y), e_2(x,y) \in \mathbb{Z}[x,y]$ are homogeneous of degree $f_\mathfrak{p}$ and the constant terms (u,v) could be one of the four pairs $\pm(u_1,v_1), \pm(u_2,v_2)$. □

Remark. In the proof of the Theorem we assume that the elliptic curve $\mathbb{E}$ has good reduction modulo $\mathfrak{B}$ since the number of cases where $\mathbb{E}$ has not good reduction is finite.

Theorem 3.6 could be used to find a representation of p once we know which reduced forms represent p. By the following theorem [2, Theorem 3.2], when $h_\mathbb{K} \leq 3$ we can use the factorization of $h_\mathbb{K}(x) \pmod p$ in $\mathbb{Z}_p$ to determine which are the reduced forms that represent p.

Theorem 3.7. *Let $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ be an imaginary quadratic field of discriminant Δ and let $h_\mathbb{K}(x) \in \mathbb{Z}[x]$ be its Hilbert class polynomial. An odd prime integer p is represented by the principal form $Q_0(x,y)$ of discriminant Δ if and only if $h_\mathbb{K}(x) \pmod p$ has only simple roots and they are all in $\mathbb{Z}_p$.*

Gauss, in his *Disquisitiones Arithmeticae* [26], found nine imaginary quadratic fields with class number 1, and he conjectured he had found all of them. It turns out he was correct. The proof follows from the results of Heegner, Baker and Stark. Furthermore, the work of Goldfeld and Gross-Zagier shows that for every fixed class number N there exist only a finite number of imaginary quadratic fields of class number N. In particular, we know all the imaginary quadratic fields with class number 1,2, and 3.
The next sections will be devoted to find explicit algorithms, deduced from our theorem, for these imaginary quadratic fields.

3.4 Class number 1

The only imaginary quadratic fields $\mathbb{Q}(\sqrt{d})$ which have class number 1 are those with $-d$ in the following set [47, pag.37]:

$$\mathcal{D}_1 = \{1, 2, 3, 7, 11, 19, 43, 67, 163\} \tag{3.24}$$

Let $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ be one of these nine fields and let Δ be its discriminant. Since $C(\Delta)$ contains only the proper equivalence class of the principal form, if $(\Delta/p) = 1$ for an odd prime integer p, then p is properly represented by the principal form $Q_0(x,y)$ of discriminant Δ. A representation could be found as in the proof of Theorem 3.6. The goal of the section

is to construct, in MAGMA language, the explicit algorithm: its structure will be discussed in the following lines and the complete algorithm will be exhibited at the end of the section. The Hilbert class field $\mathbb{L}$ of $\mathbb{K}$ has dimension $h_{\mathbb{K}} = 1$ over $\mathbb{K}$ and hence $\mathbb{K} = \mathbb{L}$. The Hilbert class polynomial $h_{\mathbb{K}}(x)$ has degree one and integral coefficients: its unique root j_0 belongs to $\mathbb{Z}$. We consider the elliptic curve $\mathbb{E}(\mathbb{L} \mid j_0)$. For (3.2), we can observe that $\mathbb{E}$ has rational coefficients. The ideal $p\mathcal{O}_{\mathbb{K}}$ is equal to the product $\mathfrak{p}\overline{\mathfrak{p}}$, where $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ are prime ideals of $\mathcal{O}_{\mathbb{K}}$ containing p with $\mathfrak{p} \neq \overline{\mathfrak{p}}$.
It is easy to see that the map:

$$\begin{array}{rccc} \varphi: & \mathbb{Z}/<p> & \rightarrow & \mathcal{O}_{\mathbb{K}}/\mathfrak{p} \\ & [\ell]_p & \mapsto & [\ell]_{\mathfrak{p}} \end{array}$$

is an isomorphism of fields. Clearly, φ is a field homomorphism, so it is injective. Furthermore, φ is surjective since domain and codomain have the same cardinality. In fact $N(\mathfrak{p}) = p$ by Theorem 2.41 since $\mathfrak{p}\overline{\mathfrak{p}} = p\mathcal{O}_{\mathbb{K}}$. In the light of the isomorphism φ, to verify if $\mathbb{E}$ has good reduction modulo $\mathfrak{p}$ it is sufficient to see wether the integral denominators of the coefficients of $\mathbb{E}$ are non-zero modulo p. Furthermore we can use φ to construct an elliptic curve $\tilde{\mathbb{E}}$ over $\mathbb{Z}_p = \mathbb{Z}/\langle p\rangle$ with the same number of rational points of $\overline{\mathbb{E}}$, the reduction of $\mathbb{E}$ modulo $\mathfrak{p}$. Using the Schoof algorithm we can find the number $N_p = p + 1 - a_p$ of rational points of $\tilde{\mathbb{E}}$. From Theorem 3.5 it follows that:

$$a_p = \pi + \overline{\pi} = (u + \omega v) + (u + \overline{\omega} v) \tag{3.25}$$

and

$$p = (u + \omega v)(u + \overline{\omega} v) \tag{3.26}$$

for some $\pi = u + \omega v \in \mathcal{O}_{\mathbb{K}}$, with u and v integers. Since $\pi\overline{\pi}$ is a representation of p by the principal form of discriminant Δ, u and v must be coprime. By Theorem 3.6, we know the formulas to obtain u and v once we know a_p.

To lower the computational complexity necessary to compute a representation of p by our method, we can construct a database with the following data for each of the nine imaginary quadratic fields of class number 1:

- the discriminant Δ;
- the unique reduced form $Q_0(x, y)$ (i.e. the principal one) of discriminant Δ;
- the root $j_0 \in \mathbb{Z}$ of the Hilbert class polynomial $h_{\mathbb{K}}(x) = x - j_0 \in \mathbb{Z}[x]$;
- the elliptic curve $\mathbb{E}(\mathbb{K} \mid j_0)$.

This information are collected in the following table:

d	Δ	ω	Q_0	$\jmath$	$\mathbb{E}(\mathbb{L} \mid \jmath_0)$
-1	-4	$\sqrt{-1}$	x^2+y^2	12^3	x^3-x
-2	-8	$\sqrt{-2}$	x^2+2y^2	20^3	$x^3-\frac{375}{98}x-\frac{125}{49}$
-3	-3	$\frac{1+\sqrt{-3}}{2}$	x^2+xy+y^2	0	x^3-1
-7	-7	$\frac{1+\sqrt{-7}}{2}$	$x^2+xy+2y^2$	$(-15)^3$	$x^3-\frac{125}{63}x-\frac{250}{189}$
-11	-11	$\frac{1+\sqrt{-11}}{2}$	$x^2+xy+3y^2$	$(-32)^3$	$x^3-\frac{1536}{539}x-\frac{1024}{539}$
-19	-19	$\frac{1+\sqrt{-19}}{2}$	$x^2+xy+5y^2$	$(-96)^3$	$x^3-\frac{512}{171}x-\frac{1024}{513}$
-43	-43	$\frac{1+\sqrt{-43}}{2}$	$x^2+xy+11y^2$	$(-960)^3$	$x^3-\frac{512000}{170667}x-\frac{1024000}{512001}$
-67	-67	$\frac{1+\sqrt{-67}}{2}$	$x^2+xy+17y^2$	$(-5280)^3$	$x^3-\frac{85184000}{28394667}x-\frac{170368000}{85184001}$
-163	-163	$\frac{1+\sqrt{-163}}{2}$	$x^2+xy+41y^2$	$(-640320)^3$	$x^3-\frac{151931373056000}{50643791018667}x-\frac{303862746112000}{151931373056001}$

Table 3.1: Imaginary quadratic fields $\mathbb{K}=\mathbb{Q}(\sqrt{d})$ of class number 1

Remark. The described method to find a representation of p by the principal form Q_0 of discriminant Δ needs some checks to be used in practice:

1. the characteristic of $\mathbb{Z}_p$ must be different from 3 to apply the Schoof algorithm;
2. the cubic curve $\mathbb{E}$ must have good reduction modulo $\mathfrak{p}$;
3. the reduced elliptic curve $\tilde{\mathbb{E}}$ must be non-singular in order to apply the Schoof algorithm.

We observe that:

1. only the quadratic forms of discriminant -8 and -7 properly represent $p=3$, while $(-3/3)=0$;
2. the prime factors of the denominators of the elliptic curve $\mathbb{E}$ used for the discriminant Δ (of one of imaginary quadratic fields with class number 1) are not represented by the principal form of discriminant Δ, so $\mathbb{E}$ has always good reduction;
3. if a_1/b_1 and a_2/b_2 are the coefficient of the elliptic curve $\mathbb{E}$ used for the discriminant Δ, the prime factors of $(b_1)^3(b_2)^2+27(a_2)^2(b_1)^3$ are not represented by the quadratic forms of discriminant Δ, so $\overline{\mathbb{E}}$ is always non-singular.

3.4.1 Algorithm for class number 1

We now attach the explicit algorithm, in MAGMA language, of our method relative to the imaginary quadratic fields of class number 1. For each discriminant Δ contained in $\{-4,-8,-3,-7,-11,-19,-43,-67,-163\}$, the function "Database1" returns the root

j_0 of the Hilbert class polynomial of $\mathbb{Q}(\sqrt{\Delta})$, the coefficient a, b, c of the principal form $Q_0(x, y)$ of discriminant Δ and the coefficients a_1/b_1, a_2/b_2 of the elliptic curve

$$\mathbb{E}(\mathbb{Q}(\sqrt{\Delta}) \mid j_0) = x^3 + (a_1/b_1)x + (a_2/b_2)$$

The function "ClassNumber1" takes the radicand of one of the nine imaginary quadratic fields of class number 1 and a prime integer p such that $(\Delta/p) = 1$, with Δ discriminant of the field. Calling the function "Database1", it constructs the elliptic curve $\tilde{\mathbb{E}}$ defined over $\mathbb{Z}_p$, computes the number of rational points of $\tilde{\mathbb{E}}$ and returns the integers u, v such that

$$Q_0(u, v) = p$$

```
//CLASS NUMBER 1

function Database1 (dK)

   if (dK eq -4) then
      j:=12^3;   a1:=-1;   a2:=1;   b1:=0;   b2:=1;
      a:=1;   b:=0;   c:=1;
   elif (dK eq -8) then
      j:=20^3;   a1:=-375;   a2:=98;   b1:=-125;   b2:=49;
      a:=1;   b:=0;   c:=2;
   elif (dK eq -3) then
      j:=0;   a1:=0;   a2:=1;   b1:=-1;   b2:=1;
      a:=1;   b:=1;   c:=1;
   elif (dK eq -7) then
      j:=(-15)^3;   a1:=-125;   a2:=63;   b1:=-250;   b2:=189;
      a:=1;   b:=1;   c:=2;
   elif (dK eq -11) then
      j:=(-32)^3;   a1:=-1536;   a2:=539;   b1:=-1024;   b2:=539;
      a:=1;   b:=1;   c:=3;
   elif (dK eq -19) then
      j:=(-96)^3;   a1:=-512;   a2:=171;   b1:=-1024;   b2:=513;
      a:=1;   b:=1;   c:=5;
   elif (dK eq -43) then
      j:=(-960)^3;   a1:=-512000;   a2:=170667;   b1:=-1024000;   b2:=512001;
      a:=1;   b:=1;   c:=11;
   elif (dK eq -67) then
      j:=(-5280)^3;   a1:=-85184000;   a2:=28394667;   b1:=-170368000;
      b2:=85184001;   a:=1;   b:=1;   c:=17;
   elif (dK eq -163) then
      j:=(-640320)^3;   a1:=-151931373056000;   a2:=50643791018667;
      b1:=-303862746112000;   b2:=151931373056001;   a:=1;   b:=1;   c:=41;
   end if;

return j,a1,a2,b1,b2,a,b,c;
end function;

function ClassNumber1(d,p)

   if ((d mod 4) eq 1) then
      dK:=d;
   else
```

```
      dK:=4*d;
   end if;
   Zp:=GF(p);
   DK:=Zp!dK;
   // IsSquare(DK);
   j,a1,a2,b1,b2,a,b,c := Database1 (dK);
   A1:=Zp!a1;
   A2:=Zp!a2;
   B1:=Zp!b1;
   B2:=Zp!b2;
   A:=A1/A2;
   B:=B1/B2;
   E:=EllipticCurve([A,B]);
   Np:=#E; //Schoof's algorithm
   ap:=p+1-Np;
   if ((dK mod 4) eq 1) then
      v:=Sqrt((4*p-ap^2)/-dK);
      u:=(ap-v)/2;
   else
      v:=Sqrt((4*p-ap^2)/-dK);
      u:=ap/2;
   end if;
   Z:=Integers();
   u:=Z!u;
   v:=Z!v;

return u,v,a,b,c;
end function;

d:=...;
p:=...;
x,y,a,b,c:=ClassNumber1(d,p);
if (b eq 0) then
   printf "%o=%o*(%o)^2+%o*(%o)^2",p,a,x,c,y;
else
   printf "%o=%o*(%o)^2+%o*(%o)+%o*(%o)^2",p,a,x,b,x*y,c,y;
end if;
```

3.5 Class number 2

The only imaginary quadratic fields $\mathbb{Q}(\sqrt{d})$ which have class number 2 are those with $-d$ in the following set [49, pag.636]:

$$\mathcal{D}_2 = \{5, 6, 10, 13, 15, 22, 35, 37, 51, 58, 91, 115, 123, 187, 235, 267, 403, 427\} \qquad (3.27)$$

Let $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ be one of these fields and let Δ be its discriminant. Given an odd prime integer p such that $(\Delta/p) = 1$, it is properly represented by the principal form $Q_0(x, y)$ or by the other reduced form, $Q_1(x, y)$. In this section we will discuss about the structure of the explicit algorithm to find a representation of p. The complete algorithm will be presented, in MAGMA language, at the end of the section.

The ideal $p\mathcal{O}_{\mathbb{K}}$ is equal to the product $\mathfrak{p}\overline{\mathfrak{p}}$, where $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ are a prime ideals of $\mathcal{O}_{\mathbb{K}}$ containing p, with $\mathfrak{p}$ different from $\overline{\mathfrak{p}}$. The Hilbert class field $\mathbb{L}$ of $\mathbb{K}$ has dimension $h_{\mathbb{K}} = 2$ over $\mathbb{K}$. The Hilbert class polynomial $h_{\mathbb{K}}(x)$ has degree two and integral coefficients. By Theorem 3.7, p is properly represented by $Q_0(x, y)$ if and only if the polynomial $h_{\mathbb{K}}(x) \pmod p$ has only simple roots and they are all in $\mathbb{Z}_p$.

3.5.1 p represented by $Q_0(x, y)$

When p is properly represented by the principal form we proceed as for the quadratic fields of class number 1, with a substantial difference that we will explain. Let $\mathfrak{B}$ be a prime ideal of $\mathcal{O}_{\mathbb{L}}$ that contains $\mathfrak{p}$. As we have seen, the cardinality of $\mathcal{O}_{\mathbb{L}}/\mathfrak{B}$ is equal to $p^{f_{\mathfrak{p}}}$. But $f_{\mathfrak{p}}$ coincides with the order of $[\mathfrak{p}]$ in $C(\mathcal{O}_{\mathbb{K}})$. Therefore $\mathcal{O}_{\mathbb{L}}/\mathfrak{B}$ is a finite field of p elements and the map

$$\begin{array}{cccc} \varphi : & \mathbb{Z}/<p> & \to & \mathcal{O}_{\mathbb{L}}/\mathfrak{B} \\ & [\ell]_p & \mapsto & [\ell]_{\mathfrak{B}} \end{array}$$

is a field isomorphism. Clearly, φ is well defined, since p belongs to $\mathfrak{B}$, and a field homomorphism, hence it isinjective. Furthermore, φ is surjective since domain and codomain have the same finite cardinality.
We consider the elliptic curve $\mathbb{E}(\mathbb{L} \mid j_0)$, where j_0 is a root of $h_{\mathbb{K}}(x)$. Unlike for the imaginary quadratic fields of class number 1, it is not easy to find explicitly the roots of $h_{\mathbb{K}}(x)$ and, consequently, the elliptic curve $\mathbb{E}(\mathbb{L} \mid j_0)$. We can use φ to find, directly, the reduction of $\mathbb{E}$ modulo $\mathfrak{B}$, which is defined over the finite field of p elements and is denoted by $\overline{\mathbb{E}}$. The idea is to consider the equivalence classes in $\mathcal{O}_{\mathbb{L}}/\mathfrak{B}$ of the coefficients of $\mathbb{E}$ and their correspondent elements in $\mathbb{Z}/\langle p\rangle = \mathbb{Z}_p$. For example, given the coefficient $2j_0/(1728 - j_0)$, we have:

$$\left[\frac{2j_0}{1728 - j_0}\right]_{\mathfrak{B}} = \frac{[2]_{\mathfrak{B}}[j_0]_{\mathfrak{B}}}{[1728]_{\mathfrak{B}} - [j_0]_{\mathfrak{B}}} \tag{3.28}$$

Since φ is an isomorphism , to compute $\varphi^{-1}([\frac{2j_0}{1728-j_0}]_{\mathfrak{B}})$ we need only to determine $\varphi^{-1}([j_0])_{\mathfrak{B}}$. We assume to know an integer j_0' such that $[j_0']_p$ is a root of $h_{\mathbb{K}}(x) \pmod p$: the equivalence class $[j_0']_{\mathfrak{B}}$ is also a root of $h_{\mathbb{K}}(x)$ modulo $\mathfrak{B}$. But the polynomial $h_{\mathbb{K}}(x) \pmod{\mathfrak{B}}$ has at most two roots in $\mathcal{O}_{\mathbb{L}}/\mathfrak{B}$. Hence j_0' is equivalent, modulo $\mathfrak{B}$, to one of the roots of $h_{\mathbb{K}}(x)$. It is important to remark that construct $\mathbb{E}$ we can consider, equivalently, one of the roots of $h_{\mathbb{K}}(x)$. Then, the elliptic curve

$$\tilde{\mathbb{E}} : y^2 = x^3 + \frac{[2]_p[j_0']_p}{[1728]_p - [j_0']_p}x + \frac{[3]_p[j_0']_p}{[1728]_p - [j_0']_p} \tag{3.29}$$

defined over $\mathbb{Z}_p$ has the same number of rational points of the reduced curve $\overline{\mathbb{E}}$.
Using the Schoof algorithm (see [50] or next chapter) we can find the number $N_p = p+1-a_p$ of rational points of $\tilde{\mathbb{E}}$. From Theorem 3.5 it follows that:

$$a_p = \pi + \overline{\pi} = (u + \omega v) + (u + \overline{\omega} v) \tag{3.30}$$

and

$$p = (u + \omega v)(u + \overline{\omega} v) \tag{3.31}$$

for some $\pi = u + \omega v \in \mathcal{O}_{\mathbb{K}}$, with u and v integers. The last relation is a representation of p by the principal form $Q_0(x, y)$, so u and v must be coprime. By Theorem 3.6, we know the formulas to obtain u and v once we know a_p.

3.5.2 p represented by $Q_1(x, y)$

Let us suppose that $h_{\mathbb{K}}(x) \pmod p$ is irreducible in $\mathbb{Z}$ or with a root o multiplicity two in $\mathbb{Z}_p$. Hence, p is properly represented by the reduced non-principal form $Q_1(x, y)$. Obviously, $\mathfrak{p}^2$ is principal and then p^2 is represented by the principal form $Q_0(x, y)$. The first step is to find this representation of p^2 using Theorem 3.5. As before, $\mathfrak{B}$ is a prime ideal of $\mathcal{O}_{\mathbb{L}}$ containing $\mathfrak{p}$. The only difference with the previous case is that there exists an isomorphism of fields

$$\varphi : \mathbb{F}_{p^2} \to \mathcal{O}_{\mathbb{L}}/\mathfrak{B}$$

where $\mathbb{F}_{p^2}$ is the finite field of p^2 elements. The cardinality of $\mathcal{O}_{\mathbb{L}}/\mathfrak{B}$ is $p^{f_{\mathfrak{p}}}$, with $f_{\mathfrak{p}}$ equal to the order of $[\mathfrak{p}]$ in $C^+(\mathcal{O}_{\mathbb{K}})$. Is necessary to spend some words about $\mathbb{F}_{p^2}$. From a theoretical point of view, there is not a *canonical* finite field of p^2 elements. But our perspective is that of MAGMA (or another computer algebra system) so with $\mathbb{F}_{p^2}$ we denote the finite field of p^2 elements provided by MAGMA using the command "*GF*(*p*^2);".
The roots of $h_{\mathbb{K}}(x) \pmod p$ lie in $\mathbb{F}_{p^2}$. We consider the elliptic curve $\mathbb{E}(\mathbb{L} \mid j_0)$, where j_0 is a root of $h_{\mathbb{K}}(x)$. As before, we do not want to explicitly find the roots of $h_{\mathbb{K}}(x)$ and, consequently, the elliptic curve $\mathbb{E}(\mathbb{L} \mid j_0)$. We can use φ to find, the reduction of $\mathbb{E}$ modulo $\mathfrak{B}$, which is defined over the finite field of p^2 elements and denoted by $\overline{\mathbb{E}}$. The strategy is to take the equivalence classes in $\mathcal{O}_{\mathbb{L}}/\mathfrak{B}$ of the coefficients of $\mathbb{E}$ and their correspondent elements of $\mathbb{F}_{p^2}$. For example, given the coefficient $2j_0/(1728 - j_0)$, we have:

$$\left[\frac{2j_0}{1728 - j_0}\right]_{\mathfrak{B}} = \frac{[2]_{\mathfrak{B}}[j_0]_{\mathfrak{B}}}{[1728]_{\mathfrak{B}} - [j_0]_{\mathfrak{B}}} \tag{3.32}$$

Since φ is a field isomorphism, to compute $\varphi^{-1}([\frac{2j_0}{1728-j_0}]_{\mathfrak{B}})$ we only need to compute $\varphi^{-1}([j_0])_{\mathfrak{B}}$. In fact $\varphi^{-1}([2]_{\mathfrak{B}}) = 2$ and $\varphi^{-1}([1728]_{\mathfrak{B}}) = 1728$. Observe that $[j_0]_{\mathfrak{B}}$ is sent by φ^{-1}in a root $j_0' \in \mathbb{F}_{p^2}$ of $h_{\mathbb{K}}(x) \pmod p$ that we assume to know. So, the elliptic curve

$$\tilde{\mathbb{E}} : y^2 = x^3 + \frac{2j_0'}{1728 - j_0'} + \frac{3j_0'}{1728 - j_0'} \tag{3.33}$$

defined over $\mathbb{F}_{p^2}$ has the same number of rational points of the reduced curve $\overline{\mathbb{E}}$.
Using the Schoof algorithm we can find the number $N_{p^2} = p^2 + 1 - a_{p^2}$ of rational points of $\tilde{\mathbb{E}}$. From Theorem 3.5 it follows that:

$$a_{p^2} = \pi + \overline{\pi} = (u + \omega v) + (u + \overline{\omega} v) \tag{3.34}$$

and

$$p^2 = (u + \omega v)(u + \overline{\omega} v) \tag{3.35}$$

for some $\pi = u + \omega v \in \mathcal{O}_{\mathbb{K}}$, with $u, v \in \mathbb{Z}$. The last relation is a representation of p^2 by the principal form $Q_0(x, y)$. By Theorem 3.6, we know the formulas to obtain u and v once we know a_{p^2}.

Now, let $\langle a, b + \omega\rangle$ be a non-zero ideal of $\mathcal{O}_{\mathbb{K}}$ such that:

$$Q_1(x, y) = \frac{N_{\mathbb{K}/\mathbb{Q}}(ax + (b + \omega y)}{a} \tag{3.36}$$

To find two integers x_0, y_0 such that $Q_1(x_0, y_0) = p$ we impose

$$u + \omega v = \frac{(ax + (b + \omega)y)^2}{\pi_a}$$

where $\langle \pi_a\rangle = \langle a, b + \omega\rangle^2$ and $\pi_a\overline{\pi_a} = a^2$. From the independence of 1 and ω over $\mathbb{Q}$ we can deduce the Diophantine systems. Since (u, v) is not uniquely determined, we have to try all its four possible values $\pm(u_1, v_1), \pm(u_2, v_2)$ until we find x_0 and y_0. This systems have two homogeneous equations of degree two in x and y. Apart from u and v, these systems do not depend on p. So they could be computed once for each of the imaginary quadratic fields of class number 2. In the following two examples, we will see how to proceed to determine the Diophantine systems.

Example. *Consider the quadratic field $\mathbb{K} = \mathbb{Q}(\sqrt{-35})$ of discriminant $\Delta = -35$. The ideal $I = \langle 3, \omega\rangle$ of $\mathcal{O}_{\mathbb{K}}$ corresponds to the reduced form $Q_1(x, y) = 3x^2 + xy + 3y^2$:*

$$Q_1(x, y) = \frac{(3x + \omega y)(3x + \overline{\omega} y)}{3}$$

The square I^2 is generated by $9, 3\omega$ and ω^2, with:

$$\omega^2 = \left(\frac{1 + \sqrt{-35}}{2}\right)^2 = \omega - 9 \tag{3.37}$$

Now we can observe that:

$$\begin{gathered}\langle 9, 3\omega, \omega - 9\rangle = \langle 9, 3\omega, \omega - 9 + 9\rangle = \langle 9, 3\omega, \omega\rangle = \langle 9, 3\omega - 3\omega, \omega\rangle = \langle 9, \omega\rangle = \\ = \langle \omega - \omega^2, \omega\rangle = \langle \omega\rangle\langle 1 - \omega, 1\rangle = \langle \omega\rangle\end{gathered} \tag{3.38}$$

and hence $\pi_a = \omega$, with $\omega\overline{\omega} = 9$. So we have:

$$\begin{gathered}u + \omega v = \frac{\overline{\omega}(3x + \omega y)^2}{9} = \frac{\overline{\omega}(9x^2 + 6\omega xy + \omega^2 y^2)}{9} = \frac{(9\overline{\omega}x^2 + 6\overline{\omega}\omega xy + \omega\omega\overline{\omega}y^2)}{9} = \\ \frac{9\overline{\omega}x^2 + 54xy + 9\omega y^2}{9} = (1 - \omega)x^2 + 6xy + \omega y^2\end{gathered} \tag{3.39}$$

from which follow the Diophantine systems

$$\begin{cases} x^2 + 6xy = u \\ -x^2 + y^2 = v \end{cases} \tag{3.40}$$

Example. *Consider the quadratic field* $\mathbb{K} = \mathbb{Q}(\sqrt{-37})$ *of discriminant* $\Delta = -37$. *The ideal* $I = \langle 2, 1+\omega\rangle$ *of* $\mathcal{O}_{\mathbb{K}}$ *corresponds to the reduced form* $Q_1(x,y) = 2x^2 + 2xy + 19y^2$*:*

$$Q_1(x,y) = \frac{(2x + (1+\omega)y)(2x + (1+\overline{\omega}y)}{2}$$

The square I^2 *is generated by* $4, 2(1+\omega)$ *and* $1 + 2\omega + \omega^2$*, with:*

$$1 + 2\omega + \omega^2 = 1 + 2\sqrt{-37} - 37 = -36 + 2\omega \tag{3.41}$$

Now we can observe that:

$$\langle 4, 2(1+\omega), 2\omega - 36\rangle = \langle 2\rangle\langle 2, 1+\omega, \omega - 18\rangle = \langle 2\rangle\langle 2, 1+\omega, \omega - 18 + 18\rangle = \tag{3.42}$$

$$\langle 2\rangle\langle 2, 1+\omega, \omega\rangle = \langle 2\rangle\langle 2, 1+\omega-\omega, \omega\rangle = \langle 2\rangle\langle 2, 1, \omega\rangle = \langle 2\rangle$$

and hence $\pi_a = 2$. *So we have:*

$$u + \omega v = \frac{(2x + (1+\omega)y)^2}{2} = \frac{4x^2 + 4(1+\omega)xy + (1+2\omega+\omega^2)y^2}{2} = \tag{3.43}$$

$$= \frac{(4x^2 + 4xy + 4\omega xy + (2\omega - 36)y^2}{2} = 2x^2 + 2xy + 2\omega xy + \omega y^2 - 18y^2$$

from which follow the Diophantine systems

$$\begin{cases} 2x^2 + 2xy - 18y^2 = u \\ 2xy + y^2 = v \end{cases} \tag{3.44}$$

As we have seen in the examples, we have to play with the generators of $\langle a, b+\omega\rangle^2$ to write the square of $\langle a, b+\omega\rangle$ as a principal ideal $\langle \pi_a\rangle$. The observations that one has to take into consideration are:

- the product of two finitely generated ideals is finitely generated. In particular, given $\langle\alpha,\beta\rangle$ and $\langle\gamma\rangle$ ideals of $\mathcal{O}_{\mathbb{K}}$, we have:

$$\langle\gamma\rangle\langle\alpha,\beta\rangle = \langle\gamma\alpha, \gamma\beta\rangle \tag{3.45}$$

$$\langle\alpha,\beta\rangle\langle\alpha,\beta\rangle = \langle\alpha^2, \alpha\beta, \beta^2\rangle \tag{3.46}$$

- a repeated generator may be erased;

- if an ideal of $\mathcal{O}_{\mathbb{K}}$ contains 1, then it is equal to all the ring $\mathcal{O}_{\mathbb{K}}$;

- if two generators of an ideal of $\mathcal{O}_{\mathbb{K}}$ are relatively prime integers, then the ideal contains 1 for the Bézout's identity;

- if $\langle\alpha_1, \dots, \alpha_n\rangle$ is an ideal of $\mathcal{O}_{\mathbb{K}}$, then

$$\langle\alpha_1, \dots, \alpha_n\rangle = \langle\alpha_1, \dots, \alpha_{i-1}, \alpha_i - \eta\alpha_j, \alpha_{i+1}, \dots, \alpha_n\rangle \tag{3.47}$$

  for every element η of $\mathcal{O}_{\mathbb{K}}$.

To lower the computational complexity necessary to compute a representation of p with our method, we can construct a database with the following data for each of the imaginary quadratic fields of class number 2:

- the discriminant Δ;
- the reduced forms $Q_0(x,y)$, $Q_1(x,y)$ of discriminant Δ;
- the ideals that correspond to $Q_0(x,y)$ and $Q_1(x,y)$ respectively;
- the generator of the square of the ideal that corresponds to $Q_1(x,y)$;
- the coefficients of the Hilbert class polynomial $h_{\mathbb{K}}(x) \in \mathbb{Z}[x]$;
- the Diophantine systems, with u and v unknown, to find a representation of p by the non-principal form.

This information are collected in the tables at the end of the chapter.

3.5.3 Algorithm for class number 2

The algorithm described in the previous two sections is here provided in MAGMA language. The input of the function "Database2" is the discriminant of one of the imaginary quadratic fields of class number 2. It returns the integral coefficients h_1, h_2 of the Hilbert class polynomial $x^2 + h_1 x + h_2 \in \mathbb{Z}[x]$ and the coefficients a,b,c of the principal form $Q_0(x,y)$ of discriminant Δ.
The function "Systems2" has the same input but returns the coefficients a, b, c of the non-principal form $Q_1(x,y)$ and the coefficients of the polynomials $e_1(x,y), e_2(x,y)$ of the Diophantine systems used to find a proper representation of a prime integer p by $Q_1(x,y)$. The third function, "ClassNumber2", takes the radicand d of one of the imaginary quadratic fields with class number 2 and a prime integer p such that $(\Delta/p) = 1$, where Δ is the discriminant of $\mathbb{K} = \mathbb{Q}(\sqrt{d})$. It calls the function "Database2" and constructs the polynomial $h_{\mathbb{K}} \pmod{p}$. If $h_{\mathbb{K}} \pmod{p}$ has only simple roots and they are all in $\mathbb{Z}_p$, the function computes one of its roots and provides the elliptic curve $\tilde{\mathbb{E}}$. Counting the rational points of $\tilde{\mathbb{E}}$, "ClassNumber2" returns two integers u, v such that $p = Q_0(u,v)$. On the other hand, if $h_{\mathbb{K}}$ (mod p) is irreducible in $\mathbb{Z}_p$ or with a root of multiplicity two in $\mathbb{Z}_p$, the function computes one of its roots (whose are contained in $\mathbb{F}_{p^2}$) and constructs the elliptic curve $\tilde{\mathbb{E}}$. As before, are found two integers u, v such that $Q_0(u,v) = p^2$. Finally, using the data obtained from "Systems2", the function build the Diophantine systems. The constant terms (u,v) could be equal to $\pm(u_1, v_1)$ or to $\pm(u_2, v_2)$, so we have to try all of them until $x_0, y_0 \in \mathbb{Z}$, such that $Q_1(x_0, y_0) = p$, are found. A solution (x_0, y_0) is returned.

```
// CLASS NUMBER: 2

function Database2 (dK)

   if (dK eq -20) then
      h1:=-1264000;
      h2:=-681472000;
      a:=1;   b:=0;   c:=5;
   elif (dK eq -24) then
      h1:=-4834944;
      h2:=14670139392;
      a:=1;   b:=0;   c:=6;
   elif (dK eq -40) then
      h1:=- 425692800;
      h2:=9103145472000;
      a:=1;   b:=0;   c:=10;
   elif (dK eq -52) then
      h1:=- 6896880000;
      h2:=- 567663552000000;
      a:=1;   b:=0;   c:=13;
   elif (dK eq -15) then
      h1:=191025;
      h2:=- 121287375;
      a:=1;   b:=1;   c:=4;
   elif (dK eq -88) then
      h1:=- 6294842640000;
      h2:=15798135578688000000;
      a:=1;   b:=0;   c:=22;
   elif (dK eq -35) then
      h1:=117964800;
      h2:=-134217728000;
      a:=1;   b:=1;   c:=9;
   elif (dK eq -148) then
      h1:=- 39660183801072000;
      h2:=- 7898242515936467904000000;
      a:=1;   b:=0;   c:=37;
   elif (dK eq -51) then
      h1:=5541101568;
      h2:=6262062317568;
      a:=1;   b:=1;   c:=13;
   elif (dK eq -232) then
      h1:=-604729957849891344000;
      h2:=14871070713157137145512000000000;
      a:=1;   b:=0;   c:=58;
   elif (dK eq -91) then
      h1:=10359073013760;
      h2:=-3845689020776448;
      a:=1;   b:=1;   c:=23;
   elif (dK eq -115) then
      h1:=427864611225600;
      h2:=130231327260672000;
      a:=1;   b:=1;   c:=29;
   elif (dK eq -123) then
      h1:=1354146840576000;
      h2:=148809594175488000000;
      a:=1;   b:=1;   c:=31;
   elif (dK eq -187) then
      h1:=4545336381788160000;
      h2:=- 3845689020776448000000;
      a:=1;   b:=1;   c:=47;
   elif (dK eq -235) then
      h1:=823177419449425920000;
      h2:=11946621170462723407872000;
      a:=1;   b:=1;   c:=59;
   elif (dK eq -267) then
      h1:=19683091854079488000000;
      h2:=531429662672621376897024000000;
      a:=1;   b:=1;   c:=67;
   elif (dK eq -403) then
      h1:=2452811389229331391979520000;
      h2:=- 108844203402491055833088000000;
      a:=1;   b:=1;   c:=101;
   elif (dK eq -427) then
      h1:=15611455512523783919812608000;
      h2:=155041756222618916546936832000000;
      a:=1;   b:=1;   c:=107;
   end if;

return h1,h2,a,b,c;
end function;

function Systems2 (dK)
   Z:=Integers();
   PZ<x,y>:=PolynomialRing(Z,2);
if (dK eq -20) then
   e1:=2*x^2+2*x*y-2*y^2;
   e2:=2*x*y+y^2;
   a:=Z!2;   b:=Z!2;   c:=Z!3;
elif (dK eq -24) then
   e1:=2*x^2-3*y^2;
   e2:=2*x*y;
   a:=Z!2;   b:=Z!0;   c:=Z!3;
elif (dK eq -40) then
   e1:=2*x^2-5*y^2;
   e2:=2*x*y;
   a:=Z!2;   b:=Z!0;   c:=Z!5;
elif (dK eq -52) then
   e1:=2*x^2+2*x*y-6*y^2 ;
   e2:=2*x*y+y^2 ;
   a:=Z!2;   b:=Z!2;   c:=Z!7;
elif (dK eq -15) then
   e1:=x^2+4*x*y ;
   e2:=-x^2+y^2 ;
   a:=Z!2;   b:=Z!1;   c:=Z!2;
elif (dK eq -88) then
   e1:=2*x^2-11*y^2 ;
   e2:=2*x*y ;
   a:=Z!2;   b:=Z!0;   c:=Z!11;
elif (dK eq -35) then
   e1:=x^2+6*x*y;
   e2:=-x^2+y^2 ;
   a:=Z!3;   b:=Z!1;   c:=Z!3;
elif (dK eq -148) then
```

```
   e1:=2*x^2+2*x*y-18*y^2 ;
   e2:=2*x*y+y^2;
   a:=Z!2;   b:=Z!2;   c:=Z!19;
elif (dK eq -51) then
   e1:=3*x^2+2*x*y-4*y^2 ;
   e2:=2*x*y+y^2 ;
   a:=Z!3;   b:=Z!3;   c:=Z!5;
elif (dK eq -232) then
   e1:=2*x^2-29*y^2 ;
   e2:=2*x*y;
   a:=Z!2;   b:=Z!0;   c:=Z!29;
elif (dK eq -91) then
   e1:=2*x^2+10*x*y+y^2;
   e2:=-x^2+y^2;
   a:=Z!5;   b:=Z!3;   c:=Z!5;
elif (dK eq -115) then
   e1:=5*x^2+4*x*y-5*y^2 ;
   e2:= 2*x*y+y^2;
   a:=Z!5;   b:=Z!5;   c:=Z!7;
elif (dK eq -123) then
   e1:=3*x^2+2*x*y-10*y^2 ;
   e2:=2*x*y+y^2;
   a:=Z!3;   b:=Z!3;   c:=Z!11;
elif (dK eq -187) then
   e1:=2*x^2+14*x*y+y^2 ;
   e2:=-x^2+y^2 ;
   a:=Z!7;   b:=Z!3;   c:=Z!7;
elif (dK eq -235) then
   e1:=5*x^2+4*x*y-11*y^2 ;
   e2:=2*x*y+y^2 ;
   a:=Z!5;   b:=Z!5;   c:=Z!13;
elif (dK eq -267) then
   e1:=3*x^2+2*x*y-22*y^2;
   e2:=2*x*y+y^2;
   a:=Z!3;   b:=Z!3;   c:=Z!23;
elif (dK eq -403) then
   e1:=5*x^2+22*x*y+4*y^2 ;
   e2:=-x^2+y^2 ;
   a:=Z!11;   b:=Z!9;   c:=Z!11;
elif (dK eq -427) then
   e1:=7*x^2+6*x*y-14*y^2;
   e2:=2*x*y+y^2;
   a:=Z!7;   b:=Z!7;   c:=Z!17;
 end if;

return e1,e2,a,b,c;
end function;


function ClassNumber2(d,p)

   if ((d mod 4) eq 1) then
      dK:=d;
   else
      dK:=4*d;
   end if;

   Zp:=GF( p);
   DK:=Zp!dK;
   // IsSquare(DK);
   h1,h2,a,b,c:=Database2(dK);
   PZp<x>:=PolynomialRing(Zp);
   hk:=x^2+(h1)*x+(h2);

   if (IsIrreducible(hk) eq false and IsSeparable(hk) eq true) then
      j0:=Roots(hk)[1][1];
      A:=(3*j0)/(1728-j0);
      B:=(2*j0)/(1728-j0);
      E:=EllipticCurve([A,B]);
      Np:=#E; // Schoof's algorithm
      ap:=p+1-Np;
      if ((dK mod 4) eq 1) then
         v:=Sqrt((4*p-ap^2)/-dK);
         u:=(ap-v)/2;
      else
         v:=Sqrt((4*p-ap^2)/-dK);
         u:=ap/2;
      end if;
      Z:=Integers();
      u:=Z!u; v:=Z!v;
   else
      Fp2:=GF(p^2);
      h1,h2,a,b,c:=Database2(dK);
      PFp2<z>:=PolynomialRing(Fp2);
      hk:=z^2+(h1)*z+(h2);
      j0:=Roots(hk)[1][1];
      A:=(3*j0)/(1728-j0);
      B:=(2*j0)/(1728-j0);
      E:=EllipticCurve([A,B]);
      Np2:=#E; //Schoof's algorithm
      ap2:=p^2+1-Np2;
      if ((dK mod 4) eq 1) then
         v1:=Sqrt((4*(p^2)-ap2^2)/-dK);
         v2:=-v1;
         u1:=(ap2-v1)/2;
         u2:=(ap2-v2)/2;
      else
         v1:=Sqrt((4*(p^2)-ap2^2)/-dK);
         v2:=-v1;
         u1:=ap2/2;
         u2:=u1;
      end if;
      UV:=[[u1,v1],[-u1,-v1],[u2,v2],[-u2,-v2]];
      sum:=0;
      for j in [1..4] do
         u:=UV[j][1];
         v:=UV[j][2];
         Z:=Integers();
         PZ<x,y>:=PolynomialRing(Z,2);
         e1,e2,a,b,c:=Systems2(dK);
         e1:=e1-Z!u;
         e2:=e2-Z!v;
         f:=Resultant(e1,e2,1);
         PZ<t>:=PolynomialRing(Z);
         ff:=UnivariatePolynomial(f);
         F:=Roots(ff);
         n:=#F;
         for i in [1..n] do
            v:=F[i][1];
            s:=Evaluate(e1,2,v);
            ss:=UnivariatePolynomial(s);
            U:=Roots(ss);
            m:=#U;
            for k in [1..m] do
               u:=U[k][1];
               sum:=a*u^2+b*u*v+c*v^2;
               if (sum eq p) then
                  u:=Z!u; v:=Z!v;
                  break j;
               end if;
            end for;
         end for;
      end for;
   end if;

return u,v,a,b,c;
end function;

d:=...;
p:=...;
x,y,a,b,c:=ClassNumber2(d,p);
if (b eq 0) then
   printf "%o=%o(%o)^2+%o(%o)^2",p,a,x,c,y;
else
   printf "%o=%o(%o)^2+%o(%o)+%o(%o)^2",p,a,x,b,x*y,c,y;
end if;
```

3.6 Class number 3

The only imaginary quadratic fields $\mathbb{Q}(\sqrt{d})$ which have class number 3 are those with $-d$ in the following set [54]:

$$\mathcal{D}_3 = \{23, 31, 59, 83, 107, 139, 211, 283, 307, 331, 379, 499, 547, 643, 883, 907\} \qquad (3.48)$$

Let $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ be one of these fields and let Δ be its discriminant. Given an odd prime integer p such that $(\Delta/p) = 1$, it is properly represented by the principal quadratic form $Q_0(x, y)$ or by the other reduced forms, $Q_1(x, y)$ and $Q_2(x, y)$. In fact $[Q_1(x, y)], [Q_2(x, y)]$ are not the unit in the multiplicative group of three elements $C(\Delta)$, hence $Q_1(x, y)$, $Q_2(x, y)$ are improperly equivalent because $[Q_1(x, y)]^{-1} = [Q_2(x, y)]$. In particular, if $Q_1(x, y) = (a, b, c)$ then $Q_2(x, y) = (a, -b, c)$. In this section we will discuss about the structure of the explicit algorithm, deduced from Theorem 3.6, to find a proper representation of p. The complete algorithm will be provided, in MAGMA language, at the end of the section.
The Hilbert class field $\mathbb{L}$ of $\mathbb{K}$ has dimension $h_{\mathbb{K}} = 3$ over $\mathbb{K}$ and the Hilbert class polynomial

$h_{\mathbb{K}}(x)$ has degree 3 and integral coefficients. The ideal $p\mathcal{O}_{\mathbb{K}}$ factorizes as the product $\mathfrak{p}\overline{\mathfrak{p}}$, where $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ are prime ideals of $\mathcal{O}_{\mathbb{K}}$ containing p and such that $\mathfrak{p} \neq \overline{\mathfrak{p}}$. We denote by $\mathfrak{B}$ one of the prime ideals of $\mathcal{O}_{\mathbb{L}}$ containing $\mathfrak{p}$. By Theorem 3.7, p is properly represented by $Q_0(x, y)$ if and only if the polynomial $h_{\mathbb{K}}(x) \pmod{p}$ has only simple roots and they are all in $\mathbb{Z}_p$.

3.6.1 p represented by $Q_0(x, y)$

Suppose that the prime integer p is represented by the principal form $Q_0(x, y)$. Then $\mathfrak{p}$ is principal and $|\mathcal{O}_{\mathbb{L}}/\mathfrak{B}| = p$. The map

$$\begin{array}{rccc} \varphi : & \mathbb{Z}/<p> & \to & \mathcal{O}_{\mathbb{L}}/\mathfrak{B} \\ & [\ell]_p & \mapsto & [\ell]_{\mathfrak{B}} \end{array}$$

is a field isomorphism. It is a field homomorphism, hence injective, and also surjective because domain and codomain have the same finite cardinality. We consider the elliptic curve $\mathbb{E}(\mathbb{L} \mid j_0)$, where j_0 is a root of $h_{\mathbb{K}}(x)$. It is not easy to explicitly compute the roots of $h_{\mathbb{K}}(x)$ and, consequently, the elliptic curve $\mathbb{E}(\mathbb{L} \mid j_0)$. We can use φ to find directly the reduction of $\mathbb{E}$ modulo $\mathfrak{B}$, which is defined over the finite field of p elements and denoted by $\overline{\mathbb{E}}$. The idea is to consider the equivalence classes in $\mathcal{O}_{\mathbb{L}}/\mathfrak{B}$ of the coefficients of $\mathbb{E}$ and their correspondent elements in $\mathbb{Z}_p$. For example, given the coefficient $2j_0/(1728 - j_0)$, we have:

$$\left[\frac{2j_0}{1728 - j_0}\right]_{\mathfrak{B}} = \frac{[2]_{\mathfrak{B}}[j_0]_{\mathfrak{B}}}{[1728]_{\mathfrak{B}} - [j_0]_{\mathfrak{B}}} \tag{3.49}$$

Since φ is an isomorphism, to compute $\varphi^{-1}([\frac{2j_0}{1728-j_0}]_{\mathfrak{B}})$, we need only to determine $\varphi^{-1}([j_0])_{\mathfrak{B}}$. We assume to know an integer j_0' such that $[j_0']_p$ is a root of $h_{\mathbb{K}}(x) \pmod{p}$: the equivalence class $[j_0']_{\mathfrak{B}}$ is a root of $h_{\mathbb{K}}(x) \pmod{\mathfrak{B}}$. Since $h_{\mathbb{K}}(x) \pmod{\mathfrak{B}}$ has at most two roots in $\mathcal{O}_{\mathbb{L}}/\mathfrak{B}$, j_0' is equivalent, modulo $\mathfrak{B}$, to one of the roots of $h_{\mathbb{K}}(x)$. It is important to remark that to construct $\mathbb{E}$ we can consider, equivalently, one of the roots of $h_{\mathbb{K}}(x)$. Then the elliptic curve

$$\tilde{\mathbb{E}} : y^2 = x^3 + \frac{[2]_p[j_0']_p}{[1728]_p - [j_0']_p}x + \frac{[3]_p[j_0']_p}{[1728]_p - [j_0']_p} \tag{3.50}$$

defined over $\mathbb{Z}_p$ has the same number of rational points of the reduced curve $\overline{\mathbb{E}}$.
Using the Schoof algorithm (see [50] or next chapter) we can find the number $N_p = p+1-a_p$ of rational points of $\tilde{\mathbb{E}}$. From Theorem 3.5 it follows that:

$$a_p = \pi + \overline{\pi} = (u + \omega v) + (u + \overline{\omega} v) \tag{3.51}$$

and

$$p = (u + \omega v)(u + \overline{\omega} v) \tag{3.52}$$

for some $\pi = u + \omega v \in \mathcal{O}_{\mathbb{K}}$, with u and v integers. The last relation is a representation of p by the principal form $Q_0(u, v)$. By Theorem 3.6, we know the formulas to obtain u and v once we know a_p.

3.6.2 p represented by $Q_1(x, y)$

Now suppose that $h_{\mathbb{K}}(x) \pmod p$ does not split in $\mathbb{Z}_p$ or that its roots are not simple. Hence, p is properly represented by the reduced non-principal form $Q_1(x, y)$. This implies that p^3 is represented by the principal form $Q_0(x, y)$ since $\mathfrak{p}$ is not principal and $[\mathfrak{p}]$ has order 3 in $C^+(\mathcal{O}_{\mathbb{K}})$. To find this representation of p^3 we use Theorem 3.5. The only difference with the previous case is that there exists an isomorphism of fields

$$\varphi : \mathbb{F}_{p^3} \to \mathcal{O}_{\mathbb{L}}/\mathfrak{B}$$

Is necessary to spend some words about $\mathbb{F}_{p^3}$. From a theoretical point of view, there is not a *canonical* finite field of p^3 elements. But our perspective is that of MAGMA (or another computer algebra system) so with $\mathbb{F}_{p^3}$ we denote the finite field of p^3 elements provided by MAGMA using the command "$GF(p$^$3);$".
We consider the elliptic curve $\mathbb{E}(\mathbb{L} \mid j_0)$, where j_0 is a root of $h_{\mathbb{K}}(x)$. As before, we do not want to explicitly find the roots of $h_{\mathbb{K}}(x)$ and, consequently, the elliptic curve $\mathbb{E}(\mathbb{L} \mid j_0)$. We can use φ to find the reduction of $\mathbb{E}$ modulo $\mathfrak{B}$, which is defined over the finite field of p^3 elements and denoted by $\overline{\mathbb{E}}$. Our strategy is to take the equivalence classes in $\mathcal{O}_{\mathbb{L}}/\mathfrak{B}$ of the coefficients of $\mathbb{E}$ and their correspondent elements of $\mathbb{F}_{p^3}$. For example, given the coefficient $2j_0/(1728 - j_0)$, we have:

$$\left[\frac{2j_0}{1728 - j_0}\right]_{\mathfrak{B}} = \frac{[2]_{\mathfrak{B}}[j_0]_{\mathfrak{B}}}{[1728]_{\mathfrak{B}} - [j_0]_{\mathfrak{B}}} \tag{3.53}$$

Since φ is a field isomorphism, to compute $\varphi^{-1}([\frac{2j_0}{1728-j_0}]_{\mathfrak{B}})$ we only need to compute $\varphi^{-1}([j_0])_{\mathfrak{B}}$. In fact $\varphi^{-1}([2]_{\mathfrak{B}}) = 2$ and $\varphi^{-1}([1728]_{\mathfrak{B}}) = 1728$. Observe that $[j_0]_{\mathfrak{B}}$ is sent by φ^{-1} in a root $j_0' \in \mathbb{F}_{p^3}$ of $h_{\mathbb{K}}(x) \pmod p$ that we assume to know. So, the elliptic curve

$$\tilde{\mathbb{E}} : y^2 = x^3 + \frac{2j_0'}{1728 - j_0'} + \frac{3j_0'}{1728 - j_0'} \tag{3.54}$$

defined over $\mathbb{F}_{p^3}$ has the same number of rational points of the reduced curve $\overline{\mathbb{E}}$.
Using the Schoof algorithm we can find the number $N_{p^3} = p^3 + 1 - a_{p^3}$ of rational points of $\tilde{\mathbb{E}}$. From Theorem 3.5 it follows that:

$$a_{p^3} = \pi + \overline{\pi} = (u + \omega v) + (u + \overline{\omega} v) \tag{3.55}$$

and

$$p^3 = (u + \omega v)(u + \overline{\omega} v) \tag{3.56}$$

for some $\pi = u + \omega v \in \mathcal{O}_{\mathbb{K}}$, with $u, v \in \mathbb{Z}$. The last relation is a representation of p^3 by the principal form $Q_0(x, y)$. By Theorem 3.6, we know the formulas to obtain u and v once we know a_{p^3}.
Now, let $\langle a, b + \omega \rangle$ be a non-zero ideal of $\mathcal{O}_{\mathbb{K}}$ such that:

$$Q_1(x, y) = \frac{N_{\mathbb{K}/\mathbb{Q}}(ax + (b + \omega y)}{a} \tag{3.57}$$

Imposing

$$\pi = u + \omega v = \frac{(ax + (b+\omega)y)^3}{\pi_a}$$

where $\langle \pi_a \rangle = \langle a, b+\omega \rangle^3$ and $\pi_a \overline{\pi_a} = a^3$, we can deduce a Diophantine system from the independence of 1 and ω over $\mathbb{Q}$. This system has two homogeneous equations of degree 3 in x and y and one of its solution (x_0, y_0) is such that $Q_1(x_0, y_0) = p$. Actually, since (u, v) is not uniquely determined, we have four Diophantine systems and not only one. Apart from u and v, these systems do not depend on p. So they could be computed once for all for each of the imaginary quadratic fields of class number 3. In the following example we show how to proceed to determine the Diophantine systems using MAGMA.

Example. *It is possible to work with quadratic fields in* MAGMA. *If $d \neq 1$ is a squarefree integer, the quadratic field $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ could be defined by the command:*

```
K<d>:=QuadraticField(d);
```

while its ring of integers $\mathcal{O}_{\mathbb{K}}$ can be created writing

```
OK<w>:=MaximalOrder(K);
```

In the ring $\mathcal{O}_{\mathbb{K}}$ we are able to introduce the ideal $\langle a, b+\omega \rangle$:

```
I:=ideal <OK| a,b+w>;
```

Furthermore, from

```
ris,pa:=IsPrincipal(I*I*I);
```

we obtain, in the second output pa, the generator π_a of the principal ideal $\langle a, b+\omega \rangle^3$. Now, we define the polynomial $(ax + (b+\omega)y)^3 \in \mathcal{O}_{\mathbb{K}}[x, y]$ and we multiply it by the conjugate of π_a:

```
R<x,y>:=PolynomialRing(OK,2);
e1+we2:=Conjugate(pa)*((7*x+w*y)^3);
```

In this way, we obtain $N_{\mathbb{K}/\mathbb{Q}}(\pi_a)(e_1(x, y) + \omega e_2(x, y))$ and it remains to divide by the norm of π_a, that could be computed writing:

```
a:=Norm(pa);
```

Obviously, one can compute by hand the Diophantine systems, playing with the generators of $\langle a, b+\omega \rangle^3$ and using the rules recalled in Section 3.5.2.

To lower the computational complexity necessary to compute a representation of p with the described method, we can construct a database with the following data for each of the imaginary quadratic fields of class number 3:

- the discriminant Δ;

- the reduced forms $Q_0(x,y)$, $Q_1(x,y)$ of discriminant Δ;
- the ideals of $\mathcal{O}_{\mathbb{K}}$ that correspond to $Q_0(x,y)$ and $Q_1(x,y)$ respectively;
- the coefficients of the Hilbert class polynomial $h_{\mathbb{K}}(x) \in \mathbb{Z}[x]$;
- the generator of the third power of the ideal that corresponds to $Q_1(x,y)$;
- the Diophantine systems, with u and v unknown, to find a representation of p by the non-principal form.

This information are collected in the tables attached at the end of the chapter.

3.6.3 Algorithm for class number 3

The algorithm described in the previous two sections is here provided in MAGMA language. The input of the function "Database3" is the discriminant of one of the imaginary quadratic fields of class number 3. It returns the integral coefficients h_1, h_2, h_3 of the Hilbert class polynomial $x^3 + h_1x^2 + h_2x + h_3 \in \mathbb{Z}[x]$ and the coefficients a,b,c of the principal form of discriminant Δ.
The function "Systems3" has the same input but returns the coefficients a, b, c of the non-principal form $Q_1(x,y)$ and the coefficients of the polynomials $e_1(x,y), e_2(x,y)$ of the Diophantine systems used to find a proper representation of a prime integer p by $Q_1(x,y)$. The third function, "ClassNumber3", takes the radicand d of one of the imaginary quadratic fields with class number 3 and a prime integer p such that $(\Delta/p) = 1$, where Δ is the discriminant of $\mathbb{K} = \mathbb{Q}(\sqrt{d})$. It calls the function "Database3" and constructs the polynomial $h_{\mathbb{K}} \pmod p$. If $h_{\mathbb{K}} \pmod p$ has only simple roots and they are all in $\mathbb{Z}_p$, the function computes one of its roots and provides the elliptic curve $\tilde{\mathbb{E}}$. Counting the rational points of $\tilde{\mathbb{E}}$, "ClassNumber3" returns two integers u, v such that $p = Q_0(u,v)$. On the other hand, if $h_{\mathbb{K}} \pmod p$ does not split in $\mathbb{Z}_p$ or it is not separable, the function computes one of its roots (whose are contained in $\mathbb{F}_{p^3}$) and constructs the elliptic curve $\tilde{\mathbb{E}}$. As before, are found two integers u, v such that $Q_0(u,v) = p^3$. Finally, using the data obtained from "Systems3", the function build the Diophantine systems. The constant terms (u,v) could be equal to $\pm(u_1, v_1)$ or to $(\pm(u_2, v_2)$, so we have to try all of them until $x_0, y_0 \in \mathbb{Z}$ such that $Q_1(x_0, y_0) = p$ are found. A solution (x_0, y_0) is returned.

```
// CLASS NUMBER: 3

function Database3 (dK)

   if (dK eq -23) then
      h1:=3491750;
      h2:=-5151296875;
      h3:=12771880859375;
      a:=1;   b:=1;   c:=6;
```

```
  elif (dK eq -31) then
     h1:=39491307;
     h2:=-58682638134;
     h3:=1566028350940383;
     a:=1;   b:=1;   c:=8;
  elif (dK eq -59) then
     h1:=30197678080;
     h2:=- 140811576541184;
     h3:=374643194001883136;
     a:=1;   b:=1;   c:=15;
  elif (dK eq -83) then
     h1:=2691907584000;
     h2:=- 41490055168000000;
     h3:=549755813888000000000;
     a:=1;   b:=1;   c:=21;
  elif (dK eq -107) then
     h1:=129783279616000;
     h2:=- 6764523159552000000;
     h3:=337618789203968000000000;
     a:=1;   b:=1;   c:=27;
  elif (dK eq -139) then
     h1:=12183160834031616;
     h2:=- 53041786755137667072;
     h3:=67408489017571610198016;
     a:=1;   b:=1;   c:=35;
  elif (dK eq -211) then
     h1:=6587358728863009968;
     h2:=277390576406111100862464;
     h3:=5310823021408898698117644288;
     a:=1;   b:=1;   c:=53;
  elif (dK eq -283) then
     h1:=89611323386832801792000;
     h2:=90839236535446929408000000;
     h3:=201371843156955365376000000000;
     a:=1;   b:=1;   c:=71;
  elif (dK eq -307) then
     h1:=805016812009981390848000;
     h2:=- 5083646425734146162688000000;
     h3:=8987619631060626702336000000000;
     a:=1;   b:=1;   c:=77;
  elif (dK eq -331) then
     h1:=6647404730173793386463232;
     h2:=368729929041040103875232661504;
     h3:=56176242840389398230218488594563072;
     a:=1;   b:=1;   c:=83;
  elif (dK eq -379) then
     h1:=364395404104624239018246144;
     h2:=-121567791009880876719538528321536;
     h3:=15443600047689011948024601807415148544;
     a:=1;   b:=1;   c:=95;
  elif (dK eq -499) then
     h1:=300510110807102620070672596992O;
     h2:=-6063717825494266394722392560011051008;
     h3:=4671133182399954782798673154437441310949376;
     a:=1;   b:=1;   c:=125;
  elif (dK eq -547) then
     h1:=812973955396316547216374784OOOOO;
```

```
      h2:=-1397123284317878279434697441280000000;
      h3:=83303937570678403968635240448000000000;
      a:=1;   b:=1;   c:=137;
   elif (dK eq -643) then
      h1:=39545575162726134099492467011584000;
      h2:=-63003785050472478764996517974507520000000;
      h3:=308052554652302847380880841299197952000000000;
      a:=1;   b:=1;   c:=161;
   elif (dK eq -883) then
      h1:=349039343410118190392242950119333928960000;
      h2:=-1519601111252452820338756195291244789760000000;
      h3:=16799028538162731818757552080012338790400000000000;
      a:=1;   b:=1;   c:=221;
   elif (dK eq -907) then
      h1:=123072080721198402394477590506838687744000;
      h2:=3918159420801481961756581157537631436800000000;
      h3:=14916127474652484132854589496927400755200000000000;
      a:=1;   b:=1;   c:=227;
   end if;

return h1,h2,h3,a,b,c;
end function;

function Systems3 (dK)
   Z:=Integers();
   PZ<x,y>:=PolynomialRing(Z,2);
if (dK eq -23) then
   e1:=x^3-9*x^2*y-9*x*y^2+3*y^3;
   e2:=x^3+3*x^2*y-3*x*y^2-2*y^3;
   a:=Z!2;   b:=Z!1;   c:=Z!3;
elif (dK eq -31) then
   e1:=-12*x^2*y-18*x*y^2+y^3;
   e2:=x^3+3*x^2*y-3*x*y^2-4*y^3;
   a:=Z!2;   b:=Z!1;   c:=Z!4;
elif (dK eq -59) then
   e1:=-4*x^3-15*x^2*y+15*x*y^2+10*y^3;
   e2:=x^3-3*x^2*y-6*x*y^2+y^3;
   a:=Z!3;   b:=Z!1;   c:=Z!5;
elif (dK eq -83) then
   e1:=2*x^3-21*x^2*y-21*x*y^2+14*y^3;
   e2:=x^3+3*x^2*y-6*x*y^2-3*y^3;
   a:=Z!3;   b:=Z!1;   c:=Z!7;
elif (dK eq -107) then
   e1:=-x^3-27*x^2*y+27*y^3;
   e2:=x^3-9*x*y^2-y^3;
   a:=Z!3;   b:=Z!1;   c:=Z!9;
elif (dK eq -139) then
   e1:=9*x^3-21*x^2*y-42*x*y^2+7*y^3;
   e2:=x^3+6*x^2*y-3*x*y^2-3*y^3;
   a:=Z!5;   b:=Z!1;   c:=Z!7;
elif (dK eq -211) then
   e1:=8*x^3-27*x^2*y-69*x*y^2+6*y^3;
   e2:=x^3+6*x^2*y-3*x*y^2-5*y^3;
   a:=Z!5;   b:=Z!3;   c:=Z!11;
elif (dK eq -283) then
   e1:=-17*x^3-45*x^2*y+48*x*y^2+35*y^3;
   e2:=x^3-6*x^2*y-9*x*y^2+y^3;
   a:=Z!7;   b:=Z!5;   c:=Z!11;
elif (dK eq -307) then
   e1:=5*x^3-66*x^2*y-33*x*y^2+33*y^3;
   e2:=2*x^3+3*x^2*y-9*x*y^2-2*y^3;
   a:=Z!7;   b:=Z!1;   c:=Z!11;
elif (dK eq -331) then
   e1:=-7*x^3-54*x^2*y+39*x*y^2+69*y^3;
   e2:=x^3-3*x^2*y-12*x*y^2+y^3;
   a:=Z!5;   b:=Z!3;   c:=Z!17;
elif (dK eq -379) then
   e1:=-6*x^3-57*x^2*y+57*x*y^2+76*y^3;
   e2:=x^3-3*x^2*y-12*x*y^2-3*y^3;
   a:=Z!5;   b:=Z!1;   c:=Z!19;
elif (dK eq -499) then
   e1:=-x^3-75*x^2*y+125*y^3;
   e2:=x^3-15*x*y^2-y^3;
   a:=Z!5;   b:=Z!1;   c:=Z!25;
elif (dK eq -547) then
   e1:=-27*x^3-60*x^2*y-123*x*y^2+5*y^3;
   e2:=2*x^3+9*x^2*y-3*x*y^2-4*y^3;
   a:=Z!11;   b:=Z!5;   c:=Z!13;
elif (dK eq -643) then
   e1:=13*x^3-69*x^2*y-138*x*y^2+69*y^3;
   e2:=x^3+6*x^2*y-9*x*y^2-7*y^3;
   a:=Z!7;   b:=Z!1;   c:=Z!23;
elif (dK eq -883) then
   e1:=16*x^3+153*x^2*y-51*x*y^2-68*y^3;
   e2:=-3*x^3+3*x^2*y+12*x*y^2-y^3;
   a:=Z!13;   b:=Z!1;   c:=Z!17;
elif (dK eq -907) then
   e1:=-11*x^3+147*x^2*y+150*x*y^2-37*y^3;
   e2:=-3*x^3-6*x^2*y+9*x*y^2+5*y^3;
   a:=Z!13;   b:=Z!9;   c:=Z!19;
end if;

return e1,e2,a,b,c;
end function;


function ClassNumber3(d,p)

   if ((d mod 4) eq 1) then
      dK:=d;
   else
      dK:=4*d;
   end if;

   Zp:=GF( p);
   DK:=Zp!dK;
   // IsSquare(DK);
   h1,h2,h3,a,b,c:=Database3(dK);
   PZp<x>:=PolynomialRing(Zp);
   hk:=x^3+(h1)*x^2+(h2)*x+(h3);

   if (SplittingField(hk) eq Zp and IsSeparable(hk) eq true) then
      j0:=Roots(hk)[1][1];
      A:=(3*j0)/(1728-j0);
      B:=(2*j0)/(1728-j0);
      E:=EllipticCurve([A,B]);
      Np:=#E; // Schoof's algorithm
      ap:=p+1-Np;
      if ((dK mod 4) eq 1) then
         v:=Sqrt((4*p-ap^2)/-dK);
         u:=(ap-v)/2;
      else
         v:=Sqrt((4*p-ap^2)/-dK);
         u:=ap/2;
      end if;
      Z:=Integers();
      u:=Z!u; v:=Z!v;
   else
      Fp3:=GF(p^3);
      h1,h2,h3,a,b,c:=Database3(dK);
      PFp3<z>:=PolynomialRing(Fp3);
      hk:=z^3+(h1)*z^2+(h2)*z+(h3);
      j0:=Roots(hk)[1][1];
      A:=(3*j0)/(1728-j0);
      B:=(2*j0)/(1728-j0);
      E:=EllipticCurve([A,B]);
      Np3:=#E; //Schoof's algorithm
      ap3:=p^3+1-Np3;
      if ((dK mod 4) eq 1) then
         v1:=Sqrt((4*(p^3)-ap3^2)/-dK);
         v2:=-v1;
         u1:=(ap3-v1)/2;
         u2:=(ap3-v2)/2;
      else
         v1:=Sqrt((4*(p^3)-ap3^2)/-dK);
         v2:=-v1;
         u1:=ap3/2;
         u2:=u1;
      end if;
      UV:=[[u1,v1],[-u1,-v1],[u2,v2],[-u2,-v2]];
      sum:=0;
      for j in [1..4] do
         u:=UV[j][1];
         v:=UV[j][2];
         Z:=Integers();
         PZ<x,y>:=PolynomialRing(Z,2);
         e1,e2,a,b,c:=Systems3(dK);
         e1:=e1-Z!u;
         e2:=e2-Z!v;
         f:=Resultant(e1,e2,1);
         PZ<t>:=PolynomialRing(Z);
         ff:=UnivariatePolynomial(f);
         F:=Roots(ff);
         n:=#F;
         for i in [1..n] do
            v:=F[i][1];
            s:=Evaluate(e1,2,v);
            ss:=UnivariatePolynomial(s);
            U:=Roots(ss);
            m:=#U;
            for k in [1..m] do
```

```
               u:=U[k][1];
               sum:=a*u^2+b*u*v+c*v^2;
               if (sum eq p) then
                  u:=Z!u; v:=Z!v;
                  break j;
               end if;
            end for;
         end for;
      end for;
   end if;

return u,v,a,b,c;
end function;

d:=...;
p:=...;
x,y,a,b,c:=ClassNumber3(d,p);
if (b eq 0) then
   printf "%o=%o(%o)^2+%o(%o)^2",p,a,x,c,y;
else
   printf "%o=%o(%o)^2+%o(%o)+%o(%o)^2",p,a,x,b,x*y,c,y;
end if;
```

d	Δ	ω	Q_i	Ideals	$h_{\mathbb{K}}(x)$
-5	-20	$\sqrt{-5}$	x^2+5y^2 $2x^2+2xy+3y^2$	$\langle 1,\omega\rangle$ $\langle 2,1+\omega\rangle$	$x^2-1264000x-$ -681472000
-6	-24	$\sqrt{-6}$	x^2+6y^2 $2x^2+3y^2$	$\langle 1,\omega\rangle$ $\langle 2,\omega\rangle$	$x^2-4834944x+$ $+14670139392$
-10	-40	$\sqrt{-10}$	x^2+10y^2 $2x^2+5y^2$	$\langle 1,\omega\rangle$ $\langle 2,\omega\rangle$	$x^2-425692800x+$ $+9103145472000$
-13	-52	$\sqrt{-13}$	x^2+13y^2 $2x^2+2xy+7y^2$	$\langle 1,\omega\rangle$ $\langle 2,1+\omega\rangle$	$x^2-6896880000x-$ -567663552000000
-15	-15	$\frac{1+\sqrt{-15}}{2}$	$x^2+xy+4y^2$ $2x^2+xy+2y^2$	$\langle 1,\omega\rangle$ $\langle 2,\omega\rangle$	$x^2+191025x-$ -121287375
-22	-88	$\sqrt{-22}$	x^2+22y^2 $2x^2+11y^2$	$\langle 1,\omega\rangle$ $\langle 2,\omega\rangle$	$x^2-6294842640000x+$ $+15798135578688000000$
-35	-35	$\frac{1+\sqrt{-35}}{2}$	$x^2+xy+9y^2$ $3x^2+xy+3y^2$	$\langle 1,\omega\rangle$ $\langle 3,\omega\rangle$	$x^2+117964800x-$ -134217728000
-37	-148	$\sqrt{-37}$	x^2+37y^2 $2x^2+2xy+19y^2$	$\langle 1,\omega\rangle$ $\langle 2,1+\omega\rangle$	$x^2-39660183801072000x-$ $-7898242515936467904000000$
-51	-51	$\frac{1+\sqrt{-51}}{2}$	$x^2+xy+13y^2$ $3x^2+3xy+5y^2$	$\langle 1,\omega\rangle$ $\langle 3,1+\omega\rangle$	$x^2+5541101568x+$ $+6262062317568$
-58	-232	$\sqrt{-58}$	x^2+58y^2 $2x^2+29y^2$	$\langle 1,\omega\rangle$ $\langle 2,\omega\rangle$	$x^2-604729957849891344000x+$ $+14871070713157137145512000000000$
-91	-91	$\frac{1+\sqrt{-91}}{2}$	$x^2+xy+23y^2$ $5x^2+3xy+5y^2$	$\langle 1,\omega\rangle$ $\langle 5,1+\omega\rangle$	$x^2+10359073013760x-$ -3845689020776448
-115	-115	$\frac{1+\sqrt{-115}}{2}$	$x^2+xy+29y^2$ $5x^2+5xy+7y^2$	$\langle 1,\omega\rangle$ $\langle 5,2+\omega\rangle$	$x^2+427864611225600x+$ $+130231327260672000$
-123	-123	$\frac{1+\sqrt{-123}}{2}$	$x^2+xy+31y^2$ $3x^2+3xy+11y^2$	$\langle 1,\omega\rangle$ $\langle 3,1+\omega\rangle$	$x^2+1354146840576000x+$ $+148809594175488000000$
-187	-187	$\frac{1+\sqrt{-187}}{2}$	$x^2+xy+47y^2$ $7x^2+3xy+7y^2$	$\langle 1,\omega\rangle$ $\langle 7,1+\omega\rangle$	$x^2+4545336381788160000x-$ -3845689020776448000000
-235	-235	$\frac{1+\sqrt{-235}}{2}$	$x^2+xy+59y^2$ $5x^2+5xy+13y^2$	$\langle 1,\omega\rangle$ $\langle 5,2+\omega\rangle$	$x^2+823177419449425920000x+$ $+11946621170462723407872000$
-267	-267	$\frac{1+\sqrt{-267}}{2}$	$x^2+xy+67y^2$ $3x^2+3xy+23y^2$	$\langle 1,\omega\rangle$ $\langle 3,1+\omega\rangle$	$x^2+19683091854079488000000x+$ $+531429662672621376897024000000$
-403	-403	$\frac{1+\sqrt{-403}}{2}$	$x^2+xy+101y^2$ $11x^2+9xy+11y^2$	$\langle 1,\omega\rangle$ $\langle 11,4+\omega\rangle$	$x^2+2452811389229331391979520000x-$ $-108844203402491055833088000000$
-427	-427	$\frac{1+\sqrt{-427}}{2}$	$x^2+xy+107y^2$ $7x^2+7xy+17y^2$	$\langle 1,\omega\rangle$ $\langle 7,3+\omega\rangle$	$x^2+15611455512523783919812608000x+$ $+155041756222618916546936832000000$

Table 3.2: Imaginary quadratic fields $\mathbb{K}=\mathbb{Q}(\sqrt{d})$ of class number 2

d	Δ	ω	π_a	Systems
-5	-20	$\sqrt{-5}$	2	$2x^2+2xy-2y^2=u$ $2xy+y^2=v$
-6	-24	$\sqrt{-6}$	2	$2x^2-3y^2=u$ $2xy=v$
-10	-40	$\sqrt{-10}$	2	$2x^2-5y^2=u$ $2xy=v$
-13	-52	$\sqrt{-13}$	2	$2x^2+2xy-6y^2=u$ $2xy+y^2=v$
-15	-15	$\frac{1+\sqrt{-15}}{2}$	ω	$x^2+4xy=u$ $-x^2+y^2=v$
-22	-88	$\sqrt{-22}$	2	$2x^2-11y^2=u$ $2xy=v$
-35	-35	$\frac{1+\sqrt{-35}}{2}$	ω	$x^2+6xy=u$ $-x^2+y^2=v$
-37	-148	$\sqrt{-37}$	2	$2x^2+2xy-18y^2=u$ $2xy+y^2=v$
-51	-51	$\frac{1+\sqrt{-51}}{2}$	3	$3x^2+2xy-4y^2=u$ $2xy+y^2=v$
-58	-232	$\sqrt{-58}$	2	$2x^2-29y^2=u$ $2xy=v$
-91	-91	$\frac{1+\sqrt{-91}}{2}$	$1+\omega$	$2x^2+10xy+y^2=u$ $-x^2+y^2=v$
-115	-115	$\frac{1+\sqrt{-115}}{2}$	5	$5x^2+4xy-5y^2=u$ $2xy+y^2=v$
-123	-123	$\frac{1+\sqrt{-123}}{2}$	3	$3x^2+2xy-10y^2=u$ $2xy+y^2=v$
-187	-187	$\frac{1+\sqrt{-187}}{2}$	$1+\omega$	$2x^2+14xy+y^2=u$ $-x^2+y^2=v$
-235	-235	$\frac{1+\sqrt{-235}}{2}$	5	$5x^2+4xy-11y^2=u$ $2xy+y^2=v$
-267	-267	$\frac{1+\sqrt{-267}}{2}$	3	$3x^2+2xy-22y^2=u$ $2xy+y^2=v$
-403	-403	$\frac{1+\sqrt{-403}}{2}$	$4+\omega$	$5x^2+22xy+4y^2=u$ $-x^2+y^2=v$
-427	-427	$\frac{1+\sqrt{-427}}{2}$	7	$7x^2+6xy-14y^2=u$ $2xy+y^2=v$

Table 3.3: Imaginary quadratic fields $\mathbb{K}=\mathbb{Q}(\sqrt{d})$ of class number 2

d	Δ	ω	Q_i	Ideals	$h_{\mathbb{K}}(x)$
-23	-23	$\frac{1+\sqrt{-23}}{2}$	$x^2+xy+6y^2$ $2x^2+xy+3y^2$	$\langle 1,\omega\rangle$ $\langle 2,\omega\rangle$	$x^3+3491750x^2-$ $-5151296875x+12771880859375$
-31	-31	$\frac{1+\sqrt{-31}}{2}$	$x^2+xy+8y^2$ $2x^2+xy+4y^2$	$\langle 1,\omega\rangle$ $\langle 2,1+\omega\rangle$	$x^3+39491307x^2-$ $-58682638134x+1566028350940383$
-59	-59	$\frac{1+\sqrt{-59}}{2}$	$x^2+xy+15y^2$ $3x^2+xy+5y^2$	$\langle 1,\omega\rangle$ $\langle 3,\omega\rangle$	$x^3+30197678080x^2-$ $-140811576541184x+374643194001883136$
-83	-83	$\frac{1+\sqrt{-83}}{2}$	$x^2+xy+21y^2$ $3x^2+xy+7y^2$	$\langle 1,\omega\rangle$ $\langle 3,\omega\rangle$	$x^3+2691907584000x^2-$ $-41490055168000000x+$ $+549755813888000000000$
-107	-107	$\frac{1+\sqrt{-107}}{2}$	$x^2+xy+27y^2$ $3x^2+xy+9y^2$	$\langle 1,\omega\rangle$ $\langle 3,\omega\rangle$	$x^3+129783279616000x^2-$ $-6764523159552000000x+$ $+337618789203968000000000$
-139	-139	$\frac{1+\sqrt{-139}}{2}$	$x^2+xy+35y^2$ $5x^2+xy+7y^2$	$\langle 1,\omega\rangle$ $\langle 5,\omega\rangle$	$x^3+12183160834031616x^2-$ $-53041786755137667072x+$ $+67408489017571610198016$
-211	-211	$\frac{1+\sqrt{-211}}{2}$	$x^2+xy+53y^2$ $5x^2+3xy+11y^2$	$\langle 1,\omega\rangle$ $\langle 5,1+\omega\rangle$	$x^3+6587358728863009968x^2+$ $+277390576406111100862464x+$ $+5310823021408898698117644288$
-283	-283	$\frac{1+\sqrt{-283}}{2}$	$x^2+xy+71y^2$ $7x^2+5xy+11y^2$	$\langle 1,\omega\rangle$ $\langle 7,2+\omega\rangle$	$x^3+89611323386832801792000x^2+$ $+90839236535446929408000000x+$ $+201371843156955365376000000000$

Table 3.4: Imaginary quadratic fields $\mathbb{K}=\mathbb{Q}(\sqrt{d})$ of class number 3

d	Δ	ω	Q_i	Ideals	$h_{\mathbb{K}}(x)$
-307	-307	$\frac{1+\sqrt{-307}}{2}$	$x^2+xy+77y^2$ $7x^2+xy+11y^2$	$\langle 1,\omega\rangle$ $\langle 7,\omega\rangle$	$x^3+805016812009981390848000x^2-$ $-5083646425734146162688000000x+$ $+8987619631060626702336000000000$
-331	-331	$\frac{1+\sqrt{-331}}{2}$	$x^2+xy+83y^2$ $5x^2+3xy+17y^2$	$\langle 1,\omega\rangle$ $\langle 5,1+\omega\rangle$	$x^3+6647404730173793386463232x^2+$ $+368729929041040103875232661504x+$ $+561762428403893982302184885945630720$
-379	-379	$\frac{1+\sqrt{-379}}{2}$	$x^2+xy+95y^2$ $5x^2+xy+19y^2$	$\langle 1,\omega\rangle$ $\langle 5,\omega\rangle$	$x^3+364395404104624239018246144x^2-$ $-121567791009880876719538528321536x+$ $+15443600047689011948024601807415148544$
-499	-499	$\frac{1+\sqrt{-499}}{2}$	$x^2+xy+125y^2$ $5x^2+xy+25y^2$	$\langle 1,\omega\rangle$ $\langle 5,\omega\rangle$	$x^3+30051011080710262007067259699 20x^2-$ $-60637178254942663947223925600110510 08x+$ $+46711331823999547827986731544374413109 49376$
-547	-547	$\frac{1+\sqrt{-547}}{2}$	$x^2+xy+137y^2$ $11x^2+5xy+13y^2$	$\langle 1,\omega\rangle$ $\langle 11,2+\omega\rangle$	$x^3+8129739553963165472163747840000 0x^2-$ $139712328431787827943469744128000000x+$ $833039375706784039686352404480000000000$
-643	-643	$\frac{1+\sqrt{-643}}{2}$	$x^2+xy+161y^2$ $7x^2+xy+23y^2$	$\langle 1,\omega\rangle$ $\langle 7,\omega\rangle$	$x^3+39545575162726134099492467011584000x^2-$ $630037850504724787649965179745075200000 0x+$ $+3080525546523028473808808412991979520000000000$
-883	-883	$\frac{1+\sqrt{-883}}{2}$	$x^2+xy+221y^2$ $13x^2+xy+17y^2$	$\langle 1,\omega\rangle$ $\langle 13,\omega\rangle$	$x^3+3490393434101181903922429501193339 2896000x^2-$ $15196011112524528203387561952912447897600 0000x+$ $+16799028538162731818757552080012338790400 0000000$
-907	-907	$\frac{1+\sqrt{-907}}{2}$	$x^2+xy+227y^2$ $13x^2+9xy+19y^2$	$\langle 1,\omega\rangle$ $\langle 13,4+\omega\rangle$	$x^3+1230720807211984023944775905068386877 44000x^2+$ $+39181594208014819617565811575376314368 000000x+$ $+14916127474652484132854589496927400755 2000000000$

Table 3.5: Imaginary quadratic fields $\mathbb{K}=\mathbb{Q}(\sqrt{d})$ of class number 3

d	Δ	ω	π_a	Systems
-23	-23	$\frac{1+\sqrt{-23}}{2}$	$2-\omega$	$x^3-9x^2y-9xy^2+3y^3=u$ $x^3+3x^2y-3xy^2-2y^3=v$
-31	-31	$\frac{1+\sqrt{-31}}{2}$	$1-\omega$	$-12x^2y-18xy^2+y^3=u$ $x^3+3x^2y-3xy^2-4y^3=v$
-59	-59	$\frac{1+\sqrt{-59}}{2}$	$-3-\omega$	$-4x^3-15x^2y+15xy^2+10y^3=u$ $x^3-3x^2y-6xy^2+y^3=v$
-83	-83	$\frac{1+\sqrt{-83}}{2}$	$3-\omega$	$2x^3-21x^2y-21xy^2+14y^3=u$ $x^3+3x^2y-6xy^2-3y^3=v$
-107	-107	$\frac{1+\sqrt{-107}}{2}$	$-\omega$	$-x^3-27x^2y+27y^3=u$ $x^3-9xy^2-y^3=v$
-139	-139	$\frac{1+\sqrt{-139}}{2}$	$10-\omega$	$9x^3-21x^2y-42xy^2+7y^3=u$ $x^3+6x^2y-3xy^2-3y^3=v$
-211	-211	$\frac{1+\sqrt{-211}}{2}$	$9-\omega$	$8x^3-27x^2y-69xy^2+6y^3=u$ $x^3+6x^2y-3xy^2-5y^3=v$
-283	-283	$\frac{1+\sqrt{-283}}{2}$	$-16-\omega$	$-17x^3-45x^2y+48xy^2+35y^3=u$ $x^3-6x^2y-9xy^2+y^3=v$
-307	-307	$\frac{1+\sqrt{-307}}{2}$	$7-2\omega$	$5x^3-66x^2y-33xy^2+33y^3=u$ $2x^3+3x^2y-9xy^2-2y^3=v$
-331	-331	$\frac{1+\sqrt{-331}}{2}$	$-6-\omega$	$-7x^3-54x^2y+39xy^2+69y^3=u$ $x^3-3x^2y-12xy^2+y^3=v$
-379	-379	$\frac{1+\sqrt{-379}}{2}$	$-5-\omega$	$-6x^3-57x^2y+57xy^2+76y^3=u$ $x^3-3x^2y-12xy^2+3y^3=v$
-499	-499	$\frac{1+\sqrt{-499}}{2}$	$-\omega$	$-x^3-75x^2y+125y^3=u$ $x^3-15xy^2-y^3=v$
-547	-547	$\frac{1+\sqrt{-547}}{2}$	$29-2\omega$	$-27x^3-60x^2y-123xy^2+5y^3=u$ $2x^3+9x^2y-3xy^2-4y^3=v$
-643	-643	$\frac{1+\sqrt{-643}}{2}$	$14-\omega$	$13x^3-69x^2y-138xy^2+69y^3=u$ $x^3+6x^2y-9xy^2-7y^3=v$
-883	-883	$\frac{1+\sqrt{-883}}{2}$	$13+3\omega$	$16x^3+153x^2y-51xy^2-68y^3=u$ $-3x^3+3x^2y+12xy^2-y^3=v$
-907	-907	$\frac{1+\sqrt{-907}}{2}$	$-14+3\omega$	$-11x^3+147x^2y+150xy^2-37y^3=u$ $-3x^3-6x^2y+9xy^2+5y^3=v$

Table 3.6: Imaginary quadratic fields $\mathbb{K}=\mathbb{Q}(\sqrt{d})$ of class number 3

Chapter 4

Schoof's algorithm

In 1985 Renè Schoof published a deterministic polynomial-time algorithm to count the rational points of non-singular elliptic curves over finite fields. Fixed a prime integer ℓ, the algorithm works over the point of order ℓ, distinguishing two cases through the group law of the elliptic curve. In the following lines we will present the possible existence of a family of elliptic curves not taken into account by Schoof's original paper [50].

4.1 Elliptic curves over finite fields

For the sake of easy references, we summarize some basic facts about elliptic curves over finite fields refering to [58]. In the rest of the chapter p, n, q will denote, respectively, a prime integer greater than 3, a non-zero natural number and the power p^n.
Let $\mathbb{E}$ be an elliptic curve defined by the Weierstrass equation over the finite field $\mathbb{F}_q$, i.e. $\mathbb{E}$ is the projective closure of the affine variety defined over $\mathbb{F}_q$ by the polynomial:

$$y^2 - x^3 - Ax - B \in \mathbb{F}_q[x, y] \tag{4.1}$$

If $\mathbb{F}$ is an extension field of $\mathbb{F}_q$ we define:

$$E(\mathbb{F}) = \{(x, y) \in \mathbb{F} \times \mathbb{F} \mid y^2 = x^3 + Ax + B\} \cup \{\infty\} \tag{4.2}$$

where ∞ is *the point at infinity.*
Since an elliptic curve is a non-singular cubic curve, the cubic $x^3 + Ax + B \in \mathbb{F}_q[x]$ doesn't have multiple roots, i.e. $4A^3 + 27B^2$ is not zero.

It is possible to defined a sum in $\mathbb{E}(F)$ that gives to it the structure of an abelian group. In particular, given two points $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ of $\mathbb{E}(\mathbb{F})$, different from ∞, their sum $P_3 = (x_3, y_3)$ is defined as :

$$P_3 := \begin{cases} \left(\left(\frac{y_2-y_1}{x_2-x_1}\right)^2 - x_1 - x_2, \left(\frac{y_2-y_1}{x_2-x_1}\right)(x_1 - x_3) - y_1\right) & \text{if } x_1 \neq x_2 \\ \infty & \text{if } x_1 = x_2 \text{ and } y_1 = -y_2 \\ \left(\left(\frac{3x_1^2+A}{2y_1}\right)^2 - 2x_1, \left(\frac{3x_1^2+A}{2y_1}\right)(x_1 - x_3) - y_1\right) & \text{if } P_1 = P_2 \text{ and } y_1 \neq 0 \\ \infty & \text{if } P_1 = P_2 \text{ and } y_1 = 0 \end{cases}$$

Moreover, $P + \infty = \infty + P = P$ for every point $P \in \mathbb{E}(\mathbb{F})$.
An estimate of the number of rational points of $\mathbb{E}$, i.e. the elements of $\mathbb{E}(\mathbb{F}_q)$, is given by a result obtained by Helmut Hasse in 1933 [28].

Hasse Theorem. *The number of elements of $\mathbb{E}(\mathbb{F}_q)$ is equal to $q + 1 - a$, where a is an integer such that $|a| \leq 2\sqrt{q}$.*

This result could be related with the Frobenius Endomorphism ϕ_q, which is a group endomorphism defined as:

$$\begin{array}{rccc} \phi_q : & \mathbb{E}(\overline{\mathbb{F}_q}) & \rightarrow & \mathbb{E}(\overline{\mathbb{F}_q}) \\ & (x, y) & \mapsto & (x^q, y^q) \end{array}$$

We have [53, pag. 142]:

$$\phi_q(\phi_q(P)) + qP = a\phi_q(P) \qquad\qquad \forall P \in \mathbb{E}(\overline{\mathbb{F}_q})$$

A useful tool to investigate the group structure of $\mathbb{E}(\overline{\mathbb{F}_q})$ is a familiy of multivariate polynomials of $\mathbb{F}_q[x, y]$, called the *division polynomials* of $\mathbb{E}$, defined recursively:

$$\begin{aligned} \psi_0(x, y) &= 0 \\ \psi_1(x, y) &= 1 \\ \psi_2(x, y) &= 2y \\ \psi_3(x, y) &= 3x^4 + 6Ax^2 + 12Bx - A^2 \\ \psi_4(x, y) &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3) \\ \psi_{2m+1}(x, y) &= \psi_{m+2}(x, y)\psi_m^3(x, y) - \psi_{m-1}(x, y)\psi_{m+1}^3(x, y) && \text{for } m \geq 2 \\ \psi_{2m}(x, y) &= (2y)^{-1}\psi_m(x, y)(\psi_{m+2}(x, y)\psi_{m-1}^2(x, y) - \psi_{m-2}(x, y)\psi_{m+1}^2(x, y)) && \text{for } m \geq 3 \end{aligned}$$

If i is odd, y has even power in every term of $\psi_i(x, y)$; if i is even $\psi_i(x, y)$ is the product of $2y$ and a polynomial of $\mathbb{F}_q[x, y]$ where y has even power in all its terms. Hence it is possible to consider a family of polynomials of $\mathbb{F}_q[x]$:

$$\begin{aligned} f_i(x) &= \psi_i'(x, y) && \text{if } i \text{ odd} \\ f_i(x) &= \frac{\psi_i'(x, y)}{y} && \text{if } i \text{ even} \end{aligned} \tag{4.3}$$

where $\psi'_i(x,y)$ denotes the polynomial obtained substituting y^2 with x^3+Ax+B in $\psi_i(x,y)$. Given $P=(x,y)\in\overline{\mathbb{F}_q}[x]$, we have:

$$iP=\left(\frac{x\psi_i^2(x,y)-\psi_{i-1}(x,y)\psi_{i+1}(x,y)}{\psi_i^2(x,y)},\frac{\psi_{i+2}(x,y)\psi_{i-1}^2(x,y)-\psi_{i-2}(x,y)\psi_{i+1}^2(x,y)}{4y\psi_i^3(x,y)}\right)$$

and therefore:

$$iP=\begin{cases}\left(\frac{x(x^3+Ax+B)f_i^2(x)-f_{i+1}(x)f_{i-1}(x)}{(x^3+Ax+B)f_i^2(x)},\frac{f_{i+2}(x)f_{i-1}^2(x)-f_{i-2}(x)f_{i+1}(x)^2}{4(x^3+Ax+B)f_i^3(x)}\right) & i \text{ even}\\ \left(\frac{xf_i^2(x)-(x^3+Ax+B)f_{i+1}(x)f_{i-1}(x)}{f_i^2(x)},\frac{(x^3+Ax+B)[f_{i+2}(x)f_{i-1}^2(x)-f_{i-2}(x)f_{i+1}^2(x)]}{4yf_i^3(x)}\right) & i \text{ odd}\end{cases} \tag{4.4}$$

If P is such that $y\neq 0$ then $iP=\infty$, with $i\in\mathbb{N}$, if and only if $f_i(x)=0$. Furthermore, if p does not divide i, we have:

$$deg(f_i(x))=\begin{cases}\frac{1}{2}(i^2-4) & i \text{ even}\\ \\ \frac{1}{2}(i^2-1) & i \text{ odd}\end{cases}$$

and the set $\mathbb{E}[i]$ defined as

$$\mathbb{E}[i]=\{P\in\mathbb{E}(\overline{\mathbb{F}_q})\mid iP=0\}$$

is isomorphic to $\mathbb{Z}_i\times\mathbb{Z}_i$. Hence $\mathbb{E}[i]$ has i^2 elements.

4.2 Case 1 of the Schoof's Algorithm

Schoof's algorithm [50] computes $\#\mathbb{E}(\mathbb{F}_q)=q+1-a$ requiring at most $\log^9 q$ elementary operations. The algorithm's basic idea is to consider the smallest set $S=\{3,\dots,L\}=\{\ell_1,\dots,\ell_t\}$ of consecutive prime integers (starting from 3 and excluding p) such that

$$\prod_{j=1}^{t}\ell_j>4\sqrt{q}$$

and to find, for every $\ell\in S$, an integer a_ℓ such that $a_\ell\equiv a \pmod{\ell}$. Then, using the Chinese remainder theorem, we can solve the system of linear congruences

$$\begin{cases}x\equiv a_{\ell_1} & \pmod{\ell_1}\\ \dots & \\ x\equiv a_{\ell_t} & \pmod{\ell_t}\end{cases}$$

finding a solution $m\in\mathbb{Z}$ unique up to congruence modulo $\prod_{j=1}^{t}\ell_j$. This means $a\equiv m$ $(\text{mod }\prod_{j=1}^{t}\ell_j)$. Since a lies in $\{0,\pm 1,\dots,\frac{\prod_{j=1}^{t}\ell_j}{2}\}$, it is the only solution of the system contained in this complete residue system. So is sufficient to reduce m modulo $\prod_{j=1}^{t} \ell_j$ to obtain a. To find a_ℓ, Schoof uses the group structure of $\mathbb{E}[\ell]$ and the division polynomials. For a fixed $\ell \in S$, the algorithm distinguishes two cases by means of the addition law in $\mathbb{E}(\overline{\mathbb{F}_q})$. We recall how to proceed in one of them, improving the notation used by Schoof in his original work.

Let ℓ be a prime integer of S. Since it is not divisible by p, $\mathbb{E}[\ell]$ has cardinality ℓ^2. So we can write:

$$\mathbb{E}[\ell] = \{\infty, P_1, \dots, P_{\ell^2-1}\}$$

The roots of the separable polynomial $f_\ell(x)$ are all and only the x-coordinates of the non-zero elements of $\mathbb{E}[\ell]$. For every $P \in \mathbb{E}[\ell]$, we have:

$$\phi_q^2(P) + k(P) = a_\ell(\phi_q(P)) \qquad k \equiv q \pmod{\ell}$$

and so we can consider the set

$$\tilde{G} = \{P \in \mathbb{E}[\ell] \setminus \{\infty\} \mid \phi_q(\phi_q(P)) = \pm kP\}$$

In the light of (4.4), this set is non empty if and only if there exist some non-zero $P = (x, y) \in \mathbb{E}[\ell]$ such that:

$$x^{q^2} - \frac{x(x^3 + Ax + B)f_k^2(x) - f_{k+1}(x)f_{k-1}(x)}{(x^3 + Ax + B)f_k^2(x)} = 0 \quad k \text{ even}$$

$$x^{q^2} - \frac{xf_k^2(x) - (x^3 + Ax + B)f_{k+1}(x)f_{k-1}(x)}{f_k^2(x)} = 0 \quad k \text{ odd}$$

We observe that $f_k(x)$ is non-zero on the x-coordinates of a non-zero $P = (x, y)$ of $\mathbb{E}[\ell]$ because we can choose $k \in \{0, \dots, l-1\}$. Hence $\tilde{G} \neq \emptyset$ if and only if the following greatest common divisor $G(x)$

$$G(x) = \begin{cases} gcd(f_l(x), (x^{q^2} - x)(f_k^2(x))(x^3 + Ax + B) + f_{k-1}(x)f_{k+1}(x)) & k \text{ even} \\ gcd(f_l(x), (x^{q^2} - x)(f_k^2(x)) + (x^3 + Ax + B)f_{k-1}(x)f_{k+1}(x)) & k \text{ odd} \end{cases}$$

is not 1. Schoof's algorithm distinguishes two cases depending on the cardinility of $\tilde{G}$: if it is different from zero we are in *Case 1* of the original paper. This is the case we are interested in and that we will consider.

If there exists a non-zero element $P \in \mathbb{E}[\ell]$ such that $\phi_q(\phi_q(P)) = -kP$, then $a(\phi_q(P)) = \infty$ and $a \equiv 0 \pmod{\ell}$ because also $\phi_q(P)$ is of order ℓ. The existence of such a non-zero element of $\mathbb{E}[\ell]$ forces $\phi_q(\phi_q(P)) = -kP$ for every $P \in \mathbb{E}[\ell]$.
So, defining the sets

$$\tilde{G}_+ = \{P \in \mathbb{E}[\ell] \setminus \{\infty\} \mid \phi_q(\phi_q(P)) = +kP\}$$

and

$$\tilde{G}_- = \{P \in \mathbb{E}[\ell] \setminus \{\infty\} \mid \phi_q(\phi_q(P)) = -kP\}$$

we have three possible scenarios:

1. $\tilde{G} = \tilde{G}_- = \mathbb{E}[\ell]$;

2. $\tilde{G} = \tilde{G}_+ = \mathbb{E}[\ell]$;

3. $\tilde{G} = \tilde{G}_+ \subsetneq \mathbb{E}[\ell]$.

It is easy to see that $\tilde{G} = \tilde{G}_+$ if and only if q is a quadratic residue modulo ℓ (i.e. $q \equiv w^2 \pmod{\ell}$ for some $w \in \mathbb{Z}$) and $\phi_q(P) = wP$ or $\phi_q(P) = -wP$ for every P in $\tilde{G}$. In fact, we observe that could not exist two different points $P_1, P_2 \in \tilde{G}$ such that $\phi_q(P_1) = wP_1$ and $\phi_q(P_2) = -wP_2$. In fact, from

$$\infty = \phi_q^2(P_1) - a\phi_q(P_1) + kP_1 = \phi_q^2(P_1) - awP_1 + kP_1 = (2k - aw)P_1$$

it would follow $2k - aw \equiv 0 \pmod{\ell}$ and hence $a \equiv 2w \pmod{\ell}$. At the same time, using P_2 we would obtain $a \equiv -2w \pmod{\ell}$. But $2w + 2w = 4w$ is not zero modulo ℓ.

If w is the square root of q in $\mathbb{Z}_\ell$, the set:

$$\tilde{F} = \{P \in \mathbb{E}[\ell] \setminus \{\infty\} \mid \phi_q(P) = \pm wP\} \subset \tilde{G}$$

is non empty if and only if there exist some non-zero $P = (x, y) \in \mathbb{E}[\ell]$ such that:

$$x^q - \frac{x(x^3 + Ax + B)f_w^2(x) - f_{w+1}(x)f_{w-1}(x)}{(x^3 + Ax + B)f_w^2(x)} = 0 \quad w \text{ even}$$

$$x^q - \frac{xf_w^2(x) - (x^3 + Ax + B)f_{w+1}(x)f_{w-1}(x)}{f_w^2(x)} = 0 \quad w \text{ odd}$$

As before, we observe that $f_w(x)$ is non-zero on the x-coordinates of the points of $\mathbb{E}[\ell]$ because we can choose $w \in \{0, \ldots, l-1\}$. Hence, $\tilde{F} \neq \emptyset$ if and only if the following greatest common divisor $F(x)$:

$$F(x) = \begin{cases} gcd(f_\ell(x), (x^q - x)(f_w^2(x))(x^3 + Ax + B) + f_{w-1}(x)f_{w+1}(x)) & w \text{ even} \\ gcd(f_\ell(x), (x^q - x)(f_w^2(x)) + (x^3 + Ax + B)f_{w-1}(x)f_{w+1}(x)) & w \text{ odd} \end{cases}$$

is not 1. So we are in the first scenario if and only if $G(x) \neq 1$ and $F(x) = 1$; we are in the other two scenarios if and only if $G(x) \neq 1$ and $F(x) \neq 1$. We assume to be in one of the last two scenarios.

As we have done for $\tilde{G}$, we can define

$$\tilde{F}_+ = \{P \in \mathbb{E}[\ell] \setminus \{\infty\} \mid \phi_q(P) = +wP\}$$

and

$$\tilde{F}_- = \{P \in \mathbb{E}[\ell] \setminus \{\infty\} \mid \phi_q(P) = -wP\}$$

To find the equivalence class of a in $\mathbb{Z}_\ell$ we have to determine if $\tilde{F} = \tilde{F}_+$ or $\tilde{F} = \tilde{F}_-$. To do this Schoof suggest to compute:

$$H_1(x) = \begin{cases} gcd(f_l(x), 4(y)^{q+3}(f_w^3(x)) - (f_{w+2}(x)f_{w-1}^2(x) - f_{w-2}(x)f_{w+1}^2(x))) & w \text{ even} \\ gcd(f_l(x), 4(y)^{q+1}(f_w^3(x)) - (y^2)(f_{w+2}(x)f_{w-1}^2(x) - f_{w-2}(x)f_{w+1}^2(x)) & w \text{ odd} \end{cases}$$

and

$$H_2(x) = \begin{cases} gcd(f_l(x), 4(y)^{q+3}(f_w^3(x)) + (f_{w+2}(x)f_{w-1}^2(x) - f_{w-2}(x)f_{w+1}^2(x))) & w \text{ even} \\ gcd(f_l(x), 4(y)^{q+1}(f_w^3(x)) + (y^2)(f_{w+2}(x)f_{w-1}^2(x) - f_{w-2}(x)f_{w+1}^2(x)) & w \text{ odd} \end{cases}$$

that corresponds to find $P = (x, y) \in \mathbb{E}[\ell] \setminus \{\infty\}$ such that

$$0 = y^q - (wP)_y = y^q - \begin{cases} \frac{f_{w+2}(x)f_{w-1}^2(x) - f_{w-2}(x)f_{w+1}(x)^2}{4y(x^3+Ax+B)f_w^3(x)} & \text{w even} \\ \\ \frac{(x^3+Ax+B)[f_{w+2}(x)f_{w-1}^2(x) - f_{w-2}(x)f_{w+1}^2(x)]}{4yf_w^3(x)} & \text{w odd} \end{cases}$$

or, respectively, such that:

$$0 = y^q + (wP)_y = y^q + \begin{cases} \frac{f_{w+2}(x)f_{w-1}^2(x) - f_{w-2}(x)f_{w+1}(x)^2}{4y(x^3+Ax+B)f_w^3(x)} & \text{w even} \\ \\ \frac{(x^3+Ax+B)[f_{w+2}(x)f_{w-1}^2(x) - f_{w-2}(x)f_{w+1}^2(x)]}{4yf_w^3(x)} & \text{w odd} \end{cases}$$

Since we have supposed $\tilde{F} \neq \emptyset$, one of $H_1(x)$ and $H_2(x)$ must be different from 1. If $\tilde{F} = \tilde{F}_+$ then $H_1(x) \neq 1$ and $a \equiv 2w \pmod{\ell}$, otherwise $H_2(x) \neq 1$ and $a \equiv -2w \pmod{\ell}$.
This conditions are necessary. Despite Schoof did not prove that they are also sufficient conditions, he used it as sufficient conditions. In fact, Schoof's paper says:

«*If* $H_1(x)$ *equals 1 then* $a \equiv -2w \pmod{\ell}$*...*».

This could lead to an error on a curve for which (for example) $\tilde{F}$ is equal to $\tilde{F}_-$ (so $H_2(x) \neq 1$ and $a \equiv -2w \pmod{\ell}$) and there exists a point $P = (x, y) \in \mathbb{E}[\ell] \setminus \tilde{G}$ such that $(\phi(P))_y = (wP)_y$, i.e. $H_1(x)$ is not equal to 1. In this case Schoof's algorithm concludes $a \equiv 2w \pmod{\ell}$ even if a is actually congruent to $-2w$ modulo ℓ.

Clearly, this problem of the original Schoof's Algorithm is easily solved substituting $f_\ell(x)$ with $G(x)$ in the computation of $H_1(x)$ and $H_2(x)$: this little change avoids the existence of elliptic curves with a "bad behavior" and also makes faster the computation of $H_1(x)$ and $H_2(x)$ because $deg(G(x))$ is less then $deg(f_\ell(x))$.

Even if the correctness and the power of the Schoof's algorithm are not damaged, it remains intriguing the problem of the existence of elliptic curves on which the Schoof's algorithm falls into an error.

4.3 Attempts and observations

After that Schoof himself confirmed, in an informal conversation, our observation about the possible existence of a family of curves not considered by his original paper, we did several attempts to find a counter-example.

As suggested by Schoof, first of all we looked for a non-singular elliptic curve $\mathbb{E}$, defined over a finite field $\mathbb{F}_q$, and a prime integer ℓ such that $\mathbb{E}[\ell]$ contains two distinct points with the same y-coordinate. Using MAGMA to test the elliptic curves, we obtain that for $q = 23$ and $\ell = 11$ there exist numerous non-singular elliptic curves defined over $\mathbb{F}_q$ with two different points of order 11 having the same y-coordinate. But $\ell = 11$ does not belong to the set S of consecutive primes used by Schoof's algorithm to find the number of rational numbers of a curve over $\mathbb{F}_{23}$. So another question arises: does exist a non-singular elliptic curve with two different points that have the same y-coordinate and the same order ℓ, where ℓ is a prime of S? Setting $q = 71$ and $\ell = 5$ (or $q = 59$ and $\ell = 5$, $q = 3$ and $\ell = 7$) we have a lot of non-singular elliptic curves defined over $\mathbb{F}_q$ for which exist two different points of order ℓ having the same y-coordinate. But these curves are not counter-examples. So the condition that $\mathbb{E}[\ell]$ contains two distinct points with the same y-coordinate is not sufficient to have a counter-example.

With the power of calculus available to us, we were able to sift all the non-singular elliptic curves over a finite field with a number of elements less than or equal to 101. We did not find the desired curve with a "bad behavior". So we tried to find an elliptic curve $\mathbb{E}$ over $\mathbb{F}_q$ with a "bad behavior" in $\mathbb{E}[\ell]$, with ℓ not necessary in the set S used by the Schoof's algorithm. The idea was to start from such a curve and then work on it to obtain a counter-example. For $p, \ell \in \{5, 7, \ldots, 101\}$ we tested the ℓ-torsion points $\mathbb{E}[\ell]$ of all the non singular elliptic curves over $\mathbb{F}_p$ by the following MAGMA program:

```
// Set of base fields
p:=3;
BaseFields:=[ ];
while (p lt 101) do
   p:=NextPrime( p);
   BaseFields:=Append(BaseFields,p);
end while;

// Set of prime integers l
l:=2;
HugeS:=[];
while (l lt 101) do
   l:=NextPrime(l);
   HugeS:=Append(HugeS,l);
end while;

// Function that constructs the t-th division polynomial of an elliptic curve
    y^2=x^3+Ax+B over the finite field of q elements
```

```
DivPol:= function (A,B,q,t)
   Z:=IntegerRing();
   K:=GF(q); // Finite field of q elements
   PolK<x>:=PolynomialRing(K);
   P:=[-1,0, 1, 2, 3*(x^4)+6*A*(x^2)+12*B*x-(A^2), 4*(x^6+5*A*(x^4)+20*B*(x^3) -
    5*(A^2)*(x^2) - 4*A*B*x - 8*(B^2) - (A^3))]; /* division polynomial that
                                                    initialize the recurrence */
   s:=t+2; /* the idea is to append the successive division polynomials until
              we obtain the t-th. This would be the (t+2)-th element of the list P */
   if t lt 5 then
      f:=P[s];
   end if;
   for i in [5..t] do // recurrence
      if (IsEven(i) eq true) then m:=i/2;
         m:=Z!m;
         P:=Append(P,(2^(-1))*P[m+2]*(P[m+4]*(P[m+1]^2)-P[m]*(P[m+3]^2)));
      else
         m:= (i - 1)/2;
         m:=Z!m;
         if (IsEven(m) eq true) then
            P:=Append(P,P[m+4]*(P[m+2]^3)*((x^3+A*x+B)^2) - (P[m+3]^3)*P[m+1]);
         else
            P:=Append(P,P[m+4]*(P[m+2]^3) - (P[m+3]^3)*(P[m+1])*((x^3+A*x+B)^2));
         end if;
      end if;
   end for;
   f:=P[s];
   return f;
end function;

for p in BaseFields do
   q:=p;
   K:=GF(q);
   l:=...; // l must be chosen in HugeS
   if (l eq p) then
      continue; // if p=l we pass to next iteration
   end if;
   Z:=IntegerRing();
   Zl:=IntegerRing(l); // ring of integers modulo l
   r:=Zl!q; // r is the rest of the division of q by l
   if (IsPower(r,2) eq false) then /* first necessary condition to have a
                                      counter-example: q must be a quadratic
                                      residue modulo l */
      continue;
   end if;
   w:= Sqrt(r);  // square root of q in Z/lZ
   w:=Z!w;
// construction of all the non-singular elliptic curves over Fq
   a:=K!0;
   b:=K!0;
   Et:=[* *]; // list of lists
   for i in [1..q] do
      Et[i]:=[]; // list of elliptic curves y^2=x^3+Ax+B with A=i-1;
      for j in [1..q] do
         if 4*a^3 + 27*b^2 ne 0 then
            E := EllipticCurve([K | a,b]) ;
            Et[i] := Append(Et[i], E);
         end if ;
         b:=b+1;
      end for ;
      a:=a+1;
   end for;
// behavior of each curve
   for i in [1..#Et] do
      for E in Et[i] do
         A:=K!Coefficients(E)[4]; /* for Magma E is a polynomial of five terms:
                                      the last two are Ax and B */
         B:=K!Coefficients(E)[5];
         PolK<x>:=PolynomialRing(K);
         if (IsEven(w) eq true) then /* F is the greatest common divisor F(x)
                                        defined in the previous section */
            f:=(x^q-x)*(x^3+A*x+B)*(DivPol(A,B,q,w)^2)+
                 DivPol(A,B,q,w-1)*DivPol(A,B,q,w+1);
         else
             f:=(x^q-x)*(DivPol(A,B,q,w)^2)+
                  (x^3+A*x+B)*DivPol(A,B,q,w-1)*DivPol(A,B,q,w+1);
         end if;
         F:=GreatestCommonDivisor(DivPol(A,B,q,l),h);
         if F eq 1 then // If F(x)=1 the tested curve is not a counter-example
            continue;
         else
            if IsEven(w) eq true then
               t:=Z!(q+3)/2;
               if w eq 1 then
                  hpp:=4*((x^3+A*x+B)^(Z!t))*(DivPol(A,B,q,w)^3)-
                           (+(DivPol(A,B,q,w+2)*DivPol(A,B,q,w-1)^2-
                           (-1)* DivPol(A,B,q,w+1)^2));
                  hpm:=4*((x^3+A*x+B)^(Z!t))*(DivPol(A,B,q,w)^3)-
                            (-(DivPol(A,B,q,w+2)*DivPol(A,B,q,w-1)^2-
                            (-1)* DivPol(A,B,q,w+1)^2));
               else
                  hpp:=4*((x^3+A*x+B)^(Z!t))*(DivPol(A,B,q,w)^3)-
                           (+(DivPol(A,B,q,w+2)*DivPol(A,B,q,w-1)^2-
                           DivPol(A,B,q,w-2)* DivPol(A,B,q,w+1)^2));
                  hpm:=4*((x^3+A*x+B)^(Z!t))*(DivPol(A,B,q,w)^3)-
                            (-(DivPol(A,B,q,w+2)*DivPol(A,B,q,w-1)^2-
                            DivPol(A,B,q,w-2)* DivPol(A,B,q,w+1)^2));
               end if;
               H1:=GreatestCommonDivisor(DivPol(A,B,q,l),hpp);
               H2:=GreatestCommonDivisor(DivPol(A,B,q,l),hpm);
               if (IsDivisibleBy(H1,F) eq true) then /* F(x) must divide one of the
                                                        polynomials H1(x), H2(x) */
                  if H2 ne 1 then
                     printf"Half Eureka!"; E; // curve that we are looking for
                  end if;
               else
                  if H1 ne 1 then
                     printf"Half Eureka!"; E;
                  end if;
               end if;
            else
               s:=Z!(q-1)/2;
               if w eq 1 then
                  hdp:=4*((x^3+A*x+B)^(Z!s))*(DivPol(A,B,q,w)^3)-
```

```
                          (+(DivPol(A,B,q,w+2)*DivPol(A,B,q,w-1)^2 -
                          (K!-1)* DivPol(A,B,q,w+1)^2));
                 hdm:=4*((x^3+A*x+B)^(Z!s))*(DivPol(A,B,q,w)^3)-
                           (-(DivPol(A,B,q,w+2)*DivPol(A,B,q,w-1)^2 -
                           (K!-1)* DivPol(A,B,q,w+1)^2));
              else
                 hdp:=4*((x^3+A*x+B)^(Z!s))*(DivPol(A,B,q,w)^3)-
                          (+(DivPol(A,B,q,w+2)*DivPol(A,B,q,w-1)^2 -
                          DivPol(A,B,q,w-2)* DivPol(A,B,q,w+1)^2));
                 hdm:=4*((x^3+A*x+B)^(Z!s))*(DivPol(A,B,q,w)^3)-
                           (-(DivPol(A,B,q,w+2)*DivPol(A,B,q,w-1)^2 -
                           DivPol(A,B,q,w-2)* DivPol(A,B,q,w+1)^2));
              end if;
              H1:=GreatestCommonDivisor(DivPol(A,B,q,l),hdp);
              H2:=GreatestCommonDivisor(DivPol(A,B,q,l),hdm);
              if (IsDivisibleBy(H1,F) eq true) then
                 if H2 ne 1 then
                    printf"Half Eureka!"; E;
                 end if;
              else
                 if H1 ne 1 then
                    printf"Half Eureka!";E;
                 end if;
              end if;
           end if;
        end if;
     end for;
   end for;
end for;

```

Unfortunately, also with this test we did not find what we were looking for. The failure in the research of a counter-example despite the number of tested curves, suggest that a more organic investigature is needed. Or, maybe, the counter-example does not exist. In this case, it remains challenging give a theoretical proof of the non-existence. An idea to obtain this proof could be that of considering the fields of ℓ-torsion points of an elliptic curve $\mathbb{E}$ over a finite field $\mathbb{F}_q$. It is the field adjoining the coordinates of the ℓ-torsion points to the base field $\mathbb{F}_q$. We did not follow this approach but we will perform this analysis in the next future.

Further results and Conclusions

Another method to determine if an indefinite quadratic form $Q(x,y)$ of discriminant $\Delta > 0$ represents a prime integer p (such that $(\Delta/p) = 1$) is here deduced using the continue fractions. To verify whether $Q(x,y)$ represents p we devise the following procedure based on Proposition 1.11, *Gauss reduction algorithm* and composition of forms:

1. Apply *Gauss reduction algorithm* to $Q(x,y)$ obtaining a quadratic form $g_o(x,y)$.

2. Construct a quadratic form (p, B, C) of discriminant Δ, which represents p by the pair $(1,0)$, and reduce it via *Gauss reduction algorithm* to a form $f_o(x,y)$.

3. Compose the form $g_o(x,y)$ with either $f_o(x,y)$ and $f_o(x,-y)$, obtaining $g_o(x,y) \circ f_o(x,y)$ and $g_o(x,y) \circ f_o(x,-y)$.

4. Check whether the reduction of $g_o(x,y) \circ f_o(x,y)$ or the reduction of $g_o(x,y) \circ f_o(x,-y)$ is a principal form.

We observe that when the discriminant Δ is positive, we call principal every reduced form properly equivalent to the form $Q_0(x,y)$, of discriminant Δ, defined in Chapter 1.

The problem of determining whether a quadratic form is a principal form can be tackled in several ways: we describe two possible approaches.

Preliminarly, we recall a classical result concerning the periodic continued fraction representation of $\sqrt{\Delta}$ written as

$$[d_0, [d_1, d_2, \ldots, d_T]]$$

where d_0 is the anti-period and the remaining entries constitute the period of length T. Let $\frac{p_i}{q_i}$ be the partial quotients, also called convergents, of the continued fraction pertaining to the period. Numerators and denominators of the convergents are computed recursively as

$$\left\{ \begin{array}{ll} p_i = d_i p_{i-1} + p_{i-2} & p_0 = d_0, \quad p_{-1} = 1 \\ q_i = d_i q_{i-1} + q_{i-2} & q_0 = 1, \quad q_{-1} = 0 \end{array} \right. \quad i = 1, 2, \ldots$$

The sequence $\mathcal{S} = \{\Delta_i = p_i^2 - \Delta q_i^2\}_{i=1}^{\infty}$ satisfies the following properties, see [31]:

1. The sequence $\mathcal{S}$ is periodic of period T.

2. $|\Delta_i| < 2\sqrt{\Delta}$ for every i.
3. $\Delta_{T-1} = \pm 1$, i.e. $p_{T-1} + q_{T-1}\sqrt{\Delta}$ is the fundamental unit in $\mathbb{Q}(\sqrt{\Delta})$.
4. All the integers of absolute value less than $\sqrt{\Delta}$, represented by a principal form of discriminant Δ, are in a period of the sequence $\mathcal{S}$. The remaining terms of the sequence $\mathcal{S}$ are of absolute value less than $2\sqrt{\Delta}$.

The previous properties offer a criterion for testing whether a quadratic form is a principal form [43]:

Proposition. *A reduced quadratic form (a, b, c), with positive discriminant Δ, is a principal form if and only if the smallest between $|a|$ and $|c|$ occurs in a period of the sequence $\mathcal{S}$ constructed from the continued fraction expansion of $\sqrt{\Delta}$.*

A second criterion can be deduced from the following theorem.

Theorem. *Let (a, b, c) be a reduced quadratic form with discriminant $\Delta > 0$, and $\mathbb{K} = \mathbb{Q}(\sqrt{\Delta})$ be a real quadratic field whose Hilbert class field $\mathbb{L}$ is defined by the root of a known polynomial $H_{\mathbb{K}}(x)$ of degree $2h_\Delta$ over $\mathbb{Q}$. Suppose that all prime factors q_i occurring in a (with the assumption $|a| < |c|$) and c are known, then (a, b, c) is principal if $H_{\mathbb{K}}(x)$ fully splits modulo q_i for every i.*

Proof. If $H_{\mathbb{K}}(x)$ fully splits modulo q_i, then q_i is representable by a principal form because q_i splits into $2h_\Delta$ prime factors in $\mathbb{L}$ ([20, Theorem 5.9] and [21]), and thus into two conjugate prime factors in $\mathbb{K}$. Hence q_i is representable by the principal quadratic form. The composition of forms implies that a and c are representable by the principal form, which in turn imply that (a, b, c) is a principal form. □

Recall that full factorization of $H_{\mathbb{K}}(x)$ modulo q_i can be checked in polynomial complexity by computing the greatest common divisor with $x^{q_i-1} - 1$ modulo q_i.

Conclusions

The issue of solving, with polynomial complexity, the representation problems for a negative discriminant Δ and for a prime integer p, was practically closed by *Gauss reduction algorithm* with the further use of Schoof's algorithm. The same problems, when the discriminant is positive, are not generally settled in polynomial complexity. The methods seen above have a restrained complexity.

In this thesis alternative algorithms for fundamental negative discriminants of class number less than 4 have been developed. Such algorithms are sped up by the precomputation of the Hilbert class polynomials and the Diophantine systems. When a prime p is represented by the principal form, the computational complexity of the algorithms is dominated by the calculation of the number of rational points of an elliptic curve over a finite field $\mathbb{F}_p$. It

can be done using the Schoof's algorithm [50], that takes $O(\log^9 p)$ elementary operations, or even better using the improvement by Schoof - Elkies - Atkin (SEA algorithm) [3].
When a prime p is represented by a non-principal reduced form, one needs to determine the number of rational points of an elliptic curve over a finite field $\mathbb{F}_q$, with $q = p^n$. As above, the Schoof's algorithm -or the SEA algorithm- can be used to perform this calculation with polynomial complexity. Furthermore, $h_{\mathbb{K}}(x) \pmod p$ has to be factorized in order to decide which are the reduced forms that represent a prime p when the imaginary quadratic fields have class number 2 and 3. This factorization could be obtained in polynomial complexity using the Cantor-Zassenhaus probabilistic algorithm [12] or a variation of it due to Schipani and Elia [24], which requires less computational cost.

Future developements of this thesis

A more accurate estimates of the numbers of operations required by the algorithms for the computations may be considered.
For the sake of comparison, many tests may be performed using a large set of primes with the algorithms, collect the timings obtained with MAGMA and compare them with respect to the various algorithms solving the representation problems.

In order to use Theorem 3.6 to deduce an algorithm solving representation problems for every imaginary quadratic field, whatever is its class number, further properties to distinguish the proper equivalence classes of the form class group are desirable. For example, let us consider the case of class number 4. This case is interesting because there are two possible non-isomorphic groups of order 4. If the narrow ideal class group is cyclic of order 4, then a hypothetical criteria to identify the classes that represent a prime integer p could be the factorization of $h_{\mathbb{K}}(x) \pmod p$: when $h_{\mathbb{K}}(x) \pmod p$ splits into 4 distinct linear factors, p would be represented by the principal quadratic form; when $h_{\mathbb{K}}(x) \pmod p$ factors into 2 quadratic factors, p would be represented by the quadratic form that, composed with itself, yields the principal form; when $h_{\mathbb{K}}(x) \pmod p$ is irreducible p would be represented by the remaining classes of quadratic forms which represent the same set of primes. If the narrow ideal class group is the group $\mathbb{Z}_2 \times \mathbb{Z}_2$, then the factorization of $h_{\mathbb{K}}(x) \pmod p$ identifies just the principal form; the remaining three classes, when composed with themselves, yield the principal form and the idea of using the factorization of $h_{\mathbb{K}}(x)$ could not be applied. Further efforts are necessary to find the properties nedeed to distinguish between non-principal reduced forms.

A future work plan would involve the extension of the research of this thesis to obtain more stringent results concerning indefinite quadratic forms. The first step will require an analogous of Theorem 3.5.

Bibliography

[1] Ash, R. B., *A course in algebraic number theory*,
online notes - http://www.math.uiuc.edu/ r-ash/ANT.html.

[2] Atkin, A. O. L., Morain, F., Elliptic curves and primality proving *Mathematics of Computation*, 61(203): 29-68, 1993.

[3] Atkin, A. O. L., The number of points on an elliptic curve modulo a prime (II), Draft, 1992

[4] Bach E., Huber K., Note on Taking Square-Roots Modulo N, *IEEE Trans. on Information Theory*, vol. 45, number 2, March 1999, pp.807-809.

[5] Bashmakova, I. G., *Diophantus and Diophantine Equations*, MAA, 1997.

[6] Berwick, W. E. H., Modular Invariants expressible in terms of quadratic and cubic irrationalities *Proc. London Math. Soc.*, vol. 28, 1928, pp.53-69.

[7] Bhargava, Manjul, Higher composition laws I: A new view on Gauss composition, and quadratic generalizations., *Ann. of Math.*, (2) 159 (2004), no. 1, 217-250.

[8] Bircan, N., Representation of Prime Powers by Binary Quadratic Forms, *Pure Math. Sciences*, vol. 1, 2012, n.2, pp.95-106.

[9] Borevich, Z. I., Shafarevich, I. R., *Number theory*, Academic Press, 1986.

[10] Buchmann, J., Vollmer U., *Binary Quadratic Forms: An algorithmic approach*, Springer-Verlag, New York, 2007.

[11] Buell, D. A., *Binary Quadratic Forms*, Springer-Verlag, New York, 1989.

[12] Cantor D.G., Zassenhaus H., A new Algorithm for Factoring Polynomials over Finite Fields, *Math. of Computation*, Vol. 36, N. 154, April 1981, pp.587-592.

[13] Chandrasekharan, K., *Elliptic Functions*, Springer-Verlag, New York, 1985.

[14] Childress, Nancy, *Class Field Theory*, Springer, New York, 2009.

[15] Cohen, H., *A Course in Computational Algebraic Number Theory*, Springer, New York, 1978.

[16] Cohn, H., *A Classical Invitation to Algebraic Numbers and Class Fields*, Springer, New York, 1962.

[17] Cohn, H., *Advanced Number Theory*, Dover, New York, 1962.

[18] Cohn, H., *Introduction to the Construction of Class Fields*, Dover, New York, 1985.

[19] Cox, D. A., *Galois theory*, Wiley-Interscience, 2004.

[20] Cox, D. A., *Primes of the form* $x^2 + ny^2$, Wiley, New York, 1989.

[21] Dedekind, R., *Theory of Algebraic Integers*, Cambridge Univ. Press, Cambridge, 1996.

[22] Dirichlet, P. G. L., *Lectures on Number Theory*, AMS, Providence, 1999.

[23] Edwards, H. M., *Higher Arithmetic: An Algorithmic Introduction to Number Theory*, AMS, Providence, 2008.

[24] Elia, M., Schipani, D., Improvements on Cantor-Zassenhaus Factorization Algorithm, *arXiv:1012.5322v2 [math.NT]*, 2011.

[25] Fröhlich, A., Taylor, M. J., *Algebraic Number Theory*, Cambridge Univ. Press, Cambridge, 1994.

[26] Gauss, C. F., *Disquisitiones Arithmeticae,* Springer-Verlag, New York, 1986.

[27] Goldfeld, D., Gauss's class number problem for imaginary quadratic fields, *Bull. Amer. Math. Soc. (N.S.)*, 13 (1985), no. 1, pp. 23-37.

[28] Hasse, H., Zur Theorie der abstrakten elliptischen Funktionenörper. I, II and III, *Crell's Journal*, 1936.

[29] Heath, T. L., *Diophantus of Alexandria: A study in the history of Greek Algebra*, Powell's Bookstore & Martino Pub., Chicago, 1910.

[30] Heilbronn, H., On the class number in imaginary quadratic fields, *Quarterly J. of Math.*, 5 (1934), pp.150-160.

[31] Hua, L. K., *Introduction to Number Theory*, Springer, New York, 1982.

[32] Ireland, K., Rosen, M., *A classical introduction to modern number theory*, Springer, 1998

[33] Janusz, G. J., *Algebraic number fields*, Academic Press & New York and London, 1973.

[34] Koblitz, Neal, *A Course in Number Theory and Cryptography,* Springer-Verlag, New York, 1987.

[35] Koch, H., *Algebraic Number Theory*, Springer-Verlag, New York, 1997.

[36] Lagrange, J. L., *Recherches d'Arithmetique*, Berlin, 1775.

[37] Lalesco, T., Sur la représentation des nombres par les classes de formes appartenant à un detérminant donné, *Bulletin de la S. M. F.*, vol. 35 (1907), pp. 248-252.

[38] Landau, Edmund, *Elementary number theory*, AMS Chelsea Publishing, 1927

[39] Lang, Serge, *Algebraic Number Theory*, Springer-Verlag, New York, 1994.

[40] Lang, Serge, *Elliptic Functions*, Springer-Verlag, New York, 1987.

[41] Legendre, A. M., *Essai sur la Theorie des Nombres*, Cambridge Univ. Press, New York, 2009.

[42] Lemmermeyer, Franz, *Online notes of algebraic number theory* http://www.fen.bilkent.edu.tr/ franz/ant-st.pdf

[43] Mathews, G. B., *Theory of Numbers*, Chelsea, New York, 1961.

[44] Mollin, R. A., *Advanced Number Theory with Applications*, Chapman & Hall, Boca Raton, 2010.

[45] Mollin, R. A., *Algebraic Number Theory*, Chapman & Hall, Boca Raton, 1999.

[46] Narkiewicz, W., *Elementary and Analytic Theory of Algebraic Numbers*, Springer-Verlag, New York, 1990.

[47] Neukirch, J., *Algebraic Number Theory,* Springer-Verlag, New York, 1999.

[48] Opolka, H., Scharlau, W., *From Fermat to Minkowski - Lectures on the theory of numbers and its historical development*, Springer, 1985.

[49] Ribenboim, Paulo, *Classical theory of algebraic numbers*, Springer, 2001

[50] Schoof, R., Elliptic Curves Over Finite Fields and the Computation of the Square Roots mod$p$, *Mathematics of Computation*, vol. 44, number 170, April 1985, pp.483-494.

[51] Shimura, G., *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton University Press, Princeton, 1969.

[52] Sierpinski, W., *Elementary Theory of Numbers*, North-Holland, New York, 1988.

[53] Silverman, J. H., *The Arithmetic of Elliptic Curves*, Springer, New York, 2009.

[54] Sloane, N. J. A., Sequences A000521/M5477, *The On-Line Encyclopedia of Integer Sequences*, http://www.research.att.com/ njas/sequences/.

[55] Somer, J., *Introduction a la Theorie des Nombres Algébriques*, Herman, Paris, 1911.

[56] Steuding, J., *Diophantine Analysis*, Chapman & Hall, Boca Raton, 2005.

[57] Venkov, B. A., *Elementary number theory*, Wolters-Noordhoff, Groningen, 1970.

[58] Washington, L. C., *Elliptic curves - Number theory and cryptography*, Chapman & Hall/CRC, 2008

[59] Watkins, M., Class Numbers of Imaginary Quadratic Fields, *Mathematics of Computation*, vol. 73, number 246, October 2003, pp.907-938.

[60] Weber, H., *Lehrbuck der Algebra*, vol III, Chelsea, New York, 2000.

[61] Weisstein, E. W., *"j-Function"* From MathWorld–A Wolfram Web Resource http://mathworld.wolfram.com/j-Function.html

[62] Yui, N., Zagier, D., On the Singular Values of Weber Modular Functions, *Mathematics of Computation*, vol. 66, n.220, 1997, pp.1645-1662.