The Mazur-Tate pairing and explicit homomorphisms between Mordell-Weil groups of elliptic curves and ideal class groups

Author: Nicolas Simard

Master of Science

Department of Mathematics and Statistics

McGill University

Montreal, Quebec

2014-04-11

Supervisor: Henri Darmon

ACKNOWLEDGEMENTS

I thank Prof. Darmon for his great advice and for the time he spent answering my questions. I would also like to thank Prof. Darmon, the math department of McGill University, the Fonds Québécois de la Recherche sur la Nature et les Technologies (FQRNT) and the Conseil de Recherche en Sciences Naturelles et en Génie (CRSNG) for their financial support during my two years of studies at McGill University. Finally, I thank my family for their constant support.

ABSTRACT

In [Buell(1977)] and [Soleng(1994)], Buell and Soleng found explicit homomorphisms between the Mordell-Weil group of elliptic curves and the ideals class group of quadratic fields, which turn out to be essentially equivalent. After recalling the basic concepts in the theories of quadratic forms, quadratic fields and elliptic curves, we prove that Soleng's homomorphism can be obtained via a height pairing introduced by Mazur and Tate [Mazur and Tate(1983)], under certain conditions. Then the technique developed in the proof of this result is used to find new homomorphisms. Examples of explicit computations of the Mazur-Tate pairing are also given.

ABRÉGÉ

Dans les articles [Buell(1977)] et [Soleng(1994)], Buell et Soleng mettent en évidence des homomorphismes explicites entre le groupe de Mordell-Weil des courbes elliptiques et le groupe des classes d'idéaux des corps quadratiques. Après avoir introduit les théories des formes quadratiques, des corps quadratiques et des courbes elliptiques, il sera démontré que l'homomorphisme de Soleng, qui est essentiellement équivalent à celui de Buell, peut être obtenu à l'aide d'un accouplement de hauteur dû à Mazur et Tate [Mazur and Tate(1983)]. Par la suite, les idées rencontrées dans la preuve de ce résultat seront utilisées pour découvrir de nouveaux homomorphismes. Des exemples de calculs explicites de l'accouplement de Mazur-Tate sont aussi donnés.

TABLE OF CONTENTS

Introduction

The subject of elliptic curves is a fascinating one. A celebrated example of the power of this theory is the proof of Fermat's last theorem in 1995, which relies on an unexpected connection between the hypothetical solutions of the equation $x^n+y^n = z^n$ and a particular family of elliptic curves.

Given an elliptic curve, a central question is to understand and describe explicitly its group of rational points, also called the Mordell-Weil group. In 1922, Mordell proved that this abelian group is finitely generated. The (algebraic) rank of an elliptic curve defined over $\mathbb{Q}$ is defined as the rank of its Mordell-Weil group. Some techniques, based on infinite descent, can be used to compute the Mordell-Weil group. However, it has not been shown yet that these techniques are algorithmic, i.e. that they always end in a finite number of steps. Many important problems in the field, such as the Birch and Swinnerton-Dyer Conjecture, remain unsolved. As another example, it is still not known whether the rank of elliptic curves can be arbitrarily large.

In this thesis, we study homomorphisms between the Mordell-Weil group of elliptic curves and the class group of quadratic fields. It seems that the first illustration of this relation was established in 1976 by Buell. In [Buell(1977)], he describes a natural map between the Mordell-Weil group of certain elliptic curves and groups of binary quadratic forms. This map turned out to be a homomorphism. The proof of this is tedious and uses the language of quadratic forms. In 1992, Soleng found a homomorphism between a subgroup of the Mordell-Weil group of elliptic curves and the ideal class group of quadratic

fields (see [Soleng(1994)]). Unlike Buell, Soleng used the more modern language of ideals to prove that his map was a homomorphism.

As Buell noted in his article, homomorphisms like those introduced above can give valuable information about Mordell-Weil groups. The basic idea is that it is relatively easy to find the order of ideal class groups. Moreover, it is not hard to construct ideal class groups with arbitrarily large 2-rank. If one could find conditions under which these homomorphisms are surjective, it could be possible to obtain information about the rank of elliptic curves.

Around 1982, Mazur and Tate defined their so-called canonical height pairing using the notion of biextensions of abelian varieties (see [Mazur and Tate(1983)]). In a second article (see [Mazur and Tate(1987)]), they define the S-pairing and give explicit formulas to compute it on elliptic curves. Using this S-pairing with a specific choice of S, it is possible to obtain a bilinear pairing between the F-rational points on an elliptic curve and the ideal class group of F, where F is a number field. In this thesis, this pairing is denoted $\langle \cdot, \cdot \rangle : E(F) \times E(F) \longrightarrow \mathrm{Cl}(F)$, where E is an elliptic curve defined over F and $\mathrm{Cl}(F)$ is the class group of F.

More recently in 2009, during a discussion between Bhargava and Darmon, Bhargava mentioned that he had found an explicit homomorphism between the Mordell-Weil group of certain elliptic curves of the form $E_D : \ Y^2 = X^3 - DX$, where D is an integer, and the class group of $\mathbb{Q}(\sqrt{D})$. Darmon believed that this homomorphism might coincide with coincide with the homomorphism $P \longmapsto \langle P, P_0 \rangle : E_D(\mathbb{Q}) \longrightarrow \mathrm{Cl}(\mathbb{Q}(\sqrt{D}))$, where $P_0 = (\sqrt{D}, 0) \in E(\mathbb{Q}(\sqrt{D}))$. This idea is the starting point of this thesis.

In this thesis, it will first be shown that the homomorphisms of Buell and Soleng coincide in most cases. Then it will be proven that Soleng's homomorphism can be obtained via the Mazur-Tate pairing under certain conditions. Since Bhargava's homomorphism

was not published, no explicit description of it is known. However, using the techniques developed to prove the above result, an explicit homomorphism $E_D(\mathbb{Q}) \longrightarrow \mathrm{Cl}(\mathbb{Q}(\sqrt{D}))$ will be described. The techniques will also be used to study an example of homomorphism between the Mordell-Weil group of a particular elliptic curve and the class group of a certain cubic extension. In the last chapter, the injectivity and surjectivity of some of Soleng's homomorphism will be briefly studied.

In the first chapter, the basic theory of integral binary quadratic forms is recalled and Gauss's composition laws are introduced. Then the theory of orders in quadratic fields is presented. Elliptic curves are introduced in the second chapter. The presentation will be very short, but not much of the theory is necessary to understand the results. The next chapter contains a description of Buell and Soleng's homomorphisms. Their relation will also be analysed. The main tool of this work, the Mazur-Tate pairing, is introduced in the fourth chapter. It will not be defined in whole generality, but only for elliptic curves and under a certain conditions. This pairing is used in chapter 5 to prove the main result of this thesis, namely that Soleng's homomorphism can be obtained via the Mazur-Tate pairing. In the next chapter, the pairing is used to obtain what could be Bhargava's homomorphism. Finally, other uses of the pairing and further research directions are presented.

CHAPTER 1
Quadratic forms and quadratic fields

This chapter introduces one of the main concept of this text, namely quadratic fields. Before that, the classical theory of integral binary quadratic forms, as elaborated by Fermat, Lagrange and Gauss is recalled.

1.1 Integral binary quadratic forms

A good reference for this subject is [Flath(1989)].

Definition 1. An integral binary quadratic form f, or quadratic form if there is no risk of confusion, is a polynomial of the form

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

where a, b and c are integers. The discriminant D of f is defined as $D = b^2 - 4ac$. The form f is called positive definite if $D < 0$ and $a > 0$ and negative definite if $D < 0$ and $a < 0$.

A quadratic form f is said to *(properly) represent* an integer n if there exist (coprime) integers x and y such that $f(x,y) = n$. If f is positive definite, it represents only positive integers.

The discriminant of a form f is always congruent to 0 or 1 mod 4. Conversely, given $D \equiv 0, 1 \pmod 4$, the *principal forms*

$$f_D(x,y) = \begin{cases} x^2 - \frac{D}{4}y^2 & \text{if } D \equiv 0 \pmod 4 \\ x^2 + xy + \frac{1-D}{4}y^2 & \text{if } D \equiv 1 \pmod 4 \end{cases} \tag{1.1}$$

have discriminant D. For this reason, the integers congruent to 0 or 1 mod 4 are sometimes called *discriminants*. Of these discriminants, some are important to distinguish.

Definition 2. A discriminant D is called fundamental if it cannot be written as $D = f^2 D_0$, where $f \in \mathbb{Z}$ and $D_0 \equiv 0, 1 \pmod 4$.

It is clear that any square-free discriminant is fundamental. However, the converse is not true since 8 is fundamental, for example. One can still give a simple description of the fundamental discriminants. They are the integers D such that D is congruent to 0 mod 4 and $D/4$ is square-free or D is congruent to 1 mod 4 and D is square-free.

The main question in the theory of quadratic forms is to determine explicitly which integers are properly represented by a given quadratic form. To simplify the question, one introduces an equivalence relation on the set of quadratic forms of discriminant D by letting $\mathrm{GL}_2(\mathbb{Z})$, the group of integral 2×2 matrices with determinant ± 1, act on them as follows: given a matrix $\gamma = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$ and a form $f(x, y) = ax^2 + bxy + cy^2$ of discriminant D, one defines

$$\begin{aligned} \gamma f(x, y) = f(rx + ty, sx + uy) &= a(rx + ty)^2 + b(rx + ty)(sx + uy) + c(sx + uy)^2 \\ &= f(r, s)x^2 + (2(art + csu) + b(st + ru))xy + f(t, u)y^2 \end{aligned}$$

A direct computation shows that this formula defines a group action. In particular, γf has discriminant D. Note also that γf is positive definite whenever f is and both f and γf represent the same integers.

If there exists $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, the group of integral 2×2 matrices with determinant 1, such that $g = \gamma f$, f and g are called *properly equivalent* (not just equivalent). This relation is denoted $f \sim g$. The distinction between equivalent and properly equivalent forms, first introduced by Gauss, is crucial in the theory: it allowed Gauss to define a group law on proper equivalence classes of quadratic forms (see Section 1.2). The proper equivalence class of f is denoted $[f]$. Note that since positive definite forms are in bijection with negative

definite forms and the action of $\mathrm{GL}_2(\mathbb{Z})$ preserves those two sets, it suffices to study positive definite forms.

To determine if a form represents a given integer, one could check if a simpler equivalent form does. This leads us to the theory of reduction.

Definition 3. A quadratic form $f(x,y) = ax^2+bxy+cy^2$ is almost reduced if $|b| \leq |a| \leq |c|$. If f is positive definite, it is reduced if it is almost reduced and $b = a$ in case $|b| = a$ and $b \geq 0$ in case $a = c$.

The term almost reduced is used in [Serre(1999)], but is not common in the literature.

Note that the principal forms introduced above are reduced (when they are positive definite). A basic theorem in the subject is the following.

Theorem 1. *There is a unique reduced form in every proper equivalence class of positive definite quadratic forms.*

Proof. See [Flath(1989), II§8, Theorem 8.7]. □

Given a negative discriminant D, one can easily find the reduced forms by using the following proposition:

Proposition 1. *Let $f(x,y) = ax^2 + bxy + cy^2$ be a positive definite almost reduced form of discriminant D. Then $0 < a \leq \sqrt{|D|/3}$.*

Proof. Since f is almost reduced,

$$4a^2 \leq 4ac = b^2 - D \leq a^2 - D$$

and the result follows. □

It also follows from this proposition that the number of proper equivalence classes of discriminant D is finite. Let us look at two examples.

Example 1. If $D = -4$, every almost reduced positive definite form is such that $0 < a \leq \sqrt{4/3}$. It follows that $a = 1$. Since $|b| \leq 1$ and b has the same parity as D, b has to be zero. Finally, c is determined by the equation $-4 = 0^2 - 4c$. This proves that the principal form $f_{-4}(x, y) = x^2 + y^2$ is the only reduced form of discriminant -4.

Example 2. If $D = -3$, the same argument as above forces a to be 1, but now b can be ± 1. It follows that $x^2 \pm xy + y^2$ are the only positive definite almost reduced forms of discriminant -3. Of these two forms, only the principal form $x^2 + xy + y^2$ is reduced.

The reduction theory of forms that are not definite (these forms are called indefinite) is more sophisticated. The problem is that many almost reduced forms can be properly equivalent and there is no canonical choice of reduced form in the proper equivalence classes. For more detail, see [Flath(1989), IV§6].

1.2 Gauss composition laws

In the previous section, the set of quadratic forms of discriminant D was partitioned into proper equivalence classes. If $D < 0$, the number of classes is easy to compute. Moreover, a canonical representative can be found in each class. Recall also that each equivalence class represents a certain set of integers. The main question is to describe precisely this set of integers. For example, Fermat claimed that the odd primes represented by the quadratic form x^2+y^2 were precisely the primes congruent to 1 mod 4. To determine if an arbitrary integer is represented by $x^2 + y^2$, one uses a reasoning based on the identity

$$(x_1^2 + y_1^2)(x_2^2 + y_2^2) = (x_1y_1 - x_2y_2)^2 + (x_1y_2 + x_2y_1)^2$$

This is an example of a *composition law*. It says that if two integers are represented by x^2+y^2, then so is their product. Gauss generalized this idea to other forms. Before stating his beautiful theorem, one more definition is needed: a form $f(x, y) = ax^2 + bxy + cy^2$ is called *primitive* if $\gcd(a, b, c) = 1$. A proper equivalence class is called *primitive* if it

contains a primitive form. One can see that all the forms in a primitive class are primitive. Then Gauss proved the following theorem.

Theorem 2. *Let D be a fixed non-zero discriminant. There exists a composition law $\circ$ on primitive proper equivalence classes of forms of discriminant D which makes these classes into a group. Moreover, this composition law has the following properties:*

1. *If the class of f_1 represents m and the class of f_2 represents n, then the class $[f_1] \circ [f_2]$ represents mn.*
2. *The identity class is the class containing the principal form of discriminant D.*
3. *The inverse of the class containing the form $ax^2 + bxy + cy^2$ is the class containing the form $cx^2 + bxy + ay^2$.*

When $D > 0$, the group of primitive classes of discriminant D is called the *form class group* and will be denoted $\mathrm{Cl}^*(D)$. When $D < 0$, the form class group $\mathrm{Cl}^*(D)$ is defined as the subgroup of positive definite forms. The order of $\mathrm{Cl}^*(D)$ (which is also finite when $D > 0$) is called the *form class number*. The examples above show that both $\mathrm{Cl}^*(-4)$ and $\mathrm{Cl}^*(-3)$ are trivial.

The simplest way of defining the composition law is probably via Dirichlet's method of *united forms*, described in [Flath(1989), Chapter 5]. To simplify the notation, a quadratic form $f(x, y) = ax^2 + bxy + cy^2$ is denoted (a, b, c) or simply $(a, b, *)$ since c is determined by a, b and D, when $a \neq 0$. Two forms $f_1 = (a_1, b_1, c_1)$ and $f_2 = (a_2, b_2, c_2)$ are called *united* if $a_1 a_2 \neq 0$, $b_1 = b_2$ and $a_1 | c_2$ and $a_2 | c_1$. If f_1 and f_2 are united, $f_1 = (a_1, b, a_2 c)$ and $f_2 = (a_2, b, a_1 c)$, where $b = b_1 = b_2$ and $c = c_1/a_2 = c_2/a_1$. Then Dirichlet defines $[f_1] \circ [f_2] = [(a_1 a_2, b, c)]$. Assuming that this composition law is well-defined, one can verify that it satisfies the properties of Theorem 2. To begin, we can suppose that f_1 and f_2 are united, since the composition law is well-defined. Then the first property follows from the

identity

$$(a_1x_1^2 + bx_1y_1 + a_2cy_1^2)(a_2x_2^2 + bx_2y_2 + a_1cy_2^2) = a_1a_2X^2 + bXY + cY^2,$$

where $X = x_1x_2 - cy_1y_2$ and $Y = a_1x_1y_2 + a_2x_2y_1 + by_1y_2$. For the second property, note that

$$\begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} (a, b, c) = (a, b + 2an, *).$$

If $f = (a, b, c)$ is a quadratic form, this formula implies that $f_D \sim (1, b, *)$, since $b \equiv D \pmod 2$. Now (a, b, c) and $(1, b, *)$ are concordant and $[(a, b, c)] \circ [(1, b, *)] = [(a, b, c)]$. For the last property, let $f = (a, b, c)$ be a quadratic form such that $ac \neq 0$. Then (a, b, c) and (c, b, a) are united and $[(a, b, c)] \circ [(c, b, a)] = [(ac, b, 1)] = [f_D]$.

Dirichlet's composition law is natural in the sense that it leads to a composition law which satisfies the first property on Theorem 2. With this composition law, the inverse of the proper class of (a, b, c) is the proper class of the equivalent form (c, b, a) (they are equivalent via $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$). The reason why it is important to consider proper equivalence classes and not just equivalence classes for composition is apparent: otherwise any proper class would be equivalent to its inverse proper class.

This method of united forms is natural and simple to define, but most modern composition algorithms use Arndt's method. This method can even be generalised to compose forms of different discriminants, under certain conditions. We will follow the description given in [Buell(1977)]. Let f_1 be a primitive form of discriminant D_1 and f_2 be a primitive form of discriminant D_2. Suppose that $D = \gcd(D_1, D_2)$ is a discriminant and that both $|D_1/D|$ and $|D_2/D|$ are perfect squares. For example, $D_1 = -4$ and $D_2 = -16$ satisfy those hypotheses, but not $D_1 = -4$ and $D_2 = 8$. Let $n_i = \sqrt{|D_i/D|}$,

$k = \gcd(a_1 n_2, a_2 n_1, (b_1 n_2 + b_2 n_1)/2)$ and define b to be a solution to

$$kn_i b \equiv kb_1 \pmod{2a_i}$$

$$k(b_1 n_2 + b_2 n_1)b \equiv k(b_1 b_2 + D n_1 n_2) \pmod{4a_1 a_2}.$$

Then $f_1 \circ f_2 = (a, b, (b^2 - D)/(4a))$, where $a = a_1 a_2 / k^2$. Note that here the forms themselves are composed, whereas before the equivalence relation was needed to find united forms. Nevertheless, this composition law is well-defined on classes. Note also that $f_1 \circ f_2$ has discriminant D. If $D = D_1 = D_2$, this composition law is the same as Dirichlet's. Arndt's method has important properties.

1. Let D be a discriminant and let $D' = f^2 D$. For any primitive class $C \in \mathrm{Cl}^*(D)$, we have that $C_{D'} \circ C = C$, where $C_{D'}$ is the identity class of $\mathrm{Cl}^*(D')$.
2. Using the notation of the previous point, the map from $\mathrm{Cl}^*(D')$ to $\mathrm{Cl}^*(D)$ sending C' to $C' \circ C_D$ is a surjective homomorphism.

Those properties are easier to understand in the modern language of ideal and orders, which we will recall in the next section. Arndt's generalised composition laws and their properties are needed to define Buell's homomorphism.

1.3 Quadratic fields

In this section, we recall some basic concepts in the algebraic theory of quadratic fields. A good reference for this material is [Cox(1989), II].

1.3.1 Orders in quadratic fields

For the rest of this text, K will be a quadratic field and $\mathcal{O}_K$ will be its ring of integers.

Definition 4. An order $\mathcal{O}$ is a subring of K containing 1 and having the following properties:

1. $\mathcal{O}$ is a finitely generated $\mathbb{Z}$-module;
2. $\mathcal{O}$ contains a $\mathbb{Q}$-basis for K, i.e. $\mathbb{Q} \otimes \mathcal{O} = K$;

An order in a quadratic field is necessarily free of rank 2 as a $\mathbb{Z}$-module. Since the elements of an order are integral over $\mathbb{Z}$, every order is contained in $\mathcal{O}_K$. The index of an order $\mathcal{O}$ in $\mathcal{O}_K$ is called the *conductor* of $\mathcal{O}$ and is denoted f.

Now suppose that $K = \mathbb{Q}(\sqrt{d})$, where d is an integer, and write $d = \ell^2 d_0$ with d_0 square-free. Then

$$\mathcal{O}_K = [1, \omega],$$

where

$$\omega = \begin{cases} \sqrt{d_0} & \text{if } d_0 \not\equiv 1 \pmod 4 \\ \frac{1+\sqrt{d_0}}{2} & \text{if } d_0 \equiv 1 \pmod 4 \end{cases}$$

and the square brackets mean that $\mathcal{O}_K$ is generated by 1 and ω as a $\mathbb{Z}$-module. With this notation, one can prove that if $\mathcal{O}$ is an order of conductor f in K, then $\mathcal{O} = [1, f\omega]$. In particular, there is a unique order of conductor f in K for any $f \geq 1$. As for the maximal order, the discriminant of an order can be defined. Using the $\mathbb{Z}$-basis $\{1, f\omega\}$ for $\mathcal{O}$, one sees that $\mathcal{O}$ has discriminant $f^2 d_0$ if $d_0 \equiv 1 \pmod 4$ and $4f^2 d_0$ if $d_0 \not\equiv 1 \pmod 4$. A more enlightening way of stating this result is to say that $\mathcal{O}$ has discriminant $f^2 D_K$, where D_K is the discriminant of K. The reader may have noticed at this point that the fundamental discriminants introduced in the first section correspond precisely to the discriminants of quadratic fields. For simplicity, let $\omega_f = f\omega$, so that $[1, \omega_f]$ is the order of conductor f in K.

1.3.2 Ideals in quadratic fields

It is sometimes useful to consider ideals as $\mathbb{Z}$-modules and a $\mathbb{Z}$-basis for a $\mathbb{Z}$-module I is denoted with square brackets. The following theorem characterises ideals in orders:

Theorem 3 (Ideal Criterion)**.** *Let I be a non-zero ideal in the order $\mathcal{O}$ of conductor f in K. Then I is of the form $I = [a, b + c\omega_f]$, where $a, b, c \in \mathbb{Z}$ are such that $c|a, b$ and*

$ac|N(b+c\omega_f)$. Conversely, every $\mathbb{Z}-$module of the form $[a, b+c\omega_f]$, where $a, b, c \in \mathbb{Z}$ are such that $c|a, b$ and $ac|N(b+c\omega_f)$, is an ideal in $\mathcal{O}$.

Proof. First, we prove that I can be put it the desired form. If I is not the zero ideal, it contains an element $x \neq 0$ and so it contains the integer $N(x)$. Then the natural surjective homomorphism $\mathcal{O} \longrightarrow \mathcal{O}/I$ factors through $N(x)\mathcal{O}$ and since $\mathcal{O}/N(x)\mathcal{O}$ has finite order $N(x)^2$, I has finite index in $\mathcal{O}$. In particular, I must be a free $\mathbb{Z}$-module of rank 2. Write $I = [\alpha_1, \alpha_2]$, where $\alpha_1 = x_1 + y_1\omega_f, \alpha_2 = x_2 + y_2\omega_f \in A$. Then for any $k \in \mathbb{Z}$, $\{\alpha_1 - k\alpha_2, \alpha_2\}$ and $\{\alpha_1, \alpha_2 - k\alpha_1\}$ are also $\mathbb{Z}-$basis for I. It follows that the Euclidean algorithm can be performed on y_1 and y_2 and so I can be written as $I = [a, b+c\omega_f]$, where $c = \gcd(y_1, y_2)$.

The rest of the theorem follows from the identities

$$-a\omega_f = \frac{b}{c}a - \frac{a}{c}(b+c\omega_f),$$

$$(b+c\omega_f)\omega_f = \begin{cases} -a\frac{N(b+c\omega_f)}{ac} + \frac{b}{c}(b+c\omega_f) & \text{if } D_0 \not\equiv 1 \pmod 4 \\ -a\frac{N(b+c\omega_f)}{ac} + \frac{b+c}{c}(b+c\omega_f) & \text{if } D_0 \equiv 1 \pmod 4 \end{cases}$$

and the fact that I is a *free* $\mathbb{Z}-$module. □

Some care must be taken when searching for a $\mathbb{Z}$-basis for an ideal. For example, if $d_0 \equiv 1 \pmod 4$ the $\mathbb{Z}$-module $[a, \sqrt{d_0}]$ is not an ideal in $\mathcal{O}_K = [1, (1+\sqrt{d_0})/2]$ whenever $a|d_0$. However, $(a, \sqrt{d_0})$ is an ideal in $\mathcal{O}_K$, by definition.

1.3.3 Norm of ideals

The main tool that will be used in the explicit computations is the norm. There are at least three definitions of the norm of an ideal. They coincide most of the time. In this section, E/L will be an extension of number fields and $\mathcal{O}_E$ and $\mathcal{O}_L$ will be their ring of integers, respectively. Our first definition of the norm is the following.

Definition 5. Let $\mathfrak{a}$ be an integral ideal in $\mathcal{O}_E$. The norm of $\mathfrak{a}$, denoted $N_{E/L}(\mathfrak{a})$, is defined as the integral $\mathcal{O}_L$-ideal generated by the norm of the elements of $\mathfrak{a}$, i.e. $N_{E/L}(\mathfrak{a}) = (N_{E/L}(a)|a \in \mathfrak{a})$.

This definition is very simple and elegant, but not suitable for computations, so an equivalent definition must be found. First, one can show that this norm is multiplicative. Using this property, it suffices to determine $N_{E/L}(\mathfrak{P})$ for all primes $\mathfrak{P}$ of $\mathcal{O}_E$ to know the norm of all the ideals of $\mathcal{O}_E$.

Proposition 2. *Using the notation above,*

$$N_{E/L}(\mathfrak{P}) = \mathfrak{p}^{f(\mathfrak{P}/\mathfrak{p})},$$

where $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_L$ *and* $f(\mathfrak{P}/\mathfrak{p})$ *is the residue class degree.*

Proof. See [Janusz(1996), I§8, Proposition 8.4]. □

This result allows us to extend the norm to a function on the whole ideal group

$$N_{E/L} : I_E \longrightarrow I_L$$

by letting $N_{E/L}(\mathfrak{P}) = \mathfrak{p}^{f(\mathfrak{P}/\mathfrak{p})}$ and extending multiplicatively. This is sometimes taken as the definition of the norm.

One would like the norm to measure, in some sense, the size of the ideals. If $\mathcal{O}$ is an order in E and $\mathfrak{a}$ is an ideal in $\mathcal{O}$, the *numerical norm*, denoted $\mathbb{N}(\mathfrak{a})$, is defined as index of $\mathfrak{a}$ in $\mathcal{O}$, i.e. $\mathbb{N}(\mathfrak{a}) = (\mathcal{O} : \mathfrak{a})$. When $\mathfrak{a}$ is not the zero ideal, $\mathbb{N}(\mathfrak{a})$ is finite (the proof of this is similar to the argument given in the proof of Theorem 3). One can show that

Proposition 3. *Using the notation above,*

$$N_{E/\mathbb{Q}}(\mathfrak{a}) = \mathbb{N}(\mathfrak{a})\mathbb{Z}.$$

Proof. See [Milne(2012), Proposition 4.2]. □

Note that the numerical norm makes sense in any order, not just the maximal order. The norm has a few important properties.

Proposition 4. *Let $\mathfrak{a}$ and $\mathfrak{b}$ be fractional $\mathcal{O}_E$-ideals, $\mathfrak{c}$ be an integral $\mathcal{O}_L$-ideal and x be any element in E. Then the norm function has the following properties:*

1. $N_{E/L}(\mathfrak{ab}) = N_{E/L}(\mathfrak{a})N_{E/L}(\mathfrak{b})$.
2. $N_{E/L}(\mathfrak{c}\mathcal{O}_E) = \mathfrak{c}^{[E:L]}$.
3. $N_{E/L}(x\mathcal{O}_E) = N_{E/L}(x)\mathcal{O}_L$.
4. *if E/L is Galois with Galois group G and $\mathfrak{P}$ is a prime of E, then*

$$N_{E/L}(\mathfrak{P})\mathcal{O}_E = \prod_{\sigma \in G} \sigma\mathfrak{P}.$$

Proof. The first property follows from the definition. For the other properties, see [Milne(2012), Proposition 4.1]. □

Now there is the question of effectively computing this norm, at least for ideals in quadratic fields K. To this end, the following result can be useful.

Proposition 5. *Let $I = [a, b + c\omega_f]$ be an ideal in the order $\mathcal{O}$ of conductor f in K. Then $\mathbb{N}(I) = ac$.*

Proof. This follows from the fact that $\mathbb{N}(I) = (\mathcal{O} : I)$. □

This result is easy to apply, but an integral basis for I is needed. The following result is not as easy to use, but it can be applied to any ideal in the maximal order of a quadratic number field:

Proposition 6. *Let $\mathfrak{a} = (\alpha, \beta)$ be an integral $\mathcal{O}_K$-ideal. Then*

$$\mathbb{N}(\mathfrak{a}) = \gcd(N(\alpha), Tr(\alpha\overline{\beta}), N(\beta)).$$

Proof. See [Conrad(2014), Theorem 5.6]. □

1.3.4 Ideal class group of orders in quadratic fields

A fractional ideal of $\mathcal{O}$ is a finitely generated $\mathcal{O}$-module contained in K. It is not hard to see that $\mathfrak{a}$ is a fractional ideal of $\mathcal{O}$ if and only if $\alpha\mathfrak{a}$ is an ordinary ideal of $\mathcal{O}$ for some $\alpha \in K$.

Definition 6. Let $\mathfrak{a}$ be a fractional ideal of an order $\mathcal{O}$ in K. Then $\mathfrak{a}$ is a *proper $\mathcal{O}$-ideal* if $\mathcal{O} = \{\alpha \in K : \alpha\mathfrak{a} \subseteq \mathfrak{a}\}$. The set of proper ideals of $\mathcal{O}$ is denoted $I(\mathcal{O})$.

Note that if $\mathfrak{a}$ is a fractional $\mathcal{O}$-ideal, $\{\alpha \in K : \alpha\mathfrak{a} \subseteq \mathfrak{a}\}$ is always an order of K which contains $\mathcal{O}$. If this order properly contains $\mathcal{O}$, the ideal comes from a larger order and it is not proper by definition. The main result for these ideals is the following:

Theorem 4. *Let $\mathcal{O}$ be an order of K. Then $I(\mathcal{O})$ is a group under multiplication.*

Proof. The only difficulty is to prove that proper ideals are invertible. See [Cox(1989), Proposition 7.4] for a proof of this. □

One can verify that the principal $\mathcal{O}$-ideals form a subgroup of $I(\mathcal{O})$, denoted $P(\mathcal{O})$. The quotient

$$\mathrm{Cl}(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O})$$

is called the *ideal class group* of the order $\mathcal{O}$. Of course, $\mathrm{Cl}(\mathcal{O}_K) = \mathrm{Cl}(K)$ is the usual ideal class group of K, since all $\mathcal{O}_K$-ideals are proper. Since the orders in quadratic fields are in bijection with discriminants (i.e. integers congruent to 0 or 1 mod 4), $\mathrm{Cl}(\mathcal{O})$ can also be denoted $\mathrm{Cl}(D)$, where D is the discriminant of $\mathcal{O}$.

An integral ideal $\mathfrak{a}$ in an order $\mathcal{O}$ of conductor f is *prime to the conductor* if $\mathfrak{a}+f\mathcal{O} = \mathcal{O}$. One can show that these ideals are proper and form a subgroup of $I(\mathcal{O})$, denoted $I(\mathcal{O}, f)$. If $P(\mathcal{O}, f)$ denotes the group of principal fractional $\mathcal{O}$-ideals generated by the elements of $\mathcal{O}$ of norm prime to f, one can prove the following theorem.

Theorem 5. *Let $\mathcal{O}$ be the order of conductor f in K, then*

$$I(\mathcal{O}, f)/P(\mathcal{O}, f) \cong I(\mathcal{O})/P(\mathcal{O})$$

.

Proof. The idea of the proof is that any ideal class in $\mathrm{Cl}(\mathcal{O})$ contains an ideal prime to f. See [Cox(1989), Proposition 7.19]. □

One can also show that an ideal in an order of conductor f is prime to the conductor if and only if its norm is prime to f.

Theorem 6. *Let $\mathcal{O}$ be the order of conductor f in K.*

1. *Let $\mathfrak{a}$ be an ideal of $\mathcal{O}_K$ prime to f. Then $\mathfrak{a} \cap \mathcal{O}$ is an ideal of $\mathcal{O}$ of the same norm.*
2. *Let $\mathfrak{a}$ be an ideal of $\mathcal{O}$ prime to f. Then $\mathfrak{a}\mathcal{O}_K$ is an ideal of $\mathcal{O}_K$ of the same norm.*
3. *The map $\mathfrak{a} \mapsto \mathfrak{a} \cap \mathcal{O}$ induces an isomorphism $I(\mathcal{O}_K, f) \to I(\mathcal{O}, f)$, and the inverse of this map is given by $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_K$.*

Proof. See [Cox(1989), Proposition 7.20]. □

This gives a way to go from the ideals of $\mathcal{O}_K$ prime to f to the ideals of $\mathcal{O}$ prime to f.

1.3.5 Factorisation of ideals in quadratic fields

As before, let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field, where $d = \ell^2 d_0$ and d_0 is square-free. Let also $\mathcal{O}_K$ be the ring of integers of K. One of the basic results of algebraic number theory says that any non-zero integral $\mathcal{O}_K$-ideal $\mathfrak{a}$ can be written uniquely as

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\alpha_{\mathfrak{p}}}, \tag{1.2}$$

where the product runs over the prime ideals of $\mathcal{O}_K$ and where each $\alpha_{\mathfrak{p}}$ is non-negative. One can also show that the ideal group $I(\mathcal{O}_K)$ (also denoted I_K) is the free abelian group

generated by the primes ideals of $\mathcal{O}_K$. Similarly, $I(\mathcal{O}_K, f)$ is the free abelian group generated by the prime ideals which are prime to f (i.e. the prime ideals $\mathfrak{p}$ such that $p \nmid f$ if $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$). It follows that any fractional $\mathcal{O}_K$-ideal admits a unique decomposition as above, where the exponent can be negative.

In quadratic fields, the splitting behaviour of rational primes is related to the Legendre symbol.

Proposition 7. *Let p be a prime in $\mathbb{Z}$. Then $p\mathcal{O}_K$ factors as follows:*

1. *If $p = 2$, then*

$$2\mathcal{O}_K = \begin{cases} \left(2, \sqrt{d_0}\right)^2 & \text{if } d_0 \equiv 0 \pmod 2 \\ \left(2, 1 + \sqrt{d_0}\right)^2 & \text{if } d_0 \equiv 3 \pmod 4 \\ \left(2, (1 + \sqrt{d_0})/2\right)\left(2, (1 - \sqrt{d_0})/2\right) & \text{if } d_0 \equiv 1 \pmod 8 \\ \text{prime} & \text{if } d_0 \equiv 5 \pmod 8 \end{cases}$$

2. *If p is odd, then*

$$p\mathcal{O}_K = \begin{cases} \left(p, \sqrt{d_0}\right)^2 & \text{if } d_0 \equiv 0 \pmod p \\ \left(p, n + \sqrt{d_0}\right)\left(p, n - \sqrt{d_0}\right) & \text{if } d_0 \equiv n^2 \not\equiv 0 \pmod p \\ \text{prime} & \text{if } d_0 \text{ is not a square} \mod p \end{cases}$$

Proof. See [Cox(1989), Proposition 5.6]. □

1.4 Correspondence between forms and ideals

A well-known result in the theory of quadratic fields says that there is a correspondence between the form class group of discriminant D and the narrow-class group of the order of discriminant D. A precise description of this correspondence is given in this section.

Definition 7. Let $\mathcal{O}$ be an order in a quadratic field and let $P^+(\mathcal{O})$ be the group of ideals generated by the principal ideals $\alpha\mathcal{O}$, where $N(\alpha) > 0$. Then the quotient

$$I(\mathcal{O})/P^+(\mathcal{O})$$

is called the narrow-class group and is denoted $\mathrm{Cl}^+(\mathcal{O})$ (or $\mathrm{Cl}^+(D)$ if $\mathcal{O}$ has discriminant D).

In quadratic fields, $N(\alpha) > 0$ if and only if α is totally positive, i.e. α is positive under every real embedding of K. When K is imaginary, $N(\alpha) > 0$ for every $\alpha \in K^\times$, so $\mathrm{Cl}^+(\mathcal{O}) = \mathrm{Cl}(\mathcal{O})$ in this case. If K is real, the same is true if there is an element with norm equal to -1. This is equivalent to saying that the fundamental unit of K has norm equal to -1. Finally, if K is real and the fundamental unit has positive norm, the narrow-class group is not isomorphic to the class group, but $[\mathrm{Cl}^+(\mathcal{O}) : \mathrm{Cl}(\mathcal{O})] = 2$.

Theorem 7. *Let D be a non-square discriminant. Then the form class group of discriminant D is isomorphic to the narrow-class group of discriminant D:*

$$Cl^*(D) \cong Cl^+(D).$$

Proof. See [Cox(1989), Theorem 7.7 and Exercises 7.12,7.17]. □

The isomorphism of the theorem is fairly simple. First, let D be a negative discriminant and let $f(x, y) = ax^2 + bxy + cy^2$ be a positive definite quadratic form of discriminant D. Then the isomorphism sends the class of f to the (narrow) class of the ideal

$$[a, (-b + \sqrt{D})/2].$$

The inverse map is defined as follows: let $\mathfrak{a} = [\alpha, \beta]$ be a proper ideal of the order of discriminant D and suppose that $\Im(\beta/\alpha) > 0$. Then the inverse map sends $\mathfrak{a}$ to the class

of

$$\frac{N(\alpha x - \beta y)}{\mathbb{N}(\mathfrak{a})}.$$

Now let D be a positive non-square discriminant and let $f(x, y) = ax^2 + bxy + cy^2$ be a quadratic form of discriminant D. Then the isomorphism sends the class of f to the class of the ideal

$$[a, a\tau],$$

where $\tau = r + s\sqrt{D}$ is such that $f(\tau, 1) = 0$ and $\mathrm{sgn}(s) = \mathrm{sgn}(a)$. The inverse map sends the proper ideal $\mathfrak{a} = [\alpha, \beta]$ of the order of discriminant D to the form

$$\frac{N(\alpha x - \beta y)}{\mathbb{N}(\mathfrak{a})}.$$

An important part in the proof of Theorem 7 is the proof that the maps given above are well-defined on classes. One also needs to check that the form corresponding to an ideal is primitive and of the right discriminant. Similarly, one needs to show that the ideal corresponding to a form is proper. Needless to say that this proof is tedious!

CHAPTER 2
Elliptic curves

Let F be a perfect field. The main reference in this chapter is [Silverman(2009)]

Definition 8. An elliptic curve is a pair $(E, 0)$ where E is a smooth projective curve of genus one and 0 is a point on E. The elliptic curve is defined over F, written E/F, if E is defined over F as a curve and $0 \in E(F)$. We generally denote the elliptic curve by E, the point 0 being understood.

Using the Riemann-Roch theorem, one can show that any elliptic curve E is isomorphic to a plane cubic of the form

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

where $a_i \in F$ if E is defined over F. When E is written in this form, the distinguished point is $[0, 1, 0]$. The affine part

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \tag{2.1}$$

is called the *Weierstrass equation* of E. The only point of E missing in this affine curve is $0 = [0, 1, 0]$. For this reason, 0 is called the *point at infinity*.

When $\mathrm{char}(F) \neq 2$, the Weierstrass equation can be put in the form

$$Y^2 = X^3 + a_2'X^2 + a_4'X + a_6'$$

by doing a change of variales. If $\mathrm{char}(F) \neq 2, 3$, the x^2 term can also be eliminated, which gives an equation of the form

$$Y^2 = X^3 + AX + B. \tag{2.2}$$

To each Weierstrass equation for E, one associates the following quantities:

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

$$\begin{aligned} b_8 &= a_1^2 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\ c_4 &= b_2^2 - 24b_4, \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6 \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6. \end{aligned}$$

In the case where $a_1 = a_2 = a_3 = 0$, these quantities simplify to

$$b_2 = 0, \qquad b_4 = 2a_4, \qquad b_6 = 4a_6,$$

$$\begin{aligned} b_8 &= -a_4^2, \\ c_4 &= -2^4 3a_4 \\ c_6 &= -2^5 3^3 a_6 \\ \Delta &= -16\left(4a_4^3 + 27a_6^2\right). \end{aligned}$$

What makes elliptic curves so special is that the points of $E(F)$ can be added: given two points P_1 and P_2 in $E(F)$, a third point $P_1 + P_2$ can be found and with this operation, $E(F)$ is an abelian group.

To define this operation, we consider the set $E(\mathbb{R})$. For simplicity, suppose that the points P_1 and P_2 are distinct. If they lie on the same vertical line, their sum is defined to be 0. Otherwise, consider the line joining the two points. In general, this line will intersect

the curve in three points: P_1, P_2 and a third point, which is denote $P_1 * P_2$. Then $P_1 + P_2$ is defined to be the reflection of $P_1 * P_2$ about the x-axis. It can be shown that this makes $E(\mathbb{R})$ into an abelian group, where the identity is the point at infinity. The hard part is to show that the operation is associative.

To define the operation in arbitrary fields, one first finds explicit formulas for the operation defined above. Since these formulas make sense over any field, they can be used to define a group operation on $E(F)$. In particular, the formula for the x-coordinate of $P_1 + P_2$, where $P_1 \neq \pm P_2$, will be used later. If $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ are in $E(F)$, the formula is

$$x(P_1 + P_2) = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 + a_1 \left(\frac{y_2 - y_1}{x_2 - x_1}\right) - a_2 - x_1 - x_2. \tag{2.3}$$

A natural question is to ask about the nature of the group $E(F)$. Is it finite? Is it finitely generated as a $\mathbb{Z}$-module? In general, it is hard to answer those questions. However, when F is a number field, the Mordell-Weil gives important information about $E(F)$.

Theorem 8 (Mordell-Weil)**.** *Let F be a number field, and let E/F be an elliptic curve. Then $E(F)$ is finitely generated as an abelian group.*

Proof. See [Silverman(2009), VIII§6, Theorem 6.7]. □

It follows that if F is a number field,

$$E(F) \cong E_{\text{tors}}(F) \oplus \mathbb{Z}^r$$

for some non-negative integer r and finite group $E_{\text{tors}}(F)$. The integer r is called the rank of E. For the moment, no algorithm to compute the rank is known. As mentioned in the introduction, the most efficient general approach to calculate the Mordell-Weil group is based on Fermat's method of infinite descent, but it has not been proven yet that these methods will always terminate in a finite number of steps.

CHAPTER 3
The Homomorphisms of Buell and Soleng

In this chapter, the homomorphisms of Buell and Soleng are presented and compared. Since the first uses the language of quadratic forms and the second uses the language of ideals, the correspondence introduced in the first chapter will be used.

3.1 Buell's homomorphism

We follow the introduction of Buell's article [Buell(1977)]. Let a, b and c be integers and let D be a fundamental discriminant (see definition 2). Let E be an elliptic curve of the form

$$E: \ Y^2 = 4(X+a)(X^2+bX+c) + D. \tag{3.1}$$

Then any rational point in E is of the form $P = \left(\frac{A}{C^2}, \frac{B}{C^3}\right)$, where $\gcd(A, C) = 1$ and $\gcd(B, C) \leq 2$. If $D < 0$, assume also that $A + a$ and $A^2 + bA + c$ are both positive (note that they must be of the same sign). Since $P \in E(\mathbb{Q})$, it satisfies the equation

$$B^2 = 4(A + aC^2)(A^2 + bC^2A + cC^4) + C^6D$$

and so the quadratic form $f_P = (A + aC^2, B, A^2 + bC^2A + cC^4)$ has discriminant C^6D and is positive definite if $D < 0$. If C_D denotes the identity class of $\mathrm{Cl}^*(D)$, composition with C_D is a homomorphism from the form class group of discriminant $(C^3)^2D$ to the form class group of discriminant D (see Chapter 1). Therefore a function $\phi : E(\mathbb{Q}) \longrightarrow \mathrm{Cl}^*(D)$ can be defined by sending P to $[f_P] \circ C_D$. The whole point of Buell's article is to prove that ϕ is a homomorphism.

Buell mentions at the end of his article that his results may be extended to non-fundamental discriminants. However, he admits that he has not been able to do it. He also points out the importance of analysing the surjectivity of the homomorphism, because this could help us find elliptic curves of high rank.

3.2 Soleng's homomorphism

Here we follow the introduction of Soleng's article [Soleng(1994)]. Letting (x, y) be a rational point on the elliptic curve

$$E: \ Y^2 = X^2 + a_2X^2 + a_4X + a_6$$

defined over $\mathbb{Q}$, Soleng notes that

$$y^2 - (x+n)(n^2 - (a_2+x)n + x^2 + a_2x + a_4) = -n^3 + a_2n^2 - a_4n + a_6 \qquad (3.2)$$

for any integer n. Multiplying this equation by 4, he then notes that the quadratic form

$$(x+n)X^2 + 2yXY + (n^2 - (a_2+x)n + x^2 + a_2x + a_4)Y^2$$

has discriminant $4(-n^3 + a_2n^2 - a_4n + a_6)$ (this quadratic form is not necessarily integral, however). This establishes a relation between elliptic curves and quadratic forms.

Soleng's homomorphism is not defined on the whole group $E(\mathbb{Q})$, but on the subgroup of *primitive points* of $E(\mathbb{Q})$, which is defined as follows.

Definition 9. Let E be an elliptic curve whose Weierstrass equation

$$E: \ Y^2 = X^2 + a_2X^2 + a_4X + a_6$$

has coefficients in $\mathbb{Z}$. Then a point $P = (A/C^2, B/C^3)$ in $E(\mathbb{Q})$, where $\gcd(A, C) = \gcd(B, C) = 1$, is primitive if $\gcd(A, 2B, A^2 + a_2AC^2 + a_4C^4)$.

It is not clear at first sight, but the set of primitive points of $E(\mathbb{Q})$ is a group. For a proof of this, see [Soleng(1994), Proposition 2.1].

Now let $P = (A/C^2, B/C^3)$ be a primitive point in $E(\mathbb{Q})$. Then (A, B) is an integral point on the curve $Y^2 = X^3 + a_2C^2X^2 + a_4C^4X + a_6C^6$. Soleng associates this point with the ideal $[A, -B + \sqrt{C^6a_6}] = [A, -B + C^3\sqrt{a_6}]$ in the order $\mathbb{Z}[C^3\sqrt{a_6}]$. This ideal is proper and so it defines a class in $\mathrm{Cl}(\mathbb{Z}[C^3\sqrt{a_6}])$. In general, the ideals associated with different points will be in different orders, so he composes with $[1, \sqrt{a_6}]$ to obtain an ideal in $\mathrm{Cl}(\mathbb{Z}[\sqrt{a_6}])$. A short computation shows that $[A, -B+C^3\sqrt{a_6}][1, \sqrt{a_6}] = [A, -kB + \sqrt{a_6}]$, where $kC^3 \equiv 1 \pmod{A}$. This defined a map $E_{\mathrm{prim}}(\mathbb{Q}) \longrightarrow \mathrm{Cl}(\mathbb{Z}[\sqrt{a_6}])$, where $(A/C^2, B/C^3)$ is sent to $[A, -kB+\sqrt{a_6}]$. Soleng shows in his article that this defines a homomorphism.

3.3 Correspondence between the two homomorphisms

The two homomorphisms are described using different theories, but as we saw in the first chapter, these theories are equivalent in many cases. One could think that the two homomorphisms are equal whenever a_6 is a fundamental discriminant. However, this is not exactly the case. In this section, the relation between the two functions is analysed.

An important point to make here is that both homomorphisms depend on the choice of Weierstrass equation. For instance, the elliptic curves $E: \ Y^2 = X^3 + a_4X + a_6$ and $E': \ Y^2 = X^3+16a_4X+64a_6$ are isomorphic over $\mathbb{Q}$, but a primitive point in $E(\mathbb{Q}) = E'(\mathbb{Q})$ can be mapped to an ideal in $\mathrm{Cl}(\mathbb{Z}[\sqrt{a_6}])$ or $\mathrm{Cl}(\mathbb{Z}[8\sqrt{a_6}])$, depending on the equation that is chosen. Therefore, some care must be taken when comparing the two homomorphisms.

Suppose that D is an even and negative fundamental discriminant. Then $D = 4a_6$, where a_6 is negative, square-free and congruent to 2 or 3 mod 4. In this case, all points of $E(\mathbb{Q})$ are primitive.

Lemma 1. *Let E be an elliptic curve defined by the equation*

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

where a_6 is square-free and congruent to 2 or 3 mod 4. Then $E_{prim}(\mathbb{Q}) = E(\mathbb{Q})$.

Proof. Let $P = (A/C^2, B/C^3)$ be a point on E, where $\gcd(A, C) = \gcd(B, C) = 1$. Then A, B and C satisfy the equation

$$B^2 = A(A^2 + a_2C^2A + a_4C^4) + a_6C^6.$$

Suppose that an odd prime p divides $\gcd(A, 2B, A^2 + a_2AC^2 + a_4C^4)$. Then p divides $A, A^2 + a_2AC^2 + a_4C^4$ and B so p^2 divides a_6, a contradiction. Similarly, if 2 divides $\gcd(A, 2B, A^2 + a_2AC^2 + a_4C^4)$, then A and $A^2 + a_2AC^2 + a_4C^4$ are even, so a_4 is even and $B^2 \equiv a_6 \pmod 4$, a contradiction. □

Now let $P = (x, y)$ be a (primitive) point on the elliptic curve

$$E:\ Y^2 - X(X^2 + a_2X + a_4) = a_6.$$

Then $P' = (x, 2y)$ is a point on the curve

$$E':\ Y^2 - 4X(X^2 + a_2X + a_4) = D.$$

Writing $P = (A/C^2, B/C^3)$, it follows that $P' = (A/C^2, 2B/C^3)$. Then Soleng's homomorphism sends P to the ideal $[A, -B + C^3\sqrt{a_6}]\mathbb{Z}[\sqrt{a_6}]$. On the other hand, Buell's map sends P' to the quadratic form

$$(A, 2B, A^2 + a_2C^2A + a_4C^4) \circ C_D$$

of discriminant D, where C_D is the identity class of discriminant D. Using the correspondence between quadratic forms and ideals for negative discriminant, the quadratic form

$(A, 2B, A^2 + a_2C^2A + a_4C^4)$ corresponds to the ideal $[A, \frac{-2B+\sqrt{C^6D}}{2}] = [A, -B + C^3\sqrt{a_6}]$. Since the following diagram commutes

$$\begin{array}{ccc} \mathrm{Cl}(\mathbb{Z}[\sqrt{C^6a_6}]) & \xrightarrow{\cdot\mathbb{Z}[\sqrt{a_6}]} & \mathrm{Cl}(\mathbb{Z}[\sqrt{a_6}]) \\ \sim\uparrow & & \sim\uparrow \\ \mathrm{Cl}^*(C^6D) & \xrightarrow{\circ f_D} & \mathrm{Cl}^*(D) \end{array},$$

it follows that this diagram commutes:

$$\begin{array}{ccc} E(\mathbb{Q}) & \xrightarrow{\text{Soleng}} & \mathrm{Cl}(\mathbb{Z}[\sqrt{a_6}]) \\ \sim\uparrow & & \sim\uparrow \\ E'(\mathbb{Q}) & \xrightarrow{\text{Buell}} & \mathrm{Cl}^*(D) \end{array}.$$

This proves that in the case where D is an even and negative fundamental discriminant, the two homomorphisms are equivalent in a natural way.

Suppose now that D is a negative fundamental discriminant, but that it is odd (e.g. $D = -3$). In this case, the form class group and the ideal class group are isomorphic. However, Soleng's homomorphism lands in the class group of an order that is not maximal. Since the two homomorphisms have image in groups that are not necessarily isomorphic, I would not say that they are equivalent.

Suppose now that D is a positive discriminant. Then the form class group of discriminant D is isomorphic to the narrow-class group of the order of discriminant D. In general, these groups are not isomorphic. Again, I would not say that the homomorphisms are equivalent in this case.

To conclude, the idea and motivation behind the two homomorphisms are the same. In both cases, they essentially come from the basic identity $Y^2 - X(X^2 + a_2X + a_4) = a_6$ (modulo a factor of 4). The main difference is that Buell's homomorphism has image in the form class group of a fundamental discriminant. Soleng removes the condition that the discriminant is fundamental, but his homomorphism is restricted to primitive points.

Moreover, Soleng's homomorphism never lands in the class group of the order $\mathbb{Z}[(1+\sqrt{D})/2]$ (the maximal order of $\mathbb{Q}(\sqrt{D})$ when $D \equiv 1 \pmod 4$), whereas Buell's homomorphism can.

CHAPTER 4
The Mazur-Tate Canonical Height Pairing

The Mazur-Tate pairing was first introduced in [Mazur and Tate(1983)]. In a second article [Mazur and Tate(1987)], Mazur and Tate gave a method to compute the pairing on elliptic curves. Before presenting it, local fields and valuations in quadratic fields will be discussed. Then the notion of minimal Weierstrass equations will be introduced.

4.1 Local fields and valuations on quadratic fields

Let F be a field. An *absolute value* on F is a function $|\cdot| : F \longrightarrow \mathbb{R}$ satisfying the following three properties:

1. $|x| > 0$, for all $x \in F$, except that $|0| = 0$.
2. $|xy| = |x||y|$, for all $x, y \in F$.
3. $|x + y| \leq |x| + |y|$, for all $x, y \in F$.

If the stronger condition $|x + y| \leq \max\{|x|, |y|\}$ holds, the absolute value is called *nonarchimedian.*

Definition 10. A *local field* is a field which is complete with respect to an absolute value and locally compact with respect to the topology induced by this absolute value.

Definition 11. A *place* or *prime* of F, denoted ν, is an equivalence class of absolute values on F.

From now on, let F is a number field. In this case, there is exactly one place of F

- for each prime ideal,
- for each real embedding,
- for each pair of complex conjugate embeddings

and the completion of F at ν, denoted F_ν, is a local field. The primes corresponding to prime ideals are called *finite primes*. The others are called *infinite primes*. An absolute value representing the place ν will be denoted $|\cdot|_\nu$ or $|\cdot|_\mathfrak{p}$ if ν corresponds to the prime $\mathfrak{p}$. The *integers* of F_ν, denoted R_ν, are the elements of F_ν with absolute value less than 1, i.e.

$$R_\nu = \{x \in F_\nu : |x|_\nu \leq 1\}.$$

The units are $R_\nu^\times = \{x \in F_\nu : |x|_\nu = 1\}$.

With each place ν of F is associated an additive valuation $v : F^\times \longrightarrow \mathbb{R}$ defined as $v(x) = -\log|x|_\nu$. When ν corresponds to a prime $\mathfrak{p}$, v is discrete and so its image in $\mathbb{R}$ is isomorphic to $n\mathbb{Z}$ for some n. If $n = 1$, this discrete valuation is called *normalized* and is denoted $\mathrm{ord}_\mathfrak{p}$. Each finite place of F contains an absolute value which induces a normalized discrete valuation. Indeed, if the discrete valuation corresponding to the absolute value $|\cdot|$ has image isomorphic to $n\mathbb{Z}$, then the valuation corresponding to $|\cdot|^{1/n}$ will be normalized. Note that any normalized discrete valuation $\mathrm{ord}_\mathfrak{p} : F^\times \twoheadrightarrow \mathbb{Z}$ satisfies the following properties:

1. $\mathrm{ord}_\mathfrak{p}(xy) = \mathrm{ord}_\mathfrak{p}(x) + \mathrm{ord}_\mathfrak{p}(y)$ for all $x, y \in F^\times$.
2. $\mathrm{ord}_\mathfrak{p}(x+y) \geq \min\{\mathrm{ord}_\mathfrak{p}(x), \mathrm{ord}_\mathfrak{p}(y)\}$ for all $x, y \in F^\times$.

The last property follows from the fact that the absolute value corresponding to a finite place is always nonarchimedian.

By construction of the completion of a field, the absolute value on F can be extended to an absolute value on F_ν. Similarly, $\mathrm{ord}_\mathfrak{p}$ can be extended to a discrete valuation on F_ν (and the extension will also be normalized). With this valuation, R_ν becomes a discrete valuation ring. An element π of R_ν such that $\mathrm{ord}_\mathfrak{p}(\pi) = 1$ is called a *uniformizer at* $\mathfrak{p}$.

Note that $\mathrm{ord}_{\mathfrak{p}}$ has a simple and explicit description on $F^{\times}$. Given $x \in F^{\times}$, the ideal generated by x factors uniquely as a product of prime ideals

$$(x) = \prod_{\mathfrak{p} \text{ prime}} \mathfrak{p}^{\alpha_{\mathfrak{p}}}.$$

Then $\mathrm{ord}_{\mathfrak{p}}(x) = \alpha_{\mathfrak{p}}$.

In brief, the situation is simple for number fields. There are the finite primes and the infinite primes. When ν is a finite prime corresponding to $\mathfrak{p}$, an absolute value $|\cdot|_{\mathfrak{p}}$ and a (normalized discrete additive) valuation $\mathrm{ord}_{\mathfrak{p}}$ are attached to it. The question is: given an element in a field F, can $\mathrm{ord}_{\mathfrak{p}}$ be evaluated explicitly? The answer is yes, at least in quadratic number fields. In fact, one can do even more than that.

Proposition 8. *Let $\mathfrak{a}$ be a fractional $\mathcal{O}_K$-ideal and let $\mathfrak{p}$ be a prime of K dividing $p\mathcal{O}_K$, where K is a quadratic field and p is a rational prime. Then*

$$ord_p(N(\mathfrak{a})) = \begin{cases} ord_{\mathfrak{p}}(\mathfrak{a}) & \text{if } p\mathcal{O}_K = \mathfrak{p}^2 \\ ord_{\mathfrak{p}}(\mathfrak{a}) + ord_{\bar{\mathfrak{p}}}(\mathfrak{a}) & \text{if } p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}} \\ 2ord_{\mathfrak{p}}(\mathfrak{a}) & \text{if } p\mathcal{O}_K = \mathfrak{p} \text{ is prime} \end{cases}.$$

Moreover, if $\mathfrak{a} \subseteq \mathcal{O}_K$, $\alpha = x + y\omega \in \mathfrak{a}$ and p does not divide α (i.e. $p \nmid x, y$), then $ord_{\mathfrak{p}}(\mathfrak{a}) = 0$ or $ord_{\bar{\mathfrak{p}}}(\mathfrak{a}) = 0$ whenever $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$ in K.

Proof. The first part of this statement follows from the multiplicativity of the norm function $N = N_{K/\mathbb{Q}}$ introduced in the first chapter and the fact that $N(\mathfrak{p}) = p$ if p is ramified or split and $N(\mathfrak{p}) = p^2$ if p is inert.

The last statement follows from the fact that in Dedekind domains "to divide is to contain". If $\mathfrak{a}$ is an integral ideal, $\alpha \in \mathfrak{a}$ and $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}), \mathrm{ord}_{\bar{\mathfrak{p}}}(\mathfrak{a}) > 0$, then $\alpha \in \mathfrak{p} \cap \bar{\mathfrak{p}} = \mathfrak{p}\bar{\mathfrak{p}} = p\mathcal{O}_K$ and so $p|a, b$. □

If $x \in \mathcal{O}_K$, this result says that in order to find $\mathrm{ord}_{\mathfrak{p}}(x)$, one can analyse $\mathrm{ord}_p(N(x))$, where $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$. The only difficulty is the case where p splits, but for this the last part of the proposition is helpful in many cases.

To illustrate some of the concepts introduced so far in quadratic fields, let us look at the following example.

Example 3. Let d_0 be a square-free integer and let p be an odd rational prime that splits in $\mathcal{O}_K$, where $K = \mathbb{Q}(\sqrt{d_0})$. Then $p\mathcal{O}_K = (p, n+\sqrt{d_0})(p, n-\sqrt{d_0})$, where $n^2 \equiv d_0 \pmod{p}$. By Hensel's lemma, there exists a p-adic integer $x = (x_k)$ such that $x^2 = d_0$ and $x_1 \equiv n \pmod{p}$. In particular, $x_k \equiv x_{k-1} \pmod{p^{k-1}}$ and $x_k^2 \equiv d_0 \pmod{p^k}$. We claim that $\mathfrak{p}^k = (p^k, x_k + \sqrt{d_0})$, where $\mathfrak{p} = (p, x_1 + \sqrt{d_0}) = (p, n + \sqrt{d_0})$.

To prove this, the ideal $(p^k, x_k + \sqrt{d_0})$ will be factored. First,

$$\mathbb{N}((p^k, x_k + \sqrt{d_0})) = \gcd(N(p^k), \mathrm{Tr}(p^k(x_k + \sqrt{d_0})), N(x_k + \sqrt{d_0}))$$

$$= \gcd(p^{2k}, 2p^k x_k, x_k^2 - d_0) = p^k \gcd(p^k, 2x_k, (x_k^2 - d_0)/p^k) = p^k.$$

Indeed, p is odd and if $p|x_k$, $d_0 \equiv 0 \pmod{p}$, which contradicts our hypothesis. It follows that $(p^k, x_k + \sqrt{d_0}) = \mathfrak{p}^{\alpha}\bar{\mathfrak{p}}^{\bar{\alpha}}$ for some non-negative integers α and $\bar{\alpha}$ such that $\alpha + \bar{\alpha} = k$. Now $x_k \notin p\mathbb{Z}$, so one of α or $\bar{\alpha}$ is zero. Using the compatibility of the x_k, there exists an integer c such that $x_k = x_1 + cp$. Then p^k and $x_k + \sqrt{d_0} = cp + x_1 + \sqrt{d_0}$ belong to $\mathfrak{p}$, which shows that $(p^k, x_k + \sqrt{d_0}) \subseteq \mathfrak{p}$ and proves the claim.

4.2 Minimal Weierstrass equations

Let F be a local field, complete with respect to a place ν inducing a normalized discrete additive valuation ord. For instance, F could be the completion of a number field at a finite place. Let $R = \{x \in F | \mathrm{ord}(x) \geq 0\}$ denote its ring of integers. Then R is a discrete valuation ring with a unique (up to unit) prime element π (the uniformizer). Let

E be an elliptic curve defined over F with Weierstrass equation

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

By making a change of variables of the form $X = u^2X'$ and $Y = u^3Y'$, where u is a sufficiently big power of π, we can suppose that all the a_i belong to R.

When working with such an elliptic curve over a local field, one is often interested in reducing it $\mod \pi$. The problem is that different choices of Weierstrass equations can lead to very different reduction maps. For example, by artificially introducing powers of π in the a_i via a change of variables, one could conclude that every elliptic curve over a local field reduces to the singular curve $Y^2 = X^3$. To avoid this problem, a canonical choice of Weierstrass equation should be found.

Definition 12. Using the same notation as above, a Weierstrass equation for E is said to be a *minimal Weierstrass equation for E at ν* if $\mathrm{ord}(\Delta)$ is minimized subject to the condition that the a_i belong to R.

Since $\mathrm{ord}(\Delta)$ is a positive integer, every elliptic curve has a minimal Weierstrass equation. One can check that the only change of variables that fix the point at infinity and preserve the shape of a Weierstrass equation are those of the form $X = u^2X' + r$ and $Y = u^3Y' + u^2sX' + t$, where $r, s, t, u \in F$. When such a change of variables is applied, one can check that $\Delta' = u^{-12}\Delta, c_4' = u^{-4}c_4$ and $c_6' = u^{-6}c_6$. It follows that if $\mathrm{ord}(\Delta) < 12$ or $\mathrm{ord}(c_4) < 4$ or $\mathrm{ord}(c_6) < 6$, the Weierstrass equation is minimal. If the characteristic of the residue field $R/\pi R$ is not 2 or 3, a converse is true: any minimal Weierstrass equation for E is such that $\mathrm{ord}(\Delta) < 12$ or $\mathrm{ord}(c_4) < 4$.

Finding a minimal Weierstrass equation by hand can be difficult, especially if the characteristic of the residue field is 2 or 3. There is an algorithm due to Tate, called Tate's algorithm, that produces a minimal Weierstrass equation (and more). A description of

this very general algorithm can be found [Silverman(1994), IV§9]. Another algorithm, due to Laska, produces a minimal Weierstrass equation for E in a simple and straightforward manner (see [Laska(1982)]).

Minimal Weierstrass equations are not unique, but the relation between them can be explicitly described.

Proposition 9. *A minimal Weierstrass equation is unique up to a change of coordinates of the form*

$$X = u^2X' + r, \qquad Y = u^3Y' + u^2sX' + t$$

with $u \in R^*$ and $r, s, t \in R$. Conversely, if one starts with a Weierstrass equation whose coefficients are in R, then any change of coordinates

$$X = u^2X' + r, \qquad Y = u^3Y' + u^2sX' + t$$

used to produce a minimal Weierstrass equation satisfies $u, r, s, t \in R$.

Proof. See [Silverman(2009), VI§1, Proposition 1.3]. □

Example 4. Let $K = \mathbb{Q}(\sqrt{5})$, let $\mathfrak{p}$ be a prime of K and let p be the prime of $\mathbb{Q}$ such that $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. The elliptic curve given by the Weierstrass equation

$$Y^2 + XY + Y = X^3 + X^2 + 22X - 9$$

over the field $K_\mathfrak{p}$, the completion of K at $\mathfrak{p}$, has discriminant $\Delta = -2^{15}5^2$ and $c_4 = -5 \cdot 211$. It follows that this equation is minimal at $\mathfrak{p}$ since $\nu_\mathfrak{p}(c_4) = 2 < 4$ if $p = 5$ and $\nu_p(c_4) = 1 < 4$ otherwise.

4.3 Explicit formulas for the Mazur-Tate pairing on elliptic curves

The Mazur-Tate S-pairing is a bilinear pairing defined on the product of two abelian varieties satisfying certain conditions, like a variety and its dual, for example. For elliptic

curves, the pairing can be described quite explicitly. The main reference in this section is [Mazur and Tate(1987)].

Let E be an elliptic curve defined over a number field F and let M_F be a complete set of inequivalent absolute values on F. Let $M_F^0 \subseteq M_F$ be the set of nonarchimedian absolute values and let $M_F^\infty \subseteq M_F$ be the set of archimedian absolute values. In the general definition of the S-pairing, S can be any finite subset of M_F^0. In our case, we choose $S = \emptyset$. Then the S-pairing $\langle \cdot, \cdot \rangle_S : E(F) \times E(F) \longrightarrow C$ with $S = \emptyset$ is defined as follows. The target group C is a quotient of the idèle class group of F:

$$C = \mathbb{I}_F / \left(F^\times \prod_{\nu \in M_F} U_\nu \right),$$

where

$$U_\nu = \begin{cases} F_\nu^\times & \text{if } \nu \in M_F^\infty \\ \\ R_\nu^\times & \text{if } \nu \in M_F^0 \end{cases}.$$

As before, R_ν is the ring of integers of F_ν. Roughly speaking, taking the quotient suppresses the infinite places and only preserves the prime powers at the finite places.

In order to compute the pairing of P and Q explicitly, Mazur and Tate suppose that there is another point P' satisfying certain local conditions at some of the primes of S. In our case S is empty so these conditions are satisfied for any choice of P'. Then $\langle P, Q \rangle_S = (c_\nu)$, where

$$c_\nu \text{ is arbitrary in } F_\nu^\times \qquad \text{for } \nu \in M_F^\infty,$$

$$c_\nu = \frac{t_{\mathfrak{p}_\nu}(P + P') t_{\mathfrak{p}_\nu}(Q + P')}{t_{\mathfrak{p}_\nu}(P') t_{\mathfrak{p}_\nu}(P + Q + P')} \mod R_\nu^\times \qquad \text{for } \nu \in M_F^0,$$

where $\mathfrak{p}_\nu$ is the prime ideal of F corresponding to ν and $t_{\mathfrak{p}_\nu}(P)$ denotes an element of $F_\nu^\times$ such that $t_{\mathfrak{p}_\nu}(P)^2$ is a denominator for the x-coordinate of P in a minimal Weierstrass equation for E at ν.

At this point, the S-pairing takes values in a quotient of the idèle class group, but a map between this group and the ideal class group can be found. First, there is a well defined homomorphism $\rho' : \mathbb{I}_F \longrightarrow \mathrm{Cl}(F)$, where $\mathrm{Cl}(F)$ is the ideal class group of F. This homomorphism sends $(c_\nu) \in \mathbb{I}_F$ to the class of the fractional ideal $\prod_{\nu \in M_F^0} \mathfrak{p}_\nu^{\mathrm{ord}_{\mathfrak{p}_\nu}(c_\nu)}$. Since $F^\times \prod_{\nu \in M_F} U_\nu$ is contained in the kernel of ρ', the homomorphism ρ' induces a well-defined homomorphism $\rho : C \longrightarrow \mathrm{Cl}(F)$.

Putting everything together gives a bilinear pairing

$$\langle \cdot, \cdot \rangle : E(F) \times E(F) \longrightarrow \mathrm{Cl}(F)$$

(note that the subscript S has been dropped to denote this pairing). With this description of the pairing, there are two computational difficulties. First, the point P' must be chosen. We choose P' to be the identity of $E(F)$. Second, the elements $t_{\mathfrak{p}_\nu}(P), t_{\mathfrak{p}_\nu}(Q), t_{\mathfrak{p}_\nu}(P')$ and $t_{\mathfrak{p}_\nu}(P+Q)$ must be computed at every $\nu \in M_F^0$. This is the main problem and it will be solved under certain conditions in the next chapter.

CHAPTER 5
Obtaining Soleng's homomorphism via the Mazur-Tate pairing

As we saw, Soleng considered a map from the primitive points of an elliptic curve

$$E:\ Y^2 = X^3 + a_2X^2 + a_4X + a_6$$

with coefficients in $\mathbb{Z}$ to the class group of the order $\mathbb{Z}[\sqrt{a_6}] \subseteq K$, where $K = \mathbb{Q}(\sqrt{a_6})$. To obtain this homomorphism via the Mazur-Tate pairing, a point P_0 in $E(K)$ is fixed and explicit formulas for the homomorphism

$$\langle \cdot, P_0 \rangle : E_{\text{prim}}(\mathbb{Q}) \longrightarrow \text{Cl}(K),$$

which sends P to $\langle P, P_0 \rangle$, are found. This is the content of Theorem 9. In Corollary 1 it will be seen that this homomorphism coincides with Soleng's homomorphism in certain cases.

Lemma 2. *Let E be an elliptic curve with Weierstrass equation*

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

and let $P_0 = (0, \theta) \in E(\mathbb{Q}(\theta))$, where $\theta = (-a_3 + \sqrt{a_3^2 + 4a_6})/2$ is a root of $Y^2 + a_3Y - a_6$. Then for any point $P = (A/C^2, B/C^3) \in E(\mathbb{Q})$, where $\gcd(A, C) = \gcd(B, C) = 1$ and $A \neq 0$,

$$x(P + P_0) = \frac{(a_4AC^2 + 2a_6C^4 - a_3BC) - (2BC + a_1AC^2 + a_3C^4)\theta}{A^2} \tag{5.1}$$

and

$$N_{K/\mathbb{Q}}((a_4AC^2+2a_6C^4-a_3BC)-(2BC+a_1AC^2+a_3C^4)\theta) = -A^2C^2(b_6A+b_8C^2), \quad (5.2)$$

so that

$$N_{K/\mathbb{Q}}(x(P+P_0)) = -\frac{C^2(b_6A+b_8C^2)}{A^2}. \quad (5.3)$$

Proof. The proof is a simple but tedious calculation. □

In the case where $a_1 = a_3 = 0$, the point P_0 is $(0, \sqrt{a_6}) \in E(K)$, $K = \mathbb{Q}(\sqrt{a_6})$ and the formulas in lemma 2 become much simpler.

Theorem 9. *Let* $P = \left(A/C^2, B/C^3\right)$, *where* $\gcd(A,C) = \gcd(B,C) = 1$, *be a primitive point on the elliptic curve*

$$E:\ Y^2 = X^3 + a_2X^2 + a_4X + a_6$$

defined over $\mathbb{Z}$, *with* a_6 *not a square, and suppose that the curve is minimal at all primes of* K. *Let* $a_6 = \ell^2 d_0$, *where* d_0 *is square-free. Then the ideal class* $\langle P, P_0\rangle$ *is given explicitly by the class of*

$$\mathfrak{I}_2 \prod_{\substack{p|A,p\nmid a_6\\ p\ split,p\ odd}} \mathfrak{p}_p^{-ord_p(A)} \prod_{\substack{p|A,p|a_6\\ p\ odd,\ p\mathcal{O}_K=\mathfrak{p}^2}} \mathfrak{p}^{-ord_p(A)} \prod_{\substack{p|A,p|a_6\\ p\ odd,\ p\mathcal{O}_K=\mathfrak{p}\bar{\mathfrak{p}}}} \mathfrak{p}^{\frac{1}{2}ord_{\mathfrak{p}}(x(P+P_0))}\bar{\mathfrak{p}}^{\frac{1}{2}ord_{\bar{\mathfrak{p}}}(x(P+P_0))},$$

where

$$\mathfrak{I}_2 = \begin{cases} \mathfrak{p}^{-ord_2(A)} & \text{if } 2\mathcal{O}_K = \mathfrak{p}^2 \\ \mathfrak{p}^{\frac{1}{2}ord_{\mathfrak{p}}(x(P+P_0))}\bar{\mathfrak{p}}^{\frac{1}{2}ord_{\bar{\mathfrak{p}}}(x(P+P_0))} & \text{if } 2\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}} \\ 1 & \text{if } 2\mathcal{O}_K \text{ is prime} \end{cases}$$

and where

$$\mathfrak{p}_p = \left(p, r_pkB + \sqrt{d_0}\right)$$

with $kC^3 \equiv 1 \pmod{A}$ *and* $r_p \ell \equiv 1 \pmod{p}$. *Moreover,*

$$\frac{1}{2} ord_{\mathfrak{p}}(x(P+P_0)) + \frac{1}{2} ord_{\bar{\mathfrak{p}}}(x(P+P_0)) = -ord_p(A)$$

if $p = 2$ *and* $2\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$ *or if* $p|A, p|a_6$ *and* $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$.

Remark 1. One sees in these explicit formulas that if the prime p splits as $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$, the $\mathfrak{p}$ and $\bar{\mathfrak{p}}$-parts in $x(P+P_0)$ are difficult to separate. However, it will be shown that both primes appear in the denominator of the ideal $x(P+P_0)\mathcal{O}_K$. In particular, whenever a_6 is not a fundamental discriminant, the ideal is not prime to the conductor of $\mathbb{Z}[\sqrt{a_6}]$.

Proof. The main part of the proof is the computation of

$$c_{\mathfrak{p}} = \frac{t_{\mathfrak{p}}(P) t_{\mathfrak{p}}(P_0)}{t_{\mathfrak{p}}(0) t_{\mathfrak{p}}(P+P_0)} \mod \mathcal{O}_{K_{\mathfrak{p}}}^{\times}$$

at every prime $\mathfrak{p}$ of K. To do so, $x(P), x(P_0)$ and $x(P+P_0)$ are carefully analysed. First, note that $A \neq 0$, otherwise a_6 is a square. Using Lemma 2 with $a_1 = a_3 = 0$ gives

$$x(P+P_0) = \frac{a_4 AC^2 + 2a_6 C^4 - 2BC\sqrt{a_6}}{A^2}. \tag{5.4}$$

Since $b_6 = 4a_6$ and $b_8 = 4a_2 a_6 - a_4^2$ when $a_1 = a_3 = 0$, the same Lemma gives

$$N_{K/\mathbb{Q}}(a_4 AC^2 + 2a_6 C^4 - 2BC\sqrt{a_6}) = A^2 C^2 (a_4^2 C^2 - 4a_6(a_2 C^2 + A)) \tag{5.5}$$

and

$$N_{K/\mathbb{Q}}(x(P+P_0)) = \frac{C^2(a_4^2 C^2 - 4a_6(a_2 C^2 + A))}{A^2}. \tag{5.6}$$

In the computations, the relation satisfied by the coordinates will be frequently used:

$$B^2 = A^3 + a_2 A^2 C^2 + a_4 AC^4 + a_6 C^6. \tag{5.7}$$

Let $\mathfrak{p}$ be a finite prime of K. Looking at equation (5.4), we see that the case where $\mathfrak{p}$ divides A is special, as $x(P+P_0)$ could have a denominator in $K_\mathfrak{p}$. The proof will be divided in a few cases, starting with the following one:

Case 1: $\mathfrak{p}$ does not divide A.

Since the equation for E is minimal at $\mathfrak{p}$ by hypothesis and the x-coordinate of $P_0, 0$ and $P+P_0$ do not have denominators in $K_\mathfrak{p}$,

$$t_\mathfrak{p}(P_0) = t_\mathfrak{p}(0) = t_\mathfrak{p}(P+P_0) = 1.$$

Using the minimality of the equation again,

$$t_\mathfrak{p}(P) = \pi_\mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(C)},$$

where $\pi_\mathfrak{p}$ is a uniformizer at $\mathfrak{p}$, i.e. an element of $K_\mathfrak{p}^\times$ with valuation exactly 1.

Case 2: $\mathfrak{p}$ divides A.

First, suppose that $\mathfrak{p}$ divides $2\mathcal{O}_K$. For the same reasons as in the previous case,

$$t_\mathfrak{p}(P_0) = t_\mathfrak{p}(0) = 1 \qquad \text{and} \qquad t_\mathfrak{p}(P) = \pi_\mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(C)}.$$

The computation of $t_\mathfrak{p}(P+P_0)$ is divided into two cases, depending if $\mathfrak{p}$ divides 2.

Case 2.1.1: $d_0 \equiv 3 \pmod 4$ **or** $d_0 \equiv 0 \pmod 2$**.**

In this case, $2\mathcal{O}_K = \mathfrak{p}^2$. Then equation (5.5) gives

$$\mathrm{ord}_\mathfrak{p}(z) = \mathrm{ord}_2(N(z)) = \mathrm{ord}_2(A^2C^2(a_4^2C^2 - 4a_6(a_2C^2 + A))) = 2\mathrm{ord}_2(A)$$

because $\mathrm{ord}_2(a_4^2C^2) = 0$ since $\gcd(A, 2B, a_4) = 1$ (recall that P is primitive) and A is even. Since $2\mathrm{ord}_2(A) = \mathrm{ord}_{\mathfrak{p}}(A)$, it follows that

$$\mathrm{ord}_{\mathfrak{p}}(x(P + P_0)) = \mathrm{ord}_{\mathfrak{p}}(z) - 2\mathrm{ord}_{\mathfrak{p}}(A) = -2\mathrm{ord}_2(A)$$

and so

$$t_{\mathfrak{p}}(P + P_0) = \pi_{\mathfrak{p}}^{\mathrm{ord}_2(A)}.$$

Case 2.1.2: $d_0 \equiv 5 \pmod 8$.

In this case, $\mathfrak{p} = 2\mathcal{O}_K$ is prime and so $t_{\mathfrak{p}}(P + P_0)$ is sent to 1 in $\mathrm{Cl}(K)$.

Case 2.1.3: $d_0 \equiv 1 \pmod 8$.

In this case, $2\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$ and

$$\mathrm{ord}_{\mathfrak{p}}(z) + \mathrm{ord}_{\bar{\mathfrak{p}}}(z) = \mathrm{ord}_2(N(z)) = 2\mathrm{ord}_2(A).$$

Now $z = a_4AC^2 + 2a_6C^4 - 2BC\sqrt{a_6} \in \mathfrak{p} \cap \bar{\mathfrak{p}}$ because $2|z$. It follows that $\mathrm{ord}_{\mathfrak{p}}(z), \mathrm{ord}_{\bar{\mathfrak{p}}}(z) > 0$ and so $\mathrm{ord}_{\mathfrak{p}}(z), \mathrm{ord}_{\bar{\mathfrak{p}}}(z) < 2\mathrm{ord}_2(A)$ (using the previous equation). Now since $\mathrm{ord}_2(A) = \mathrm{ord}_{\mathfrak{p}}(A)$, it follows that

$$\mathrm{ord}_{\mathfrak{p}}(x(P + P_0)) = \mathrm{ord}_{\mathfrak{p}}(z) - 2\mathrm{ord}_{\mathfrak{p}}(A) < 0$$

and similarly

$$\mathrm{ord}_{\bar{\mathfrak{p}}}(x(P + P_0)) = \mathrm{ord}_{\bar{\mathfrak{p}}}(z) - 2\mathrm{ord}_{\bar{\mathfrak{p}}}(A) < 0.$$

This is not a precise value, but it tells us at least that $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ appear in the denominator of $x(P + P_0)$ and so

$$t_{\mathfrak{p}}(P + P_0) = \pi_{\mathfrak{p}}^{-\frac{1}{2}\mathrm{ord}_{\mathfrak{p}}(x(P+P_0))} \neq 1 \qquad \text{and} \qquad t_{\bar{\mathfrak{p}}}(P + P_0) = \pi_{\bar{\mathfrak{p}}}^{-\frac{1}{2}\mathrm{ord}_{\bar{\mathfrak{p}}}(x(P+P_0))} \neq 1.$$

Now consider the cases where $\mathfrak{p}$ does not divide $2\mathcal{O}_K$. First,

$$t_{\mathfrak{p}}(P_0) = t_{\mathfrak{p}}(0) = 1 \qquad \text{and} \qquad t_{\mathfrak{p}}(P) = \pi_{\mathfrak{p}}^{\mathrm{ord}_{\mathfrak{p}}(C)}$$

by the minimality of the equation at $\mathfrak{p}$. For $t_{\mathfrak{p}}(P + P_0)$, there are three cases to consider. Let p be the rational prime such that $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$.

Case 2.2.1: p does not divide a_6.

In this case, reducing equation (5.7) mod p gives

$$B^2 \equiv C^6 \ell^2 d_0 \pmod{p}$$

which is equivalent to

$$(r_p k B)^2 \equiv d_0 \pmod{p},$$

where $r_p \ell \equiv 1 \pmod{p}$. This says that p splits in K as $p\mathcal{O}_K = \mathfrak{p}_p \bar{\mathfrak{p}}_p$, using the same notation as in the statement of the theorem, where $\mathfrak{p}_p = \mathfrak{p}$. Since $C^2(a_4 A + 2a_6 C^2)$ is not divisible by p, the element z belongs to at most one of the ideals $\mathfrak{p}_p$ and $\bar{\mathfrak{p}}_p$. To prove that $z \in \bar{\mathfrak{p}}_p$, we show that there exists integers m and n such that

$$a_4 A C^2 + 2a_6 C^4 - 2BC\ell\sqrt{d_0} = mp + n(r_p k B - \sqrt{d_0}).$$

This is equivalent to

$$a_4 A C^2 + 2a_6 C^4 - 2B^2 C(\ell r_p) k \equiv 0 \pmod{p}$$

$$\Leftrightarrow a_4 A C^2 + 2a_6 C^4 - 2B^2 C k \equiv 0 \pmod{p}$$

$$\Leftrightarrow a_4 A C^2 + a_4 A C^2 + 2a_6 C^4 - 2B^2 C k = 2a_4 A C^2 + 2a_6 C^4 - 2B^2 C k \equiv 0 \pmod{p}$$

$$\Leftrightarrow C^2(2a_4 A C^2 + 2a_6 C^4 - 2B^2 C k) = 2a_4 A C^4 + 2a_6 C^6 - 2B^2 (C^3 k) \equiv 0 \pmod{p}$$

$$\Leftrightarrow 2a_4AC^4 + 2a_6C^6 - 2B^2 = -2(B^2 - a_4AC^4 - a_6C^6) \equiv 0 \pmod{p}$$

which is clearly true since $p|A$. Since $\mathrm{ord}_{\mathfrak{p}_p}(A) = \mathrm{ord}_p(A)$, it follows that

$$\mathrm{ord}_{\mathfrak{p}_p}(x(P+P_0)) = \mathrm{ord}_{\mathfrak{p}_p}(z) - 2\mathrm{ord}_{\mathfrak{p}_p}(A) = 0 - 2\mathrm{ord}_p(A).$$

For $\bar{\mathfrak{p}}_p$, the above computation shows that $\mathrm{ord}_p(N(z)) = \mathrm{ord}_{\bar{\mathfrak{p}}_p}(z)$. Therefore

$$\mathrm{ord}_{\bar{\mathfrak{p}}_p}(z) = \mathrm{ord}_p(A^2C^2(a_4^2C^2 - 4a_6(a_2C^2 + A)))$$

$$= 2\mathrm{ord}_p(A) + \mathrm{ord}_p(a_4^2C^2 - 4a_6(a_2C^2 + A)) \geq 2\mathrm{ord}_p(A)$$

and so

$$\mathrm{ord}_{\bar{\mathfrak{p}}_p}(x(P+P_0)) = \mathrm{ord}_{\bar{\mathfrak{p}}_p}(z) - 2\mathrm{ord}_{\bar{\mathfrak{p}}_p}(A) = \mathrm{ord}_{\bar{\mathfrak{p}}_p}(z) - 2\mathrm{ord}_p(A) \geq 0.$$

Case 2.2.2: p divides d_0.

In this case p is ramified in K. Using equation (5.6), one sees that

$$\mathrm{ord}_{\mathfrak{p}}(x(P+P_0)) = \mathrm{ord}_p\left(\frac{C^2(a_4^2C^2 - 4a_6(a_2C^2 + A))}{A^2}\right).$$

Since $p|d_0$ and $p|A$, it follows that $p|B$ and so $p \nmid a_4$, by the primitivity of P. Therefore $\mathrm{ord}_p(a_4^2C^2 - 4a_6(a_2C^2 + A)) = 0$ and so

$$\mathrm{ord}_{\mathfrak{p}}(x(P+P_0)) = -2\mathrm{ord}_p(A).$$

Case 2.2.3: p does not divide d_0 and p divides ℓ.

In this case, p is either inert or split. If it is inert, it will be sent to 1 in the ideal class group, so this case can be ignored. Suppose now that $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$. Then

$$2\mathrm{ord}_p(A) = \mathrm{ord}_p(N(z)) = \mathrm{ord}_{\mathfrak{p}}(z) + \mathrm{ord}_{\bar{\mathfrak{p}}}(z).$$

Since $p|z = a_4AC^2 + 2a_6C^4 - 2BC\sqrt{a_6}$, the element z belongs to $\mathfrak{p}$ and $\bar{\mathfrak{p}}$. It follows that $\mathrm{ord}_{\mathfrak{p}}(z), \mathrm{ord}_{\bar{\mathfrak{p}}}(z) < 2\mathrm{ord}_p(A)$ and so

$$\mathrm{ord}_{\mathfrak{p}}(x(P+P_0)), \mathrm{ord}_{\bar{\mathfrak{p}}}(x(P+P_0)) < 0.$$

To complete the proof, it suffices to put everything together and map the idèle class to an ideal of $\mathrm{Cl}(\mathcal{O}_K)$. First, both $t_{\mathfrak{p}}(P_0)$ and $t_{\mathfrak{p}}(0)$ are 1 for all $\mathfrak{p}$, so they will not contribute in $\mathrm{Cl}(K)$. For $t_{\mathfrak{p}}(P)$, it is always equal to $\pi_{\mathfrak{p}}^{\mathrm{ord}_{\mathfrak{p}}(C)}$ and so when mapped to $\mathrm{Cl}(\mathcal{O}_K)$, its contribution is $(C) = (1)$. Finally, combining all the different values of $t_{\mathfrak{p}}(P+P_0)$ gives the statement of the theorem. □

Corollary 1. *Suppose that a_6 is square-free and not congruent to 1 mod 4 (so that $\mathcal{O}_K = \mathbb{Z}[\sqrt{a_6}]$). Suppose further that the equation for E is minimal at the primes above 2 and 3. Then every point of $E(\mathbb{Q})$ is primitive and the homomorphism obtained via the Mazur-Tate pairing coincides with Soleng's homomorphism.*

Proof. The fact that every point is primitive when a_6 is square-free and congruent to 2 or 3 mod 4 was proven in Lemma 1.

In order to apply the previous theorem, is must be checked that the equation for E is minimal at the primes $\mathfrak{p}$ of K not dividing 2 or 3. This follows directly from the fact that $\mathrm{ord}_{\mathfrak{p}}(c_6) = \mathrm{ord}_{\mathfrak{p}}(-2^5 3^3 a_6) = \mathrm{ord}_{\mathfrak{p}}(a_6) \leq 2 < 6$.

Since a_6 is square-free, we have $\ell = 1$ and $d_0 = a_6$. Then the formula of the theorem becomes

$$\mathfrak{p}_2^{-\mathrm{ord}_2(A)} \prod_{\substack{p|A, p\nmid a_6 \\ p \text{ odd}}} (p, kB + \sqrt{a_6})^{-\mathrm{ord}_p(A)} \prod_{\substack{p|A, p|a_6 \\ p \text{ odd},\ p\mathcal{O}_K = \mathfrak{p}^2}} \mathfrak{p}^{-\mathrm{ord}_p(A)},$$

where $2\mathcal{O}_K = \mathfrak{p}_2^2$ and $kC^3 \equiv 1 \pmod{A}$. Indeed if $p|a_6$, p is ramified in K.

To complete the proof, one must show that this ideal is in the same class as

$$\mathfrak{a} = (A, -kB + \sqrt{a_6})\,.$$

This can be done by computing $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a})$ for each prime $\mathfrak{p}$ of K. The first step is to prove that $\mathbb{N}(\mathfrak{a}) = A$. By Proposition 6, it suffices to show that

$$A = \gcd(N(A), \mathrm{Tr}(A(kB - \sqrt{a_6})), N(kB - \sqrt{a_6})) = \gcd(A^2, 2kAB, (kB)^2 - a_6)$$

$$= A\gcd(A, 2kB, ((kB)^2 - a_6)/A),$$

which is equivalent to proving that $\gcd(A, 2kB, ((kB)^2 - a_6)/A) = 1$. Note that $((kB)^2 - a_6)/A$ is an integer because

$$B^2 \equiv a_6C^6 \pmod{A} \Longleftrightarrow (kB)^2 \equiv a_6 \pmod{A}$$

by definition of k. Suppose that a prime q divides $\gcd(A, 2kB, ((kB)^2 - a_6)/A)$. There are two cases to consider.

Case 1: q odd.

Then $q|A$ and $q|B$ (because $\gcd(q, k) = 1$), so $q|a_6$. Taking the equation

$$B^2 = A(A^2 + a_2AC^2 + a_4C^4) + a_6C^6,$$

multiplying it by k^2 and rearranging the terms gives

$$\frac{(kB)^2 - a_6}{A} + a_6\frac{(kC^3 - 1)(kC^3 + 1)}{A} = k^2(A^2 + a_2AC^2 + a_4C^4). \tag{5.8}$$

Since q divides the left hand side, it divides the right hand side and so it divides a_4. But this contradicts the primitivity of the point P, i.e. the fact that $\gcd(A, 2B, a_4) = 1$.

Case 2: $q = 2$.

Referring to equation (5.8) again, the left hand side is even (because $kC^3 + 1$ is even) and so the right hand side is also even. It follows that a_4 is even, which contradicts the primitivity of P. This completes the proof that $\mathbb{N}(\mathfrak{a}) = A$.

This computation implies that $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) > 0$ if and only if $\mathfrak{p}$ divides $A\mathcal{O}_K$. Let $\mathfrak{p}$ be a prime dividing $A\mathcal{O}_K$ and let p be the rational prime such that $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$. Then

$$\mathrm{ord}_p(N(\mathfrak{a})) = \mathrm{ord}_p(A) = \begin{cases} \mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) & \text{if } p\mathcal{O}_K = \mathfrak{p}^2 \\ \mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) + \mathrm{ord}_{\bar{\mathfrak{p}}}(\mathfrak{a}) & \text{if } p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}} \\ 2\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) & \text{if } p\mathcal{O}_K \text{ is prime} \end{cases}.$$

First suppose that $p = 2$. Then p is ramified and so $\mathrm{ord}_2(A) = \mathrm{ord}_{\mathfrak{p}_2}(\mathfrak{a})$.

Now suppose that p is odd and that $p|a_6$. Then p is ramified in K and again $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) = \mathrm{ord}_p(A)$.

Finally, suppose that p is odd and $p \nmid a_6$. Since

$$(kB)^2 \equiv a_6 \pmod{p}$$

(see the proof of the lemma), it follows that p splits as $p\mathcal{O}_K = \left(p, kB + \sqrt{a_6}\right)\left(p, kB - \sqrt{a_6}\right)$ in K. Let $\mathfrak{p} = \left(p, kB + \sqrt{a_6}\right)$. Now $-kB + \sqrt{a_6} \in \mathfrak{a}$, but $-kB + \sqrt{a_6} \notin p\mathcal{O}_K$, so only one of $\mathfrak{p}$ or $\bar{\mathfrak{p}}$ divides $\mathfrak{a}$. But clearly, $\mathfrak{a} \subseteq \bar{\mathfrak{p}}$, so $\mathrm{ord}_p(A) = \mathrm{ord}_{\bar{\mathfrak{p}}}(\mathfrak{a})$. This proves that

$$\mathfrak{a} = (A, -kB + \sqrt{a_6}) = \mathfrak{p}_2^{\mathrm{ord}_2(A)} \prod_{\substack{p|A, p\nmid a_6 \\ p \text{ odd}}} (p, -kB + \sqrt{a_6})^{\mathrm{ord}_p(A)} \prod_{\substack{p|A, p|a_6 \\ p \text{ odd}, p\mathcal{O}_K = \mathfrak{p}^2}} \mathfrak{p}^{\mathrm{ord}_p(A)}$$

which completes the proof because the inverse of $\mathfrak{p}$ in $\mathrm{Cl}(K)$ is $\mathfrak{p}$ if $\mathfrak{p}$ is ramified and the inverse of $\left(p, kB + \sqrt{a_6}\right)$ in $\mathrm{Cl}(K)$ is $\left(p, kB - \sqrt{a_6}\right)$. □

There are two important hypotheses in Theorem 9: the minimality of the Weierstrass at all primes of K and the primitivity of the point P. The second hypothesis is there to help us find explicit formulas: if P is not primitive, the homomorphism is still defined at P, but it might not be possible to find explicit formulas for its image in $\mathrm{Cl}(K)$. The first hypothesis is much more important. Without it, it is not possible to find general explicit formulas. Indeed, the primes at which a Weierstrass equation is not minimal depend on the equation itself. Nevertheless, given a Weierstrass equation, there are at most finitely many primes at which this equation is not minimal. To find explicit formulas for this equation, one can apply Theorem 9 and treat the non-minimal primes separately. An example of this technique is given in the next chapter.

A well know fact in the theory of elliptic curves is that every elliptic curve $E/\mathbb{Q}$ has a *global minimal Weierstrass equation* over $\mathbb{Q}$, i.e. a Weierstrass equation that is minimal at all finite primes of $\mathbb{Q}$ (see [Silverman(2009), VIII§8, Corollary 8.3]). If the elliptic curve is defined over a number field F with class number one, the corresponding statement is also true. However, some elliptic curves E defined over F may fail to have a global minimal Weierstrass equation if F has class number grater than 1. This depends on the so-called *Weierstrass class* of E. Of course, if the quadratic field K has class number one the homomorphism is trivial, so the homomorphism is interesting precisely in the cases where some elliptic curves do not have a global minimal Weierstrass equation. It can be shown that

Theorem 10. *If F is a number field, then a positive proportion of elliptic curves E/F have a global minimal Weierstrass equation.*

Proof. See [Bekyel(2004)]. □

The only problem is that this minimal Weierstrass equation might not have the desired form, i.e. $a_1 = a_3 = 0$. This motivates a possible generalisation of Theorem 9 that will be presented later.

CHAPTER 6
Other uses of the pairing and examples

So far, the Mazur-Tate pairing has been used on a particular type of elliptic curves (those that had a global minimal Weierstrass equation with $a_1 = a_3 = 0$). Of course, the techniques developed can be used in other cases. The purpose of this chapter is to illustrate this.

6.1 A homomorphism on a different family of elliptic curves

When a_6 is a square in $\mathbb{Z}$, theorem 9 gives the trivial homomorphism. When a_1, a_2, a_3 and a_6 are zero, the Weierstrass has the form

$$E_D : Y^2 = X^3 - DX,$$

where D is an integer, not necessarily a discriminant (the notation for E_D is standard). An easily found point on this curve is $P_0 = (\sqrt{D}, 0) \in E(K)$, where $K = \mathbb{Q}(\sqrt{D})$. The Mazur-Tate paring then gives a homomorphism from $E(\mathbb{Q})$ to $\mathrm{Cl}(K)$ defined by $P \mapsto \langle P, P_0 \rangle$. Under similar restrictions as in Theorem 9, explicit formulas for this homomorphism can be found.

Theorem 11. *Let* $P = (A/C^2, B/C^3)$, *where* $\gcd(A, C) = \gcd(B, C) = 1$, *be a rational point on the curve*

$$E_D : Y^2 = X^3 - DX,$$

where D *is square-free and congruent to* $5 \mod 8$ *(so that* 2 *is inert in* $\mathbb{Q}(\sqrt{D})$*). Then the map sending* $(0, 0)$ *to the trivial ideal class and* $P \neq (0, 0)$ *to the ideal class of*

$$(B_A, kA - \sqrt{D}),$$

where $kC^2 \equiv 1 \pmod{B}$ *and* $B_A = \prod_{p|B, p\nmid A} p^{ord_p(B)}$*, is a homomorphism.*

Proof. In order to find general explicit formulas for the Mazur-Tate pairing, we first prove that the Weierstrass equation of E_D is minimal at all primes of K. This follows at once from the fact that E_D has discriminant $\Delta = 2^6 D^3$ and that D is square-free and congruent to 5 mod 8. Indeed, this implies that $\nu_{\mathfrak{p}}(\Delta) \leq 6 < 12$ for all primes $\mathfrak{p}$ of K.

Let $P_0 = (\sqrt{D}, 0)$. First, the explicit formulas for addition on elliptic curves give $x((0,0) + P_0) = -\sqrt{D}$ and so the homomorphism sends $(0,0)$ to the trivial ideal class.

From now on, suppose that $P = (A/C^2, B/C^3)$ with $AB \neq 0$ and $\gcd(A, C) = \gcd(B, C) = 1$. Since the equation for E_D is globally minimal, one sees that $t_{\mathfrak{p}}(P_0) = t_{\mathfrak{p}}(0) = 1$ and $t_{\mathfrak{p}}(P) = \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(C)}$ for all the primes $\mathfrak{p}$ of K. In particular, $\prod_{\mathfrak{p}} t_{\mathfrak{p}}(P) = C\mathcal{O}_K$ does not contribute in $\mathrm{Cl}(K)$. For $t_{\mathfrak{p}}(P + P_0)$, a more careful analysis is required.

On E_D, the formulas of Lemma 2 give

$$x(P + P_0) = \frac{2DA^2C^2 + (A^3 + DAC^4)\sqrt{D}}{B^2}. \tag{6.1}$$

Letting $z = 2DA^2C^2 + (A^3 + DAC^4)\sqrt{D}$, the same Lemma gives

$$N(z) = -DB^4 \tag{6.2}$$

and so

$$N(x(P + P_0)) = -D. \tag{6.3}$$

From now on, let $\mathfrak{p}$ be a prime of K above the prime p of $\mathbb{Z}$ such that p divides B (the other primes will not contribute, by Formula 6.1). There are a few cases to consider.

Case 1: $p = 2$**.**

Since $D \equiv 5 \pmod{8}$, 2 is inert in K and so

$$2\mathrm{ord}_{\mathfrak{p}}(x(P + P_0)) = \mathrm{ord}_2(N(x(P + P_0))) = \mathrm{ord}_2(-D) = 0.$$

Case 2.1: $p \neq 2$ **and** p **does not split in** K**.**

In this case,

$$\mathrm{ord}_{\mathfrak{p}}(x(P+P_0)) = 0$$

using the same idea as above.

Case 2.2: $p \neq 2$ **and** p **splits in** K**.**

In this case, p cannot divide D. Suppose that $p|A$. Then the equation

$$B^2 = A(A^2 - DC^4)$$

implies that

$$2\mathrm{ord}_p(B) = \mathrm{ord}_p(A).$$

It follows that $\mathrm{ord}_{\mathfrak{p}}(x(P+P_0)) = \mathrm{ord}_{\mathfrak{p}}(z/A) + \mathrm{ord}_{\mathfrak{p}}(A) - 2\mathrm{ord}_{\mathfrak{p}}(B) = \mathrm{ord}_{\mathfrak{p}}(z/A) \geq 0$ since $z/A \in \mathcal{O}_K$. Similarly, $\mathrm{ord}_{\bar{\mathfrak{p}}}(x(P+P_0)) \geq 0$.

These computations imply that only the odd primes that divide B, but not A, can contribute. Let p be such a prime. Then

$$0 \equiv B^2 \equiv A(A^2 - DC^4) \pmod{B} \Longleftrightarrow (kA)^2 \equiv D \pmod{B},$$

where $kC^2 \equiv 1 \pmod{B}$. It follows that $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$, where $\mathfrak{p} = (p, kA + \sqrt{D})$. Since $2DA^2C^2$ is not divisible by p, the element z belongs to at most one of $\mathfrak{p}$ or $\bar{\mathfrak{p}}$ and in fact, $z \in \mathfrak{p}$. To see this, note that there exists integers m and n such that

$$z = 2DA^2C^2 + (A^3 + DAC^4)\sqrt{D} = mp + n(kA + \sqrt{D}).$$

Indeed, after replacing A^3 by $B^2 + DAC^4$, one sees that this equation is equivalent to

$$2DAC^2 - (B^2 + 2DAC^4)kA \equiv 0 \pmod{p}$$

$$\Longleftrightarrow 2DA^2C^2(1 - C^2k) - kAB^2 \equiv 0 \pmod{p}$$

which is true since $p|B$. Then

$$\mathrm{ord}_{\mathfrak{p}}(x(P+P_0)) = \mathrm{ord}_p(z) - 2\mathrm{ord}_p(B) = \mathrm{ord}_p(N(z)) - 2\mathrm{ord}_p(B) = 2\mathrm{ord}_p(B) > 0$$

and

$$\mathrm{ord}_{\bar{\mathfrak{p}}}(x(P+P_0)) = 0 - 2\mathrm{ord}_p(B) = -2\mathrm{ord}_p(B).$$

Putting everything together,

$$\langle P, P_0 \rangle = \text{ideal class of } \prod_{p|B, p\nmid 2A} (p, kA - \sqrt{D})^{\mathrm{ord}_p(B)}$$

To complete the proof, it suffices to show that this ideal class is equal to the ideal class of $\mathfrak{a} = (B_A, kA - \sqrt{D})$. The idea is the same as in Corollary 1. First, we show that $\mathbb{N}(\mathfrak{a}) = B_A$ or $2B_A$. By Proposition 6,

$$\mathbb{N}(\mathfrak{a}) = \gcd(N(B_A), \mathrm{Tr}(B_A(kA - \sqrt{D})), N(kA - \sqrt{D}))$$

$$= B_A \gcd(B_A, 2kA, (k^2A^2 - D)/B_A).$$

Note that $(k^2A^2 - D)/B_A$ is an integer since

$$A(A^2 - DC^4) \equiv 0 \pmod{B} \Longrightarrow A^2 - DC^4 \equiv 0 \pmod{B_A} \Longrightarrow k^2A^2 - D \equiv 0 \pmod{B_A}$$

because $\gcd(A, B_A) = 1$ and $kC^2 \equiv 1 \pmod{B}$. The claim now follows from the fact that $\gcd(B_A, 2kA) = \gcd(B_A, 2) \leq 2$.

When comparing the decomposition of $\mathfrak{a}$ to the product representing $\langle P, P_0 \rangle$, the prime 2 can be ignored since it is inert in K. Now let p be an odd rational prime dividing B_A. Then p does not divide D (or else it would divide A) and it splits in K as $p\mathcal{O}_K = (p, kA + \sqrt{D})(p, kA - \sqrt{D})$, since $(kA)^2 \equiv D \pmod{p}$. Now $kA - \sqrt{D}$ belongs to $\mathfrak{a}$, but p does not divide kA. It follows that $\mathfrak{a}$ is divisible by either $(p, kA + \sqrt{D})$ or $(p, kA - \sqrt{D})$, but not both. Since $\mathfrak{a}$ is clearly contained in $(p, kA - \sqrt{D})$, the ideal $\mathfrak{a}$ is divisible exactly

by $(p, kA - \sqrt{D})^{\mathrm{ord}_p(B_A)} = (p, kA - \sqrt{D})^{\mathrm{ord}_p(B)}$. This completes the proof that

$$\text{class of } \mathfrak{a} = \text{class of } \prod_{p|B, p\nmid A} (p, kA - \sqrt{D})^{\mathrm{ord}_p(B)} = \langle P, P_0 \rangle.$$

□

Soleng's work shows that the homomorphism obtained in Theorem 9 is valid even if the Weierstrass equation is not globally minimal. It would be interesting to see if the homomorphism in Theorem 11 is still valid when the equation is not globally minimal. Maybe this could be proved using Soleng's type of argument.

6.2 A concrete example

As mentioned, the two main hypotheses in Theorem 9 are the global minimality of the Weierstrass equation and the primitivity of the point to which the homomorphism is applied. The next example shows what happens when those hypotheses are not satisfied.

Let $K = \mathbb{Q}(\sqrt{1625})$ and consider the elliptic curve E defined by the Weierstrass equation

$$E: \ Y^2 = X^3 + 10X^2 + 25X - 1625.$$

This curve has discriminant $\Delta = -2^4 5^7 13 \cdot 71$ and the field K has discriminant $D = -4 \cdot 5 \cdot 13$. It follows that 5 ramifies in K, say $5\mathcal{O}_K = \mathfrak{p}_5^2$, and so the Weierstrass equation for E is minimal at all primes of K, except $\mathfrak{p}_5$. With the help of a computer, it can be seen that the Weierstrass class of E/K is the class of $\mathfrak{p}_5$ in $\mathrm{Cl}(K)$. Since this class is not trivial, it follows that E does not have a global minimal Weierstrass equation over K (even if we allow a_1 and a_3 to be non-zero, see [Silverman(2009), VIII§8,Proposition 8.2]). Therefore it is not possible to apply Theorem 9 directly.

With the help of a computer, one sees that the curve

$$Y'^2 = X'^3 + X'^2 - 56X' + 28705$$

is a minimal Weierstrass equation for E at $\mathfrak{p}_5$. The isogeny ϕ between the curves is given by

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

where $(u, r, s, t) = (\sqrt{1625}/65, -45/13, 0, 0)$.

The group $E(\mathbb{Q})$ has rank 2 with generators $P = (10, 25)$ and $Q = (274/9, 5167/27)$. The point Q is primitive, but not P.

Let us determine the image of $\langle P, P_0\rangle$ in $\mathrm{Cl}(K)$, where $P_0 = (0, \sqrt{1625})$. To do so, it is necessary to compute $t_{\mathfrak{p}_5}(P_0), t_{\mathfrak{p}_5}(P)$ and $t_{\mathfrak{p}_5}(P + P_0)$. First,

$$\phi(P + P_0) = (69 + 13/10\sqrt{1625}, 1859/4 + 65/4\sqrt{1625})$$

and $\mathrm{ord}_{\mathfrak{p}_5}(69 + 13/10\sqrt{1625}) = 0$. It follows that $t_{\mathfrak{p}_5}(P + P_0) = 1$. The value of $t_{\mathfrak{p}_5}(P_0)$ and $t_{\mathfrak{p}_5}(P)$ are also equal to $1 \mod \mathcal{O}^{\times}_{K_{\mathfrak{p}_5}}$. For all the other primes $\mathfrak{p}$ of K, the $\mathfrak{p}$-part of $\langle P, P_0\rangle$ is the same in Theorem 9. This proves that the formula of theorem 9 is not valid without the primitivity assumption (the $\mathfrak{p}_5$-parts differ).

The image of $\langle Q, P_0\rangle$ is computed in a similar way. In this case,

$$\frac{t_{\mathfrak{p}_5}(Q)t_{\mathfrak{p}_5}(P_0)}{t_{\mathfrak{p}_5}(0)t_{\mathfrak{p}_5}(Q + P_0)} = \mathfrak{p}_5 \mod \mathcal{O}^{\times}_{K_{\mathfrak{p}_5}}$$

and it turns out that the class of $\langle Q, P_0\rangle$ in $\mathrm{Cl}(K)$ coincides with the class given in Theorem 9 since $\mathfrak{p}_5 = \mathfrak{p}_5^{-1}$.

This example shows that the formula of theorem 9 can still be useful in finding the value of the homomorphism. One simply needs to consider the prime(s) for which the Weierstrass equation is not minimal separately and apply the formula for the other primes.

6.3 A homomorphism into the class group of a cubic extension

In [Soleng(1994)], Soleng asks if it is possible to find homomorphisms between the Mordell-Weil group of elliptic curves and the class group of number fields of degree greater

than two. Considering what we have seen so far, the answer is yes. Indeed, if E is an elliptic curve defined over $\mathbb{Q}$ and P_0 is a point defined over a number field F, then the Mazur-Tate pairing induces a homomorphism $\langle \cdot, P_0 \rangle : E(\mathbb{Q}) \longrightarrow \mathrm{Cl}(F)$. But one question remains: is it possible to find explicit formulas for these homomorphisms?

In this section, the elliptic curve

$$E : \ Y^2 = X^3 - 163X + 163$$

will be analysed and the last question will be discussed. This curve has been chosen because is has some interesting properties. First of all, $E(\mathbb{Q})$ is free of rank 3 as a $\mathbb{Z}$-module with generators $Q = (-11, 25), R = (-7, 31)$ and $S = (-3, 25)$ (i.e. there is no torsion) and has discriminant $\Delta = 2^4 5^4 163^2$. Moreover, the cubic $f(X) = X^3 - 163X + 163$ is irreducible over the rational numbers (Eisenstein at $p = 163$) and has discriminant $5^4 163^2$, which is a square. It follows that $F = \mathbb{Q}(\theta)$ is a cubic Galois extension of $\mathbb{Q}$, where θ is any root of $f(X)$. The number field F has discriminant $D_F = 163^2$ and class group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (this was computed using the Sage computer algebra software). Since 163 is the only rational prime that ramifies in F, it can be seen by looking at Δ that the Weierstrass equation for E is globally minimal over F. Fixing the point $P_0 = (\theta, 0) \in E(F)$, the Mazur-Tate pairing induces a homomorphism $\langle \cdot, P_0 \rangle : E(\mathbb{Q}) \longrightarrow \mathrm{Cl}(F)$. Can this homomorphism be described explicitly?

As in the proof of Theorems 9 and 11, the first thing to do is to take an arbitrary point $P = (x, y) = (A/C^2, B/C^3) \in E(\mathbb{Q})$ and to compute $x(P + P_0)$ explicitly. This gives

$$x(P + P_0) = \frac{(x - \theta_1)(x - \theta_2) - (x + \theta)y^2}{y^2},$$

where θ_1 and θ_2 are the Galois conjugates of θ. Using the relations between θ, θ_1 and θ_2, this expression can be rewritten as

$$x(P+P_0) = \frac{163(163-3x-x^2)+(x^3+163x-2\cdot 163)\theta+(3x^2-163)\theta^2}{y^2}.$$

Using Sage, one sees that this elements has norm

$$N_{F/\mathbb{Q}}(x(P+P_0)) = -163\frac{x^9-163x^8+3\cdot 7\cdot 23\cdot 163x^6-5\cdot 163^2x^5-3\cdot 157\cdot 163^2x^4}{y^6}$$

$$-163\frac{3^2107\cdot 163^2x^3+2\cdot 3\cdot 5^2163^3x^2-2^27\cdot 11\cdot 163^3x-5\cdot 31\cdot 163^3}{y^6}.$$

Those formulas are not simple. For the moment, I have not been able to use them to find a simple closed formula as in the previous theorems. However, given a particular point $P \in E(\mathbb{Q})$, it is possible to compute $\langle P, P_0\rangle$ and to find the image of the homomorphism. First, using Sage it can be seen that $\mathrm{Cl}(F)$ is generated by the class of $\mathfrak{p}_5$ and the class of $\mathfrak{p}_5'$, where

$$\mathfrak{p}_5 = \left(5, \frac{67+11\theta-\theta^2}{25}\right) \quad \text{and} \quad \mathfrak{p}_5' = \left(5, \frac{167+11\theta-\theta^2}{25}\right)$$

are two of the three primes above $5\mathbb{Z}$. Let us now compute $\langle Q, P_0\rangle$. The formula above gives

$$x(Q+P_0)\mathcal{O}_F = \left(\frac{489-138\theta+8\theta^2}{25}\right) = \mathfrak{p}_{163},$$

where $163\mathcal{O}_F = \mathfrak{p}_{163}^3$, and so $\langle Q, P_0\rangle = 1$ in $\mathrm{Cl}(F)$ because the equation for E is globally minimal and $x(Q+P_0)\mathcal{O}_F$ has no denominator. To compute $\langle R, P_0\rangle$, one first finds that

$$x(R+P_0)\mathcal{O}_F = \mathfrak{p}_{163}\mathfrak{p}_{14653}\mathfrak{p}_{31}^{-2},$$

where $\mathfrak{p}_{14653}$ is one of the three primes above $14653\mathbb{Z}$ and $\mathfrak{p}_{31} = (31, (467+11\theta-\theta^2)/25)$ is one of the three primes above $31\mathbb{Z}$. It follows that $\langle R, P_0\rangle =$ class of $\mathfrak{p}_{31} =$ class of $\mathfrak{p}_5$ in $\mathrm{Cl}(F)$. A similar computation gives $\langle S, P_0\rangle = 1$ in $\mathrm{Cl}(F)$.

Since $E(\mathbb{Q})$ has no torsion, this determines the image of the homomorphism: it is the subgroup of $\mathrm{Cl}(F)$ generated by the class of $\mathfrak{p}_5$. In theory, the homomorphism can be computed for every point of $E(\mathbb{Q})$ since it was computed on the generators. However, this is not always possible in practice. Indeed, given a point P in $E(\mathbb{Q})$, there is no quick way of determining the integers a, b and c such that $P = aQ + bR + cS$. In fact, this observation is at the basis of the cryptography systems that use elliptic curves.

To conclude this section, it seems like Soleng's question has only been partially answered. Yes, there are homomorphisms between rational points on elliptic curves and the class group of general number fields, but it seems difficult to find general formulas. Given a specific elliptic curve and a rational point on it, it is theoretically possible to evaluate the homomorphism using a computer. However, the coordinates of the points become so large that the technique outlined above becomes rapidly impractical. The reason is that the Mazur-Tate pairing is defined locally and essentially requires the factorisation of big integers. For instance, I have never been able to find $\langle 10Q, P_0 \rangle$ on a computer.

CHAPTER 7
Further directions

7.1 A more general homomorphism

In his master's thesis [Sivertsen(2000)], Sivertsen studied the elliptic curves defined over $\mathbb{Z}$ of the form

$$E:\ Y^2 + a_3 Y = X^3 + a_2 X^2 + a_4 X + a_6,$$

where a_3 is odd. He found a homomorphism between the primitive points of this curve and the ideal class group of $\mathbb{Q}(\sqrt{a_3^2 + 4a_6})$. It seems reasonable to expect that this homomorphism could be obtained and even generalised (a_3 not necessarily odd and a_1 not necessarily 0) by using the Mazur-Tate pairing. Indeed, note that the point $P_0 = (0, (-a_3 + \sqrt{a_3^2 + 4a_6})/2)$ is on this curve and its coordinates belong to $\mathbb{Q}(\sqrt{a_3^2 + 4a_6})$. In fact, all the necessary formulas are in Lemma 2. The computations will probably be tedious, though.

7.2 A geometric interpretation of the homomorphisms

In [Bhargava(2004)], Bhargava presented a new approach to Gauss composition, more suitable to generalisations. To do so, he considered cubes, where each of the eight vertices are integers. With each such cube, he associates three integral binary quadratic forms (which are all of the same discriminant) and defines a composition law on forms in the following way: the composition of the three forms associated with a cube is 1. In other words, he considers the free abelian group generated by all forms of discriminant D modulo the relation $[f_1] \circ [f_2] \circ [f_3] = 0$ whenever there exists a cube whose associated forms are f_1, f_2 and f_3. The first main result of his paper is that this composition law is the same as Gauss's composition law.

As Bhargava mentioned, his composition law on forms is inspired from the addition law on elliptic curves: imposing the relation $P+Q+R=0$ whenever there is a line (in $\mathbb{P}^2$) going through P, Q and R on the free abelian group generated by the points of $E(F)$ induces the usual addition law on $E(F)$. This suggests that the homomorphisms between $E(K)$ and $\mathrm{Cl}(K)$ in Theorem 11 could be interpreted in terms of tangents, cords and Bhargava cubes. If such a geometric interpretation could be found, it should be relatively easy to prove that it is a homomorphism because of the similarity between the composition laws.

In [Buell(2012)], Buell found a method to make Bhargava's composition law algorithmic. More precisely, given two forms f_1 and f_2 which compose to f_3, he gives a simple method to find a cube whose corresponding forms are f_1, f_2 and f_3^{-1}. This could be a good starting point in our search of a geometric interpretation. Given two points P and Q in $E(\mathbb{Q})$ mapping respectively to the ideals $[A, -kB+\sqrt{a_6}]$ and $[A', -k'B'+\sqrt{a_6}]$, one could first find the cube corresponding to those two forms and then see if there is a pattern. This direction will be explored in the near future.

7.3 Analysing the injectivity and surjectivity of the homomorphisms

As mentioned before, analysing the injectivity and surjectivity of the homomorphisms from $E(\mathbb{Q})$ to the class group of a quadratic field is important. Suppose for a moment that one could find conditions under which one of these homomorphisms is surjective. Since it is relatively easy to find the class number of a quadratic field, surjectivity could give a lower bound on the rank of the elliptic curve. In this section, we present the first steps of this analysis of injectivity and surjectivity.

Let E be an elliptic curve defined by the Weierstrass equation

$$E:\ Y^2 = X^3 + a_2X^2 + a_4X + a_6,$$

where the a_i are integers and a_6 is square-free and congruent to 2 or 3 mod 4 and denote Soleng's homomorphism by $\phi : E(\mathbb{Q}) \longrightarrow \mathrm{Cl}(K)$. To compute the kernel of ϕ and study its image, the following lemma will be used:

Lemma 3. *Let $\mathfrak{a}$ be an ideal in an order $\mathcal{O}$ in K. Then $\mathfrak{a}$ is principal if and only if there exists $\alpha \in \mathfrak{a}$ such that $\mathbb{N}(\mathfrak{a}) = |N(\alpha)|$.*

Proof. Recall that if α is an element in $\mathcal{O}$, then $\mathbb{N}(\alpha\mathcal{O}) = |N(\alpha)|$. If $\mathfrak{a}$ is principal, then $\mathfrak{a} = \alpha\mathcal{O}$ for some $\alpha \in \mathfrak{a}$ and the claim follows from the previous remark. Conversely, if $\alpha \in \mathfrak{a}$, then $\alpha\mathcal{O} \subseteq \mathfrak{a}$. Since $\mathbb{N}(\mathfrak{a}) = |N(\alpha)|$ is the index of $\mathfrak{a}$ and $\alpha\mathcal{O}$ in $\mathcal{O}$, equality follows. □

With this lemma, it is possible to find a system of Diophantine equations that describes the kernel of ϕ. Let $P = (A/C^2, B/C^3)$ be a rational point on E such that $\phi(P) = 1$ in $\mathrm{Cl}(K)$. In Corollary 1, we saw that $\mathbb{N}(A, -kB + \sqrt{a_6}) = |A|$. It follows that

$$(A, -kB + \sqrt{a_6}) = [A, -kB + \sqrt{a_6}],$$

since the second ideal is contained in the first and they both have the same norm. Then $\phi(P)$ is principal if and only if there exists integers x and y such that

$$|N(xA + y(-kB + \sqrt{a_6}))| = \mathbb{N}([A, -kB + \sqrt{a_6}]) = |A|$$

$$\iff |A^2x^2 - 2kABxy + ((kB)^2 - a_6)y^2| = |A|.$$

Since $(kB)^2 \equiv a_6 \pmod{A}$, the last equation can be written as

$$Ax^2 - 2kBxy + \frac{(kB)^2 - a_6}{A}y^2 = \pm 1.$$

Note that this quadratic form has discriminant $4a_6$. This proves that the kernel of ϕ is described by the system of Diophantine equations

$$\begin{cases} B^2 = A^3 + a_2A^2C^2 + a_4AC^4 + a_6C^6 \\ Ax^2 - 2kBxy + \frac{(kB)^2 - a_6}{A}y^2 = \pm 1 \\ kC^3 + Al = 1 \end{cases},$$

where A, B, C, x, y, k and l are integers.

For surjectivity, first fix a class $\mathcal{C}$ in $\mathrm{Cl}(K)$ and let $\mathfrak{c}$ be an integral ideal representing this class. Suppose that $\mathfrak{c} = [a', b' + g'\sqrt{a_6}]$, where a', b' and g' are integers. Since $g'|a', b'$ (see Theorem 3), we can suppose that $\mathfrak{c} = [a, b+\sqrt{a_6}]$ since the ideals differ by the principal ideal $g'\mathcal{O}_K$. Determining if $\mathfrak{c}$ is in the image of ϕ is equivalent to determining if there exists a point $P = (A/C^2, B/C^3) \in E(\mathbb{Q})$ such that $[A, -kB + \sqrt{a_6}][a, b + \sqrt{a_6}]$ is principal. Indeed, this would imply that $\phi(-P)$ is $\mathcal{C}$, the class of $\mathfrak{c}$. Using the lemma above again to write this statement in terms of Diophantine equations gives

$$\mathbb{N}([A, -kB+\sqrt{a_6}][a, b+\sqrt{a_6}]) = |N(raA+sA(b+\sqrt{a_6})+ta(kB-\sqrt{a_6})+u(b+\sqrt{a_6})(kB+\sqrt{a_6}))|$$

$$\Leftrightarrow |aA| = |N(raA + sA(b + \sqrt{a_6}) + ta(kB - \sqrt{a_6}) + u(b + \sqrt{a_6})(kB + \sqrt{a_6}))|,$$

where r, s, t and u are integers. Expanding the norm of the term on the right and grouping like terms gives

$$\begin{aligned} |aA| =& |a^2\left(A^2r^2 - a_6t^2\right) + 2a\left(A^2r(bs + Bkt) + A(-a_6ru + \mathrm{a6}st + bBkru) + a_6b(k-1)tu\right) \\ &+ A^2\left((bs + Bkt)^2 - a_6s^2\right) + 2Aku(bB(bs + Bkt) - a_6(bs + Bt)) \\ &+ u^2\left(a_6^2 - a_6b\left(b(k-1)^2 + 2Bk\right) + b^2B^2k^2\right)|. \end{aligned}$$

In a similar way as above, this gives a systems of Diophantine equations.

It would be interesting to see if those systems have a geometric interpretation in terms of invariants of the elliptic curve. But recall that the homomorphism depends on the Weierstrass equation that is chosen. For example, by changing the variables $X = X' + n$ and $Y = Y'$, the constant term of the Weierstrass equation for E changes from a_6 to $n^3 + a_2n^2 + a_4n + a_6$ and the homomorphism lands in the order $\mathbb{Z}[\sqrt{n^3 + a_2n^2 + a_4n + a_6}]$ instead of $\mathbb{Z}[\sqrt{a_6}]$. For this reason, the existence of a criteria of the form *"Let E be an elliptic curve with invariant property X, then the homomprhism is surjective."* seems unlikely. Nonetheless, surjectivity certainly needs to be analysed in greater detail.

CHAPTER 8
Conclusion

In this thesis, we proved that once the obvious point $P_0 = (0, \sqrt{a_6})$ was found on the elliptic curve $E : \ Y^2 = X^3 + a_2X^2 + a_4X + a_6$, the Mazur-Tate pairing induces Soleng's homomorphism under certain conditions. We also proved the Buell's homomorphism coincides with Soleng's at least in the case where a_6 is negative and $\mathbb{Z}[\sqrt{a_6}]$ is the maximal order in $\mathbb{Q}(\sqrt{a_6})$. In the other cases, the two homomorphism are still essentially equivalent. As noted in the last chapter, chances are that the Mazur-Tate pairing could be used to find a homomorphism between the rational points of the elliptic curve $E : \ Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$ and the class group of $\mathbb{Q}(\sqrt{a_3^2 + 4a_6})$, generalising the above homomorphisms and generalising Sivertsen's homomorphism. The only obstacle is to find the correct generalisation of the notion of primitive point, which was of great help in the proof of Theorem 9.

The global minimality hypothesis may seem very restrictive in Theorems 9 and 11, but it is essential. As the examples of Chapter 6 prove, the techniques can still be applied if the equation is not globally minimal as one simply needs to consider the non-minimal primes separately. In the same chapter, the question of the existence of homomorphisms between the Mordell-Weil group of elliptic curves and the class group of general number fields has been partially answered. Indeed, given an elliptic curve E and a number field F, a homomorphism is given by $\langle \cdot, P_0 \rangle : E(F) \longrightarrow \mathrm{Cl}(F)$, where $P_0 \in E(F)$. It is still not clear however that these homomorphisms can be described by general explicit formulas.

As the reader may have noticed, the question of obtaining Soleng's homomorphism using the Mazur-Tate pairing when $\mathbb{Z}[\sqrt{a_6}]$ is not the maximal order remains unanswered.

For many reasons, I believe the answer to this question is that the Mazur-Tate cannot induce Soleng's homomorphism in its whole generality. The main reason is that in order to compare the product of ideals obtained via the Mazur-Tate pairing with the ideal in Soleng's homomorphism, unique factorisation of ideals was used. However, this unique factorisation fails in every non-maximal order. In fact, the only ideals which factor uniquely in an order are those that are prime to the conductor (this follows from the isomorphism $I(\mathcal{O}_K, f) \cong I(\mathcal{O}, f)$, where f is the conductor of $\mathcal{O}$). But looking at the ideal in the statement of Theorem 9, one sees that the ideal is not prime to the conductor (see Remark 1). One could try to ignore the ideals that divide the conductor, i.e. define a new homomorphism $C \longrightarrow \mathrm{Cl}(\mathbb{Z}[\sqrt{a_6}])$ which sends an idèle class to the corresponding product of primes in $\mathrm{Cl}(\mathbb{Z}[\sqrt{a_6}])$, except that the primes that divide the conductor are omitted. But the ideal in Soleng's homomorphism is not always prime to the conductor (take the primitive point $P = (180, 2415) \in E(\mathbb{Q})$, where $E: \ Y^2 = X^3 + X + 3^2 5$), so it seems unlikely that the product of ideals prime to the conductor obtained via the pairing will be equal to this ideal.

Finally, many questions still need to be answered. Hopefully, most of them will be answered in the near future.

REFERENCES

[Bekyel(2004)] E. Bekyel. The density of elliptic curves having a global minimal weierstrass equation. *Journal of Number Theory*, (109):41–58, 2004.

[Bhargava(2004)] M. Bhargava. Higher composition laws: A new view on gauss composition. *Annals of Mathematics*, (159):217–250, 2004.

[Buell(1977)] D.A. Buell. Elliptic curves and class groups of quadratic fields. *J. London Math. Soc.*, pages 19–25, 1977.

[Buell(2012)] D.A. Buell. Ideal composition in quadratic fields: from Bhargava to Gauss. *Ramanujan J.*, pages 31–49, 2012.

[Conrad(2014)] K. Conrad. Factoring in quadratic fields, 2014. Available at www.math.uconn.edu/ kconrad/blurbs/.

[Cox(1989)] D.A. Cox. *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication.* Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts. Wiley, 1989.

[Flath(1989)] D.E. Flath. *Introduction to number theory.* Wiley-interscience publication. John Wiley & Sons, Incorporated, 1989.

[Janusz(1996)] G.J. Janusz. *Algebraic Number Fields.* Advances in the Mathematical Sciences. American Mathematical Society, 1996.

[Laska(1982)] M. Laska. An algorithm for finding a minimal weierstrass equation for an elliptic curve. *Mathematics of Computation*, 38(157), 1982.

[Mazur and Tate(1983)] B. Mazur and J. Tate. Canonical height pairings via biextensions. In *Arithmetic and Geometry*, volume 35 of *Progress in Mathematics*, pages 195–237. Birkhäuser Boston, 1983. ISBN 978-0-8176-3132-1.

[Mazur and Tate(1987)] B. Mazur and J. Tate. Refined conjectures of the "birch and swinnerton-dyer type". *Duke Mathematical Journal*, 54(2), 1987.

[Milne(2012)] J.S. Milne. Algebraic number theory (v3.04), 2012. Available at www.jmilne.org/math/.

[Serre(1999)] J.P. Serre. *Oeuvres, Collected Papers: 1985-1998*, 1999.

[Silverman(1994)] J.H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Graduate texts in mathematics. Springer-Verlag, 1994.

[Silverman(2009)] J.H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer, 2009.

[Sivertsen(2000)] T.K. Sivertsen. Klassgrupper, elliptiske kruver og kryptografi. Master's thesis, University of Tromso, 2000.

[Soleng(1994)] R. Soleng. Homomorphisms from the group of rational points on elliptic curves to class groups of quadratic number fields. *Journal of number theory*, pages 214–229, 1994.