[chapter]

Heegner points on elliptic curves of conductor less than 3000

Antoine Gournay

Department of Mathematics and Statistics,

McGill University, Montréal

Québec, Canada

June, 2004

A thesis submitted to the Faculty of Graduate Studies and Research

in partial fulfillment of the requirements of the degree of

Master of Science

Abstract

Elliptic curves are one of the important class of problems in diophantine equations. In this thesis, we describe how to obtain algebraic points (called Heegner points) on elliptic curves. We first go over the necessary definitions and theorems in order to properly study these points and their properties. We pay a particular attention to the property of these point to have integral coordinates or not. We also explain how to make explicit computations of these points and discuss the result of extensive computations made on the elliptic curves of conductor less than 3000, and give a list of the curves that were found to always have Heegner points with integral coordinates.

Résumé

Les courbes elliptiques sont une classe de problèmes importante d'équation diophantienne. Dans ce mémoire nous décrirons comment il est possible d'obtenir des points algébriques, appelés points de Heegner, sur les courbes elliptiques. Quelques éléments essentiels pour mener à bien la construction de ces points seront d'abord rappelés. On verra comment faire des calculs explicites de ces points, et on discutera ensuite des résultats de ces calculs fait sur les courbes de conducteur inférieur à 3000. Une attention particulière sera réservée l'intégralité des points de Heegner, plus précisement aux courbes dont les points de Heegner ont toujours des coordonnées intégrales.

Acknowledgments

First of all, I would like to thank my supervisor Henri Darmon, for his help, support and enthusiasm these last years. I would also like to thank NSERC for allowing me to pursue my studies in mathematics. I also want to thank McGill University, and in particular the Mathematics and Statistics department and its professors: I learned valuable knowledge from them in all branches of mathematics. I would also like to thank my fellow students and friends, particularly Hugo, for the all the advices and distractions.

Table of Contents

Introduction

The diophantine problem consists in finding solutions over the integers or the rational numbers to polynomial equations. After the linear case (for example $ax + by + c = 0$ solved by the euclidian algorithm) and the quadratic case (for example Pell's equation), the next degree of complexity comes with elliptic curves. Like the two first examples where solutions can be seen as an abelian group (albeit a infinite cyclic group), solutions to the diophantine problem of an elliptic curve form an abelian group, via the chord and tangent method. Though it has been shown that elliptic curves over a finite field or a number field K are finitely generated, there is still no reliable method to find the generators.

In the last decades, there emerged the idea that elliptic curves could be parametrized by another object. Looking at certain subgroups of $SL_2(\mathbb{Z})$ acting by M obius transformations on the complex upper half-plane $\mathcal{H}$, it is possible to form new Riemann surfaces by the usual quotient operation. These surfaces are not compact, however a proper compactification turns them into complete complex algebraic varieties, called modular curves. Thanks to the work of Wiles and all the improvements that have been made to it, we are now aware that a model over $\mathbb{Q}$ of these varieties admits an algebraic map to a certain class of elliptic curves (see [25], [24], [6], [3], [2] and [7]).

Gross and Zagier used this map to construct points on elliptic curves. The algebraicity of this parametrization gives Galois control on the image of this map. Heegner points are points on the modular curve of which we know that the image by

the modular parametrization are going to be algebraic. Apart from being an explicit method to get an algebraic point on a curve, it is also possible to make actual calculations of this point. Though these points have been used to prove important results related to the Birch and Swinnerton-Dyer conjecture, few of them have actually been computed.

In the following pages we will make a brief recall of the concepts and results necessary in order to define properly Heegner points and study their basic properties. In hope of getting more insight on the modular parametrization, explicit computations of such points have been made on all the elliptic curves of conductor less than 3000. A question that is of particular concern to us, is whether coordinates of the Heegner points obtained are algebraic integer or not, and if this is not the case, does the modular parametrization maps certain points of the modular curve (non-cuspidal point) to the point at infinity of the elliptic curve.

Chapter 1

Elliptic Curves

This chapter begins by a very brief recall of the concepts that are necessary to define Heegner points. A complete discussion of these subjects can be found in [15] and [22]. However, we will go more leisurely over the theory of complex multiplication for it is crucial in the constructions we wish to make.

1.1 Definitions and Basic Properties

Definition 1.1. An elliptic curve E over a field F (denoted $E_{/F}$) is an algebraic curve of genus 1, possessing a specified base point.

One can show ([22] III.§3) that an elliptic curve over F is isomorphic to the zero locus in $\mathbb{P}^2(\overline{F})$ of an equation

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{1.1}$$

where $a_i \in F$ and the specified base point is the "point at infinity" denoted $O_E = [0, 1, 0]$. This is known as the Weierstrass equation of E. When $K \supseteq F$, we write $E(K)$ to denote the zero locus of the same equation in $\mathbb{P}^2(K)$. To ease notation, it is convenient to write $x = X/Z$ and $y = Y/Z$, O_E being the only point which cannot

be described by (x, y). If $\text{char}(F) \neq 2$ then one can replace y by $\frac{1}{2}(y - a_1x - a_3)$ to get

$$\begin{aligned} &E : y^2 = x^3 + b_2x^2 + b_4x + b_6 \\ &\text{where } b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3, \quad \text{and } b_6 = a_3^2 + 4a_6 \end{aligned} \tag{1.2}$$

Definition 1.2. Let $b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$, then we define

$$\begin{aligned} \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\ \text{and} \quad \omega &= dx/(2y + a_1x + a_3) = dy/(3x^2 + 2a_2x + a_4 - a_1y) \end{aligned} \tag{1.3}$$

as respectively the discriminant and the invariant differential (unique up to scalar multiplication) of the Weierstrass equation, and

$$j = (b_2^2 - 24b_4)^3/\Delta \tag{1.4}$$

as the j-invariant of the elliptic curve E.

One can check that the only change of variables that preserve the Weierstrass form and fix $O_E = [0, 1, 0]$ are of the form $x = u_0^2x' + u_2$ and $y = u_0^3y' + u_0^2u_1x' + u_3$ for $u_0, u_1, u_2, u_3 \in K$ and $u_0 \neq 0$. When two equations are related by such a transformation we say that they are equivalent, or that the 2 curves they describe are isomorphic over $K \supseteq F$. The quantities we just defined change as follows:

$$\Delta = u_0^{12}\Delta', \; u_0\omega = \omega' \text{ and } j = j' \tag{1.5}$$

In particular, if $u_i = 0$ for $i = 1, 2, 3$ then one has that $u_0^ja'_j = a_j$ and $u_0^jb'_j = b_j$. This makes the j-invariant stand out as a quantity independent of the equation chosen to represent E. In fact, if two curves have the same j-invariant then they are isomorphic over $\overline{F}$ as algebraic curves. Also, since E has genus one, ω is the only holomorphic non-vanishing differential, up to scalar multiplication, attached to the Weierstrass equation. Simple calculations ([22] III.§1) reveal that $\Delta = 0$ if and only if the curve E is singular.

Actually if $P = (x_0, y_0)$ is a singular point, it is instructive to consider the Taylor expansion of the curve equation at that point. Let $f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$, then $f(x_0, y_0) = 0$, $\frac{\partial f}{\partial x}(x_0, y_0) = 0$ and $\frac{\partial f}{\partial y}(x_0, y_0) = 0$. Thus,

$$f(x, y) - f(x_0, y_0) = ((y - y_0) - \alpha(x - x_0))((y - y_0) - \beta(x - x_0)) - (x - x_0)^3 \quad (1.6)$$

where α and β are at most in a quadratic extension of F. We distinguish two types of singular points:

Definition 1.3. We say P is a node (resp. cusp) if $\alpha \neq \beta$ (resp. $\alpha = \beta$), it then has two tangent lines $y - y_0 = \alpha(x - x_0)$ and $y - y_0 = \beta(x - x_0)$ (resp. one tangent line $y - y_0 = \alpha(x - x_0)$).

Further inspection of these cases show that E has a unique cusp when $\Delta = b_2^2 - 24b_4 = 0$ and a unique node when $\Delta = 0, b_2^2 - 24b_4 \neq 0$.

Lastly, since elliptic curves are algebraic varieties with a specified point it makes sense to define a more refined class of morphisms:

Definition 1.4. Let $E_{/F}$ and $E'_{/F}$ be two elliptic curves. An isogeny of E to E' over $K \supseteq F$ is a non-constant morphism $f : E \to E'$ defined over K such that $f(O_E) = O_{E'}$. Two curves E and E' are said to be isogenous if such an isogeny exists over $\overline{F}$.

Since morphisms of curves are either constant or surjective (with each point having a finite preimage), either $f(E) = \{O_{E'}\}$ or $f(E(K)) = E'(K)$. Like all morphism of curves we can define the (separable, inseparable) degree of an isogeny as the (separable, inseparable) degree of the extension $K(E)/f^*K(E')$ where $K(E)$ is the function field of E. Over fields of characteristic $p > 0$, if the pullback of a differential by an isogeny is 0, then it is inseparable. Also, if the curve is non-singular and the isogeny is inseparable, then $f = \lambda \circ Fr$ where Fr is the q^{th}-power Frobenius map ($q = \deg_i(f)$ is a power of p), and λ is separable (see [22] II and [12]).

1.2 The Group Law

One of the crucial properties of elliptic curves is that one can explicitly construct a point on the curve from two other ones. On the real numbers, the method is simple. First make a change of variables to get $E : y^2 = x^3 + b_2x^2 + b_4x + b_6$. Then the line through two points (say P and Q) on the curve intersects a third point (if one consider the point at infinity to be on all the lines with x constant). The reflection of this point by the x-axis is called $P + Q$. We can extend this construction when $P = Q$ by taking the tangent at P. Interestingly, we can express the coordinates $P + Q$ explicitly as an algebraic formula on the coordinates of P and Q (see [22] III.2). As a consequence, we can extend this construction to any number field F, and the resulting point is always defined on F. Note that these formulas can be found without making a change of variables so that even when $\mathrm{char}(F) = 2$, the points can be combined.

The most interesting property of the construction $+$ is that it defines an abelian group law on the points $E(F)$ with identity element O. This law also enables us turn the set of isogenies from A to A' over K, into a group $\mathrm{Hom}_K(A, A')$ with the law $(f + g)(P) = f(P) + g(P)$ for f, g isogenies. As usual, we define the ring of endomorphism $\mathrm{End}_K(A) = \mathrm{Hom}_K(A, A)$ by setting multiplication as composition.

It is important to point out that the group law on E gives a map from $\mathbb{Z}$ to $\mathrm{End}_K(E)$. For $n \in \mathbb{Z}_{\geq 0}$ we define $[n](P) = P + \cdots + P$ (n times) , and for $n \in \mathbb{Z}_{<0}$, $[n]P = [-n](-P)$. This is always an injection, and in fact $\mathrm{End}_K(E)$ is $\mathbb{Z}$-module of rank one, two or four. Over fields of characteristic 0, elliptic curves with endomorphism ring bigger than $\mathbb{Z}$ have many additional properties, and the last section of this chapter is devoted to their study.

Before going on, we will state 3 important theorems that explain the structure of the group of E:

Theorem 1.1. (Singular curves) *Let $E_{/F}$ be a elliptic curve defined over a field F by a singular Weierstrass equation. If the singular point on E is a cusp, then $E(F) \simeq F^+$. If the singular point is a node, let α, β be the slopes of the tangent lines at the node, and set $K = F(\alpha) = F(\beta)$. If $K = F$ then $E(F) \simeq F^\times$. If $[K : F] = 2$ then $E(F) \simeq \{x \in K^\times \mid N_{K/F}(x) = 1\}$.*

Theorem 1.2. (Mordell-Weil) *Let E be a non-singular elliptic curve defined over a number field F. The abelian group $E(F)$ is finitely-generated. It's rank over $\mathbb{Z}$ is called the rank of E over F.*

Theorem 1.3. (Weierstrass uniformisation) *Let E be a non-singular elliptic curve defined over $\mathbb{C}$, then there is a lattice $\Lambda \subseteq \mathbb{C}$ (i.e. a discrete subgroup of $(\mathbb{C}, +)$ of rank 2 over $\mathbb{Z}$) such that there is a complex analytic Lie group isomorphism of $E(\mathbb{C})$ with $\mathbb{C}/\Lambda$. The isomorphism is defined as follows: let ω_E be the invariant differential of E, let Ω_1 and Ω_2 be two closed paths on $E(\mathbb{C})$ that generate the fundamental group, let $\omega_i = \int_{\Omega_i} \omega_E$, and let $\Lambda_E = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_1$ be the Néron lattice of E. Then the isomorphism is given by*

$$\begin{aligned} \Phi_w^{-1} : E(\mathbb{C}) &\to \mathbb{C}/\Lambda \\ P &\mapsto \textstyle\int_O^P \omega_E \pmod{\Lambda} \end{aligned} \tag{1.7}$$

Conversely, if Λ is lattice in $\mathbb{C}$, then

$$\begin{aligned} \Phi_w : \mathbb{C}/\Lambda &\to E(\mathbb{C}) : y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda) \\ z &\mapsto \Phi_w(z) = (\wp_\Lambda(z), \wp'_\Lambda(z)) \\ 0 &\mapsto O \end{aligned} \tag{1.8}$$

$$\begin{aligned} \textit{where} \quad & \wp_\Lambda(z) = \tfrac{1}{z^2} + \sum_{\lambda \in \Lambda - \{0\}} \left(\tfrac{1}{(z-\lambda)^2} - \tfrac{1}{\lambda^2} \right) \\ \textit{and} \quad & g_2(\Lambda) = 60 \sum_{\lambda \in \Lambda - \{0\}} \tfrac{1}{\lambda^4} \\ & g_3(\Lambda) = 140 \sum_{\lambda \in \Lambda - \{0\}} \tfrac{1}{\lambda^6} \end{aligned} \tag{1.9}$$

is the inverse isomorphism, with $\Phi_w^*(dx/y) = dz$.

The full strength of the last theorem is summarized as the equivalence of the following categories:

$$\left\{ \begin{array}{c} \text{Elliptic curves over } \mathbb{C} \\ \text{with isogenies} \end{array} \right\} \simeq \left\{ \begin{array}{c} \text{tori } \mathbb{C}/\Lambda \text{ with analytic} \\ \text{maps sending 0 to 0} \end{array} \right\} \tag{1.10}$$

This equivalence will be very useful to study $\mathrm{End}_K(E)$, as isogenies are more difficult to characterize a priori than analytic maps from $\mathbb{C}/\Lambda$ to itself.

Since all curves isomorphic over $\mathbb{C}$ have the same j-invariant, it is convenient to denote the j-invariant of E by $j(\tau)$ where the lattice Λ associated to E is homothetic to $\langle 1, \tau \rangle := \mathbb{Z} \oplus \mathbb{Z}\tau$, and $\Im(\tau) > 0$. Similarly $\Delta(\tau)$ stands for the discriminant of the equation of the curve $\Phi_w(\mathbb{C}/\langle 1, \tau \rangle)$. Note that the choice of τ is made up to the action of $SL_2(\mathbb{Z})$ as described by A.4.

1.3 Reduction modulo $\mathfrak{p}$

Weierstrass uniformisation shows us that we gain insight on curves defined over a number field by looking at them over a larger field (namely $\mathbb{C}$). One could then be tempted to do the same but looking at "smaller" fields, namely the finite fields obtained by looking at the algebraic integers modulo some prime ideal. A naive idea would be to look at the Weierstrass equation modulo some prime $\mathfrak{p}$. Of course, for such a thing to be possible we first have to make sure the a_i are integers in F. Since the change of variables $\phi : (x, y) \mapsto (u^{-2}x, u^{-3}y)$ multiplies each a_i by u^i, it is always possible to do so. However, taking $u \in \mathfrak{p}^k$ for k big enough would make all the coefficients reduce to 0 (mod $\mathfrak{p}$), so we have to find a proper equation before reducing.

Definition 1.5. Let $E_{/F}$ an elliptic curve defined over F, R be the ring of integers of F, $\mathfrak{p}$ be a prime ideal of R, and $\nu_\mathfrak{p}$ be the valuation at $\mathfrak{p}$. The Weierstrass equation

$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ is said to be minimal for a prime $\mathfrak{p}$ of R if of all equations $y^2 + a'_1xy + a'_3y = x^3 + a'_2x^2 + a'_4x + a'_6$ describing the curve E with $a'_i \in R$ for $i = 1, 2, 3, 4, 6$, $\nu_\mathfrak{p}(\Delta(a_i)) \leq \nu_\mathfrak{p}(\Delta(a'_i))$.

Note that the possible values of $\nu_\mathfrak{p}(\Delta)$ form a discrete set ($a_i \in R$), thus it takes a minimal value. Once we have found this minimal equation, we can define the reduction of E at $\mathfrak{p}$ (written $\widetilde{E}_\mathfrak{p}$) as the curve over $R/\mathfrak{p}$ whose equation has the same coefficients but modulo $\mathfrak{p}$. Amongst many thing, this reduced elliptic curve helps to determine the torsion on the original curve (see [22] V). Sometimes, it may happen that for a given prime the valuation of Δ_E is greater than 0 even when E is described by the minimal equation. In this case, the reduced curve is singular, $\Delta \equiv 0 \pmod{\mathfrak{p}}$. For these primes we say that E has bad reduction.

Definition 1.6. Let E an elliptic curve defined over F, and $\mathfrak{p}$ a prime for which the reduction of E at $\mathfrak{p}$ is a singular curve. We say that $E_{/F}$ has bad reduction at $\mathfrak{p}$. Furthermore,

1. if $\widetilde{E}_\mathfrak{p}$ has a cusp then $E_{/F}$ has additive bad reduction at $\mathfrak{p}$.
2. if $\widetilde{E}_\mathfrak{p}$ has a node and $\widetilde{E}_\mathfrak{p}(R/\mathfrak{p}) \simeq (R/\mathfrak{p})^\times$ then $E_{/F}$ has split multiplicative reduction at $\mathfrak{p}$.
3. if $\widetilde{E}_\mathfrak{p}$ has a node and $\widetilde{E}_\mathfrak{p}(R/\mathfrak{p}) \not\simeq (R/\mathfrak{p})^\times$ then $E_{/F}$ has non-split multiplicative reduction at $\mathfrak{p}$.

Finally, when $\widetilde{E}_\mathfrak{p}$ is non-singular we say that $E_{/F}$ has good reduction at $\mathfrak{p}$.

Note that since Δ is only divisible by finitely many primes, the number of primes with bad reduction is always finite for a given elliptic curve. There is a ideal that one usually associates to an elliptic curve $E_{/F}$ to encode the bad and good reduction. Though a proper definition would require the introduction of many concept from the

representation theory of local fields (see [23] IV.§10), we can almost always reduce to the following one:

Definition 1.7. The arithmetic conductor of a curve $E_{/F}$ is $\mathfrak{N} = \prod_{\text{prime } \mathfrak{p} \lhd R} \mathfrak{p}^{f(\mathfrak{p})}$, where $f(\mathfrak{p})$

is 0 when $E_{/F}$ has good reduction at $\mathfrak{p}$

is 1 when $E_{/F}$ has multiplicative reduction at $\mathfrak{p}$

is 2 when $E_{/F}$ has additive reduction at $\mathfrak{p}$ and $\mathfrak{p} \mid p \geq 5$

is greater or equal to 2 otherwise.

When $K = \mathbb{Q}$ we define the conductor to be the positive integer such that $(N) = \mathfrak{N}$.

Note that both definition 1.6 and 1.7 depend heavily on the field over which the curve is defined.

One of the interesting properties of reducing elliptic curves is that when the reduction is good, the degree of the isogenies remain unchanged. Another interesting quality of the reduced curve $\widetilde{E}_{\mathfrak{p}}(R/\mathfrak{p})$ is its number of elements, $n_{\mathfrak{p}}$. As we do not expect a cubic polynomial to favor squares over non-squares in its value, it seems reasonable to give $|\mathfrak{p}| + 1 := N_{F/\mathbb{Q}}(\mathfrak{p}) + 1$ as an estimate of $n_{\mathfrak{p}}$ (when the reduction is good), as every square value of the polynomial give two root, and we expect them to happen 50% of the time ($|\mathfrak{p}| = \sharp R/\mathfrak{p}$). We then define $a_{\mathfrak{p}} = |\mathfrak{p}| + 1 - n_{\mathfrak{p}}$ as our error term. However, when $E_{/F}$ has bad reduction at $\mathfrak{p}$, our estimate should be $|\mathfrak{p}|$ as we have to take out the singular point, and one can find, thanks to theorem 1.5, that $a_{\mathfrak{p}}$ is 0 (resp. 1, -1) when $E_{/F}$ has additive (resp. split, non-split multiplicative) reduction.

We can now define the L-series of $E_{/F}$ as

$$L(E_{/F}, s) = \prod_{\text{prime } \mathfrak{p} \lhd R} L_{\mathfrak{p}}(E_{/F}, |\mathfrak{p}|^{-s})^{-1} \tag{1.11}$$

$$\begin{array}{rll} \text{where} & L_{\mathfrak{p}}(E_{/F}, X) & = 1 - a_{\mathfrak{p}}X + |\mathfrak{p}|X^2 \quad \text{when } \mathfrak{p} \text{ has good reduction} \\ & L_{\mathfrak{p}}(E_{/F}, X) & = 1 - a_{\mathfrak{p}}X \qquad\qquad\quad \text{when } \mathfrak{p} \text{ has bad reduction} \end{array} \tag{1.12}$$

Note that $L_{\mathfrak{p}}(E_{/F}, |\mathfrak{p}|^{-1}) = n_{\mathfrak{p}}/|\mathfrak{p}|$.

1.4 Complex Multiplication

As we observed in the first section of this chapter, the nature of the group structure that we defined on an elliptic curve enables us to embed $\mathbb{Z}$ in the ring of endomorphisms of the curve. Though in most cases this map is also surjective, there also exist curves with endomorphism ring bigger than $\mathbb{Z}$. We will devote the rest of this chapter to the study of these curves, which will be henceforth referred to as CM curves or curves with complex multiplication.

1.4.1 Endomorphisms rings

Our first step will be to attempt to describe $\mathrm{End}(E)$. As we are only concerned about fields of characteristic 0, it will be enough to do it over $\mathbb{C}$. The general case will follow from the Lefschetz principle (see [22] VI.§6). We can reduce to an easier problem using Weierstrass uniformisation. Indeed, since elliptic curves over $\mathbb{C}$ are isomorphic to $\mathbb{C}/\Lambda$ (as Riemann surfaces), where $\Lambda = \langle \omega_1, \omega_2 \rangle$ is a lattice, it is sufficient to look at their endomorphism ring.

First, let's show that $\mathrm{End}(\mathbb{C}/\Lambda) = \{\alpha \in \mathbb{C} \mid \alpha\Lambda \subseteq \Lambda\}$. If $\alpha \in \mathbb{C}$ is such that $\alpha\Lambda \subseteq \Lambda$ then $f(z) = \alpha z \in \mathrm{End}(\mathbb{C}/\Lambda)$.

Conversely, take $f \in \mathrm{End}(\mathbb{C}/\Lambda)$, then f is an analytic map sending 0 to 0. There is a projection p (so also a covering map) from $\mathbb{C}$ to $\mathbb{C}/\Lambda$. From algebraic topology, namely the general lifting lemma, $\{1\} = (f \circ p)_*(\pi_1(\mathbb{C})) \subseteq p_*(\pi_1(\mathbb{C})) = \{1\}$, where π_1 is the fundamental group, guarantees the existence of a lift of $f : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$ to

$\tilde{f} : \mathbb{C} \to \mathbb{C}$, such that the diagram commutes:

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\tilde{f}} & \mathbb{C} \\ {\scriptstyle p}\downarrow & & {\scriptstyle p}\downarrow \\ \mathbb{C}/\Lambda & \xrightarrow{f} & \mathbb{C}/\Lambda \end{array} \tag{1.13}$$

But $\tilde{f}$ is easy to describe:

$$\begin{array}{rlll} & p \circ \tilde{f}(z+\lambda) & = p \circ \tilde{f}(z) & \forall z \in \mathbb{C}, \forall \lambda \in \Lambda \\ \Rightarrow & \tilde{f}(z+\lambda) & \equiv \tilde{f}(z) \pmod{\Lambda} & \forall z \in \mathbb{C}, \forall \lambda \in \Lambda \\ \Rightarrow & \tilde{f}(z+\lambda) & -\tilde{f}(z) \in \Lambda & \forall z \in \mathbb{C}, \forall \lambda \in \Lambda \end{array} \tag{1.14}$$

However Λ is a discrete set, and $\tilde{f}(z+\lambda) - \tilde{f}(z)$ is a holomorphic function, so it must be a constant possibly depending on λ. Taking the derivative, one has that $\tilde{f}'(z+\lambda) - \tilde{f}'(z) = 0 \; \forall \lambda \in \Lambda$ which means that $\tilde{f}'(z)$ is bounded on $\mathbb{C}$, and consequently also a constant (by Liouville's theorem). We can then conclude that $\tilde{f}(z) = \alpha z + \beta$. Finally since $\tilde{f}(0) \in \Lambda$, we get that $f(z) = \alpha z + \beta$ with $\alpha\Lambda \subseteq \Lambda$ and $\beta \in \Lambda$. Without loss of generality we can assume that $\beta = 0$

So $\mathrm{End}(E) = \mathcal{O}_\Lambda = \{\alpha \in \mathbb{C} \,|\, \alpha\Lambda \subseteq \Lambda\}$. Taking $\tau = \omega_2/\omega_1$ of positive imaginary part, and replacing Λ by $\langle 1, \tau \rangle$ (as they are homothetic) we find that for any $\alpha \in \mathcal{O}_\Lambda$ there are $a, b, c, d \in \mathbb{Z}$ with $\alpha = a + b\tau$ and $\alpha\tau = c + d\tau$. Simple manipulations give that α is integral over $\mathbb{Z}$ as $\alpha^2 - (a+d)\alpha + bc = 0$. Now since $\mathcal{O}_\Lambda \neq \mathbb{Z}$, we have that for an $\alpha \notin \mathbb{Z}$ the corresponding $b \neq 0$ so $b\tau^2 + (d-a)\tau + c = 0$. Thus $\mathbb{Q}(\tau)$ is a quadratic extension, and as $\tau \notin \mathbb{R}$ (else Λ is not lattice) it is also imaginary. Finally since $\mathcal{O}_\Lambda \subseteq \mathbb{Q}(\tau)$ is a ring and is integral over $\mathbb{Z}$, $\mathcal{O}$ is an order in a quadratic field.

Theorem 1.4. *Let K be a field of characteristic 0, and E an elliptic curve over K with endomorphism ring different from $\mathbb{Z}$ (a CM curve). Then End(E) is an order in a quadratic field.*

There is actually a preferred identification of $\mathrm{End}_{\mathbb{C}}(E)$ with $\mathcal{O}_\Lambda$. The lattice identification of $\mathcal{O}_\Lambda$ with $\mathrm{End}_{\mathbb{C}}(E)$ consists of associating $\alpha \in \mathcal{O}_\Lambda$ with the endomorphism

$[\alpha]$ such that for any invariant differential ω of E, $[\alpha]^*\omega = \alpha\omega$.

The idea to fix such an identification is simple. To $\alpha \in \mathcal{O}$ one associates the endomorphism $[\alpha]$ such that the following diagram commutes:

$$\begin{array}{ccc} \mathbb{C}/\Lambda & \xrightarrow{f_\alpha} & \mathbb{C}/\Lambda \\ {\scriptstyle \Phi_w}\downarrow & & {\scriptstyle \Phi_w}\downarrow \\ E & \xrightarrow{[\alpha]} & E, \end{array} \tag{1.15}$$

where f_α is defined by $z \mapsto \alpha z$. To prove that $[\alpha]^*\omega = \alpha\omega$, we first note that both any two invariant differentials on $\mathbb{C}/\Lambda$ are equal up to multiplication by a non zero constant, as their quotient is a function invariant under translation on $\mathbb{C}$. Now tracing through the diagram, $[\alpha] = f \circ f_\alpha \circ f^{-1}$ so

$$\begin{aligned} [\alpha]^*(\omega) &= (\Phi_w^{-1})^* \circ f_\alpha^* \circ \Phi_w^*(\omega) \\ &= (\Phi_w^{-1})^* \circ f_\alpha^*(c\,dz) = (\Phi_w^{-1})^*(\alpha c\,dz) \\ &= \alpha\omega \end{aligned} \tag{1.16}$$

Example 1.1. *Here are two classical examples of elliptic curves (over $\mathbb{C}$) with complex multiplication:*

1. *$E : y^2 = x^3 + x$ with $End(E) = \mathbb{Z}[i]$ and $[i](x, y) = (-x, iy)$*

2. *$E : y^2 = x^3 + 1$ with $End(E) = \mathbb{Z}[\rho]$ and $[\rho](x, y) = (\rho x, y)$, where $\rho = e^{2\pi i/3}$*

1.4.2 Finiteness of Ell($\mathcal{O}$)

Rather than concentrate on a particular elliptic curve with CM by $\mathcal{O}$, it is useful to look at all the elliptic curves with CM by some given order. We will further denote by $K = \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q}$ the fraction field of $\mathcal{O}$ lies, and by $\mathcal{O}_K$ the maximal order of K.

For $\mathfrak{a}$ a lattice in $\mathbb{C}$ let us denote $\mathcal{O}_\mathfrak{a} = \mathrm{End}(\mathbb{C}/\mathfrak{a}) = \{\alpha \in \mathbb{C} \mid \alpha\mathfrak{a} \subseteq \mathfrak{a}\}$. Further-

more, for $\mathcal{O} \subseteq K$ define

$$\begin{aligned} \mathrm{Ell}(\mathcal{O}) &:= \{\text{elliptic curves with CM by } \mathcal{O}\}/\text{isomorphisms over } \mathbb{C} \\ &= \{j(E) \mid E \text{ has CM by } \mathcal{O}\} \\ &= \{\text{lattices } \mathfrak{a} \subseteq \mathbb{C} \mid \mathcal{O}_\mathfrak{a} = \mathcal{O}\}/\mathbb{C}^\times \\ &= \{\text{lattices } \mathfrak{a} \subseteq K \mid \mathcal{O}_\mathfrak{a} = \mathcal{O}\}/K^\times \end{aligned} \tag{1.17}$$

where the meaning of $=$ is that there is a one to one correspondance. The third equality comes from the fact that two complex tori are isomorphic is and only if their lattices Λ, Λ' are homothetic (i.e. $\exists \alpha \in \mathbb{C}$ such that $\Lambda = \alpha\Lambda'$.The last equality holds since if $\mathfrak{a} = \langle 1, \tau \rangle$ and $\mathcal{O}_\mathfrak{a} = \mathcal{O} = \mathbb{Z} + c\mathbb{Z}\omega$ (where c is the conductor of $\mathcal{O}$) then $c\omega\tau = a + b\tau$ for some $a, b \in \mathbb{Z}$ and thus $\tau \in \mathbb{Q}(\omega) = K$.

It is consequently natural to pursue our studies by looking at the set $\mathrm{Lat}(\mathcal{O}) = \{\text{lattices } \mathfrak{a} \subseteq K \mid \mathcal{O}_\mathfrak{a} = \mathcal{O}\}$.

Lemma 1.1. *If $\mathfrak{a}$ is an invertible fractional $\mathcal{O}$-ideal, then $\mathfrak{a}$ is in Lat($\mathcal{O}$).*

Proof. Clearly, $\mathcal{O} \subseteq \mathcal{O}_\mathfrak{a}$. On the other hand if $\alpha \in \mathbb{C}$ is such that $\alpha\mathfrak{a} \subseteq \mathfrak{a}$ then $\alpha\mathcal{O} = \alpha\mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}$. So $\alpha \in \mathcal{O}$. □

As a consequence of this lemma, we get that the ideal class group of $\mathcal{O}$, $\mathrm{Cl}(\mathcal{O}) = \{\text{invertible fractional } \mathcal{O}\text{-ideals}\}/K^\times$ injects in $\mathrm{Lat}(\mathcal{O})/K^\times = \mathrm{Ell}(\mathcal{O})$. As usual one is led to wonder how much of the target is missed by such a map, which is the goal of our next lemma:

Lemma 1.2. *Given a lattice $\mathfrak{a} \subseteq K$ such that $\mathcal{O}_\mathfrak{a} = \mathcal{O}$ then $\mathfrak{a}$ is an invertible fractional $\mathcal{O}$-ideal*

Proof. Without loss of generality, let $\mathfrak{a} = \mathbb{Z} + \mathbb{Z}\tau$ for τ in K. τ has a minimal polynomial of the form $Ax^2 + Bx + C$ with $\gcd(A, B, C) = 1$. Let $D = B^2 - 4AC$,

and $\bar{\tau}$ be the Galois conjugate of τ. We have $\tau + \bar{\tau} = -B/A$ and $\tau \cdot \bar{\tau} = C/A$, so if we define $\bar{\mathfrak{a}} =< 1, \bar{\tau} >$, we get

$$\begin{aligned}
\mathfrak{a}\bar{\mathfrak{a}} &= \langle 1, \tau, \bar{\tau}, \tau\bar{\tau} \rangle \\
&= \langle 1, \tau, \bar{\tau} + \tau, C/A \rangle \\
&= \langle 1, (-B + \sqrt{D})/2A, -B/A, C/A \rangle \\
&= A^{-1}\langle A, (-B + \sqrt{D})/2, B, C \rangle \\
&= A^{-1}\langle 1, (B + \sqrt{D})/2 \rangle
\end{aligned} \tag{1.18}$$

The last equality holding because $\gcd(A, B, C) = 1$. Now if we have that

$$\mathcal{O} = \langle 1, (B + \sqrt{D})/2 \rangle \tag{1.19}$$

then our proof is over as $A\bar{\mathfrak{a}}$ is an inverse to $\mathfrak{a}$.

Let's denote $\omega = (B + \sqrt{D})/2$ and $M = \langle 1, \omega \rangle$. Since $1\tau \in \mathfrak{a}$ and $\omega\tau = -(B^2 - D)/4A = C \in \mathbb{Z} \subseteq \mathfrak{a}$, $M \subseteq \mathcal{O}_{\mathfrak{a}} = \mathcal{O}$. Now for a $z \in \mathcal{O} = \mathcal{O}_{\mathfrak{a}}$,

$$z\mathfrak{a} \subseteq \mathfrak{a} \Rightarrow z\mathfrak{a}(\overline{\mathfrak{a}}A) \subseteq \mathfrak{a}(\overline{\mathfrak{a}}A) \Rightarrow zM \subseteq M \tag{1.20}$$

In particular z belongs to M. Therefore $M = \mathcal{O}$. □

Putting the two lemmas together we get our first significant result

Theorem 1.5. $\mathrm{Ell}(\mathcal{O}) \simeq \mathrm{Cl}(\mathcal{O})$

So in particular, since $\mathrm{Cl}(\mathcal{O})$ is finite (see lemma A.1 or [14]) we have that $\mathrm{Ell}(\mathcal{O})$ is also finite. An important observation for the proper use of this result is that given an elliptic curves $E : y^2 = x^3 + ax + b$ over $\mathbb{C}$ with CM by an order $\mathcal{O}$, then for any automorphism σ of $\mathbb{C}$, $\sigma E : y^2 = x^3 + ({}^{\sigma}a)x + ({}^{\sigma}b)$ possess the same endomorphism ring, by the identification $f \mapsto (\sigma f)$, where σf is obtained from f by applying σ to the coefficients of the morphism.

Lemma 1.3. *Let A be an elliptic curve with CM by $\mathcal{O}$, and let $[\cdot]_A$, $[\cdot]_{\sigma A}$ denote the respective lattice identifications of $\mathcal{O}$. Then ${}^{\sigma}([\alpha]_A) = [{}^{\sigma}(\alpha)]_{\sigma A}$ $\forall \alpha \in \mathcal{O}$ and $\forall \sigma \in \mathrm{Aut}(\mathbb{C})$. Furthermore, if A is defined over L and $K = \mathrm{Quot}(\mathcal{O})$ then every endomorphism of E is defined over $L \cdot K$*

Proof. Let ω_E denote the invariant differential of the elliptic curve E. Then one notes that ${}^{\sigma}\omega_A = \omega_{\sigma A}$ (by Def 1.2) and thus

$$\begin{aligned} ({}^{\sigma}[\alpha]_A)(\omega_{\sigma A}) &= {}^{\sigma}([\alpha]_A^* \omega_A) &= {}^{\sigma}(\alpha \omega_A) \\ &= {}^{\sigma}\alpha \omega_{\sigma A} &= [{}^{\sigma}\alpha]_{\sigma A} \omega_{\sigma A} \end{aligned}$$

Using the fact that the pullback is an injection of $\mathrm{End}(E)$ into the endomorphism of the space of invariant differentials of E (see [22] II.§4), we conclude that ${}^{\sigma}([\alpha]_A) = [{}^{\sigma}(\alpha)]_{\sigma A}$

If A possesses an equation over L, and $\sigma \in Aut(\mathbb{C})$ fixes L, then ${}^{\sigma}A = A$. So in particular, we get that ${}^{\sigma}([\alpha]_A) = [{}^{\sigma}\alpha]_A$. If σ also fixes K, then ${}^{\sigma}([\alpha]_A) = [\alpha]_A$ and so $[\alpha]_A$ can be defined over $L \cdot K$ □

The fact that the endomorphism ring remains unchanged when we apply an automorphism of $\mathbb{C}$ to an elliptic curve, gives us a way to produce other curves with CM from an existing one. Using this idea one can already find useful results:

Theorem 1.6. *Let E over $\mathbb{C}$ be a CM curve, then $j(E)$ is an algebraic number.*

Proof. If E is a CM curve, then $E \in \mathrm{Ell}(\mathcal{O})$ for some $\mathcal{O}$. The algebraic definition of the j-invariant (see definition 1.2) makes it clear that ${}^{\sigma}j(E) = j({}^{\sigma}E)$, thus if $j(E)$ is transcendental then there are infinitely many automorphisms of $\mathbb{C}$ not fixing $j(E)$, giving infinitely many non-isomorphic (since their j-invariant is different) elliptic curves with CM by $\mathcal{O}$, contradicting the finiteness of $\mathrm{Ell}(\mathcal{O})$. □

Since $j(E)$ is algebraic, it seems reasonable to ask what is the field generated by all the j-invariants of the curves in $\mathcal{O}$. This theorem also exhibits an action of the

Galois group $G_{\overline{K}/K}$ on the set $\mathrm{Ell}(\mathcal{O})$ via the j-invariants, which deserves a deeper inspection.

But first, let us define another action of $\mathrm{Cl}(\mathcal{O})$, (which is related to $G_{K/\mathbb{Q}}$ by class field theory) in the hope of getting more insights.

1.4.3 The action of $\mathbf{Pic}(\mathcal{O})$

To do so, we need a classical result, namely that $\mathrm{Cl}(\mathcal{O})$ is isomorphic to

$$\mathrm{Pic}(\mathcal{O}) = \{\text{rank one projective } \mathcal{O}\text{-module, up to isomorphisms}\}. \tag{1.21}$$

The group law on the latter is defined as follows:

$$(\mathfrak{a}, \mathfrak{b}) \mapsto \mathfrak{a} \otimes_{\mathcal{O}} \mathfrak{b} \tag{1.22}$$

The identity is $\mathcal{O}$ and the inverse of $\mathfrak{a}$ is $\mathrm{Hom}_{\mathcal{O}}(\mathfrak{a}, \mathcal{O})$. The isomorphism $\mathrm{Cl}(\mathcal{O}) \to \mathrm{Pic}(\mathcal{O})$ is then described as $[\mathfrak{a}] \mapsto [\mathfrak{a}]$, and is a group homomorphism since $\mathfrak{a} \otimes_{\mathcal{O}} \mathfrak{b} = \mathfrak{a}\mathfrak{b} \otimes_{\mathcal{O}} \mathcal{O}$. The proof of this can be found in [13]. This isomorphism is very useful to define an action of $\mathrm{Pic}(\mathcal{O})$ on the set $\mathrm{Ell}(\mathcal{O})$.

Let $A \in \mathrm{Ell}(\mathcal{O})$, and $\mathfrak{a} \in \mathrm{Cl}(\mathcal{O})$ such that $\mathfrak{a}$ is coprime to the conductor of $\mathcal{O}$, so that $\mathfrak{a}$ is invertible in $\mathcal{O}$. Since it is always possible to choose such an ideal in every equivalence class (see remark A.1), we can define the action of $\mathrm{Pic}(\mathcal{O})$ on $\mathrm{Ell}(\mathcal{O})$ as

$$\mathfrak{a} \star A = \mathrm{Hom}_{\mathcal{O}}(\mathfrak{a}, A) \tag{1.23}$$

for $\mathfrak{a}$ an invertible ideal. However this only makes sense if $\mathrm{Hom}_{\mathcal{O}}(\mathfrak{a}, A)$ is an elliptic curve. To see this, we will consider $A(\mathbb{C}) = \mathbb{C}/\Lambda$. Then we look at the following exact sequences:

$$\begin{array}{ccccccccc} 0 \to & & \Lambda & \to & & \mathbb{C} & \to & \mathbb{C}/\Lambda & \to 0 \\ 0 \to & \mathrm{Hom}_{\mathcal{O}}(\mathfrak{a}, \Lambda) & \to & \mathrm{Hom}_{\mathcal{O}}(\mathfrak{a}, \mathbb{C}) & \to & \mathrm{Hom}_{\mathcal{O}}(\mathfrak{a}, \mathbb{C}/\Lambda) & & & \end{array} \tag{1.24}$$

But the second one is also right exact since $\mathfrak{a}$ is a projective $\mathcal{O}$-module (for it is invertible). To make explicit the structure of modules of the form $\mathrm{Hom}_{\mathcal{O}}(\mathfrak{a}, -)$ we need some lemmas:

Lemma 1.4. *Let $\mathfrak{a}$ be an invertible $\mathcal{O}$-ideal. Then the ideal $\mathfrak{a}_{\mathfrak{p}} = \mathfrak{a}\mathcal{O}_{\mathfrak{p}}$ is principal for every prime $\mathfrak{p}$ of $\mathcal{O}$.*

Proof. Let $\mathfrak{b}$ be such that $\mathfrak{ab} = \mathcal{O}$, then for some $a_i \in \mathfrak{a}$ and $b_i \in \mathfrak{b}$, where $i = 1, \ldots k$, $\sum_{i=1}^{k} a_i b_i = 1$. Thus it is impossible for all $a_i b_i$ to be in $\mathfrak{p}\mathcal{O}_{\mathfrak{p}}$. Suppose $a_1 b_1 \notin \mathfrak{p}\mathcal{O}_{\mathfrak{p}}$. Then it is a unit. Take any $a \in \mathfrak{a}$, then $b_1 a \in \mathfrak{b}\mathfrak{a}_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}$. It follows that $ab_1(b_1 a_1)^{-1} a_1 \in a_1 \mathcal{O}_{\mathfrak{p}}$ so $\mathfrak{a}_{\mathfrak{p}} = a_1 \mathcal{O}_{\mathfrak{p}}$. □

Lemma 1.5. *Let $\mathfrak{a}$ be an invertible $\mathcal{O}$-ideal, and M a torsion-free $\mathcal{O}$-module. Then the map*

$$\begin{array}{rccl} f: & \mathfrak{a}^{-1} \otimes_{\mathcal{O}} M & \to & \mathit{Hom}_{\mathcal{O}}(\mathfrak{a}, M) \\ & \alpha \otimes_{\mathcal{O}} m & \mapsto & (\phi_{\alpha,m} : x \mapsto (\alpha x)m), \end{array} \tag{1.25}$$

extended by $\mathcal{O}$-linearity is an isomorphism

Proof. It is trivial to show that this is a group homomorphism. Bijectivity requires more work; we need to study the localization at every prime of $\mathcal{O}$. To do so, recall that there is a natural isomorphism ($\mathcal{O}_{\mathfrak{p}}$ is the localization of $\mathcal{O}$ at $\mathfrak{p}$)

$$\begin{array}{rcl} \mathcal{O}_{\mathfrak{p}} \otimes_{\mathcal{O}} \mathrm{Hom}_{\mathcal{O}}(\mathfrak{a}, M) & \simeq & \mathrm{Hom}_{\mathcal{O}_{\mathfrak{p}}}(\mathcal{O}_{\mathfrak{p}} \otimes_{\mathcal{O}} \mathfrak{a}, \mathcal{O}_{\mathfrak{p}} \otimes_{\mathcal{O}} M) \\ (\beta, f) & \mapsto & (\phi : a \otimes_{\mathcal{O}} m \mapsto \beta a \otimes_{\mathcal{O}} f(m)) \end{array} \tag{1.26}$$

under the hypothesis that $\mathfrak{a}$ is finitely presented. But the sequence

$$0 \to \mathfrak{a}^{-1}(\alpha_2, -\alpha_1) \to \mathcal{O} \oplus \mathcal{O} \to \mathfrak{a} \to 0 \tag{1.27}$$

where $\mathfrak{a}^{-1}(\alpha_2, -\alpha_1) = \{(a\alpha_2, -a\alpha_1) \text{ for } a \in \mathfrak{a}^{-1}\}$, is exact. But since $\mathfrak{a}^{-1}$ is also a fractional ideal, it has at most two generators, thus is contained in $\mathcal{O} \oplus \mathcal{O}$, so $\mathfrak{a}$ is finitely presented. Alternatively, we recall that all finitely generated modules over noetherian rings are finitely presented.

Using 1.25 we can localize (i.e. tensor over $\mathcal{O}$ by $\mathcal{O}_\mathfrak{p}$) the sequence

$$0 \to K \to \mathfrak{a}^{-1} \otimes_{\mathcal{O}} M \xrightarrow{f} \mathrm{Hom}(\mathfrak{a}, M) \to C \to 0 \tag{1.28}$$

and still get an exact sequence (we denote by $C = \mathrm{Coker}(f)$ and by $K = \mathrm{Ker}(f)$). The idea is to show that at every localization the map is bijective, so $K_\mathfrak{p}$ and $C_\mathfrak{p}$ are trivial for every $\mathfrak{p} \in \mathcal{O}$. A classical result will then imply that K and C are trivial. Take a prime $\mathfrak{p} \lhd \mathcal{O}$, and denote by $-_\mathfrak{p}$ the local version of $-$.

By the previous lemma, $\mathfrak{a}_\mathfrak{p} := \mathfrak{a}\mathcal{O}_\mathfrak{p}$ is principal for it is invertible. Say $\mathfrak{a}_\mathfrak{p} = \alpha_\mathfrak{p}\mathcal{O}_\mathfrak{p}$, then we also have that $\mathfrak{a}_\mathfrak{p}^{-1} = \alpha_\mathfrak{p}^{-1}\mathcal{O}_\mathfrak{p}$. Then the localized sequence is

$$0 \to K_\mathfrak{p} \to \alpha_\mathfrak{p}^{-1}\mathcal{O}_\mathfrak{p} \otimes_{\mathcal{O}_\mathfrak{p}} M_\mathfrak{p} \to \mathrm{Hom}_{\mathcal{O}_\mathfrak{p}}(\alpha_\mathfrak{p}, M_\mathfrak{p}) \to C_\mathfrak{p} \to 0 \tag{1.29}$$

We begin by showing injectivity. An element u of $\mathfrak{a}_\mathfrak{p}^{-1} \otimes M_\mathfrak{p}$ can be written as

$$\begin{aligned} u &= \sum \alpha_\mathfrak{p}^{-1} a_i/s_i \otimes m_i/t_i \\ &= \alpha_\mathfrak{p}^{-1} \otimes \sum \tfrac{a_i m_i}{s_i t_i} \end{aligned} \tag{1.30}$$

where $a_i \in \mathcal{O}$, $m_i \in M$ and $s_i, t_i \in \mathcal{O} \setminus \mathfrak{p}$. Then for $x \in \mathfrak{a}_\mathfrak{p}$

$$f(u)(x) = (\alpha_\mathfrak{p}^{-1} x) \sum \tfrac{a_i m_i}{s_i t_i} \tag{1.31}$$

If $f(u)(x) = 0$ for all x then it follows that $\sum \frac{a_i m_i}{s_i t_i} = 0$ for M is torsion-free. Therefore $u = \alpha_\mathfrak{p}^{-1} \otimes 0 = 0$

As for surjectivity, let $\phi \in \mathrm{Hom}_{\mathcal{O}_\mathfrak{p}}(\mathfrak{a}_\mathfrak{p}, M_\mathfrak{p})$, then $\phi(\alpha_\mathfrak{p}) = m_\mathfrak{p}$ determines completely the map as it is a $\mathcal{O}_\mathfrak{p}$ homomorphism. So $\alpha_\mathfrak{p}^{-1} \otimes_{\mathcal{O}_\mathfrak{p}} m_\mathfrak{p} \in \mathfrak{a}_\mathfrak{p}^{-1} \otimes_{\mathcal{O}_\mathfrak{p}} M_\mathfrak{p}$ is a preimage of ϕ, and the map is surjective. □

Replacing the two first elements in the second line of 1.24 by their equivalent module we get

$$0 \to \mathfrak{a}^{-1}\Lambda \to \mathfrak{a}^{-1}\mathbb{C} \to \mathrm{Hom}_{\mathcal{O}}(\mathfrak{a}, \mathbb{C}/\Lambda) \to 0 \tag{1.32}$$

Thus $\mathrm{Hom}_{\mathcal{O}}(\mathfrak{a}, \mathbb{C}/\Lambda)$ can be identified with $\mathbb{C}/\mathfrak{a}^{-1}\Lambda$ (for $\mathfrak{a}^{-1}\mathbb{C} = \mathbb{C}$) which is an elliptic curve with CM by $\mathcal{O}$. Interestingly one has a natural map $A \simeq \mathbb{C}/\Lambda$ to $\mathfrak{a}\star A \simeq \mathbb{C}/\mathfrak{a}^{-1}\Lambda$ of kernel

$$\mathfrak{a}^{-1}\Lambda/\Lambda = \{P \in A \mid aP = O \; \forall a \in \mathfrak{a}\} =: A[\mathfrak{a}] \tag{1.33}$$

We will now prove a basic fact on invertible ideals in order to get more information this kernel (and on the kernel of $[\alpha]_A$).

Lemma 1.6. *Let $\mathfrak{a}, \mathfrak{b}$ be integral invertible ideals of $\mathcal{O}$, such that $\mathfrak{b} \subseteq \mathfrak{a}$, then $\mathcal{O}/\mathfrak{b}\mathfrak{a}^{-1} \simeq \mathfrak{a}/\mathfrak{b}$.*

Proof. Let $\mathfrak{b} = \prod_{i=1}^{k} \mathfrak{p}_i^{f_i}$, with $f_i > 0$, and $\mathfrak{a} = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}$, with $0 \leq e_i \leq f_i$. Pick $x_i \in \mathfrak{p}_i^{e_i} \setminus \mathfrak{p}_i^{e_i+1}$, and let k be the solution of $x \equiv x_i \pmod{\mathfrak{p}_i^{e_i+1}}$ $\forall i$ (which exists by the Chinese remainder theorem). Then the valuation of $k \in \mathcal{O}$ (well-defined for $\mathcal{O}_{\mathfrak{p}_i}$ is a discrete valuation ring) at $\mathfrak{p}_i$ is e_i (i.e. $\nu_{\mathfrak{p}_i}(k) = e_i$). We can then define a map $m : \mathcal{O}/\mathfrak{b}\mathfrak{a}^{-1} \to \mathfrak{a}/\mathfrak{b}$, by sending $x \in \mathcal{O}$ to kx (well defined as $k\mathfrak{b}\mathfrak{a}^{-1} \subseteq \mathfrak{b}$). Localization is an exact functor, so if we prove that the map m is injective and surjective at every prime of $\mathcal{O}$, its kernel and cokernel will be trivial (a $\mathcal{O}$-module is trivial if and only if all its localization are).

Since $\mathfrak{a}$ and $\mathfrak{b}$ are invertible, then every localization is principal (see lemma 1.4) so denote $\alpha_{\mathfrak{p}}$ and $\beta_{\mathfrak{p}}$ as a principal element in $\mathfrak{a}_{\mathfrak{p}}$ and $\mathfrak{b}_{\mathfrak{p}}$ respectively. If $\mathfrak{p} = \mathfrak{p}_i$ for some i, then $k = u_{\mathfrak{p}}\alpha_{\mathfrak{p}}$ where $u_{\mathfrak{p}}$ is a unit in $\mathcal{O}_{\mathfrak{p}}$ and the multiplication map by $\alpha_{\mathfrak{p}}$ from $\mathcal{O}_{\mathfrak{p}}/(\beta_{\mathfrak{p}}\alpha_{\mathfrak{p}}^{-1}\mathcal{O}_{\mathfrak{p}}$ to $\alpha_{\mathfrak{p}}\mathcal{O}_{\mathfrak{p}}/\beta_{\mathfrak{p}}\mathcal{O}_{\mathfrak{p}}$ is easily seen to be bijective. If $\mathfrak{p} \neq \mathfrak{p}_i \; \forall i$ then localizing at $\mathfrak{p}$ yields a trivial map: $\mathcal{O}_{\mathfrak{p}} = \mathfrak{a}\mathcal{O}_{\mathfrak{p}} = \mathfrak{b}\mathcal{O}_{\mathfrak{p}}$, which is also bijective. □

Up to a isomorphism of A we can make $\mathfrak{a}^{-1}\Lambda$ into an integral $\mathcal{O}$-ideal. It then follows that $\sharp A[\mathfrak{a}] = N_{K/\mathbb{Q}}(\mathfrak{a})$. Similarly one can get that $\sharp\mathrm{Ker}([\alpha]_A) = N_{K/\mathbb{Q}}(\alpha)$.

The action of $\mathrm{Pic}(\mathcal{O})$ we defined is simple and transitive. Transitive for if two elements of $\mathrm{Pic}(\mathcal{O})$ give the same elliptic curve then they are equal up to homothety

in $\mathrm{Cl}(\mathcal{O})$:

$$\begin{aligned}\mathfrak{a}\star A=\mathfrak{b}\star A &\Leftrightarrow \mathbb{C}/\mathfrak{a}^{-1}\Lambda\simeq\mathbb{C}/\mathfrak{b}^{-1}\Lambda\\ &\Leftrightarrow \mathfrak{a}^{-1}\Lambda \text{ is homothetic to } \mathfrak{b}^{-1}\Lambda\\ &\Leftrightarrow \mathfrak{a}^{-1} \text{ is homothetic to } \mathfrak{b}^{-1}\\ &\Leftrightarrow [\mathfrak{a}^{-1}]=[\mathfrak{b}^{-1}]\end{aligned}$$

It is simple since the sets $\mathrm{Pic}(\mathcal{O})$ and $\mathrm{Ell}(\mathcal{O})$ have the same cardinality. As promised, we now inspect the relation between this action and the one from $G_{\overline{K}/K}$.

Theorem 1.7. *Let $\sigma\in G_{\overline{K}/K}$, and $\mathfrak{a}\in Pic(\mathcal{O})$ then $\sigma(\mathfrak{a}\star A)=\mathfrak{a}\star(\sigma A)$*

Proof. From the isogeny $A\to A/A[\mathfrak{a}]$ one gets ${}^{\sigma}A\to{}^{\sigma}(A/A[\mathfrak{a}])$. Since ${}^{\sigma}A$ also has CM by $\mathcal{O}$, there is another isogeny ${}^{\sigma}A\to({}^{\sigma}A)/({}^{\sigma}A)[\mathfrak{a}]$. However, by lemma 1.3 their kernel (${}^{\sigma}(A[\mathfrak{a}])$ and $({}^{\sigma}A)[\mathfrak{a}]$) are equal. But for a given finite subgroup L of E there is an unique elliptic curve and an isogeny $f:E\to E'$ such that $\mathrm{Ker}f=L$ (see [22] III.§4). It follows that the images of the two maps are equal and thus that the two action commutes. □

Remark 1.1. *The action of $Pic(\mathcal{O})$ we introduced might seem awkward due to the work involved in proving the commutativity of the actions. Indeed, one could be tempted to define directly $\mathfrak{a}\star A=A/A[\mathfrak{a}]$. Though this last definition makes commutativity easy to prove, it does not respects so clearly the properties of an action ($\mathfrak{b}\mathfrak{a}\star A\stackrel{?}{=}\mathfrak{b}\star(\mathfrak{a}\star A)$).*

Since the action of $\mathrm{Pic}(\mathcal{O})$ is simply transitive, we can define for a given $A\in\mathrm{Ell}(\mathcal{O})$ a map $\eta_A:G_{\overline{K}/K}\to\mathrm{Pic}(\mathcal{O})$ by the rule $\eta_A(\sigma)\star A=\mathfrak{a}\star A$.

Lemma 1.7. *η_A is a group homomorphism independent of A.*

Proof. Independence follows from the commutativity of the actions:

$$\begin{aligned}\eta_A({}^{\sigma})\star A' &= \eta_A(\sigma)\star\mathfrak{a}\star A=\mathfrak{a}\star\eta_A(\sigma)\star A\\ &=\mathfrak{a}\star({}^{\sigma}A)={}^{\sigma}(\mathfrak{a}\star A)\\ &={}^{\sigma}A'\end{aligned}\tag{1.34}$$

where $A' = \mathfrak{a} \star A$ And as a simple consequence is a group homomorphism:

$$\eta(\sigma\tau) \star A = {}^{\sigma\tau} A = {}^{\sigma} (\eta(\tau) \star A) = \eta(\sigma) \star \eta(\tau) \star A$$

□

Thus we get our first piece of information by looking at

$$\mathrm{Ker}(\eta) = \{\sigma \in G_{\overline{K}/K} \mid {}^{\sigma} A = A\} = \{\sigma \in G_{\overline{K}/K} \mid {}^{\sigma} j(A) = j(A)\} \tag{1.35}$$

for then $K(j(A)) = \bar{K}^{\mathrm{Ker}(\eta)} =: H$. More importantly $G_{H/K} = \mathrm{Im}(\eta) \subseteq \mathrm{Pic}(\mathcal{O})$, and so H is an abelian extension of K.

1.4.4 Explicit Galois Action on $j(E)$

To get more information about H, we need to use class field theory. As a recall when L/K is an abelian extension of number fields, $\mathfrak{p} \subseteq K$ a prime ideal unramified in L, $\wp$ a prime of L above (or dividing) $\mathfrak{p}$, $l = \mathcal{O}_L/\wp$ and $k = \mathcal{O}_K/\mathfrak{p}$, we have an isomorphism between the decomposition group of $\wp$, $D_\wp$, and the galois group $G_{l/k}$. It is determined by sending the frobenius in $G_{l/k}$ to $\sigma_\wp \in G_{L/K}$ where the restriction of $\sigma_\wp$ to $\mathcal{O}_K/\mathfrak{p}$ corresponds to the frobenius (raising to the $|l|^{th}$ power). Actually $\sigma_\wp$ is unique with this property and is independent of $\wp$, so we will write it $\sigma_\mathfrak{p}$ instead. The assignment $\mathfrak{p} \mapsto \sigma_\mathfrak{p}$ is actually a isomorphism of $\mathrm{Cl}(K)$ with $G_{K^{ur}/K}$ where $K^{ur,ab}$ is the maximal unramified abelian extension of K. When $\mathcal{O}$ is not maximal the isomorphism is slightly different: we only consider primes $\mathfrak{p}$ of K prime to the conductor c of $\mathcal{O}$, then

$$\begin{array}{rccc} \mathrm{rec}: & \mathrm{Pic}(\mathcal{O}) & \to & G_{H_\mathcal{O}/K} \\ & \mathfrak{p} & \mapsto & \sigma_{\mathfrak{p}\mathcal{O}_K} \end{array} \tag{1.36}$$

is an isomorphism, where $H_\mathcal{O}$ is an abelian extension of K unramified outside the primes dividing c.

Theorem 1.8. $H = H_{\mathcal{O}}$

Proof. Let $L = H \cdot H_{\mathcal{O}}$, then it is an abelian extension of K. Furthermore we have homomorphisms $G_{L/K} \overset{\pi}{\twoheadrightarrow} G_{H_{\mathcal{O}}/K} \overset{rec}{\simeq} \mathrm{Pic}(\mathcal{O})$, so we define $\xi = r \circ \pi$. On the other hand, since $G_{\overline{K}/L} \subseteq \mathrm{Ker}(\eta)$ we might as well restrict η to $G_{L/K}$. Then $L^{\mathrm{Ker}(\eta)} = H$ and $L^{\mathrm{Ker}(\xi)} = H_{\mathcal{O}}$, so what we really need to prove is that $\eta|_{G_{L/K}} = \xi$. To prove this we will first have to describe $G_{L/K}$ properly.

When L/K is a finite extension of number fields, we can define the Tchebotarev density δS of a set S of primes of L. The properties of this density that are of interest to us are the following:

1. If $T \subseteq S$ is a finite set then $\delta S = \delta(S \setminus T)$.
2. If $T = \{\wp \text{ in } S \text{ with } N_{L/\mathbb{Q}}(\wp) \text{ a rational prime}\}$ then $\delta S = \delta(T)$.
3. If $\delta S = 1$ then $G_{L/K} = \{\sigma_{\mathfrak{p}} \mid \exists \wp \in S \text{ such that } \mathfrak{p} \text{ divides } \wp\}$.

Note that since every $\wp \in L$ divides some $\mathfrak{p} \in K$, and that $\sigma_{\wp} = \sigma_{\mathfrak{p}}$ by definition, it is more convenient to speak of the set S as a set of primes of K. The set S that we will use is define as all the primes $\mathfrak{p}$ of $\mathcal{O}$ satisfying:

$C1-$ $\mathfrak{p}$ is prime to c the conductor of $\mathcal{O}$.

$C2-$ $\mathfrak{p}$ is unramified in L.

$C3-$ Every elliptic curve $A \in \mathrm{Ell}(\mathcal{O})$ has good reduction at all $\wp \mid \mathfrak{p}$.

$C4-$ $N_{K/\mathbb{Q}}(\mathfrak{p})$ is a rational prime.

$C5-$ $\mathfrak{p}$ does not divide $N_{L/K}(j(A) - j(A'))\mathcal{O}_K$ $\forall A, A' \in \mathrm{Ell}(\mathcal{O})$ such that $A \neq A'$.

So our set S has density 1 (at every step except $C4$ we took out a finite number of prime, and $C4$ is a condition that does not affect δS). The purpose of these conditions will be made clear as we go trough the proof. According to the third property of the density, and using our first condition on S, one notes that we now only need to show that $\eta(\sigma_{\mathfrak{p}}) = \xi(\sigma_{\mathfrak{p}}) = [\mathfrak{p}]$ to have $\eta = \xi$.

Let $\beta \in \mathfrak{p} \setminus \mathfrak{p}^2$ and $\mathfrak{q}$ be such that $\mathfrak{pq} = p\mathcal{O}$ for $p \in \mathbb{Z}$ (exists by $C1$, $C2$ and $C4$). Then, by the Chinese remainder theorem, there is a $\alpha \in \mathcal{O}$ such that

$$\alpha \equiv \beta \pmod{\mathfrak{p}^2}, \quad \alpha \equiv 1 \pmod{\mathfrak{q}}, \quad \alpha \equiv 1 \pmod{c} \tag{1.37}$$

Consequently $\alpha\mathcal{O} = \mathfrak{ap}$ for some $\mathfrak{a} \lhd \mathcal{O}$ such that $\mathfrak{a}$ is prime to both c and $\mathfrak{p}$. For some $A \in \mathrm{Ell}(\mathcal{O})$ consider the maps

$$A \xrightarrow{\varphi} \mathfrak{p} \star A \xrightarrow{\psi} \mathfrak{ap} \star A = (\alpha) \star A \xrightarrow{\mu} A \tag{1.38}$$

Then $\mu \circ \psi \circ \varphi = [\alpha]_A$, so in particular the isogeny is of degree $N_{K/\mathbb{Q}}(\alpha)$ and $(\mu \circ \psi \circ \varphi)^*\omega = \alpha\omega$. For some $\wp \,|\, \mathfrak{p}$, we now reduce everything modulo $\wp \,|\, \mathfrak{p}$ (note that no 2 j-invariants become equal due to $C5$), and denote by $\widetilde{-}_\wp$ the reduced version of $-$. Then $\widetilde{[\alpha]}_\wp = \widetilde{\mu}_\wp \circ \widetilde{\psi}_\wp \circ \widetilde{\varphi}_\wp$ is inseperable since $\wp | \alpha$ ($\alpha \in \mathfrak{p}$) and $\widetilde{[\alpha]}^*{}_\wp \widetilde{\omega}_\wp = \widetilde{\alpha}_\wp \widetilde{\omega}_\wp$. The degree of the isogenies is not changed by good reduction ($C3$) and $\alpha \in \mathfrak{p}$. Furthermore, $\deg(\widetilde{\mu}_\wp) = \deg(\mu) = 1$ since μ is an isomorphism, and $\deg(\widetilde{\psi}_\wp) = \deg(\psi) = N_{K/\mathbb{Q}}(\mathfrak{a})$ is separable since $\mathfrak{a}$ is coprime to $\mathfrak{p}$. Thus, $\widetilde{\varphi}_\wp$ is of degree p ($C4$)and must be inseparable. It can be expressed as $Fr \circ \lambda$, where Fr is the p^{th}-power Frobenius map and λ is separable. Since the Frobenius is of degree at least p it follows that λ is of degree one, so an isomorphism. Consequently, $\mathfrak{p} \star \widetilde{A}_\wp = \widetilde{\varphi}_\wp(\widetilde{A}_\wp) = Fr(\widetilde{A}_\wp) = \widetilde{A}_\wp^{(p)}$, where $\widetilde{A}_\wp^{(p)}$ is the curve $\widetilde{A}_\wp$ with all the coefficients to the p^{th} power. By definition of j, we have $j(\widetilde{A}_\wp^{(p)}) = j(\widetilde{A}_\wp)^p$, so

$$j(\mathfrak{p} \star A) = j(\widetilde{\mathfrak{p} \star A}_\wp) = j(\widetilde{A}_\wp^{(p)}) = j(\widetilde{A}_\wp)^p \equiv \sigma_\mathfrak{p} j(\widetilde{A}_\wp) \equiv j(\sigma_\mathfrak{p} \widetilde{A}_\wp) \pmod{\wp} \tag{1.39}$$

But then

$$j(\mathfrak{p} \star A) \equiv j(\sigma_\mathfrak{p} A) \pmod{\wp} \tag{1.40}$$

So since the j-invariants stay different ($C5$), we have that

$$\begin{aligned} j(E) \equiv j(E') \pmod{\wp} &\Leftrightarrow E \simeq E' \\ \Rightarrow \qquad \mathfrak{p} \star A \simeq \sigma_\mathfrak{p} A &= \eta(\sigma_\mathfrak{p}) \star A \end{aligned} \tag{1.41}$$

Thus $\xi(\sigma_\mathfrak{p}) = [\mathfrak{p}] = \eta(\sigma_\mathfrak{p})$, $\eta = \xi$ and $H = H_\mathcal{O}$ $\square$

In fact we have proved much more: we have an explicit relation between the action of $G_{H_{\mathcal{O}}/K}$ with that of $\mathrm{Pic}(\mathcal{O})$ by

$$\sigma_{\mathfrak{p}} j(A) = j(\mathfrak{p} * A) \tag{1.42}$$

Now if we let Λ_A be the lattice associated to A, then $\Lambda_A \simeq \langle 1, \tau \rangle$ with $\Im(\tau) > 0$, then we define $j(A) = j(\tau)$. Since $\Lambda_{\mathfrak{p}\star A} = \mathfrak{p}^{-1}\Lambda_A$ we will write

$$\sigma_{\mathfrak{p}} j(\tau) = j(\mathfrak{p} \star \tau), \tag{1.43}$$

where $\langle 1, \mathfrak{p} \star \tau \rangle \simeq \mathfrak{p}^{-1}\Lambda_A$.

Furthermore, since $\langle 1, \tau \rangle$ homothetic to $\langle c\tau + d, a\tau + b \rangle$ if $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$, one sees that τ is only well-defined up to an action by $SL_2(\mathbb{Z})$ defined by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\tau + b}{c\tau + d} \tag{1.44}$$

These observations enables us to rewrite $\mathrm{Ell}(\mathcal{O})$ as the set

$$\{\tau \in SL_2(\mathbb{Z}) \backslash \mathcal{H} \mid \mathcal{O}_{\langle 1,\tau \rangle} = \mathcal{O}\} \tag{1.45}$$

where $\mathcal{H} = \{z \in \mathbb{C} \mid \Im(\tau) > 0\}$ and using the usual equivalence between latices and elliptic curves.

Chapter 2

Heegner Points

A crucial tool in the construction of Heegner points is the modular parametrization. We will briefly describe the properties of this parametrization and the objects that are necessary to define it. We will follow by the definition of Heegner points, their properties, how to compute them, and a quick survey of the results of our computations on curves of conductor less than 3000.

2.1 Modular Parametrization

Through the work of many mathematicians there emerged the remarkable conjecture that elliptic curves over $\mathbb{Q}$ could be in some sense parametrized by other objects, namely cusp forms. This insight has now been confirmed to be true. Consequently, we will devote this first section to a very short outline of the results that will be needed to make proper definitions of Heegner points and their properties.

There are many reasons to consider the upper-half plane $\mathcal{H} = \{z \in \mathbb{C} \mid \Im(z) > 0\}$ and the action of $SL_2(\mathbb{Z})$ that one defines on it. One of them is introduced in the appendix, where (quadratic) points in the upper half plane represent a positive definite primitive binary quadratic form, and another one comes from the description

of representatives for $\mathrm{Ell}(\mathcal{O})$, as seen in 1.44. These notions of equivalence then yield the action of $SL_2(\mathbb{Z})$ on $\mathcal{H}$, and we can obtain a fundamental domain F for $SL_2(\mathbb{Z})\backslash\mathcal{H}$ (see A.5).

On the other hand $\mathcal{H}$ is also a Riemann surface, and the group of matrices of positive determinant $\mathrm{GL}_2^+(\mathbb{R})$ acts on $\mathcal{H}$ as in A.4 or 1.44. Since scalar multiples of the identity act trivially on $\mathcal{H}$, we can consider this as the action of the group $\mathrm{PGL}_2^+(\mathbb{R}) = \mathrm{GL}_2^+(\mathbb{R})/\mathbb{R}^\times I$. Furthermore, this action leave both the hyperbolic line element $ds^2 = dz\,d\bar{z}/y^2 = (dx^2+dy^2)/y^2$ and the hyperbolic surface element $d\mu = dz\wedge d\bar{z}/2iy^2 = dx\wedge dy/y^2$ unchanged (here $x+iy=z\in\mathcal{H}$). Indeed for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) \in \mathrm{GL}_2^+(\mathbb{R})$, one has

$$\begin{aligned} d(\gamma z) &= \tfrac{d\gamma z}{dz} dz \\ &= ((cz+d)a - (az+b)c)h(\gamma,z)^{-2}dz \\ &= \mathrm{Det}(\gamma)h(\gamma,z)^{-2}dz \end{aligned}$$

where $h(\gamma,z) = cz+d$, and similarly $d(\gamma\bar{z}) = \mathrm{Det}(\gamma)h(\gamma,\bar{z})^{-2}d\bar{z}$. Since $\Im(\gamma z) = y|h(\gamma,z)|^{-2}$ it follows that the action of $\mathrm{GL}_2^+(\mathbb{R})$ is a hyperbolic isometry. Since the riemannian structure is invariant under these transformations, it can also be defined on the quotient of $\mathcal{H}$ by any subgroup of $\mathrm{GL}_2^+(\mathbb{R})$. In fact, for some subgroups, this quotient is also a Riemann surface. The subgroups that are of interest to us are the Hecke congruence subgroups:

$$\Gamma_0(N) = \{\gamma\in SL_2(\mathbb{Z}) \,|\, \gamma \text{ is upper triangular} \pmod N\}$$

The quotients $\Gamma_0(N)\backslash\mathcal{H}$ are not compact (see for example the description of $SL_2(\mathbb{Z})\backslash\mathcal{H}$ in A.5). This can be corrected by considering $\mathcal{H}^* = \mathcal{H}\cup\mathbb{Q}\cup\{\infty\}$. We call the points added to $\mathcal{H}$ the cusps. One can check that the action of $SL_2(\mathbb{Z})$ extends properly to these points given that $\left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right)\infty = a/c$. To make $\mathcal{H}^*$ a topological space, we define the neighborhoods of ∞ to be the points of imaginary value greater than a given constant. For compatibility, their image under $SL_2(\mathbb{Z})$ gives the neighborhood of points in $\mathbb{Q}$.

It can be shown (see [15] Ch.XI or [19] Ch.II) that the quotients $X_0(N) := \Gamma_0(N)\backslash\mathcal{H}^*$ can be given the structure of a compact Riemannian surface.

Remark that since $T = \{\left(\begin{smallmatrix}1 & k\\ 0 & 1\end{smallmatrix}\right) | k \in \mathbb{Z}\}$ forms an infinite subgroup of $SL_2(\mathbb{Z})$, every finite index subgroup of $SL_2(\mathbb{Z})$ possess a non-trivial subgroup of T. It is useful to call the width of a cusp $x = \alpha^{-1}\infty$ the positive integer k_α such that $\left(\begin{smallmatrix}1 & k_\alpha\\ 0 & 1\end{smallmatrix}\right)$ generates $T \cap \alpha\Gamma_0(N)\alpha^{-1}$. It does not depend on the matrix α, but only on the cusp x.

To study a compact Riemannian surface, it is natural to consider its holomorphic differentials. In the case of $X_0(N)$ they can be seen as very explicit objects namely cusp forms of weight 2 for $\Gamma_0(N)$. For $\alpha \in \mathrm{GL}_2^+(\mathbb{R})$, denote by $f|_\alpha(z) := \mathrm{Det}(\alpha)h(\alpha, z)^{-2}f(\alpha z)$.

Definition 2.1. A cusp form of weight 2 for $\Gamma_0(N)$ is a function $f : \mathcal{H} \to \mathbb{C}$ such that

1. $f(z) = f(\gamma z)\, h(\gamma, z)^{-2}$ for all $\gamma \in \Gamma_0(N)$.

2. For all $\alpha \in SL_2(\mathbb{Z})$, the function $f|_\alpha(z) = h(\alpha, z)^{-2}f(\alpha z)$ possesses a Fourier expansion of the form
$$f\,|_\alpha = \sum_{n>0} a_n^{(\alpha)} e^{2\pi i n z/k_\alpha} \tag{2.1}$$

In particular, since $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right) \in \Gamma_0(N)$, a cusp forms f can be written as $\sum a_n q^n$ with $q = e^{2\pi i\tau}$ and $a_1 = a_1^\infty$. Cusp forms form a vector space over $\mathbb{C}$ denoted by $S_2(N)$. To describe the relation that these objects have with elliptic curve we still need to introduce more notations.

First, note that if $f \in S_2(N)$ then, for $s \geq 1$, f is also in $S_2(sN)$. Furthermore, if $\alpha_s = \left(\begin{smallmatrix}1 & 0\\ 0 & s\end{smallmatrix}\right)$ and $g(z) = f\,|_{\alpha_s}(z) = s^{-1}f(s^{-1}z)$ then $g \in S_2(sN)$. Indeed, since $\alpha_s^{-1}\Gamma_0(sN)\alpha_s \subseteq \Gamma_0(N)$, then $f\,|_{\alpha_s}|_\gamma = f\,|_{\alpha_s^{-1}\gamma\alpha_s}|_{\alpha_s} = f\,|_{\alpha_s}$ for any $\gamma \in \Gamma_0(sN)$. Cusp forms in $S_2(N)$ obtained from cusp forms in $S_2(N')$ for some $N' \mid N$ and $N' \neq N$, are called old forms, and the space they generate is denoted $S_2^{\mathrm{old}}(N)$. These are the

elements that are not of interest to us, and in order to define a complementary space we need some extra structure on the vector space.

Definition 2.2. The Peterson scalar product for $f, g \in S_2(N)$ is

$$\langle f, g \rangle = \int_{\mathcal{H}/\Gamma_0(N)} f(z)\overline{g(z)}dx\,dy \tag{2.2}$$

The region $\Gamma_0(N)\backslash\mathcal{H}$ is described as follows: we write $SL_2(\mathbb{Z}) = \cup_i \beta_i \Gamma_0(N)$ and obtain a fundamental domain for $\Gamma_0(N)\backslash\mathcal{H}$ as $\cup \beta_i^{-1} F$, where F is the fundamental domain of $SL_2(\mathbb{Z})\backslash\mathcal{H}$. It is not too hard to check that the integral is convergent (due to the behavior at the cusp) and that it is well-defined (i.e. that it does not depend on the choice of the fundamental region). It is also non-degenerate (see [20]).

It is now possible to define a perpendicular subspace to $S_2^{\text{old}}(N)$. It is denoted $S_2^{\text{new}}(N)$. One is then led to consider a family of self-adjoint operators (Hecke operators see [15]) for this new space. Since these operators commute, it is possible to find a basis of simultaneous eigenvectors of $S_2(N)$. We say f is a newform of level N when it is a simultaneous eigenvector and its first Fourier coefficient a_1 is 1. It is actually possible to choose a basis for $S_2(N)$ consisting of newforms with integer Fourier coefficients.

To a newform of level N we attach an L-function by setting

$$L(f, s) = \sum_{n=1}^{\infty} a_n n^{-s} \tag{2.3}$$

This function satisfies many of the properties that the one defined for elliptic curves does.

Theorem 2.1. (Eichler-Shimura construction) *Given f a newform of level N with integer Fourier coefficients there exists an elliptic curve E_f over $\mathbb{Q}$ such that $L(E_f, s) = L(f, s)$*

For a discussion of this construction see [6], [15] or [21]. An important step in the proof is to realize that $X_0(N)$ is an algebraic curve over $\mathbb{C}$ that possess a model

over $\mathbb{Q}$. Simply said it is in bijection with a curve described by the vanishing of a polynomial with coefficients in $\mathbb{Q}$. In this model, points on the modular curve $X_0(N)$ are given by a pair of elliptic curves (actually, their j-invariant) related together by a cyclic N-isogeny (an isogeny whose kernel is cyclic and of cardinality N)

Crucial to our aims is the fact that this construction also gives an algebraic map $\Phi_N : X_0(N) \to E_f$ where E_f is obtained by the Eichler-Shimura construction. Further, one has that $\Phi_N^*(\omega) = c2\pi i f(\tau)d\tau$ where ω is the Néron differential of E_f, $c \in \mathbb{Q}^*$ is a constant (called the Manin constant of E_f), and $f(\tau)d\tau$ is the differential of $X_0(N)$ given by f. This map can be actually be made explicit:

Theorem 2.2. *Let Λ_E be the Néron lattice of E_f and let c be the Manin constant attached to E_f. Let $\Phi_w : \mathbb{C}/\Lambda_E \to E(\mathbb{C})$ be the Weierstrass uniformisation. Then for $\tau \in \mathcal{H}^*$,*

$$\Phi_N(\tau) = \Phi_w(z_\tau) \text{ where } z_\tau = c\int_{i\infty}^{\tau} 2\pi i f(z)dz = c\sum_{n=1}^{\infty}\frac{a_n}{n}q^n, \text{ with } q = e^{2\pi i\tau} \qquad (2.4)$$

Though the description given here is purely analytic, this is actually an algebraic map between $X_0(N)$ and E_f. It can also be showed that this maps sends cusps to torsion points (see [15] XI). One question naturally raised from this construction is which curves can be obtained in such a manner. It has been recently solved thanks to a fundamental breakthrough of Wiles. Indeed, every isogeny class possesses an elliptic curve which can be constructed from a newform, and this specific curve is called the strong Weil curve. If a curve is not a strong Weil curve then we say it is a weak Weil curve in the isogeny class.

2.2 Definition

Considering that we have an algebraic map from $X_0(N)$ to an elliptic curve E of conductor N, and that our aim is to produce a point in E defined over $\mathbb{Q}$, it seems

reasonable to look at points on $X_0(N)$ on which we have some Galois theoretic control. The definition then comes naturally (see also [10]):

Definition 2.3. A Heegner point (on $X_0(N)$) associated to the order $\mathcal{O}$ (of a quadratic imaginary field K) is a point $(j(A),\, j(A'))$ where A, A' both have complex multiplication by $\mathcal{O}$ and are, like all points of $X_0(N)$, related by a cyclic N-isogeny.

Alternatively, using Weierstrass description of elliptic curves over $\mathbb{C}$, we can see the isogeny as a map $A \simeq \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda' \simeq A'$ where Λ and Λ' are the lattices associated to A and A'. Since the isogeny is cyclic and we can use a homothety of $\mathbb{C}^\times$ (i.e. an isomorphism over $\mathbb{C}$), to have that $\Lambda \subseteq \Lambda' \subseteq \mathcal{O}$ and $\Lambda'/\Lambda \simeq \mathbb{Z}/N$. Then $\mathfrak{n} = \Lambda \cdot \Lambda'^{-1}$ is an integral ideal. A consequence of interest to lemma 1.6 is that we can get a nice description of $\mathfrak{n}$:

$$\mathcal{O}/\mathfrak{n} = \mathcal{O}/\Lambda \cdot \Lambda'^{-1} \simeq \Lambda'/\Lambda \simeq \mathbb{Z}/N \tag{2.5}$$

It follows that $\mathfrak{n}$ is of norm $N_{K/\mathbb{Q}}(\mathfrak{n}) = N$ and yields a cyclic quotient.

The first question that one should ask is whether or not it is possible choose such a pair of elliptic curves. The above discussion already gives us part of the answer:

Theorem 2.3. *For a given an order $\mathcal{O}$ of discriminant D, and a conductor $N \in \mathbb{Z}$, the following are equivalent:*

1. *A Heegner point exists on $X_0(N)$.*
2. *There exists an ideal $\mathfrak{n}$ of $\mathcal{O}$ such that $\mathfrak{n}$ is cyclic of norm N, i.e. $\mathcal{O}/\mathfrak{n} = \mathbb{Z}/N$.*
3. *The equation $D = B^2 - 4NC$ has a solution (B, C) with $\gcd(N, B, C) = 1$.*

Proof. The fact that $1 \Leftrightarrow 2$ follows from discussion we just made: we have that given a Heegner point we can produce the required ideal as $\mathfrak{n} = \Lambda \cdot \Lambda'^{-1}$. Conversely given

an ideal $\mathfrak{n} \lhd \mathcal{O}$, then any invertible ideal $\mathfrak{a} \lhd \mathcal{O}$ will be a lattice, thus yields an elliptic curve. Taking $\Lambda' = \mathfrak{a} \cdot \mathfrak{n}^{-1}$ and $\Lambda = \mathfrak{a}$ we have the required pair of elliptic curves.

The proof of $2 \Leftrightarrow 3$ comes from the theory of binary quadratic form, thus it has been relegated to appendix A, lemma A.3. □

Remark 2.1. It is important to point out that this theorem also gives us a complete description of a Heegner point as a triplet $(\mathcal{O}, \mathfrak{n}, \mathfrak{a})$, since the last two elements give all the information that is contained in the pair $(A,\, A')$ and the cyclic N-isogeny that relates them, and $\mathcal{O}$ is their endomorphism ring. Furthermore, as the curve $\mathbb{C}/\mathfrak{a}$ is defined up to isomorphism, the ideal $\mathfrak{a}$ is only defined up to principal ideals (homothety of lattices). As a consequence we will write Heegner points as $(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])$ where $[\mathfrak{a}]$ is the equivalence class of $\mathfrak{a}$ in the class group $\mathrm{Cl}(\mathcal{O})$. The conductor of the order $\mathcal{O}$ is often referred to as the conductor of the Heegner point.

Let c be the conductor of $\mathcal{O}$ and suppose that $\gcd(c, N) = 1$, then condition 3 in theorem 3.2 is just $D \equiv B^2 \pmod{4N}$. Indeed, write $D = c^2 \cdot d$ (where d is a fundamental discriminant) and suppose that $D = B^2 - 4NC$. If there is a $p \,|\, \gcd(N, B, C)$ then $p^2 \,|\, d$ which is impossible unless $p = 2$. If this is the case, then one notes that $d \equiv 8$ or $12 \pmod{16}$ and $B^2 \equiv 0$ or $4 \pmod{16}$ a contradiction.

Definition 2.4. We say that an order $\mathcal{O} \subseteq K$ of discriminant D and conductor c satisfies the Heegner Hypothesis (HH) for a given elliptic curve of conductor N if D is a square $\mathrm{mod} 4N$ and $\gcd(c, N) = 1$.

This definition is actually slightly weaker than the usual one, in which we ask for the discriminant to be coprime to N. We will refer to the latter as the Strong Heegner Hypothesis (SHH). Note that some cases fall outside HH, for example, a curve of conductor $N = 40$ with $D = -96$ has a cyclic ideal of norm 40, namely $\langle 40, 4 + 2\sqrt{-6} \rangle$. Remark that this is not an invertible ideal, and is consequently very awkward to work with.

2.3 Galois action on Heegner points

Now that we have defined a proper point on $X_0(N)$, we can start to apply the tools that come from CM theory. As a recall, we had a curve E' with CM by $\mathcal{O}$, and we defined τ such that $\langle 1, \tau \rangle$ is homothetic to the lattice associated to E'. We then had to consider $\mathcal{O} = \mathcal{O}_{\langle 1,\tau \rangle}$, so that $\forall \alpha \in \mathrm{Cl}(\mathcal{O})$, $j(\alpha \star \tau) = \mathrm{rec}(\alpha)^{-1} j(\tau)$. An important point in the proof of this result is that $j(\tau)$ belongs to the Hilbert class field of $\mathcal{O}$, $H_{\mathcal{O}}$.

Since we will want to apply this theorem to the point $(j(A), j(A'))$ on $X_0(N)$ we first have to describe the action on the two j-invariants. First, let's define υ and τ such that $\Lambda \simeq \langle 1, \upsilon \rangle$ and $\Lambda' \simeq \langle 1, \tau \rangle$. Note that we can choose them so that $\upsilon = N\tau$, as there is a cyclic N-isogeny $A \to A'$, to avoid the need of specifying both of them. We are then led to consider the order $\mathcal{O}_{\tau,N} = \mathcal{O}_{\langle 1, N\tau \rangle} \cap \mathcal{O}_{\langle 1,\tau \rangle}$ as its class field $H_{\mathcal{O}_{\tau,N}}$ contains both $j(\tau)$ and $j(N\tau)$. This can be seen using the description 1.43 of the action of the Galois group of $H_{\mathcal{O}_{\tau,N}}$. Thus the Heegner point $X_\tau = (j(N\tau), j(\tau))$ is in $X_0(N)(H_{\mathcal{O}_{\tau,N}})$. The following corollary follows directly since the map $\Phi_N : X_0(N) \to E$ is a map of algebraic curves defined over $\mathbb{Q}$.

Corollary 2.1. *The image of the Heegner point X_τ by Φ_N lies in $E(H_{\mathcal{O}_{\tau,N}})$.*

So far, we have found a point on E in a specific number field. As we wish to obtain a point on $E(\mathbb{Q})$ from this, we will now look at the Galois action. Using the reciprocity map, this will translate to the familiar action of $\mathrm{Cl}(\mathcal{O}_{\tau,N})$:

$$\begin{aligned} \mathrm{rec}(\mathfrak{a})^{-1}(j(N\tau), j(\tau)) &= (\mathrm{rec}(\mathfrak{a})^{-1} j(N\tau), \mathrm{rec}(\mathfrak{a})^{-1} j(\tau)) \\ &= (j(\mathfrak{a} \star N\tau), j(\mathfrak{a} \star \tau)) \\ &= (j(\upsilon'), j(\tau')) \end{aligned} \tag{2.6}$$

Where υ' and τ' are both defined modulo the action of $SL_2(\mathbb{Z})$. However there is still a cyclic N-isogeny between the elliptic curves represented by υ' and τ' thus they can again be chosen so that $\upsilon' = N\tau'$.

It is convenient to write this action as $\mathfrak{a} \star_N \tau = \tau'$ to emphasize it is a level N lift of the $\star$ action. Also note that the result τ' is defined up to $\Gamma_0(N)$. Indeed, if $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$ then $\langle 1, \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\tau\rangle$ and $\langle 1, N\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\tau\rangle$ are both homothetic (by a factor of $c\tau + d$) to $\langle 1, \tau\rangle$ and $\langle 1, N\tau\rangle$. It then makes sense to define the set of Heegner points as $\mathrm{HP}(\mathcal{O}) = \{\tau \in \mathcal{H}/\Gamma_0(N) \mid \mathcal{O}_{\tau,N} = \mathcal{O}\}$. In fact, written like this, the elements in $\mathrm{HP}(\mathcal{O})$ are just different representatives of the elements in $\mathrm{Ell}(\mathcal{O})$. We will now make explicit the relation between this description and the previous one $(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])$, and doing so will enable us to get a very simple method to determine the Galois action and the Heegner points.

It is actually very easy to state the actual relation between these two notations. From $\mathfrak{n}$ and $\mathfrak{a}$ we produce the lattice Λ, and then get a homothetic lattice whose generators are 1 and τ. However the choice of τ is not fortuitous, since we must make sure that $\mathcal{O}_{\tau,N} = \mathcal{O}$.

$$\begin{aligned}
\mathcal{O}_{\tau,N} &= \mathcal{O}_{\langle 1,N\tau\rangle} \cap \mathcal{O}_{\langle 1,\tau\rangle} \\
&= \{\alpha \in \mathcal{O} | \alpha \cdot \langle 1, N\tau\rangle \subseteq \langle 1, N\tau\rangle \text{ and } \alpha \cdot \langle 1, \tau\rangle \subseteq \langle 1, \tau\rangle\} \\
&= \{\alpha \in \mathcal{O} | \exists \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right) \in M_2(\mathbb{Z}) \text{ such that } \alpha\binom{N\tau}{1} = \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right)\binom{N\tau}{1} \\
&\qquad\qquad \text{and } \alpha\binom{\tau}{1} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\binom{\tau}{1}\} \\
&= \{\alpha \in \mathcal{O} | \exists \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right) \in M_2(\mathbb{Z}) \text{ such that } \alpha\binom{\tau}{1} = \left(\begin{smallmatrix} 1/N & 0 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right)\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)\binom{\tau}{1} \\
&\qquad\qquad \text{and } \alpha\binom{\tau}{1} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\binom{\tau}{1}\} \\
&= \{\alpha \in \mathcal{O} | \exists \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{Z}) \text{ and } N \,|\, c \text{ such that } \alpha\binom{\tau}{1} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\binom{\tau}{1}\} \\
&= \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{Z}) \text{ and } N \,|\, c \text{ such that } \tau = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\tau := \tfrac{a\tau+b}{c\tau+d}\}
\end{aligned} \tag{2.7}$$

It is convenient to define $M_0(N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{Z}) \text{ and } N \,|\, c\}$, the set of upper triangular matrices modulo N. In the last step we replace the usual quadratic imaginary order by an order of matrices. Note that one can pass from one to the other by looking at the eigenvalues of such matrices. Their eigenvectors are $\binom{\tau}{1}$ and $\binom{\bar{\tau}}{1}$, and by taking the eigenvalue associated to the first one , we recover an element of $\mathcal{O}_{\tau,N}$.

From this one can explicitly describe a Heegner point. Suppose $\mathcal{O} = \langle 1, \omega_D \rangle$. We will use 2.7 to find a τ such that $\mathcal{O}_{N,\tau} = \mathcal{O}$. Since the identity matrix is always in $\mathcal{O}_{N,\tau}$, it suffices to find another one $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $N \mid c$ that behaves like ω, i.e. satisfies $A^2 - Tr_{K/\mathbb{Q}}(\omega_D) \cdot A + N_{K/\mathbb{Q}}(\omega_D) = 0$. From small calculations one finds that this is equivalent to $Tr(A) = Tr_{K/\mathbb{Q}}(\omega_D)$ and $\mathrm{Det}(A) = N_{K/\mathbb{Q}}(\omega_D)$. τ can finally be obtained by solving $\tau = A\tau$ so $\tau = ((2a - Tr_{K/\mathbb{Q}}(\omega)) + \sqrt{D})/2c$ where D is the discriminant of $\mathcal{O}$. Interestingly $(2a - Tr_{K/\mathbb{Q}}(\omega_D))^2 = -4bc + D \equiv D \pmod{4N}$. Thus $s = 2a - Tr_{K/\mathbb{Q}}(\omega_D)$ is a square root of D modulo $4N$.

Though the preceding method is very efficient to compute one Heegner point, and does not rely on the more cumbersome $(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])$ notation, it does not help expressing the Galois action on such points. For this, it is more useful to proceed using binary quadratic forms. As in the appendix, here I will denote the map that sends a form f to its associated integral ideal.

To get τ from $(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])$ one has to proceed with more care than simply picking a point in $\mathcal{H}$ with $\langle 1, \tau \rangle \simeq \mathfrak{a}\mathfrak{n}^{-1}$. For a start, $\langle 1, \tau \rangle$ must have endomorphism ring $\mathcal{O}$; it is a fractional $\mathcal{O}$-ideal. As such, it is associated to a primitive binary quadratic form f of discriminant $D = \mathrm{Disc}(\mathcal{O})$ (i.e. $f(\tau, 1) = 0$). Indeed, if $f(x, y) = Ax^2 + Bxy + Cy^2$ is such that $\tau_f = \tau$, we must have that $N \mid A$ and $B^2 \equiv D \pmod{4N}$, in order to have $\mathcal{O}_{\tau,N} = \mathcal{O}$. Furthermore, as $\langle 1, \tau \rangle \simeq \Lambda'$, $I(f) \in [\Lambda'] = [\mathfrak{a}\mathfrak{n}^{-1}]$. The ideal $\mathfrak{n}^{-1}$ is in turn represented by a form $g(x, y) = Nx^2 - sxy + jy^2$ where s is a square root of $D \mod 4N$ and $4Nj = s^2 - D$ (see lemmas A.2 and A.3, note the $-s$ as opposed to s when we are looking at $\mathfrak{n}$). Let $h(x, y)$ be the form associated to some $\mathfrak{i} \in [\mathfrak{a}]$, then $\Lambda' = \mathfrak{i}\mathfrak{n}^{-1}$ is equivalent to $f = g \cdot h$. Finally, to have that $N \mid A$ and $B^2 \equiv D \pmod{4N}$ (so B is determined $\mathrm{mod} 2N$), it follows that $\mathfrak{i}$ must be chosen so that the Dirichlet composition of g and h is possible (it always exists by remark A.1). So τ is obtained as the point in $\mathcal{H}$ associated to $g \cdot h$ where $I(g) = \mathfrak{n}^{-1}$, and $I(h) = \mathfrak{i}$ ($\mathfrak{i}$ chosen as above).

We work out the inverse correspondence as follows. First, from τ we recover $\mathcal{O} = \mathcal{O}_{\tau,N}$. Second, we find the binary quadratic form of $\tau = \frac{s+\sqrt{D}}{2kN} \sim f(x,y) = kN\ x^2 + s\ xy + j\ y^2$. Then we define $\mathfrak{n}^{-1}$ as the ideal represented by $g(x,y) = Nx^2 + (s \bmod 2N)xy + j'y^2$, and $\mathfrak{i} \sim h(x,y) = kx^2 + (s \bmod 2k)xy + j''y^2$. Since $\gcd(N,k,s) = 1$, Dirichlet composition of g and h is possible and $f = g \cdot h \Rightarrow \langle 1, \tau \rangle \simeq \mathfrak{i}\mathfrak{n}^{-1}$. Consequently $(\mathcal{O}, \mathfrak{n}, [\mathfrak{i}])$ is just the long notation for τ.

Theorem 2.4. *Let $(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])$ be a Heegner point, and $\mathfrak{b} \in \mathrm{Cl}(\mathcal{O})$ then*

$$\mathrm{rec}(\mathfrak{b})^{-1}(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}]) = (\mathcal{O}, \mathfrak{n}, [\mathfrak{a}\mathfrak{b}^{-1}]) \tag{2.8}$$

Proof. This result is direct from the translation of the two notations and the definition of $\star_N$. Indeed, $\mathfrak{n}^{-1}[\mathfrak{a}]$ is related to τ by the usual homothety. On the other hand, $\tau' = \mathfrak{b} \star_N \tau$ is defined so that $\langle 1, \tau' \rangle = \langle 1, \tau \rangle I^{-1}$ where I is a representative of $[\mathfrak{b}]$. τ' then translates back to a representative of $\mathfrak{n}^{-1}[\mathfrak{a}\mathfrak{b}^{-1}]$. □

As a consequence of this, one can note that the $\star_N$ action on $\mathrm{HP}(\mathcal{O})$ is simply transitive. We are now also able to produce a point on $E(\mathbb{Q})$: first we can make a point $P_K \in E(K)$ simply by adding all the points in $\Phi_N(\mathrm{HP}(\mathcal{O}))$, and then $P_K + \overline{P_K}$ yields the desired point. Unfortunately, we have no guarantee that this point is not the point at infinity.

However, getting a point on $E(\mathbb{Q})$ is almost nothing when compared to the properties of P_K. Gross and Zagier [11] made an impressive link between this a priori algebraic data and the first derivative of the L-function of $E(K)$. They proved that $\langle P_K, P_K \rangle$, where $\langle\ ,\ \rangle$ denotes the Néron-Tate height on $E(K)$, is proportional to $L'(E/K, 1)$, and as a consequence, P_K is torsion $\Leftrightarrow L'(E/K,1) = 0$. Kolyvagin ([16] and [17]) then showed that we can get an upper bound on the Mordell-Weil group E(K). Indeed, if P_K is non-torsion, then it generates a finite-index subgroup of E(K). However, this also shows that P_K cannot be properly used on curves with rank bigger than one. Combining these two important facts about P_K, it is possible to prove that

if the analytic rank of the curve $E(\mathbb{Q})$ is 0 or 1, then it is equal to the algebraic rank of E.

2.4 Calculation of Heegner Points

One of the most exceptional properties of Heegner points is that they are very simple to compute as was sketched in the preceding section. Indeed, they are described only in terms of binary quadratic forms, and by virtue of theorem 2.2, we can explicit the point to which they map to. In order to illustrate this, we will produce some examples, beginning trivial class group examples before moving to slightly more complex cases.

Example 2.1. Let's begin by the first curve on Cremona's table (see [5]): b$y^2 + y = x^3 - x^2 - 10x - 20$ of conductor 11. First we must find a D (discriminant of a quadratic field) which is a square modulo $4 \cdot N = 44$. A nice choice would be -43, as its class group is trivial and its square root $\bmod 4N$ is 1. So $\sharp HP(\mathcal{O}) = 1$, and we can get τ by the first method mentioned: $-43 = 1^2 \pmod{44} \Rightarrow s = 1$, and $A = \left(\begin{smallmatrix} 1 & 11 \\ 1 & 0 \end{smallmatrix}\right) \Rightarrow \tau = (1 + \sqrt{-43})/22$. The z_τ in theorem 2.2 is then given by

$$\sum_{n \geq 1} a_n \cdot q^n / n = q - q^2 - q^3/3 + \dots \tag{2.9}$$

(the Manin constant for the strong Weil curves of conductor less than 8000 has been found to be one) where $q = e^{2\pi i \tau}$. The result of this sum maps to a point on the elliptic curve using Weierstrass uniformisation: $\Phi_w(z) = (53 - 4\sqrt{-43}, -347 + 44\sqrt{-43})$. Of course, we have not proved that this is the image, but it numerically fits to a few thousands of digits, and is an exact solution to the Weierstrass equation.

Example 2.2. Let's take the first curve of rank one that appears in the tables: $y^2 + y = x^3 - x$ of conductor 37. If we pick -67 ($\equiv 9^2 \pmod{148}$) as our discriminant for the quadratic field, we again conveniently find ourself in a trivial class group case,

thus we need only to find one $\tau = (9 + \sqrt{-67})/74$. Summing up the $a_n e^{2\pi n i \tau}/n$ and using Φ_w we are given the point $(6, -15)$. One can check that this point is of infinite order.

When the class group is non-trivial, it becomes more convenient to see Heegner points as the triplet $(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])$. If for each equivalence class of $Cl(\mathcal{O})$, we take a representative say $\mathfrak{a}_i$ for $i = 1, \ldots, h(\mathcal{O})$, we can associate to each of them a distinct $\tau_i \in HP(\mathcal{O})$ as described in the previous section. For these computations, one can rely only on binary quadratic forms. We first compute the class group $h_i(x, y)$ as in Remark A.2, and find the form $g(x, y)$ associated to our ideal of norm N. If h_i cannot be composed with g using Dirichlet composition, then we replace it by an equivalent form for which it is. Once we have a proper set of representatives for $Cl(\mathcal{O})$, we have our $\tau_i \sim f_i(x, y) = g(x, y) \cdot h_i(x, y)$.

Example 2.3. The first curve for which no $\mathcal{O}$ with $\mathrm{Cl}(\mathcal{O}) = 1$ satisfies the SHH is $y^2 + xy + y = x^3 + 4x - 6$ of conductor 14. We can take $D = -31 \equiv 5^2 \pmod{56}$, which gives

$$\begin{aligned} h_1(x, y) &= x^2 + xy + 8y^2, \\ h_2(x, y) &= 2x^2 - xy + 4y^2, \\ h_3(x, y) &= 2x^2 + xy + 4y^2, \\ g(x, y) &= 14x^2 + 5xy + y^2 \end{aligned} \tag{2.10}$$

Only h_2 does not satisfy our requirement ($\gcd(14, 2, (5-1)/2) = 2$), but it is equivalent to $4x^2 + xy + 2y^2$ that does. As a consequence

$$\begin{aligned} f_1(x, y) &= 14x^2 + 5xy + y^2 && \Rightarrow \tau_1 = (-5 + \sqrt{-31})/28 \\ f_2(x, y) &= 56x^2 + 33xy + 5y^2 && \Rightarrow \tau_2 = (-33 + \sqrt{-31})/112 \\ f_3(x, y) &= 28x^2 + 33xy + 10y^2 && \Rightarrow \tau_3 = (-33 + \sqrt{-31})/56 \end{aligned} \tag{2.11}$$

We can then find the 3 points to which they correspond on $E(H_{\mathcal{O}})$, however their algebraic expression can be very complicated. It is easier to look at the polynomial

their x and y coordinates satisfy:

$$X^3 + X^2\left(\frac{5-5\sqrt{-31}}{2}\right) + X(-27+2\sqrt{-31}) + (12-3\sqrt{-31}) \textit{ for the x-coordinate}$$
$$Y^3 + Y^2\left(\frac{-85+5\sqrt{-31}}{2}\right) + Y(35+48\sqrt{-31}) + (404+11\sqrt{-31}) \textit{ for the y-coordinate} \tag{2.12}$$

or to compute the point $P_K = \sum \Phi_N(\tau_i) = \left(\left(\frac{1-\sqrt{-31}}{2}\right), \sqrt{-31}\right)$

An interesting thing to point out is that the points we obtained so far on the elliptic curves have coordinates which are algebraic integers, and none of them are torsion points. One can ask whether this is always the case. The answer is no. For example the first strong Weil curve appearing in the tables that has non-integral Heegner points is $33A1$ (with $D = -8$ for example); note that $11A2$ is actually the first curve in the tables not to possess this property. Also, if one looks at the curve 121A1 ($y^2 + xy + y = x^3 + x^2 + x + 1$) and pick $D = -19$, then $\tau = \frac{49+\sqrt{-19}}{242}$ and $\Phi_N(\tau)$ is the point at infinity.

2.5 Numerical Results

We will now comment on the Heegner points that were calculated on all the elliptic curves of conductor less than 3000. The actual data being too lengthy to fit in these pages, it is going to be available on Henri Darmon's website.

2.5.1 Modular uniformisation

First there is an interesting application of Heegner points to the Manin constant c. Here are a few facts (see [1], [8], [9] and [18]) that we know about it:

$$1 - c \text{ is an integer}$$
$$2 - \text{if } p \mid c \text{ then } p = 2, 3, 5 \text{ or } 7$$
$$3 - \text{if } p \mid c \text{ then } p \mid N$$
$$4 - \text{if } p \mid c \text{ then } p^2 \mid 4N$$
$$5 - \text{if } 4 \mid c \text{ then } 4 \mid N$$

So we can only be certain that $c = 1$ when N is odd and not divisible by 9, 25, and 49. It has been verified by Cremona that the strong Weil-curve of each isogeny class (the first one to appear in the tables) has $c = 1$. Since the points z_τ are multiplied by c before using Weierstrass uniformisation, it could be possible that assuming $c = 1$ yield points that are not algebraic. In fact it happens for the curve 27A3 ($y^2 + xy = x^3$), where $c = \pm 3$ or ± 9 give algebraic points but not $c = 1$ (at least not the first thousand digits). Similarly for 32A2 ($y^2 = x^3 - x$), and this time $c = \pm 2$ or ± 4 give algebraic points.

2.5.2 Integrality

As was mentioned in the preceding section, on some curves the Heegner points are algebraic integers for a given discriminant. Surprisingly, on some curves these points seem to be integral for any given discriminant (the first example is 11A1 on Cremona's table, for which it has been tested for a hundred discriminants). Sometimes, the minimal polynomial satisfied by the Heegner points is even defined over the order we chose to get the points (which is not necessarily maximal), and again some curves seem to possess this property for any discriminant (the first example is 37A1).

Definition 2.5. *(IP)* An elliptic curve E of conductor N is said to have the integrality

property if for all (not necessarily fundamental) discriminant $D < 0$ with $D \equiv B^2 \pmod{4N}$ for some $B \in \mathbb{Z}$, the Heegner points are integral points of E over the Hilbert class field of $\mathcal{O}_D$, i.e. their coordinates belong to $\mathcal{O}_{H_D}$.
(SIP) If moreover the coordinates of the Heegner points satisfy polynomials in $\mathcal{O}_D[x]$, then we say the curve have the strong integrality property.

Of course, squares mod$4N$ coprime to N are infinite, since such numbers need only give satisfies congruence relations for every primes dividing N. Since we only tried a finite number of discriminant (the first 18 that satisfies the SHH, the first 12 that satisfy HH but not SHH), the results discussed here are uncertain in nature, but they indicate some nice behavior.

conductor	IP	SIP
< 1000	387	183
$1000 - 2000$	31	22
$2000 - 3000$	7	4

An interesting thing to note is that the conductor of the integral curves of conductor bigger than 701 all have a valuation greater or equal to 3 at some prime (forcefully 2 or 3). Furthermore of the 162 conductors (totalling 356 curves) less than 701 with integral curves, 72 (totalling 232 curves) have high valuation at 2 or 3 and only 50 (totalling 64 curves) are squarefree. In fact, the last curve whose conductor is squarefree to have this property is 238B1. Lastly, even if at first it seems all the integral curves of rank 1 have Heegner points that are defined over the order, 11 of them do not have it and 6 rank 0 curve do.

Lastly, note that whenever a weak Weil curve (one that is not directly obtained by the modular parametrization) satisfies the integrality property, the strong Weil curve also does.

2.5.3 Trivial points

Even if we know that Heegner points are algebraic, one of the disappointing occurrence is when it is a point at infinity. This means that points that are not cusp in $X_0(N)$ yield a trivial point (recall that cusp always give torsion points). This property of the parametrization (mapping "non-cusp" to O) is never in conjunction with integrality. It has been observed that the Heegner points of a discriminant satisfying HH but not SHH are more frequently points at infinity.

2.5.4 The point P_K

If we sum up all the Heegner points for a given discriminant D, then we get a point P_K which is in K the quotient field of the order of discriminant D. Due to the theorem of Kolyvagin, we know that if the rank of the curve (over K) is greater than one then P_K is torsion. However, we observed that all the curves of rank 2 (there are no curve with bigger rank for conductors less than 3000) considered $P_K = O$, the point at infinity. It thus consolidate the fact that Heegner points (restricted to quadratic fields) are purely rank one phenomenon, being a completely trivial construction for higher ranks. Another interesting fact is that for curves of rank 1, the points P_K are always real. This suggests that the P_K have complex coordinates only when the rank of the curve (over $\mathbb{Q}$) is zero (as in example 2.3). One could think that this is expected by Kolyvagin: when P_K is non-torsion then it generates a finite index group in $E(K)$ and $E(\mathbb{Q})$ is already such a subgroup when the curve is of rank 1 over $\mathbb{Q}$. However if P_K is torsion, nothing guarantees that it should be real, and in general there is no reason to believe that the torsion-free part over $\mathbb{Q}$ is equal to the torsion-free part over K.

Conclusion

In this thesis, we described a method to construct algebraic points on any elliptic curve, using complex multiplication and the modular parametrization. This construction can be made explicit by simple computations on binary quadratic forms and coefficients of the L-series of the elliptic curve. The results of these computations raise a number of questions.

1. Does the fact that the modular parametrization does not map non-cuspidal point of $X_0(N)$ to O imply the integrality property?

2. Is there a finite number of elliptic curves (with squarefree, cube free conductor) with the integrality property? And if so, how complete is the list given?

3. Why is P_K real for any discriminant when we consider a rank one curve?

There are some indications that the first question can be answered positively, which might also explain why weak Weil curves rarely have this property. There is still work to do before modular parametrization is fully understood.

Appendix A

Binary Quadratic Forms

Binary quadratic forms are a concrete object which are intimately related to the ideals in quadratic orders. They are a very useful tool (if not the most convenient) to make explicit operations on those ideal. As is seen in the second chapter they are also useful to calculate Heegner Points.

Definition A.1. A binary quadratic form is a function f of two variables of the form $f(X,Y) = AX^2 + BXY + CY^2$ with $A, B, C \in \mathbb{Z}$. We say it is

$$\begin{aligned} \text{primitive} \quad & \text{when } \gcd(A,B,C) = 1 \\ \text{definite} \quad & \text{when } \mathrm{Disc}(f) := B^2 - 4AC < 0 \text{ and } A > 0. \\ \text{reduced} \quad & \text{when } -A < B \leq A \leq C \text{ and if } A = C \text{ then } B \geq 0 \end{aligned} \tag{A.1}$$

Furthermore, we say $n \in \mathbb{Z}$ is represented by f if $\exists X_n, Y_n \in \mathbb{Z}$ such that $f(X_n, Y_n) = n$. If $\gcd(X_n, Y_n) = 1$ then n is said to be properly represented.

Since we will restrict our attention to positive primitive binary quadratic form, they will henceforth only be called forms. A classical question that led to the study of these forms was to find what were the integers represented by a given form. The first thing to remark is that if we make an invertible change of variable then this set

remains invariant. So we define an action of $SL_2(\mathbb{Z})$ on the binary quadratic forms as follows:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot f(X,Y) = f(aX+bY, cX+dY) = A'X^2 + B'XY + C'Y^2$$
$$\text{where } A' = a^2A + acB + c^2C, B' = 2(abA + bcB + cdC) + B, C' = b^2A + bdB + d^2C$$
$$\text{and } B'^2 - 4A'C' = B^2 - 4AC \tag{A.2}$$

We say that 2 forms f, g are properly equivalent if there is an $M \in SL_2(\mathbb{Z})$ such that $M \cdot f = g$. Two equivalent forms represent the same integers, however the converse is not true (take $M \in GL_2(\mathbb{Z})$ with $\text{Det}(M) = -1$). The reason to favor $SL_2(\mathbb{Z})$ over $GL_2(\mathbb{Z})$, is that the former sends positive (resp. primitive) forms to positive (resp. primitive) forms, but not the latter.

Theorem A.1. *Every form is equivalent to a unique reduced form.*

Proof. Let f be a form and $D = \text{Disc}(f)$, then it is convenient to define

$$\tau_f = \frac{-B + \sqrt{D}}{2A} \in \mathcal{H} = \{z \in \mathbb{C} \mid \Im(\tau) > 0\} \tag{A.3}$$

First, we can show that $f \mapsto \tau_f$ is a injection. Since $f(X,1)$ is a minimal polynomial for τ over $\mathbb{Z}$, if g is also mapped to τ_f then $g(X,Y) = kf(X,Y)$ as $g(X,1)$ has τ as a solution and is of degree 2. If $|k| > 1$, then g is not primitive, and if $k = -1$ then g is not positive definite. Therefore $g = f$, and we have a bijection between quadratic points in $\mathcal{H}$ and forms. One can check that for $M \in SL_2(\mathbb{Z})$,

$$\tau_{M \cdot f} = \frac{a\tau + b}{c\tau + d} =: M \cdot \tau \tag{A.4}$$

and that $\Im(M \cdot \tau) > 0$. We will show that under this action any point τ in the complex upper half-plane $\mathcal{H}$, there is a unique point in

$$F = \{\tau \in \mathcal{H} \mid -\frac{1}{2} \leq \Re(\tau) < \frac{1}{2}, |\tau| \geq 1 \text{ and if } |\tau| = 1 \text{ then } \Re(\tau) \leq 0\} \tag{A.5}$$

that is the image of $N \cdot \tau$, for some $N \in SL_2(\mathbb{Z})$. Once this is established, it is easy to see that the form associated of such points will give reduced forms.

Existence. To show this first note that for $A \in M_2(\mathbb{Z})$ then

$$\Im\left(\frac{a\tau+b}{c\tau+d}\right) = \mathrm{Det}(A)|c\tau+d|^{-2}\Im(\tau) \tag{A.6}$$

Since the function $F(c,d) = |c\tau+d|^2 = Cc^2/A - Bcd/A + d^2$ admits a minimum for $c,d \in \mathbb{Z}$ with $\gcd(c,d) = 1$ (else divide c and d by their gcd), we can find some $a,b \in \mathbb{Z}$ such that $ad-bc = 1$, so $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$. Let $\tau' = M_1 \cdot \tau$, and $T_n = \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$, then $T_n \cdot \tau' = \tau' + n$ and in particular $\Re(T_n \cdot \tau') = Re(\tau') + n$. Take n such that $-\frac{1}{2} \leq \Re(\tau') + n < \frac{1}{2}$, and write $\tau'' = T_n \cdot \tau' = T_n M \cdot \tau$. Note that $M_n = T_n M$ has the same lower row than M, thus $\Im(\tau'')$ is maximal amongst equivalent representatives of τ. Consequently $|\tau''| \geq 1$ else $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \cdot \tau'' = |\tau''|^{-1}(-\Re(\tau'') + \imath\Im(\tau''))$ would have greater imaginary part. If $|\tau''| = 1$ and $\frac{1}{2} > \Re(\tau'') \geq 0$ then $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \cdot \tau''$ will have the same real part time -1 and thus will be in F. Otherwise $\tau'' \in F$.

Unicity. Suppose that there is $\tau \in F$ such that $\exists z = x + \imath y \in \mathcal{H}$ and $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ such that $M \cdot z = \tau$. First if $c = 0$ then $a = d = 1$ so $\tau = z + b$. Since both have a real part smaller than $1/2$ in absolute value, $b = 0$ and $\tau = z$. If $c \neq 0$ then we note that for any $\nu \in F$, $\Im(\nu) \geq \sqrt{3}/2$, and also that $|cz+d| \geq cy$, so

$$\frac{\sqrt{3}}{2} \leq \Im(\nu) = \frac{y}{|cz+d|^2} \leq \frac{1}{c^2 y} \leq \frac{2}{c^2\sqrt{3}} \tag{A.7}$$

Consequently $c^2 \leq 4/3 \Rightarrow c = \pm 1$. Since $-M$ and M have the same action, we can suppose $c = 1$. Then $M = \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & d \\ 0 & 1 \end{smallmatrix}\right)$. So if we let $z' = z + d$ and $\nu' = \nu - a$ then $|z'| \geq |z| \geq 1$ and $|\nu'| \geq |\nu| \geq 1$. However if $|z'| = 1$ (resp. $|\nu'| = 1$) then $d = 0$ (resp. $a = 0$). Furthermore, $\frac{-1}{z'} = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) z' = \nu'$ implies that $|\nu'| = |z'| = 1$ and so $a = d = 0$. Thus $M = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, and $|\nu| = |z| = 1$. But $\frac{-1}{z} = \nu$ also implies that $0 \geq x = -\Re(\nu)$ so $\nu \in F$, $|\nu| = 1$ and $\Re(\nu) \geq 0$ a contradiction. □

An interesting thing about the set of reduced forms is that it is finite for a fixed D. Indeed for reduced forms, $D = B^2 - 4AC \leq -3A^2$, so $A \leq \sqrt{-D/3}$. Thus there

at most $-2D/3$ possible choices of A and B (C being determined by $(B^2 - D)/4A$).

Remark A.1. Also for any integer n we can find a form f in any equivalence set such that $\gcd(A, n) = 1$. Indeed, let A' bet the X^2 coefficient in $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot f(X, Y)$, then $A' = a^2A + acB + c^2C$. So we take a, c such that for every prime $p \mid n$,

$$\begin{array}{rcl} \textit{if } p \nmid A & \textit{then} & p \nmid a \textit{ and } p \mid c \\ \textit{if } p \mid A \textit{ and } p \nmid C & \textit{then} & p \mid a \textit{ and } p \nmid c \\ \textit{if } p \mid A \textit{ and } p \mid C & \textit{then} & p \nmid ac \end{array} \tag{A.8}$$

so that $p \nmid A'$ and $\gcd(a, c) = 1$. b and d are the chosen so that $ad - bc = 1$.

There is another operation that one can do on forms, namely composition. Though Gauss defined it in a very general way, it is also very clumsy to work with. Later, Dirichlet gave an equivalent description of it which is more simple but does not apply for arbitrary forms.

Definition A.2. Let $f(X, Y) = AX^2 + BXY + CY^2$ and $g(X, Y) = A'X^2 + B'XY + C'Y^2$ be two forms of discriminant D, and such that $\gcd(A, A', \frac{B+B'}{2}) = 1$. The Dirichlet composition of f and g is defined as the form $h(X, Y) = AA'X^2 + B''XY + \frac{B''^2 - D}{4AA'}Y^2$, with B'' such that

$$\begin{array}{rcl} B'' & \equiv B & \pmod{2A} \\ B'' & \equiv B' & \pmod{2A'} \\ B''^2 & \equiv D & \pmod{4AA'} \end{array} \tag{A.9}$$

Though this definition is not general enough to encompass all the pairs of forms of a given discriminant, we can use it to define the composition of reduced forms. First, given two reduced forms, it is possible to make their X^2 coefficients coprime by changing one of them to another equivalent form. Then the composition is possible using the above definition. Finally, it suffice to find the reduced form equivalent to this composition.

Theorem A.2. *Let the form class group be*

$$\mathrm{Cl}(D) = \{\textit{equivalence classes of forms of discriminant } D\} \tag{A.10}$$

Then Dirichlet composition makes $\mathrm{Cl}(D)$ *into an abelian group.*

Though we will not show the proof of this theorem ([4] p.51), one can easily see that the identity is $X^2 + \alpha XY + \frac{\alpha - D}{4} Y^2$ (where $D \equiv \alpha \pmod 4$). Furthermore, the inverse of $AX^2 + BXY + CY^2$ is $AX^2 - BXY + CY^2$, as can be seen by acting with $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ on the latter.

The association $f \mapsto \tau_f$ almost bridges forms of discriminant D and $\mathcal{O}$ ideals for $\mathrm{Disc}(\mathcal{O}) = D$. Indeed, one can define a map I from forms to lattices as follows $I(f) = A\langle 1, \tau_f \rangle$, where A is the X^2 coefficient in f. In fact we already saw in lemma 1.2 that $\mathcal{O} = \langle 1, A\tau_f \rangle$, thus $I(f)$ is actually an integral $\mathcal{O}$ ideal and its norm is easily seen to be A. Again in lemma 1.2, we saw that this ideal has an inverse, the fractional $\mathcal{O}$ ideal $\langle 1, \overline{\tau_f} \rangle$ where $\overline{\tau_f}$ is the complex conjugate of τ_f.

Lemma A.1. *The map* $I : \mathrm{Cl}(D) \to \mathrm{Cl}(\mathcal{O})$ *is a bijection. In particular* $\mathrm{Cl}(\mathcal{O})$ *is finite.*

Proof. Injectivity. Let $K = \mathrm{Quot}(\mathcal{O})$, we will show that

$$\begin{aligned} \tau' = \tfrac{a\tau + b}{c\tau + d} \quad & \text{for } \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) \\ \Leftrightarrow \quad & \langle 1, \tau \rangle = \lambda \langle 1, \tau' \rangle \text{ for } \lambda \in K^\times \end{aligned} \tag{A.11}$$

If $\tau' = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot \tau$ then

$$\langle 1, \tau' \rangle = (c\tau + d)\langle c\tau + d, a\tau + b \rangle = c\tau + d\langle 1, \tau \rangle \tag{A.12}$$

since $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ defines an invertible change of variable. If $\langle 1, \tau \rangle = \lambda \langle 1, \tau' \rangle$, then

$$\begin{aligned} \lambda\tau' &= a\tau + b \\ \lambda &= c\tau + d \end{aligned} \quad \text{where } \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{Z}) \tag{A.13}$$

However by equation A.2, if $\mathrm{Det}\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) < 0$ then $\tau' \notin \mathcal{H}$ a contradiction so $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$.

Since f and g are equivalent if and only if τ_f is equivalent to τ_g, it follows that $I(f)$ is homothetic to $I(g)$ if and only if f and g are equivalent, proving injectivity.

Surjectivity. Write the fractional ideal $\mathfrak{a}$ as $\langle \alpha, \beta \rangle$, then (up to switching α and β) one has that $\mathfrak{a} \simeq \langle 1, \tau \rangle$ for $\tau = \alpha/\beta \in \mathcal{H}$. τ admits a minimal polynomial of degree 2 over $\mathbb{Z}$, say $AX^2 + BX + C$ with $\gcd(A, B, C) = 1$. Let $f(X, Y) = AX^2 + BXY + CY^2$, then $\tau = \tau_f$ and $\langle 1, \tau \rangle = A^{-1}\tau_f$ □

This bijection is extremely useful, as it enables us to extend results we have on forms to ideal, for example:

Corollary A.1. *Let $\mathcal{O}$ be an order in a quadratic number field. Then $Cl(\mathcal{O})$ is finite.*

Corollary A.2. *Let $\mathfrak{a}$ be an integral $\mathcal{O}$ ideal, and $k \in \mathbb{Z}$ then there is a equivalent integral ideal $\mathfrak{b}$ such that no prime dividing k divides $\mathfrak{b}$ ($\mathfrak{b}$ is coprime to k).*

The map $I : Cl(D) \to Cl(\mathcal{O})$ actually gives an isomorphism of group, but is rather long to prove (see [4] §.7).

Remark A.2. One can very efficiently obtain the form class group simply by enumerating all the possible values of A (recall $0 < A \leq \sqrt{-D/3}$) and B ($-A < B \leq A$) for which $(B^2 - D)/4A$ is an integer. For example, take $D = -31$ ($\sqrt{-D/3} = 3.21\ldots$). One easily find that the pairs (A, B) satisfying these conditions are $(1, 1)$, $(2, -1)$ and $(2, 1)$.

For completeness, one can check that an inverse map I^{-1} can be defined as follows: given $\mathfrak{a} = \langle \alpha, \beta \rangle$ then

$$I^{-1}(\mathfrak{a}) = \frac{N_{K/\mathbb{Q}}(\alpha X + \beta Y)}{N_{K/\mathbb{Q}}(\mathfrak{a})} \tag{A.14}$$

But note that $I \circ I^{-1}$ is not the identity map on ideals, but on equivalence class of ideals, I^{-1} being defined up to a change of basis for $\mathfrak{a}$.

As a conclusion to this appendix, we will show two lemmas that will be useful to determine conditions for the existence of Heegner points.

Lemma A.2. *Let $f(X,Y) = AX^2 + BXY + CY^2$ be a quadratic form, then f represents $N \in \mathbb{Z}$ properly if and only if f is equivalent to $NX^2 + B'XY + C'Y^2$.*

Proof. If f is equivalent to $NX^2 + B'XY + C'Y^2$, then for some $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$, $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot f(1,0) = f(a,c) = N$ and $\gcd(a,c) = 1$. So N is properly represented.

If N is properly represented then there exists $a, c \in \mathbb{Z}$ such that $f(a,c) = N$ and $\gcd(a,c) = 1$. Take $b, d \in \mathbb{Z}$ such that $ad - bc = 1$, then $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot f(X,Y) = NX^2 + B'XY + C'Y^2$ by equation A.2. □

Lemma A.3. *The following are equivalent:*

1− *There is $\mathfrak{n} \lhd \mathcal{O}$ such that $\mathcal{O}/\mathfrak{n} = \mathbb{Z}/N$.*

2− *There is a primitive binary quadratic form with discriminant equal to $D = Disc(\mathcal{O})$ which properly represents N.*

3− *The equation $D = B^2 - 4NC$ has a solution with* $\gcd(N, B, C) = 1$

Proof. $(3 \Rightarrow 2)$ If the solution to the equation exist the $f(X,Y) = NX^2 + BXY + CY^2$ is a form of discriminant D properly representing N.

$(2 \Rightarrow 3)$ If such a form exists find its equivalent form whose X^2 coefficient is N. Its discriminant is of the form $B^2 - 4NC$ with $\gcd(N, B, C) = 1$.

$(2 \Rightarrow 1)$ We saw that $\mathcal{O}/I(f)$ is $\mathbb{Z}/f(1,0)$, so it is sufficient to take the ideal associated to the form $NX^2 + BXY + CY^2 \in [f]$.

$(1 \Rightarrow 2)$ Let $\mathfrak{n}$ be such that $\mathcal{O}/\mathfrak{n} = \mathbb{Z}/N$, and let $A^2 + BXY + CY^2 = f(X,Y) = I^{-1}(\mathfrak{n})$. Then for some $\alpha \in K^\times$, $\mathfrak{n} = \alpha\langle 1, \tau_f \rangle$. Now

$$\begin{aligned} A\mathfrak{n} = \alpha A\langle 1, \tau_f \rangle \quad &\Rightarrow \quad A^2 N_{K/\mathbb{Q}}(\mathfrak{n}) = N_{K/\mathbb{Q}}(\alpha) A \\ &\Rightarrow \quad N_{K/\mathbb{Q}}(\mathfrak{n}) = N_{K/\mathbb{Q}}(\alpha)/A \end{aligned} \tag{A.15}$$

However, $\alpha\langle 1, \tau_f\rangle = \mathfrak{n} \subseteq \mathcal{O} = \langle 1, A\tau_f\rangle$, consequently,

$$\begin{aligned} \alpha\tau_f &= a + bA\tau_f \\ \alpha &= c + dA\tau_f \end{aligned} \Rightarrow (c + dA\tau_f)\tau_f = a + bA\tau_f \tag{A.16}$$

Using $A\tau_f^2 = -B\tau_f - C$, we get that $c = Ab + Bd$ and $Cd + a = 0$. On the other hand

$$A^{-1}N_{K/\mathbb{Q}}(\alpha) = A^{-1}(c^2 - Bcd + ACd^2) = \cdots = Ab^2 + Bab + Ca^2 = f(b, a) \tag{A.17}$$

If $f(b, a) = k > 1$, then $k \mid c$ and $k \mid d$ so

$$\mathfrak{n} = \alpha\langle 1, \tau\rangle = \langle c + dA\tau_f, a + bA\tau_f\rangle = k\mathfrak{a} \tag{A.18}$$

and $\mathcal{O}/\mathfrak{n} = \mathcal{O}/k\mathfrak{a}$ contains a subgroup of the form $(\mathbb{Z}/k\mathbb{Z})^2$, a contradiction. So $\gcd(a, b) = 1$ and f properly represents N. □

Appendix B

List of integral curves

Here are the names, referring to Cremona's table (see [5] or his website), of the elliptic curves that appear to have the integrality property. As mentioned before (see 2.5.2) the integrality of the Heegner points has been verified for the first 18 discriminants satisfying SHH and the first 12 discriminants satisfying HH but not SHH.

11A1, 14A1, 14A2, 15A1, 15A4, 17A1, 19A1, 20A1, 20A3, 21A1, 21A3, 24A1, 24A2, 24A3, 24A5, 24A6, 26A1, 26B1, 27A1, 30A1, 30A2, 32A1, 34A1, 35A1, 36A1, 36A2, 36A3, 36A4, 37A1, 38B1, 39A1, 39A2, 40A1, 40A2, 40A4, 42A1, 43A1, 44A1, 44A2, 45A1, 45A2, 48A1, 48A2, 48A3, 48A5, 48A6, 49A1, 49A2, 50A1, 50B1, 50B2, 51A1, 52A1, 53A1, 54A1, 54B1, 54B3, 55A1, 55A2, 56A1, 56A2, 56A3, 56B1, 56B2, 57A1, 58A1, 61A1, 62A1, 64A1, 64A2, 64A3, 65A1, 65A2, 66A1, 66B1, 66B2, 69A1, 69A2, 70A1, 70A2, 72A1, 72A2, 75C1, 76A1, 77A1, 79A1, 80A1, 80A3, 80A4, 80B1, 82A1, 83A1, 84A1, 84A2, 84B1, 84B2, 88A1, 89A1, 90A1, 90B1, 91A1, 92A1, 92A2, 92B1, 94A1, 94A2, 96A1, 96A2, 96A3, 96A4, 96B1, 96B2, 96B3, 96B4, 99A1, 99A2, 101A1, 102A1, 104A1, 105A1, 105A2, 108A1, 108A2, 110B1, 112A1, 112A2, 112B1, 112B2, 112B4, 112C1, 118A1, 120A1, 120A2, 120B1, 120B2, 123B1, 124A1, 124B1, 126A1, 128A1, 128A2, 128B1, 128C1, 128C2, 128D1, 130B1, 131A1, 132A1, 132A2,

135A1, 136A1, 136B1, 138A1, 140A1, 141D1, 142B1, 143A1, 144A1, 144A2, 144A3, 144A4, 144B1, 144B2, 145A1, 150A1, 152A1, 152B1, 153A1, 155C1, 156A1, 156B1, 160A1, 160A2, 160B1, 160B2, 162A1, 162B1, 162C1, 162D1, 168A1, 168A2, 176A1, 176B1, 176C1, 180A1, 180A2, 184A1, 184B1, 189A1, 190B1, 192A1, 192A2, 192A4, 192B1, 192B2, 192B4, 192C1, 192C2, 192D1, 192D2, 196A1, 200B1, 200E1, 204B1, 208B1, 208C1, 210D1, 216A1, 216B1, 220B1, 224A1, 224A2, 224B1, 224B2, 225A1, 225A2, 234C1, 236A1, 238B1, 240A1, 240A2, 240C1, 240C2, 240D1, 243A1, 243A2, 243B1, 248A1, 248C1, 256A1, 256A2, 256B1, 256B2, 256C1, 256C2, 256D1, 256D2, 264A1, 264B1, 272A1, 272C1, 280A1, 288A1, 288A2, 288D1, 288D4, 297B1, 300A1, 304C1, 304D1, 304F1, 312A1, 312B1, 312C1, 320A1, 320B1, 320C1, 320D1, 320D2, 320E1, 320E2, 320F1, 324B1, 324C1, 325B1, 336A1, 336A2, 336B1, 336B2, 336F1, 336F2, 342E1, 348A1, 348B1, 350C1, 360B1, 368C1, 368D1, 368E1, 368E2, 368F1, 378D1, 384A1, 384A2, 384B1, 384B2, 384C1, 384C2, 384D1, 384D2, 400D1, 400H1, 405C1, 405F1, 416A1, 416B1, 420D1, 425C1, 432A1, 432A3, 432B1, 432B2, 432D1, 432H1, 440B1, 459A1, 480A1, 480B1, 480C1, 480G1, 486A1, 486B1, 496A1, 496B1, 496D1, 496E1, 504A1, 504E1, 528A1, 528D1, 528E1, 528E2, 540B1, 540F1, 544A1, 544D1, 558A1, 560A1, 560F1, 567A1, 575A1, 576A1, 576A3, 576D1, 576E1, 576E3, 576F1, 576F2, 576H1, 576H2, 576I1, 600B1, 624A1, 624C1, 624D1, 624G1, 624J1, 640C1, 640G1, 648A1, 648B1, 672A1, 672G1, 675B1, 700B1, 700C1, 702B1, 704A1, 704B1, 704C1, 704G1, 704J1, 704K1, 720A1, 720I1, 768B1, 768D1, 768E1, 768F1, 768G1, 768H1, 784I1, 800B1, 800F1, 816G1, 864A1, 864D1, 880A1, 880H1, 896B1, 896C1, 944F1, 960A1, 960F1, 972A1, 972B1, 972C1, 1008B1, 1008D1, 1080A1, 1080K1, 1152B1, 1152D1, 1200F1, 1200O1, 1216A1, 1216E1, 1296B1, 1296C1, 1296G1, 1296K1, 1296L1, 1344C1, 1344F1, 1350A1, 1392L1, 1392O1, 1440B1, 1440I1, 1680O1, 1728A1, 1728A2, 1728C1, 1728H1, 1728R1, 1728V1, 1728V3, 1728AA1, 2160C1, 2160G1, 2160Q1, 2160X1, 2304B1, 2304I1, 2700L1, 2800P1, 2800W1

Bibliography

[1] A. Abbes and E. Ullmo. À propos de la conjecture de Manin pour les courbes elliptiques modulaires. *Compositio Math.*, 103(3):269–286, 1996.

[2] F. D. B. Conrad and R.Taylor. Modularity of certain potentially Barsotti-Tate Galois representations. *J. Amer. Math. Soc.*, 12(2):521–567, 1999.

[3] F. D. C. Breuil, B. Conrad and R.Taylor. On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843939, 2001.

[4] D. A. Cox. *Primes of the form $x^2 + ny^2$*. John Wiley and Sons, 1989.

[5] J. E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, 1997.

[6] H. Darmon, F. Diamond, and R. Taylor. Fermat's last theorem. *Current developpement in mathematics*, pages 1–154, 1995.

[7] F. Diamond. On deformation rings and Hecke rings. *Ann. of Math. (2)*, 144, 1996.

[8] B. Edixhoven. *Stable models of modular curves and applications*. PhD thesis, Université d'Utrecht, 1989.

[9] B. Edixhoven. On the Manin constant of modular elliptic curves. *Arithmetic algebraic geometry (Texel, 1989), Birkhauser Boston, Boston, MA*, pages 25–39, 1991.

[10] B. H. Gross. *Heegner Points on $X_0(N)$,* Modular forms (Durham, 1983). Ellis Horwood Ser. Math. Appl.: Statist. Oper. Res. Horwood, Chichester, 1984.

[11] B. H. Gross and D. B. Zagier. *Heegner points and derivatives of* L*-series*, invent. math. , 84(2):407–447, 1986.

[12] R. Hartshorne. *Algebraic Geometry*. Graduate Text in Mathematics. Springer-Verlag, 1977.

[13] T. W. Hungerford. *Algebra*. Graduate Text in Mathematics 73. Springer-Verlag, 1974.

[14] G. J. Janusz. *Algebraic Number Fields*. Graduate Studies in Mathematics. American Mathematical Society, 1996.

[15] A. W. Knapp. *Elliptic Curves*. Mathematical Notes, 40. Princeton University Press, 1992.

[16] V. Kolyvagin. Finiteness of $E(\mathbb{Q})$ and $LLI(E, \mathbb{Q})$ for a subclass of Weil curves. *Ivz. Akad. Nauk SSSR Ser. Math.*, 52(3):522-540 . 1988.

[17] V. Kolyvagin. The Mordell-Weil and Shafarevich-Tate groups for Weil elliptic curves. *Ivz. Akad. Nauk SSSR Ser. Math.*, 52(6):1154–1180, 1988.

[18] B. Mazur. Rational isogenies of prime degree. *Invent. Math.*, 44(2):129–162, 1978.

[19] T. Miyake. *Modular forms*. Springer-Verlag, 1989.

[20] P. Sarnak. *Some Applications of Modular Forms*. Cambridge Tracts in Mathematics 99. Cambridge University Press, 1990.

[21] G. Shimura. *Introduction to the arithmetic theory of automorphic functions*. Kano Memorial Lectures, No.1. Mathematical Society of Japan, No.11. Iwanami Shoten, Publishers, Tokyo; Princeton University Press, 1971.

[22] J. H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Text in Mathematics 106. Springer-Verlag, 1986.

[23] J. H. Silverman. *Advances Topics in the Arithmetic of Elliptic Curves*. Graduate Text in Mathematics 151. Springer-Verlag, 1994.

[24] R. Taylor and A. Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3):553–572, 1995.

[25] A. Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.