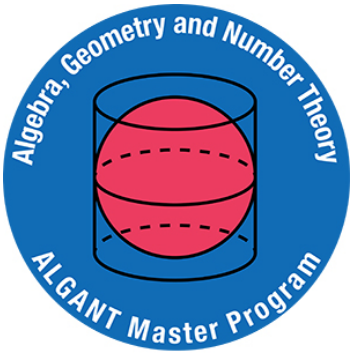

ALGANT MASTER THESIS

Primes that can be written as the sum of two cubes using mock Heegner points

Supervisor:
Dr. E. Rosu
Prof R. N. Kloosterman

Student:
S. Varljen
2053888

UNIVERSITEIT LEIDEN
UNIVERSITÀ DEGLI STUDI DI PADOVA

22nd June 2023

Acknowledgments

I would like to thank my supervisor, Eugenia Rosu, for the opportunity to work on this interesting topic and for her guidance. Her patience and thoughtfulness have been invaluable in my journey.

I also want to thank Marco Streng and Jan Vonk for the extensive feedback and their sincerity. Although I still have a lot to learn, they helped me grow significantly.

My gratitude goes out to all the people who have helped me in some way in the past months. Thanks to my mom Daniela, to my dad Fulvio, and to my sister Elena for supporting me from a thousand kilometres away. Thanks to my tutor in Leiden, Federica Pasquotto, for helping me find a light even in dark times. Thanks to all the staff and faculty in both Padova and Leiden for making my ALGANT experience possible. And last, but not least, thanks to all of my friends, old and new, who have been there for me. A special thank you goes to Virginia, who travelled all the way to the Netherlands just to spend some time together, and to Gioella, who put up with me as a roommate in the craziest building in Leiden.

Contents

Introduction

We start from a classical question: which positive integers n can be written as the sum of the cubes of two non-zero rational numbers?

$$a^3 + b^3 = n,\ a, b \in \mathbb{Q} \tag{0.0.1}$$

After writing a and b with a common denominator, $a = x/z$, $b = y/z$, the problem can be equivalently restated as follows: for which n are there nontrivial solutions to the diophantine equation

$$x^3 + y^3 = nz^3 \tag{0.0.2}$$

If $n = 1$, 0.0.2 only has solutions $(x, y, z) \in \mathbb{Z}^3$ with $xyz = 0$, as this is Fermat's Last Theorem in the case of exponent 3. If $n = 2$, there is an easy decomposition $2 = 1^3 + 1^3$. Hence, n will be assumed to be an integer greater than 2.

In 1879, Sylvester was able to prove that for many integers n, 0.0.2 has no solutions., and furthermore:

Theorem 0.0.3. *(Pépin, Lucas, Sylvester) [19, Section 2, Title 1] If p is an odd prime congruent to 2 or 5 modulo 9, then neither p nor p^2 can be decomposed as the sum of two cubes.*

Further developments on the problem were reached through a more modern approach, which starts by restating the question in the language of elliptic curves. The cubic projective equation $E_n : x^3 + y^3 = nz^3$ defines an elliptic curve over $\mathbb{Q}$ equipped with the base point $(1 : -1 : 0)$. Therefore, n can be written as the sum of two rational cubes if and only if the group of rational points $E_n(\mathbb{Q})$ is not trivial. By Mordell-Weil theorem, $E_n(\mathbb{Q})$ is a finitely generated abelian group, and thus it is of the form $E_n(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r$, for $r \in \mathbb{Z}_{\geq 0}$ the rank of the elliptic curve E_n. Under the assumption that $n \geq 3$ is a cubefree integer, E_n has only one rational torsion point, that at infinity (see [16]). Thus, 0.0.2 admits a solution if and only if the rank of E_n is positive.

Using a descent argument, Selmer [14, 9.15.16] showed that if $n = p$ or p^2 for a prime $p > 3$, then

$$\text{rk}(E_n(\mathbb{Q})) \leq \begin{cases} 0 & \text{if } p \equiv 2, 5 \pmod 9 \\ 1 & \text{if } p \equiv 4, 7, 8 \pmod 9 \\ 2 & \text{if } p \equiv 1 \pmod 9 \end{cases} \tag{0.0.4}$$

The case $p \equiv 2, 5 \pmod 9$ confirms the previous result published by Sylvester.

The case $p \equiv 4, 7, 8 \pmod 9$ is related to the following conjecture attributed to Sylvester:

Conjecture. *If $p \equiv 4, 7, 8 \pmod 9$, then p is the sum of two rational cubes.*

This conjecture has not been proven in general, but Dasgupta and Voight in 2018 published the following result, providing progress towards a full proof.

Theorem 0.0.5. *[7] If p is a prime congruent to 4 or 7 modulo 9 and 3 is not a cube modulo p, then $\operatorname{rk} E_p(\mathbb{Q}) = \operatorname{rk} E_{p^2}(\mathbb{Q}) = 1$.*

To prove the theorem, by 0.0.4, it is sufficient to find a rational nontorsion point on E_p and E_{p^2}. Constructing the point on $E_p(\mathbb{Q})$ and $E_{p^2}(\mathbb{Q})$ and checking that it is nontorsion are the two main steps of this proof.

In this thesis, we are going to follow the paper by Dasgupta and Voight [7], providing corrections to [7, Proposition 4.4.2] and [7, Lemma 5.2.4].

In order to construct a rational point on the elliptic curve E_p, one could use the method of Heegner points [5, Chapter 3]. Such method starts from a modular parametrization $\Phi : X_0(N) \to E_p$, where N denotes the conductor of the elliptic curve E_p. We have that $N = 27p^2$ if $p \equiv 4 \pmod 9$ and $N = 9p^2$ if $p \equiv 7 \pmod 9$. Next, one picks an imaginary quadratic field $K = \mathbb{Q}(\sqrt{D})$ of discriminant D satisfying the "Heegner hypothesis". This assumption requires that the divisors of N, namely 3 and p, split in K. Denoting by $\mathcal{O}_K$ the ring of integers of K, the Heegner hypothesis guarantees that there is an ideal $\mathcal{N} \subseteq \mathcal{O}_K$ such that $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$. This makes it possible to consider the N-isogeny $\mathbb{C}/\mathcal{O}_K \to \mathbb{C}/\mathcal{N}^{-1}$, which defines a point $P \in X_0(N)(H)$, for H the Hilbert class field of K. A Heegner point is then obtained by taking the trace $X = \operatorname{Tr}_{H/K} \Phi(P) \in E_p(K)$. Up to adding a torsion point, one has that $X \in E_p(\mathbb{Q})$.

However, for this method, we first need to choose an imaginary quadratic field K satisfying the Heegner hypothesis. There is, in general, no natural choice for K that satisfies the requirement for 3 and p to split. Furthermore, there does not seem to be a direct and unconditional way to show that the Heegner point on $E_p(\mathbb{Q})$ is nontorsion.

For these reasons, in the proof by Dasgupta and Voight that we are following, the construction is different, and it is based on so-called mock Heegner points. The term "mock Heegner points" is due to Monsky [12]. This method uses the imaginary quadratic field $K := \mathbb{Q}(\omega)$, for ω the primitive cubic root of unity with positive imaginary part. The field K is naturally associated to the elliptic curve E_n for every n, because E_n has complex multiplication by the ring of integers $\mathcal{O}_K$ of K. In addition to K, we need the following chain of field extensions

$$\mathbb{Q} \subset K \subset K(\sqrt[3]{p}) \subset H_{3p} \subset H_{9p} = H_{3p}(\sqrt[3]{3}),$$

where H_f denotes the ring class field of K of conductor f.

The construction starts from a fixed modular parametrization $\Phi : X_0(243) \to E_9$ of the elliptic curve E_9 of conductor 243. Using the correspondence between cyclic 243-isogenies and the points on the affine curve $Y_0(243)$, it is possible to find a point $P_0 \in X_0(243)(H_{9p})$. The point P_0 is different, depending on whether we want to produce

a point on $E_p(\mathbb{Q})$ or $E_{p^2}(\mathbb{Q})$. In this thesis, the initial point P_0 for the construction relative to $E_{p^2}(\mathbb{Q})$ is not the same as the one used in the proofs by Dasgupta and Voight, but we will show that it is a suitable choice nevertheless.

It would be possible to go from the point $P = \Phi(P_0) \in E_9(H_{9p})$ to a point on $E_p(\mathbb{Q})$ or $E_{p^2}(\mathbb{Q})$ simply by taking the trace over the field extension H_{9p}/K. Although this would yield a rational point, the argument used by Dasgupta and Voight to prove that the point on $E_{p^i}(\mathbb{Q})$ is nontorsion would not work. Thus it would not be possible to conclude that p and p^2 can be written as the sum of two rational cubes.

Instead, we take several intermediate steps, as in Figure 1, using as our main tools twisting isomorphisms and taking the trace of a point. First, we go from $P \in E_9(H_{9p})$ to $Q \in E_1(H_{3p})$, via a twist by $\sqrt[3]{3}$. For this argument, it will be important to compare the action of $\mathrm{Gal}(H_{9p}/H_{3p})$ on $X_0(243)$ to the automorphisms of $X_0(243)$. In particular, identifying the Galois actions on points will be done using Shimura's reciprocity law. The second step, from $E_1(H_{3p})$ to $E_1(K(\sqrt[3]{3})$, consists of taking the trace $R = \mathrm{Tr}_{H_{3p}/K(\sqrt[3]{3})} Q \in E_1(K(\sqrt[3]{3})$. After adding to R a torsion point of $E_1(K(\sqrt[3]{p}))$, a twist by $\sqrt[3]{p^i}$ will yield a point Z on $E_{p^i}(K)$, for $i \in \{1, 2\}$. Finally, taking the trace of Z over $K/\mathbb{Q}$ produces a point on $E_{p^i}(\mathbb{Q})$.

Notice that the construction of the rational point does not use the hypothesis that 3 is not a cube modulo p.

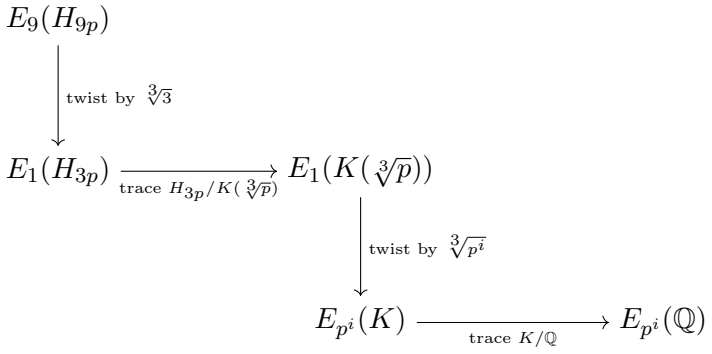

Figure 1: Diagram of the main steps from $E_9(H_{9p})$ to $E_{p^i}(\mathbb{Q})$, for $i \in \{1, 2\}$

In order to prove that the point we have constructed is indeed nontorsion, we use [7, Proposition 5.2.1] to see what the reduction of the point $R \in E_1(K(\sqrt[3]{p}))$ modulo p looks like. This does not match the image of the reduction modulo p of any torsion point of $E_1(K(\sqrt[3]{p}))$, and therefore R is non torsion. Here, the additional hypothesis on 3 not being a cube modulo p becomes crucial. Without it, reducing R modulo p we might find the same image as that of a torsion point, and thus we have no guarantees that the point we constructed is nontorsion.

Once we know that $R \in E_1(K(\sqrt[3]{p}))$ is nontorsion, we are also able to prove that $Z \in E_{p^i}(K)$ is nontorsion, and from there we are able to produce a nontorsion point on $E_{p^i}(\mathbb{Q})$, and conclude the proof of Theorem 0.0.5.

Chapter 0

Preliminaries

0.1 Elliptic curves

This section is dedicated to introducing a few tools for working with elliptic curves. They are going to be used in Chapter 2, when constructing rational points on E_p and E_{p^2}, which are themselves elliptic curves. The main reference for this section is [16, Chapter VIII, Chapter X].

Recall that an elliptic curve E is a smooth, projective, algebraic, irreducible curve of genus one, together with a base point O on it. We say that an elliptic curve E is defined over a field K, and write E/K, if E is defined over K as a curve and O is a K-rational point.

In Chapters 1 and 2, we are mostly going to work with elliptic curves defined over a number field K. In such situation, the following theorem describes the structure of the group of K-rational points of E.

Theorem 0.1.1. *(Mordell-Weil) Let K be a number field and E/K an elliptic curve. Then the group $E(K)$ is finitely generated and we may write $E(K) \cong E(K)_{tors} \times \mathbb{Z}^r$ for some integer $r \geq 0$.*

Definition 0.1.2. In the notation of the Mordell-Weil theorem, we define the *rank* of the elliptic curve E/K as the integer $r \geq 0$ such that $E(K) \cong E(K)_{\text{tors}} \times \mathbb{Z}^r$.

The following three subsections provide basic information about different aspects of elliptic curves that will be used in Chapters 1 and 2.

Twisting

This subsection refers to [16, Section X.5].

We start with defining the group of isomorphisms of an elliptic curve E.

Definition 0.1.3. Let E/K be an elliptic curve over a number field K. The *isomorphism group* of E, which we denote by $\text{Aut}_{\text{curve}}(E)$, is the group of $\overline{K}$-isomorphisms from E to E itself. We do not require the isomorphisms to be of elliptic curves, only of smooth

curves of genus one. We denote the group of isomorphisms of E defined over K by $\mathrm{Aut}_{\mathrm{curve},K}(E)$.

Remark. For an elliptic curve E, we are using the term isomorphism group, as in [16, X.2.1], because the automorphism group $\mathrm{Aut}(E)$ usually refers to invertible isogenies of E.

We now introduce the concept of twist of an elliptic curve. This will be used in Propositions 2.3.1 and 2.4.1 in a more specific way, but the main idea is the same as that behind the following definition.

Definition 0.1.4. Let E/K be an elliptic curve defined over a number field. A *twist* of E/K is another elliptic curve curve E'/K isomorphic to E over $\overline{K}$.

Two twists are said to be equivalent if they are isomorphic over K.

The set of twists of E/K modulo K-isomorphism is denoted by $\mathrm{Twist}(E/K)$.

Example 0.1.5. Let K be a number field and $d \in K$ squarefree. Let E/K be the elliptic curve defined by the equation $E : y^2 = x^3 + Ax + B$. Then, the quadratic twist of E by d is given by the isomorphism

$$\begin{array}{ccc} E : y^2 = x^3 + Ax + B & \cong & E_d : y^2 = x^3 + Ad^2x + Bd^3 \\ (x, y) & \mapsto & \left(\frac{x}{d}, \frac{y}{d\sqrt{d}}\right) \end{array}$$

Example 0.1.6. Let K be a number field and $d \in K$ cubefree. Let E/K be the elliptic curve defined by the equation $E : y^2 = x^3 + B$. Then, the cubic twist of E by d is given by the isomorphism

$$\begin{array}{ccc} E : y^2 = x^3 + B & \cong & E_d : y^2 = x^3 + Bd^2 \\ (x, y) & \mapsto & \left(\frac{x}{\sqrt[3]{d^2}}, \frac{y}{d}\right) \end{array}$$

Trace

In Sections 2.3 and 2.4, we will be working with Galois extensions of number fields L/K. Given an elliptic curve E defined over $\mathbb{Q}$, we would like a way to compute a point of $E(K)$ given a point of $E(L)$. The following definition and proposition give us such a tool.

Definition 0.1.7. Let K be a perfect field and L/K a finite Galois extension. Let E/K be an elliptic curve. Then we can define a *trace* map $\mathrm{Tr}_{L/K} : E(L) \to E(K)$ given by $P \mapsto \mathrm{Tr}_{L/K}(P) = \sum_{\sigma \in G(L/K)} P^\sigma$.

Proposition 0.1.8. *With notation as in the above definition,* $\mathrm{Tr}_{L/K} : E(L) \to E(K)$ *is a well-defined homomorphism.*

Proof. We will denote by G the Galois group $\mathrm{Gal}(L/K)$.

First of all, note that $\mathrm{Tr}_{L/K}(E(L)) \subseteq E(K)$. Indeed, if $P \in E(L)$ and $\tau \in G$, then $\mathrm{Tr}_{L/K}(P)^\tau = \left(\sum_{\sigma \in G} P^\sigma\right)^\tau = \sum_{\sigma \in G} P^{\sigma\tau} = \sum_{\rho = \sigma\tau \in G} P^\rho = \mathrm{Tr}_{L/K}(P)$.

Moreover, the group law of the elliptic curve E is preserved. Let $P, Q \in E(L)$, then we have that $\mathrm{Tr}_{L/K}(P+Q) = \sum_{\sigma \in G} (P+Q)^\sigma = \sum_{\sigma \in G} P^\sigma + Q^\sigma = \mathrm{Tr}_{L/K}(P) + \mathrm{Tr}_{L/K}(Q)$.

Hence, $\mathrm{Tr}_{L/K}$ is a group homomorphism. □

Complex Multiplication

Let K be a number field and E an elliptic curve over K. Since $\mathrm{char}(K) = 0$, [16, Cor III.9.4] states that the endomorphism ring of E, $\mathrm{End}(E)$, is isomorphic to either the ring of integers $\mathbb{Z}$ or an order in an imaginary quadratic field . Recall that an order $\mathcal{O}$ in a finitely-generated $\mathbb{Q}$-algebra k is a subring $\mathcal{O}$ of k such that $\mathcal{O} \otimes \mathbb{Q} = k$ and $\mathcal{O}$ is finitely generated as a $\mathbb{Z}$-module.

Definition 0.1.9. Let K be a number field and E/K an elliptic curve. We say E is an elliptic curve with *complex multiplication* if $\mathbb{Z}$ is strictly contained in $\mathrm{End}(E)$.

Equivalently, if $\mathrm{End}(E) = \mathcal{O}$ is an order in an imaginary quadratic field $\mathbb{Q}(\sqrt{D})$, we say that E has complex multiplication by $\mathcal{O}$.

The elliptic curves we are going to be considering from Section 1.1 all have complex multiplication.

0.2 Modular curves and modular functions

In this section, we would first like to give a brief introduction to modular curves, since we are going to use one of them, namely $X_0(243)$, as the basis for the construction of rational points on E_p and E_{p^2}. In the second subsection, we will the essential definition we are going to need regarding modular functions, and then give a criterion to recognize modular functions of a certain form, which will be used in Chapter 3.

Modular curves

The main reference for this subsection, which introduces modular curves, is [16, C.13]

We denote $\mathcal{H} = \{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\}$. We also define, for every non-zero integer N, the following subgroup of $\mathrm{SL}_2(\mathbb{Z})$:

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : b \equiv c \equiv 0 \bmod N, a \equiv d \equiv 1 \bmod N \right\}.$$

We call Γ a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$, that is a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ containing $\Gamma(N)$ for some integer N.

The group Γ acts on $\mathcal{H}$ as follows: given $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, γ induces a map $\gamma : \mathcal{H} \to \mathcal{H}$ defined by $\tau \mapsto \gamma(\tau) = \frac{a\tau+b}{c\tau+d}$.

Furthermore, we can set $\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$, and define the action of Γ on $\mathbb{P}^1(Q)$ as follows. For any $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, there is a map $\gamma : \mathbb{P}^1(\mathbb{Q}) \to \mathbb{P}^1(\mathbb{Q})$ given by $[x, y] \mapsto \gamma([x, y]) = [ax + by, cx + dy]$.

The quotient space $\Gamma \setminus \mathcal{H}^*$ is well-defined and has the structure of a Riemann surface.

Theorem 0.2.1. *With notation as above, there exists a smooth projective curve $X(\Gamma)$ over a number field K depending on Γ and a complex analytic isomorphism $j_\Gamma : \Gamma \setminus \mathcal{H}^* \to X(\Gamma)(\mathbb{C})$.*

The curve $X(\Gamma)$ is called a *modular curve*. The set of *cusps* of $X(\Gamma)$ is the finite set of points $j_\Gamma(\Gamma \setminus \mathbb{P}^1(\mathbb{Q}))$. The complement of the set of cusps of $X(\Gamma)$ is a smooth affine curve denoted by $Y(\Gamma)$.

We will now focus on the following subgroups of $\mathrm{SL}_2(\mathbb{Z})$, for any non-zero integer N:

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \bmod N \right\}.$$

Notice that $\Gamma_0(N)$ is a congruence subgroup, as it contains $\Gamma(N)$.

The modular curve obtained from $\Gamma_0(N)$ is denoted by $X_0(N)$. It is a projective curve defined over $\mathbb{Q}$, which means that the ideal $\{f \in \overline{\mathbb{Q}}[X] : f \text{ homogeneous and } f(P) = 0 \ \forall P \in X_0(N)\}$ can be generated by homogeneous polynomials in $\mathbb{Q}[X]$. The affine curve obtained from $X_0(N)$ by removing the cusps is denoted by $Y_0(N)$.

The following theorem relates elliptic curves defined over the $\mathbb{Q}$ to modular curves.

Theorem 0.2.2. *(Modularity theorem, Wiles et al.) Let $E/\mathbb{Q}$ be an elliptic curve. Then, there exist an integer N and a surjective morphism $\phi : X_0(N) \to E$ defined over $\mathbb{Q}$.*

We call such a surjective morphism a modular parametrization for the elliptic curve E.

Remark. The integer N in the statement of the Theorem 0.2.2 may be taken to be the conductor of $E/\mathbb{Q}$.

Modular functions and modular forms

We start this subsection by defining a function that will be used in the definition of the modular parametrization of the elliptic curve E_9 in Proposition 1.2.7, and then later in Chapter 3 in the proof that the points constructed on $E_p(\mathbb{Q})$ and $E_{p^2}(\mathbb{Q})$ are nontorsion.

Definition 0.2.3. The *Dedekind η-function* is the modular form of weight $1/2$ defined as the infinite product $\eta(z) := q^{1/24} \prod_{n=1}^{\infty}(1-q^n)$, for $q := e^{2\pi i z}$.

The infinite product defining the Dedekind η-function converges absolutely for $z \in \mathcal{H}$. We can see this because in that case $|q| = |e^{2\pi i z}| < 1$ and, as $|\log(|1-q^n|)| = O(|q|^n)$, $\sum_{n\geq 1} |\log(|1-q^n|)| < \infty$. It follows that η is holomorphic on the upper half plane and that $\eta(z) \neq 0$ for every $z \in \mathcal{H}$.

Proposition 0.2.4. *The Dedekind η-function satisfies the following functional equations:*

$$\eta(\tau+1) = e^{\pi i/12}\eta(\tau)$$
$$\eta\left(-\frac{1}{\tau}\right) = \sqrt{-i\tau}\,\eta(\tau)$$

In the second equation, the branch of the square root is chosen such that $\sqrt{-i\tau} = 1$ if $\tau = i$.

We are now going to define a class of complex-valued functions related to the modular curves $X_0(N)$ we defined in the previous subsection.

Definition 0.2.5. Let $\Gamma_0(N)$ be a congruence subgroup. A *modular function* f is a complex-valued function $f : \mathcal{H} \to \mathbb{C}$ such that

- f is meromorphic on $\mathcal{H}$,
- f is $\Gamma_0(N)$-invariant, meaning $f(\gamma z) = f(z)$ for all $\gamma \in \Gamma_0(N)$ and $z \in \mathcal{H}$,
- f is meromorphic at cusps.

The last condition can be restated by requiring that for every $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, the q-expansion $f(\gamma z) = \sum_{n=-\infty}^{\infty} a_n q^{n/N}$ is such that $a_n = 0$ for all but finitely many $n < 0$.

The following proposition will give us a criterion to check whether complex functions of a certain form, namely given as a product or quotient of Dedekind η-functions, are modular functions for some $\Gamma_0(N)$. This criterion will be used in Section 3.1, to work out an alternative way of writing a modular parametrization for the elliptic curve E_9.

Proposition 0.2.6. *[10, Proposition 3.2.1] Consider a meromorphic function on $\mathcal{H}$ of the form $f(z) = \prod_{0<\delta|N} \eta(\delta z)^{r_\delta}$ and assume it satisfies*

- $\sum_{0<\delta|N} \delta r_\delta \equiv 0 \pmod{24}$,
- $\sum_{0<\delta|N} \frac{N}{\delta} r_\delta \equiv 0 \pmod{24}$,
- $\sum_{0<\delta|N} r_\delta = 0$,
- $\prod_{0<\delta|N} \delta^{r_\delta} \in \mathbb{Q}^2$

Then f is a modular function for $\Gamma_0(N)$.

0.3 Class field theory

In this section, we give a brief introduction to the language of class field theory. In the first subsection, we will treat it in terms of ideals, while in the second subsection we will introduce it in terms of idèles. The last subsection is dedicated to the statement of Shimura's reciprocity law, which will be used several times in Chapter 2.

The references used for this section are [11], [17] and [4]. For the subsection on Shimura's reciprocity law, the resources we refer to are [9] and [18].

Class field theory with ideals

The main idea behind class field theory in the case of number fields is to describe abelian Galois extension of a number field K using information about K itself.

We start by introducing objects that encode data about the finite and real places of a number field.

Definition 0.3.1. A *modulus* $\mathfrak{m}$ of a number field K is a formal product over all primes $\mathfrak{p}$ of K, $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n(\mathfrak{p})}$, such that $n(\mathfrak{p})$ is a non negative integer for all primes $\mathfrak{p}$ satisfying

$n(\mathfrak{p}) = 0$ for all but finitely many primes $\mathfrak{p}$, $n(\mathfrak{p}) \in \{0, 1\}$ for any real prime $\mathfrak{p}$, and $n(\mathfrak{p}) = 0$ for any complex prime $\mathfrak{p}$.

A modulus $\mathfrak{m}_1 = \prod_{\mathfrak{p}} \mathfrak{p}^{n_1(\mathfrak{p})}$ is said to *divide* a modulus $\mathfrak{m}_2 = \prod_{\mathfrak{p}} \mathfrak{p}^{n_2(\mathfrak{p})}$ if $n_1(\mathfrak{p}) \leq n_2(\mathfrak{p})$ for all primes $\mathfrak{p}$.

We can write a modulus $\mathfrak{m}$ as a formal product $\mathfrak{m}_0\mathfrak{m}_\infty$, where $\mathfrak{m}_0$ denotes a product over finite primes, while $\mathfrak{m}_\infty$ denotes a product over infinite real primes. Notice that since $\mathfrak{m}_0$ corresponds to a product of finitely many positive powers of finite prime ideals of K, $\mathfrak{m}_0$ can be identified with an ideal of the ring of integers $\mathcal{O}_K$.

Remark. In the case of an imaginary quadratic number field, since there are no real primes, the notion of modulus is equivalent to that of integral ideal.

Let $\mathfrak{p}$ be a prime of a number field K and n a non-negative integer. For any element $x \in K^*$ we write that $x \equiv 1 \bmod^* \mathfrak{p}^n$ if one of the following holds

- $n = 0$;
- $\mathfrak{p}$ is real, $n = 1$, and x is positive at $\mathfrak{p} : K^* \to \mathbb{R}^*$;
- $\mathfrak{p}$ is finite, $n > 0$, and $x \in 1 + \mathfrak{p}^n$.

For a modulus $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n(\mathfrak{p})}$ of K and an element $x \in K^*$, we write $x \equiv 1 \bmod^* \mathfrak{m}$ if and only if $x \equiv 1 \bmod^* \mathfrak{p}^{n(\mathfrak{p})}$ for all primes $\mathfrak{p}$ of K.

With this notation, we are ready to define what a ray class group is. The definition bears some resemblance to that of ideal class group.

Definition 0.3.2. Let $\mathfrak{m}$ be a modulus of a number field K. Denote by $I_K(\mathfrak{m})$ the group of fractional ideals of K that are coprime to $\mathfrak{m}_0$. Denote by $P_{K,1}(\mathfrak{m})$ the group of principal ideals $x\mathcal{O}_K$ such that $x \equiv 1 \bmod^* \mathfrak{m}$. We define the *ray class group modulo* $\mathfrak{m}$ as the quotient $C_\mathfrak{m} = I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m})$.

A *congruence subgroup modulo* $\mathfrak{m}$ is a group H such that $P_{K,1}(\mathfrak{m}) \subseteq H \subseteq I_K(\mathfrak{m})$. For any such H, the quotient $I_K(\mathfrak{m})/H$ is said to be a *generalized ideal class group.*

Remark 0.3.3. [17] Let $\mathfrak{m}$ and $\mathfrak{m}'$ be moduli of a number field K. Let H be a congruence subgroup modulo $\mathfrak{m}$ and H' a congruence subgroup modulo $\mathfrak{m}'$. Then, H and H' are said to be equivalent if, for every common multiple $\mathfrak{n}$ of $\mathfrak{m}$ and $\mathfrak{m}'$, the inverse images of H and H' under the natural maps $I_K(\mathfrak{n}) \to I_K(\mathfrak{m})$ and $I_K(\mathfrak{n}) \to I_K(\mathfrak{m}')$ coincide. If this is the case, the corresponding generalized ideal class groups $I_K(\mathfrak{m})/H$ and $I_K(\mathfrak{m}')/H'$ are isomorphic.

Definition 0.3.4. Let L/K be an abelian extension of number fields, meaning L/K is Galois and $\mathrm{Gal}(L/K)$ is abelian. If $\mathfrak{p}$ is a prime of K that is unramified over L, there is a unique Frobenius automorphism, also called *Artin symbol*, $\sigma = (\mathfrak{p}, L/K) \in \mathrm{Gal}(L/K)$ satisfying $\sigma(x) \equiv x^{N_{K/\mathbb{Q}}\mathfrak{p}} \mod \mathfrak{P}$ for every $x \in \mathcal{O}_L$ and $\sigma(\mathfrak{P}) = \mathfrak{P}$ for every prime ideal $\mathfrak{P}$ of L lying over $\mathfrak{p}$.

If $\mathfrak{m}$ is a modulus divisible by all the primes of K that ramify in L, we can define a homomorphism called *Artin map*:

$$\psi_{L/K} : I_K(\mathfrak{m}) \to \mathrm{Gal}(L/K), \qquad \prod_{i=1}^{t} \mathfrak{p}_i^{n_i} \mapsto \prod_{i=1}^{t} (\mathfrak{p}_i, L/K)^{n_i}.$$

Theorem 0.3.5. *(Artin's reciprocity law) Let L/K be a finite abelian extension of number fields. There exists a modulus $\mathfrak{m}$ divisible by all the primes of K ramifying in L such that $\psi_{L/K}(P(\mathfrak{m})) = 0$ and the Artin map $\psi_{L/K}$ induces an isomorphism*

$$I_K(\mathfrak{m})/(P(\mathfrak{m}) \cdot \mathrm{Nm}_{L/K}(I_L(\mathfrak{m}))) \xrightarrow{\sim} \mathrm{Gal}(L/K)$$

The statement of Artin's reciprocity allows us to define the conductor of an abelian extension of number fields. As we will see in Theorem 0.3.7, the conductor contains information about the ramification in an abelian extension.

Definition 0.3.6. A *defining modulus* for an abelian extension of number fields L/K is a modulus that satisfies the statement of Theorem 0.3.5.

The highest common factor of all the defining moduli for L/K is called the *conductor* of the extension L/K and is denoted by $\mathfrak{f}(L/K)$.

Theorem 0.3.7. *[17] Let L/K be a finite abelian extension of number fields with conductor $\mathfrak{f}$. For every prime $\mathfrak{p}$ of K it holds*

- $\mathfrak{p} \mid \mathfrak{f}$ *if and only if* $\mathfrak{p}$ *is ramified in* L/K*;*
- $\mathfrak{p}^2 \mid \mathfrak{f}$ *if and only if* $\mathfrak{p}$ *is wildly ramified in* L/K*.*

The following is a result from [3] that gives explicitly the conductor of certain cubic extensions of the number field $\mathbb{Q}(\sqrt{-3})$. We report it here, because it will be used in Section 1.3.

Theorem 0.3.8. *[3, 8.2.14] Let $K = \mathbb{Q}(\sqrt{-3})$ and let $L = K(\sqrt[3]{a^2 b})$ for a, b coprime. The field extension L/K is abelian of conductor $\mathfrak{f}$, where $\mathfrak{f} = 3ab$ if $a^2 \not\equiv b^2 \pmod 9$ and $\mathfrak{f} = ab$ if $a^2 \equiv b^2 \pmod 9$.*

The following is the main theorem of class field theory. It shows the connection between finite abelian extensions of a number field and its generalized ideal class groups.

Theorem 0.3.9. *(Existence theorem) Let K be a number field. There is an inclusion-reversing bijection between the set of finite abelian extensions of K inside a fixed algebraic closure and the set of generalized ideal class groups of K, up to the equivalence described in Remark 0.3.3.*

More precisely, for every congruence subgroup H modulo $\mathfrak{m}$, there exists a finite abelian extension L/K unramified at primes not dividing $\mathfrak{m}$, such that $H = P(\mathfrak{m}) \cdot \mathrm{Nm}_{L/K}(I_L(\mathfrak{m}))$. The Artin map then induces an isomorphism between the generalized ideal class group corresponding to H and the Galois group of L/K.

The existence theorem allows us to define for each modulus $\mathfrak{m}$ of a number field K a finite abelian field extension of K associated to the ray class group $C_{\mathfrak{m}}$.

Definition 0.3.10. Let $\mathfrak{m}$ be a modulus of a number field K. The field $L_{\mathfrak{m}}$ associated by Theorem 0.3.9 to the ray class group $C_{\mathfrak{m}}$ is called *ray class field modulo* $\mathfrak{m}$, and there is an isomorphism $C_{\mathfrak{m}} \cong \mathrm{Gal}(L_{\mathfrak{m}}/K)$ induced by the Artin map.

If $\mathfrak{m} = 1$, then the corresponding ray class field is called *Hilbert class field.*

Remark. The Hilbert class field H of a number field K is the maximal unramified abelian extension of K.

In the rest of this section, we are going to introduce ray class groups and ray class fields, together with some of their properties. Ray class fields will be used in Section 1.3 and in Chapter 2 as field extensions of $\mathbb{Q}$ through which we will pass when constructing rational points on E_p and E_{p^2}.

Let $\mathcal{O}$ be an order inside a quadratic number field K. Since both $\mathcal{O}$ and $\mathcal{O}_K$ are free $\mathbb{Z}$-modules of rank 2, the index $f = [\mathcal{O}_K : \mathcal{O}]$ is finite. The positive integer f is called the *conductor* of $\mathcal{O}$. Actually, by [4, Lemma 7.2], we have that $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$. To an order $\mathcal{O}$ of conductor f we can associate a generalized ideal class group modulo f.

Definition 0.3.11. Let $\mathcal{O}$ be the order of conductor f in a quadratic number field K. Denote the subgroup of $I_K(f)$ isomorphic to the group of principal ideals of $\mathcal{O}$ prime to f by $P_{K,\mathbb{Z}}(f) := \{(\alpha) \subseteq \mathcal{O}_K | \exists\, a \in \mathbb{Z} : \alpha \equiv a \pmod{f\mathcal{O}_K}, (a, f) = 1\}$.

The *ring class group* of $\mathcal{O}$ is defined as the quotient $C(\mathcal{O}) := I_K(f)/P_{K,\mathbb{Z}}(f)$.

The *ring class field* associated to $\mathcal{O}$ is the abelian extension of K associated to the ring class group of $\mathcal{O}$ by the existence theorem.

We conclude this subsection with some further results about ring class fields. These will be used in Section 1.3.

Proposition 0.3.12. *Let $\mathcal{O}_1$ and $\mathcal{O}_2$ be orders inside the imaginary quadratic number field K of conductor f_1 and f_2, respectively. If f_1 divides f_2, then the ring class field associated to $\mathcal{O}_2$ contains the ring class field associated to $\mathcal{O}_1$.*

Proof. Let $\mathcal{O}_K$ denote the ring of integers of the imaginary quadratic number field K.

Recall that, by [4, Lemma 7.2], if $\mathcal{O}$ is an order in K of conductor f, then $\mathcal{O} = \mathbb{Z} + f$.

If f_1 divides f_2, we can write $f_2 = df_1$, for some positive integer d. Let x be an element of $\mathcal{O}_2$. Then we can write $x = n + f_2 w$ for some $n \in \mathbb{Z}$ and some $w \in \mathcal{O}_K$. Notice that $z = dw$ lies in $\mathcal{O}_K$ as well. Thus, we have $x = n + f_1 z \in \mathcal{O}_1$. This proves that $\mathcal{O}_2 \subseteq \mathcal{O}_1$, if f_1 divides f_2.

Now, by 0.3.9, it suffices to show that if $\mathcal{O}_2 \subseteq \mathcal{O}_1$, then $C(\mathcal{O}_2) \subseteq C(\mathcal{O}_1)$. If $f_1 \mid f_2$, then we have $I_K(f_2) \subseteq I_K(f_1)$ and $P_{K,\mathbb{Z}}(f_2) \subseteq P_{K,\mathbb{Z}}(f_1)$. But then we have $I_K(f_2)/P_{K,\mathbb{Z}}(f_2) \subseteq I_K(f_1)/P_{K,\mathbb{Z}}(f_1)$. □

Theorem 0.3.13. *[4, Theorem 7.24] Let $\mathcal{O}$ be the order of conductor f in an imaginary quadratic number field K. Then the order of the ring class group of $\mathcal{O}$ is*

$$h(\mathcal{O}) = \frac{h(\mathcal{O}_K) f}{[\mathcal{O}_K^* : \mathcal{O}^*]} \prod_{p \mid f} \left(1 - \left(\frac{d_K}{p}\right) \frac{1}{p}\right)$$

where d_K is the discriminant of the number field K, $h(\mathcal{O}_K)$ is the class number of K.

Proposition 0.3.14. *[4] For an order of conductor f in an imaginary quadratic number field K there are long exact sequences*

$$0 \longrightarrow I_K(f) \cap P_K / P_{K,\mathbb{Z}}(f) \longrightarrow I_K(f)/P_{K,\mathbb{Z}}(f) \longrightarrow I_K/P_K$$

$$1 \longrightarrow \{\pm 1\} \xrightarrow{\iota} (\mathbb{Z}/f\mathbb{Z})^* \times \mathcal{O}_K^* \xrightarrow{\psi} (\mathcal{O}_K/f\mathcal{O}_K)^* \xrightarrow{\phi} I_K(f) \cap P_K/P_{K,\mathbb{Z}}(f) \longrightarrow 1$$

Where $\{\pm 1\} \hookrightarrow (\mathbb{Z}/f\mathbb{Z})^* \times \mathcal{O}_K^*$ *is defined by* $j \mapsto (j, j)$*, and* $(\mathbb{Z}/f\mathbb{Z})^* \times \mathcal{O}_K^* \to (\mathcal{O}_K/f\mathcal{O}_K)^*$ *is defined by* $(n + f\mathbb{Z}, z) \mapsto nz \mod f\mathcal{O}_K$.

Proof. The first exact sequence follows immediately from the inclusions $I_K(f) \subseteq I_K$ and $P_{K,\mathbb{Z}}(f) \subseteq I_K(f) \cap P_K$.

As for the second sequence, it is clear that ι is an injection. The map ϕ sends the coset $\alpha + f\mathcal{O}_K$ to the principal $\mathcal{O}_K$-ideal generated by α, modulo $P_{K,\mathbb{Z}}(f)$. As $\alpha + f\mathcal{O}_K \in (\mathcal{O}_K/f\mathcal{O}_K)^*$ if and only if $\alpha \in \mathcal{O}_K$ is coprime with f, it follows that ϕ is surjective.

Let $(n + f\mathbb{Z}, w) \in (\mathbb{Z}/f\mathbb{Z})^* \times \mathcal{O}_K^*$. We have that the $\mathcal{O}_K$-ideal generated by nw can also be generated by $n = nww^{-1}$. Using the fact that the integer n is coprime to the integer f, we have $nw\mathcal{O}_K \in P_{K,\mathbb{Z}}(f)$. It follows that $\operatorname{Im}\psi \subseteq \ker\phi$. Now, let the class of $(\mathcal{O}_K/f\mathcal{O}_K)^*$ represented by $\alpha \in \mathcal{O}_K$ lie in the kernel of ϕ. It follows $\alpha\mathcal{O}_K \in P_{K,\mathbb{Z}}(f)$, so that we can write $\alpha\mathcal{O}_K = \beta\mathcal{O}_k\gamma^{-1}\mathcal{O}_K$, with $\beta \equiv b \pmod{f\mathcal{O}_K}$ and $\gamma \equiv c \pmod{f\mathcal{O}_K}$ for some integers b and c coprime to f. Then we have $\alpha = w\beta\gamma^{-1}$ for some $w \in \mathcal{O}_K^*$. Let $d \in \mathbb{Z}$ such that $cd \equiv 1 \pmod{f}$. Then $(bd + f\mathbb{Z}, w) \in (\mathbb{Z}/f\mathbb{Z})^* \times \mathcal{O}_K^*$ is sent to the class of α by ψ. This shows that $\ker\phi = \operatorname{Im}\psi$.

It is clear by definition that $\psi(\iota(-1)) = 1$, so that $\operatorname{Im}\iota \subseteq \ker\psi$. On the other hand, consider $(n + f\mathbb{Z}, w) \in (\mathbb{Z}/f\mathbb{Z})^* \times \mathcal{O}_K^*$ that belongs to the kernel of ψ. Without loss of generality, we have $0 < n < f$. But then $nw + f\mathcal{O}_K = 1 + f\mathcal{O}_K$ if and only if $nw = 1$. This implies that either $n = w = 1$ or $n = w = -1$. Hence, $\ker\psi = \operatorname{Im}\iota$.

This concludes the proof that the second sequence of the proposition is exact. □

Remark. In particular, if the imaginary quadratic number field K has class number 1, for an order of conductor f in K there are isomorphisms

$$I_K(f)/P_{K,\mathbb{Z}}(f) \cong I_K(f) \cap P_K/P_{K,\mathbb{Z}}(f) \cong (\mathcal{O}_K/f\mathcal{O}_K)^*/((\mathbb{Z}/f\mathbb{Z})^* \times (\mathcal{O}_K^*/\{\pm 1\}))$$

Class field theory with idèles

In this section, K always denotes a number field.

Class field theory can be restated in terms of idèles, with the advantage of not having to work up to the equivalence described in Remark 0.3.3.

We start by introducing the concepts of adèle and idèle.

Definition 0.3.15. For any finite prime $\mathfrak{p}$ of K, denote by $A_\mathfrak{p}$ the ring of integers of the completion of K at $\mathfrak{p}$. If $\mathfrak{p}$ is an infinite prime, set $A_\mathfrak{p} = K_\mathfrak{p}$.
The *adèle ring* $\mathbb{A}_K$ of K is

$$\mathbb{A}_K = \left\{ (x_\mathfrak{p})_\mathfrak{p} \in \prod_\mathfrak{p} K_\mathfrak{p} : x_\mathfrak{p} \in A_\mathfrak{p} \text{ for all but finitely many } \mathfrak{p} \right\}$$

The *idèle group* $\mathbb{A}_K^*$ of K is the unit group of the ring of adèles:

$$\mathbb{A}_K^* = \left\{ (x_\mathfrak{p})_\mathfrak{p} \in \prod_\mathfrak{p} K_\mathfrak{p}^* : x_\mathfrak{p} \in A_\mathfrak{p}^* \text{ for all but finitely many } \mathfrak{p} \right\}.$$

We also define the group of *finite idèles*

$$\mathbb{A}_{K,f}^* = \left\{ (x_\mathfrak{p})_\mathfrak{p} \in \prod_{\text{finite } \mathfrak{p}} K_\mathfrak{p}^* : x_\mathfrak{p} \in A_\mathfrak{p}^* \text{ for all but finitely many } \mathfrak{p} \right\}.$$

The idèle group $\mathbb{A}_K^*$ is a topological group, once endowed with the topology generated by open sets of the form $\prod_{\mathfrak{p}\in S} U_\mathfrak{p} \times \prod_{\mathfrak{p}\notin S} A_\mathfrak{p}^*$, where S is any finite set of primes of K and $U_\mathfrak{p}$ is an open subgroup of $K_\mathfrak{p}^*$ for all $\mathfrak{p} \in S$.

There is a canonical diagonal embedding $K^* \to \mathbb{A}_K^*$. Its image is discrete in $\mathbb{A}_K^*$ and consists of the principal idèles.

Definition 0.3.16. We define the *idèle class group* of K as the quotient $C_K = \mathbb{A}_K^*/K^*$.

We would like to describe the open subgroups of $\mathbb{A}_K^*$. Recall that, for any finite prime $\mathfrak{p}$ of K, we have a basis of open neighbourhoods of $1 \in K_\mathfrak{p}^*$ given by $\{U_\mathfrak{p}^n\}_{n\in\mathbb{Z}_{\geq 0}}$, where $U_\mathfrak{p}^0 = A_\mathfrak{p}^*$ and $U_\mathfrak{p}^n = 1 + \mathfrak{p}^n$ if $n > 0$. If $\mathfrak{p}$ is a real prime, then the subgroups of $K_\mathfrak{p}^*$ which are also open neighbourhoods of $1 \in K_\mathfrak{p}^*$ are $U_\mathfrak{p}^0 = K_\mathfrak{p}^* \cong \mathbb{R}^*$ and $U_\mathfrak{p}^1 = \mathbb{R}_{>0}$. If $\mathfrak{p}$ is complex, then the only open subgroup of $K_\mathfrak{p}^*$ is $U_\mathfrak{p}^0 = K_\mathfrak{p}^* \cong \mathbb{C}^*$ itself. For every modulus $\mathfrak{m} = \prod_\mathfrak{p} \mathfrak{p}^{n(\mathfrak{p})}$ of K we can now define $W_\mathfrak{m} = \prod_p U_\mathfrak{p}^{n(\mathfrak{p})}$, which is an open subgroup of $\mathbb{A}_K^*$.

A basis of the open subgroups of $\mathbb{A}_K^*$ is given by $\{W_\mathfrak{m} : \mathfrak{m} \text{ is a modulus of K}\}$.

The last concept we want to introduce before stating the main theorems of class field theory is that of norm of an idèle.

Definition 0.3.17. Let L/K be a finite extension. If $\mathfrak{p}$ is a prime of K, denote by $\mathfrak{P}$ a prime of L over $\mathfrak{p}$. We define the *norm* of an idèle $x \in \mathbb{A}_L^*$ as the idèle $\mathrm{Nm}_{L/K}(x) = (y_\mathfrak{p})_\mathfrak{p} \in \mathbb{A}_K^*$ such that $y_\mathfrak{p} = \prod_{\mathfrak{P}|\mathfrak{p}} \mathrm{Nm}_{L_\mathfrak{P}/K_\mathfrak{p}} x_\mathfrak{P}$.

We are now going to restate the two main results of class field theory we presented in the previous subsection with the language of idèles.

Theorem 0.3.18. *(Reciprocity law) Consider the global Artin map $\phi_K : \mathbb{A}_K^* \to \mathrm{Gal}(K^{ab}/K)$. The subgroup K^* of $\mathbb{A}_K^*$ lies in the kernel of ϕ_K. Moreover, for every finite abelian extension L/K, ϕ_K induces an isomorphism $\phi_{L/K} : C_K/\mathrm{Nm}_{L/K}(C_L) \to \mathrm{Gal}(L/K)$.*

Theorem 0.3.19. *(Existence theorem) Let $\overline{K}$ be a fixed algebraic closure of K. There is an inclusion-reversing bijection between the finite abelian extensions L/K and the closed subgroups of finite index in C_K given by*

$$L \leftrightarrow \mathrm{Nm}_{L/K}(C_L)$$

Shimura's reciprocity law

In this small section, we adapt the language used in [9, Chapter 7] to our situation.

The affine modular curve $Y_0(N)$ can be written as

$$Y_0(N) \cong \mathrm{GL}_2^+(\mathbb{Q}) \setminus \mathcal{H} \times \mathrm{GL}_2(\mathbb{A}_{\mathbb{Q},f})/\mathcal{K},$$

where $\mathcal{K} = \prod_{v\nmid N} \mathrm{GL}_2(\mathbb{Z}_p) \times \prod_{v|N} \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_v) : c \equiv 0 \pmod{N} \right\}$ is a compact subgroup of $\mathrm{GL}_2(\mathbb{A}_{\mathbb{Q},f})$. Under this isomorphism, $\tau \in Y_0(N)$ is sent to the equivalence class $[\tau, 1]$. The group $\mathrm{GL}_2^+(\mathbb{Q})$ acts on $\mathrm{GL}_2^+(\mathbb{Q}) \times \mathcal{H}$ on the left as follows: if $\gamma \in \mathrm{GL}_2^+(\mathbb{Q})$ and $[\tau, g] = [\tau, (g_v)_v] \in \mathcal{H}^* \times \mathrm{GL}_2(\mathbb{A}_{\mathbb{Q},f})$, then $\gamma[\tau, g] = [\gamma\tau, (\gamma_v g_v)_v]$. Here, γ acts on τ by linear fractional transformation, while the action of γ on g relies on the diagonal embedding $\mathbb{Q} \to \mathbb{A}_{\mathbb{Q},f}$. The group $\mathcal{K}$ codifies the invariance under $\Gamma_0(N)$ and acts on the right as follows: if $m = (m_v)_v \in \mathcal{K}$ and $[\tau, g] = [\tau, (g_v)_v] \in \mathcal{H} \times \mathrm{GL}_2(\mathbb{A}_{\mathbb{Q},f})$, then $[\tau, g]m = [\tau, (g_v m_v)_v]$.

A point $[\tau, g] \in Y_0(N)$ is called a *complex multiplication point* or *CM point* if for some imaginary quadratic field K it holds $\tau \in K \cap \mathcal{H}$. Then, $\{1, \tau\}$ is a basis for K over $\mathbb{Q}$, and τ satisfies a quadratic equation with rational coefficients $AX^2 + BX + C \in \mathbb{Q}[X]$. To such τ, we can associate a homomorphism $g_\tau : \mathbb{A}_{K,f}^* \to \mathrm{GL}_2(\widehat{\mathbb{Z}})$ such that for any finite idèle x,

$$g_\tau(x) \begin{pmatrix} \tau \\ 1 \end{pmatrix} = \begin{pmatrix} x\tau \\ x \end{pmatrix}$$

The action of g_z can be described explicitly:

$$x = sA\tau + t \mapsto g_\tau(x) = \begin{pmatrix} t - Bs & -Cs \\ As & t \end{pmatrix} \tag{0.3.20}$$

With this notation, we can state Shimura's reciprocity law, which will be used several times in the proofs of Chapter 2.

Theorem 0.3.21 (Shimura's reciprocity law on points)**.** *Let $[\tau, g]$ be a CM point on $Y_0(N)$, and let K be the quadratic imaginary field containing τ. Let $\sigma \in \mathrm{Gal}(K^{ab}/K)$ corresponding to the idèle x^{-1} via Artin reciprocity, then*

$$\sigma([\tau, g]) = [\tau, g_\tau(x)g]$$

Chapter 1

Preparation

This chapter serves as a foundation for the construction that we are going to describe in Chapter 2. Section 1.1 collects information about the curves $E_n : x^3 + y^3 = nz^3$ mentioned in the Introduction. In Section 1.2, we are going to study the modular curve $X_0(243)$ in some detail, describing its modular automorphisms and finding an alternative way to define points on it. We are also going to use $X_0(243)$ to parametrize the curve E_9. Section 1.3 is used to describe the field extensions of $\mathbb{Q}$ that will be relevant in Chapters 2 and 3.

1.1 About curves E_n

An important object throughout this thesis are going to be projective algebraic curves of the form $E_n : x^3 + y^3 = nz^3$, for n a positive integer.

Proposition 1.1.1. *Let n be a positive integer. The curve E_n defined by the projective cubic equation $x^3 + y^3 = nz^3$ is an elliptic curve defined over $\mathbb{Q}$, equipped with the base point $O = (1 : -1 : 0)$.*

Proof. We need to prove that the curve E_n is non-singular and of genus one.

A singular point $(x_0 : y_0 : z_0) \in \mathbb{P}^2(\overline{\mathbb{Q}})$ should satisfy $3x_0^2 = 3y_0^2 = 3nz_0^2$, i.e. $x_0 = y_0 = z_0 = 0$, which is impossible. Hence, E_n is smooth.

As E_n is a smooth plane curve define by a homogeneous polynomial of degree $d = 3$, its genus is $\frac{(d-1)(d-2)}{2} = 1$. □

We can always define the elliptic curve E_n via an affine Weierstrass equation.

Proposition 1.1.2. *The elliptic curve $E_n : x^3 + y^3 = nz^3$ defined over $\mathbb{Q}$ admits affine Weierstrass equation*

$$Y^2 = X^3 - 432n^2$$

Proof. Consider the change of variables $X = 12n\frac{z}{x+y}, Y = 36n\frac{x-y}{x+y}$.

Then, $X^3 - Y^2 = 2^6 3^3 n^3 \frac{z^3}{(x+y)^3} - 2^4 3^4 n^2 \frac{(x-y)^2}{(x+y)^2} = 432n^2$. □

Let $K = \mathbb{Q}(\omega)$, for $\omega \in \mathcal{H}$ a primitive cubic root of unity. The field K is imaginary quadratic, and its ring of integers is $\mathcal{O}_K = \mathbb{Z}[\omega]$. Consider the action of ω on E_n that sends a point $P = (X, Y)$ satisfying $Y^2 = X^3 - 432n^2$ to the point $\omega P = (\omega X, Y)$. We checked using [16, Algorithm 2.3] that the action of ω commutes with the sum operation on the elliptic curve E_n. It follows that the endomorphism ring of E_n contains the maximal order $\mathcal{O}_K$ of the imaginary quadratic field K.

In Chapter 2 and in Subsection 1.2.1 we are going to need different models for the elliptic curves E_1, E_9 and E_{p^i}, for p a prime number congruent to 4 or 7 modulo 9 and $i \in \{1, 2\}$. In the next three propositions, we provide affine equations for such curves that we are going to use, other than that from Proposition 1.1.2.

Proposition 1.1.3. *The elliptic curve E_1 can be defined via the following affine equation:*

$$y^2 + y = 3x^3 - 1 \tag{1.1.4}$$

Proof. We saw in Proposition 1.1.2 that E_1 has Weierstrass equation $Y^2 = X^3 - 432$. With the change of coordinates $x = \frac{X}{2^2 3}, y = \frac{Y}{2^3 3} - \frac{1}{2}$ we obtain the model in the statement.

Indeed, $\left(\frac{Y}{2^3 3} - \frac{1}{2}\right)^2 + \left(\frac{Y}{2^3 3} - \frac{1}{2}\right) - 3\left(\frac{X}{2^2 3}\right)^3 + 1 = \frac{Y^2 - X^3 + 2^4 3^3}{2^6 3^2} = 0$ □

Proposition 1.1.5. *The elliptic curve E_9 admits affine equation:*

$$y^2 + y = x^3 - 1 \tag{1.1.6}$$

Proof. We showed in Proposition 1.1.2 that E_9 is defined by the Weierstrass equation $Y^2 = X^3 - 432 \cdot 9^2$. The model in the statement is obtained from the change of coordinates $x = \frac{X}{6^2}, y = \frac{Y}{6^3} - \frac{1}{2}$.

Indeed, it holds $\left(\frac{Y}{6^3} - \frac{1}{2}\right)^2 + \left(\frac{Y}{6^3} - \frac{1}{2}\right) - \left(\frac{X}{6^2}\right)^3 + 1 = \frac{Y^2 - X^3 + 2^4 3^7}{6^6} = 0.$ □

Proposition 1.1.7. *Let p be a prime number congruent to 4 or 7 modulo 9. Let $i \in \{1, 2\}$. The elliptic curve E_{p^i} admits affine equation:*

$$E_{p^i} : y^2 + y = 3p^i x^3 - 1 \tag{1.1.8}$$

Proof. From Proposition 1.1.2, we know that E_{p^i} has Weierstrass equation $Y^2 = X^3 - 432p^i$. The model in the statement is obtained after the the change of coordinates $x = \frac{X}{2^2 3 p^i}, y = \frac{Y}{2^3 3 p^i} - \frac{1}{2}$.

Indeed, we have $\left(\frac{Y}{2^3 3 p^i} - \frac{1}{2}\right)^2 + \left(\frac{Y}{2^2 3 p^i} - \frac{1}{2}\right) - 3\left(\frac{X}{2^2 3 p^i}\right)^3 + 1 = \frac{Y^2 - X^3 + 2^4 3^3 p^{2i}}{2^6 3^2 p^{2i}} = 0.$ □

Finally, as the 3-torsion points of the elliptic curve E_9 in the model (1.1.6) will be used in the proof of Proposition 1.2.8, we note that:

$$E_9[3] = \{O, (0, \omega), (0, \omega^2), (\omega^i \sqrt[3]{3}, -2), (\omega^i \sqrt[3]{3}, 1) : i \in \{0, 1, 2\}\} \tag{1.1.9}$$

1.2 About $X_0(243)$

Our aim in this section is to study a little more in depth the modular curve $X_0(243)$ of genus 19, following [7, Chapter 2]. We will use $X_0(243)$ to define a modular parametrization for the elliptic curve E_9 of conductor 243. We will also use isogenies of elliptic curves over $\mathbb{C}$ to describe the points of $X_0(243)$ that we will be using in our construction of a point on $E_p(\mathbb{Q})$ and $E_{p^2}(\mathbb{Q})$, for p a prime congruent to 4 or 7 modulo 9.

We denote $\omega := \frac{-1+\sqrt{3}}{2}$, the cubic root of unity lying on the upper half-plane. We denote $K := \mathbb{Q}(\omega) \subset \mathbb{C}$, and its ring of integers $\mathcal{O}_K := \mathbb{Z}[\omega]$.

Recall that we have an isomorphism of Riemann surfaces $X_0(243) \cong \Gamma_0(243) \setminus \mathcal{H}^*$.

Define the group of modular automorphisms of $X_0(243)$ to be the normalizer of $\Gamma_0(243)$ inside $\mathrm{PGL}_2^+(\mathbb{Q})$ quotiented out by $\Gamma_0(243)$:

$$\mathrm{MAut}(X_0(243)) := N_{\mathrm{PGL}_2^+(\mathbb{Q})}(\Gamma_0(243))/\Gamma_0(243).$$

If $M \in \mathrm{GL}_2^+(\mathbb{Q})$ represents a matrix in $\mathrm{PGL}_2^+(\mathbb{Q})$, we denote its class modulo multiplication by diagonal matrices and modulo $\Gamma_0(243)$ by $\overline{M}$.

In order to determine the structure of the group $\mathrm{MAut}(X_0(243))$, we are going to need generators for the group. Atkin and Lehner in [2] introduced Atkin-Lehner involutions.

Definition 1.2.1. Let N be a positive integer and let q be a divisor of N such that $\gcd(q, N/q) = 1$. For each such q, an integral matrix W_q of the form $\begin{pmatrix} aq & b \\ cN & dq \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q})$ with $\det W_q = q$ is called an *Atkin-Lehner involution.*

Atkin and Lehner proved that a matrix of the form W_q, for q a divisor of $N \in \mathbb{Z}_{>0}$, as in Definition 1.2.1, normalizes the congruence subgroup $\Gamma_0(N)$.

Lemma 1.2.2. *[2, Lemma 8] For any choice of $N \in \mathbb{Z}_{>0}$ and q, W_q as in Definition 1.2.1, it holds*

- *W_q normalizes $\Gamma_0(N)$, i.e. $W_q\Gamma_0(N)W_q^{-1} = \Gamma_0(N)$;*
- *$(W_q)^2$ can be written as qA for some $A \in \Gamma_0(N)$;*
- *for a different choice of W_q' satisfying Definition 1.2.1, $W_q' \equiv W_q \mod \Gamma_0(N)$.*

We are going to use the notion of Atkin-Lehner involution when describing the structure of $\mathrm{MAut}(X_0(243))$.

Let $v := \begin{pmatrix} 1 & 0 \\ 81 & 1 \end{pmatrix}$ and $w := \begin{pmatrix} 0 & -1 \\ 243 & 0 \end{pmatrix}$ be matrices in $\mathrm{GL}_2^+(\mathbb{Q})$. In [7, Section 2.1], Dasgupta and Voight show that the classes of v and w generate $\mathrm{MAut}(X_0(243))$.

Proposition 1.2.3. *Let $v := \begin{pmatrix} 1 & 0 \\ 81 & 1 \end{pmatrix}$ and $w := \begin{pmatrix} 0 & -1 \\ 243 & 0 \end{pmatrix}$. Then the group of modular automorphisms of $X_0(243)$ has structure:*

$$\mathrm{MAut}(X_0(243)) = \langle \overline{w}, \overline{v^{-1}wv} \rangle \rtimes \langle \overline{v} \rangle \cong S_3 \rtimes \mathbb{Z}/3\mathbb{Z}$$

Proof. We start by checking that the classes of v and w generate $\mathrm{MAut}(X_0(243))$.

We know from Lemma 1.2.2 that Atkin-Lehner involutions normalize $\Gamma_0(243)$. Since $243 = 3^7$, the only divisors q of 243 such that $\gcd(q, 243/q) = 1$ are $q = 1$ and $q = 243$. However, if $q = 1$, then $\det W_1 = 1$, and so $W_1 \in \Gamma_0(243)$. The only nontrivial Atkin-Lehner involution inside $\mathrm{MAut}(X_0(243))$ is given by $q = 243$. $W_{243} = \begin{pmatrix} 243a & b \\ 243c & 243d \end{pmatrix}$ must satisfy $a, b, c, d \in \mathbb{Z}$ and $\det W_{243} = 243$. Any valid choice of a, b, c, d is equivalent over $\Gamma_0(243)$, so by taking $a = d = 0$, $b = -1$, $c = 1$, we can pick W_{243} to be w. Recall that, by Lemma 1.2.2, $\overline{w}$ has order 2.

We claim that $\overline{v}$ also belongs to $\mathrm{MAut}(X_0(243))$. Let $M = \begin{pmatrix} a & b \\ 243c & d \end{pmatrix} \in \Gamma_0(243)$, with $a, b, c, d \in \mathbb{Z}$ satisfying $ad - 243bc = 1$. Looking at this relation modulo 3, we get that $ad \equiv 1 \pmod 3$, so either both a and d are congruent to 1 or to 2 modulo 3. In any case, $a - d \equiv 0 \pmod 3$, so the bottom left entry of $vMv^{-1} = \begin{pmatrix} a - 81b & b \\ 81(a - 81b + 3c - d) & 81b + d \end{pmatrix}$ is a multiple of 243. As $\det(vMv^{-1}) = 1$, we conclude $vMv^{-1} \in \Gamma_0(243)$. Notice that $v^3 = \begin{pmatrix} 1 & 0 \\ 243 & 1 \end{pmatrix} \in \Gamma_0(243)$, so $\overline{v}$ has order 3.

The classes $\overline{w}$ and $\overline{v}$ are distinct generators for $\mathrm{MAut}(X_0(243))$, as they have different orders. It remains to check what group structure they define.

Denote $\Sigma = \langle \overline{w}, \overline{v^{-1}wv} \rangle$. We need to prove that $\overline{v}$ normalizes Σ and that Σ has the structure of the symmetric group of order 6. Denote $\tilde{w} := v^{-1}wv$.

From $\overline{w}^2 = 1$, we immediately get $\overline{\tilde{w}}^2 = \overline{v}^{-1}\overline{w}^2\overline{v} = 1$. We also have that $-3^{-15}(w\tilde{w})^3 = \begin{pmatrix} 23491 & 280 \\ 68040 & 811 \end{pmatrix} \in \Gamma_0(243)$, so that $(\overline{w\tilde{w}})^3 = 1 \in \mathrm{MAut}(X_0(243))$. Therefore, Σ is isomorphic to the group S_3.

It is clear that $\overline{v}\overline{\tilde{w}}\overline{v}^{-1} = \overline{w} \in \Sigma$. We see that $\overline{vwv}^{-1}$ is equivalent to $\overline{w}^{-1}\overline{\tilde{w}}^{-1}\overline{w} \in \Sigma$, because $(vwv^{-1})(w^{-1}\tilde{w}^{-1}w)^{-1} = \begin{pmatrix} -26 & 9 \\ -2187 & 757 \end{pmatrix} \in \Gamma_0(243)$ Therefore, $\overline{v}$ normalizes Σ, and $\Sigma \trianglelefteq \mathrm{MAut}(X_0(243))$. □

Recall the notation $\Sigma := \langle \overline{w}, \overline{v^{-1}wv} \rangle \trianglelefteq \mathrm{MAut}(X_0(243))$. Define the subgroup G of $\mathrm{PGL}_2^+(\mathbb{Q})$ generated by Σ and by the image of $\Gamma_0(243)$ modulo multiplication by diagonal matrices. We will use this group when defining the modular parametrization for the elliptic curve E_9 in Subsection 1.2.1. Thus, we would like to understand if there are elements of $\mathrm{PGL}_2^+(\mathbb{Q})$ that normalize G.

Define the element of $\mathrm{PGL}_2^+(\mathbb{Q})$ represented by

$$t := \begin{pmatrix} 9 & 1 \\ -243 & -18 \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{Q}) \tag{1.2.4}$$

Notice that $t^3 = \begin{pmatrix} 729 & 0 \\ 0 & 729 \end{pmatrix}$, so $\bar{t}$ has order 3 in $\mathrm{PGL}_2^+(\mathbb{Q})$.

We claim that t normalizes $\mathrm{MAut}(X_0(243))$.

To prove this, it suffices to look at its action on the generators of $\mathrm{MAut}(X_0(243))$. We have that $tvt^{-1} = \begin{pmatrix} -179 & -1 \\ 1863 & 19 \end{pmatrix} v^{-1}$, for $\begin{pmatrix} -179 & -1 \\ 1863 & 19 \end{pmatrix} \in \Gamma_0(243)$, so $\bar{t}\overline{v}\bar{t}^{-1} = \overline{v^2}$. On the other hand, $twt^{-1} = \begin{pmatrix} 85 & 1 \\ -1701 & 20 \end{pmatrix} \tilde{w}$ for $\begin{pmatrix} 85 & 1 \\ -1701 & 20 \end{pmatrix} \in \Gamma_0(243)$, so that $\bar{t}\overline{w}\bar{t}^{-1} = \overline{\tilde{w}} \in \mathrm{MAut}(X_0(243))$. We conclude that $\mathrm{MAut}(X_0(243))$ is fixed under conjugation by $\bar{t}$.

Proposition 1.2.5. *Define G to be the subgroup of $\mathrm{PGL}_2^+(\mathbb{Q})$ generated by $\Gamma_0(243)$ and Σ. Then G is normalized by $\overline{v}$ and $\bar{t}$.*

Proof. Since $\overline{v}$ normalizes both $\Gamma_0(243)$ and Σ, it normalizes G.

We have already shown that $\bar{t}\overline{w}\bar{t}^{-1} = \overline{\tilde{w}}$. From this, we also obtain $\bar{t}\overline{\tilde{w}}\bar{t}^{-1} = \overline{w}$. In particular, $\bar{t}$ normalizes Σ. To prove that $\bar{t}$ normalizes the group G, it remains to show that for any $M = \begin{pmatrix} a & b \\ 243c & d \end{pmatrix} \in \Gamma_0(243)$, we have $\bar{t}\overline{M}\bar{t}^{-1} \in G$. This will actually depend on $a, d \pmod 9$. As $\det M = 1$, we have that $ad \equiv 1 \pmod 9$. The possibilities for the pair $(a \pmod 9, d \pmod 9)$ are $\{(1,1),(2,5),(4,7),(5,2),(7,4),(8,8)\}$. If $a \equiv d \pmod 9$, then in $\mathrm{PGL}_2^+(Q)$ we have $tMt^{-1} = \begin{pmatrix} -2a+27b-54c+3d & b-3c+\frac{d-a}{9} \\ 243\left(-3b+4c+\frac{2a-2d}{9}\right) & 3a-27b+54c-2d \end{pmatrix}$, which lies in $\Gamma_0(243)$. If (a,d) is congruent to $(4,7)$ or $(5,2)$ modulo 9, then we find $tMt^{-1} = w \begin{pmatrix} 66a-513b+1188c-38d & -6b+14c+\frac{7a-4d}{9} \\ 243\left(-19b+66c+\frac{22a-19d}{9}\right) & 7a-54b+189c-6d \end{pmatrix} \tilde{w}^{-1}$ is in $w\Gamma_0(243)\tilde{w}^{-1}$. If the pair (a,d) is congruent to $(7,4)$ or $(2,5)$ modulo 9, then we see that $tMt^{-1} = \tilde{w} \begin{pmatrix} -6a+54b-189c+7d & -6b+14c+\frac{4a-7d}{9} \\ 243\left(-19b+66c+\frac{19a-22d}{9}\right) & -38a+513b-1188c+66d \end{pmatrix} w^{-1}$ lies in $\tilde{w}\Gamma_0(243)w^{-1}$. In any case, we conclude that $\bar{t}\overline{M}\bar{t}^{-1}$ belongs to the group G. □

1.2.1 A modular parametrization for E_9

In this subsection we will present an explicit modular parametrization of the curve E_9, with model (1.1.6), and then show how the actions from Proposition 1.2.5 relate to endomorphisms of E_9. This will be used in Chapter 2, when determining the action of a Galois action on points of E_9.

In Proposition 1.2.3, we showed $\Sigma \trianglelefteq \mathrm{MAut}(X_0(243))$, for $\Sigma = \langle \overline{w}, \overline{v^{-1}wv} \rangle$. Recalling that G is the subgroup of $\mathrm{PGL}_2^+(\mathbb{Q})$ generated by Σ and $\Gamma_0(243)$, we may consider

$$X(G) := G \setminus \mathcal{H}^* = X_0(243)/\Sigma \tag{1.2.6}$$

There is a natural surjection $X_0(243) \to X(G)$, and using the Riemann-Hurwitz formula, we compute the genus of $X(G)$ to be 1. We consider the image of the cusp at infinity $\infty \in X_0(243)(\mathbb{Q})$ as a rational point O of $X(G)$. Then, $X(G)$ has the structure of an elliptic curve over $\mathbb{Q}$ with base point O.

The following proposition by Dasgupta and Voight [7] asserts that the elliptic curve $X(G)$ is isomorphic to the elliptic curve E_9, and it can be parametrized by the modular curve $X_0(243)$ via an explicit parametrization.

Proposition 1.2.7. *There is a modular parametrization*

$$\begin{aligned}\Phi : X_0(243) \to X(G) &\xrightarrow{\sim} E_9 : y^2 + y = x^3 - 1 \\ z &\mapsto (x, y)\end{aligned}$$

where $x(z) = \frac{\eta(9z)\eta(27z)}{\eta(3z)\eta(81z)}$, $y(z) = -\frac{\eta(9z)^4+9\eta(9z)\eta(81z)^3}{\eta(27z)^4-3\eta(9z)\eta(81z)^3} - 2$.

Proof. See [7, Proposition 2.2.3]. □

We showed in Proposition 1.2.5 that $\bar{t}$ and $\overline{v}$ normalize the subgroup G of $\mathrm{PGL}_2^+(\mathbb{Q})$ generated by Σ and $\Gamma_0(243)$. As E_9 is isomorphic to $G \setminus \mathcal{H}^*$, it means that $\bar{t}$ and $\overline{v}$ give rise to automorphisms of E_9 as a curve of genus 1. We would now like to understand how to write the actions given by $\bar{t}$ and $\overline{v}$ in terms of endomorphisms of E_9.

The elliptic curve E_9 has complex multiplication by the ring of integers $\mathcal{O}_K = \mathbb{Z}[\omega]$ of $K = \mathbb{Q}(\omega)$, where $\omega \in \mathcal{H}$ is a primitive cubic root of unity. The endomorphism of E_9 given by ω is defined in the model (1.1.6) by $(x, y) \mapsto (\omega x, y)$.

Any morphism of E_9 to itself as a curve of genus 1 can be written as the composition of an isogeny and a translation. Thus, every endomorphism of E_9 as a curve is of the form $Z \mapsto aZ + b$, for some $a \in \mathcal{O}_K$ and $b \in E_9$.

Proposition 1.2.8. *The action of* $\bar{t}$ *on* E_9 *as a curve is given by* $t(Z) = \omega^2 Z + (0, \omega)$, *while the action of* $\overline{v}$ *on* E_9 *as a curve is* $v(Z) = \omega^2 Z$.

Proof. This proof follows that of [7, Proposition 2.2.7].

We want to find $a \in \mathcal{O}_K$ and $b \in E_9$ such that $\bar{t}(Z) = aZ + b$. Recall that $\bar{t}$ has order 3 as a linear fractional transformation, so from writing $Z = \bar{t}^3(Z)$ we deduce $a^3 = 1$, i.e. $a \in \{1, \omega, \omega^2\}$, and $b \in E_9(\overline{\mathbb{Q}})$. If we look at the action of $\bar{t}$ on the cusp $\infty = [1, 0] \in \mathbb{P}^1(\mathbb{Q})$ of $X(G)$, we see that $\bar{t}(\infty) = [9, -243] = [-1, 27]$. There are three cusps in $X(\Gamma)$: the cusp at infinity is mapped to the base point O of E_9, while the other two cusps are mapped to the points $(0, \omega)$ and $(0, \omega^2)$ in E_9. The cusp $[-1, 27]$ is not equivalent to the cusp at infinity under the action of G. We use the modular parametrization $\Phi : X_0(243) \to E_9$ from Proposition 1.2.7 and the fact that $\begin{pmatrix}-1\\27\end{pmatrix} = \begin{pmatrix}1 & 0\\-27 & 1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}$ to compute $\Phi\left(-\frac{1}{27}\right) = \lim_{n\to\infty} \Phi\left(\begin{pmatrix}1 & 0\\-27 & 1\end{pmatrix} ni\right) = (0, \omega)$. Therefore, we obtain $b = b + O = \Phi(\bar{t}(\infty)) = \Phi(-1/27) = (0, \omega)$. Let $\tau = (\omega - 1)/27 \in \mathcal{H}$. We have that $\bar{t}(\tau) = -\frac{1}{27}\frac{\omega+2}{\omega+1} = \frac{\omega-1}{27} = \tau$. Let $T = \Phi(\tau)$. We must have $T = aT + b$, i.e. $(1 - a)T = b = (0, \omega) \in E_9[3]$. This implies that T itself must be a 3-torsion point of E_9. Numerically, we see that $T = \Phi(\tau) \approx (\sqrt[3]{3}, -2) \in E_9[3]$. Comparing with the remaining eight 3-torsion points of the elliptic curve E_9 we found in (1.1.9), we deduce that $T = (\sqrt[3]{3}, -2)$. Now, we have that $aT = T - (0, \omega) = ((-\omega - 1)\sqrt[3]{3}, -2)$, so we conclude $a = \omega^2$. Thus, $\bar{t}$ acts on E_9 as claimed.

We are now going to deal with $\overline{v}$. We look for $a \in \mathcal{O}_K, b \in E_9$ such that $\overline{v}(Z) = aZ + b$. We showed $\overline{v}$ has order 3, so, as in the previous case, we must have $a \in \{1, \omega, \omega^2\}$ and $b \in E_9(\overline{\mathbb{Q}})$. Looking at the action on the cusp at infinity, we see that $\overline{v}(\infty) = [1, 81]$. The cusp $[1, 81] \in X_0(243)$ belongs to the orbit of the cusp at infinity under the action

of Σ, therefore they give rise to the same cusp on $X(G)$. It follows that $\Phi(1/81) = \infty$, and in particular $b = 0$. To compute a, we consider $\Phi(\overline{v}(\tau)) = a\Phi(\tau)$, for $\tau = (\omega - 1)/27$. We saw that $\Phi(\tau) = (\sqrt[3]{3}, -2)$ is a 3-torsion point of E_9, so also $a\Phi(\tau)$ must belong to $E_9[3]$. Numerically, we see that $\Phi(\overline{v}(\tau)) \approx (\omega^2\sqrt[3]{3}, -2)$. Comparing with the remaining 3-torsion points found in (1.1.9), we deduce $\Phi(\overline{v}(\tau)) = (\omega^2\sqrt[3]{3}, -2)$. We conclude that $a = \omega^2$. Therefore, $\overline{v}$ acts on E_9 as claimed. □

1.2.2 Seeing the points of $X_0(243)$ as isogenies

In this subsection, we are going to show an alternative way of considering the points of $Y_0(243)$, as they correspond to cyclic 243-isogenies. This interpretation will be used in Section 2.1, when defining a point of $X_0(243)$ to start our construction of a rational point on E_p and E_{p^2}.

The first step to stating this correspondence is Theorem 1.2.10. It says there is a bijection between points of a modular curve $Y_0(N)$ and enhanced elliptic curves, which we are about to define.

Definition 1.2.9. Let N be a positive integer. An *enhanced elliptic curve* for $\Gamma_0(N)$ is an ordered pair (E, K), consisting of a complex elliptic curve E and a cyclic subgroup K of E of order N. Two enhanced elliptic curves (E, K), (E', K') are equivalent if there is an isomorphism $E \to E'$ such that K is mapped to K'. If this is the case, we write $(E, K) \sim (E', K')$. The set of equivalence classes of enhanced elliptic curves for $\Gamma_0(N)$ is denoted by $S_0(N)$, and an element of $S_0(N)$ is denoted by $[E, K]$.

Theorem 1.2.10. *[8, Theorem 1.5.1(a)] For a complex number $\tau \in \mathcal{H}$, denote by Λ_τ the lattice $\mathbb{Z} + \mathbb{Z}\tau$ in $\mathbb{C}$.*

For any positive integer N, there is a bijection

$$\begin{aligned} S_0(N) &\to Y_0(N) \\ [\mathbb{C}/\Lambda_\tau, \langle 1/N + \Lambda_\tau\rangle] &\mapsto \Gamma_0(N)\tau \end{aligned}$$

A further step in understanding the points of $Y_0(N))$ is to find another object to encode the data of a pair of the form $(\mathbb{C}/\Lambda_\tau, \langle 1/N + \Lambda_\tau\rangle)$, representing an enhanced elliptic curve for $\Gamma_0(N)$. We are going to show that such a suitable object, in our case where $N = 243$, is a certain cyclic isogeny.

Definition 1.2.11. We say that an isogeny $\phi : E \to E'$ is *cyclic* if its kernel $\ker\phi$ is a cyclic group.

Remark. If $E = \mathbb{C}/\Lambda$ and $E' = \mathbb{C}/\Lambda'$ are two complex elliptic curves associated to the complex lattices $\Lambda \subseteq \Lambda'$, then there is an induced isogeny $\phi : E \to E'$. The isogeny ϕ is cyclic if and only if the finite abelian group Λ'/Λ is cyclic.

In our case, we want to view $Y_0(243)$ as parametrizing cyclic 243-isogenies. Following Theorem 1.2.10, to each $\tau \in \mathcal{H}$ we associate the data $(\mathbb{C}/\Lambda_\tau, \langle P_\tau\rangle)$, where $\Lambda_\tau = \mathbb{Z} + \mathbb{Z}\tau$ and $P_\tau = 1/243 + \Lambda_\tau$. The pair $(\mathbb{C}/\Lambda_\tau, \langle P_\tau\rangle)$ corresponds to the cyclic

243-isogeny $\phi_\tau : \mathbb{C}/\Lambda_\tau \to \mathbb{C}/\Lambda_{243\tau}$ defined by $z \mapsto 243z$. The kernel $\ker \phi_\tau$ is generated by P_τ. Indeed, we have $\ker \phi_\tau = \{a + b\tau \in \mathbb{C}/\Lambda_\tau : 243a + 243b\tau \in \mathbb{Z} + 243\mathbb{Z}\tau\} = \{a + b\tau \in \mathbb{C}/\Lambda_\tau : a \in \frac{1}{243}\mathbb{Z}, b \in \mathbb{Z}\} = \{\frac{1}{243}a \in \mathbb{C}/\Lambda_\tau : a \in \mathbb{Z}\}$.

Now, we want to construct explicit cyclic 243-isogenies, in order to obtain a point of $X_0(243)$.

Recall the notation $K = \mathbb{Q}(\omega)$, for $\omega \in \mathcal{H}$ a primitive cubic root of unity.

We will build a 243-isogeny by considering the composition of five 3-isogenies. The 3-isogenies we are going to consider will be between elliptic curves of the form $\langle\tau\rangle := \mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)$, for $\tau \in K \cap \mathcal{H}$.

For an inclusion of lattices $\mathbb{Z} + \mathbb{Z}\tau_1 \subset \mathbb{Z} + \mathbb{Z}\tau_2$ with $\tau_2 \notin \mathbb{Z} + \mathbb{Z}\tau_1$ and $3\tau_2 \in \mathbb{Z} + \mathbb{Z}\tau_1$, we have an isogeny $\phi : \langle\tau_1\rangle \to \langle\tau_2\rangle$ and the dual isogeny $\widehat{\phi} : \langle\tau_2\rangle \to \langle\tau_1\rangle$ defined by $z \mapsto 3z$. The composition $\phi \circ \widehat{\phi}$ is the multiplication-by-3 map on $\langle\tau_2\rangle$, so both ϕ and $\widehat{\phi}$ are 3-isogenies.

For a prime p congruent to 1 modulo 3, we obtain the tree of isogenies in Figure 1.1.

If the elliptic curve $\langle\tau\rangle = \mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau)$ has complex multiplication by the order $\mathbb{Z}+f\mathcal{O}_K$ of K of conductor f, then in Figure 1.1 we denote the elliptic curve by $\langle\tau\rangle_f$. Refer to Lemma 1.2.12 to see how the orders were computed.

Any path of length 5 on the tree in Figure 1.1 from one of the curves on the leftmost column to one of the curves on the rightmost column gives rise to a cyclic 243-isogeny, and hence to a point on $X_0(243)$.

Lemma 1.2.12. *The elliptic curves $\langle\tau\rangle = \mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)_f$ in Figure 1.1 have complex multiplication by the order $\mathbb{Z} + f\mathcal{O}_K$ of K of order f, where:*

- *$f = p$ if τ is $p\omega$ or $\frac{p\omega+2}{3}$,*
- *$f = 3p$ if τ is of the form $3p\omega$, $\frac{p\omega}{3}$, $\frac{p\omega+1}{3}$, or $\frac{p\omega+2+3l}{9}$ for $l \in \{0, 1, 2\}$,*
- *$f = 9p$ if τ is of the form $9p\omega$, $\frac{3p\omega+i}{3}$ for $i \in \{1, 2\}$ $\frac{p\omega+j+3l}{9}$ for $j \in \{1, 2\}$ and $l \in \{0, 1, 2\}$, or $\frac{p\omega+2+3n}{27}$ for $n \in \{0, \ldots, 8\}$.*

Proof. To find the conductor f of the order $\mathrm{End}(\langle\tau\rangle)$, we need to find the minimal $f \in \mathbb{Z}_{>0}$ such that $f\omega(x + y\tau) \in \mathbb{Z} + \mathbb{Z}\tau$ for every $x, y \in \mathbb{Z}$. By linearity, it suffices to check what happens for $(x, y) \in \{(0, 1), (1, 0)\}$.

As p is congruent to 1 modulo 3, we may write $p = 3k + 1$ for some integer k.

Now, we will consider several different cases for the elliptic curve $\langle\tau\rangle$, checking the requirements for $f\omega$ and $f\tau\omega$ to lie in $\mathbb{Z} + \mathbb{Z}\tau$.

Case $\langle 3^\ell p\omega\rangle$, $\ell \in \{0, 1, 2\}$:

From $f\omega \in \mathbb{Z} + 3^\ell p\mathbb{Z}\omega$ we get $3^\ell p \mid f$, while $f\omega(3^\ell p\omega) = -3^\ell fp\omega - 3^\ell fp \in \mathbb{Z} + 3^\ell p\mathbb{Z}\omega$ gives no additional condition on f. Therefore, $f = 3^\ell p$.

Case $\langle\frac{p\omega+3l+j}{9}\rangle, l \in \{0, 1, 2\}, j \in \{0, 1, 2\}$:

Requiring $f\omega \in \mathbb{Z} + \mathbb{Z}\frac{p\omega+3l+j}{9}$ gives $p \mid f$. So we set $f = pn$, with $n \in \mathbb{Z}_{>0}$. Thus, we are requiring $f\omega\frac{p\omega+3l+j}{9} \equiv -n\frac{6k+1+6lj-3l+j^2-3kj-j}{9} \in \mathbb{Z} + \mathbb{Z}\frac{p\omega+3l}{9}$.

If $j \in \{0, 1\}$, the last inclusion can only happen if $9 \mid n$. If $j = 2$, it suffices to ask that $3 \mid n$, as the numerator would be divisible by 3.

We conclude that $f = 9p$ if $j \in \{0, 1\}$, while $f = 3p$ if $j = 2$.

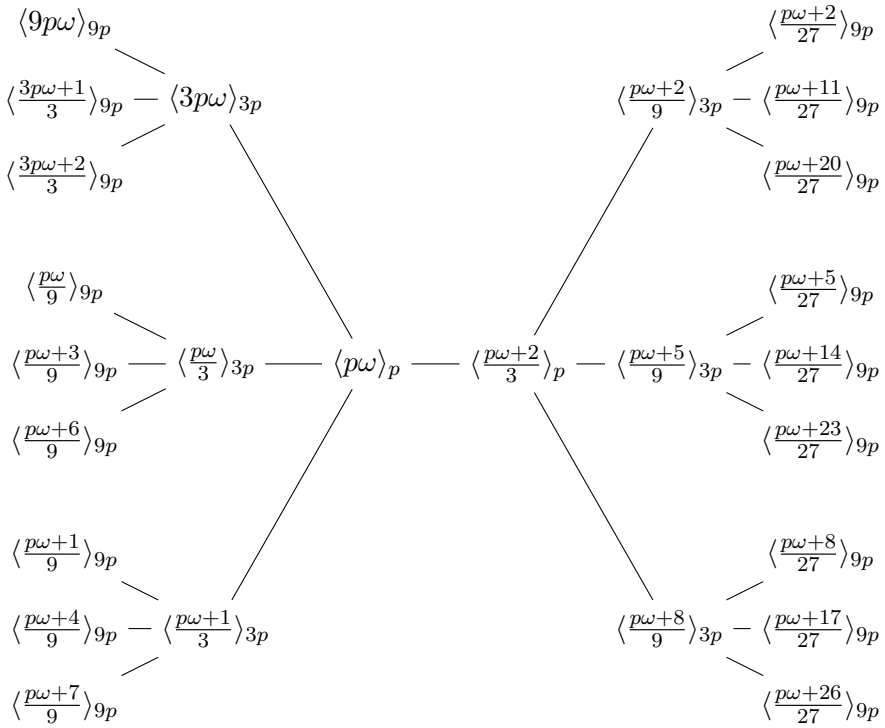

Figure 1.1: Isogeny tree between complex elliptic curves $\langle\tau\rangle_f := \mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau)$ with complex multiplication by the order of K of conductor f. The number p denotes a prime congruent to 1 modulo 3.

Case $\langle\frac{3p\omega+l}{3}\rangle, l \in \{1,2\}$:

The condition $f\omega \in \mathbb{Z} + \mathbb{Z}\frac{3p\omega+l}{3}$ yields $3p \mid f$. So we set $f = 3pn$, with $n \in \mathbb{Z}_{>0}$. Now, we require $f\omega\frac{3p\omega+l}{3} \equiv -n\frac{l^2}{3} \equiv -n\frac{1}{3} \in \mathbb{Z} + \mathbb{Z}\frac{3p\omega+l}{3}$. The last inclusion holds if and only if 3 divides n, therefore, we have $f = 9p$.

Case $\langle\frac{p\omega+j}{3}\rangle, j \in \{0,1,2\}$:

Requiring $f\omega \in \mathbb{Z} + \mathbb{Z}\frac{p\omega+j}{3}$ gives $p \mid f$. So we set $f = pn$, with $n \in \mathbb{Z}_{>0}$. Now, we seek $f\omega\frac{p\omega+j}{3} \equiv -n\frac{1+j(j-1)}{3} \in \mathbb{Z} + \mathbb{Z}\frac{p\omega+3i}{9}$. This last inclusion is trivial if $j = 2$, while in case $j \in \{0,1\}$ it holds if and only if $3 \mid n$.

We conclude that $f = 3p$ if $j \in \{0,1\}$ and $f = p$ if $j = 2$.

Case $\langle\frac{p\omega+3l+2}{27}\rangle, l \in \{0,\ldots,8\}$:

The condition $f\omega \in \mathbb{Z} + \mathbb{Z}\frac{p\omega+3l+2}{27}$ gives $p \mid f$, so we set $f = pn$, with $n \in \mathbb{Z}_{>0}$. Thus, we demand $f\omega\frac{p\omega+3l+2}{27} \equiv -n\frac{9k^2+6k+1+9l^2+9l-9kl+4-3k-2}{27} \in \mathbb{Z} + \mathbb{Z}\frac{p\omega+3l}{9}$. Requiring the last inclusion (since the numerator is divisible by 3) leads to $9 \mid n$, so that $f = 9p$. □

1.3 Relevant field extensions

In this section, we are going to collect useful information about the fields that are going to be used in the construction of the rational points on E_p and E_{p^2} in Chapter 2.

Recall that we define K as the imaginary quadratic field $\mathbb{Q}(\omega)$, for $\omega \in \mathcal{H}$ a primitive cubic root of unity. We denote the ring of integers of K by $\mathcal{O}_K = \mathbb{Z}[\omega]$. We note that K has class number $h(\mathcal{O}_K) = 1$ and discriminant $d_K = -3$.

We will denote by H_f the ring class field corresponding to the order $\mathcal{O}_f = \mathbb{Z} + f\mathcal{O}_K$ of conductor $f \in \mathbb{Z}_{>0}$ in K.

Proposition 1.3.1. *The class numbers of the ring class fields H_f, $h(\mathcal{O}_f) = [H_f : K]$, for $f \in \{3, 9, 3p, 9p\}$ are as follows:*

$$h(\mathcal{O}_3) = 1, \quad h(\mathcal{O}_9) = 3, \quad h(\mathcal{O}_{3p}) = p - 1, \quad h(\mathcal{O}_{9p}) = 3(p-1)$$

Proof. In order to compute $h(\mathcal{O}_f)$, we will use Theorem 0.3.13, which says

$$h(\mathcal{O}_f) = \frac{h(\mathcal{O}_K) f}{[\mathcal{O}_K^* : \mathcal{O}_f^*]} \prod_{p \mid f} \left(1 - \left(\frac{d_K}{p}\right) \frac{1}{p}\right) \tag{1.3.2}$$

Here, d_K denotes the discriminant of the number field K, $\mathcal{O}_K^*$ denotes the group of units of the ring of integers $\mathcal{O}_K$ of K, and $\mathcal{O}_f^*$ denotes the invertible elements of the order $\mathcal{O}_f$.

The group $\mathcal{O}_K^*$ consists of the elements in $\mathcal{O}_K$ of norm ± 1, namely $\{\pm 1, \pm\omega, \pm\omega^2\}$, so that $|\mathcal{O}_K^*| = 6$. For any conductor $f \in \{3, 9, 3p, 9p\}$, the units of the order $\mathcal{O}_f$ are $\mathcal{O}_f^* = \{\pm 1\}$. This yields $[\mathcal{O}_K^* : \mathcal{O}_f^*] = 3$.

We now compute the Legendre symbol $\left(\frac{d_K}{q}\right)$ for $q \in \{3, p\}$ and $d_K = -3$ to be $\left(\frac{-3}{3}\right) = 0$ and $\left(\frac{-3}{p}\right) = 1$. For the second value we used the fact that $p \equiv 1 \pmod 3$.

Plugging what we obtained into 1.3.2 gives the class numbers in the statement. □

Recall that by Proposition 0.3.12, if $f_1 \mid f_2$ are conductors of orders in K, then there is an inclusion between the respective ring class fields $H_{f_1} \subseteq H_{f_2}$. This, together with Proposition 1.3.1 tells us that there is the diagram of abelian extensions of K shown in Figure 1.2.

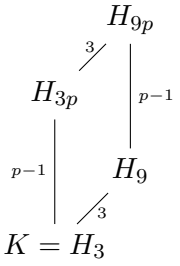

Figure 1.2: Diagram of ring class fields H_f of K of conductor $f \in \{3, 9, 3p, 9p\}$

Now, we would like to better understand how the cubic extension L/K for $L = K(\sqrt[3]{p})$ fits into the diagram of Figure 1.2.

Proposition 1.3.3. *It holds that* $L = K(\sqrt[3]{p}) \subseteq H_{3p}$.

Proof. The field extension L/K is abelian, as $\mathrm{Gal}(L/K) \cong \mathbb{Z}/3\mathbb{Z}$. Denote by $\mathfrak{f}$ its conductor. Since $L = \sqrt[3]{1^2 \cdot p}$, and $p^2 \not\equiv 1 \pmod 9$ for $p \equiv 4, 7 \pmod 9$, Theorem 0.3.8 implies that $\mathfrak{f} = 3p$.

Recall that we denote by $I_K(\mathfrak{f})$ the group of fractional ideals of $\mathcal{O}_K$ that are prime to $\mathfrak{f}$, and we denote by $P_{K,1}(\mathfrak{f})$ the group of principal ideals $\alpha\mathcal{O}_K$ generated by an element $\alpha \equiv 1 \bmod^* \mathfrak{f}$. By class field theory, there is a group J such that $P_{K,1}(3p) \subseteq J \subseteq I_K(3p)$ and such that $\mathrm{Gal}(L/K) \cong I_K(3p)/J$. Thus, we can write $I_K(3p)/J = \langle [\mathfrak{c}] \mid [\mathfrak{c}]^3 = 1 \rangle$, for $[\mathfrak{c}]$ the class of a fractional ideal $\mathfrak{c}$ prime to $3p$ not lying in J.

Let $[\mathfrak{c}]$ be a nontrivial class in $I_K(3p)/J$. Consider the class of the conjugate of the ideal $\mathfrak{c}$, $[\overline{\mathfrak{c}}]$. This is still a nontrivial class in $I_K(3p)/J$, so it must be equal to either $[\mathfrak{c}]$ or $[\mathfrak{c}^{-1}]$. If $[\overline{\mathfrak{c}}] = [\mathfrak{c}^{-1}]$, then we would have that $L = \mathbb{Q}(\sqrt[3]{p}, \sqrt{-3})$ is an abelian extension of $\mathbb{Q}$. But this is false, as $\mathrm{Gal}(L/\mathbb{Q}) \cong S_3$. Hence, $[\overline{\mathfrak{c}}] = [\mathfrak{c}^{-1}]$.

Recall the notation $P_{K,\mathbb{Z}}(3p) = \{\alpha\mathcal{O}_K \mid \exists\, a \in \mathbb{Z}, (a, 3p) = 1 : \alpha \equiv a \pmod{3p\mathcal{O}_K}\}$.

Let $\mathfrak{a} = \alpha\mathcal{O}_K \in P_{K,\mathbb{Z}}(3p)$, where $\alpha = a + 3px$ for some integer a coprime to $3p$ and some $x \in \mathcal{O}_K$. Then, $\overline{\alpha} = a + 3p\overline{x} \equiv \alpha \pmod{3p\mathcal{O}_K}$. Consider the class $[\mathfrak{a}]$ in $I_K(3p)/J$, and assume it is non-trivial. Since $[\overline{\mathfrak{a}}] = [\mathfrak{a}]$, we deduce $[\mathfrak{a}] = [\mathfrak{a}^{-1}]$, contradicting the assumption that $[\mathfrak{a}]$ is non-trivial. Therefore, $\mathfrak{a}$ must lie in J. As this holds for any $\mathfrak{a} \in P_{K,\mathbb{Z}}(3p)$, it follows that $P_{K,\mathbb{Z}}(3p) \subseteq J$.

Actions in the Galois group $\mathrm{Gal}(K^{\mathrm{ab}}/H_{3p})$ correspond to ideals in $P_{K,\mathbb{Z}}(3p)$, while actions in the Galois group $\mathrm{Gal}(K^{\mathrm{ab}}/L)$ corresponds to ideals in J. Applying the fundamental theorem of Galois theory to $P_{K,\mathbb{Z}}(3p) \subseteq J$ we conclude that $L \subseteq H_{3p}$. □

In Chapters 2 and 3, we will be considering the following chain of field extensions:

$$\mathbb{Q} \subset K \subset L := K(\sqrt[3]{p}) \subset H_{3p} \subset H_{9p}$$

We would now like to characterize the cubic extension H_{9p}/H_{3p}, as it will be used in Section 2.3 when dealing with the twisting isomorphism from $E_9(H_{9p})$ to $E_1(H_{3p})$.

Proposition 1.3.4. *It holds that* $H_{9p} = H_{3p}(\sqrt[3]{3})$.

Proof. First, we show that $K(\sqrt[3]{3}) \not\subset H_{3p}$.

From Proposition 1.3.1, we know that the extension H_{3p}/K has degree $p - 1$. As $p \equiv 4, 7 \pmod 9$, we have that 3 divides $p - 1$, while 9 does not.

In Proposition 1.3.3 we showed that $K(\sqrt[3]{p}) \subset H_{3p}$. Thus, if we assume, for sake of a contradiction, that $\sqrt[3]{3} \in H_{3p}$, we must have $K(\sqrt[3]{p}, \sqrt[3]{3}) \subset H_{3p}$. The Galois group $\mathrm{Gal}(K(\sqrt[3]{p}), \sqrt[3]{3})/K)$ is isomorphic to the group $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ of order 9, and it is contained in $\mathrm{Gal}(H_{3p}/K)$ of order $p - 1$. This is a contradiction, because 9 does not divide $p - 1$. Hence, $\sqrt[3]{3}$ does not lie in H_{3p}.

Next, we show that $K(\sqrt[3]{3}) \subset H_{9p}$. For this, it suffices to show $K(\sqrt[3]{3}) \subset H_9$, because $H_9 \subseteq H_{9p}$, as shown in the diagram in Figure 1.2.

The field extension $K(\sqrt[3]{3})/K$ is abelian of degree 3. Using Theorem 0.3.8, we see its conductor is $\mathfrak{f}(K(\sqrt[3]{3})/K) = 9$, because $3^2 \not\equiv 1 \pmod 9$.

By class field theory, $\mathrm{Gal}(K(\sqrt[3]{3})/K) \cong I_K(9)/J$, for some subgroup J of $I_K(9)$ containing the ray class group $P_{K,1}(9)$. On the other hand, $\mathrm{Gal}(K(\sqrt[3]{3})/K) \cong \mathbb{Z}/3\mathbb{Z}$, therefore we can write $I_K(9)/J$ as $\langle [\mathfrak{c}] \mid [\mathfrak{c}]^3 = 1 \rangle$ for some fractional ideal $\mathfrak{c}$ coprime to 9 and not belonging to J.

Since $\mathrm{Gal}(K(\sqrt[3]{3})/\mathbb{Q})$ is the symmetric group of order 6, the extension $K(\sqrt[3]{3})/\mathbb{Q}$ is not abelian. This implies that for any nontrivial class $[\mathfrak{c}]$ of $I_K(9)/J$ it holds $[\overline{\mathfrak{c}}] = [\mathfrak{c}^{-1}]$, as shown in the proof of Proposition 1.3.3.

Now, let $\mathfrak{a} = \alpha\mathcal{O}_K \in P_{K,\mathbb{Z}}(9)$, where $\alpha = a + 9x$ for some integer a coprime to 9 and some algebraic integer $x \in \mathcal{O}_K$. Notice that $\overline{\alpha} = a + 9\overline{x} \equiv \alpha \pmod{9\mathcal{O}_K}$. Assume the class $[\mathfrak{a}] \in I_K(9)/J$ is non-trivial. Then, we have $[\mathfrak{a}^{-1}] = [\overline{\mathfrak{a}}] = [\mathfrak{a}]$, in contradiction with $[\mathfrak{a}]$ not being trivial. Hence, $\mathfrak{a}$ must lie in J. It follows that $P_{K,\mathbb{Z}}(9) \subseteq J$.

Morphisms in $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ correspond to ideals in $P_{K,\mathbb{Z}}(9)$, while morphisms in $\mathrm{Gal}(K^{\mathrm{ab}}/K(\sqrt[3]{3}))$ corresponds to ideals in J. By Galois theory, it holds $K(\sqrt[3]{3}) \subseteq H_9$, because $P_{K,\mathbb{Z}}(9) \subseteq J$. In particular, $K(\sqrt[3]{3}) \subseteq H_{9p}$.

Finally, since $\sqrt[3]{3} \in H_{9p} \setminus H_{3p}$ and $[H_{9p} : H_{3p}] = 3$, we can conclude that we have the identity $H_{9p} = H_{3p}(\sqrt[3]{3})$. □

Putting Figure 1.2, Proposition 1.3.3 and Proposition 1.3.4 together, we have the following field diagram:

$$
\begin{array}{c}
H_{9p} = H_{3p}(\sqrt[3]{3}) \\
{\scriptstyle 3}\,| \\
H_{3p} \\
{\scriptstyle (p-1)/3}\,| \\
L = K(\sqrt[3]{p}) \\
{\scriptstyle 3}\,| \\
K = \mathbb{Q}(\omega) \\
{\scriptstyle 2}\,| \\
\mathbb{Q}
\end{array}
$$

Figure 1.3: Diagram of field extensions used to construct a rational point on E_p and E_{p^2}

To conclude this section, we provide a group that is isomorphic to the Galois group of field extensions of the form H_f/K for H_f the ring class field of K of conductor f.

By class field theory, there is an isomorphism between the ring class group of the order $\mathcal{O}_f$ of K of conductor f and the Galois group $\mathrm{Gal}(H_f/K)$ induced by the Artin map: $\mathrm{Gal}(H_f/K) \cong I_K(f)/P_{K,\mathbb{Z}}(f)$.

Using Proposition 0.3.14 and the fact that K has class number 1, we can write the Artin isomorphism as

$$\mathrm{Gal}(H_f/K) \cong (\mathcal{O}_K/f\mathcal{O}_K)^*/((\mathbb{Z}/f\mathbb{Z})^* \times (\mathcal{O}_K^*/\{\pm 1\})) \tag{1.3.5}$$

Chapter 2

Constructing the point on $E_p(\mathbb{Q})$ and $E_{p^2}(\mathbb{Q})$

The aim of this chapter is to construct a rational point on the elliptic curves E_p and E_{p^2}, for p a prime number congruent to 4 or 7 modulo 9. We will be referring to the construction relative to $E_p(\mathbb{Q})$ as "case 1" and to that relative to $E_{p^2}(\mathbb{Q})$ as "case 2". We will be treating the two cases at the same time throughout the chapter.

The starting point of our construction will be the modular curve $X_0(243)$, on which we are going to define a point P_0. The point P_0 yields a point $P \in E_9(\mathbb{C})$ via the modular parametrization $\Phi : X_0(243) \to E_9$ defined in Proposition 1.2.7. After doing this in Section 2.1, we will use Section 2.2 to show that P lies in $E_9(H_{9p})$. The rest of the chapter will be devoted to the steps illustrated in Figure 1, to reach $E_p(\mathbb{Q})$ and $E_{p^2}(\mathbb{Q})$ using twisting isomorphisms and taking traces of points.

The main reference for Section 2.1 is [7, Section 3.2], while Sections 2.3 and 2.4 refer to [7, Chapter 4]. Section 2.2 is used to prove one result via a method different from the one used by Dasgupta and Voight in [7]. Computations shown in the proofs of this chapter are new compared to what is shown in [7], as computations in the paper are explicitly carried out only in case 2, and we are going to be considering a different starting point for that case.

2.1 Starting from a point on $X_0(243)$

We start by choosing a point P_0 on $X_0(243)(\mathbb{C})$ corresponding to one of the cyclic 243-isogenies in Figure 1.1. The point considered for case 1, which will eventually lead to a point on $E_p(\mathbb{Q})$, is the one used in [7, Section 3.2]. We chose the point P_0 we are considering for case 2, which will yield a point on $E_{p^2}(\mathbb{Q})$, so as to provide original computations compared to those shown in the proofs of [7, Chapter 4].

$$P_0 = \begin{cases} \langle \frac{p\omega}{9} \rangle \to \langle \frac{p\omega+23}{27} \rangle = \langle \frac{p\omega-4}{27} \rangle, & \text{in case 1;} \\ \langle \frac{p\omega+3}{9} \rangle \to \langle \frac{p\omega+17}{27} \rangle = \langle \frac{p\omega-10}{27} \rangle, & \text{in case 2.} \end{cases} \tag{2.1.1}$$

Recall that we are denoting by $\langle\tau\rangle$ elliptic curves of the form $\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z})$, for $\tau\in\mathcal{H}$.

Now that we have defined a point $P_0\in X_0(243)(\mathbb{C})$, we use the modular parametrization $\Phi: X_0(243)\to E_9$ from Proposition 1.2.7 to obtain a point

$$P:=\Phi(P_0)\in E_9(\mathbb{C}). \tag{2.1.2}$$

In the rest of this section, we find a representative in $\mathcal{H}$ for the point P_0. To do so, we are going to use the moduli interpretation of $Y_0(243)$, and renormalize the isogenies defining P_0.

Lemma 2.1.3. *Referring to the cases described in (2.1.1), the point $P_0\in X_0(243)(\mathbb{C})$ is represented in $\mathcal{H}$ by*

$$\tau=\begin{cases}\begin{pmatrix}2&-1\\9&-4\end{pmatrix}\left(\frac{p\omega}{9}\right), & \text{in case 1;}\\ \begin{pmatrix}2&-3\\9&-13\end{pmatrix}\left(\frac{p\omega+3}{9}\right), & \text{in case 2.}\end{cases} \tag{2.1.4}$$

Proof. This proof is based on that of [7, Lemma 3.2.4].

Recall that by Theorem 1.2.10, each point $\Gamma_0(243)\tau$ in $Y_0(243)(\mathbb{C})\cong\Gamma_0(243)\setminus\mathcal{H}$ corresponds to the isogeny $\phi_\tau:\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z})\to\mathbb{C}/(\mathbb{Z}+243\tau\mathbb{Z})$, defined by $z\mapsto 243z$. The kernel of ϕ_τ is generated by $1/243+(\mathbb{Z}+\tau\mathbb{Z})$. Therefore, to find a complex number τ in the upper half plane representing P_0, we need to normalize the isogenies defining P_0 in (2.1.1) to obtain an isogeny of the form ϕ_τ.

Case 1.

The point P_0 corresponds to the isogeny $\phi:\langle p\omega/9\rangle\to\langle(p\omega-4)/27\rangle$. Notice that ϕ is defined by $z\mapsto 9z$, as it is given by the following composition:
$\left\langle\frac{p\omega}{9}\right\rangle\xrightarrow{z\mapsto 3z}\left\langle\frac{p\omega}{3}\right\rangle\xrightarrow{z\mapsto 3z}\langle p\omega\rangle\xrightarrow{z\mapsto z}\left\langle\frac{p\omega+2}{3}\right\rangle\xrightarrow{z\mapsto z}\left\langle\frac{p\omega+5}{9}\right\rangle\xrightarrow{z\mapsto z}\left\langle\frac{p\omega-4}{27}\right\rangle$.

Therefore, the kernel of ϕ is generated by $\frac{1}{9}\frac{p\omega-4}{27}=\frac{p\omega-4}{243}$ modulo $\mathbb{Z}+\frac{p\omega}{9}\mathbb{Z}$.

We wish to find a matrix $M=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\mathrm{SL}_2(\mathbb{Z})$ that makes the following diagram commute.

$$\begin{array}{ccc}\langle p\omega/9\rangle & \xrightarrow{z\mapsto 9z} & \langle(p\omega-4)/27\rangle\\ {\scriptstyle z\mapsto\frac{z}{c(p\omega/9)+d}}\downarrow & & \downarrow{\scriptstyle z\mapsto\frac{27z}{c(p\omega/9)+d}}\\ \langle M(p\omega/9)\rangle & \xrightarrow{z\mapsto 243z} & \langle 243M(p\omega/9)\rangle\end{array}$$

The vertical map on the left is an invertible isogeny of elliptic curves over $\mathbb{C}$, because $\alpha=(c(p\omega/9)+d)\in\mathbb{C}^*$ is such that $\alpha(\mathbb{Z}+M(p\omega/9)\mathbb{Z})=\mathbb{Z}+(p\omega/9)\mathbb{Z}$. Indeed, given $n,m\in\mathbb{Z}$, there exist unique $x,y\in\mathbb{Z}$ such that $\alpha\left(n+mM\left(\frac{p\omega}{9}\right)\right)=x+y\frac{p\omega}{9}$, under the requirement $M\in\mathrm{SL}_2(\mathbb{Z})$. The vertical map on the right is holomorphic over $\mathbb{C}$ and makes the diagram commute. It is also an invertible isogeny once we require that a generator for $\ker\phi$ is mapped to $\frac{1}{243}+(\mathbb{Z}+M(p\omega/9)\mathbb{Z})$ under multiplication by α^{-1}.

Let's check that the matrix $M = \begin{pmatrix} 2 & -1 \\ 9 & -4 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ satisfies this last condition. The generator $\frac{p\omega-4}{243} + (\mathbb{Z} + (p\omega/9)\mathbb{Z}) \in \ker\phi$ is mapped to $\frac{(p\omega-4)/243}{9(p\omega/9)-4} + (\mathbb{Z} + M(p\omega/9)\mathbb{Z}) = \frac{1}{243} + (\mathbb{Z} + M(p\omega/9)\mathbb{Z})$, as required.

Case 2.

The isogeny ϕ corresponding to P_0 can be decomposed as $\langle\frac{p\omega+3}{9}\rangle \to \langle p\omega\rangle \to \langle\frac{p\omega-10}{27}\rangle$. Therefore, ϕ is defined by $z \mapsto 9z$. Then, $\ker\phi$ is generated by $\frac{p\omega-10}{243}$ modulo $\mathbb{Z} + \frac{p\omega+6}{9}\mathbb{Z}$. The diagram to be satisfied in this case is:

$$\begin{array}{ccc} \langle (p\omega+3)/9\rangle & \xrightarrow{z\mapsto 9z} & \langle (p\omega-10)/27\rangle \\ {\scriptstyle z\mapsto \frac{z}{c((p\omega+3)/9)+d}}\downarrow & & \downarrow{\scriptstyle z\mapsto \frac{27z}{c((p\omega+3)/9)+d}} \\ \langle M((p\omega+3)/9)\rangle & \xrightarrow{z\mapsto 243z} & \langle 243M((p\omega+3)/9)\rangle \end{array}$$

We check that $M = \begin{pmatrix} 2 & -3 \\ 9 & -13 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ gives the correct action on the kernel, which ensures that the vertical maps are invertible isogenies.

The generator of $\ker\phi$, $\frac{p\omega-10}{243} + (\mathbb{Z} + ((p\omega+3)/9)\mathbb{Z})$ is sent to $\frac{(p\omega-10)/243}{9((p\omega+3)/9)-13} = \frac{1}{243}$ modulo $\mathbb{Z} + ((p\omega+3)/9)\mathbb{Z})$, which is the required generator. □

2.2 $P \in E_9(H_{9p})$

The goal of this section is to prove that $P \in E_9(H_{9p})$. To do so, we will check that $P_0 \in X_0(243)(H_{9p})$, by showing that the point P_0 is invariant under any action in $\mathrm{Gal}(K^{\mathrm{ab}}/H_{9p})$ using Shimura's reciprocity law from Theorem 0.3.21.

Proposition 2.2.1. *For the point P_0 defined in (2.1.1) it holds that $P_0 \in X_0(243)(H_{9p})$.*

Proof. In order to apply Shimura's reciprocity law, we first need to identify which CM point $[z, g] \in Y_0(243)$ we are considering.

In Lemma 2.1.3 we showed we could represent the point $P_0 \in Y_0(243)$ by some $\tau \in \mathcal{H}$. To make computations easier, instead of working with $P_0 = [\tau, 1]$, we will work with $[\omega, g]$, for an appropriate choice of $g \in \mathrm{GL}_2^+(\mathbb{Q})$. We have that such $[\omega, g]$ is a CM point of $Y_0(243)$, because ω lies in the imaginary quadratic field K. The minimal polynomial of ω is $X^2 + X + 1$, therefore the morphism $g_\omega : \mathbb{A}_{K,f}^* \to \mathrm{GL}_2(\widehat{Z})$ defined in (0.3.20) maps a finite idèle x of the form $(\alpha)_{v\nmid\alpha}$ for $\alpha = s\omega + t$ to $g_\omega(x) = \begin{pmatrix} t-s & -s \\ s & t \end{pmatrix}_{v\nmid(\alpha)}$.

We also need to describe in terms of idèles the Galois actions we need.

The Galois actions in $\mathrm{Gal}(K^{\mathrm{ab}}/H_{9p})$ correspond to the ideals in the group $P_{K,\mathbb{Z}}(9p)$, which is generated by principal $\mathcal{O}_K$-ideals (α), where $\alpha \in \mathcal{O}_K$ satisfies $\alpha \equiv a \mod 9p\mathcal{O}_K$ for some integer a relatively prime to $9p$. Without loss of generality, we can write $\alpha = a + 9pb\omega$ for some $a, b \in \mathbb{Z}$ such that $(a, 9p) = 1$. To such α we associate the finite idèle $x = (\alpha)_{v\nmid\alpha}$. Then, $g_\omega(x) = \begin{pmatrix} a-9pb & -9pb \\ 9pb & a \end{pmatrix}_{v\nmid(\alpha)}$.

If we denote by σ_x the Galois action in $\mathrm{Gal}(K^{\mathrm{ab}}/H_{9p})$ corresponding to the idèle x, Shimura's reciprocity law tells us that $\sigma_x^{-1}[\omega, g] = [\omega, g_\omega(x)g]$.

As we have to check that $[\omega, g]$ is invariant under all actions in $\mathrm{Gal}(K^{\mathrm{ab}}/H_{9p})$, we can equivalently show that for every idèle $x = (\alpha)_{v\nmid\alpha}$ with $\alpha\mathcal{O}_K \in P_{K,\mathbb{Z}}(9p)$ it holds $[\omega, g] = [\omega, g_\omega(x)g]$. As $g \in \mathrm{GL}_2^+(\mathbb{Q})$, it suffices to show that, for every such idèle x, $g^{-1}g_\omega(x)g$ belongs to $\mathcal{K} = \prod_{v\neq 3}\mathrm{GL}_2(\mathbb{Z}_v) \times \left\{\begin{pmatrix} a & b \\ c & d\end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_3) : 243|c\right\}$.

Now, we proceed to prove this for $P_0 = [\tau, 1]$ as in (2.1.4). Recall that the cases 1 and 2 refer to the fact that P_0 will eventually yield a point on $E_p(\mathbb{Q})$ and $E_{p^2}(\mathbb{Q})$, respectively.

Case 1.

We have $\tau = \begin{pmatrix} 2 & -1 \\ 9 & -4\end{pmatrix}\left(\frac{p\omega}{9}\right)$. Then, $[\tau, 1] = [\omega, g]$ for $g = \begin{pmatrix} -4/p & 1/p \\ -1 & 2/9\end{pmatrix}$. We also note that $g^{-1} = \begin{pmatrix} 2p & -9 \\ 9p & 36\end{pmatrix}$.

Let (α) be an ideal of $P_{K,\mathbb{Z}}$, with $\alpha = a + 9pb$ for a, b integers such that a and $9p$ are coprime. For $x = (\alpha)_{v\nmid\alpha}$ we need to prove that $g^{-1}g_\omega(x)g \in \mathcal{K}$.

If $v|(\alpha)$, then certainly $v \neq 3$. We have $(g^{-1}g_\omega(x))g)_v = g^{-1}g = 1 \in \mathrm{GL}_2(\mathbb{Z}_v)$.

If $v \nmid (\alpha)$, in particular $v \nmid \mathrm{Nm}(\alpha) = \det((g_\omega(x))_v)$. Then, $(g^{-1}g_\omega(x)g)_v$ becomes

$$\begin{pmatrix} 2p & -9 \\ 9p & 36\end{pmatrix}\begin{pmatrix} a - 9pb & -9pb \\ 9pb & a\end{pmatrix}\begin{pmatrix} -4/p & 1/p \\ -1 & 2/9\end{pmatrix} = \begin{pmatrix} a + 2^2 3^4 b + 2^3 3^2 pb + 2\cdot 3^2 p^2 b & -3^4 b - 2\cdot 3^2 pb - 2^2 p^2 b \\ 2^4 3^4 b + 2^2 3^4 pb + 3^4 p^2 b & a - 2^2 3^4 b - 3^4 pb - 2\cdot 3^2 p^2 b\end{pmatrix}$$

The matrix has all entries in $\mathbb{Z}_v$ and is invertible, as the determinant is coprime with v. This happens in particular when $v = p \nmid 243$: we see that the determinant lies in $a^2 + p\mathbb{Z}_p$, but $(a, p) = 1$. Thus the matrix belongs to $\mathrm{GL}_2(\mathbb{Z}_v)$.

At $v \mid 3$, we have to check that the bottom left entry is a multiple of 243. Recalling that $p \equiv 1 \pmod 3$, we have $2^4 3^4 b + 2^2 3^4 pb + 3^4 p^2 b = 3^4 b(16 + 4p + p^2) \equiv 0 \pmod{243}$.

We conclude that in case 1, the point $P_0 = [\tau, 1]$ is invariant under $\mathrm{Gal}(K^{\mathrm{ab}}/H_{9p})$.

Case 2.

Now, from $\tau = \begin{pmatrix} 2 & -3 \\ 9 & -13\end{pmatrix}\left(\frac{p\omega+3}{9}\right)$, writing $[\tau, 1] = [\omega, g]$, we find $g = \begin{pmatrix} -10/p & 7/3p \\ -1 & 2/9\end{pmatrix}$. We note that $g^{-1} = \begin{pmatrix} 2p & -21 \\ 9p & -90\end{pmatrix}$.

As in the previous case, we are going to show that $g^{-1}g_\omega(x)g \in \mathcal{K}$ for all $x = (\alpha)_{v\nmid\alpha}$ with $(\alpha) = (a + 9pb\omega)$.

If $v|(\alpha)$, in particular $v \neq 3$. As before, we have $(g^{-1}g_\omega(x)g)_v = g^{-1}g = 1 \in \mathrm{GL}_2(\mathbb{Z}_v)$.

If $v \nmid (\alpha)$, then $v \nmid \mathrm{Nm}(\alpha) = \det(g^{-1}g_\omega(x)g)$. We compute $(g^{-1}g_\omega(x)g)_v$ to be

$$\begin{pmatrix} 2p & -21 \\ 9p & -90 \end{pmatrix} \begin{pmatrix} a-9pb & -9pb \\ 9pb & a \end{pmatrix} \begin{pmatrix} -10/p & 7/3p \\ -1 & 2/9 \end{pmatrix} = \\ \begin{pmatrix} a + 2\cdot 3^3 5\cdot 7b + 3^3 7pb + 23^2p^2b & -3^2 7^2 b - 2\cdot 3\cdot 7pb - 2^2p^2b \\ 2^2 3^4 5^2 b + 2\cdot 3^4 5pb + 3^4 p^2 b & a - 2\cdot 3^3 5\cdot 7b - 3^3 7pb - 23^2p^2b \end{pmatrix}$$

In this case as well, the determinant is coprime with v, in particular when $v = p$, as it lies in $a^2 + p\mathbb{Z}_p$, so it is a unit in $\mathbb{Z}_p$. It follows that the matrix is in $\mathrm{GL}_2(\mathbb{Z}_v)$.

Looking at $v \mid 3$, we check that the bottom left entry is a multiple of 243. Using $p \equiv 1 \pmod 3$, we see that $2^2 3^4 5^2 b + 2\cdot 3^4 5pb + 3^4 p^2 b = 3^4 b(100 + 10p + p^2) \equiv 0 \pmod{243}$.

Hence, also in case 2, the point $P_0 = [\tau, 1]$ lies in $X_0(243)(H_{9p})$. □

2.3 From $E_9(H_{9p})$ to $E_1(K(\sqrt[3]{p}))$

In this section, we will first obtain a point in $E_1(H_{3p})$ from the point P we have defined in $E_9(H_{9p})$. This will be shown in Corollary 2.3.4, using the twisting isomorphism defined in Proposition 2.3.1. Afterwards, taking the trace over the field extension $H_{3p}/K(\sqrt[3]{p})$, we will produce a point in $E_1(K(\sqrt[3]{p}))$.

As shown in Proposition 1.3.4, we have $H_{9p} = H_{3p}(\sqrt[3]{3})$, so H_{9p}/H_{3p} is a Galois extension with $\mathrm{Gal}(H_{9p}/H_{3p}) \cong \mathbb{Z}/3\mathbb{Z}$. Pick the generator $\rho \in \mathrm{Gal}(H_{9p}/H_{3p})$ such that $\rho(\sqrt[3]{3}) = \omega\sqrt[3]{3}$.

The following proposition is a case of cubic twisting. It tells us that once we are able to prove that $P^\rho = \omega P$, which will be done in Proposition 2.3.2, we can twist P to a point of $E_1(H_{3p})$.

Proposition 2.3.1. *Consider the elliptic curves $E_9 : y^2 + y = x^3 - 1$ and $E_1 : y^2 + y = 3x^3 - 1$. There is an isomorphism*

$$\{X \in E_9(H_{9p}) : \rho(X) = \omega X\} \to E_1(H_{3p})$$
$$(x, y) \mapsto \left(\frac{x}{\sqrt[3]{3}}, y\right)$$

Proof. A point $(x, y) \in E_9(H_{9p})$ can be written as $(x_0 + x_1\sqrt[3]{3} + x_2\sqrt[3]{9}, y_0 + y_1\sqrt[3]{3} + y_2\sqrt[3]{9})$ for $x_i, y_i \in H_{3p}$. Then, $\rho(x, y) = (x_0 + x_1\omega\sqrt[3]{3} + x_2\omega^2\sqrt[3]{9}, y_0 + y_1\omega\sqrt[3]{3} + y_2\omega^2\sqrt[3]{9})$.

On the other hand, recall that $\omega(x, y) = (\omega x, y)$. We deduce that $\rho(x, y) = \omega(x, y)$ if and only if $x_0 = x_2 = y_1 = y_2 = 0$. Thus, the claim can be restated as the existence of an isomorphism $\{(x_1\sqrt[3]{3}, y_0) \in E_9(H_{9p}) : x_1, y_0 \in H_{3p}\} \to E_1(H_{3p})$, which is given by $(x_1\sqrt[3]{3}, y_0) \mapsto (x_1, y_0)$.

Now, it is clear that $(x_1\sqrt[3]{3}, y_0)$ lies on $E_9(H_{9p})$ if and only if $y_0^2 + y_0 = 3x_1^3 - 1$, if and only if (x_1, y_0) is in $E_1(H_{3p})$. This concludes our proof. □

Proposition 2.3.2. *For $P \in E_9(H_{9p})$ as defined in (2.1.2), we have $P^\rho = \omega P$.*

Proof. This proof is based on that of [7, Proposition 4.3.3].

The key idea behind the proof is to compute the Galois conjugate of P using Shimura's reciprocity law, and then to compare it with the action of the modular automorphisms of $X_0(243)$, which we have computed explicitly in Proposition 1.2.8.

First of all, we need to find the element $\alpha_\rho \in \mathcal{O}_K$ corresponding to ρ under the Artin isomorphism (1.3.5). As $\rho \in \mathrm{Gal}(H_{9p}/H_{3p})$, it has to fix H_{3p}. This means α_ρ has to satisfy $\alpha_\rho \equiv a \pmod{3p\mathcal{O}_K}$ for some $a \in (\mathbb{Z}/3p\mathbb{Z})^* \times (\mathcal{O}_K^*/\{\pm 1\})$. Next, we can look at what element of $\mathcal{O}_K$ gives the action $\sqrt[3]{3} \mapsto \omega\sqrt[3]{3}$ inside $H_9 = K(\sqrt[3]{3})$, and then lift it to the element we need for H_{9p}. Let $\overline{\rho} \in \mathrm{Gal}(H_9/K)$ such that $\overline{\rho}(\sqrt[3]{3}) = \omega\sqrt[3]{3}$. Consider $\beta = 1 + 3\omega \in \mathcal{O}_K$. The ideal $\beta\mathcal{O}_K$ is prime and it is inert in H_9. As $\overline{\rho}(\beta) = \beta$, we have that $\overline{\rho}(\beta\mathcal{O}_{H_9}) = \beta\mathcal{O}_{H_9}$. It holds $\sqrt[3]{3}^{\mathrm{Nm}(\beta)-1} \equiv (-1/\omega)^{\frac{7-1}{3}} = (-\omega^2)^2 = \omega \pmod{\beta}$. It follows that β corresponds to $\overline{\rho}$ under the Artin isomorphism. We need to require $\alpha_\rho \equiv \beta \pmod{9\mathcal{O}_K}$. As $p \equiv 1 \pmod 3$, the choice $\alpha_\rho = 1 + 3p\omega$ satisfies $\alpha \equiv 1 \pmod{3p\mathcal{O}_K}$ and $\alpha \equiv \beta \pmod{9\mathcal{O}_K}$. Recall that in order to use Shimura's reciprocity law, we also need the inverse of $\alpha_\rho\mathcal{O}_K$ in the ring class group of conductor $9p$. Notice that $(1 + 3p\omega)(1 + 3p\omega^2) \equiv 1 - 3p \pmod{9p\mathcal{O}_K}$, and $1 - 3p$ is an integer coprime with $9p$. It follows that $(\alpha_\rho\mathcal{O}_K)^{-1} = (1 + 3p\omega^2)$. We note that the norm of the $\mathcal{O}_K$-ideal generated by α_ρ is $1 - 3p + 9p^2$, and that the ideal generated by $1 + 3p\omega^2$ has the same norm.

Therefore, the idèle we neeed to consider when applying Shimura's reciprocity law is $x = (1 + 3p\omega^2)_{v\nmid 1-3p+9p^2}$. To x we associate the matrix

$$g_\omega(x) = \begin{pmatrix} 1 & 3p \\ -3p & 1 - 3p \end{pmatrix}_{v\nmid 1-3p+9p^2} \in \mathrm{GL}_2(\widehat{\mathbb{Z}}) \tag{2.3.3}$$

Now, we proceed to compute the action of ρ on the point $P_0 = [\tau, 1] \in Y_0(243)$, for τ defined in Lemma 2.1.3. We are also going to compare the resulting conjugate to the modular autormorphisms of $X_0(243)$ from Proposition 1.2.8. We split the rest of the proof into the two cases for which we defined P_0. Recall that the first case is relative to the point used in the construction of a rational point on E_p, whereas the second case is needed for the construction on E_{p^2}.

Case 1.

We write $P_0 = [\tau, 1] = [\omega, A^{-1}]$, for $A := \begin{pmatrix} 2p & -9 \\ 9p & -36 \end{pmatrix}$.

Using $g_\omega(x) \in \mathrm{GL}_2(\widehat{\mathbb{Z}})$ defined in (2.3.3), we have that the action of ρ on P_0 is given by Shimura's reciprocity law: $\rho([\tau, 1]) = \left[\omega, g_\omega(x)A^{-1}\right]$.

We claim that the point $[B\omega, 1] \in Y_0(243)$, for $B := \begin{pmatrix} -p & -15 \\ 9p & 123 \end{pmatrix}$, is $\rho([\tau, 1])$. The point $[B\omega, 1] \in Y_0(243)$ corresponds to the cyclic 243-isogeny $\langle \frac{p\omega+6}{9} \rangle \to \langle \frac{p\omega+14}{27} \rangle$ in Figure 1.1.

To prove $\rho[\omega, A^{-1}] = [B\omega, 1]$, it suffices to show that $Bg_\omega(x)A^{-1} \in \mathrm{GL}_2(\mathbb{A}_{\mathbb{Q},f})$ lies in $\mathcal{K} = \prod_{v\neq 3} \mathrm{GL}_2(\mathbb{Z}_v) \times \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_3) : 243|c \right\}$.

At places $v|1-3p+9p^2$, in particular $v \neq 3$, using $\det(BA^{-1}) = 1$ and $-13/3 \in \mathbb{Z}_v$, we find that $B(g_\omega(x))_v A^{-1} = BA^{-1} = \begin{pmatrix} 19 & -13/3 \\ -162 & 37 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_v)$.

Now, consider places $v \nmid 1-3p+9p^2$. As $\det(B(g_\omega(x))_v A^{-1}) = 1-3p+9p^2$ is coprime to v, we see $B(g_\omega(x))_v A^{-1} = \begin{pmatrix} 3p^2-45p-161 & \frac{-2p^2+122}{3}+10p \\ -27p^2+378p+1350 & 6p^2-84p-341 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_v)$. Notice that the top right entry lies in $\mathbb{Z}_v$, because $122-2p^2 \equiv 0 \pmod 3$.

If $v = 3$, using the fact that $p = 1+3k$ for some $k \in \mathbb{Z}$, we observe that the bottom left entry of $B(g_\omega(x))_v A^{-1}$ equals $243(7+4k-k^2)$, which is in $243\mathbb{Z}$.

This allows us to conclude that $Bg_\omega(x)A^{-1} \in \mathcal{K}$, as claimed. Hence $\rho([\tau,1]) = [B\omega, 1]$.

Since we are working over $X_0(243)$, we are free to multiply $B\omega$ on the left by a matrix in $\Gamma_0(243)$. We can, thus, consider $M := \begin{pmatrix} 109p & -489 \\ -9162p & 41103 \end{pmatrix}$, which is equivalent to B modulo $\Gamma_0(243)$. Therefore, $P^\rho = \Phi(\Gamma_0(243)M\omega)$, for Φ the modular parametrization from Proposition 1.2.7.

Searching over $\mathrm{MAut}(X_0(243))$, we see that $\overline{M} = \overline{\tilde{w}wv^2}\overline{A}$, where w and v are the matrices defined in Proposition 1.2.3, and $\tilde{w}$ is $v^{-1}wv$. Recall that w and $\tilde{w}$ lie in Σ as in 1.2.6, so their action on E_9 is trivial. We proved in Proposition 1.2.8 that v acts on E_9 by ω^2. Therefore, we have $\Phi(M\omega) = \Phi(\tilde{w}wv^2P_0) = (\omega^2)^2P$.

Putting everything together, we conclude $\rho(P) = \omega P$.

Case 2.

Write $P_0 = [\tau,1] = [A\omega, 1]$ for $A := \begin{pmatrix} 2p & -21 \\ 9p & -90 \end{pmatrix}$.

By Shimura's reciprocity law, the action of ρ on P_0 is given by $\rho([\tau,1]) = [\omega, g_\omega(x)A^{-1}]$, where $g_\omega(x)$ was defined in (2.3.3).

Let $B := \begin{pmatrix} -p & -9 \\ 9p & 72 \end{pmatrix}$. The point $[B\omega, 1] \in Y_0(243)$ corresponds to the cyclic 243-isogeny $\langle \frac{p\omega}{9} \rangle \to \langle \frac{p\omega+8}{27} \rangle$. We claim $\rho([\tau,1]) = [B\omega, 1]$.

As in the previous case, we are going to look at $Bg_\omega(x)A^{-1} \in \mathrm{GL}_2(\mathbb{A}_{\mathbb{Q},f})$ and show it lies in $\mathcal{K}$.

First, consider places $v|1-3p+9p^2$. In particular, v is not 3. Since $\det(BA^{-1}) = 1$ and $-13/3 \in \mathbb{Z}_v$, we have $B(g_\omega(x))_v A^{-1} = BA^{-1} = \begin{pmatrix} -19 & -13/3 \\ -162 & 37 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_v)$.

At places $v \nmid 1-3p+9p^2$, we have that the determinant of $B(g_\omega(x))_v A^{-1}$ is $1-3p+9p^2$, which is coprime to v. Using the fact that $176-2p^2 \equiv 0 \pmod 3$, we find $B(g_\omega(x))_v A^{-1} = \begin{pmatrix} 3p^2-27p-251 & \frac{-2p^2+176}{3}+6p \\ -27p^2+216p+1998 & 6p^2-48p-467 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_v)$.

If $v = 3$, writing $p = 1+3k$ for $k \in \mathbb{Z}$, the bottom left entry of $B(g_\omega(x))_v A^{-1}$ equals $243(9+2k-k^2)$, so it is in $243\mathbb{Z}$.

We conclude that $Bg_\omega(x)A^{-1} \in \mathcal{K}$, and therefore $\rho([\tau,1]) = (B\omega, 1)$, as claimed.

Up to multiplying $B\omega$ on the left by a matrix in $\Gamma_0(243)$, we may consider $M\omega$, for

$M := \begin{pmatrix} 109p & -1143 \\ -9162p & 96075 \end{pmatrix}$. Thus, $P^\rho = \Phi(\Gamma_0(243)B\omega) = \Phi(\Gamma_0(243)M\omega)$, with Φ the modular parametrization from Proposition 1.2.7.

We search over the finite group $\mathrm{MAut}(X_0(243))$, and realize $\overline{M} = \overline{\tilde{w}wv^2A}$, with the matrices w, v and $\tilde{w}$ defined as in Proposition 1.2.3. The conclusion that $P^\rho = \omega P$ follows from this as in the previous case. □

Corollary 2.3.4. *The point $P \in E_9(H_{9p})$ defined in (2.1.2) yields a point $Q \in E_1(H_{3p})$ via cubic twist.*

Proof. This follows immediately from putting Proposition 2.3.1 and Proposition 2.3.2 together. □

Let $L = K(\sqrt[3]{p})$. We would like to obtain a point on $E_1(L)$ taking the trace of the point $Q \in E_1(H_{3p})$, as defined in Proposition 0.1.8.

The field L is perfect, as it has characteristic zero. Moreover, H_{3p}/L is a finite Galois extension, because H_{3p}/K is a finite Galois extension and $K \subset L$. Therefore, there is a well-defined trace map $\mathrm{Tr}_{H_{3p}/L} : E_1(H_{3p}) \to E_1(L)$. We define the point

$$R := \mathrm{Tr}_{H_{3p}/L}\, Q \in E_1(L). \tag{2.3.5}$$

2.4 From $E_1(K(\sqrt[3]{p}))$ to $E_{p^i}(\mathbb{Q})$

In this section, we are finally going to produce a point on $E_{p^i}(\mathbb{Q})$, for $i \in \{1, 2\}$. At first, we are going to obtain a point on $E_{p^i}(K)$. This will be done adding to $R \in E_1(K(\sqrt[3]{p}))$ defined in (2.3.5) a torsion point, and then using the twisting isomorphism in Proposition 2.4.1. Adding a torsion point at this stage is necessary, because, as we will show in Propositions 2.4.2 and 2.4.6, the point R does not itself satisfy the conditions necessary to apply the twisting isomorphism. The point we will have constructed on $E_{p^i}(K)$, is going to yield a rational point on the elliptic curve E_{p^i} after taking the trace over the field extension $K/\mathbb{Q}$.

For ease of notation, recall that we are denoting $L = K(\sqrt[3]{p})$.

The field extension L/K is Galois extension with Galois group isomorphic to $\mathbb{Z}/3\mathbb{Z}$. Denote by σ the generator of $\mathrm{Gal}(L/K)$ such that $\sigma(\sqrt[3]{p}) = \omega\sqrt[3]{p}$.

The following proposition is a case of cubic twisting. It says that if we have a point Y on $E_1(L)$ satisfying $Y^\sigma = \omega^i Y$, then we can twist it to a point on $E_{p^i}(K)$, for $i \in \{1, 2\}$. This clarifies why we have been considering two separate cases, for $i = 1$ and $i = 2$.

Proposition 2.4.1. *Consider the elliptic curve E_1 with model $y^2 + y = 3x^3 - 1$, as in (1.1.4), and the elliptic curves E_{p^i} for $i \in \{1, 2\}$, with model $y^2 + y = 3p^i x^3 - 1$, as in (1.1.8). There is an isomorphism:*

$$\begin{aligned} \{X \in E_1(L) : \sigma(X) = \omega^i X\} &\to E_{p^i}(K) \\ (x, y) &\mapsto \left(\frac{x}{\sqrt[3]{p^i}}, y\right) \end{aligned}$$

Proof. Writing $(x,y) \in E_1(L)$ as $(x,y) = (x_0 + x_1\sqrt[3]{p^i} + x_2\sqrt[3]{p^{2i}}, y_0 + y_1\sqrt[3]{p^i} + y_2\sqrt[3]{p^i})$ for $x_j, y_j \in K$, we see that $\sigma(x,y) = \omega(x,y)$ if and only if $x_0 = x_{3-i} = y_1 = y_2 = 0$.

The proposition can be restated as an isomorphism $\{(x_i\sqrt[3]{p^i}, y_0) \in E_1(L) : x_i, y_0 \in K\} \to E_{p^i}(K)$ given by $(x_i\sqrt[3]{p^i}, y_0) \mapsto (x_i, y_0)$.

In the models we are considering for E_1 and E_{p^i} we find that indeed $(x_i\sqrt[3]{p^i}, y_0)$ lies on $E_1(L)$ if and only if $y_0^2 + y_0 = 3p^i x_i^3 - 1$, if and only if (x_i, y_0) is in $E_{p^i}(K)$. □

In Propositions 2.4.2 and 2.4.6 we are going to see what the action of $\sigma \in \mathrm{Gal}(L/K)$ on the point $R \in E_1(L)$ is. The first proposition will deal with case 1, while the second will deal with case 2. Recall that the final point of the construction in case i, $i \in \{1,2\}$, lies in $E_{p^i}(\mathbb{Q})$.

Proposition 2.4.2. *Let $R \in E_1(L)$ obtained as in (2.3.5) from the point $P_0 \in X_0(243)$ considered as in case 1 of (2.1.1). We can compute the action of $\sigma \in \mathrm{Gal}(L/K)$ on R explicitly:*

$$R^\sigma = \omega R + (0, \omega^2). \tag{2.4.3}$$

Proof. This proof is based on that of [7, Proposition 4.4.2].

Recall that, in this case, the point $P_0 \in X_0(243)$ we obtained R from is $[A\omega, 1]$, for $A = \begin{pmatrix} 2p & -9 \\ 9p & -36 \end{pmatrix}$.

We choose $\sigma \in \mathrm{Gal}(H_{9p}/K)$ such that, in addition to the action on $\sqrt[3]{p}$, it satisfies $\sigma(\sqrt[3]{3}) = \sqrt[3]{3}$. This will make it easier later in the proof when we will have to pass through the twisting isomorphism from Proposition 2.3.1.

The proof will follow the same structure as that of Proposition 2.3.2. The main difference is that we have to treat the cases $p \equiv 4 \pmod 9$ and $p \equiv 7 \pmod 9$ separately.

In both of these cases, we are first going to compute the Galois action of σ on the point P_0 we obtained $R \in E_1(L)$ from, and then find which modular automorphism of $X_0(243)$ has the same action on P_0. Proposition 1.2.8 will allow us to conclude that $R^\sigma = \omega R + (0, \omega^2)$.

Case $p \equiv 4 \pmod 9$.

In this case, we can write $p = 4 + 9k$ for some $k \in \mathbb{Z}$.

To apply Shimura's reciprocity law, we first need to find an element $\alpha_\sigma \in \mathcal{O}_K$ corresponding to σ under the Artin isomorphism (1.3.5). Since we want σ to fix $\sqrt[3]{3}$, we require $\alpha_\sigma \equiv a \pmod{9\mathcal{O}_K}$, for some $a \in (\mathbb{Z}/9\mathbb{Z})^* \times (\mathcal{O}_K^*/\{\pm 1\})$. As we have shown in Proposition 1.3.3, $\sqrt[3]{p} \in H_{3p}$. Thus, we must also ask $\alpha_\sigma \equiv \beta \pmod{3p\mathcal{O}_K}$, where $\beta\mathcal{O}_K$ corresponds to $\sqrt[3]{p} \mapsto \omega\sqrt[3]{p}$ under the Artin isomorphism (1.3.5). Consider $\beta = 1 + p\omega^2$, nontrivial in $(\mathcal{O}_K/3p\mathcal{O}_K)/((\mathbb{Z}/3p\mathbb{Z})^* \times (\mathcal{O}_K^*/\{\pm 1\}))$. From $p \equiv -1/\omega^2 \pmod\beta$, we see that $\sqrt[3]{p}^{\mathrm{Nm}(\beta)-1} \equiv (-1/\omega^2)^{\frac{1-p+p^2-1}{3}} = (-\omega)^{4+21k+27k^2} = \omega \pmod\beta$, meaning $\sqrt[3]{p}^{\mathrm{Nm}(\beta)} \equiv \omega\sqrt[3]{p} \pmod\beta$. This tells us that β has the required action on $\sqrt[3]{p}$ under the Artin isomorphism. Now, let $\alpha_\sigma = 1 - 2p\omega^2$. Clearly, $\alpha_\sigma \equiv \beta \pmod{3p\mathcal{O}_K}$. Writing $\alpha_\sigma = 1 - 8\omega^2 - 18k\omega^2 \equiv -\omega \pmod{9\mathcal{O}}$, we also see that α_σ fixes $\sqrt[3]{3}$.

Recall that to apply Shimura's reciprocity law, we need to work with the inverse of $\alpha_\sigma\mathcal{O}_K$ inside the ring class group of K of conductor $9p$. Computing $(1-2p\omega^2)(1-2p\omega) =$

$1+9(8+34k+36k^2) \in (\mathbb{Z}/9p\mathbb{Z})^*$, we see that $(\alpha_\sigma \mathcal{O}_K)^{-1}$ is generated by $1-2p\omega$. We note that the norm of $\alpha_\sigma \mathcal{O}_K$ and of its inverse is $1+2p+4p^2$.

Define the idèle $x \in \mathbb{A}_{K,f}^*$ associated to the inverse of $\alpha_\sigma \mathcal{O}_K$ as $x = (1-2p\omega)_{v \nmid 1+2p+4p^2}$.

Therefore, the matrix of the form (0.3.20) we will need to consider to compute the action of σ is

$$g_\omega(x) = \begin{pmatrix} 1+2p & 2p \\ -2p & 1 \end{pmatrix}_{v \nmid 1+2p+4p^2} \in \mathrm{GL}_2(\widehat{\mathbb{Z}}) \tag{2.4.4}$$

By Shimura's reciprocity law, we have $\sigma(P_0) = \sigma([A\omega, 1]) = [\omega, g_\omega(x)A^{-1}]$.

We claim the point $[B\omega, 1] \in X_0(243)$, for $B := \begin{pmatrix} 4p & 7 \\ 9p & 18 \end{pmatrix}$ in $X_0(243)$, is $\sigma(P_0)$. We note that $[B\omega, 1]$ corresponds to the isogeny $\langle \frac{p\omega+4}{9} \rangle \to \langle \frac{p\omega+2}{27} \rangle$ in Figure 1.1.

Let's check this indeed holds by looking at $Bg_\omega(x)A^{-1} \in \mathrm{GL}_2(\mathbb{A}_{\mathbb{Q},f})$ and verifying it lies in $\mathcal{K} = \prod_{v \neq 3} \mathrm{GL}_2(\mathbb{Z}_v) \times \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_3) : 243 | c \right\}$.

Let $v \mid 1+2p+4p^2$. In particular, $v \neq 3$, as $1+2p+4p^2 \equiv 1 \pmod 3$. Using that $\det(BA^{-1}) = 1$ and $50/9 \in \mathbb{Z}_v$, at such v we have $(Bg_\omega(x)A^{-1})_v = BA^{-1} = \begin{pmatrix} -23 & 50/9 \\ -54 & 13 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_v)$.

At places $v \nmid 1+2p+4p^2$, we have that $\det(B(g_\omega(x))_v A^{-1}) = 1+2p+4p^2$ is coprime with v. Since $p \equiv 1 \pmod 3$, it holds. $16p^2 - 76 \equiv 0 \pmod 9$. Thus, we compute $B(g_\omega(x))_v A^{-1} = \begin{pmatrix} -8p^2-32p+33 & \frac{16p^2-76}{9} + 8p \\ -18p^2-72p+90 & 4p^2+18p-23 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_v)$.

If $v = 3$, writing $p = 4+9k$ for $k \in \mathbb{Z}$, the bottom left entry of $B(g_\omega(x))_3 A^{-1}$ becomes $243(-2-8k-6k^2)$, which is in $243\mathbb{Z}$.

This allows us to conclude that $\sigma(P_0) = [B\omega, 1]$. as we claimed.

After multiplying B on the left by a matrix in $\Gamma_0(243)$, we consider $\sigma(P_0) = [M\omega, 1]$, for $M := \begin{pmatrix} 119p & -523 \\ 342p & -1503 \end{pmatrix}$.

Searching over the modular automorphisms of $X_0(243)$, we find that $\overline{M} = \overline{w\tilde{w}t^2}\overline{A}$, where the matrix t was defined in (1.2.4), while w and $\tilde{w}$ were defined in Proposition 1.2.3. Recall that $w\tilde{w}$ lies in Σ as in (1.2.6), so it fixes $P \in E_9(H_{9p})$. Recall from Proposition 1.2.8 that for a point X of E_9, we have $t(X) = \omega^2 X + (0, \omega)$. It follows $\sigma(P) = (\omega^2)^2 P + [2](0,\omega) = \omega P + (0, \omega^2)$.

In Proposition 2.3.1 we obtained $Q \in E_1(H_{3p})$ from $P \in E_9(H_{9p})$ via a cubic twist by $\sqrt[3]{3}$. The Galois action σ was chosen such that $\sigma(\sqrt[3]{3}) = \sqrt[3]{3}$, and $(0, \omega^2)$ is invariant under the twisting isomorphism $E_9(H_{9p}) \to E_1(H_{3p})$, thus we have $\sigma(Q) = \omega Q + (0, \omega^2)$.

Recall that $\mathrm{Gal}(H_{9p}/K)$ is abelian, that $[H_{3p} : L] = (p-1)/3$ and that $(0, \omega^2)$ is a 3-torsion point of $E_1(L)$. Finally, we can compute, using the assumption $p \equiv 4 \pmod 9$, $\sigma(R) = \sum_{\varsigma \in \mathrm{Gal}(H_{3p}/L)} \sigma(\varsigma(Q)) = \sum_\varsigma \varsigma(\sigma(Q)) = \omega \left(\sum_\varsigma \varsigma(Q) \right) + \frac{p-1}{3}(0, \omega^2) = \omega R + (0, \omega^2)$.

This concludes the proof that $R^\sigma = \omega R + (0, \omega^2)$ when $p \equiv 4 \pmod 9$.

Case $p \equiv 7 \pmod 9$.

We can write $p = -2 + 9k$ for some $k \in \mathbb{Z}$.

We proceed to find $\alpha_\sigma \in \mathcal{O}_K$ corresponding to σ under the Artin isomorphism (1.3.5) as we did in the previous case. We require $\alpha_\sigma \equiv a \pmod{9\mathcal{O}_K}$, for some $a \in (\mathbb{Z}/9\mathbb{Z})^* \times (\mathcal{O}_K^*/\{\pm 1\})$, and $\alpha_\sigma \equiv \beta \pmod{3p\mathcal{O}_K}$, for $\beta\mathcal{O}_K$ corresponding to $\sqrt[3]{p} \mapsto \omega\sqrt[3]{p}$ under the Artin isomorphism for $\mathrm{Gal}(H_{3p}/K)$. Consider again $\beta = 1 + p\omega$, nontrivial in $(\mathcal{O}_K/3p\mathcal{O}_K)/((\mathbb{Z}/3p\mathbb{Z})^* \times (\mathcal{O}_K^*/\{\pm 1\}))$. This time, as $p \equiv -1/\omega \pmod{\beta}$, we have $\sqrt[3]{p}^{\mathrm{Nm}(\beta)-1} \equiv (-1/\omega)^{\frac{1-p+p^2-1}{3}} = (-\omega^2)^{2-15k+27k^2} = \omega \pmod{\beta}$. Thus, β has indeed the required action on $\sqrt[3]{p}$. Set $\alpha_\sigma = 1 + 4p\omega$. We see that $\alpha_\sigma \equiv \beta \pmod{3p\mathcal{O}_K}$. Writing $\alpha_\sigma = 1 - 8\omega + 36k\omega \equiv -\omega^2 \pmod{9\mathcal{O}}$, it becomes clear that α_σ fixes $\sqrt[3]{3}$.

The inverse of $\alpha_\sigma\mathcal{O}_K$ in the ring class group of K of conductor $9p$ is generated by $1+4p\omega^2$. Indeed, we have that $(1+4p\omega)(1+4p\omega^2) = 1+9(8-68k+144k^2) \in (\mathbb{Z}/9p\mathbb{Z})^*$. We note that the norm of $\alpha_\sigma\mathcal{O}_K$ and of its inverse is $1 - 4p + 16p^2$.

Define the idèle $x \in \mathbb{A}_{K,f}^*$ associated to the inverse of $\alpha_\sigma\mathcal{O}_K$ by $x = (1+4p\omega^2)_{v\nmid 1-4p+16p^2}$.

Thus, the matrix of the form (0.3.20) we will consider to determine the action of σ with Shimura's reciprocity law is

$$g_\omega(x) = \begin{pmatrix} 1 & 4p \\ -4p & 1-4p \end{pmatrix} \tag{2.4.5}$$

We proceed as before: by Shimura's reciprocity law, $\sigma(P_0) = \sigma([A\omega, 1]) = \left[\omega, g_\omega(x)A^{-1}\right]$.

We claim that $\sigma(P_0)$ is the point of $X_0(243)$ represented by $B\omega$, for $B := \begin{pmatrix} -9p & 8 \\ 9p & -9 \end{pmatrix}$. The point $[B\omega, 1]$ corresponds to the isogeny $\langle 9p\omega\rangle \to \langle \frac{p\omega-1}{27}\rangle$ in Figure 1.1.

We look at $Bg_\omega(x)A^{-1} \in \mathrm{GL}_2(\mathbb{A}_{\mathbb{Q},f})$ and prove it lies in $\mathcal{K}$.

At places $v|1-4p+16p^2$, using that $-65/9 \in \mathbb{Z}_v$, we find a matrix with coefficients in $\mathbb{Z}_v$ of determinant 1, $BA^{-1} = \begin{pmatrix} 28 & -65/9 \\ -27 & 7 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_v)$.

At places $v \nmid 1 + -4p + 16p^2$, we have that $\det(B(g_\omega(x))_v A^{-1}) = 1 - 4p + 16p^2$ is coprime to v. Using that $64p + 353 \equiv 0 \pmod 9$, we see that $B(g_\omega(x))_v A^{-1} = \begin{pmatrix} 36p^2+32p+156 & -8p^2 - \frac{64p+353}{9} \\ -36p^2-36p-171 & 8p^2+8p+43 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_v)$.

If $v = 3$, recalling $p = -2 + 9k$ for $k \in \mathbb{Z}$, the bottom left entry of $B(g_\omega(x))_3 A^{-1}$ equals $-243(1 - 4k + 12k^2)$, which lies in $243\mathbb{Z}$.

This allows us to conclude that $\sigma(P_0) = [B\omega, 1]$.

Multiplying B on the left by a matrix in $\Gamma_0(243)$, we consider $\sigma(P_0) = [M\omega, 1]$, where $M := \begin{pmatrix} 54p & -233 \\ -4545p & 19611 \end{pmatrix}$.

Searching over $\mathrm{MAut}(X_0(243)$, we find that $\overline{M} = \overline{\tilde{w}wvtA}$, so that, by Proposition 1.2.8, $\sigma(P) = (\omega^2)^2 P + (0, \omega) = \omega P + (0, \omega)$. Thus, $\sigma(Q) = \omega Q + (0, \omega)$.

We compute the action of σ on $R = \mathrm{Tr}_{H_{3p}/L} Q$ using that $[2](0, \omega) = (0, \omega^2)$, and that recalling that we are under the assumption $p \equiv 7 \pmod 9$:
$\sigma(R) = \sum_{\varsigma \in \mathrm{Gal}(H_{3p}/L)} \varsigma(\sigma(Q)) = \omega\left(\sum_\varsigma \varsigma(Q)\right) + \frac{p-1}{3}(0, \omega) = \omega R + (0, \omega^2)$.

This concludes the proof that $R^\sigma = \omega R + (0, \omega^2)$ when $p \equiv 7 \pmod 9$. □

Proposition 2.4.6. *Let $R \in E_1(L)$ obtained as in (2.3.5) from the point $P_0 \in X_0(243)$ considered as in case 2 of (2.1.1). We can compute the action of $\sigma \in \mathrm{Gal}(L/K)$ on R explicitly:*

$$R^\sigma = \omega^2 R + (0, \omega^2). \tag{2.4.7}$$

Proof. We will be referring to the proof of Proposition 2.4.2, as it is very similar.

In this case, the point $P_0 \in X_0(243)$ that R was constructed from is $[A\omega, 1]$, for $A = \begin{pmatrix} -10/p & 7/3p \\ -1 & 2/9 \end{pmatrix}$.

Case $p \equiv 4 \pmod 9$.

We can write $p = 4 + 9k$ for some $k \in \mathbb{Z}$.

The inverse of the Galois action σ corresponds to the finite idèle $x = (1-2p\omega)_{v \nmid 1+2p+4p^2}$. This yields the matrix $g_\omega(x) \in \mathrm{GL}_2(\widehat{\mathbb{Z}})$ as in (2.4.4).

By Shimura's reciprocity law, we have $\sigma(P_0) = \sigma([A\omega, 1]) = [\omega, g_\omega(x)A^{-1}]$.

Let $B := \begin{pmatrix} 4p & 19 \\ 9p & 45 \end{pmatrix}$. We claim that $[B\omega, 1] \in X_0(243)$, corresponding to the 243-isogeny $\langle \frac{p\omega+7}{9} \rangle \to \langle \frac{p\omega+5}{27} \rangle$ in Figure 1.1, satisfies $\sigma(P_0) = [B\omega, 1]$.

We prove this by looking at $Bg_\omega(x)A^{-1} \in \mathrm{GL}_2(\mathbb{A}_{\mathbb{Q},f})$ and showing it lies in the compact subgroup $\mathcal{K} = \prod_{v \neq 3} \mathrm{GL}_2(\mathbb{Z}_v) \times \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_3) : 243 | c \right\}$.

At places $v | 1 + 2p + 4p^2$, we have $v \neq 3$, and so $122/9 \in \mathbb{Z}_v$. Since $\det(BA^{-1}) = 1$, we have $B(g_\omega(x))_v A^{-1} = BA^{-1} = \begin{pmatrix} -59 & 122/9 \\ -135 & 31 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_v)$.

At places $v \nmid 1 + 2p + 4p^2$, we have $\det(B(g_\omega(x))_v A^{-1}) = 1 + 2p + 4p^2$ is coprime with v. Using the fact that $16p^2 + 168p - 676 \equiv 0 \pmod 9$, we have that it holds $B(g_\omega(x))_v A^{-1} = \begin{pmatrix} -8p^2 - 80p + 321 & -\frac{16p^2-168p+676}{9} \\ -18p^2 - 180p + 765 & 4p^2 + 42p - 179 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_v)$.

At $v = 3$, writing $p = 4 + 9k$ for $k \in \mathbb{Z}$, the bottom left entry of $B(g_\omega(x))_3 A^{-1}$ equals $243(-1 - 12k - 6k^2)$, which lies in $243\mathbb{Z}$.

It follows that $\sigma(P_0) = [B\omega, 1]$, as we claimed.

Multiplying B on the left by a matrix in $\Gamma_0(243)$, we consider $\sigma(P_0) = [M\omega, 1]$, for $M := \begin{pmatrix} 1019p & -10687 \\ 2934p & -30771 \end{pmatrix}$.

Searching over $\mathrm{MAut}(X_0(243))$, we find that $\overline{M} = \overline{w\tilde{w}t^2v^2}\overline{A}$ and conclude by Proposition 1.2.8 that $\sigma(P) = (\omega^2)^4 P + [2](0, \omega) = \omega^2 P + (0, \omega^2)$.

Since σ fixes $\sqrt[3]{3}$, we also have $\sigma(Q) = \omega^2 Q + (0, \omega^2)$.

As in Proposition 2.4.2, using the assumption $p \equiv 4 \pmod 9$, we may compute $\sigma(R) = \sum_{\varsigma \in \mathrm{Gal}(H_{3p}/L)} \varsigma(\sigma(Q)) = \omega^2 \left(\sum_\varsigma \varsigma(Q) \right) + \frac{p-1}{3}(0, \omega^2) = \omega^2 R + (0, \omega^2)$.

This concludes the proof that $R^\sigma = \omega^2 R + (0, \omega^2)$ when $p \equiv 4 \pmod 9$.

Case $p \equiv 7 \pmod 9$.

In this case, we can write $p = 7 + 9k$ for some integer k.

Now, the inverse of the Galois action σ corresponds to the idèle $x = (1+4p\omega)_{v \nmid 1-4p+16p^2}$. This yields the matrix $g_\omega(x) \in \mathrm{GL}_2(\widehat{\mathbb{Z}})$ as in (2.4.4).

Applying Shimura's reciprocity law, we have $\sigma(P_0) = \sigma([A\omega, 1]) = [\omega, g_\omega(x)A^{-1}]$.

Let $B := \begin{pmatrix} 3p & -22 \\ 9p & -63 \end{pmatrix}$. We claim that $[B\omega, 1] \in X_0(243)$, corresponding to the 243-isogeny $\langle \frac{3p\omega+2}{3} \rangle \to \langle \frac{p\omega-7}{27} \rangle$ from Figure 1.1, satisfies $\sigma(P_0) = [B\omega, 1]$.

We prove this by checking that $Bg_\omega(x)A^{-1} \in \mathrm{GL}_2(\mathbb{A}_{\mathbb{Q},f})$ lies in $\mathcal{K}$.

If v is a place $v|1-4p+16p^2$, we have $v \neq 3$, and so $-2/9 \in \mathbb{Z}_v$. As $\det(BA^{-1}) = 1$, we obtain $B(g_\omega(x))_v A^{-1} = BA^{-1} = \begin{pmatrix} -8 & 19/9 \\ -27 & 7 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_v)$.

At places $v \nmid 1-4p+16p^2$, we have that $\det(B(g_\omega(x))_v A^{-1}) = 1-4p+16p^2$ is coprime with v. Since $24p^2+176p+1867 \equiv 0 \pmod 9$, we get that $B(g_\omega(x))_v A^{-1} = \begin{pmatrix} -12p^2-88p-88 & \frac{24p^2+176p+1867}{9} \\ -36p^2-252p-2547 & 8p^2+56p+595 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_v)$.

At $v = 3$, the bottom left entry of $(B(g_\omega(x))_3 A^{-1}$ equals $-243(9+4k+12k^2)$, which is in $243\mathbb{Z}$.

It follows that $\sigma(P_0) = [B\omega, 1]$, as claimed.

After we multiply B on the left by a matrix in $\Gamma_0(243)$, we consider $\sigma(P_0) = [M\omega, 1]$ for $M := \begin{pmatrix} 3p & -31 \\ -72p & 747 \end{pmatrix}$.

Searching over $\mathrm{MAut}(X_0(243))$, we find that $\overline{M} \equiv \bar{t}\overline{A}$, and so by Proposition 1.2.8 $\sigma(P) = \omega^2 P + (0, \omega)$. Thus, we also have $\sigma(Q) = \omega^2 Q + (0, \omega)$.

We compute $\sigma(R)$ as in the previous case, under the assumption that $p \equiv 7 \pmod 9$: $\sigma(R) = \sum_{\varsigma \in \mathrm{Gal}(H_{3p}/L)} \varsigma(\sigma(Q)) = \omega^2 \left(\sum_\varsigma \varsigma(Q)\right) + \frac{p-1}{3}(0, \omega) = \omega^2 R + (0, \omega^2)$.

This concludes the proof that $R^\sigma = \omega^2 R + (0, \omega^2)$ when $p \equiv 7 \pmod 9$. □

Recall again that the notation "case i", for $i \in \{1, 2\}$, means that the construction is leading to a point on $E_{p^i}(\mathbb{Q})$. In Propositions 2.4.2 and 2.4.6 we showed that $R^\sigma \in E_1(L)$ is not of the form $\omega^i R$ in case i. Therefore, we cannot apply the twisting isomorphism in Proposition 2.4.1 to $R \in E_1(L)$. To remedy this, we add to R a torsion point, as in the following lemma.

Lemma 2.4.8. *Let $T = (1, -2) \in E_1(\mathbb{Q})_{tors}$ in case 1 and $T = (1, 1) \in E_1(\mathbb{Q})_{tors}$ in case 2. Define the point*

$$Y := R - T \in E_1(L) \tag{2.4.9}$$

Then, $Y^\sigma = \omega^i Y$, and Y twists to a point $Z \in E_{p^i}(K)$.

Proof. In case 1, we set $T = (1, -2) \in E_1(\mathbb{Q})_{\mathrm{tors}}$. It holds $T^\sigma = T = \omega T + (0, \omega^2)$. Thus, $T = (1, -2)$ satisfies the same equation as the point R in case 1, namely (2.4.3).

Similarly, in case 2, $T = (1, 1) \in E_1(\mathbb{Q})_{\mathrm{tors}}$ satisfies $T^\sigma = T = \omega^2 T + (0, \omega^2)$. Thus, $T = (1, 1)$ satisfies the equation (2.4.7), which holds for R in case 2.

Defining the point Y as $R - T$ in case i, for $i \in \{1, 2\}$, we have the chain of equalities $Y^\sigma = R^\sigma - T^\sigma = \omega^i R - \omega^i T = \omega^i Y$.

Therefore, using the cubic twisting isomorphism 2.4.1, we conclude that Y yields a point Z on $E_p(K)$ or $E_{p^2}(K)$, in case 1 or 2, respectively. □

The final step in our construction consists of taking the trace over the finite Galois extension $K/\mathbb{Q}$ of the point Z defined in Lemma 2.4.8. We denote the only nontrivial action of $\mathrm{Gal}(K/\mathbb{Q})$, which is conjugation, by $z \mapsto \overline{z}$. Finally, we can define the point

$$\mathrm{Tr}_{K/\mathbb{Q}}\, Z = Z + \overline{Z} \in E_{p^i}(\mathbb{Q}). \tag{2.4.10}$$

Chapter 3

Checking the point is nontorsion

This chapter is devoted to the proof that we are always able to produce a nontorsion point in $E_{p^i}(\mathbb{Q})$ from the point of $E_{p^i}(\mathbb{Q})$ defined in (2.4.10). We use Section 3.1 to compute in a different way the x-coordinate of the modular parametrization $\Phi : X_0(243) \to E_9$ from Proposition 1.2.7, while the main argument happens in Section 3.2. First, we are going to prove that the point $R \in E_1(K(\sqrt[3]{p}))$, which was defined in (2.3.5), is nontorsion. To do this, we consider the reduction of R modulo p. From there, we are able to deduce that the point $Z \in E_{p^i}(K)$ defined in Lemma 2.4.8 is nontorsion as well. Finally, we see that such Z always yields a nontorsion point in $E_{p^i}(\mathbb{Q})$.

The main reference for this chapter is [7, Chapter 5].

3.1 Rewriting the modular parametrization

In Proposition 1.2.7, we defined the modular parametrization $\Phi : X_0(243) \to E_9$. Recall that the x-coordinate of the parametrization Φ is given by $x(z) = \frac{\eta(9z)\eta(27z)}{\eta(3z)\eta(81z)}$.

Also, recall that the starting point $P_0 \in X_0(243)$ (2.1.1) of the construction of Chapter 2 can be represented by a complex number $\tau \in \mathcal{H}$, as in (2.1.4).

In order to work modulo p in Section 3.2, we would like to rewrite $x(\tau)$ as $g(p\tau_0)$, for some modular function g and some $\tau_0 \in \mathcal{H}$ independent of p.

Consider the complex function defined over $\mathcal{H}$

$$f(z) := \frac{\eta(27z)}{\eta(3z)}. \tag{3.1.1}$$

As $f(z) = \prod_{0<d|81} \eta(dz)^{r_d}$, with $r_{27} = 1$, $r_3 = -1$ and $r_1 = r_9 = r_{81} = 0$, Proposition 0.2.6 tells us that f is a modular function for $X_0(81)$.

Recall that throughout Chapter 2 we distinguished two cases. Case 1 refers to the construction leading to $E_p(\mathbb{Q})$, while case 2 refers to the construction leading to $E_{p^2}(\mathbb{Q})$.

Lemma 3.1.2. *Let $j \in \mathbb{Z}$ such that $jp \equiv 4 \pmod{27}$ in case 1 and $jp \equiv 1 \pmod{27}$ in case 2. Then, for f defined as in (3.1.1),*

$$x(\tau) = e^{\pi i/6}\sqrt{3}\frac{f(p(\omega - j)/27)f(p\omega/9)}{f(p(\omega - j)/9)}$$

Proof. This proof is based on that of [7, Lemma 5.1.3].

We denote $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. The Dedekind η-function satisfies $\eta(T(z)) = \eta(z+1) = e^{\pi i/12}\eta(z)$ and $\eta(S(z)) = \eta(-1/z) = \sqrt{-iz}\eta(z)$, with branch of the square root chosen such that $\sqrt{-iz} = 1$ when $z = i$.

Case 1.

We have $\tau = M\left(\frac{p\omega}{9}\right) \in \mathcal{H}$, for $M = \begin{pmatrix} 2 & -1 \\ 9 & -4 \end{pmatrix}$. Therefore, we find

$$\begin{aligned} 81M\left(\frac{p\omega}{9}\right) &= T^{18}S\left(\frac{p\omega-4}{9}\right), & 9M\left(\frac{p\omega}{9}\right) &= T^2ST^{-4}(p\omega), \\ 27M\left(\frac{p\omega}{9}\right) &= T^6S\left(\frac{p\omega-4}{3}\right), & 3M\left(\frac{p\omega}{9}\right) &= TST^3ST^{-1}\left(\frac{p\omega}{3}\right). \end{aligned}$$

Using the transformation formulas for the Dedekind η-function, we have

$$\begin{aligned} \eta(81\tau) &= e^{3\pi i/2}\sqrt{-i(p\omega-4)/9}\,\eta\left(\frac{p\omega-4}{9}\right), & \eta(9\tau) &= e^{-\pi i/6}\sqrt{-i(p\omega-4)}\,\eta(p\omega), \\ \eta(27\tau) &= e^{\pi i/2}\sqrt{-i(p\omega-4)/3}\,\eta\left(\frac{p\omega-4}{3}\right), & \eta(3\tau) &= \sqrt{-i(p\omega-4)}\,\eta\left(\frac{p\omega}{3}\right). \end{aligned}$$

Substituting into the expression for $x(\tau)$ we find:

$$x(\tau) = e^{5\pi i/6}\sqrt{3}\frac{\eta(p\omega)}{\eta((p\omega-4)/9)}\frac{\eta((p\omega-4)/3)}{\eta(3p\omega)}\frac{\eta(3p\omega)}{\eta((p\omega)/3)}$$

We need to choose $j \in \mathbb{Z}$ such that $jp \equiv 4 \pmod{27}$. If $p \equiv 4 \pmod 9$, then p is congruent to $4, 13$ or 22 modulo 27. We choose $j = 1, -8, 10$ respectively. If $p \equiv 7 \pmod 9$, then p is congruent to $7, 16$ or 25 modulo 27, so we choose $j = -11, 7, -2$, respectively. With these choices, let $k := (4 - jp)/9 \in 3\mathbb{Z}$. Then, $\frac{p\omega-4}{9} = \frac{p(\omega-j)}{9} - k$ and $\frac{p\omega-4}{3} = \frac{p(\omega-j)}{3} - 3k$. Using these substitutions and the fact that $k + jp = k - 9k + 4 \equiv 4 \pmod{24}$, we obtain $\frac{\eta(p\omega)}{\eta((p\omega-4)/9)} = e^{\pi i/3}f(p(\omega-j)/27)$ and $\frac{\eta((p\omega-4)/3)}{\eta(3p\omega)} = e^{-\pi i}\frac{1}{f(p(\omega-j)/9)}$.

Therefore, since $e^{5\pi i/6}e^{\pi i/3}e^{-\pi i} = e^{\pi i/6}$, we obtain the final result:

$$x(\tau) = e^{\pi i/6}\sqrt{3}\frac{f(p(\omega-j)/27)f(p\omega/9)}{f(p(\omega-j)/9)}$$

Case 2:

In this case, $\tau = M\left(\frac{p\omega+3}{9}\right) \in \mathcal{H}$, where $M = \begin{pmatrix} 2 & -3 \\ 9 & -13 \end{pmatrix}$. Therefore, it holds

Using the transformation formulas for the Dedekind η-function, we find

$$\begin{aligned} \eta(81\tau) &= e^{-7\pi i/12}\sqrt{-i(p\omega-10)/9}\,\eta\left(\frac{p\omega-1}{9}\right), & \eta(9\tau) &= e^{-2\pi i/3}\sqrt{-i(p\omega-10)}\,\eta(p\omega), \\ \eta(27\tau) &= e^{\pi i/4}\sqrt{-i(p\omega-10)/3}\,\eta\left(\frac{p\omega-1}{3}\right), & \eta(3\tau) &= e^{-\pi i/6}\sqrt{-i(p\omega-10)}\,\eta\left(\frac{p\omega}{3}\right). \end{aligned}$$

$$81M\left(\frac{p\omega+3}{9}\right)=T^{18}ST^{-1}\left(\frac{p\omega-1}{9}\right),\quad 9M\left(\frac{p\omega+3}{9}\right)=T^2ST^{-10}(p\omega),$$
$$27M\left(\frac{p\omega+3}{9}\right)=T^6ST^{-3}\left(\frac{p\omega-1}{3}\right),\quad 3M\left(\frac{p\omega+3}{9}\right)=TST^3ST^{-3}\left(\frac{p\omega}{3}\right).$$

We can thus rewrite $x(\tau)$ as:

$$x(\tau)=e^{\pi i/3}\sqrt{3}\frac{\eta(p\omega)}{\eta((p\omega-1)/9)}\frac{\eta((p\omega-1)/3)}{\eta(3p\omega)}\frac{\eta(3p\omega)}{\eta((p\omega)/3)}$$

We choose $j\in\mathbb{Z}$ such that $jp\equiv 1 \pmod{27}$. If $p\equiv 4 \pmod 9$, then p is congruent to $4, 13$ or 22 modulo 27. We choose $j=7,-2,-11$ respectively. If $p\equiv 7 \pmod 9$, then p is congruent to $7, 16$ or 25 modulo 27, so we choose $j=4,-5,13$, respectively. With these choices, let $k:=(1-jp)/9\in 3\mathbb{Z}$. Then, $\frac{p\omega-1}{9}=\frac{p(\omega-j)}{9}-k$,and $\frac{p\omega-1}{3}=\frac{p(\omega-j)}{3}-3k$.

We proceed as in the previous case, and use the congruence $k+jp=k-9k+1\equiv 1 \pmod{24}$, to obtain $\frac{\eta(p\omega)}{\eta((p\omega-1)/9)}=e^{\pi i/12}f(p(\omega-j)/27)$ and $\frac{\eta((p\omega-1)/3)}{\eta(3p\omega)}=e^{-\pi i/4}\frac{1}{f(p(\omega-j)/9)}$.

As $e^{\pi i/3}e^{\pi i/12}e^{-\pi i/4}=e^{-\pi i/2}$, plugging everything into the expression for $x(\tau)$ we see:

$$x(\tau)=e^{\pi i/6}\sqrt{3}\frac{f(p(\omega-j)/27)f(p\omega/9)}{f(p(\omega-j)/9)}$$

□

3.2 Reducing the point in $E_1(K(\sqrt[3]{p}))$ modulo p

The objective of this section is to prove that, under the assumption that 3 is not a cube modulo p, the point $R\in E_1(K(\sqrt[3]{p}))$ defined in (2.3.5) is nontorsion. To do this, following the proofs in [7], we are going to show that the reduction modulo p of R does not match the reduction modulo p of any of the points in $E_1(K(\sqrt[3]{p}))_{\text{tors}}$. First, we will determine what the elements of $E_1(K(\sqrt[3]{p}))_{\text{tors}}$ are in Lemma 3.2.1. Then, we will build up on Lemma 3.1.2 with some technical results, in order to better understand how the x-coordinate of the point R looks like modulo p.

As $p\equiv 1 \pmod 3$, it splits into $2=[K:\mathbb{Q}]$ primes in K, thus $p\mathcal{O}_K=(\mathfrak{P}\overline{\mathfrak{P}})$. If $\mathcal{O}_L$ denotes the ring of integers of $L=K(\sqrt[3]{p})$, then $p\mathcal{O}_L=(\mathfrak{p}\overline{\mathfrak{p}})^3=(\mathfrak{p}\overline{\mathfrak{p}})^{[L:K]}$. It follows that the primes $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ have residue degree 1, and hence residue field $\mathbb{F}_p$. For a point $X\in E_1(L)$, we may then consider

$$(X \bmod \mathfrak{p}, X \bmod \overline{\mathfrak{p}})\in E_1(\mathbb{F}_p)^2.$$

Lemma 3.2.1. *Consider the elliptic curve E_1 with affine equation $y^2+y=3x^3-1$. Then,*

$$E_1(L)_{tors}=E_1[3]=\{\infty,(0,\omega),(0,\omega^2),(\omega^i,1),(\omega^i,-2):i=0,1,2\}\cong(\mathbb{Z}/3\mathbb{Z})^2$$

Proof. This proof is based on that of [7, Lemma 5.2.9].

First observe that, by inspection, the points listed in the lemma are in $E_1(K)$ and are all the 3-torsion points of E_1. Therefore, $\#E_1(L)_{\text{tors}} \geq 9$.

Recall from [16, Proposition VII.3.1] that to gain information about the torsion subgroup of an elliptic curve E defined over a number field K, we can reduce it modulo a prime v of good reduction with residue field k. If $\tilde{E}$ denotes the reduction of E modulo v, the torsion subgroup of $E(K)$ injects into $\tilde{E}(k)$.

The elliptic curve E_1 has Weierstrass equation $Y^2 = X^3 - 2^4 3^3$, as shown in Proposition 1.1.2. In this form, 2-torsion points have Y-coordinate 0 and X-coordinate satisfying $X^3 = 2 \cdot 6^3$. Since $\sqrt[3]{2} \notin L$, we have $E_1[2](L) = \{\infty\}$. The change of coordinates $x' = \frac{X}{4}, y' = \frac{Y}{8} - \frac{1}{2}$ yields the model $y'^2 + y' = x'^3 - 7$, which is minimal with respect to the prime 2. Reducing this minimal equation modulo 2 we find $\tilde{E_1} : y'^2 + y' = x'^3 + 1$, which is nonsingular. Hence, E_1 has good reduction at 2. The prime 2 is inert in $\mathcal{O}_K$, so it has residue degree $2 = [K : \mathbb{Q}]$ and residue field $\mathcal{O}_K/(2) \cong \mathbb{F}_4$. The prime $2\mathcal{O}_K$ splits into $3 = [L : K]$ primes in $\mathcal{O}_L$, since the polynomial $x^3 - p$ defining L/K factors as $(x-1)(x-\omega)(x+1+\omega)$ modulo $2\mathcal{O}_K$. The relative residue degree of 2 in L/K is 1. It follows that for any prime $\mathfrak{q}$ of L above 2, its residue field is $\mathcal{O}_l/\mathfrak{q} \cong \mathbb{F}_4$. If we write $\mathbb{F}_4 = \{0, 1, \xi, \xi+1\}$, we have that $\tilde{E_1}(\mathbb{F}_4) = \{\infty, (0,0), (0,1), (1,0), (1,1), (\xi,\xi), (\xi,\xi+i), (\xi+1,\xi), (\xi+1,\xi+1)\}$.

In total, $\#\tilde{E_1}(\mathbb{F}_4) = 9$, and thus $9 \leq \#E_1(L)_{\text{tors}}$.

We conclude that $\#E_1(L)_{\text{tors}} = 9$, and the torsion points of $E_1(L)$ are precisely those listed in the statement of this lemma. □

We now shift our focus to understanding what happens for $R \in E_1(L)$.

Recall that in the construction of Chapter 2 we started from a point $P_0 \in X_0(243)$ (see (2.1.1)), represented by a complex number $\tau \in \mathcal{H}$ (see (2.1.4)). We then considered the point $P = \Phi(P_0) \in E_9(H_{9p})$ in (2.1.2). The point $Q \in E_1(H_{3p})$ was obtained from P in Proposition 2.3.1 via a twist by $\sqrt[3]{3}$. Lastly, recall the point R is defined as $\text{Tr}_{H_{3p}/L}(Q) \in E_1(L)$.

Before considering $(R \bmod \mathfrak{p}, R \bmod \overline{\mathfrak{p}}) \in E_1(\mathbb{F}_p)^2$, we would like to understand what the x-coordinate of the point $Q \in E_1(H_{3p})$ looks like modulo p. In Proposition 3.2.8, we will be able to conclude that R is nontorsion using the information we will have collected on the shape of $x(Q)^p$ modulo p in the following propositions.

Using Lemma 3.1.2, we see that we can rewrite the x-coordinate of Q as

$$x(Q) = \frac{x(P)}{\sqrt[3]{3}} = \frac{x(\tau)}{\sqrt[3]{3}} = e^{\pi i/6}\sqrt[6]{3}\frac{f(p(\omega-j)/27)f(p\omega/9)}{f(p(\omega-j)/9)}. \tag{3.2.2}$$

We would like to use the following result, which is [7, Proposition 5.2.1], together with Proposition 3.2.4 and Lemma 3.2.6 to find an explicit expression for $x(Q)^p$ modulo p starting from (3.2.2).

Proposition 3.2.3. *Let $F(z) = \sum_n a_n q^n$ be a nonconstant modular function on $\Gamma_0(N)$ with $a_n \in \mathbb{Z}$ such that f only has poles at cusps. Let K be a quadratic imaginary field and p a prime that splits in K with $p \nmid N$. Let $\tau \in \mathcal{H}$ have image in $X_0(Np)$ corresponding*

to a cyclic Np-isogeny $\phi : E_1 \to E_2$ of elliptic curves with CM by orders in K. Suppose the index $[\mathcal{O}_K : \mathrm{End}(E_1)]$ is not divisible by p but that $[\mathcal{O}_k : \mathrm{End}(E_2)]$ is divisible by p.

Let H be the ring class field of K associated to $\mathrm{End}(\phi)$ and let $\mathcal{O}_{H,(p)}$ denote the ring of p-integral elements of H. Then $f(\tau), f(p\tau) \in H^\times$ are integral at each prime of H above p and satisfy the congruence $f(\tau) \equiv f(p\tau) \pmod{p\mathcal{O}_{H,(p)}}$.

Proof. See [7, Appendix A]. □

Proposition 3.2.4. *Let $j \in \mathbb{Z}$ as in the statement of Lemma 3.1.2, meaning $jp \equiv 4 \pmod{27}$ in case 1 and $jp \equiv 1 \pmod{27}$ in case 2.*

The modular function f defined in (3.1.1) by $f(z) = \eta(27z)/\eta(3z)$ and the points $p\omega/9$, $(\omega - j)/9$ and $p(\omega - j)/27$ satisfy the hypotheses of Proposition 3.2.3.

In particular, $f\left(\frac{p(\omega-j)}{27}\right)^p \equiv f\left(\frac{\omega-j}{27}\right)$, $f\left(\frac{p(\omega-j)}{9}\right)^p \equiv f\left(\frac{\omega-j}{9}\right)$, and $f\left(\frac{p\omega}{9}\right)^p \equiv f\left(\frac{\omega}{9}\right)$ modulo $p\mathcal{O}_{H_{3p}}$.

Proof. We have already shown that f is a modular function on $X_0(81)$. It has integer Fourier coefficients, as its q-expansion is $q\prod_{n\geq 1}(1+q^{3n}+q^{9n}) \in \mathbb{Z}[[q]]$. As an η-quotient, f can only have poles or zeros at cusps. Therefore, f satisfies the assumptions of Proposition 3.2.3.

The prime p splits in $K = \mathbb{Q}(\sqrt{-3})$, and it doesn't divide 81.

We will write $\langle\tau\rangle$ as a shorthand for an elliptic curve of the form $\mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$, for $\tau \in \mathcal{H}$. In the proof of Lemma 3.1.2, we found that j must assume one of the following values modulo 27: $-11, -8, -5, -2, 1, 4, 7, 10, 13$. For such j, $(\omega - j)/27$ corresponds to the $81p$-isogeny $\langle\frac{\omega-j}{27}\rangle \to \langle 3p\omega\rangle$ defined by $z \mapsto 81pz$. We have shown in Lemma 1.2.12 that $\langle 3p\rangle$ has CM by the order of K of conductor $3p$, which is divisible by p. The elliptic curve $\langle\frac{\omega-j}{27}\rangle$ has complex multiplication by the order of K of conductor 27, not divisible by p. Similarly, for j as above or $j = 0$, $(\omega - j)/9$ corresponds to the $81p$-isogeny $\langle\frac{\omega-j}{9}\rangle \to \langle 9p\omega\rangle$ defined by $z \mapsto 81pz$. We know from Lemma 1.2.12 that $\langle 9p\omega\rangle$ has CM by the order of K of conductor $9p$, and we find $\langle\frac{\omega-j}{9}\rangle$ has complex multiplication by the order of K of conductor 9.

Therefore, f and the points $(\omega - j)/27, (\omega - j)/9, (\omega/9)$ satisfy the assumptions of Proposition 3.2.3.

Applying Proposition 3.2.3, we have that $f\left(\frac{p(\omega-j)}{27}\right)^p \equiv f\left(\frac{\omega-j}{27}\right) \pmod{p\mathcal{O}_{H_{27p}}}$, $f\left(\frac{p(\omega-j)}{9}\right)^p \equiv f\left(\frac{\omega-j}{9}\right) \pmod{p\mathcal{O}_{H_{9p}}}$ and $f\left(\frac{p\omega}{9}\right)^p \equiv f\left(\frac{\omega}{9}\right) \pmod{p\mathcal{O}_{H_{9p}}}$.

The statement follows from the inclusions $H_{3p} \subseteq H_{27p}$ and $H_{3p} \subseteq H_{9p}$, given by Proposition 0.3.12. □

Applying Proposition 3.2.4 to the expression (3.2.2), we obtain

$$f((\omega - j)/9)x(Q)^p \equiv (e^{\pi i/6}\sqrt[6]{3})^p f((\omega - j)/27)f(\omega/9) \pmod{p\mathcal{O}_{H_{3p}}} \tag{3.2.5}$$

We can refine this equivalence by computing the explicit values $f((\omega-j)/9), f((\omega-j)/27)$ and $f(\omega/9)$.

Lemma 3.2.6. *For $j \in \{-11, -8, -5, -5, 1, 4, 7, 10, 13\}$, it holds*

$$f\left(\frac{\omega - j}{9}\right) = -\frac{\omega^2}{\sqrt[3]{9}}, \quad \frac{f((\omega-j)/27)f(\omega/9)}{f((\omega-j)/9)} = -e^{\pi i/6}\frac{1}{\sqrt[6]{3}}.$$

Proof. This proof is based on that of [7, Lemma 5.2.4].

Define the complex function h mapping $z \in \mathcal{H}$ to $h(z) := (f(z/3))^{-3}$. Observe that $h(z) = \prod_{0<d|9} \eta(dz)^{r_d}$, with $r_1 = 3$, $r_3 = 0$ and $r_9 = -3$. By Proposition 0.2.6, h is a modular function on $X_0(9)$.

Using Mathematica with an accuracy of 200 digits, we find that: $h(\omega/3) \approx 3\sqrt{-3}$, $h((\omega - j)/3) \approx -9$, and $h((\omega - j)/9) \approx -3$.

The point of $X_0(9)$ represented by $\omega/3$ corresponds to the cyclic 9-isogeny $\langle \omega/3\rangle \to \langle 3\omega\rangle$ between elliptic curves with complex multiplication by the order of $\mathcal{O}_K$ of conductor 3. Similarly, the point of $X_0(9)$ represented by $(\omega - j)/3$ corresponds to the 9-isogeny $\langle(\omega - j)/3\rangle \to \langle 3\omega\rangle$, between elliptic curves with CM by the order of $\mathcal{O}_K$ of conductor 3. The point $\Gamma_0(9)(\omega - j)/9 \in X_0(9)$ corresponds to the isogeny $\langle(\omega - j)/9)\rangle \to \langle\omega\rangle$, where $\langle(\omega - j)/9)\rangle$ has complex multiplication by the order of K of conductor 9, while $\langle\omega\rangle$ has complex multiplication by the ring of integers $\mathcal{O}_K$ of K. By CM theory, we expect $h(\omega/3)$ to lie in $H_3 = K$, and $h((\omega - j)/3^n)$ to lie in H_{3^n}, for $n \in \{1, 2\}$. From this, we deduce $h(\omega/3) = 3\sqrt{-3}$, $h((\omega - j)/3) = -9$, and $h((\omega - j)/9) = -3$.

Using the equality $f(z) = h(3z)^{-1/3}$, we see that we have $f(\omega/9) = e^{-\pi i/6}/\sqrt{3}$, $f((\omega - j)/9) = -\omega^2/\sqrt[3]{9}$, and $f((\omega - j)/27) = -\omega^2/\sqrt[3]{3}$.

These results allow us to compute

$$\frac{f((\omega-j)/27)f(\omega/9)}{f((\omega-j)/9)} = \frac{(-\omega^2/\sqrt[3]{3})(-e^{-\pi i/6}/\sqrt{3})}{-\omega^2/\sqrt[3]{9}} = -e^{\pi i/6}\frac{1}{\sqrt[6]{3}}.$$

□

Applying Lemma 3.2.6 to the expression (3.2.5) it follows that:

$$x(Q)^p \equiv (e^{\pi i/6}\sqrt[6]{3})^p \left(\frac{-e^{\pi i/6}}{\sqrt[6]{3}}\right) = \omega^2(-3)^{(p-1)/6} \pmod{p\mathcal{O}_{H_{3^p}}} \tag{3.2.7}$$

This equivalence is going to be used in the following proposition to prove that the point R is nontorsion.

Proposition 3.2.8. *If 3 is not a cube modulo p, then the image of $R \in E_1(L)$ in $E_1(\mathbb{F}_\mathfrak{l})^2$ given by reduction by $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ is not equal to the image of any torsion point in $E_1(L)$. Hence, R is nontorsion.*

Proof. This proof is based on that of [7, Proposition 5.2.8].

From (3.2.7), we have that $x(Q)^p \equiv \omega^2(-3)^{(p-1)/6} \pmod{p\mathcal{O}_{H_{3^p}}}$.

Since $\left(\frac{-3}{p}\right) = 1$, -3 is a non-zero square modulo p. Therefore, we see that $(-3)^{(p-1)/6}$ is a cubic root of unity inside $\mathbb{F}_p^*$, and it is trivial if and only if -3 is a cube modulo p, that is if and only if 3 is a cube modulo p.

On the other hand, the image of ω^2 in $\mathcal{O}_K/p\mathcal{O}_K \cong \mathcal{O}_K/\mathfrak{p} \times \mathcal{O}_K/\overline{\mathfrak{p}} \cong \mathbb{F}_p \times \mathbb{F}_p$ is of the form (u, u^2), where $1 \leq u \leq p-1$ is a primitive cubic root of unity in $\mathbb{F}_p^* \cong (\mathbb{Z}/p\mathbb{Z})^*$.

It follows that, under our assumption that 3 is not a cube modulo p, the image of $x(Q)^p$ in $\mathbb{F}_p \times \mathbb{F}_p$ has the form $(u, 1)$ or $(1, u)$ for a primitive cubic root of unity $u \in \mathbb{F}_p^*$.

Hence, by Fermat's little theorem, the image of $x(Q)$ in $\mathbb{F}_p \times \mathbb{F}_p$ is also of the form $(u, 1)$ or $(1, u)$. As we are considering E_1 in the equation $y^2 + y = 3x^3 - 1$ (1.1.4), in $E_1(\mathbb{F}_p)$ we have $y(Q)^2 + y(Q) = 2$, implying $y(Q) \in \{1, -2\}$. This means that the image of Q in each copy of $E_1(\mathbb{F}_p)$ is of the form $(u^i, 1)$ or $(u^i, -2)$ for $i \in \{0, 1, 2\}$. Points in $E_1(\mathbb{F}_p)$ of this form are 3-torsion points, as they are the reduction modulo p of points found in Lemma 3.2.1.

We have that $R = \mathrm{Tr}_{H_{3p}/L} Q \equiv \frac{p-1}{3} Q \equiv \pm Q \in E_1(\mathbb{F}_p)$, where the sign is $+$ if $p \equiv 4 \pmod 9$ and $-$ if $p \equiv 7 \pmod 9$. The first congruence comes from the fact that p is totally ramified in H_{3p}/L. The second congruence relies on the fact that Q is a 3-torsion point in $E_1(\mathbb{F}_p)$.

Finally, to prove R is nontorsion, since $R \equiv \pm Q \in E_1(\mathbb{F}_p)$, it suffices to prove that the image of Q in $E_1(\mathbb{F}_p)^2$ is not equal to that of any torsion point of $E_1(L)$.

From Lemma 3.2.1, we compute the images in $\mathbb{F}_p^2$ of the x-coordinates of the torsion points $Z \in E_1[3] \setminus \{\infty\}$. They are of the form $(0, 0)$ if $x(Z) = 0$, $(1, 1)$ if $x(Z) = 1$, and (u, u^2) for u a primitive cubic root of unity of $\mathbb{F}_p$ in the other cases.

We have shown that the image of $x(Q)$ in $\mathbb{F}_p^2$ is $(u, 1)$ or $(1, u)$, so it doesn't match that of any torsion point of $E_1(L)$. This concludes the proof that $R \in E_1(L)$ is nontorsion. □

3.3 Obtaining a nontorsion point on $E_{p^i}(\mathbb{Q})$

In this section we are finishing the proof of Theorem 0.0.5, by showing that from the nontorsion point $R \in E_1(L)$ we can always produce a nontorsion point on $E_{p^i}(\mathbb{Q})$, for $i \in \{1, 2\}$.

Recall that in Lemma 2.4.8 we defined the point $Y \in E_1(L)$ as $R - T$, for a point $T \in E_1(L)_{\mathrm{tors}}$. We proved in Proposition 3.2.8 that R is nontorsion, so Y is nontorsion as well.

The image of Y under the twisting isomorphism of Proposition 2.4.1, $Z \in E_{p^i}(K)$, is again nontorsion. To see this, consider the models $E_1 : y^2 = x^3 - 432$ and $E_{p^i} : y^2 = x^3 - 432p^{2i}$. Considering the cubic twist from Proposition 2.4.1 in these models, two points $Y_1 = (x_1, y_1), Y_2 = (x_2, y_2) \in E_1(L)$ are twisted to $Z_1 = (p^{2i/3}x_1, p^i y_1)$ and $Z_2 = (p^{2i/3}x_2, p^i y_2) \in E_{p^i}(K)$, respectively. If $Y_1 + Y_2 = (x, y) \in E_1(L)$, then $Z_1 + Z_2 = (p^{2i/3}x, p^i y) \in E_{p^i}(K)$. Hence, if there were a positive integer n such that $[n-1]Z = -Z$, the same equation would hold for Y. This would imply Y is torsion, yielding a contradiction.

We note that, since E_{p^i} has complex multiplication by $\mathcal{O}_K$ and $\omega - \omega^2 \in \mathcal{O}_K$, then also $\sqrt{-3}Z = (\omega - \omega^2)Z$ is nontorsion. Indeed, if there were a positive integer n such that $[n](\sqrt{-3}Z) = O$, then we would have $\omega([n]Z) = \omega^2([n]Z)$. Writing $[n]Z = (x, y)$ for $x, y \in K$ satisfying $y^2 = x^3 - 432p^{2i}$, this would imply $\omega x = \omega^2 x$ and $y = -y$,

and thus $(x, y) = (0, 0)$. However, the point $(0, 0)$ does not lie on $E_{p^i}(K)$. Therefore, $\sqrt{-3}Z \in E_{p^i}(K)$ is nontorsion.

Finally, we consider the rational point on E_{p^i} $Z + \overline{Z}$, as in (2.4.10). Either this is already nontorsion, or $Z = -\overline{Z}$ and we can consider $\mathrm{Tr}_{K/\mathbb{Q}} \sqrt{-3}Z \in E_{p^i}(\mathbb{Q})$. In this case, we also obtain a nontorsion point, because $(\sqrt{-3}Z) + \overline{\sqrt{-3}Z} = \sqrt{-3}Z - \sqrt{-3}\overline{Z} = [2](\sqrt{-3}Z)$, and $[2](\sqrt{-3}Z) \neq O$ in $E_{p^i}(K)$, as observed previously.

This concludes the proof of Theorem 0.0.5.

Bibliography

[1] M. Akbaş, D. Singerman, *The normalizer of* $\Gamma_0(N)$ *in* $\mathrm{PSL}(2,\mathbb{R})$. Glasgow Mathematical Journal. **32** (1990), no. 3, 317-327.

[2] A. O. L. Atkin and J. Lehner, *Hecke operators on* $\Gamma_0(m)$, Math. Ann. **185** (1970), 134–160.

[3] Harvey Cohn, *Introduction to the construction of class fields*, Cambridge University Press, 1985.

[4] David A. Cox, *Primes of the Form* $x^2 + ny^2$, John Wiley & Sons, New York, 1989.

[5] Henri Darmon, *Rational points on modular elliptic curves*, CBMS Reg. Conf. Ser. in Math., vol 101, Amer. Math. Soc., Providence, 2004.

[6] Samit Dasgupta and John Voight, *Heegner points and Sylvester's conjecture*, Arithmetic geometry, Clay Math. Proc., vol. 8, Amer. Math. Soc., Providence, 2009, 91–102.

[7] Samit Dasgutpa and John Voight, *Sylvester's problem and mock Heegner points*, Proc. Amer. Math. Soc. **146** (2018), no. 8, 3257-3273.

[8] Fred Diamond, Jerry Shurman, *A First Course in Modular Forms*, Springer, New York, 2005.

[9] Haruzo Hida, *Elliptic Curves and Arithmetic Invariants*, Springer, New York 2013.

[10] Gérard Ligozat. *Courbes modulaires de genre 1.*, Mémoires de la Société Mathématique de France **45** (1975), 5-80.

[11] J. S. Milne, *Class Field Theory*, v4.03. August 2020, retrieved April 2023 `https://www.jmilne.org/math/CourseNotes/cft.html`

[12] Paul Monsky, *Mock Heegner points and congruent numbers*, Math. Z. **204** (1990), 45-68.

[13] Philippe Satgé, *Groupes de Selmer et corps cubiques*, J. Number Theory, **23** (1986), 294-317.

[14] Ernst S. Selmer, *The diophantine equation* $ax^3 + by^3 + cz^3 = 0$, Acta Math. **85** (1951), 203-362.

[15] Joseph H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer, New York, 1994.

[16] Joseph H. Silverman, *The Arithmetic of Elliptic Curves, 2nd edition*, Springer, New York, 2009.

[17] Peter Stevenhagen, *Class Field Theory*, retrieved May 2023
`https://websites.math.leidenuniv.nl/algebra/Stevenhagen-CFT.pdf`

[18] Peter Stevenhagen, *Hilbert's 12th problem, complex multiplication and Shimura reciprocity*, Class field theory - its centenary and prospect, Math. Soc. Japan. **30** (1998), 161-176.

[19] J.J. Sylvester, *On Certain Ternary Cubic-Form Equations*, Amer. J. Math, **2** (1879), no. 4, 357-393.