Endomorphisms of degree 2, 3 and 4 on Elliptic Curves

Bachelor Project Mathematics,

University of Groningen

Berno Reitsma
1st Supervisor: Dr. M.C. Kronberg,
2nd supervisor: Prof. Dr. J. Top

July 2017

Abstract

This manuscript gives an elementary approach to computing separable endomorphisms on elliptic curves that have degree 2, 3 and 4. Before doing so, all theory that is being used is introduced. The theory is developed using different perspectives on elliptic curves, varying from algebra to complex analysis, geometry and number theory. After having constructed such endomorphisms, we describe conditions for reduction modulo p for prime numbers p, which generates endomorphisms of degree 2, 3 and 4 on curves over finite fields $\mathbb{F}_p$.

Contents

1 Introduction **2**

2 Preliminaries **3**
- 2.1 The group law on K-rational points of an elliptic curve 3
- 2.2 The Weierstrass form and the discriminant 4
- 2.3 Isogenies 5
- 2.4 The j-invariant 6
- 2.5 Endomorphisms on elliptic curves 6

3 A general method in finding elliptic curves with endomorphisms of degree m **9**
- 3.1 Finding the corresponding imaginary quadratic field extensions of $\mathbb{Q}$ 9
- 3.2 Finding isogenies with kernel of order m 10
- 3.3 Choosing the isogenies that map to curves isomorphic to E. . . . 12
- 3.4 Reduction modulo p 12

4 Finding endomorphisms of degree 2 **15**
- 4.1 Finding the corresponding imaginary quadratic field extensions of $\mathbb{Q}$ 15
- 4.2 Finding isogenies of degree 2 16
- 4.3 Finding isogenies that map to curves isomorphic to its domain . 16
- 4.4 Reduction modulo p 21

5 Finding Endomorphisms of Degree 4 **22**
- 5.1 Finding the corresponding quadratic imaginary field extensions of $\mathbb{Q}$ 22
- 5.2 Finding endomorphisms of degree 4 23
- 5.3 Reduction modulo p 27

6 Finding Endomorphisms of degree 3 **29**
- 6.1 Finding the corresponding imaginary quadratic field extensions of $\mathbb{Q}$ 29
- 6.2 Finding isogenies of degree 3 30
- 6.3 Reduction Modulo p 33

7 Summary and Conclusion **34**

1 Introduction

Theory of elliptic curves have many applications in cryptography and algebraic number theory. This is a result of the fact that the K-rational points of an elliptic curve, for a perfect field K, have a group structure defined on them. An intriguing and non-trivial part of research is then to find what kind of endomorphisms exist on these groups.

A map that is structure-preserving from a geometric point of view is called an morphism. We then define an isogeny as a morphism that also preserves the "point at infinity", which will be the unit element of the group. These isogenies have a degree defined on them. Mapping K-rational points on an isogeny from an elliptic curve to itself gives an endomorphism. The degree of such an isogeny is then the order of its kernel. Hence, we can define a degree on such endomorphisms, and then we arrive at the central question of this project: "Given a certain degree m, what are the elliptic curves that have endomorphisms of such degree m, and how do we find such endomorphisms explicitly?"

This manuscript answers that question for degree 2, 3 and 4. Before we will be at the point of actually computing the elliptic curves, we will introduce elliptic curves and the basic theory, and then we will create a recipe for finding these endomorphisms in general. The construction of such endomorphisms uses results from complex analysis, number theory, algebra and geometry. Silverman [10] computed the endomorphisms of degree 2 as an example. We will follow his example, but we will provide more details. Afterwards, we will also construct the endomorphisms of degree 3 and 4, using the same approach.

2 Preliminaries

2.1 The group law on K-rational points of an elliptic curve

We will give a basic definition of K-rational points on elliptic curves and their group structure, and make some basic observations that will be used throughout the research. The theory that is introduced is mainly based on [5].

An elliptic curve is a curve defined over a field K is a curve that has the form

$$y^2 = x^3 + Ax + B.$$

K-rational points on such an elliptic curve have a group structure. Here, we will define K-rational points.

Definition 2.1. *Let E be an elliptic curve defined by $y^2 = x^3 + Ax + B$, where A, B are in some perfect field L with $char(L) \neq 2$, and let $4A^3 + 27B^2 \neq 0$. Let K be a finite field extension of L. Then the set of K-rational points of E, denoted by $E(K)$, is the set $\{(x, y) \in K^2 : y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}$.*

To get some idea of what we are considering, we first show some pictures of how the curves look like if we consider $E(\mathbb{R})$ in Figure 1. Note that the graph of the curve on the left picture is the result of a curve for which $x^3 + Ax + B$ has one real root, while picture on the right displays the graph of a curve where this polynomial has three distinct real roots.

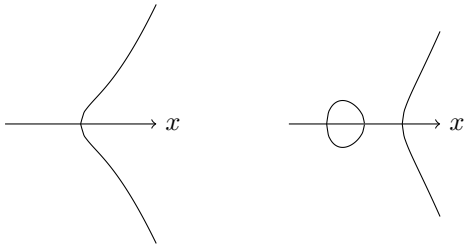


Figure 1: Elliptic Curves on $\mathbb{R}$

It follows from the Intermediate Value Theorem that the polynomial $x^3 + Ax + B$ (in fact, all polynomials over $\mathbb{R}$ of odd degree) have at least one real root. Also, using that a root of a polynomial can be represented as a linear factor, we can observe that if our polynomial has two real roots, then it follows that the third root is also real. Hence, $E(\mathbb{R})$ has either one or three points that lie on the x-axis.

We will now define the group structure on $E(K)$. We will introduce the group law using $E(\mathbb{R})$ and generalize later. For any two points P_1 and P_2 in $E(\mathbb{R})$, we can define a unique line l that intersects both these points, by drawing a line through both points when $P_1 \neq P_2$, and defining l to be the tangent line

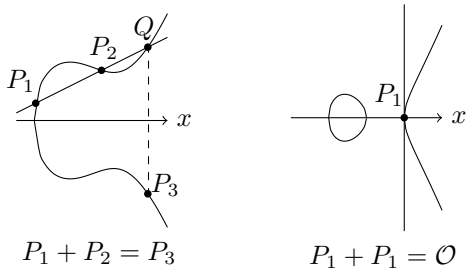


Figure 2: Addition of $\mathbb{R}$-rational points

on the point of the curve in case $P_1 = P_2$.

A property of K-rational points on elliptic curves is that, given l is not vertical, l intersects $E(\mathbb{R})$ at a third K-rational point on the curve. Let us call this third point Q. If we then reflect the point Q on the x-axis, we will get a point P_3. We then define the sum of P_1 and P_2 as the point P_3. In the case that P_1 and P_2 will result in a vertical line l, we define $P_1 + P_2 = \mathcal{O}$. Furthermore, we define $P + \mathcal{O} = P$ for all points $P \in E(\mathbb{R})$. The operation "+" will then give an abelian group structure on $E(\mathbb{R})$, with unit element $\mathcal{O}$. In figure 2, we see two examples of addition on $\mathbb{R}$-rational points.

Note that for points P_1, P_2, P_3 on the elliptic curve, P_1, P_2, P_3 lie on the same line if and only if $P_1 + P_2 + P_3 = \mathcal{O}$. This is particularly visible in the left picture on Figure 2, noting that Q and P_3 are on a vertical line, hence $P_1 + P_2 + Q = P_3 + Q = \mathcal{O}$, or equivalently $P_3 = -Q$. Although closure, invertibility and commutativity are easy to check, it is hard to see why the operatoin is associative. For a more elaborate explanation of the group law, we refer to [5, Section 1.2].

We can compute explicit expressions for the lines and hence, the group law. The expressions allow us to generalize the group structure that we just defined for $E(\mathbb{R})$ to $E(K)$ for any field K. We simply take the same expressions we used to define the group structure for the real numbers, but now apply them to any field K. This defines a group structure for K-rational points in general.

2.2 The Weierstrass form and the discriminant

We call the equation $y^2 = x^3 + Ax + B$ the short Weierstrass form. Sometimes, it is convenient for us to write the equation of an elliptic curve in the longer form $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, using a transformation of coordinates. This is called the long Weierstrass form. We can do this because a transformation of coordinates is always an isomorphism of elliptic curves. During our research, we will use a lot of transformations of coordinates because it

allows us to express endomorphisms in a more convenient way. Therefore, we will sometimes use the long Weierstrass form when introducing some parts of the theory.

Note that in the definition of K-rational points of an elliptic curve, Definition 2.1, we have excluded the case where $4A^3 + 27B^2 = 0$. This is because we want the *discriminant* of the curve to be non-zero. In a curve that does not have the short Weierstrass form, hence a curve with equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, the discriminant is defined as

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

where $b_2 = a_1^2 + 4a_2$, $b_4 = 2a_4 + a_1a_3$, $b_6 = a_3^2 + 4a_6$, $b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$. Then, for the short Weierstrass Form $y^2 = x^3 + Ax + B$, the discriminant reduces to

$$\Delta = -16(4A^3 + 27B).$$

The discriminant indicates whether a curve is singular or non-singular, which is often important because we do not consider singular curves. We summarize this in the following theorem.

Theorem 2.2. *Let E be an elliptic curve, and let Δ be the discriminant as we defined earlier. Then, the following statements are equivalent.*

1. $\Delta \neq 0$.
2. *The curve is non-singular.*

Proof. For the proof, we refer to [9, Proposition 1.4]. □

2.3 Isogenies

Isogenies are maps between elliptic curves that are structure-preserving from a geometric perspective (a *morphism*), and also map the point at infinity to itself. For the details, we refer to [9, Section I.3, II.2, III.4].

The interesting property about isogenies on elliptic curves is that any isogeny on an elliptic curve gives a group homomorphism on K-rational points, and any group homomorphism on K-rational points gives an isogeny on elliptic curves. The degree of an isogeny is defined in [9, section II.2].

In our case, the degree of an isogeny reduces to the order of the kernel of the isogeny. We remark that the degree of an isogeny is multiplicative under composition, that is,

$$\deg(\phi \circ \varphi) = \deg(\phi)\deg(\varphi).$$

Hence, so is the degree of an endomorphism. A more in-depth explanation can be found in [9, Section III.4].

2.4 The j-invariant

Another important invariant of an elliptic curve is its j-invariant. A j-invariant is an expression of $E(K)$ dependent on the coefficients of the curve E. For equations of the form $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, we have the following formula for the j-invariant [9, Section III.1].

$$j(E) = \frac{(b_2^2 - 24b_4)^3}{\Delta}$$

where b_2 and b_4 are as in Section 2.2, $b_2 = a_1^2 + 4a_2$ and $b_4 = 2a_4 + a_1a_3$. In case we use the short Weierstrass Form, the j-invariant reduces to

$$j(E) = 1728\frac{4A^3}{4A^3 + 27B^2}.$$

Two curves have the same j-invariant if and only if the curves are isomorphic to each other. Hence, the j-invariant determines the *isomorphism class* of an elliptic curve. If two elliptic curves are isomorphic, they also have the same endomorphism ring. In the context of our research, we therefore want to find the isomorphism classes that have an endomorphism of certain degree on them. For an elementary proof of this result, we recommend [11, Proposition 1.8].

2.5 Endomorphisms on elliptic curves

For now, we assume that we work over the field $K = \mathbb{C}$. In this case, $\mathrm{End}(E)$ turns out to be isomorphic to either $\mathbb{Z}$, or $\mathbb{Z}[\alpha]$, in which α satisfies some specific conditions. In this section, we will give an explanation on how this result is obtained.

Let us first introduce a very simple endomorphism. For any integer n, we can define the multiplcation-by-n-map as follows.

$$[n] : P \mapsto nP.$$

This is an endomorphism, which is explained in [9, Example III.4.1]. Hence, in the isomorphism from $\mathrm{End}(E)$ to $\mathbb{Z}$ or $\mathbb{Z}[\alpha]$, the multiplication-by-n-map is mapped to the integer n.

For endomorphisms that are represented by non-integers, we will need some more background information. We use the fact that $E(\mathbb{C})$ is isomorphic to a certain structure on the additive group of complex numbers.

For $\omega \in \mathbb{C} \setminus \mathbb{R}$, we define the lattice $L := \{n_1 + \omega n_2 : n_1, n_2 \in \mathbb{Z}\}$. We remark that ω depends on the elliptic curve E. For the full construction and explanation, we refer to [5, Section 2.2]. Note that in the referenced textbook, the lattice is introduced in the form $\omega_1 n_1 + \omega_2 n_2$. It does not make a difference up to isomorphism, since we can rescale the lattice such that $\omega_1 = 1$. This is

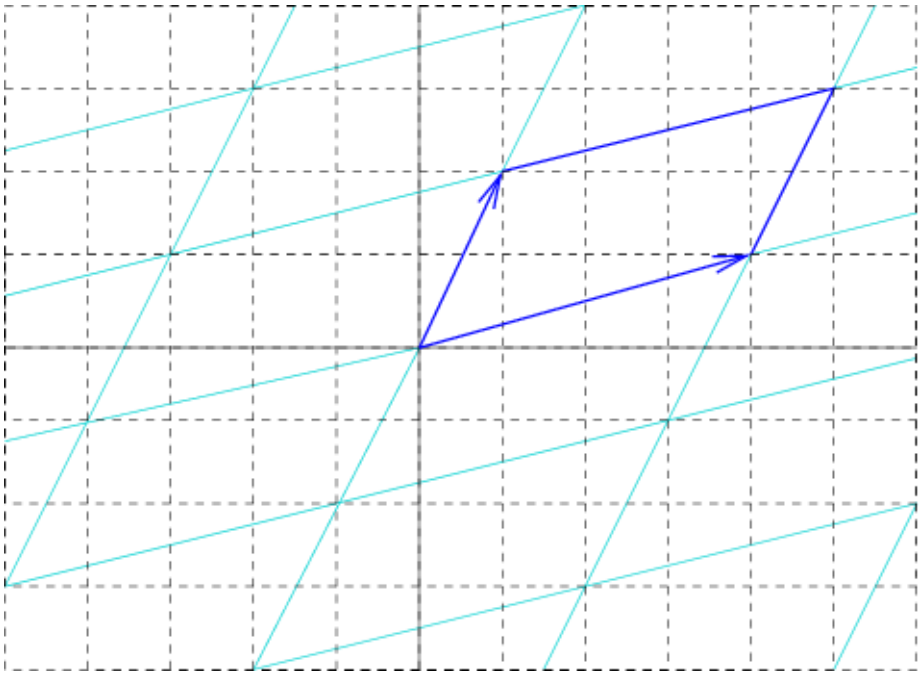


Figure 3: The period parallogram; Source: Wikipedia

proven in [11, Proposition 2.2].

This lattice will produce a grid of identical parallelograms on the complex plane. Now, $E(\mathbb{C})$ is isomorphic to $\mathbb{C}/L$, which is intuitively just $\mathbb{C}$ "reduced modulo L". In more detail, $\mathbb{C}/L$ is the parallelogram defined by the lattice, which we represent with the parallelogram that has the lower left corner as the origin. We call this parallelogram the *period parallelogram*, see Figure 3, in which we have L of the form $\{\omega_1 n_1 + \omega_2 n_2 : n_1, n_2 \in \mathbb{Z}\}$. We then apply addition as group operation on this parallelogram. Note that, since any complex number lies in a certain parallelogram on the grid, we can define reduction modulo L as setting each position in each parallelogram equivalent to the same position in the period parallelogram.

In our research, we are especially interested in how an endomorphism on an elliptic curve looks like on $\mathbb{C}/L$. Such an endomorphism is a holomorphic function f such that $f(z_1 + z_2) = f(z_1) + f(z_2)$ for all z_1, z_2 in $\mathbb{C}$. We now can apply results from complex analysis to conclude that any endomorphism that is not a multiplication-by-n-map is a map that "multiplies" a point by a complex, non-real number. Any endomorphism f on $\mathbb{C}/L$ satisfies $f(z) = \alpha z$ for some complex, non-real number α. We hence say that curves on which such behaviour appears have *complex multiplication*. A proof is done in [5, Propo-

sition 6.18]. For a more fundamental approach, we refer to [9, Section VI.2-VI.4].

Such a complex non-real number α is not entirely arbitrary. If we have $z_1, z_2 \in \mathbb{C}$ such that $z_1 - z_2 \in L$, then in $\mathbb{C}/L$, these numbers represent the same element. Using that f is an endomorphism of the form $f(z) = \alpha z$ gives us the requirement that $\alpha L \subset L$. The converse is also true: If we find a α such that $\alpha L \subset L$, then we can define an endomorphism on $\mathbb{C}/L$ and hence on $E(\mathbb{C})$ using this α. In one expression, we can summarize this to

$$\mathrm{End}(E) \cong \{\alpha \in \mathbb{C} : \alpha L \subset L\}$$

Another property of α is that α solves a quadratic, monic polynomial over the integers. This is explained in [11], Proposition 2.39. We now conclude that some curves have an endomorphism that can be represented by a quadratic integer α that has a non-zero imaginary part. Also, we have that for an elliptic curve E, α all possible $\alpha's$ lie in the same extension of the integer $\mathbb{Z}$, which is proven in [11, Proposition 2.39] Hence, we do have an endomorphism ring that is larger than the ring of integers: $\mathrm{End}(E) \cong \mathbb{Z}[\alpha]$. In the next chapter, we will use this result to find all curves with complex multiplication of a certain degree.

3 A general method in finding elliptic curves with endomorphisms of degree m

We have treated the basics of elliptic curves, together with some theory about complex multiplication. Now, we can start finding explicit endomorphisms having a certain degree. In this section, we will give the general process of finding the elliptic curves E over a number field K, with endomorphisms of degree m that works for $m \in \{1, 2, \cdots, 10, 12\}$, together with the computation of the endomorphisms itself. Then, we will describe how we can use these results to generate endomorphisms of degree m on elliptic curves over finite field $\mathbb{F}_p$.

3.1 Finding the corresponding imaginary quadratic field extensions of $\mathbb{Q}$

In this section, we will apply theory that is introduced in [10, Section II.1, II.2]. We first summarize the content that we need for our research.

It follows from Section 2.5 that every elliptic curve E over $\mathbb{C}$ has an endomorphism ring $\mathrm{End}(E)$ which is isomorphic to either $\mathbb{Z}$ or $\mathbb{Z}[\alpha]$, in which α is an algebraic integer living in a quadratic imaginary number field. That is: We have a number field of the form $\mathbb{Q}(\sqrt{-d})$, where d is a positive and square-free integer. In this number field, we can find an α that has a minimal polynomial over the integers. From now on, we denote $\mathbb{Q}(\sqrt{-d})$ by K_d.

In the first case, $\mathrm{End}(E) \cong \mathbb{Z}$, the only endomorphisms that exist on the curve are multiplcation-by-n-maps. It follows that E does not have complex multiplication. The second case, $\mathrm{End}(E) \cong \mathbb{Z}[\alpha]$ is the case where E does have complex multiplication. We still have that each integer n represents the multiplication-by-n-map, but we now also have endomorphisms that are represented by non-integers. It follows directly from [10, Corollary II.1.5] that the degree of such an endomorphism is equal to the norm of $\alpha \in K_d$. The norm is defined as $N(a+b\sqrt{-d}) = a^2+db^2$. Also, note that the norm is multiplicative.

In order to find elliptic curves with complex multiplication that have endomorphisms of a certain degree m, we need to find positive, squarefree integers d such that we have an algebraic integer α that lives in the field K_d. Furthermore, we want $N(\alpha) = m$. In more detail, we want d and α such that the following conditions hold:

- $\alpha \in K_d$
- α solves a monic quadratic polynomial $p(x) = x^2 + Bx + C$ with integer coefficients B, C.
- $N(\alpha) = m$.

The second condition implies that α is of the form

$$\alpha = \begin{cases} a + b\sqrt{-d} & d \equiv 1, 2 \mod 4 \\ \frac{a+b\sqrt{-d}}{2} & d \equiv 3 \mod 4 \end{cases} \tag{1}$$

in which $a, b \in \mathbb{Z}$. It follows immediately by computing the norm that

$$N(\alpha) = \begin{cases} a^2 + db^2 & d \equiv 1, 2 \mod 4 \\ \frac{a^2+db^2}{4} & d \equiv 3 \mod 4 \end{cases} \tag{2}$$

Using the third condition, we can find α such that $N(\alpha) = m$ by solving $a^2 + db^2 = m$ for $a, b \in \mathbb{Z}$, $d \equiv 1, 2 \mod 4$ and $a^2 + db^2 = 4m$ for $a, b \in \mathbb{Z}$ and $d \equiv 3 \mod 4$. Note that, since integer squares are always non-negative and d is assumed to be positive, there are finitely many solutions for such equations. Therefore, trying out the different possibilities for the integers leaves us with all possible α and their corresponding number fields K_d where α lives in. Every such case represents a curve having complex multiplication. Hence, we have computed the endomorphism rings for every curve with complex multiplication of degree m.

3.2 Finding isogenies with kernel of order m

Now, we want to find these endomorphisms of degree m explicitly. For this, we look at isogenies $\phi : E \to E'$ that have a kernel of order m. If we then find the isogenies for which the image curve E' is isomorphic to E, we can construct an endomorphism by composing the isogeny with the isomorphism between E' and E. This endomorphism then also has a kernel of order m.

The construction of these isogenies takes two steps. First, we describe all possible groups of order m generally, and then we describe these groups explicitly using knowledge about points of certain order on the elliptic curves. The second step is then to construct the isogenies that have a kernel equal to such a subgroup. Here, we can use the following theorem, called the *formulae of Vélu*, attributed to the French mathematician J. Vélu [12]. We use the formulation Galbraith described in [4, Theorem 25.1.6].

Theorem 3.1. *Let E be an elliptic curve defined by the equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, and let G be a subgroup of the elliptic curve. Define G_2 as the points of order 2 in G, and G_1 as all the points $\mathcal{O} \neq (x, y) \in G$ such that $G = \{\mathcal{O}\} \cup G_2 \cup G_1 \cup \{Q : -Q \in G_1\}$. If we define for $P = (x_p, y_p)$,*

$F_x(x,y) = 3x^2 + 2a_2x + a_4 - a_1y$, $F_y(x,y) = -2y - a_1x - a_3$,

$$\begin{aligned}
t(P) &= \begin{cases} F_x(x_p, y_p) & \text{if } (x_p, y_p) \in G_2 \\ 2(F_x(x_p, y_p)) - a_1(F_y) & \text{if } (x_p, y_p) \in G_1 \end{cases} \\
u(P) &= (F_y(x_p, y_p))^2 \\
u(G) &= \sum_{P=(x_p,y_p)\in G_1 \cup G_2} t(P) \\
w(G) &= \sum_{P=(x_p,y_p)\in G_1 \cup G_2} (u(P) + x_p t(P))
\end{aligned}$$

and

$$\begin{aligned}
Y(P) = &\frac{u(P)(2y + a_1x + a_3)}{(x - x_p)^3} \\
&+ \frac{t(P)(a_1(x - x_p) + y - y_p)}{(x - x_p)^2} \\
&+ \frac{a_1u(P) - F_x(x_p, y_p)F_y(x_p, y_p)}{(x - x_p)^2}
\end{aligned}$$

and then construct an isogeny $\phi : E \to E'$ *such that if* $\phi(x,y) = (f_1(x,y), f_2(x,y))$, *where*

$$f_1(x,y) = x + \sum_{P=(x_p,y_p)\in G_1 \cup G_2} \left(\frac{t(P)}{x - x_p} + \frac{u(P)}{(x - x_p)^2} \right) \tag{3}$$

$$f_2(x,y) = y - \sum_{P=(x_p,y_p)\in G_1 \cup G_2} Y(P) \tag{4}$$

then $\ker \phi = G$. *Moreover, an explicit formula for the defining equation of* E' *is* $y^2 + \widetilde{a_1}xy + \widetilde{a_3}y = x^3 + \widetilde{a_2}x^2 + \widetilde{a_4}x + \widetilde{a_6}$, *where*

$$\begin{aligned}
\widetilde{a_1} &= a_1 \\
\widetilde{a_2} &= a_2 \\
\widetilde{a_3} &= a_3 \\
\widetilde{a_4} &= a_4 - 5t(G) \\
\widetilde{a_6} &= a_6 - (a_1^2 + 4a_4)t(G) - 7w(G)
\end{aligned}$$

It is important to understand that in the theorem, G_1 does not consist of *all* points in G that are not $\mathcal{O}$ or a point of order 2, but we make pairs of those points that are each others inverse, and remove one of each pair.

We construct all isogenies ϕ that have the subgroups of order m we found earlier. Hence, we have group homomorphisms with a kernel of order m on E.

We want to remark that, in 1977, Mazur [8] proved that the torsion subgroup of elliptic curves over $\mathbb{Q}$, consisting of all points of finite order, can only be isomorphic to $\mathbb{Z}/n\mathbb{Z}$ for $n \in \{1, 2 \cdots, 10, 12\}$, or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ for $n \in \{2, 4, 6, 8\}$. Since Theorem 3.1, Vélu's formulae, require a subgroup of such a torsion subgroup, constructing such isogenies using this technique will construct endomorphisms on curves defined over $\mathbb{Q}$ for degree $m \in \{1, 2, \cdots, 10, 12\}$.

3.3 Choosing the isogenies that map to curves isomorphic to E.

If we now find those curves E that have isogenies mapping to an elliptic curve E' that is isomorphic to E, we can compose the resulting isomorphism with our isogeny to construct an endomorphism with a kernel of order m.

We know from j-invariants that $E \cong E'$ if and only if $j(E) = j(E')$. Note that the j-invariant is just an expressions of the coefficients a_i of an elliptic curve. Using theorem 3.1, we arrive at coefficients $\widetilde{a_i}$ expressed in terms of the coefficients a_i. It follows that $j(E') = j(E)$ just ends up in an equation for coefficients of our original curve. We obtain all curves E for which $E' \cong E$ by solving this equation for the coefficients a_i.

We then know exactly the curves E for which there exists an isogeny that maps to a curve E' that is isomorphic to E. If we compose the isogeny ϕ with an isomorphism φ, we create an endomorphism

$$\varphi \circ \phi : E \longrightarrow E' \longrightarrow E.$$

Note that since φ is an isomorphism, $\ker(\varphi \circ \phi) = \ker(\phi)$, hence $\#\ker(\varphi \circ \phi) = \#\ker(\phi) = m$. We then have constructed an endomorphism of degree m.

3.4 Reduction modulo p

Finally, we want to see whether we can reduce the constructed endomorphisms modulo p. This means that, given an endomorphism on a curve E, we generate a similarly behaving endomorphism on a curve $\bar{E}$ defined over a finite field $\mathbb{F}_p$. In most cases, the j-invariants we find are of isomorphism classes that have curves over $\mathbb{Q}$. In this case, we can sometimes reduce the produced endomorphisms modulo p for a prime number p.

The first conditions we will introduce are conditions that will prevent us from mapping to a singular curve $\bar{E}$. As we know from Theorem 2.2, the discriminant of the reduced curve has to be non-zero. In [5, Section 4.3], it is explained that $\bar{E}(\mathbb{F}_p)$ is a group if $p > 2$ and $p \nmid \Delta$ because the discriminant of the reduced

curve is equal to the original discrimant reduced modulo p. It follows that we need $p \nmid 2\Delta$ to map to a non-singular curve over $\mathbb{F}_p$. In this case, we say that E has *good reduction modulo p*.

For elliptic curves over fields with a positive characteristic, there are two possibilities. Either the curve is ordinary or the curve is supersingular. Our research focuses only on ordinary curves, in which one could intuitively say that the endomorphisms behave similar to endomorphism rings for curves over fields with characteristic 0. In case a curve is supersingular, we have that $\mathrm{End}(\bar{E})$ is an order in a quaternion algebra. More information about this case can be found in [9, Section V.3] and [2]. Note that supersingular curves are non-singular, although the naming might suggest otherwise.

Under what conditions are we reducing modulo p to ordinary curves? These are described in Deuring's Reduction Theorem, introduced by German mathematician M. Deuring in 1941 [3]. We use [2] combined with [10, Proposition 4.4] to get a nice formulation of the theorem. We adjusted the theorem a little bit to fit in our case. A proof of this theorem can be found in [7, Chapter 13, Section 4, Theorem 12], however this proof is far from elementary.

Theorem 3.2. *Let E be an elliptic curve defined over a number field K. Let End(E) be isomorphic to some order $\mathcal{R}$ in an imaginary quadratic field $\mathcal{K}$, and let E have good reduction modulo p to $\bar{E}$. Then, $\bar{E}(\mathbb{F}_p)$ is ordinary if and only if p splits in $\mathcal{K}$. Let in this case $c = p^r c_0$ be the conductor of End(E) in $\mathcal{K}$ such that $p \nmid c_0$. Then, End$(E) \cong \mathbb{Z} + c_0 R_K$. In this case, $c = c_0$ and reduction modulo p is an isomorphism that preserves degree.*

An explanation of what a conductor is can be found in [7, Section 8.1]. In the cases we treat during this research, we only find conductors that are equal to 1 and 2. It follows that the conditions for the conductor as described in the theorem always holds, hence reduction modulo p is in our case always an isomorphism that preserves degree. We will give the conductor of $\mathbb{Z}[\alpha]$ after we computed the possible quadratic imaginary field extensions and the corresponding α's for each case we will treat.

In our research, the order $\mathcal{R}$ is the ring $\mathbb{Z}[\alpha]$ we have found in section 3.1. We say that p splits in K if (p) can be factorized into two distinct ideals in R_K, which, in our case, is the ring of quadratic integers of the number field K_d. Since in any case $\mathbb{Z}[\sqrt{-d}] \subset R_K$, p can be factorized into two ideals in R_K if

$$(a + b\sqrt{-d})(a - b\sqrt{-d}) = a^2 + db^2 = p$$

for integers $a, b \in \mathbb{Z}$, in which $(a + b\sqrt{-d}) \neq (a - b\sqrt{-d})$ as ideals in R_K.

We now find conditions on a and b such that p is a ramified prime, so we can exclude these cases. We have to check when $(a + b\sqrt{-d}) = (a - b\sqrt{-d})$ as ideals. The two ideals are equal to each other if and only if there exists a unit ϵ such that $\epsilon(a + \sqrt{-d}) = a - b\sqrt{-d}$. Using that the norm is multiplicative, we

can observe that ϵ is a unit if and only if $N(\epsilon) = 1$.

For $d \neq 1, 3$, $N(\epsilon) = 1$ if and only if $\epsilon = \pm 1$. It follows that we have a ramified prime if and only if $a = 0$. Hence, we need to require $a \neq 0$. In case we get such a ramified prime p, we have $db^2 = p$, which, by definition of a prime number in the integers, requires $b^2 = 1$ and $d = p$ to be a prime number.

In the case where $d = 1$, $\epsilon = \pm 1$ is still possible, but there is also the possibility that $\epsilon = \pm\sqrt{-1}$. Let us explore that case. For convenience, we say $\epsilon = \delta\sqrt{-1}$, where δ can be either 1 or -1. Observe that from $\delta\sqrt{-1}(a+b\sqrt{-1}) = (a-b\sqrt{-1})$, it follows that $a = -\delta b$. Hence, we have a ramified prime whenever $a^2 = b^2$, or equivalently, when we have a factorization of the form

$$\begin{aligned}(\delta a + a\sqrt{-1})(\delta a - a\sqrt{-1}) &= p \\ a^2 + a^2 &= p \\ 2a^2 &= p\end{aligned}$$

It follows that we only need to exclude $p = 2$ to avoid ramified primes in $\mathbb{Z}[\sqrt{-1}]$, but this case is already excluded in order to have good reduction modulo p.

In case $d = 3$, we can also have $\epsilon = \frac{1\pm\sqrt{-3}}{2}$. In a method similar to the previous method, we can conclude that $12a^2 = p$ for a prime number p and an integer a. This is impossible, hence also here, we do not exclude anything.

In conclusion, we require $p = a^2 + db^2$, where $a \neq 0$, b are integers. Interestingly enough, finding primes that can be written in this form is a relevant topic of research in number theory. We will use [1] and write the results for all values of d we discover in our research. It is important to note that the book sometimes does use complex multiplication to find these prime numbers, but the cases for d we will encounter are done with a different approach, hence we are not at risk for circular reasoning.

4 Finding endomorphisms of degree 2

Before we want to find elliptic curves that have endomorphisms of degree 3 and 4, we will first work out the computation for an easier case, namely endomorphisms of degree 2. Silverman [10, Proposition II.2.3.1] computes all such curves as an example. Although the general steps are in there, a lot of details are left out. Therefore, we will work out the degree-2-case in more detail here. Note that, although this computation partly serves as an example, using the fact that degrees on endomorphisms are multiplicative, some of the work done here will show up again in the case of degree 4.

4.1 Finding the corresponding imaginary quadratic field extensions of $\mathbb{Q}$

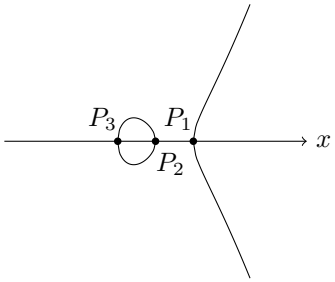
We will follow the procedure as described in Section 3.1, with $m = 2$. We first want to note that $b \neq 0$ in this case because it would require $a = \pm\sqrt{2}$, while we require $a \in \mathbb{Z}$. In case m would be a square, say n^2, this case would correspond to the multiplication-by-n-map.

Now, we continue for the cases where the E has complex multiplication. First, assume $d \equiv 1, 2 \mod 4$. We want to find integers a, b such that $a^2 + db^2 = 2$.
If $a = 0$, then $db^2 = 2$. It follows that $b = \pm 1$, $d = 2$. This results in $\alpha = \pm\sqrt{-2}$.
If $a = \pm 1$, then $db^2 = 1$. Since $b \neq 0$, we have $b = 1$ and $d = 1$. This results in $\alpha = 1 \pm \sqrt{-1}$.
Now, we consider $d \equiv 3 \mod 4$, hence we try to find integers a, b such that $\frac{a^2+db^2}{4} = 2$, hence $a^2 + db^2 = 8$. It is then easy to check for cases $a = 0, 1, 2$ that the only possibility that solves the equation for $d \equiv 3 \mod 4$ is $a = b = 1, d = 7$, so $\alpha = \frac{1\pm\sqrt{-7}}{2}$.

If ρ is the isomorphism we described in Section 2.5, then we can see that in each case, $\mathbb{Z}[\alpha] \subseteq \rho(\mathrm{End}(E)) \subseteq R_K = \mathbb{Z}[\alpha]$. Hence, $\mathrm{End}(E) \cong \mathbb{Z}[\alpha]$. We summarize what we have found so far.

- $K = \mathbb{Q}(\sqrt{-1}), \quad \alpha = 1 + \sqrt{-1}, \quad \mathrm{End}(E) \cong \mathbb{Z}[\sqrt{-1}]$.
- $K = \mathbb{Q}(\sqrt{-2}), \quad \alpha = \sqrt{-2}, \quad \mathrm{End}(E) \cong \mathbb{Z}[\sqrt{-2}]$.
- $K = \mathbb{Q}(\sqrt{-7}), \quad \alpha = \frac{1+\sqrt{-7}}{2}, \quad \mathrm{End}(E) \cong \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$.

In all these cases, the ring of maximal order R_K is equal to $\mathcal{R} = \mathbb{Z}[\alpha]$. Hence, the conductor will be equal to 1 in each case.



4.2 Finding isogenies of degree 2

This section will try to construct isogenies that have a kernel of order 2, using Vélu's formulae, Theorem 3.1. As discussed in Section 3.2, we want to know how a subgroup with order 2 looks like. Note that a group of order 2 always consists of a point of order 2 together with the unit element. Let us hence look at how a point of order 2 looks like on the curve.

A point P is of order 2 if and only if $2P = P + P = \mathcal{O}$, hence, P is of order 2 if the tangent line l at P on the curve is vertical, which happens when P lies on the x-axis. It follows that any point of order 2 is of the form $(c, 0)$ for some $c \in \mathbb{Q}$.

Now, using that translation of coordinates is an isomorphism, we can use that the map $T : (x, y) \mapsto (x + c, y)$ is an isomorphism. T maps to a curve $\bar{E}$ defined by

$$\begin{aligned} y^2 &= (x+c)^3 + A(x+c) + B \\ &= x^3 + 3cx^2 + (3c^2 + A)x + c^3 + Ac + B \\ &= x^3 + 3cx^2 + (3c^2 + A)x \\ &= x^3 + ax^2 + bx \end{aligned}$$

where $a = 3c$, $b = 3c^2 + A$. Visually we could say that without loss of generality, for any point P_1 of order 2, we can place the y-axis such that P_1 lies on the origin. Using this isomorphism, we lose our constant term and gain a quadratic term in the defining equation for E.

4.3 Finding isogenies that map to curves isomorphic to its domain

Since $G = \{\mathcal{O}, (0, 0)\}$, we have $G_1 = \emptyset$ and $G_2 = (0, 0)$ in the notation of Vélu's formulae. We get $F_x(0, 0) = b$, $F_y(0, 0) = 0$, hence $t((0, 0)) = b$ and $u((0, 0)) = 0$. In order to align our computations with those of Silverman, we use Theorem 3.1, but we apply the translation of coordinates $x \mapsto x + a$ after we applied Vélu's formulae. The resulting isogenies with kernel G have the form

$$\phi(x, y) = \left(x + a + \frac{b}{x}, y - \frac{by}{x^2} \right). \tag{5}$$

In this case, ϕ maps to E' with equation

$$y^2 = x^3 - 2ax^2 + (a^2 - 4b)x.$$

We now compute the j-invariants of both E and E'

$$\begin{aligned} j(E) &= 256\frac{(a^2-3b)^3}{b^2(a^2-4b)}, \\ j(E') &= 256\frac{(4a^2-3(a^2-4b))^3}{(a^2-4b)^2(4a^2-4(b^2-4a))} \\ &= 256\frac{(a^2+12b)^3}{16b(a^2-4b)^2} \end{aligned}$$

We know that $E \cong E'$ if and only if $j(E) = j(E')$ which leads to the equation

$$\begin{aligned} & j(E) = j(E') \\ \iff & 256\frac{(a^2-3b)^3}{b^2(a^2-4b)} = 256\frac{(a^2+12b)^3}{16b(a^2-4b)^2} \\ \iff & \frac{(a^2-3b)^3}{b^2(a^2-4b)} - \frac{(a^2+12b)^3}{16b(a^2-4b)^2} = 0 \end{aligned}$$

If we factorize the numerator of the resulting fraction, we get

$$16b(a^2-4b)a^2(a^2-8b)(16a^4-81a^2b+324b^2) = 0$$

Hence, the isogeny we found maps to a curve with the same j-invariant if and only if one of these factors is zero. However, we need to exclude two of these factors. Note that for equations of the form $y^2 = x^3+ax^2+bx$, the discriminant is

$$\begin{aligned} \Delta &= b^2a^2 - 4b^3 \\ &= b^2(a^2-4b) \end{aligned}$$

Hence, $b = 0$ and $a^2 - 4b = 0$ are excluded because in that case, E is singular. Note that in these cases, also the j-invariant is undefined. Then, there are three cases left, corresponding to three factors.

Case 1: $a = 0$

Now, consider the case $a = 0$. Note that it follows that we have a curve of the form $y^2 = x^3 + bx$. Since the j-invariant of this curve is

$$\begin{aligned} j &= \frac{-27 \cdot 256b^3}{-4b^3} \\ &= 1728, \end{aligned}$$

it is independent of b, hence every curve of such form in in the same isomorphism class, independent of our choice for b. If we take the curve $E : y^2 = x^3 + x$, we get the isogeny

$$\phi(x, y) = \left(x + \frac{1}{x}, y - \frac{y}{x^2}\right)$$

that maps to the curve $E' : Y^2 = X^3 - 4X$.
This corresponds to the field extension $\mathbb{Q}(\sqrt{-1})$ with $\alpha = 1 + \sqrt{-1}$. We can construct an isomorphism φ from E' to E using the Magma code that at the bottom of this section:

$$\varphi(x, y) = \left(-\frac{\sqrt{-1}}{2}x, \frac{\sqrt{-1}+1}{4}y\right).$$

Using $\mu = \varphi \circ \phi$, our endomorphism becomes

$$\mu(x, y) = \left(-\frac{\sqrt{-1}}{2}\left(x + \frac{1}{x}\right), \frac{\sqrt{-1}+1}{4}\left(y - \frac{2y}{x^2}\right)\right).$$

Case 2: $a^2 - 8b = 0$

The next case is the case $a^2 - 8b = 0$. Here, we can write the j-invariant as

$$\begin{aligned} j &= 256\frac{(a^2 - 3b)^3}{b^2(a^2 - 4b)} \\ &= 256\frac{(a^2 - 8b + 5b)^3}{b^2(a^2 - 8b + 4b)} \\ &= 256\frac{(5b)^3}{b^2(4b)} \\ &= \frac{256 \cdot 125}{4} \\ &= 8000. \end{aligned}$$

Hence, if $a^2 - 8b = 0$, then independent of our choice for a and hence our choice of b, we end up in the same isomorphism class. Therefore, this case leads to the isomorphism class with j-invariant 8000, or the class of curves isomorphic to $E : y^2 = x^3 + 4x^2 + 2x$. This results in the isogeny

$$\phi(x, y) = \left(x + 4 + \frac{2}{x}, y - \frac{2y}{x^2}\right)$$

that maps to the curve $E' : Y^2 = X^3 + 4X^2 - 8X - 32$. The case where $j = 8000$ corresponds to the field extension $\mathbb{Q}(\sqrt{-2})$ with $\alpha = \sqrt{-2}$. The isomorphism φ from E' to E is found to be

$$\varphi(x, y) = \left(-\frac{1}{2}x, \frac{\sqrt{-2}}{4}y\right).$$

Using $\mu = \varphi \circ \phi$, our endomorphism becomes

$$\mu(x, y) = \left(-\frac{1}{2}\left(x + 4 + \frac{2}{x}\right), \frac{\sqrt{-2}}{4}\left(y - \frac{2y}{x^2}\right)\right).$$

Case 3: $16a^4 - 81a^2b + 324b^2 = 0$

The last case we need to consider is the case where $16a^4 - 81a^2b + 324b^2 = 0$. It follows from considering the equation as a polynomial in b that

$$\begin{aligned} b &= \frac{81a^2 \pm \sqrt{81^2a^4 - 4 \cdot 16 \cdot 324a^4}}{2 \cdot 324} \\ &= \frac{a^2}{648}(3^4 \pm \sqrt{3^8 - 2^8 3^4}) \\ &= \frac{3^2a^2}{2^3 3^4}(3^2 \pm \sqrt{3^4 - 2^8}) \\ &= \frac{a^2}{72}(9 \pm \sqrt{-175}) \\ &= \frac{a^2}{72}(9 \pm 5\sqrt{-7}) \end{aligned}$$

In this case, the j-invariant can be computed:

$$\begin{aligned} j &= 256\frac{(a^2 - 3b)^3}{b^2(a^2 - 4b)} \\ &= 256\frac{(a^2 - \frac{a^2}{24}(9 + 5\sqrt{-7}))^3}{\frac{a^4}{5184}(-94 + 90\sqrt{-7})(a^2 - \frac{a^2}{18}(9 + 5\sqrt{-7})} \\ &= 256 \cdot 5184\frac{a^6}{a^6}\frac{(\frac{5}{8} - \frac{5}{24}\sqrt{-7})^3}{(-94 + 90\sqrt{-7})(\frac{1}{2} - \frac{5}{18}\sqrt{-7})} \\ &= 256 \cdot 5184\frac{a^6}{a^6}\frac{(\frac{5}{8} - \frac{5}{24}\sqrt{-7})^3}{(128 + \frac{640}{9}\sqrt{-7})} \\ &= 256 \cdot 5184\frac{-125}{49152} \\ &= -3375 \end{aligned}$$

Hence, again, once we satisfy $16a^4 - 81a^2b + 324b^2 = 0$, we stay in the same isomorphism class independent of the values for a and b.
One of the curves in this isomorphism class is the curve where $a = 12$ and $b = 2(9 + 5\sqrt{-7})$, so one curve in this isomorphism class is $y^2 = x^3 + 12x^2 + (18 + 10\sqrt{-7})x$. This results in the isogeny

$$\phi(x, y) = \left(x - 12 + \frac{2(9 + 5\sqrt{-7})}{x}, y + \frac{2(9 + 5\sqrt{-7}))y}{x^2}\right)$$

that maps to the curve $E' : y^2 = x^3 - 24x^2 + 8(9 - 5\sqrt{-7})x$.

This case corresponds to the field extension $\mathbb{Q}(\sqrt{-7})$ with $\alpha = \frac{1+\sqrt{-7}}{2}$. Here, we use two transformations of coordinates because we want to define our endomorphism on a curve defined over $\mathbb{Q}$. All the following curves have j-invariant

-3375:

$$\widetilde{E} : y^2 = x^3 - 35x + 98$$
$$E : y^2 = x^3 + 12x^2 + (18 + 10\sqrt{-7})x$$
$$E' : y^2 = x^3 - 24x^2 + 8(9 - 5\sqrt{-7})x$$

We have constructed an isogeny ϕ from $E \to E'$. Hence, we can construct an endomorphism $\mu = \delta \circ \phi \circ \varphi : \widetilde{E} \to \widetilde{E}$, where $\varphi : \widetilde{E} \to E$ is a transformation of coordinates, $\phi : E \to E'$ is the isogeny we constructed, and $\delta : E' \to \widetilde{E}$ is another transformation of coordinates. Using Magma, we construct δ and φ:

$$\varphi(x, y) = (u^2x - 4, u^3y)$$
$$\delta(x, y) = (v^2x - 8v^2, v^3y)$$

where $u = \sqrt{\frac{7-\sqrt{-7}}{7}}$, $v = \sqrt{\frac{\sqrt{-7}-7}{16}}$.
The resulting endomorphism $\mu : \widetilde{E} \to \widetilde{E}$ is then found.

$$\mu = \delta \circ \mu \circ \varphi : (x, y) \mapsto (X, Y) \tag{6}$$

where

$$\begin{aligned} X &= v^2 \left(u^2x - 4 - 12 + \frac{2(9 + 5\sqrt{-7})}{u^2x - 4} \right) - 8v^2 \\ &= u^2v^2x - 24v^2 + \frac{2(9 + 5\sqrt{-7})v^2}{u^2x - 4} \\ &= \left(\frac{\sqrt{-7} - 3}{8}x - \frac{3\sqrt{-7} - 21}{2} - \frac{91\sqrt{-7} + 343}{(28 - 4\sqrt{-7})x - 112} \right) \\ Y &= v^3 \left(u^3y + \frac{2(9 + 5\sqrt{-7}))u^3y}{(u^2x - 4)^2} \right) \\ &= \left(\frac{\sqrt{-7} - 3}{8} \right)^{3/2} \left(\frac{7(9 + 5\sqrt{-7})}{(7 - \sqrt{-7})x - 28} \right) \end{aligned}$$

The code that is used for the construction of the isomorphisms is the following:

```
K:=AlgebraicClosure();
R<x>:=PolynomialRing(K);
Roots(x^2 + 7);
f1:=x^3 + 12*x^2 + 2*(9 + 5*K.1)*x;
f2:=x^3 - 24*x^2 + 8*(9 - 5*K.1)*x;
f3:=x^3 - 35*x + 98;
E1:=EllipticCurve(f1);
E2:=EllipticCurve(f2);
E3:=EllipticCurve(f3);
Isomorphism(E3,E1);
K;
```

in which we of course change the polynomials `f1`, `f2`, `f3` to find isomorphisms between the curves that we are interested in.

4.4 Reduction modulo p

Now, we want to see whether we can generate endomorphisms of degree 2 over finite fields, by reducing modulo p. We assume $p > 2$ because $p = 2$ prevents us from having good reduction modulo p. In general, we want $p \nmid 2\Delta$ and $a^2 + db^2 = p$ for $a, b \in \mathbb{Z}$.

In section 3.4, the exact conditions for p are derived. In the isomorphism class $j = 1728$, we have the corresponding quadratic imaginary field extension $\mathbb{Q}(\sqrt{-1})$. The conditions for p are then that we can find integers a, b such that $a^2 + b^2 = p$. In [1, Introduction], we find that this is equivalent to requiring $p \equiv 1 \mod 4$.

Proposition 4.1. *Let $\bar{E}$ be an elliptic curve defined by $y^2 = x^3 + x$ over $\mathbb{F}_p$, where p is a prime number such that $p \equiv 1 \mod 4$. Then, End$(\bar{E}) \cong \mathbb{Z}[\sqrt{-1}]$.*

For reducing endomorphisms in the class with j-invariant 8000 in the form that we derived earlier, the corresponding field extension is $\mathbb{Q}(\sqrt{-2})$, hence we require $a^2 + 2b^2 = p$ for $a, b \in \mathbb{Z}$, which is equivalent to $p \equiv 1, 3 \mod 8$, according to [1, Introduction].

Proposition 4.2. *Let $\bar{E}$ be an elliptic curve defined by $y^2 = x^3 + 4x^2 + 2x$ over $\mathbb{F}_p$, where p is a prime number such that $p \equiv 1, 3 \mod 8$. Then, End$(\bar{E}) \cong \mathbb{Z}[\sqrt{-2}]$.*

For $j = -3375$, we can take the curve $x^3 - 35x + 98$. Reduction modulo p will be possible under the condition that $p \equiv 1, 9, 11, 15, 23, 25 \mod 28$, according to [1, Equation (2.17)].

Proposition 4.3. *Let $\bar{E}$ be an elliptic curve defined by $y^2 = x^3 - 35x + 98$ over $\mathbb{F}_p$, where p is a prime number such that $p \equiv 1, 9, 11, 15, 23, 25 \mod 28$. Then, End$(\bar{E}) \cong \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$.*

5 Finding Endomorphisms of Degree 4

In this section, we will describe all possible endomorphisms of degree 4 on elliptic curves over $\mathbb{Q}$. The approach is very comparable to what we did earlier in degree 2, and some of the cases will show up again in case of degree 4. One of the cases we will compute will have j-invariant that is not in $\mathbb{Q}$ anymore, but lives in $\mathbb{Q}(\sqrt{5})$. This makes some of the things we did earlier a bit harder. Often, the expressions become harder to deal with, hence we will utilize Magma to compute the expressions.

5.1 Finding the corresponding quadratic imaginary field extensions of $\mathbb{Q}$

Again, we compute the quadratic imaginary field extensions of $\mathbb{Q}$ in a similar approach as in degree 2.

In case $d \equiv 1, 2 \mod 4$, we get the equation $a^2 + bd^2 = 4$. In case $b = 0$, $a = 2$, this corresponds to the multiplication-by-2-map, which is an endomorphism of degree 4, see also the beginning of Section 2.5. In case $b \neq 0$, we are looking for curves with complex multiplication of degree 4:
If $a = 0$, $db^2 = 4$, hence $b = 2$, $d = 1$: $\alpha = 2\sqrt{-1}$.
If $a = \pm 1$, $db^2 = 3$, hence $b = 1$ and $d = 3 \not\equiv 1, 2 \mod 4$. This possibility shows up in the case $d \equiv 3 \mod 4$, we will have $1 + \sqrt{-3}$.

In case $d \equiv 3 \mod 4$, we solve the equation $a^2 + bd^2 = 16$.
If $a = \pm 0$, then $db^2 = 16$, hence $b = 4$, $1 \not\equiv 3 \mod 4$, hence we exclude this case.
If $a = \pm 1$, then $db^2 = 15$, hence $b = 1$, $d = 15 \equiv 3 \mod 4$, so $\alpha = \frac{1+\sqrt{-15}}{2}$.
If $a = \pm 2$, then $db^2 = 12$, hence $b = 2$, $d = 3 \equiv 3 \mod 4$, so $\alpha = 1 + \sqrt{-3}$
If $a = \pm 3$, then $db^2 = 7$, hence $b = 1$, $d = 7 \equiv 3 \mod 4$, so $\alpha = \frac{3+\sqrt{-7}}{2}$.
$a = 4$ again corresponds to the multiplication-by-2-map.

Since we have already in degree 2, $1 + \sqrt{-1} \in \mathrm{End}(E)$, hence $\mathrm{End}(E) \cong \mathbb{Z}[\sqrt{-1}]$. In this case, we will also find a class of curves E with $\mathrm{End}(E) \cong \mathbb{Z}[2\sqrt{-1}]$. Also, since $\frac{1+\sqrt{-3}}{2}$ is a unit in $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$, it is an automorphism of degree 1, which is an isomorphism on the curve. It follows that $\mathrm{End}(E) \cong \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$. For the other two cases, we have that $\mathrm{End}(E) \cong \mathbb{Z}[\alpha]$. We summarize the results we have now.

In conclusion, we get the following cases with complex multiplication of degree 4:

- $K = \mathbb{Q}(\sqrt{-1})$, $\alpha = 2\sqrt{-1}$, $\mathrm{End}(E) \cong \mathbb{Z}[\sqrt{-1}]$ or $\mathrm{End}(E) \cong \mathbb{Z}[2\sqrt{-1}]$

- $K = \mathbb{Q}(\sqrt{-3}), \quad \alpha = 1 + \sqrt{-3}, \quad \text{End}(E) \cong \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$
- $K = \mathbb{Q}(\sqrt{-7}), \quad \alpha = \frac{3+\sqrt{-7}}{2}, \quad \text{End}(E) \cong \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$
- $K = \mathbb{Q}(\sqrt{-15}), \quad \alpha = \frac{1+\sqrt{-15}}{2}, \quad \text{End}(E) \cong \mathbb{Z}\left[\frac{1+\sqrt{-15}}{2}\right]$

In the cases where $\alpha = 2\sqrt{-1}$ and $\alpha = 1 + \sqrt{-3}$, we have that the maximal orders are $R_K = \mathbb{Z}[\sqrt{-1}]$ and $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ respectively. Hence, in these two cases, the conductor is equal to 2. Note that $\frac{3+\sqrt{-7}}{2} = 1 + \frac{1+\sqrt{-7}}{2}$, hence $\mathbb{Z}[\frac{3+\sqrt{-7}}{2}] = \mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$, and the conductor is equal to 1.
Note that all cases for α in degree 2 also appear as α^2 here.

$$\begin{aligned}(1+\sqrt{-1})^2 &= 2\sqrt{-1} \\ (\sqrt{-2})^2 &= -2 \text{ corresponds to multiplication by 2} \\ \left(\frac{1+\sqrt{-7}}{2}\right)^2 &= \frac{-3+\sqrt{-7}}{2}\end{aligned}$$

5.2 Finding endomorphisms of degree 4

A group of order 4 can only take 2 forms. Either they consist of the unit element and 3 points of order 2, the so-called *Klein Four Group*, or it is a cyclic group generated by a point of order 4.

We find the Klein subgroup by finding the three points of order 2 of the elliptic curve. If we want an endomorphism with such a subgroup as kernel, we want to find an endomorphism μ such that $\mu(P) = 0 \iff 2P = \mathcal{O}$. Any elliptic curve that has three points of order 2 has such an endomorphism because it is the multiplication-by-2-map. Hence, we will not find any curves with complex multiplication here.

In the case where the subgroup is a cyclic group, we will find curves with complex multiplication. Since expressions for the coefficients tend to become complicated in this case, we prevent this by assuming a very specific form. For this, we refer to [6, Theorem 3.11], where we find a form that is constructed in such a way that the curve has point of order 4 at $(0, 0)$.

$$y^2 + xy - by = x^3 - bx^2$$

Note that this form is only dependent on one parameter b, which makes some of the computations a lot more convenient.

Let us first explain why $(0,0)$ is a point of order 4. Note that, since we use the long Weierstrass form, it is no longer true that points of order 2 lie on the x-axis. Also, note that $(0,0)$ lies on the curve as it satisfies the defining equation. To compute $(0,0)+(0,0)$, we compute the tangent line at $(0,0)$. Using implicit differentiation, we compute

$$\frac{dy}{dx} = \frac{3x^2 - 2bx - y}{2y + x - b},$$

hence at $(0,0)$, $\frac{dy}{dx} = 0$. Hence, our tangent line l will be equal to the x-axis, which intersects the curve at $x = 0$ and $x = b$. It follows that $(0,0) + (0,0) = (b,0)$. Again, using the formula for $\frac{dy}{dx}$, it is clear that $(b,0)$ has a vertical tangent line. In general, using a long Weierstrass form, we do not have that a vertical line necessarily intersects the point at infinity. However, it is the case here, as we can check using Magma. We conclude that $(b,0)$ is a point of order 2. It follows that our equation has a cyclic subgroup of order 4 generated by $(0,0)$.

Now, we will compute the isogeny and its image curve having this subgroup as its kernel by applying theorem 3.1 once again. Note that $a_1 = 1$, $a_2 = -b$, $a_3 = -b$, $a_4 = a_6 = 0$. We have $G_1 = \{(0,0)\}$ and $G_2 = \{(b,0)\}$. Hence,

$$\begin{aligned} t((0,0)) &= -b \\ u((0,0)) &= b^2 \\ t((b,0)) &= b^2 \\ u((b,0)) &= 0 \\ t(G) &= b^2 - b \\ w(G) &= b^3 + b^2 \end{aligned}$$

The isogeny then becomes

$$\phi(x,y) \mapsto (X,Y)$$

where

$$\begin{aligned} X &= x + \frac{b}{x} + \frac{b^2}{x^2} + \frac{b^2}{x-b} \\ Y &= y - \frac{b^2(2y+x-b)}{x^3} - \frac{b^2 - b(x+y)}{x^2} - \frac{b^2(x+y-b)}{(x-b)^2} \end{aligned} \tag{7}$$

which maps to the curve E' defined by

$$Y^2 + XY - bY = X^3 - bX^2 - 5(b^2 - b)X - 3b^3 - 12b^2 + b \tag{8}$$

We follow the same strategy we used earlier in the degree-2-case. This means that we will solve for which b the image curve and the original curve have the same j-invariant. Instead of doing this by hand, we use the following Magma code:

```
K<b>:=RationalFunctionField(Rationals());
R<x>:=PolynomialRing(K);
E:=EllipticCurve(x^3-b*x^2,x-b);
E2:=
EllipticCurve(x^3-b*x^2 -5*(b^2 - b)*x -3*b^3 - 12*b^2 + b, x-b);
Factorization(Numerator(jInvariant(E)-jInvariant(E2)));
```

The code first defines b as a variable, and we define our polynomial ring. Then, we define the original curve and the image curve, and solve $j(E)-j(E')=0$ by factorizing its numerator. This gives the following factors:

$$b+\frac{1}{32}$$
$$b^2+\frac{1}{16}b+\frac{1}{256}$$
$$b^2+\frac{1}{16}b+\frac{1}{16}$$
$$b^4+\frac{1}{8}b^3+\frac{753}{256}b^2+\frac{47}{256}b+\frac{1}{256}$$

Case 1: $b=-\frac{1}{32}$

The case $b=-\frac{1}{32}$ corresponds to j-invariant 287496. Using Magma, we construct the isomorphism

$$\varphi(x,y)=\left(-\frac{1}{4}x-\frac{15}{28},-\frac{1}{4\cdot 2\sqrt{-1}}y+\left(\frac{1}{8}-\frac{1}{8\cdot 2\sqrt{-1}}\right)x-\frac{1}{256\cdot 2\sqrt{-1}}+\frac{11}{256}\right)$$

which corresponds to the field $\mathbb{Q}(\sqrt{-1})$. We create our endomorphism by composing this with the isogeny defined in equation (7), substituting $b=-\frac{1}{32}$

Case 2: $b^2+\frac{1}{16}b+\frac{1}{256}=0$

The case $b^2+\frac{1}{16}b+\frac{1}{256}=0$ gives us the j-invariant 54000. We substitute the root $b=\frac{1}{32}(-1-\sqrt{-3})$ into the equation (8). The other root will result in a curve that is isomorphic to this one, so we do not have two distinct cases. Let ϕ be the isogeny of equation (7), using $b=\frac{1}{32}(-1-\sqrt{-3})$. Similar to the case with j-invariant -3375 in degree 2, we can construct a curve $\widetilde{E}$ defined over $\mathbb{Q}$ with j-invariant 54000. In this case, we have the following three curves, all isomorphic to each other:

$$\widetilde{E}: y^2=x^3-\frac{3375}{121}x+\frac{6750}{121}$$
$$E: y^2+xy-by=x^3-bx^2$$
$$E': y^2+xy-by=x^3-bx^2-5(b^2-b)x-3b^3-12b^2+b$$

We construct two transformations of coordinates, $\varphi : \widetilde{E} \to E$ and $\delta : E' \to \widetilde{E}$. Using Magma, we find

$$\varphi(x,y) = \left(u^2 x - \frac{9+\sqrt{-3}}{96}, u^3 y - \frac{u}{2}x + \frac{3-\sqrt{-3}}{96}\right)$$
$$\delta(x,y) = \left(v^2 x + \frac{15\sqrt{-3}-75}{88}, v^3 y + \frac{v^3}{2}x - 15v\frac{3+\sqrt{-3}}{176}\right)$$

where

$$u = \sqrt{\frac{33-11\sqrt{-3}}{1440}}$$
$$v = \sqrt{\frac{30\sqrt{-3}-90}{11}}$$

We then construct our endomorphism by the composition $\mu = \delta \circ \phi \circ \varphi$.

Case 3: $b^2 + \frac{1}{16}b + \frac{1}{16} = 0$

The case $b^2 + \frac{1}{16}b + \frac{1}{16} = 0$ yields the j-invariant -3375. Note that this is the same isomorphism class, corresponding to $\mathbb{Q}(\sqrt{-7})$, as in the degree-2-case. It follows that the endomorphism is created by composing the map described in equation (6) with itself, using that the degree of an isogeny is multiplicative.

Case 4: $b^4 + \frac{1}{8}b^3 + \frac{753}{256}b^2 + \frac{47}{256}b + \frac{1}{256} = 0$

The case $b^4 + \frac{1}{8}b^3 + \frac{753}{256}b^2 + \frac{47}{256}b + \frac{1}{256} = 0$ is harder because the j-invariant is irrational. Using the following code,

```
K:=AlgebraicClosure();
R<x>:=PolynomialRing(K);
Roots(x^4 + 1/8*x^3 + 753/256*x^2 + 47/256*x + 1/256);
b:=K.1;
E:=EllipticCurve(x^3-b*x^2,x-b);
E2:=EllipticCurve(x^3-b*x^2 - 5*(b^2 - b)*x - 3*b^3 - 12*b^2 + b,
x-b);
jInvariant(E);
jInvariant(E2);
MinimalPolynomial(jInvariant(E2));
```

we find that the j-invariant is a root of the polynomial $x^2+191025x-121287375$, which is irreducible over $\mathbb{Q}$. This polynomial has two distinct roots. Since distinct j-invariants give distinct isomorphism classes, we actually have two isomorphism classes here.

Let us take a closer look. There are 4 possible values for b, that is, there are 4 roots of the original factor, $b^4 + \frac{1}{8}b^3 + \frac{753}{256}b^2 + \frac{47}{256}b + \frac{1}{256} = 0$:

$$b = -\frac{1}{32} \pm \frac{\sqrt{-1503 - 672\sqrt{5}}}{32}$$
$$b = \frac{-47 - 21\sqrt{5} \pm \sqrt{-1605 - 714\sqrt{5}}}{32(47 + 21\sqrt{5})}$$

Depending on which of the four roots we take, we create two j-invariants by substituting each b for each of these roots. The two j-invariants are

$$j = -\frac{191025 + 85995\sqrt{5}}{2}$$

and

$$j = \frac{-191025 + 85995\sqrt{5}}{2}$$

as these are the solutions of the polynomial we found earlier.

```
K:=AlgebraicClosure();
R<x>:=PolynomialRing(K);
Roots(x^2 - 5);
Roots((x + 1/32)^2 - (-1503 - 672*K.2)/(32^2));
b:=K.4;
E:=EllipticCurve(x^3-b*x^2,x-b);
E2:=EllipticCurve(x^3-b*x^2 - 5*(b^2 - b)*x - 3*b^3 - 12*b^2 + b,
x-b);
jInvariant(E);
jInvariant(E2);
Isomorphism(E2,E);
K;
```

The isomorphisms can be computed using the provided Magma code, allowing us to give an endomorphism of degree 4. Due to lack of space, we will not write the full result here.

5.3 Reduction modulo p

The conditions for reduction modulo p are very similar to how we described the conditions in Section 4.4. Again, we assume $p \geq 3$.

Proposition 5.1. *Let $\bar{E}$ be an elliptic curve defined by $y^2 + xy + \frac{1}{32}y = x^3 + \frac{1}{32}x^2 - \frac{155}{1024}x - \frac{1405}{32768}$ reduced modulo p, hence defined over $\mathbb{F}_p$, where p is a prime number such that $p \equiv 1 \mod 4$. Then, End$(\bar{E}) \cong \mathbb{Z}[2\sqrt{-1}]$.*

For j-invariant -3375, the results are already in Proposition 4.3.

We now also have the case where $d = 3$. We still want $a^2 + db^2 = p$ for $a, b \in \mathbb{Z}$ here, which happens if $p \equiv 1 \mod 3$, according to [1, Introduction].

Proposition 5.2. *Let $\bar{E}$ be an elliptic curve defined by $y^2 = x^3 - \frac{3375}{121}x + \frac{6750}{121}$ reduced modulo p, hence defined over $\mathbb{F}_p$, where p is a prime number such that $p \equiv 1 \mod 3$. Then, $End(\bar{E}) \cong \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$.*

For the last case, we have a j-invariant that lives in $\mathbb{Q}(\sqrt{-5})$. In Deuring's theorem, Theorem 3.2, we have $K = \mathbb{Q}(\sqrt{5})$, and $\mathcal{K} = \mathbb{Q}(\sqrt{-15})$. We can still reduce modulo p, but the construction of the endomorphism is much harder. The conditions on p will be $p \equiv 1, 19, 31, 49 \mod 60$, taken from [1, Equation (2.28)].

Proposition 5.3. *Let b be such that*

$$b^4 + \frac{1}{8}b^3 + \frac{753}{256}b^2 + \frac{47}{256}b + \frac{1}{256} = 0.$$

Let $\bar{E}$ be the elliptic curve defined by $y^2 + xy - by = x^3 - bx^2 - 5(b^2 - b)x - 3b^3 - 12b^2 + b$, reduced modulo P, hence over $\mathbb{F}_p$, where p is a prime number such that $p \equiv 1, 19, 39, 41 \mod 60$. Then, $End(\bar{E}) \cong \mathbb{Z}\left[\frac{1+\sqrt{-15}}{2}\right]$.

6 Finding Endomorphisms of degree 3

Similarly to the previous cases, we can find the curves that have endomorphisms of degree 3. Finding endomorphisms of degree 3 is not much harder than finding endomorphisms of degree 2. We first did degree 4 because that was initially the main part of the research, and because there are some connections between the problem for degree 2 and for degree 4. For completeness, we also compute endomorphisms of degree 3.

6.1 Finding the corresponding imaginary quadratic field extensions of $\mathbb{Q}$

We find the quadratic imaginary field extensions of $\mathbb{Q}$ here. Note that 3 is not an integer square, hence all curves with endomorphisms of degree 3 are curves with complex multiplication. We try to find quadratic integers α living in a quadratic imaginary field extension of $\mathbb{Q}$ such that $N(\alpha) = 3$. We hence want to solve $a^2 + db^2 = 3$ for $d \equiv 1, 2 \mod 4$, and $a^2 + db^2 = 12$ for $d \equiv 3 \mod 4$.

First, we consider the case $d \equiv 1, 2 \mod 4$.
If $a = 0$, then $db^2 = 3$, hence $b = 1$, $d = 3 \equiv 3 \mod 4$, which we excluded here.
If $a = 1$, then $db^2 = 2$, hence $b = 1$, $d = 2$: We find $\alpha = 1 + \sqrt{-2} \in \mathbb{Q}(\sqrt{-2})$.
If $a \geq 2$, then $db^2 < 0$, so we have considered all cases for $d \equiv 1, 2 \mod 4$.

Now, we consider the case $d \equiv 3 \mod 4$.
If $a = 0$, then $db^2 = 12$, hence $b = 2$, $d = 3$. We find $\alpha = \sqrt{-3} \in \mathbb{Q}(\sqrt{-3})$.
If $a = 1$, then $db^2 = 11$, hence $b = 1$, $d = 11$. We find $\alpha = \frac{1+\sqrt{-11}}{2} \in \mathbb{Q}(\sqrt{-11})$.
If $a = 2$, then $db^2 = 8$, hence $b = 2$, $d = 2$, which corresponds to $\alpha = 1 + \sqrt{-2}$.
If $a = 3$, then $db^2 = 3$, hence $b = 1$, $d = 3$. We find $\alpha = \frac{3+\sqrt{-3}}{2} \in \mathbb{Q}(\sqrt{-3})$.

Note that we have two possible α's in $\mathbb{Q}(\sqrt{-3})$. However, we will only find one class of curves corresponding to the imaginary quadratic field extension $\mathbb{Q}(\sqrt{-3})$, corresponding to $\alpha = \frac{3+\sqrt{-3}}{2}$ because $\frac{3+\sqrt{-3}}{2} = \sqrt{-3}\left(\frac{1-\sqrt{-3}}{2}\right)$, where $\frac{1+\sqrt{-3}}{2}$ is a unit, hence an isomorphism. Therefore, we can compose each endomorphism with an isomorphism in the other curve.

We conclude that we have the following field extensions corresponding to curves having an endomorphism of degree 3:

- $K = \mathbb{Q}(\sqrt{-2}), \quad \alpha = 1 + \sqrt{-2}, \quad \mathrm{End}(E) \cong \mathbb{Z}[\sqrt{-2}]$
- $K = \mathbb{Q}(\sqrt{-3}), \quad \alpha = \frac{1+\sqrt{-3}}{2}, \quad \mathrm{End}(E) \cong \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$
- $K = \mathbb{Q}(\sqrt{-11}), \quad \alpha = \frac{1+\sqrt{-11}}{2}, \quad \mathrm{End}(E) \cong \mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right]$

In all three cases, the conductor is equal to 1.

6.2 Finding isogenies of degree 3

This section deals with constructing isogenies of degree 3 by looking at possible subgroups of order 3, and applying Vélu's Formulae, Theorem 3.1. Note that a group of order 3 is always a cyclic group generated by a point of order 3. For our convenience, we now use a Weierstrass form that has $(0,0)$ as point of order 3. This form can be found in [6, Theorem 3.11], where we also found a convenient form of degree 4.

$$y^2 + axy + by = x^3$$

Let us first explore how the group looks like, and why $(0,0)$ is a point of order 3 here. P is a point of order 3 if and only if $3P = \mathcal{O}$, which is equivalent to $2P = -P$. Hence, we want $(0,0)$ to have a tangent line that intersects at a point Q, such that $-Q = -(0,0)$, hence $Q = (0,0)$. Note that, since we use the long Weierstrass form, $-(0,0)$ is not reflected on the x-axis anymore, but it is still the point on the curve intersecting with the vertical line through $(0,0)$. The vertical line through $(0,0)$ is defined by $x = 0$, hence $-(0,0) = (0,-b)$. If we now show that $(0,0)$ is a point of order 3, then $\{\mathcal{O}, (0,0), (0,-b)\}$ is a subgroup of order 3 on the curve.

Let us now show that $(0,0)$ is a point of order 3, or equivalently, that the tangent line of the curve on $(0,0)$ intersects $(0,0)$ with multiplicity 3. Using implicit differentiation,

$$\frac{dy}{dx} = \frac{3x^2 - ay}{2y + ax + b}$$

Hence, at $(0,0)$, $\frac{dy}{dx} = 0$, which means that the tangent line on the point $(0,0)$ is equal to the x-axis, defined by the equation $y = 0$. It follows by substituting $y = 0$ into the equation of the curve that $x^3 = 0$, which means that the third point that intersects the x-axis is also $(0,0)$. Hence, $(0,0)$ is a point of order 3.

We now apply Theorem 3.1 to the curve with the subgroup of order 3 we found. As defined in the theorem, $a_1 = a, a_3 = b, a_2 = a_4 = a_6 = 0$. Since $G = \{\mathcal{O}, (0,0), (0,-b)\}$ consists of no points of order 2, we have $G_2 = \emptyset, G_1 = \{(0,0)\}$. We have

$$\begin{aligned} t((0,0)) &= ab, \\ u((0,0)) &= b^2, \\ t(G) &= ab, \\ w(G) &= b^2 \end{aligned}$$

Hence, the isogeny ϕ with kernel G is:

$$\phi(x,y) = \left(x + \frac{ab}{x} + \frac{b^2}{x^2}, y - \frac{b^3}{x^3} - \frac{ab(ax + y + b)}{x^2}\right)$$

which maps to the curve

$$y^2 + axy + by = x^3 - 5abx - a^3b - 7b^2$$

We run the following Magma code, which we also used earlier.

```
K<a,b>:=RationalFunctionField(Rationals(),2);
R<x>:=PolynomialRing(K);
E:=EllipticCurve(x^3,a*x + b);
E2:=EllipticCurve(x^3 - 5*a*b*x - a^3*b - 7*b^2, a*x + b);
Factorization(Numerator(jInvariant(E)-jInvariant(E2)));
```

This results in the equation

$$a^3(a^3 - 54b)(a^6 - 64a^3b + 1728b^2)(a^6 - 8a^3b + 216b^2) = 0$$

The case $a = 0$ results in a singular curve, hence we exclude this case. Then, there are three cases left, corresponding to the three field extensions $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\sqrt{-11})$.

Case 1: $a^3 - 54b = 0$

If $a^3 - 54b = 0$, then we get the isomorphism class with j-invariant 54000. Since the j-invariant is independent of our coefficients a and b once $a^3 - 54b = 0$ is satisfied, we choose $a = 6, b = 4$. We find the isogeny

$$\phi(x, y) = \left(x + \frac{24}{x} + \frac{16}{x^2}, y - \frac{64}{x^3} - \frac{24(6x + y + 4)}{x^2}\right)$$

that maps from $E : y^2 + 6xy + 4y = x^3$ to the curve

$$E' : y^2 + 6xy + 4y = x^3 - 120x - 976$$

Using Magma, we construct the isomorphism

$$\varphi(x, y) = \left(-\frac{1}{3}x - 4, -\frac{1}{3\sqrt{-3}}y + \frac{3 - \sqrt{-3}}{3}x - \frac{2}{3\sqrt{-3}} + 10\right)$$

and we obtain our endomorphism by constructing the composition $\varphi \circ \phi$.

Case 2: $1728b^2 - 64a^3b + a^6 = 0$

In the case $1728b^2 - 64a^3b + a^6 = 0$ we can express b in terms of a by considering the equation as a polynomial in b.

$$\begin{aligned} b &= \frac{64a^3 \pm a^3\sqrt{4096 - 6912}}{3456} \\ &= a^3\frac{2^6 \pm 2^4\sqrt{-11}}{2^7 \cdot 3^3} \\ &= a^3\frac{4 \pm \sqrt{-11}}{216}. \end{aligned}$$

In this case, the j-invariant is

$$\begin{aligned} j(E) &= \frac{(a^4 - 24ab)^3}{b^3(a^3 - 27b)} \\ &= \frac{(1 - 24\frac{4\pm\sqrt{-11})}{216})^3}{(1 - 27\left(\frac{4\pm\sqrt{-11}}{216}\right)^3)} \end{aligned}$$

is independent of a and b. For now, we pick the example curve where $a = 6, b = 12 + \sqrt{-11}$. We then have the isogeny $\phi(x, y) = (X, Y)$, where

$$\begin{aligned} X &= x + \frac{6(4 + \sqrt{-11})}{x} + \frac{(4 + \sqrt{-11})^2}{x^2} \\ Y &= y - \frac{(4 + \sqrt{-11})^3}{x^3} - \frac{6(4 + \sqrt{-11})(6x + y + (4 + \sqrt{-11}))}{x^2} \end{aligned}$$

Using similar to what we used in the degree-4-case,

```
K:=AlgebraicClosure();
R<x>:=PolynomialRing(K);
Roots(x^2 + 11);
a:=6;
b:=4 + K.1;
E:=EllipticCurve(x^3,a*x + b);
E2:=EllipticCurve(x^3 - 5*a*b*x - a^3*b - 7*b^2, a*x + b);
jInvariant(E);
jInvariant(E2);
E3:= EllipticCurveFromjInvariant(jInvariant(E));
E3;
varphi:=Isomorphism(E3,E);
delta:=Isomorphism(E3,E2);
K;
```

we get the following three curves with j-invariant -32768:

$$\begin{aligned} \widetilde{E} &: y^2 + xy = x^3 + \frac{9}{8624}x + \frac{1}{34496} \\ E &: y^2 + axy + by = x^3 \\ E' &: y^2 + axy + by = x^3 - 6abx - a^3b - 7b^2 \end{aligned}$$

where $a = 6$, $b = 12 + \sqrt{-11}$. In the code, we have constructed the isomorphisms $\varphi : \widetilde{E} \to E$, `varphi` in the code, and $\delta : E' \to \widetilde{E}$, `delta` in the code. The endomorphism is then found by $\mu = \delta \circ \phi \circ \varphi$, in which ϕ is the isogeny mapping from E to E'.

Case 3: $a^6 - 8a^3b + 216b^2 = 0$

The last case we found is the case where $a^6 - 8a^3b + 216b^2 = 0$. Note that this factor is very similar to the previous one. First we express b in terms of a:

$$\begin{aligned} b &= \frac{8a^3 \pm a^3\sqrt{64 - 864}}{432} \\ &= a^3 \frac{2^3 \pm 2^2\sqrt{-10}}{2^4 3^3} \\ &= a^3 \frac{2 \pm 5\sqrt{-2}}{108} \end{aligned}$$

Again, we get that the j-invariant is independent of our choice of a and hence b once the initial equation $a^6 - 8a^3b + 216b^2 = 0$ is satisfied:

$$\begin{aligned} j(E) &= \frac{(a^4 - 24ab)^3}{b^3(a^3 - 27b)} \\ &= \frac{(1 - 24\frac{2\pm5\sqrt{-2}}{108})^3}{(1 - 27\left(\frac{2\pm5\sqrt{-2}}{108}\right)^3)} \end{aligned}$$

Here, we take an example curve with $a = 6$, $b = 4 + 10\sqrt{-2}$ as parameters. We can find that this case corresponds to the j-invariant 8000. We can use an equivalent approach as in the previous case to find the endomorphism by simply adjusting the values for a and b.

Now we have computed all endomorphisms of degree 3, we want to remark that two of the three cases have found a j-invariant that also showed up in other cases. In the isomorphism class with j-invariant 8000, we have found isogenies of degree 2 and 3, hence we can also construct isogenies for degree 6, by composing these two isogenies. Also, similar behaviour happens with j-invariant 54000 with degree 3 and 4.

6.3 Reduction Modulo p

Again, we describe the conditions for reduction modulo p of the curves E to $\bar{E}$, defined over finite field $\mathbb{F}_p$. Note that we already described the conditions for the fields $\mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\sqrt{-3})$ in Proposition 4.2 and Proposition 5.2 respectively.

The only field extension that we have not seen earlier is $\mathbb{Q}(\sqrt{-11})$. Finding primes of the form $a^2 + 11b^2$ is a harder task compared to earlier cases. Hence, we simply describe the conditions that are derived in Section 3.4.

Proposition 6.1. *Let $\bar{E}$ be an elliptic curve defined by $y^2 + xy = x^3 + \frac{9}{8624}x + \frac{1}{34496}$ reduced modulo p, hence defined over $\mathbb{F}_p$, where p is a prime number of the form $a^2 + 11b^2 = p$. Then, End$(\bar{E}) \cong \mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right]$.*

7 Summary and Conclusion

Computing endomorphisms of degree 2, 3 and 4 uses theory on elliptic curves from many different perspectives. We combined results from complex analysis, algebra, geometry and number theory to describe endomorphisms on elliptic curves over subfields of $\mathbb{C}$. Endomorphisms of degree 4 exist on every curve because we have the multiplication-by-2-map, but the most intriguing cases are the curves that have complex multiplication.

We have computed all isomorphism classes that have complex multiplication of degree 2, 3 and 4, for which we have taken the following steps. First, we showed how a subgroup of order 2, 3 or 4 looks like on an elliptic curve, mostly from a geometrical perspective. Then, we applied Vélu's formulae to find isogenies that have this subgroup as kernel. After that, we used j-invariants to find those isogenies that map to a curve that is isomorphic to the original curve, so that we can construct an isomorphism. We used Magma to construct such an isomorphism, thus creating an endomorphism of the desired degree.

We also did research on how these curves corresponded to imaginary quadratic field extensions, and we described conditions for which we can reduce the constructed endomorphisms modulo p for some prime number p, using Deuring's theorem.

Further research could be done on how to make the endomorphisms reduced modulo p explicit in the harder cases where our curves are no longer defined over $\mathbb{Q}$. Also, the same technique as done in this manuscript can be applied to higher degree.

References

[1] David A. Cox. *Primes of the Form $x^2 + ny^2$*. Wiley, 2013.

[2] Christina Delfs. *Isogenies and Endomorphism Rings of Abelian Varieties of Low Dimension*. PhD thesis, Carl von Ossietzky Universität Oldenburg, 2015.

[3] Max Deuring. Die typen der multiplikatorenringe elliptischer funktionenkörper. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 14:197–272, 1941.

[4] Steven D. Galbraith. *Mathematics of Public Key Cryptography*. Cambridge University Press, 2012.

[5] John T. Tate Joseph H. Silverman. *Rational Points on Elliptic Curves*. Springer, 2015.

[6] Max Kronberg. *Characterizing the Torsion Subgroup of Elliptic Curves over Number Fields*. Master's thesis, Carl von Ossietzky Universität Oldenburg, 2011.

[7] Serge Lang. *Elliptic Functions*. Springer-Verlag, 1973.

[8] Barry Mazur. Modular curves and the eisenstein ideal. *Publications Mathématiques de l'IHÉS*, 47(1):33–186, 1977.

[9] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer, 2009.

[10] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer, 2013.

[11] Horst G. Zimmer Susanne Schmitt. *Elliptic Curves : A Computational Approach*, volume 31 of *De Gruyter studies in Mathematics*. De Gruyter, 2003.

[12] J. Vélu. Isogénies entry courbes elliptiques. *Comptes Rendus de l'Académie des Sciences Paris, Série 1*, (273):238–241, 1971.