UNIVERSITY
OF OSLO

Master's thesis

Supersingular Elliptic Curves

Properties and examples

Andreas Palm Sivertsen

Mathematics
60 ECTS study points

Department of mathematics
Faculty of Mathematics and Natural Sciences

Spring 2023

Andreas Palm Sivertsen

Supersingular Elliptic Curves

Properties and examples

Supervisor:
Kristian Ranestad

Abstract

In this thesis we present the theory of supersingular elliptic curves and provide extensive examples of their properties. We develop necessary theory of orders in number fields and orders in quaternion algebras to describe their endomorphism rings. Examples are calculated using the computer algebra systems SageMath and Magma.

Contents

List of Figures

List of Tables

Introduction

An important property of an elliptic curve is what its endomorphism ring looks like. Most elliptic curves over the rationals or the complex numbers have an endomorphism ring isomorphic to the integers. An interesting class of elliptic curves in and of itself are those which have endomorphism rings isomorphic to some order in an imaginary quadratic number field. These are called elliptic curves with complex multiplication. It turns out every elliptic curve over a field of prime characteristic have an endomorphism ring larger than the integers. In fact, some have an endomorphism rings which are isomorphic to an order of a quaternion algebra and is non-commutative. It is these we call *supersingular* elliptic curves and is the subject of study in this thesis. We present their most important properties and supply comprehensive examples.

There are many equivalent properties one may use to identify whether or not an elliptic curve is supersingular. A supersingular elliptic curve over a field of characteristic equal to some prime p, finite or otherwise, will have no p-torsion points. The computer algebra system SageMath [Sag23] uses this property in a probabilistic supersingular test on curves, taking a number of points and checking their order. For a deterministic test for supersingularity of an elliptic curve, one may use the fact that the number of rational points on the curve is congruent to 1 modulo p, where again p is the characteristic of the field the elliptic curve is defined over. Both Magma [BCP97] and SageMath uses Schoofs point counting algorithm [Sch95] and this property to determine supersingularity deterministically. One may also use the j-invariant of the elliptic curve to confirm supersingularity and is often used for curves over fields of small characteristic in which one knows the Weierstrass equation. More modern algorithms, like that of Sutherland [Sut12] uses the structure of the isogeny graph from an elliptic curve to determine supersingularity. While we define a supersingular elliptic curve by the non-commutativity of its endomorphism rings, a sometimes overlooked class of curves are those who are supersingular but does not have all their endomorphisms defined over the field the curves are defined over.

Using Waterhouse's seminal paper [WM71] on abelian varities over finite fields, Kohel described an equivalence of categories between the category of supersingular elliptic curves and projective right modules of rank one over some order in a quaternion algebra that arises as an endomorphism ring of a supersingular elliptic curve [Koh96, Proposition 5.3]. A similar equivalence categories is described in [Voi21, Chapter 42] which is the one we will present in the course of this thesis.

Outline

The outline of the thesis is as follows. In the first section of chapter 1 we define the general construction of an elliptic curve as a non-singular projective curve of degree 3

in the projective plane. Any such curve will by the Riemann-Roch theorem be given by some Weierstrass equation, and we then do a change of basis to get the classic equation of an elliptic curve in the affine plane, remembering always the point at infinity. We then describe the group law on the rational points of an elliptic curve.

In the second section of chapter 1 we define morphisms between elliptic curves, called isogenies. We present some properties of an isogeny of elliptic curves, and we present the algebraic structures these isogenies admit. We need to define the Tate module of an elliptic curve, and with the help of an important result due to Tate we use this construction to learn about the endomorphism ring.

The second chapter is a collection of the relevant facts relating to supersingular elliptic curves. Section one uses the definition of [Sch87] and [WM71] that a supersingular elliptic curve is an elliptic curve with an non-commutative endomorphism ring over the algebraic closure of the finite field it is defined over. We then present some well known properties that are used to identify supersingularity.

Section two concerns the question of how many supersingular elliptic curves there are. A question to which the answers depends on which field the curves are defined over. We present: which isomorphism classes over the algebraic closure, gives a supersingular elliptic curve, the structure of the supersingular isogeny classes, and lastly the number of twists of elliptic curves.

The two next sections concerns which rings arise as endomorphism rings of supersingular elliptic curves. We begin by introducing some theory of orders in imaginary quadratic number fields, and orders in quaternion algebras. Then we present some results due to [WM71] which uses the structure of endomorphism rings to count isomorphism classes over finite fields. We also give extended examples on what the endomorphism rings looks like for curves over different field extensions of square dimension.

The last section in this chapter's goal is to present the equivalence of categories talked from [Voi21]. We develop some theory of ideals of endomorphism rings of supersingular elliptic curves. We apply this theory to calculate an l-isogeny graph with Magma.

The last chapter consists of some tables of the number of supersingular isomorphism classes and their isogeny classes over the quadratic extension of prime fields. We also discuss methods used in some larger calculations of isomorphism classes and isogenies done in SageMath.

Chapter 1

Elliptic curves and isogenies

1.1 Elliptic curves

This construction is mostly taken from [Sil09, III]. An elliptic curve is a pair (E, O), where $E \subset \mathbb{P}^2$ is a non-singular projective curve of genus 1 and $O \in E$. An elliptic curve (E, O), often just written E, is defined over a field k, written E/k, if the coefficents of a polynoamial defning E are in k and O is a k-rational point.
Using the Riemann-Roch theorem one can prove that every non-singular curve described by the Weierstrass equation 1.1 is an elliptic curve, and conversely any elliptic curve can be given by a Weierstrass equation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^6 \tag{1.1}$$

where $a_i \in k$.
To ease notation, we de-homogenize, letting $x = X/Z$, and $y = Y/Z$, remembering the point $O = [0, 1, 0]$ as the point at infinity and we get the following non-homogeneus equation in the affine plane.

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.2}$$

Assuming the characterstic of k is not 2, we can preform the following change of basis

$$y \to \frac{1}{2}(y - a_1x - a_3)$$

which gives us

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

where the b_i's are polynomials in the a_i's. Then, assuming the characteristics of k is not 3, we preform an additional change of basis

$$(x, y) \to \left(\frac{x - 3b_2}{36}, \frac{y}{108}\right).$$

this gives us

$$y^2 = x^3 - 27c_4x - 54c_6$$

where the c_i's are polynomials in b_i's. Finally we let

$$A := (-27c_4)$$

$$B := (-54c_6)$$

and get the most commonly used equation for an elliptic curve over a field with $\text{char}(k) \neq 2, 3$

$$E : y^2 = x^3 + Ax + B \tag{1.3}$$

This gives an non-singular curve, and therefore an elliptic curve when

$$\Delta := -16(4A^4 + 27B^2).$$

is nonzero. Isomorphism classes of $E/\overline{k}$ are defined by the j-invariant:

$$j := -1728\frac{(4A)^3}{\Delta}.$$

Non-isomorphic elliptic curves with the same j-invariant over a proper subfield of $\overline{k}$, are called twists of each other. There are two special j-invariants worth noting; 0 and 1728, for E/k where $\text{chark}(k) \neq 2, 3$ these occur when $A = 0$ and $B = 0$ respectively. For $\text{char} = 2, 3$ we have that $j = 1728 = 0$.

Example 1.1. Let $\text{char}(k) \neq 2, 3$, E_1 has j-invariant 0, and E_2 has j-invariant 1728 $\forall A, B \in k$.

$$E_1 : y^2 = x^3 + B \tag{1.4}$$

$$E_2 : y^2 = x^3 + Ax \tag{1.5}$$

1.1.1 Group of k-rational points

The k-rational points of an elliptic curve E/k that is points $(x, y) \in E$ such that $x, y \in k$ are solutions to the Weierstrass equation. These points along with the points at infinity as the identity, admits a group stucutre. By Bezout's theorem, a line and and an elliptic curve will intersect with a multiplicity of 3. We can define the binary operation as follows; to add two points P and Q on E, we draw the line intersecting P and Q and define the point $P + Q$ as the reflection along the x-axis of the third point the line intersect.

Definition 1.2. ([Gal12, 9.1]) Let E/k be an elliptic curve of the expanded Weierstrass from 1.2 and $E(k)$ the set of k-rational points of E, and $O_E \in E(k)$ the point and infinity. Then

$$P + O_E = P \quad \forall P \in E(k).$$

Let $P = (x_0, y_0) \in E(k)$, then

$$[-1]P := -P = (x_0, -y_0 - a_1x - a_3).$$

Finally, let $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E(k)$ be two points not equal to O_E, and

$$\lambda = \begin{cases} \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} & \text{if } P_1 = P_2 \\ \\ \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } P_1 \neq \pm P_2 \end{cases}$$

then $P_1 + P_2 = (x_3, y_3)$, where

$$x_3 = \lambda^2 + a_1\lambda - x_1 - x_2 - a_2$$

$$y_3 = -\lambda(x_3 - x_1) - y_1 - a_1x_3 - a_3).$$

If $\mathrm{char}(k) \neq 2, 3$ then $a_1 = a_2 = a_3 = 0$ in 1.2, so we often have the easier equations to work with. So letting E be of the short Weierstrass form 1.3, and P_1, P_2 as above:

$$\lambda = \begin{cases} \dfrac{3x_1^2 + A}{2y_1} & \text{if } P_1 = P_2 \\ \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } P_1 \neq \pm P_2 \end{cases}$$

and

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = -\lambda(x_3 - x_1) - y_1.$$

If the elliptic curve is over for example $\mathbb{Q}$, then one can imagine this "chord and tangent" group law geometrically, as in the figure below. Here we have the points $P, Q, R, S \in E(\mathbb{Q})$ with the relations

$$P + Q = S$$

$$S + R = O_E$$

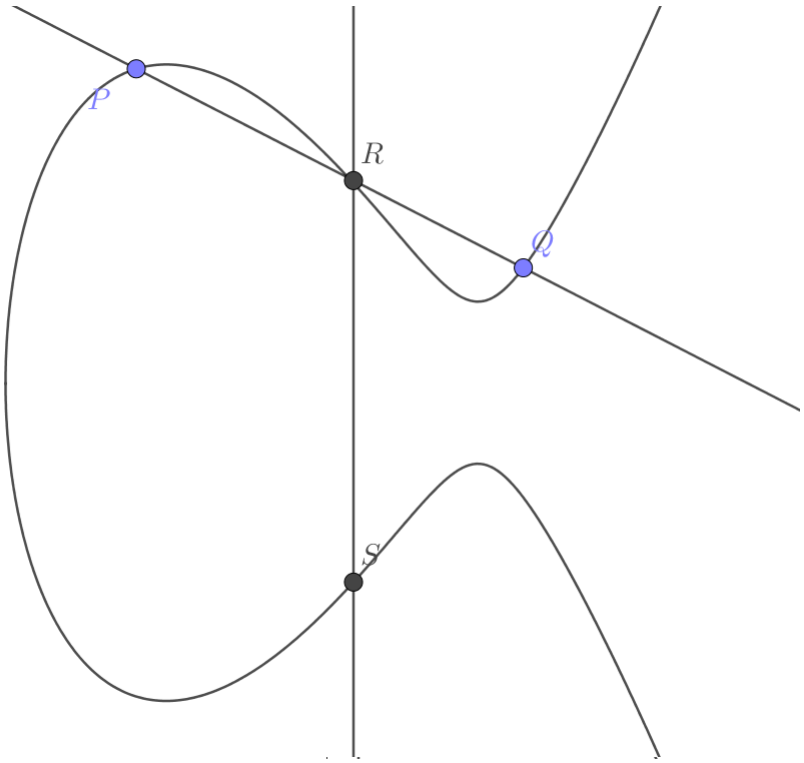


Figure 1.1: $E/\mathbb{Q} : y^2 = x^3 - 5x + 5$

However, in the case of an elliptic curve over a finite field, say $\mathbb{F}_{419}$ we can not rely on this geometric intuition.

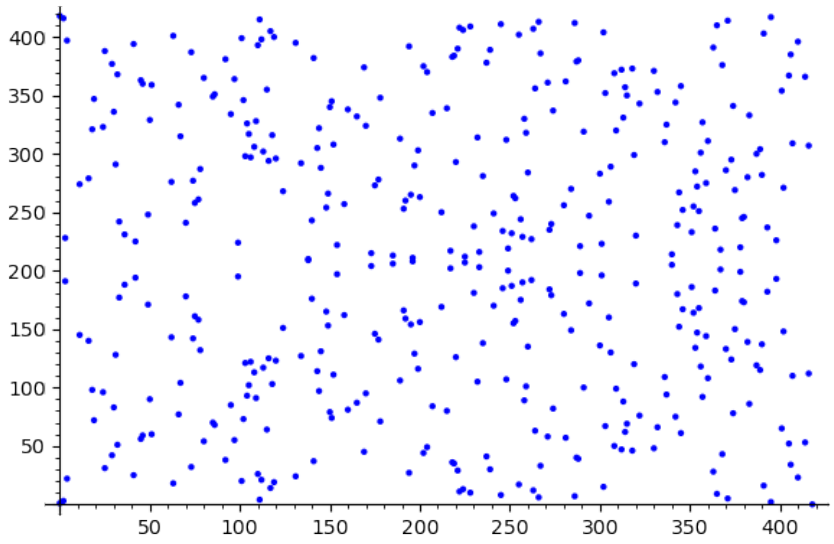


Figure 1.2: $E/\mathbb{F}_{419} : y^2 = x^3 + 1$

1.2 Isogenies

Definition 1.3. Let E_1/k and E_2/k be elliptic curves over a field k. An isogeny ϕ over k is a collection of three homogenous polynomials $F, G, H \in k[X, Y, Z]$ with finitely many common zeros such that if

$$(X : Y : Z) \in E_1 \quad \text{then} \quad \phi(X : Y : Z) = (F(X : Y : Z), G(X : Y : Z), H(X : Y : Z)) \in E_2$$

and $\phi(O_1) \mapsto O_2$.

An isogeny induces an homomorphism of fields

$$\phi^* : k(E_2) \to k(E_1).$$

Definition 1.4. The degree of an isogeny, $\deg(\phi)$ is

$$\deg(\phi) = [k(E_1) : \phi(k(E_2))]$$

or if ϕ is constant, we define it to be 0.

Definition 1.5. We call an isogeny $\phi : E_1/k \to E_2/k$ separable, inseparable, or purely inseparable if the field extension

$$k(E_1)/\phi^*(k(E_2))$$

has the corresponding properties.

Remark. Every isogeny over a field in characteristic 0 will necessarily be separable, as inseparable extension may only occur in fields in postive characteristic.

Theorem 1.6. *Let $\phi : E/\overline{k} \to E'/\overline{k}$ be a separable, non-zero isogeny, then*

$$|\ker(\phi)| = \deg(\phi).$$

Proof. See [Sil09, III.4.10(c)] □

Example 1.7. Let $f : E \to E'$ be a rational map with coefficients in k. If zeros of F, H are in k, then the kernel of f is a subgroup of $E(k)$, but if not, there are elements of the kernel of f that are not k-rational points of E even if f is defined over k.

An isogeny is either surjective or constant as a map of the varieties [Sil09, II.2.3]. The zero isogney [0] is defined as $[0]P \mapsto O_2 \forall P \in E_1$. We have for isogenies

$$E_1 \xrightarrow{\phi} E_2 \xrightarrow{\psi} E_3$$

then

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

An isogeny $E_1/k \to E_2/k$ is also a homomorphism of the group of rational points $E_1(k) \to E_2(k)$. This group homomorphism, however, is not always either constant or surjective. Hom-sets of isogenies admit a group structure themselves.

$$\mathrm{Hom}(E_1, E_2) = \{\text{isogneies } E_1 \to E_2\}$$

and

$$\mathrm{Hom}_k(E_1, E_2) = \{k - \text{isogneies } E_1 \to E_2\}$$

where $\forall \phi, \psi \in \mathrm{Hom}(E_1, E_2)$

$$(\phi + \psi)(P_1) = \phi(P_1) + \psi(P_1).$$

Example 1.8. For each $m \in \mathbb{Z}$ we have

$$[m] : E \to E$$

such that

$$[m](P) = \underbrace{P + P + \cdots + P}_{m \text{ terms}}$$

Furthermore,

$$[-1](P) = -P$$

so

$$([m] \circ [-1])(P) = [-m](P) = -(\underbrace{P + P + \cdots + P}_{m \text{ terms}}).$$

Theorem 1.9. *Let E be an elliptic curve and $G \subset E$ a subgroup of E, then there exists some unique elliptic curve E/G and separable isogeny*

$$\phi : E \to E/G$$

where $\ker(\phi) = G$.

Proof. See [Sil09, III.4.12] □

We define the endomorphism ring of E as

$$\mathrm{End}(E) := \mathrm{Hom}(E, E)$$

and

$$\mathrm{End}_k(E) := \mathrm{Hom}_k(E, E).$$

Where the multiplicative operation is composition of isogenies. We therefore have that there is an injection from

$$\mathbb{Z} \hookrightarrow \mathrm{End}_k(E).$$

The automorphism group is a subring of the endomorphism ring and is composed of all isogenies with an inverse, denoted

$$\mathrm{Aut}(E)$$

or

$$\mathrm{Aut}_k(E)$$

for automorphism defined over k.

Theorem 1.10. *Let E/k and $\mathrm{char}(k) \neq 2, 3$, then there exists a natural $\mathrm{Gal}(\bar{k}/k)$-module isomorphism*

$$\mathrm{Aut}(E) \cong \begin{cases} \mu_2, & j(E) \neq 0, 1728 \\ \mu_4, & j(E) = 1728 \\ \mu_6, & j(E) = 0. \end{cases} \tag{1.6}$$

Proof. See [Sil09, III.10.1] □

Definition 1.11. Let $\mathrm{char}(k) = p$, and $E/\mathbb{F}_q$ be an elliptic curve. The *Frobenius endomorphism* $\phi \in \mathrm{End}_{\mathbb{F}_q}(E)$ of degree q. It acts on E by raising the cooridantes of the points to the qth power

$$\phi(X : Y : Z) \mapsto (X^q : Y^q : Z^q).$$

Theorem 1.12. *Let $E/\mathbb{F}_q$, and ϕ_q the q'th Frobenius endomorphism, then*

$$\ker(1 - \phi_q) = E(\mathbb{F}_q).$$

Proof. We know that the absolute Galois group of $\mathbb{F}_q$, $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ is generated by the q^{th} power Frobenius field automorphism. For an element $\alpha \in \overline{\mathbb{F}_q}$, we have that $\alpha^q = \alpha$ if and only if $\alpha \in \mathbb{F}_q$. Therefore , as ϕ_q acts as the Frobenius automorphism on coordinates of $P \in E$, we have that it only acts as the identity on $P \in E(\mathbb{F}_q)$ and we are done. □

Using this we get the following bound on the number for rational points, called the Hasse bound.

Theorem 1.13. *Let $E/\mathbb{F}_q$, then $||E(\mathbb{F}_q)| - (q + 1)| \leq 2\sqrt{q}$.*

Proof. See [Sil09, V.1.1]. □

The kernel of the induced group endomorphism from the each $[n] \in \mathrm{End}_k(E)$ is denoted

$$E(k)[n] = \ker([n]) \subset E(k).$$

Theorem 1.14. *Let* $\mathrm{char}(k) = p$ *and* E/k *and elliptic curve over* k*.*

(i) If $p \nmid n$*, then* $E(\overline{k})[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$

(ii) If $p \mid n$*, then* $E(\overline{k})[n] \cong \begin{cases} 0 \\ \mathbb{Z}/n\mathbb{Z} \end{cases}$

Proof. See [Sil09, III.6.4]. □

Remark. We will see in the next chapter that the case of (ii) in 1.14, the trivial torsion group will arise when E is supersingular and the non-trivial when E is ordinary.

Theorem 1.15. E_1 *and* E_2 *is isogenous over* k *if and only if* $|E_1(k)| = |E_2(k)|$*.*

Proof. See [Gal12, 9.7.4]. □

Example 1.16. Let us look at a specific example of an isogeny. Let

$$E/\mathbb{F}_5 : y^2 = x^3 + 1$$

and

$$[3] : E \to E.$$

Now this is how [3] acts on every element of $E(\mathbb{F}_5)$

$$\begin{aligned} O_E &\mapsto O_E \\ (0:1:1) &\mapsto O_E \\ (0:4:1) &\mapsto O_E \\ (2:2:1) &\mapsto (4:0:1) \\ (2:3:1) &\mapsto (4:0:1) \\ (4:0:1) &\mapsto (4:0:1). \end{aligned}$$

We see that there are 3 3-torsion $\mathbb{F}_5$-rational points on E. By 1.14 we are missing 6 3-torsion points defined on some extension of $\mathbb{F}_5$.

1.2.1 Dual isogeny

Definition 1.17. Let $\phi : E \to E'$ be a nonconstant isogeny of degree m, then the unique isogeny

$$\hat{\phi} : E' \to E \quad \text{satisfying} \quad \hat{\phi} \circ \phi = [m].$$

is called the dual isogeny to ϕ.

Theorem 1.18. *Let* $\phi : E \to E'$ *be an isogeny of degree* m *then the following hold*

(i)

$$\hat{\phi} \circ \phi = [m] \in \mathrm{End}(E) \quad \text{and} \quad \phi \circ \hat{\phi} = [m] \in \mathrm{End}(E')$$

(ii) Let $\lambda : E' \to E''$ *be another isogeny, then*

$$\widehat{\lambda \circ \phi} = \hat{\phi} \circ \hat{\lambda}$$

(iii) Let $\psi : E \to E'$ *be another isogeny, then*

$$\widehat{\psi + \phi} = \hat{\phi} + \hat{\lambda}$$

(iv) For all $m \in \mathbb{Z}$

$$[m] = \widehat{[m]} \quad \text{and} \quad \text{and} \quad \deg([m]) = m^2$$

(v)

$$\deg(\hat{\phi}) = \deg(\phi) \quad \text{and} \quad \hat{\hat{\phi}} = \phi$$

Proof. See [Sil09, III6.2] □

Example 1.19. Let $E/\mathbb{F}_{11}$, be given by the Weierstrass equation

$$E : y^2 = x^3 + 2$$

and let ϕ_{11} be the 11^{th}-power Frobenius endomorphism. It is given by the following rational maps.

$$(x, y) \mapsto (x^{11}, y^{11})$$

using SageMath we may calculate the dual isogeny, which is given by

$$(x, y) \mapsto (x^{11} - y^{11})$$

The Frobenius endomorphism is of degree 11 [Sil09, Theorem II.2.11]. Then by definition we should have that $\hat{\phi_{11}} \circ \phi_{11} = [11]$. We have ϕ_{11} acts as the identity on all $(x, y) \in E(\mathbb{F}_{11})$, as $\alpha = \alpha^{11}$ for all $\alpha \in \mathbb{F}_{11}$. Calculation with SageMath gives that $\hat{\phi_{11}}(P) = -P$ for all $P \in E$, so the composition acts as $[-1]$ on $E(\mathbb{F}_{11})$. Lastly, we need that $[11]$ should also act as $[-1]$ on $E(\mathbb{F}_{11})$. A calculation with Sage Math gives this, so this example agrees with 1.18. Note, it is not unexpected that $[11]$ acts as $[-1]$ as we will later see that $E(\mathbb{F}_{11}) \cong \mathbb{Z}/(12)$.

1.2.2 Tate module

The structure of the endomorphism ring of an elliptic curve is of great interest, and we will begin its description with the Tate module.

Definition 1.20. We define the Tate module as the inverse limit through $n \in \mathbb{Z}_{>0}$

$$T_l(E) = \varprojlim E(k)[l^n]$$

with the inverse system

$$E(\overline{k})[l^{n+1}] \xrightarrow{[l]} E(\overline{k})[l^n].$$

We know from 1.14 that if $\text{char}(k) = p$ and $l \nmid p$,

$$E(\overline{k})[l^n] \cong \mathbb{Z}/l^n\mathbb{Z} \oplus \mathbb{Z}/l^n\mathbb{Z}$$

From this, we get

$$\varprojlim E(\overline{k})[l^n] \cong \varprojlim(\mathbb{Z}/l^n\mathbb{Z} \oplus \mathbb{Z}/l^n\mathbb{Z}) \cong \mathbb{Z}_l \oplus \mathbb{Z}_l.$$

Theorem 1.21. *Let* $E, E'/k$ *be elliptic curves and* $l \neq \text{char}(k)$ *be prime, then there exists a canonical injection.*

$$\text{Hom}(E, E') \otimes \mathbb{Z}_l \hookrightarrow \text{Hom}(T_l(E), T_l(E')).$$

Proof. See [Sil09, III.7.4]. □

Remark. Since $T_l(E) \cong \mathbb{Z}_l \oplus \mathbb{Z}_l$, we have that $\mathrm{Hom}(T_l(E), T_l(E')) \cong M_2(\mathbb{Z}_l)$.

Corollary 1.22. $\mathrm{rank}_{\mathbb{Z}}(\mathrm{Hom}(E, E')) = 1, 2, 4$.

Proof. See [Sil09, III.7.5]. □

And in fact, over a field k where $\mathrm{char}(k) = 0$, the endomorphism ring $\mathrm{End}_{\bar{k}}(E)$ can only be of rank 1 or 2. And in the case the rank is 2 we say that the elliptic curve have *complex multiplication*. If $\mathrm{char}(k) = p$ then the rank of the of $\mathrm{End}_k(E)$ is always at least 2, and in the case it's 4 it's always non-commutative.

Definition 1.23. We define the l-adic representation of the absolute Galois group of k associated to E to be

$$\rho_l : \mathrm{Gal}(\bar{k}/k) \to \mathrm{Aut}(T_l(E)),$$

induced from the action of $\mathrm{Gal}(\bar{k}/k)$ on the l^n-torsion elements of $E(k)$.

Definition 1.24. We denote the subset of $\mathbb{Z}_l$-module homomorphism between Tate modules that commute with an action from the absolute Galois group, $\mathrm{Gal}(\bar{k}/k)$ as given by the l-adic representation as

$$\mathrm{Hom}_k(T_l(E), T_l(E')) \subset \mathrm{Hom}(T_l(E), T_l(E')).$$

This can be looked at as a parallel to how the subset of isogenies over $\bar{k}$ that commute with the action from $\mathrm{Gal}(\bar{k}/k)$, which are exactly k-isogenies. The $\mathbb{Z}_l$-module homomorphisms $\psi \in \mathrm{Hom}_k(T_l(E), T_l(E'))$ are exactly the ψ's such that the following diagram commutes for all $g \in \mathrm{Gal}(\bar{k}/k)$

$$\begin{array}{ccc} T_l(E) & \xrightarrow[\rho_l(g)]{} & T_l(E) \\ \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \psi} \\ T_l(E') & \xrightarrow{\rho'_l(g)} & T_l(E'). \end{array}$$

Theorem 1.25. *Let $E/\mathbb{F}_q$, and $E'/\mathbb{F}_q$, then the natural map*

$$\mathrm{Hom}_{\mathbb{F}_q}(E, E') \otimes \mathbb{Z}_l \to \mathrm{Hom}_{\mathbb{F}_q}(T_l(E), T_l(E'))$$

is an isomorphism.

Proof. See [Sil09, 7.7]. □

Theorem 1.26. *Let $\phi \in \mathrm{End}(E)$ and let $\phi_l : T_l(E) \to T_l(E)$ be the $\mathbb{Z}_l$-module homomorphism induced by ϕ. Then*

$$\det(\phi_l) = \deg(\phi) \quad \text{and} \quad tr(\phi_l) = 1 + \deg(\phi) - \deg(1 - \phi).$$

Proof. See [Sil09, 8.6]. □

Example 1.27. We will often in the next section refer to the trace of the Frobenius endomorphism. It will be in the sense of 1.26. Let ϕ_q be the q^{th} power Frobenius endomorphism, and let $(\phi_q)_l$ be corresponding endomorphism of $T_l(E)$ given by a matrix in $M_2(\mathbb{Z}_l)$. Then

$$\begin{aligned} tr((\phi_q)_l) &= 1 + \deg(\phi_q) - \deg(1 - \phi_q) \\ &= 1 + q - |E(\mathbb{F}_q)| = t \end{aligned}$$

the number t is what is refered to as the *trace of the Frobenius*.

Chapter 2

Supersingular Elliptic Curves and Isogenies

2.1 Properties

Definition 2.1. An elliptic Curve, E/k is supersingular if

$$\mathrm{End}_{\overline{k}}(E)$$

is not commutative. An elliptic curve that is not supersingular is called ordinary.

This will coincides with the case of $\mathrm{rank}_{\mathbb{Z}}(\mathrm{End}_{\overline{\mathbb{F}}_p}(E)) = 4$.

Remark. This is not the easiest property to calculate nor is it the necessarily the most useful, it is though the etymological root of the name *supersingular*. Singularity here does not refer to a singular point on the elliptic curve, as by definition an elliptic curve is non-singular. Historically, one used *singular* (as in "rare", or "special" to refer to elliptic curves over a field of characteristic of 0 with complex multiplication. Furthermore, as all elliptic curves of field of finite characteristic have at least complex multiplication, *supersingular* came to mean "even more special", even as the term singular fell out of use.

Theorem 2.2. *Let E/k be an elliptic curve over a field k with $\mathrm{char}(k) = p > 0$, then the following are equivalent*

(i) *E is supersingular,*

(ii) *$E(k)[p^r]$ is trivial for all $r > 1$,*

(iii) *The endomorphism $[p] : E \to E$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$,*

(iv) *$|E(\mathbb{F}_q)| \equiv 1 \mod p$.*

Proof. See [Sil09, V.3.1]. □

From 2.2 we can see that there are many different ways of distinguish supersingular elliptic curves from ordinary ones. One can test the order of points, if a point has order p we know its elliptic curve is not supersingular. One can also use a point counting algorithm to test for supersingularity.

Corollary 2.3. *La $\phi : E_1 \to E_2$ be an isogeny of elliptic curves, then E_1 is supersingular if and only if E_2 is supersingular.*

Proof. If E_1 is supersingular, then by (iv) in 2.2, we have that $|E_1(\mathbb{F}_q)| \equiv 1$ and by 1.15 we have that $|E_1(\mathbb{F}_q)| = |E_2(\mathbb{F}_q)|$ if and only if there is an isogeny $\phi : E_1 \to E_2$. □

Example 2.4. $E/\mathbb{F}_{11^2}$ is given by the following Weierstrass equation

$$E : y^2 = x^3 + \omega$$

where $\omega^2 + 7\omega + 2 = 0$. Using SageMath and the properties of supersingular curves in 2.2 we want to check if this curve is supersingular. Firstly, we can check using (iv) in 2.2. E has 133 $\mathbb{F}_{11^2}$-rational points. $133 \equiv 1 \pmod{11}$, and we know that E is supersingular. We could also check that no point $P \in E(\mathbb{F}_{11^2})$ in the kernel of $[11]$. Iterating through every element in element in $E(\mathbb{F}_{11^2})$ we find that none are of order 11, again confirming its supersingularity.

2.2 How many supersingular curves are there

In order to answer this sections question we have to look at some different theory. Firstly, we look at how many supersingular j-invariants there are. Secondly, by 2.3 we have that if one elliptic curve in an isogeny class is supersingular, then every curve in that isogeny class is supersingular as well. This is why we are interested in what each of the supersingular isogeny classes looks like and how many there are. Then, we will look at twists of elliptic curves, which will be the first step of finding out how many supersingular isomorphism classes there are over a finite field. Lastly, in order to finalize the count of the isomorphisms classes we need to develop some theory of what rings occur as endomorphism rings of supersingular curves.

2.2.1 j-invariants

Since supersingularity is only dependent on the endomorphisms defined over the algebraic closure of k, and therefore only dependent on the j-invariant. We call a j-invariant of an elliptic curve that is supersingular, a *supersingular j-invariant.*

Theorem 2.5. *Let* $\mathrm{char}(k) = p$*, and* E/k *be an elliptic curve. Then there are*

$$\lfloor \frac{p}{12} \rfloor + \begin{cases} 0 & if\ p \equiv 1 \mod 12 \\ 1 & if\ p \equiv 5 \mod 12 \quad \text{(corresponds to } j = 0 \text{ supersingular)} \\ 1 & if\ p \equiv 7 \mod 12 \quad \text{(corresponds to } j = 1728 \text{ supersingular)} \\ 2 & if\ p \equiv 11 \mod 12 \end{cases}$$

supersingular j-invariants in $\mathbb{F}_{p^2}$.

Proof. See [Sil09, V.4.1(c)]. □

There is a surjection of j-invariants elliptic curves over $\overline{\mathbb{F}}_q$ and λ of elliptic curves over $\overline{\mathbb{F}}_q$ of the form

$$E : y^2 = x(x-1)(x-\lambda)$$

where, $\lambda \in \overline{\mathbb{F}}_q$ and $\lambda \neq 0, 1$ with the transformation

$$j(E) = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{(\lambda^2(\lambda - 1)^2)}.$$

Theorem 2.6. *Let $m = (p-1)/2$, $\mathrm{char}(\mathbb{F}_q) = p$ and $E/\overline{\mathbb{F}}_q$ of the form above, and define the polynomial*

$$H_p(t) = \sum_{i=0}^{m} \binom{m}{i}^2 t^i$$

Now E is supersingular if and only if $H_p(\lambda) = 0$.

Proof. See [Sil09, V.4.1(b)]. □

Remark. Let $E/\mathbb{F}_q$ and $E'/\mathbb{F}_q$ with $j(E) = j(E')$, but $E \ncong E'$, that is they are twists of each other. Then both will still be supersingular but as we will see they will not necessarily be isogenous.

Example 2.7. Continuing the example 1.19. We can now explain why the dual of the 11^{th} Frobenius endomorphism on $E/\mathbb{F}_{11}$, given by the Weierstrass equation

$$E : y^2 = x^3 + 2,$$

had a trivial kernel. Inspection of E gives that $j(E) = 0$ and by 2.5 0 is a supersingular j-invariant over $\mathbb{F}_{11}$. Now, remembering that the degree of ϕ_{11} is 11 and that the composition of $\hat{\phi_{11}} \circ \phi_{11} = [11]$, by (ii) in 2.2 the kernel of $[11]$ must be trivial as E is supersingular. An ordinary curve E' would not have a trivial kernel.

2.2.2 Isogeny classes

Two elliptic curves over $\mathbb{F}_q$ are isogenous (over $\mathbb{F}_q$) if they have the same number of $\mathbb{F}_q$-rational points, which is uniquely defined by the number $t = \mathrm{Tr}(\phi_q)$, the trace of the Frobenius endomorphism of $E/\mathbb{F}_q$.

Definition 2.8.

$$I(t) := \{\text{Elliptic curves with } q + 1 - t \ \mathbb{F}_q\text{−rational points}\}$$

$$N(t) := \#\{\mathbb{F}_q\text{−isomorphism classes in } I(t)\}.$$

Corollary 2.9. *Let $\phi_q \in \mathrm{End}(E)$, then $E/\mathbb{F}_q$ is supersingular if and only if*

$$\mathrm{Tr}(\phi_q) \equiv 0 \mod p$$

Proof. We have that $|E(\mathbb{F}_q)| = q + 1 - t \equiv 1 \pmod p$ 2.2 (iv), then t must be 0 modulo p □

Theorem 2.10. *Let $[\mathbb{F}_q : \mathbb{F}_p]$ be even, $E/\mathbb{F}_q$ and $\phi_q \in \mathrm{End}(E)$ the Frobenius endomorphism. Then if $t = \mathrm{Tr}(\phi_q)$ and $t \mid p$, $N(t)$ is non-empty if and only if one the following hold*

(i) $t = \pm 2\sqrt{q}$.

(ii) $t = \pm\sqrt{q}$ *and* $p \not\equiv 1 \pmod 3$.

(iii) $t = 0$ *and* $p \not\equiv 1 \pmod 4$.

Proof. See [Sch87, 4.2]. □

Theorem 2.11. *Let $[\mathbb{F}_q : \mathbb{F}_p]$ be odd, $E/\mathbb{F}_q$ and $\phi_q \in \mathrm{End}(E)$ the Frobenius endomorphism. Then if $t = T(\phi_q)$, $N(t)$ is non-empty if and only if one the following hold*

(i) $t = 0$.

(ii) $t = \pm\sqrt{2q}$ *and* $p = 2$.

(iii) $t = \pm\sqrt{3q}$ *and* $p = 3$.

Proof. See [Sch87, 4.2]. □

Corollary 2.12. *There are either 4 or 5 isogeny classes of supersingular elliptic curves over $\mathbb{F}_q$ where $q = p^{2n}$. There is just 1 if $q = p^{2n+1}$.*

Proof. Immediate from 2.10 and 2.11 and 1.15. □

Example 2.13. Let $E/\mathbb{F}_7$, and given by the following equation

$$E : y^2 = x^3 + 3.$$

Then we look to 2.11 and see that $N(t)$ is nonzero only when $t = 0$ in this case and that the number of $\mathbb{F}_p$-rational points is $7 + 0 + 1 = 8$. If we then look at the case of $\mathbb{F}_{7^2}$-rational points of E, 2.10 does not tell us exactly how many points we have, from just the curve. By SageMath calculations, we find that $|E(\mathbb{F}_{7^2})| = 64$ and therefor $\mathrm{Tr}(\phi_{7^2}) = 14 = 2\dot{7}$.

In fact any supersingular elliptic curve defined over a prime field will be in the same $\mathbb{F}_q$-isogeny class for all extension [Sil09, Problem 5.15]. Furthermore, let $E/\mathbb{F}_p$ supersingular elliptic curves defined over a prime field, if $q = p^{2n}$ then the trace of $\phi_q \in \mathrm{End}_{\mathbb{F}_q}(E)$, will be $T(\phi_q) = 2\sqrt{q}(-1)^{2n/2}$.

Theorem 2.14. *Let $E/\mathbb{F}_q$, $q = p^{2n}$ with $p \neq 2, 3$ and $t = \mathrm{Tr}(\phi_q)$, then*

$$E(\mathbb{F}_q) \cong \begin{cases} \mathbb{Z}/(\sqrt{q}-1) \oplus \mathbb{Z}/(\sqrt{q}-1) & \text{if } t = 2\sqrt{q} \\ \mathbb{Z}/(\sqrt{q}+1) \oplus \mathbb{Z}/(\sqrt{q}+1) & \text{if } t = -2\sqrt{q} \\ \mathbb{Z}/(q+t+1) & \text{if } t = \pm\sqrt{q} \\ \mathbb{Z}/(q+t+1) & \text{if } t = 0. \end{cases}$$

Proof. See [Sch87, 4.8] □

Example 2.15. We expand on example 1.19. Since E is defined over $\mathbb{F}_{11}$, from 2.13 that $t = 2\sqrt{q}$ for all extensions of even degree. This and the theorem above gives us that $[11]$ acts as $[-1]$ on E, and generally $[p]$ acts as $[-1]$ on any supersingular elliptic curve defined over a prime field.

2.2.3 Twists

The group

$$\mathrm{Twist}((E,O)/k)$$

contains all elliptic curves defined over k which are not k-isomorphic to E, but which are isomorphic over $\bar{k}$. In other words, non-isomorphic curves with the same j-invariant. We say that E'/k is a twist of E/k if $E' \in \mathrm{Twist}((E,O)/k)$. One may identify each twist of E with an element of the first Galois cohomology of the automorphism group of E, $H^1(G, \mathrm{Aut}(E))$ [Sil09, X.5].

Remark. It is not immediate that any curve in $\mathrm{Twist}((E,O),k)$ can be given the structure of an elliptic curve. Specifically, we need that there exists at least one k-rational point on the curve. See [Sil09, X.5.3(b)] for a proof that this is the case.

Theorem 2.16. *Let* $\mathrm{char}(k) \neq 2,3$ *and let*

$$n = \begin{cases} 2 & \text{if } j(E) \neq 0, 1728 \\ 4 & \text{if } j(E) = 1728 \\ 6 & \text{if } j(E) = 0. \end{cases}$$

Then

$$\mathrm{Twist}(E/k) \cong k^*/(k^*)^n$$

where $(k^*)^n$ are the units in k that are n^{th} powers.

Proof. For brevity let $G := \mathrm{Gal}(\bar{k}/k)$. There is an isomorphism of G-modules

$$\mathrm{Aut}(E) \cong \mu_n$$

Consider then, the exact sequence of G-modules:

$$1 \longrightarrow \mu_n \longrightarrow \bar{k}^* \xrightarrow{a \mapsto a^n} \bar{k}^* \longrightarrow 1$$

using long exactness of Galois cohomology we get the following exact sequence, remembering that applying G to $\bar{k}$ fixes k:

$$\ldots \longrightarrow k^* \xrightarrow{a \mapsto a^n} k^* \xrightarrow{\delta} H^1(G, \mu_n) \longrightarrow H^1(G, \bar{k}^*) \longrightarrow \ldots$$

From Hilbert 90 we know that $H^1(G, \bar{k}^*) = 0$, which gives us that $H^1(G, \mu_n) \cong k/(k^*)^n$ if $\mathrm{char}(k) \nmid n$.
We now get that

$$\mathrm{Twist}(E/k) = H^1(G, \mathrm{Aut}(E)) \cong H^1(G, \mu_n) \cong k^*/(k)^*.$$

□

The size of the group $k^*/(\bar{k}^*)^n$ can be then be described using elementary number theory.

Theorem 2.17. *Let* k *be a finite field of size* $q = p^m$*, with* $p \neq 2,3$.

$$|k^*/(k^*)^n| \cong \begin{cases} 2 & \text{if } n = 2 \\ 4 & \text{if } n = 4 \text{ and } q \equiv 1 \mod 4 \\ 6 & \text{if } n = 6 \text{ and } q \equiv 1 \mod 3 \end{cases}$$

Proof. By Silverman [Sil14] we may reduce the question to ask which primitive roots of unity there are in the field k. If k has a primitive third root of unity then then $k^*/(k^*)^6$ has order 6 and if k has a primitive fourth root of unity then $k^*/(k^*)^4$ has order 4. Since k^* is cyclic of order $q-1$, then for primitive third root of unity to be in k^* we need $q-1 \equiv 0 \pmod 3$ and for a fourth primitve root we need $q-1 \equiv 0 \pmod 4$. □

From this we have that over every finite field $\mathbb{F}_q$ with $\text{char}(\mathbb{F}_q) \neq 2, 3$, there are exactly two twists of every elliptic curve of with $j(E) \neq 0, 1728$. And over every non-prime $\mathbb{F}_q$ with $\text{char}(\mathbb{F}_q) \neq 2, 3$ there are respectively 6 and 4 twists of elliptic curves with $j(E) = 0, 1728$.

Example 2.18. Let $E/\mathbb{F}_{13}$ given by the following Weierstrass equation

$$E : y^2 = x^3 + x + 4$$

We calculate the j-invariant to be 5 so and there should be just one other non-isomorphic curves of the same j-invariant. Using SageMath we confirm this and calculate it to be

$$E' : y^2 = x^3 - x + 7$$

2.3 Quaternion algebras and orders

Definition 2.19. Let $K/\mathbb{Q}$ be an algebraic number field of degree n, with a ring of integers $\mathcal{O}_K$. An order of K is subring $\mathcal{O}$ of $\mathcal{O}_K$ which contains an integral basis with n elements.

Example 2.20. $\mathcal{O} = \mathbb{Z}[\sqrt{-3}] \subset \mathbb{Q}[\sqrt{-3}] = K$ is not the ring of integers of K. It is $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$, where ζ_3 is the third root of unity, that is the ring of integers in K. $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K, while $\mathcal{O}$ is not integrally closed. $\mathcal{O}$ is however an example of an order in K. It is important to note that since $\mathcal{O}$ is not integrally closed it is not a Dedekind domain. $\mathcal{O}_K$ also satisfies the conditions for an order, and is sometimes called the maximal order in K.

We will see that later that orders of some number field arise as endomorphism rings of some elliptic curves. These orders are in some complex quadratic field, and will be called a *complex quadratic order*. A complex quadratic order is equipped with an embedding $\mathcal{O} \hookrightarrow \mathbb{C}$ that is unique up to complex conjugation. This embedding is inherited from $\mathcal{O}_K$.

Furthermore, we denote by $\Delta(\mathcal{O})$ the discriminant of $\mathcal{O}$. $\mathcal{O}_K$ has exactly one subring of $\mathcal{O}$ of index $k \in \mathbb{Z}_{>0}$ up to isomorphism. We have that $\Delta(\mathcal{O}) = \Delta(\mathcal{O}_K)k^2$. This means we can use the discriminant of the $\mathcal{O}$'s to characterize their isomorphism classes. Lastly, if $\mathcal{O} \cong \mathbb{Z}[\alpha]$, where α is an algebraic number, then $\Delta(\mathcal{O}) = \text{Disc}(\text{minpoly}(\alpha))$.

We want to construct a notion of class group for our complex quadratic orders. However as orders need not necessarily be integrally closed, and therefore not a Dedekind domain the set of fractional ideals of $\mathcal{O}$ does admit a group structure. We therefore restrict the construction to invertible ideals.

Definition 2.21. Let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}$. Then $\mathfrak{a}$ is invertible if there exists some fractional ideal $\mathfrak{b}$ such that

$$\mathfrak{a}\mathfrak{b} = \mathcal{O}$$

And the inverse of $\mathfrak{a}$ is given by

$$\mathfrak{a}^{-1} = \{x \in K | x\mathfrak{a} \subseteq \mathcal{O}\}$$

Remark. If $\mathcal{O}$ happens to be Dedekind, then every fractional ideal of $\mathcal{O}$ is invertible.

Definition 2.22. Let $\mathcal{O}$ be a complex quadratic order, then the class group of $\mathcal{O}$ denoted $Cl(\mathcal{O})$ is the group of invertible fractional $\mathcal{O}$-ideals, modulo the group of principle fraction $\mathcal{O}$-ideals. And the class number of $\mathcal{O}$ is the order of the class group and denoted $h(\mathcal{O})$.

Remark. In [Sch87] the class group of a complex quadratic order is just called the class group, however [Neu99] refers to this group as the Picard group of $\mathcal{O}$ whenever $\mathcal{O}$ is not Dedekind.

We now have the properties of complex quadratic orders we need to talk about some of the rings that occur as endomorphism rings of supersingular elliptic curves. However, the definition we have for a supersingular elliptic curve constitutes that its endomorphism ring over the algebraic closure is non-commutative. We will now look at what these non-commutative rings look like.

Definition 2.23. Let $a, b \in F^*$. An F-algebra $\mathcal{A}$ is a quaternion algebra if there exists $i, j \in \mathcal{A}$ such that $1, i, j, k$ is a F-basis for $\mathcal{A}$ and

$$i^2 = a$$

$$j^2 = b$$

$$ij = -ji = k.$$

We denote the a quaternion algebra as $\mathcal{A} := (\frac{a,b}{F})$. By definition we have that $\dim_F(\mathcal{A}) = 4$. Lastly, let $F \subset K$ be a field extension of F, then there is a canonical isomorphism

$$\left(\frac{a,b}{F}\right) \otimes_F K \cong \left(\frac{a,b}{K}\right)$$

Example 2.24. The ring $M_2(F)$ is the quaternion algebra $\left(\frac{1,1}{F}\right)$, with the following identifications

$$i = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$j = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Generally one can always view a quaternion algebra as a subalgebra of some matrix ring.

Definition 2.25. We define the involution map on $\mathcal{A} = \left(\frac{a,b}{F}\right)$ as

$$\bar{}: \mathcal{A} \to \mathcal{A}$$

$$\bar{x} = \overline{x_1 + x_2 i + x_3 j + x_4 k} = x_1 - x_2 i - x_3 j - x_4 k$$

And similarly to the complex quadratic order, we define the reduced map and reduced trace map as $nrd(x) = x\bar{x}$ and $trd(x) = x + \bar{x}$, respectively.

Theorem 2.26. *A quaternion algebra over F is either isomorphic to a division ring or $M_2(F)$.*

Proof. See [Koh96, p. 5.1]. □

Definition 2.27. A quaternion algebra $\mathcal{A}$ is said to be ramified at a place ν if $\mathcal{A} \otimes F_\nu$ is a division ring. Here F_ν is a local field localized at prime place ν, and a division ring is a non-commutative field.

If the place ν is a nonarchimedean place of F, corresponding to a prime $\mathfrak{p}$ of the ring of integers $\mathcal{O}_F$ of F, we say that $\mathcal{A}$ is ramified at $\mathfrak{p}$. In all cases we cover, if a place $\mathcal{A}$ is ramified at is archimedean, we will say that it is ramified at ∞. The next theorem tells us what $\mathcal{A} \otimes F_\nu$ looks like if $\mathcal{A}$ is not ramified (splits) at ν .

We denote the set of ramified places of $\mathcal{A}$ as Ram $\mathcal{A}$

Definition 2.28. Let $\text{Ram}'\mathcal{A}$ denote the nonarchimedian places of Ram $\mathcal{A}$, then

$$\text{Disc}(\mathcal{A}) := \prod_{\nu \in \text{Ram}'} \nu$$

Remark. In general the discriminant is an ideal, but if $\mathcal{A}$ is a $\mathbb{Q}$-algebra, this will correspond to some integer in $\mathbb{Z}$ since $\mathbb{Z}$ is a PID.

Example 2.29. Let $\mathcal{A} = \left(\frac{-1,-p}{\mathbb{Q}}\right)$, where $p \equiv 3 \pmod 4$. Then we have that $\text{Ram}(\mathcal{A}) = \{\infty, p\}$ and $\text{Disc}(\mathcal{A}) = p$.

Let us now fix $\mathbb{Q}$ as F. By convention one writes quaternion algebras on the form

$$\mathcal{A} = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}ij$$

satisfying $i^2 = a, j^2 = b$ and $ij = -ji$.
The following results allows us to talk about a quaternion algebra just from the places it is ramified at, which is how we will construct a given quaternion algebra in later sections.

Theorem 2.30. *Let $\mathcal{A}, \mathcal{A}'$ be quaternion algebras over $\mathbb{Q}$, then the following are equivalent*

(i) $\mathcal{A} \cong \mathcal{A}'$,

(ii) Ram $\mathcal{A}$ = Ram $\mathcal{A}'$,

(iii) $\mathcal{A} \otimes \mathbb{Q}_\nu \cong \mathcal{A}' \otimes \mathbb{Q}_\nu$ *for all places* ν *of* $\mathbb{Q}$,

(iv) $\mathcal{A} \otimes \mathbb{Q}_\nu \cong \mathcal{A}' \otimes \mathbb{Q}_\nu$ *for but one place* ν.

Proof. See [Voi21, 14.6.5]. □

With this we can write out all the quaternion algebras our endomorphims rings lies in.

Theorem 2.31. *Let p be a prime and $(-/-)$ the Legendre symbol. Then the unique quaternion algebra $\mathcal{A}$ over $\mathbb{Q}$, with* $\text{Ram}(\mathcal{A}) = \{\infty, p\}$ *is*

$$\mathcal{A} = \begin{cases} \left(\frac{-1,-1}{\mathbb{Q}}\right), & p = 2 \\ \left(\frac{-1,-p}{\mathbb{Q}}\right), & p \equiv 3 \mod 4 \\ \left(\frac{-2,-p}{\mathbb{Q}}\right), & p \equiv 5 \mod 8 \\ \left(\frac{-p,-q}{\mathbb{Q}}\right), & p \equiv 1 \mod 8. \end{cases}$$

where q is a prime with $q \equiv 3 \mod 4$ and $(p/q) = -1$.

Proof. See [Piz80, 5.1] □

Definition 2.32. Let V be an n-dimensional $\mathbb{R}$ vector space with a basis $B = \{v_i\}_{1 \leq i \leq n}$. Then an $\mathbb{Z}$-lattice I is a subgroup of V generated as a $\mathbb{Z}$-module by B of the form

$$I = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_n.$$

Remark. If the rank of an $\mathbb{Z}$-lattice I is equal to the dimension of the vector space it is in, the lattice is sometimes called full or complete.

Example 2.33. The Gaussian integers $\mathbb{Z}[i]$ and the Eisenstein integers $\mathbb{Z}[\zeta_3]$ are $\mathbb{Z}$-lattices in $\mathbb{C}$.

Definition 2.34. An order in $\mathcal{O} \subset \mathcal{A}$ is a $\mathbb{Z}$-lattice that is also a subring of $\mathcal{A}$. A maximal order is an order that is not properly contained in another order.

Example 2.35. Let $\mathcal{A} = \left(\frac{a,b}{\mathbb{Q}}\right)$ The lattice generated by $1, i, j, ij$ a $\mathbb{Z}$-module:

$$\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}ij$$

is an order in $\mathcal{A}$. This order will never be maximal.

Theorem 2.36. *Let $\mathcal{A} = \left(\frac{a,b}{\mathbb{Q}}\right)$ of one of the forms in 2.31 ramified at $\{\infty, p\}$. Then depending on p, the following orders $\mathcal{O} \in \mathcal{A}$ occur as a maximal order.*

$$\mathcal{O} = \begin{cases} \mathbb{Z}\dfrac{1+i+j+k}{2} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}k & \text{if } p = 2 \\ \mathbb{Z}\dfrac{1+j}{2} \oplus \mathbb{Z}\dfrac{i+k}{2} \oplus \mathbb{Z}j \oplus \mathbb{Z}k & \text{if } p \equiv 3 \mod 4 \\ \mathbb{Z}\dfrac{1+j+k}{2} \oplus \mathbb{Z}\dfrac{i+2j+k}{4} \oplus \mathbb{Z}j \oplus \mathbb{Z}k & \text{if } p \equiv 5 \mod 8 \\ \mathbb{Z}\dfrac{1+j}{2} \oplus \mathbb{Z}\dfrac{i+k}{2} \oplus \dfrac{j+mk}{q} \oplus \mathbb{Z}k & \text{if } p \equiv 1 \mod 8. \end{cases}$$

where $m \in \mathbb{Z}$, and $(p/q) = -1$ as with 2.31, such that $q \mid (m^2p + 1)$.

Proof. See [Piz80, 5.2]. □

2.4 Endomorphism rings

The structure of the supersingular endomorphism ring is also determined by the trace of the Frobenius endomorphism $t = \mathrm{Tr}(\phi_q)$. As we've seen before all endomorphism rings of elliptic curves over finite field are at least of rank 2 over $\mathbb{Z}$. As usual elliptic curves with $j(E) = 0, 1728$ are of special interest.

Theorem 2.37. *Let $E/\mathbb{F}_q$, $\mathrm{Tr}(\phi_q) = \pm 2\sqrt{q}$, and $p^n = q$ a square. Then*

$$\mathrm{End}_{\mathbb{F}_q}(E) = \mathcal{O} \subset \mathcal{A}$$

where $\mathcal{A}$ is a quaternion algebra ramified at ∞ and p, $\mathcal{O}$ a maxmial order in $\mathcal{A}$. Furthermore, every maximal order of $\mathcal{A}$ will occur as an endomorphism ring of E in $I(t)$.

Proof. See [WM71, 4.2]. □

Theorem 2.38. *Let $E/\mathbb{F}_q$, $t = \mathrm{Tr}(\phi_q) \neq \pm 2\sqrt{q}$, $p|t$ and $p^n = q$ is a square. Then*

$$\mathrm{End}_{\mathbb{F}_q}(E) = \mathcal{O} \subset \mathbb{Q}(\sqrt{t^2 - 4q})$$

where $\mathcal{O}$ a complex quadratic order such that

$$\sqrt{t^2 - 4q} \in \mathcal{O} \quad \text{and} \quad p \nmid [\mathcal{O}_{\mathbb{Q}(\sqrt{t^2-4q})} : \mathcal{O}].$$

Furthermore, every such complex quadratic order occur as endomorphism ring for some E in $I(t)$.

Proof. See [WM71, 4.2]. □

The curves in 2.37 have all their endomorphisms defined over $\mathbb{F}_q$, that is $\mathrm{End}_{\mathbb{F}_q}(E) = \mathrm{End}_{\overline{\mathbb{F}}_q}(E)$. The curves in 2.38 do not.

Theorem 2.39. *Let $\mathcal{O}$ be commutative, that is, $\mathcal{O}$ is a complex quadratic order, that occur as an endomorphism ring over $\mathbb{F}_q$ of some E in $I(t)$, where $t = Tr(\phi_q)$. Let f denote the residue class degree of p in $\mathcal{O}$ and $h(\mathcal{O})$ the class number of $\mathcal{O}$. Then the number of $\mathbb{F}_q$-isomorphism classes of curves that have $\mathcal{O}$ has its endomorphism ring is*

$$h(\mathcal{O})f.$$

Proof. See [Sch87, 4.5(i)]. □

We are interested in which supersingular elliptic curves gives rise to which endomorphisms rings. We start by looking at curves with $t = 0$ over a finite field with $q = p^{2n}$ elements. By 2.10, $N(0)$ is only nonzero when $p \equiv 3 \pmod 4$, when $\mathrm{char}(\mathbb{F}_q) \neq 2, 3$. We have that $\mathrm{End}(E) = \mathcal{O}$ is an order in

$$\mathbb{Q}(\sqrt{t^2 - 4q}) = \mathbb{Q}(\sqrt{-4q}) = \mathbb{Q}(\sqrt{-1}),$$

with $\mathcal{O}_{\mathbb{Q}(\sqrt{-1})} = \mathbb{Z}[\sqrt{-1}]$. The first restriction on $\mathcal{O}$ is that it should contain $\sqrt{t^2 - 4q} = \sqrt{-4q}$. The minimal order satisfying this condition is $\mathbb{Z}[\sqrt{-4q}]$. The second restriction is that p should not divide its index over $\mathcal{O}_{\mathbb{Q}(\sqrt{-1})} = \mathbb{Z}[\sqrt{-1}]$. But p does divide the index of all orders lying over $\mathbb{Z}[\sqrt{-4q}]$ except $\mathbb{Z}[\sqrt{-1}]$, which is then the only endomorphism ring which arises in $I(0)$.

We preform a similar calculation for $t = \pm\sqrt{q}$. Then $\mathrm{End}(E) = \mathcal{O}$ is and order in $\mathbb{Q}(\sqrt{t^2 - 4q}) = \mathbb{Q}(\sqrt{-3q}) = \mathbb{Q}(\sqrt{-3})$, with the ring of integers $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})} = \mathbb{Z}[\zeta_3]$. The only order containing $\sqrt{-3q}$ with p not dividing its index in $\mathbb{Z}[\zeta_3]$ is again $\mathbb{Z}[\zeta_3]$ itself, so then that is the only endomorphism ring that arises in $I(\pm\sqrt{q})$.

It is in the same characteristics that $N(0)$ is nonzero and $j = 1728$ is supersingular, and likewise $N(\pm\sqrt{q})$ being nonzero in the same characteristics that $j = 0$ is supersingular. By looking at the units in the endomorphism rings

$$\mathbb{Z}[\sqrt{-1}]^* = \{\pm 1, \pm\sqrt{-1}\}$$

$$\mathbb{Z}[\zeta_3]^* = \{\pm 1, \pm\zeta, \pm\overline{\zeta}\}$$

and comparing with 1.10, we can confirm that the only supersingular elliptic curves that do not have all their endomorphisms defined over the field they are defined over are those with $j = 0, 1728$.

Finally, we want to figure out how many $\mathbb{F}_q$-isomorphism classes of curves have these these rings as their endomorphism rings. We use the Minkowski bound [Mil11, 4.3], to determine the class number of $\mathbb{Z}_{[}i]$ and $\mathbb{Z}[\zeta_3]$. It states that

$$h(\mathcal{O}_K) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\Delta(\mathcal{O}_K))|}.$$

where $n = [K : \mathbb{Q}]$, s is the number of nonreal complex embeddings of K up to complex conjugation. Using

$$\Delta(\mathbb{Z}[i]) = \mathrm{Disc}(x^2 + 1) = -4$$

$$\Delta(\mathbb{Z}[\zeta_3]) = \mathrm{Disc}(x^2 + x + 1) = -3$$

we get that both have a class number less than 2, therefore 1. Lastly, p splits in $\mathbb{Q}(i)$ and $\mathbb{Q}(\zeta_3)$ if and only if $(\Delta(\mathbb{Z}[i])/p) = -1$ and $(\Delta(\mathbb{Z}[\zeta_3])/p) = -1$ respectively [Neu99, 8.5]. We have that $(-4/p) = -1$ if $p \equiv 1 \pmod 4$ and $(-3/p) = -1$ if $p \equiv 2 \pmod 3$. All together this gives the following corollary.

Corollary 2.40. *Let $t = \mathrm{Tr}(\phi_q)$, with $q = p^{2n}$, $p \neq 2, 3$, then the number of isomorphism classes in $I(t)$ only depends on the characteristic of $\mathbb{F}_q$ in the following way*

$$N(0) = \begin{cases} 0 & \text{if } p \equiv 3 \mod 4 \\ 2 & \text{if } p \equiv 1 \mod 4 \end{cases}$$

$$N(\pm\sqrt{q}) = \begin{cases} 0 & \text{if } p \equiv 1 \mod 3 \\ 2 & \text{if } p \equiv 2 \mod 3. \end{cases}$$

Remark. The conjugation map and involution maps on elements of complex quadratic orders and orders in quaternion algebras corresponds to taking the dual of isogeny in the endomorphism ring.

Theorem 2.41. *Let $E/\mathbb{F}_q$, with $q = p^{2n}$, and $(-/-)$ the Legendre symbol, then*

$$N(\pm 2\sqrt{q}) = \frac{1}{12}(p + 6 - 4(-3/p) - 3(-4/p)).$$

Proof. See [Sch87, 4.6]. □

Example 2.42. We continue building on 2.13. From the theory developed in this section we now know that any supersingular elliptic curve $E/\mathbb{F}_p$ will have an endomorphism ring that is a maximal order in a quaternion algebra ramified at ∞ and p. Furthermore, in characteristic 7 there is only one supersingular j-invariant, all other supersingular curves are twists of E . Such as

$$E_1 : y^2 = x^3 + (4\omega + 2)x, \quad E_2 : y^2 = x^3 + \omega x$$

where $\omega \in \mathbb{F}_{7^2}$ such that $\omega^2 - \omega + 3 = 0$. E_1 has 36 $\mathbb{F}_{7^2}$-rational points and therefore has $\mathrm{Tr}(\phi_q) = -14$, which corresponds to $\mathrm{End}(E_1)$ being a maximal order, while E_2 has 50 $\mathbb{F}_{7^2}$-rational points, which gives us $T(\phi_q) = 0$.

It is also worth noting that isogenous twists are not necessarily isomorphic. Another twist of E,

$$E_3 : y^2 = x^3 + (\omega + 5)x$$

is in the same isogeny class of E_2, meaning they have the same number of points and same trace of their Frobenius endomorphism, and the same j-invariant, but they still are not $\mathbb{F}_{7^2}$-isomorphic. We now have an elliptic curve representing each isomorphism class of the twists of E, and all supersingular curves over $\mathbb{F}_{7^2}$.

Example 2.43. We are now interested in seeing what the isogeny classes our representatives show up in in extensions of $\mathbb{F}_{7^2}$. All these extensions would have to be of even degree. The isogeny clases over $\mathbb{F}_{7^4}$ are detirmined by the $\mathbb{F}_{7^4}$-rational points.

$$|E_2(\mathbb{F}_{7^4})| = |E_3(\mathbb{F}_{7^4})| = 2500 = 7^4 + 2 \cdot 7^2 + 1$$

$$|E(\mathbb{F}_{7^4})| = |E_1(\mathbb{F}_{7^4})| = 2304 = 7^4 - 2 \cdot 7^2 + 1$$

Firstly, we see that in the case of E_2 and E_3, over $\mathbb{F}_{7^2}$ they did not have all their endomorphism defined, as their endomorphism ring would be a complex quadratic order. However, over $\mathbb{F}_{7^4}$ the trace of their Frobenius endomorphism is $t = 2 \cdot 7^2 = 2\sqrt{q}$. Which means that both of their endomorphism rings over $\mathbb{F}_{7^4}$ are maximal orders in $\left(\frac{-1,-7}{\mathbb{Q}}\right)$, and all their endomorphisms are defined.

E_1 and E_2 was in two different isogeny classes over $\mathbb{F}_{7^2}$, but come together over $\mathbb{F}_{7^4}$. If we extend our example to every supersingular elliptic curve over $\mathbb{F}_{7^2}$ and calculate the isogeny classes, we see that every curve with $t = 0$ over $\mathbb{F}_{7^2}$ end up in the same isogeny class, $t = 2\sqrt{q}$ over $\mathbb{F}_{7^4}$. And every curve in either $I(2 \cdot 7)$ or $I(-2 \cdot 7)$ ends up in $I(-2 \cdot 7^2)$. But from 2.10 we know that both $N(2 \cdot 7^2)$ and $N(0)$ must be non-empty, so some new elliptic curves not before defined over $\mathbb{F}_{7^2}$ fill those classes.

Lastly, looking at the same curves over $\mathbb{F}_{7^6}$, noting that this field is not an extension of $\mathbb{F}_{7^4}$, but of $\mathbb{F}_{7^2}$. Now we have that

$$E \in I(2\sqrt{q}) = I(2 \cdot 7^4)$$

$$E_1 \in I(-2\sqrt{q}) = I(-2 \cdot 7^4)$$

$$E_2, E_3 \in I(0).$$

Which are the same relations we had over $\mathbb{F}_{7^2}$. The same is true for all other supersingular elliptic curves over $\mathbb{F}_{7^2}$. This gives us that neither E_2 nor E_3 have all their endomorphisms defined over $\mathbb{F}_{7^6}$.

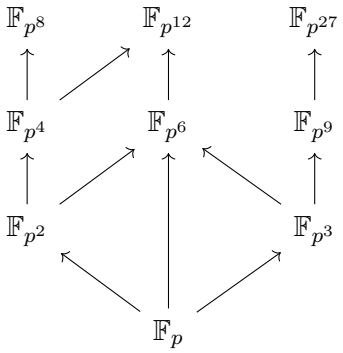
Example 2.44. Below is the table of the value of the trace of the Frobenius endomorphism for each elliptic curve in the example above.

E	E_1	E_2	E_3	Field
$2 \cdot 7$	$-2 \cdot 7$	0	0	$\mathbb{F}_{7^2}$
$-2 \cdot 7^2$	$-2 \cdot 7^2$	$2 \cdot 7^2$	$2 \cdot 7^2$	$\mathbb{F}_{7^4}$
$2 \cdot 7^3$	$-2 \cdot 7^3$	0	0	$\mathbb{F}_{7^6}$
$-2 \cdot 7^4$	$-2 \cdot 7^4$	$2 \cdot 7^4$	$2 \cdot 7^4$	$\mathbb{F}_{7^8}$
$2 \cdot 7^5$	$-2 \cdot 7^5$	0	0	$\mathbb{F}_{7^{10}}$

And by 2.37 and 2.38, we can make the following table for the correspondning rank of each endomorphism ring.

E	E_1	E_2	E_3	Field
4	4	2	2	$\mathbb{F}_{7^2}$
4	4	4	4	$\mathbb{F}_{7^4}$
4	4	2	2	$\mathbb{F}_{7^6}$
4	4	4	4	$\mathbb{F}_{7^8}$
4	4	2	2	$\mathbb{F}_{7^{10}}$

If the rank is 4 we have all endomorphisms defined over the given field and the endomorphism ring corresponds to some maximal order in $\left(\frac{-1,-7}{\mathbb{Q}}\right)$. If the rank is 2, then the corresponding endomorphism ring is a complex quadratic order and we do not have all endomorphisms defined. Note that E_2 and E_3 have all their endomorphisms defined over $\mathbb{F}_{7^4}$, but not over say $\mathbb{F}_{7^6}$. To make sense of this one must remember that $\mathbb{F}_{7^6}$ is not an extension of $\mathbb{F}_{7^4}$ but of $\mathbb{F}_{7^3}$ and $\mathbb{F}_{7^2}$. The following Hasse diagram of finite field extensions where the edges are inclusions explains our situation.



Example 2.45. Similar patterns exists for all characteristics $p \neq 2, 3$. The following elliptic curves over $\mathbb{F}_{11^2}$ are a representative of each non empty isogeny class $I(t)$

$$\begin{aligned}
E &: y^2 = x^3 + 2x && \in I(2 \cdot 11) \\
E_1 &: y^2 = x^3 + \omega x && \in I(0) \\
E_2 &: y^2 = x^3 + (-\omega + 2)x && \in I(-2 \cdot 11) \\
E_3 &: y^2 = x^3 + \omega && \in I(11) \\
E_4 &: y^2 = x^3 + 4\omega + 5 && \in I(-11)
\end{aligned}$$

where $\omega \in \mathbb{F}_{11^2}$ such that $\omega^2 + 7\omega + 2 = 0$. The supersingular j-invariants in $\mathbb{F}_{11^2}$ are only 0 and $1728 \equiv 1 \pmod{11}$, E, E_1 and E_2 has j-invariant 1, and E_3, E_4 have j-invariant 0. We generate similar tables as with $\mathbb{F}_7$

E	E_1	E_2	E_3	E_4	Field
$2 \cdot 11$	0	$-2 \cdot 11$	11	-11	$\mathbb{F}_{11^2}$
$-2 \cdot 11^2$	$2 \cdot 11^2$	$-2 \cdot 11^2$	11^2	11^2	$\mathbb{F}_{11^4}$
$2 \cdot 11^3$	0	$-2 \cdot 11^3$	$-2 \cdot 11^3$	$2 \cdot 11^3$	$\mathbb{F}_{11^6}$
$-2 \cdot 11^4$	$-2 \cdot 11^4$	$-2 \cdot 11^4$	11^4	11^4	$\mathbb{F}_{11^8}$
$2 \cdot 11^5$	0	$-2 \cdot 11^5$	11^5	-11^5	$\mathbb{F}_{11^{10}}$
$-2 \cdot 11^6$	$2 \cdot 11^6$	$-2 \cdot 11^6$	$-2 \cdot 11^6$	$-2 \cdot 11^6$	$\mathbb{F}_{11^{12}}$

And the table of ranks of the endomorphism rings

E	E_1	E_2	E_3	E_4	Field
4	2	4	2	2	$\mathbb{F}_{11^2}$
4	4	4	2	2	$\mathbb{F}_{11^4}$
4	2	4	4	4	$\mathbb{F}_{11^6}$
4	4	4	2	2	$\mathbb{F}_{11^8}$
4	2	4	2	2	$\mathbb{F}_{11^{10}}$
4	4	4	4	4	$\mathbb{F}_{11^{12}}$

Note again that both E_3 and E_4 do not have all endomorphism defined over before $\mathbb{F}_{11^6}$, while E_1 has all their endomorphism defined over $\mathbb{F}_{11^4}$. Now every endomorohism of E_3 and E_4 is defined for every extension of $\mathbb{F}_{11^6}$ and every endomorphism of E_1 is defined for every extension of $\mathbb{F}_{11^4}$. We again refer to the Hasse diagram of field extensions of $\mathbb{F}_p$ above to explain this cyclic behavior. From the diagram we can see that the first field in which E, E_1, E_2, E_3, E_4, E_5 all have all their endomorpisms defined is $\mathbb{F}_{11^{12}}$. This is because $\mathbb{F}_{11^{12}}$ is the smallest extensions with an inclusion from both $\mathbb{F}_{11^4}$ and $\mathbb{F}_{11^6}$. In every extension of $\mathbb{F}_{11^{12}}$ all our curves will have all their endomorphisms defined.

Example 2.46. We now want to categorize every Weierstrass equation that gives us a supersingular elliptic curve over $\mathbb{F}_{5^2}$, and place them in a the right isogeny and isomorphism class. We know that there are 6 isomorphism classes. From 2.5 we have that there is just one supersingular j-invariant over $\mathbb{F}_{5^2}$ and that is 0, and we know from 2.17 that over $\mathbb{F}_5$, there are 6 twists. And we know from 2.10 that there are 4 non-empty supersingular isogeny classes. Lastly, there are 24 Weierstrass equations over $\mathbb{F}_{5^2}$ which gives an elliptic curve with $j(E) = 0$. Categorized by isomorphicm classses and isogeny classes those are:

t=10	t=5	t=5
$y^2 = x^3 + 2$	$y^2 = x^3 + 4\omega + 1$	$y^2 = x^3 + \omega$
$y^2 = x^3 + 4$	$y^2 = x^3 + 3\omega + 2$	$y^2 = x^3 + 2\omega$
$y^2 = x^3 + 3$	$y^2 = x^3 + \omega + 4$	$y^2 = x^3 + 4\omega$
$y^2 = x^3 + 1$	$y^2 = x^3 + 2\omega + 3$	$y^2 = x^3 + 3\omega$
t=-10	t=-5	t=-5
$y^2 = x^3 + 4\omega + 3$	$y^2 = x^3 + \omega + 3$	$y^2 = x^3 + 2\omega + 2$
$y^2 = x^3 + 3\omega + 1$	$y^2 = x^3 + 2\omega + 1$	$y^2 = x^3 + 4\omega + 4$
$y^2 = x^3 + \omega + 2$	$y^2 = x^3 + 4\omega + 2$	$y^2 = x^3 + 3\omega + 3$
$y^2 = x^3 + 2\omega + 4$	$y^2 = x^3 + 3\omega + 4$	$y^2 = x^3 + \omega + 1$

Where $\omega \in \mathbb{F}_{5^2}$ with $\omega^2 - \omega + 2 = 0$. Each box of Weierstrass curves in the table above is an isomorphisms class, the isogeny class is indicated by the t, which is the trace of the Frobenius endomorphism.

2.5 Supersingular functor

We have up to now seen that if a supersingular elliptic curve E have all their endomorphisms defined, then $\mathrm{End}_{\overline{\mathbb{F}_p}}(E)$ will be a maximal order in a quaternion algebra ramified at ∞ and p. Every maximal order in a quaternion algebra ramified at ∞ and p occurs as an endomorphism ring of a supersingular elliptic curve over some $\mathbb{F}_{p^n}$.

2.5.1 Ideals of maximal orders

In this section we will survey the properties of ideals of orders. As orders are rings, these ideals are just ideals of rings. Orders and quaternion algebras are not commutative so it is necessary to distinguish between left and right ideals of an order. Note that an ideal of an order is also a $\mathbb{Z}$-lattice.

We will now define some constructions of orders based on lattices. We fix $\mathcal{A}$ be a quaternion algebra. We start with an important construction of an order from a lattice.

Definition 2.47. Let I be a $\mathbb{Z}$-lattice, we define its left order as

$$\mathcal{O}_L(I) := \{\alpha \in \mathcal{A} | \alpha I \subset I\},$$

and similarly its right order as

$$\mathcal{O}_R(I) := \{\alpha \in \mathcal{A} | I\alpha \subset I\}.$$

Theorem 2.48. *$\mathcal{O}_L(I) \subset \mathcal{A}$ is an order.*

Proof. See [Voi21, 10.2.7]. □

Our goal now is to bring the concept of a class groups to orders in quaternion algebras. We start by defining left (right) invertible ideals.

Definition 2.49. Let $I \subset \mathcal{A}$ be a $\mathbb{Z}$-lattice. We say that I is left (right) invertible if there exists some $I' \subset \mathcal{A}$ $\mathbb{Z}$-lattice such that $II' = \mathcal{O}_L(I)$ ($I'I = \mathcal{O}_R(I)$). I is said to be invertible if I' is both the left and right sided inverse,

$$II' = \mathcal{O}_L(I) = \mathcal{O}_R(I') \quad \text{and} \quad I'I = \mathcal{O}_L(I') = \mathcal{O}_R(I).$$

If I is invertible, then the $\mathbb{Z}$-lattice I' is uniquely given by

$$I' = I^{-1} := \{\alpha \in \mathcal{A} | I\alpha I \subseteq I\}.$$

Definition 2.50. Let $\mathcal{O} \subset \mathcal{A}$ be an order. A left (right) fractional $\mathcal{O}$-ideal is a lattice $I \subset \mathcal{A}$ such that $\mathcal{O} \subseteq \mathcal{O}_L(I)$ ($\mathcal{O}_R(I)$).

Remark. As with fractional ideals of rings of integers, which are modules, fractional ideals of orders are not in fact necessarily ideals but $\mathbb{Z}$-lattices. Of course a $\mathbb{Z}$-lattice may be an ideal in the usual sense of an order.

Theorem 2.51. *Let $\mathcal{O} \subset \mathcal{A}$ be a maximal order. Then every left (right) fractional $\mathcal{O}$-ideal is invertible.*

Proof. See [Voi21, 16.1.2]. □

Definition 2.52. Let I be a $\mathbb{Z}$-lattice, the reduced norm of I, denoted $\mathrm{nrd}(I)$ is defined to be

$$\mathrm{nrd}(I) := \gcd(\{\mathrm{nrd}(\alpha) | \alpha \in I\}).$$

We are now able to define the class set of an order. We start by defining the following equivelance relation:

Definition 2.53. Let $I, J \in \mathcal{A}$ be $\mathbb{Z}$-lattices, then we say that I and J are in the same right class and write $I \sim_R J$ if there exists some $\alpha \in \mathcal{A}^*$ such that $\alpha I = J$. Equivalently

$$I \sim_R J \iff \mathcal{O}_R(I) = \mathcal{O}_R(I).$$

Finally, the equivalence class of I is denoted $[I]_R$.

Definition 2.54. Let $\mathcal{O} \in \mathcal{A}$ be an order then the right class set of $\mathcal{O}$ is defined as

$$\mathrm{Cls}_R\mathcal{O} := \{[I]_R | I \text{ an invertible right fractional } \mathcal{O} - \text{ideal}\}.$$

The order of the right class set is called the right class number of $\mathcal{O}$ and denoted $\#\mathrm{Cls}_R\mathcal{O}$.

Remark. $\mathrm{Cls}_R\mathcal{O}$ is not a group unlike the class groups for Dedekind rings, for example the lattices IJ and $I\alpha J$, for $\alpha \in \mathcal{A}^*$ are not necessarily in the same equivalence class.

2.5.2 An equivalence of categories

The goal of this section is to describe a categorical equivalence between supersingular elliptic curves and left modules of maximal orders, and isogenies and left modules homomorphism. We do this to use the language of quaternion algebras developed earlier to describe isogenies. We have some connection to from elliptic curves and quaternion algebras, but it is not yet described functorially. Unlike the earlier sections we specifically want to look at elliptic curves over $\overline{\mathbb{F}_p}$. For brevity let now $\mathrm{End}(E) := \mathrm{End}_{\overline{\mathbb{F}_q}(E)}$ and $\mathrm{Hom}(E, E') := \mathrm{Hom}_{\overline{\mathbb{F}_q}}(E, E')$ unless otherwise specified.
We get our first desired functoral property by the following result.

Theorem 2.55. *Let E, E' be supersingular elliptic curves over $\overline{\mathbb{F}_q}$. Then $\mathrm{Hom}(E, E')$ is a $\mathbb{Z}$-module of rank 4, and is invertible as a right $\mathrm{End}(E)$-module under precomposition and a left $\mathrm{End}(E')$-module under post composition.*

Proof. See [Voi21, 42.1.11] □

The following construction gives us a left ideal of $\mathrm{End}(E)$ for each finite subgroup $G \subset E$:

$$I(G) := \{\alpha \in \mathrm{End}(E) | \alpha(P) = O_E, \forall P \in G\}.$$

Then $I(G)$ will be a non-zero left ideal of $\mathrm{End}(E)$, as $[|G|] \in I(G)$. Conversely, we have a construction for a nonzero left ideal I in $\mathcal{O} = \mathrm{End}(E)$ with $p \nmid \mathrm{nrd}(I)$. We define it as:

$$E[I] := \bigcap_{\alpha \in I} \{P \in E | \alpha(P) = O_E\}.$$

Furthermore, we denote $E_I = E/E[I]$, and have the corresponding seprable isogeny $\phi_I : E \to E_I$ by 1.9. The relationship of these constructions is fleshed out by the following result.

Theorem 2.56. *The precomposition map*

$$\phi_I^* : \mathrm{Hom}(E_I, E) \to I$$

$$\psi \mapsto \psi\phi_I$$

is an isomorphism of left $\mathcal{O}$-modules.

Proof. See [Voi21, 42.2.7]. □

Theorem 2.57. *Let E_I be as defined above, then*

$$\mathrm{End}(E_I) \cong \mathcal{O}_R(I).$$

Proof. See [Voi21, 42.2.9]. □

The next result gives us that the isomorphism class of E_I is defined by the left ideal class of I.

Theorem 2.58. *If $J = I\alpha \subset \mathcal{O}$ be left ideals, with $\alpha \in \mathcal{A}$, that is $J \in [I]_R$, then $E_J \cong E_I$.*

Proof. See [Voi21, 42.2.13]. □

Theorem 2.59. *The following holds*

(i) $\deg(\phi_I) = \mathrm{nrd}(I)$.

(ii) $I(E[I]) = I$.

Proof. See [Voi21, 42.2.16]. □

Theorem 2.60. *For every isogeny from $\phi : E \to E'$, there exists a left $\mathcal{O}$-ideal I and an isomorphism $\rho : E_I \to E'$.*

Proof. See [Voi21, 42.2.21]. □

As we've seen in 2.37 we have that each maximal order of $\mathcal{A}$ occurs as an endomorphism ring of some supersingular elliptic curve. We now have that each supersingular isogeny from some elliptic curve occur as some left $\mathcal{O}$-ideal with the reduced norm of I being equal to the degree of the isogeny. The next result gives us that this correspondence is not only surjective but also injective.

Theorem 2.61. *Let $E_0/\overline{\mathbb{F}_p}$ be a supersingular curve and $\mathcal{O}_0 := \mathrm{End}(E_0)$ its endomorphism ring. Then the functor*

$$\mathbf{I} : E \mapsto \mathrm{Hom}(E, E_0)$$

gives an equivalence of categories between

$$\left[\text{supersingular elliptic curves over } \overline{\mathbb{F}_p} \text{ under isogenies}\right]$$

and

$$\left[\text{invertible left } \mathcal{O}_0\text{−modules under left } \mathcal{O}_0\text{−module homomorphisms}\right].$$

Proof. See [Voi21, 43.3.2]. □

Remark. The functor $\mathbf{I}$ above is contravariant, one can define a covariant functor $\mathrm{Hom}(E_0, -)$ to right $\mathcal{O}_0$-modules, the dual category to left $\mathcal{O}_0$-modules, which are also categorically equivalent.

Corollary 2.62 (Deuring correspondence)**.** *There exists a bijection between isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}_p}$ and the left class set $\mathrm{Cls}_L\mathcal{O}_0$.*

$$E \cong E_I \leftrightarrow [I]_L.$$

Proof. See[Voi21, 42.3.7]. □

Using this theory we can now work with supersingular elliptic curves over $\overline{\mathbb{F}_p}$ by doing calculation on quaternion algebras. We're using the computer algebra system Magma for the computations.

Example 2.63. We begin by choosing supersingular elliptic curves over $\overline{\mathbb{F}_{23}}$. $23 \equiv 3 \mod 4$ so we have that every supersingular elliptic curve over $\overline{\mathbb{F}_{23}}$ will be a maximal order of the quaternion algebra $\mathcal{A} = \left(\frac{-1,-23}{\mathbb{Q}}\right)$ by 2.31. Conversely every maximal order will occur as some endomorphism ring. We construct the maximal ideal from 2.36 as our starting endomorphism ring $\mathcal{O}_0$

```
K:=Rationals();
A<i,j,k>:=QuaternionAlgebra<K|-23,-1>;
B:=[1/2+1/2*j,1/2*i+1/2*k,j,k];
O:=QuaternionOrder(B);
```

Now, we check that the Deuring correspondance holds. From 2.5 we expect there should three isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}_{23}}$, which means there should be three equivalence classes in $\mathrm{CLs}_R(O)$, this is confirmed by.

```
#RightIdealClasses(O);
3
```

Now, we want to generate every maximal order that occurs as an endomorphism ring of some E_I, where I is of some specific $\mathrm{nrd}(I) = l$, with $p \nmid l$. This will give us both the supersingular isogeny graph over $\overline{\mathbb{F}_{23}}$ restricted to isogenies of degree l, called the supersingular l-isogeny graph, and the explicit description of the endomorphism rings. We set $l = 3$ and proceed with the calculations.

```
L:=MaximalLeftIdeals(O,3);
O1:=RightOrder(L[1]);
O2:=RightOrder(L[2]);
O3:=RightOrder(L[3]);
O4:=RightOrder(L[4]);
```

In the case of $\overline{\mathbb{F}_{23}}$, we know that the 3 isomorphism classes have distinct automorphism groups in which we can easily distinguish them by. Calculating the number of units in each `O`, `O1`, `O2`, `O3`, `O4`, gives us, respectively, 4, 2, 2, 6, 6. Which means that there exists two isogenies of degree 3 from E_{1728} to E_0 and E_{19}. Lastly to get the full picture, we want to check what isogenies of degree 3 exists between E_{1728} and E_0. We have that $\mathrm{End}(E_{19}) =$`O`, $\mathrm{End}(E_{1728}) =$`O1` and $\mathrm{End}(E_0) =$`O3`, and look at all maximal ideals of `O1` with $\mathrm{nrd}(I) = 3$.

```
S:=MaximalLeftIdeals(O1,3);
S1:=RightOrder(S[1]);
S2:=RightOrder(S[2]);
S3:=RightOrder(S[3]);
S4:=RightOrder(S[4]);
#Units(O1);
#Units(S1);
#Units(S2);
#Units(S3);
#Units(S4);
```

We get that there are no right orders of `O1` that have an automorphism group with 6 elements, therefore there are no isogeny of degree 3 between E_{1728} and E_0. The full 3-isogeny graph is then done. It is connected which all supersingular l-isogeny graphs over $\overline{\mathbb{F}_p}$ are [Koh96, 78]

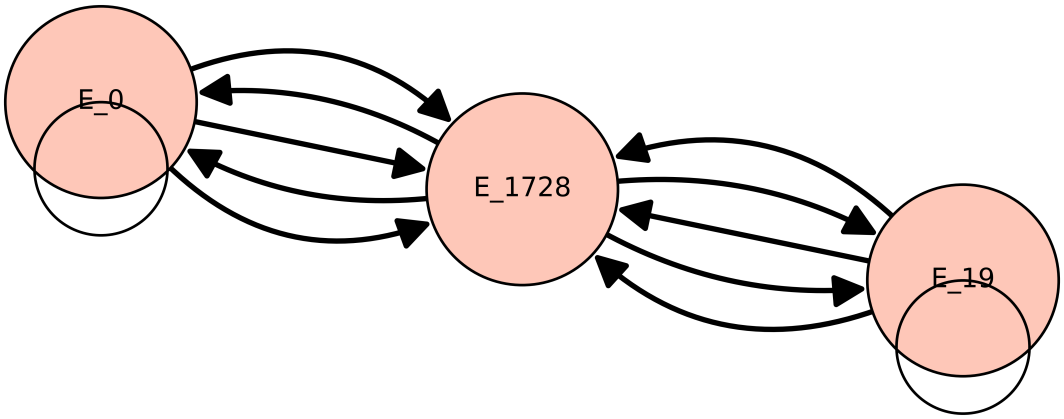


Figure 2.1: 3-isogeny graph over $\overline{\mathbb{F}_{23}}$

Chapter 3

Tables and Code

3.1 Code

3.1.1 Isomorphism and isogeny classes

The code below generates all elliptic curves by making a list, `curves`, with every Weierstrass curve over $\mathbb{F}_{5^2}$, along the corresponding trace of their Frobenius endomorphism and j-invariant.

```
p=5
F.<w> = GF(p^2)
curves = []
for a_4 in F:
    for a_6 in F:
        try:
            E=EllipticCurve(F,[a_4,a_6])
            curves.append([[a_4,a_6],(E.count_points()-p^2-1),E.
    j_invariant()])
        except:#passes in the cases that a_4 and a_6 gives singular curve
            pass
curves.sort(key=lambda x: x[2])#sorts after j-invariants
```

The following code generates the $\mathbb{F}_{5^2}$-isomorphism adjacency matrix.

```
jinv=0
curvessubset = []#curves with j-invariant equal to jinv
for e in curves:
    if (e[2] == jinv):
        curvessubset.append(e)

mat=[[0]*len(curvessubset) for i in range(len(curvessubset))]#initialize
    adjiaceny matrix
for i in range(len(curvessubset)):
    for j in range(len(curvessubset)):
        if EllipticCurve(F,curvessubset[i][0]).is_isomorphic(
    EllipticCurve(F,curvessubset[j][0])):
            mat[i][j] =1
#construction of n works for q=p^2, does NOT work for all field sizes
#construction of isomorphism classes lists
if jinv==0:
    n=[[] for i in range(6)]
elif jinv == (1728%p):
    n=[[] for i in range(4)]
else:
```

```
    n=[[] for i in range(2)]
for i in range(len(curvessubset)):#adding the curves into right
    isomorphism classes
    for j in range(len(n)):
        if mat[i][j]==1:
            n[j].append(EllipticCurve(F,curvessubset[i][0]))
m=matrix(mat)
print(m)
[1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0]
[0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0]
[0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0]
[0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0]
[0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0]
[0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1]
[1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0]
[0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0]
[0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0]
[0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0]
[0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0]
[0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1]
[1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0]
[0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0]
[0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0]
[0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0]
[0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0]
[0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1]
[1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0]
[0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0]
[0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0]
[0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0]
[0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0]
[0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1]
```

Using the adjacency matrix we can categorize all the Weierstrass equations into their isomorphism classes. In this case there are 6 classes since $j = 0$. Then using the number of rational points we can place them in their isogeny class.

3.1.2 Supersingular j-invariants

The following code uses algorithm of Sage based on 2.6 to find the unique polynomial with roots equal to supersingular j-invariants for each characteristic p. The first element of each list is the prime characteristic, and if the polynomial is 1 then the only supersinuglar j-invariants are either 0, 1728 or both.

```
from sage.schemes.elliptic_curves.ell_finite_field import
    supersingular_j_polynomial
polys= [p,supersingular_j_polynomial(p).factor() for p in prime_range(83)
    ]
[2, 1]
[3, 1]
[5, 1]
[7, 1]
[11, 1]
[13, j + 8]
[17, j + 9]
[19, j + 12]
[23, j + 4]
[29, (j + 4) * (j + 27)]
[31, (j + 27) * (j + 29)]
[37, (j + 29) * (j^2 + 31*j + 31)]
```

```
[41, (j + 9) * (j + 13) * (j + 38)]
[43, (j + 2) * (j^2 + 19*j + 16)]
[47, (j + 3) * (j + 37) * (j + 38)]
[53, (j + 3) * (j + 7) * (j^2 + 50*j + 39)]
[59, (j + 11) * (j + 12) * (j + 31) * (j + 44)]
[61, (j + 11) * (j + 20) * (j + 52) * (j^2 + 38*j + 24)]
[67, (j + 1) * (j^2 + 8*j + 45) * (j^2 + 44*j + 24)]
[71, (j + 5) * (j + 23) * (j + 30) * (j + 31) * (j + 54)]
[73, (j + 17) * (j + 64) * (j^2 + 57*j + 8) * (j^2 + 68*j + 9)]
[79, (j + 15) * (j + 58) * (j + 62) * (j + 64) * (j^2 + 14*j + 62)]
[83, (j + 16) * (j + 33) * (j + 55) * (j + 66) * (j^2 + 7*j + 73)]
```

3.1.3 Isogenies

The SageMath code used to calculate example 1.19.

```
from sage.schemes.elliptic_curves.hom_frobenius import
    EllipticCurveHom_frobenius
p=11
F.<w>= GF(p)
E=EllipticCurve(F,[2, 0])
phi= EllipticCurveHom_frobenius(E)
phihat= phi.dual()
for P in E:
    if phihat(P) != -P:
        print("E is not supersingular")
```

The Sagemath code used to calculte example 1.16

```
p=5
F.<w>= GF(p)
E=EllipticCurve(F,[0, 1])
for P in E:
    print(P, 3*P)
```

And to see where all points were defined we need not look further than $\mathbb{F}_{5^2}$

```
p=5
F.<w>= GF(p^2)
E=EllipticCurve(F,[0, 1])
torsion3=[]
for P in E:
    if 3*P==0*P:
        torsion3.append(P)
len(torsion3)
9
```

More generally, one may use [Sch87, 3.7] to see which torsion groups are defined over which field extensions.

3.2 Tables

The following tables are generated by the code in the prior section.

Supersingular elliptic curves over $\mathbb{F}_{5^2}$

t	$\lvert E(\mathbb{F}_q)\rvert = q+1-t$	$N(t)$	$j(E) \mod p$
10	16	1	0
5	21	2	0
0	26	0	-
-5	31	2	0
-10	36	1	0

All curves in both $N(\pm 10)$ have the same endomorphism ring, as they are $\bar{\mathbb{F}}_5$-isomorphic and have all their endomorphism defined already over $\mathbb{F}_{25}$. That endomorphism is the maximal order in $\mathcal{O} \subset \mathcal{A} = \left(\frac{-5,-2}{\mathbb{Q}}\right)$. The following Magma code generates a basis for this maximal order.

```
K:= Rationals () ;
A<i,j,k>:=QuaternionAlgebra < K | -2 , -5 >;
O:=MaximalOrder(A);
Basis(O)
```

Which gives us

$$\mathcal{O} = \left\langle 1, \frac{2-i+k}{4}, \frac{2+3i+k}{4}, \frac{-1+i+j}{2} \right\rangle.$$

This is, up to isomorphism, the only maximal order of $\mathcal{A}$, and is the endomorphism ring of curves in $N(\pm 10)$.

Supersingular elliptic curves over $\mathbb{F}_{7^2}$

height t	$\lvert E(\mathbb{F}_q)\rvert = q+1-t$	$N(t)$	$j(E) \mod p$
14	36	1	$1728 \equiv 6$
7	43	0	-
0	50	2	$1728 \equiv 6$
-7	57	0	-
-14	64	1	$1728 \equiv 6$

Over $\mathbb{F}_{7^2}$ the only supersingular j-invariant is $1728 \equiv 3 \pmod 7$. As excepted by 2.40 there are two isomorphism classes in $I(0)$, and in total 4 twists.

Supersingular elliptic curves over $\mathbb{F}_{11^2}$

t	$\lvert E(\mathbb{F}_q)\rvert = q+1-t$	$N(t)$	$j(E) \mod p$
22	100	2	$0, 1728 \equiv 1$
11	111	2	0
0	122	2	$1728 \equiv 1$
-11	133	2	0
-22	144	2	$0, 1728 \equiv 1$

Characteristic 11 is an example of a characteristic where we have the maxmial amount of supersingular isogeny classes: 5. Both 0 and 1728 are supersingular j-invariants, then by 2.40 we have that both $N(\pm 11)$ and $N(0)$ are non-zero.

Supersingular elliptic curves over $\mathbb{F}_{37^2}$

t	$\lvert E(\mathbb{F}_q)\rvert = q+1-t$	$N(t)$	$j(E) \mod p$
74	1296	3	$8, 10w+20, 27w+23$
37	1333	0	-
0	1370	0	-
-37	1407	0	-
-74	1444	3	$8, 10w+20, 27w+23$

Characteristic 37 is the first characteristic we see a j-invariant not in $\mathbb{F}_p$ but in $\mathbb{F}_{p^2}$. We have that $37 \equiv 1 \pmod{12}$ so neither 0 nor 1728 are supersingular, and we can see from the table that there are no curves with $t \neq \pm 2\sqrt{q}$ which agrees with 2.40. Therefore, all supersingular elliptic curves over $\mathbb{F}_{37^{2n}}$ will have all their endomorphisms defined.

Bibliography

[BCP97] Wieb Bosma, John Cannon and Catherine Playoust. 'The Magma algebra system. I. The user language'. In: *J. Symbolic Comput.* 24.3-4 (1997). Computational algebra and number theory (London, 1993), pp. 235–265. ISSN: 0747-7171. DOI: 10.1006/jsco.1996.0125. URL: http://dx.doi.org/10.1006/jsco.1996.0125.

[Gal12] Steven D. Galbraith. *Mathematics of public key cryptography*. Cambridge University Press, Cambridge, 2012, pp. xiv+615. ISBN: 978-1-107-01392-6. DOI: 10.1017/CBO9781139012843. URL: https://doi.org/10.1017/CBO9781139012843.

[Koh96] David Russell Kohel. *Endomorphism rings of elliptic curves over finite fields*. Thesis (Ph.D.)–University of California, Berkeley. ProQuest LLC, Ann Arbor, MI, 1996, p. 117. ISBN: 978-0591-32123-4. URL: http://gateway.proquest.com/openurl?url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mtx:dissertation&res_dat=xri:pqdiss&rft_dat=xri:pqdiss:9723065.

[Mil11] James S. Milne. *Algebraic Number Theory (v3.03)*. Available at www.jmilne.org/math/. 2011.

[Neu99] Jürgen Neukirch. *Algebraic number theory*. Vol. 322. Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. Springer-Verlag, Berlin, 1999, pp. xviii+571. ISBN: 3-540-65399-6. DOI: 10.1007/978-3-662-03983-0. URL: https://doi.org/10.1007/978-3-662-03983-0.

[Piz80] Arnold Pizer. 'An algorithm for computing modular forms on $\Gamma_0(N)$'. In: *J. Algebra* 64.2 (1980), pp. 340–390. ISSN: 0021-8693. DOI: 10.1016/0021-8693(80)90151-9. URL: https://doi.org/10.1016/0021-8693(80)90151-9.

[Sag23] Sage. *SageMath, the Sage Mathematics Software System (Version 9.3.10)*. `https://www.sagemath.org`. 2023.

[Sch87] René Schoof. 'Nonsingular plane cubic curves over finite fields'. In: *J. Combin. Theory Ser. A* 46.2 (1987), pp. 183–211. ISSN: 0097-3165. DOI: 10.1016/0097-3165(87)90003-3. URL: https://doi.org/10.1016/0097-3165(87)90003-3.

[Sch95] René Schoof. 'Counting points on elliptic curves over finite fields'. In: vol. 7. 1. Les Dix-huitièmes Journées Arithmétiques (Bordeaux, 1993). 1995, pp. 219–254. URL: http://jtnb.cedram.org/item?id=JTNB_1995__7_1_219_0.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*. Second. Vol. 106. Graduate Texts in Mathematics. Springer, Dordrecht, 2009, pp. xx+513. ISBN: 978-0-387-09493-9. DOI: 10.1007/978-0-387-09494-6. URL: https://doi.org/10.1007/978-0-387-09494-6.

[Sil14] Joe(https://mathoverflow.net/users/11926/joe-silverman) Silverman. *j-invariants of elliptic curves over finite fields*. MathOverflow. URL:https://mathoverflow.net/q/185291 (version: 2014-10-24). 2014. eprint: https://mathoverflow.net/q/185291. URL: https://mathoverflow.net/q/185291.

[Sut12] Andrew V. Sutherland. 'Identifying supersingular elliptic curves'. In: *LMS Journal of Computation and Mathematics* 15 (Sept. 2012), pp. 317–325. DOI: 10.1112/s1461157012001106. URL: https://doi.org/10.1112%5C%2Fs1461157012001106.

[Voi21] John Voight. *Quaternion algebras*. Vol. 288. Graduate Texts in Mathematics. Springer, Cham, [2021] ©2021, pp. xxiii+885. ISBN: 978-3-030-56692-0; 978-3-030-56694-4. DOI: 10.1007/978-3-030-56694-4. URL: https://doi.org/10.1007/978-3-030-56694-4.

[WM71] W. C. Waterhouse and J. S. Milne. 'Abelian varieties over finite fields'. In: *1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969)*. Amer. Math. Soc., Providence, R.I., 1971, pp. 53–64.