2014-09-23

An Elliptic Curve over Q has an Isogenous Quadratic Twist if and Only if it has complex Multiplication

B.Langlois, Marie-Andree

UNIVERSITY OF CALGARY

An Elliptic Curve Over Q has an Isogenous Quadratic Twist if and Only if it has Complex Multiplication

by

Marie-Andrée B.Langlois

A THESIS

SUBMITTED TO THE FACULTY OF GRADUATE STUDIES

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE

DEGREE OF MASTERS OF SCIENCE

DEPARTMENT OF MATHEMATICS AND STATISTICS

CALGARY, ALBERTA

September, 2014

Abstract

In this thesis we prove that, for every elliptic curve E over the rational numbers, E is isogenous to a quadratic twist if and only if E admits complex multiplication. To prove this, we use a famous result of Faltings comparing local and global isogenies of elliptic curves over number fields, and a famous theorem proven by Serre on the density of supersingular primes for elliptic curves over the rational numbers. While the result of this thesis is certainly known to experts, a proof seems to not appear in the literature. The thesis includes background on elliptic curves, isogenies, twists and complex multiplication.

Acknowledgements

I would like to express my sincere gratitude to my supervisor Professor Clifton Cunningham for all his help, encouragement and support. This work would not have been possible without his guidance and enthusiasm to share his great knowledge of the subject.

I am grateful to all the members of the committee who took the time to read and comment on the manuscript. I especially would like to thank Professor Mark Bauer for always taking the time to answer my questions. I would like to thank the faculty and staff of the department of Mathematics and Statistics of the university of Calgary, especially Yanmei Fei and Professor Renate Scheidler who believed in me and gave me many opportunities to develop myself during this degree.

Finally I would like to thank my friends who always had faith in me and encouraged me through all my degree. A special thanks to Lyudmila Korobenko for all of her support and wonderful advice, to Jean-François Biasse who read many versions of this thesis, and Marie-Claude Samson for being the one catching me every time I would fall during the last two years.

Table of Contents

Chapter 1

Elliptic Curves

1.1 Introduction

Elliptic curves have proven themselves to be very useful in cryptography. Working with the group structure of points on an elliptic curve provides more efficient computations for the same level of security than other public key systems such as RSA that relies on the fact that integer factoring is a difficult problem. Elliptic curves also played a role in proving Fermat's last theorem. These are some reasons why it is important to develop computational tools for elliptic curves. When looking at elliptic curves, isogenies are a predominant topic. They are used in many famous algorithms about elliptic curves, including Schoof, Elkies, Atkin's [15] method for counting points on an elliptic curve. Isogenies preserve some of the structure of a curve without necessarily keeping the exact same equation, so they can be used to make certain problems relating to elliptic curves easier. For example they reduce the instance of the discrete logarithm problem on the group of points of a curve to an instance of the same problem on an isogenous curve where it might be easier to solve.

The main goal of this thesis is to prove that elliptic curves (defined in Section 1.3) with complex multiplication, which is introduced in Chapter 5, and elliptic curves that are isogenous (see Chapter 2) to a quadratic twist, as explained in Chapter 4 are actually the same curves. The main theorem in Chapter 6 proves this, giving an easier way of detecting if an elliptic curve has complex multiplication. Chapter 2 provides background on isogenies and includes computational explorations. Chapter 3 deals with reduction of elliptic curves (mod p) and how this can be used to establish that curves are isogenous over $\mathbb{Q}$ (see Section 3.1). The following chapter is about quadratic twists and includes some examples of

elliptic curves isogenous to their quadratic twist (see Section 4.1).

We assume the reader is familiar with basic notions from algebraic geometry, as found, for example, in Chapter 1 of [6] and recalled briefly in Appendix A. In particular recall that, if K is a field, then an algebraic variety over K (see Definition A.5.1) is a K-scheme (see Definition A.2.2) covered by affine K-schemes $X = \bigcup X_i$ for which $K[X_i] = K[x_1, \ldots, x_n]/I$ for some n and for some ideal $I \lhd K[x_1, \ldots, x_n]$ such that $I = \sqrt{I}$.

1.2 Projective Plane and Curves

Since elliptic curves are projective varieties (see Section A.5), we begin with a description of the projective plane as a scheme (see Section A.2) and then as a variety, to finally show how to define projective curves as subvarieties of the projective plane.

We start by defining the schemes $\mathbb{P}^2$ and $\mathbb{A}^2$, then we show how to obtain the relative schemes (see Section A.4) $\mathbb{P}^2_K$ and $\mathbb{A}^2_K$, for a field K. The projective plane $\mathbb{P}^2$ is a scheme produced by glueing together three copies of the affine plane $\mathbb{A}^2$, as follows. Set $X = \mathrm{Spec}(\mathbb{Z}[y, z])$, $Y = \mathrm{Spec}(\mathbb{Z}[x, z])$ and $Z = \mathrm{Spec}(\mathbb{Z}[x, y])$. Let $X_y \subset X$ be the open affine subscheme defined by localization at $y \in \mathbb{Z}[y, z]$ as explained in Section A.2; likewise define $X_z \subset X$, $Y_x \subset Y$, $Y_z \subset Y$, $Z_x \subset Z$ and $Z_y \subset Z$.

We now glue X to Y along the open subschemes X_y and Y_x using the isomorphism $X_y \cong Y_x$ corresponding (under Proposition A.2.1), to $\mathbb{Z}[y, z]_y \to \mathbb{Z}[x, z]_x$ defined by $y \mapsto x^{-1}$. Likewise, glue X to Z along the open subschemes X_z and Z_x using the isomorphism $X_z \cong Z_x$ corresponding to $\mathbb{Z}[y, z]_z \to \mathbb{Z}[x, y]_x$ defined by $z \mapsto x^{-1}$. Finally, glue Y to Z along the open subschemes Y_z and Z_y using the isomorphism $Y_z \cong Z_y$ corresponding to $\mathbb{Z}[x, z]_z \to \mathbb{Z}[x, y]_y$ defined by $z \mapsto y^{-1}$. The resulting scheme, covered by the affine schemes X, Y and Z, is the projective plane:

$$\mathbb{P}^2 = X \cup Y \cup Z.$$

Using this glueing, the set of R-rational points $\mathbb{P}^2(R)$, for any commutative ring with identity R, is given by

$$\mathbb{P}^2(R) = \{[a : b : c] \mid a, b, c \in R \text{ and } a \in R^* \text{ or } b \in R^* \text{ or } c \in R^*\}.$$

The R-rational points on the affine subscheme $X \subset \mathbb{P}^2$ correspond to the subset

$$X(R) = \{[a : b : c] \in \mathbb{P}^2(R) \mid a \in R^*\}.$$

Likewise,

$$Y(R) = \{[a : b : c] \in \mathbb{P}^2(R) \mid b \in R^*\} \qquad \text{and} \qquad Z(R) = \{[a : b : c] \in \mathbb{P}^2(R) \mid c \in R^*\}.$$

The relative scheme $\mathbb{A}^2_K \to \mathrm{Spec}(K)$, where $\mathbb{A}^2_K = \mathbb{A}^2 \times_{\mathrm{Spec}(\mathbb{Z})} \mathrm{Spec}(K)$, is obtained by pulling back $\mathbb{A}^2 \to \mathrm{Spec}(\mathbb{Z})$ along $\mathrm{Spec}(K) \to \mathrm{Spec}(\mathbb{Z})$; see Section A.2 and, for more details, [24]. Glueing three copies of $\mathbb{A}^2_K$ in the same manner as above produces $\mathbb{P}^2_K = X_K \cup Y_K \cup Z_K$.

Now we look at how to write the equation of a curve that is a variety in $\mathbb{P}^2_K$. Given $h(x, y, z) \in K[x, y, z]$, a homogenous polynomial, we can consider the two variable polynomial $h_x(y, z)$ which is obtained by letting $x = 1$ and similarly, we obtain $h_y(x, z)$ and $h_z(x, y)$. We consider the variety $V_x = \mathrm{Spec}(K[y, z]/\langle h_x \rangle) \subseteq \mathbb{A}^2_K$, and similarly affine varieties V_y and V_z. Given how $\mathbb{P}^2_K$ was defined, we have an injection $\mathbb{A}^2_K \hookrightarrow \mathbb{P}^2_K$, hence we can embed V_x, V_y and V_z in $\mathbb{P}^2_K$. When glueing these three varieties as above, we obtain $V := V_x \cup V_y \cup V_z$ a variety in $\mathbb{P}^2_K$.

Example 1.2.1. *Consider the affine equation over K given by $y^2 = x^3 - 1$; this corresponds to the affine variety $\mathrm{Spec}(K[x, y]/\langle y^2 - x^3 + 1 \rangle)$. This affine curve can be embedded in $\mathbb{P}^2_K$ by passing to the variety in $\mathbb{P}^2_K$ defined by the homogenous equation $y^2 z = x^3 - z^3$ as above. If $z \neq 0$ then $[x : y : z] = [\frac{x}{z} : \frac{x}{z} : 1]$; if $z = 0$ and $[x : y : z]$ lies on the curve then the equation gives $x^3 = 0$, thus $x = 0$ so $[x : y : z] = [0 : 1 : 0]$, the point at infinity.*

1.3 Definition

We have seen that the projective variety $\mathbb{P}^2_K$ is covered by three affine planes:

$$\mathbb{P}^2_K = \mathbb{A}^2_K \cup \mathbb{A}^2_K \cup \mathbb{A}^2_K$$

with glueing data described in Section 1.2. An *elliptic curve over* K (denoted E/K) is a smooth variety that is K-isomorphic to a subvariety of $\mathbb{P}^2_K$, defined by a homogeneous polynomial of the form

$$E: \qquad Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \qquad a_1, \ldots, a_6 \in K \quad (1.1)$$

following the recipe of Example 1.2.1, and with at distinguished element $\mathcal{O}_E$ corresponding to $[0:1:0]$. Polynomials of the form (1.1) are called Weierstrass equations.

Remark 1.3.1. *For the reader familiar with function fields, the Riemann-Roch theorem can be used to get an alternate characterization of elliptic curves; an elliptic curve is a function field of genus 1, having a divisor of degree 1. More details about this can be found in [19, §3].*

It is not true that every Weierstrass equation defines an elliptic curves, since the corresponding projective variety might not be smooth (recall Definition A.5.2). The projective variety defined by a Weierstrass equation is smooth when its discriminant Δ, defined below, is non-zero:

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

where

$$b_2 = a_1^2 + 4a_2$$

$$b_4 = 2a_4 + a_1a_3$$

$$b_6 = a_3^2 + 4a_6$$

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$$

$$c_4 = b_2^2 - 24b_4.$$

When $\mathrm{char}(K) \neq 2, 3$ the following change of variables

$$x \mapsto \frac{1}{36}(x - 3a_1^2 - 12a_2)$$
$$y \mapsto \frac{1}{216}(y - a_1x - 12a_3)$$

transforms (1.1) into

$$E: \qquad Y^2Z = X^3 + AXZ^2 + BZ^3, \qquad A,\ B\ \in K. \tag{1.2}$$

The discriminant of this curve simplifies to $\Delta = -(4A^3 + 27B^2)$.

Much can be learned about E, for example the group law that is defined in Section 1.4, through the affine curve E_{aff} defined by

$$E_{\mathrm{aff}} := E \cap \mathbb{A}^2_Z. \tag{1.3}$$

Note that the ring of regular functions on E_{aff} is given by

$$K[E_{\mathrm{aff}}] = K[x, y]/\langle y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6\rangle.$$

The *function field* for E/K is

$$K(E) := K(x)[y]/\langle y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6\rangle.$$

1.4 Group Law

This section shows how points on an elliptic curve form a group, and how two points on a curve can be composed by the group law.

Proposition 1.4.1 ([24, §19.10.4]). *Every elliptic curve over K admits a unique group scheme structure (see Section A.6) over K with identity $\mathcal{O}_E$.*

For an algebraically closed field $\overline{K}$, elliptic curves have the property that every line $L \subset \mathbb{P}^2_{\overline{K}}$ intersects E at exactly 3 points, which may not be distinct; see [19, III,§2]. This fact can be used to define the group law on points, as pictured in the following example where $K = \mathbb{R}$.

Example 1.4.1. *Let E be a curve defined over $\mathbb{R}$, as pictured below. Let P, Q be points of E and $L(x)$ the line connecting P and Q, and R the third point of intersection of L with E (when starting with $P = Q$ take the tangent to E at P). Let L' be the line connecting R and $\mathcal{O}_E$; then $P + Q$ is the third point of intersections of L' and E. We have $P + Q + R = \mathcal{O}_E$. The point $\mathcal{O}_E$ cannot be represented in $\mathbb{R}^2$, but it can be thought of as located at where both*

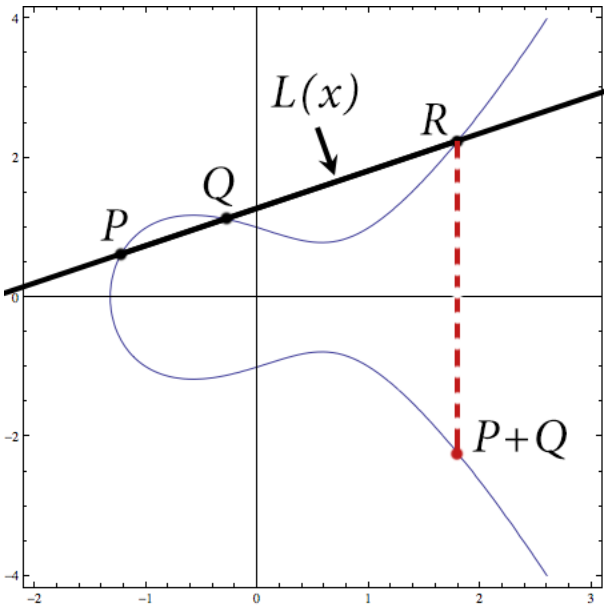


Figure 1.1: Addition of Points on an Elliptic Curve

ends of the y-axis meet.

1.5 j-invariants

Two elliptic curves E and E' are isomorphic when one can find scheme morphisms $\phi_i \colon E_i \to E_i'$ and $\psi_i \colon E_i' \to E_i$ such that their compositions $\psi_i \circ \phi_i$ and $\phi_i \circ \psi_i$ are the identities on E_i and E_i' respectively. When ϕ_i and ψ_i are defined over K (see Definition A.5.3), E and E' are K-isomorphic.

Determining if two elliptic curves are K-isomorphic might require constructing K-morphisms between them and verifying if one can obtain a K-isomorphism. This section explains how the j-invariant can be used to determine if two curves defined over K are isomorphic when allowing $\overline{K}$-morphisms. The *j-invariant* of an elliptic curve E/K is defined by

$$j(E) = \frac{3c_4}{\Delta}, \tag{1.4}$$

where c_4 is defined in Section 1.3. For $\mathrm{char}(K) \neq 2, 3$ using the above change of variables this simplifies to

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

Proposition 1.5.1 ([19, §3.1])**.** *Two elliptic curves defined over K have the same j-invariant if and only if they are isomorphic over $\overline{K}$.*

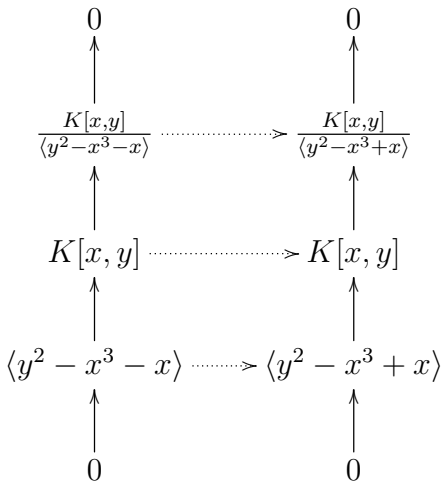
Example 1.5.1. *Consider the two following affine equations of elliptic curves:*

$$E \colon y^2 = x^3 + x \qquad \text{and} \qquad E' \colon y^2 = x^3 - x$$

over K. The j-invariants are

$$j(E) = 1728\frac{4 \cdot 1}{-4 \cdot 1} = -1728 \qquad \text{and} \qquad j(E') = 1728\frac{4 \cdot (-1)}{-4 \cdot (-1)} = -1728.$$

One way of seing that E and E' are isomorphic, is by considering the following diagram:



If we obtain an isomorphism

$$K[x,y] \to K[x,y]$$

such that

$$y^2 - x^3 - x \mapsto y^2 - x^3 + x,$$

then we can use the short five lemma to conclude that both elliptic curves are isomorphic. This map can be obtained if our field contains $i = \sqrt{-1}$*, and we can take:*

$$y \mapsto y$$

$$x \mapsto ix$$

thus giving

$$y^2 - x^3 - x \mapsto (y)^2 + (ix)^3 - ix = -i(i(y)^2 - x^3 + x)$$

and this gives the desired isomorphism if $y \mapsto iy$*. This argument suggests that in order to have a* K*-isomorphism between these two curves we need* $\sqrt{-1} \in K$*. In particular, since* $\sqrt{-1} \in \overline{K}$*, we can conclude that* E *and* E' *are* $\overline{K}$*-isomorphic, thus illustrating the utility of Proposition 1.5.1.*

1.6 Frobenius Endomorphism

This section focuses on elliptic curves defined over $\mathbb{F}_q$, where where $q = p^n$ and n is an integer greater than 1. The goal of this section is to introduce the Frobenius endomorphism.

The Frobenius endomorphism of the affine plane $\mathbb{A}^2_{\mathbb{F}_q}$ is given by

$$\begin{aligned} \mathrm{Frob}_{\mathbb{A}^2} \colon \mathbb{A}^2_{\mathbb{F}_q} &\to \mathbb{A}^2_{\mathbb{F}_q} \\ (x, y) &\mapsto (x^q, y^q), \end{aligned}$$

and the Frobenius endomorphism of the projective plane $\mathbb{P}^2_{\mathbb{F}_q}$ (see Section 1.2) is given by

$$\begin{aligned} \mathrm{Frob}_{\mathbb{P}^2} \colon \mathbb{P}^2_{\mathbb{F}_q} &\to \mathbb{P}^2_{\mathbb{F}_q} \\ [x : y : z] &\mapsto [x^q : y^q : z^q]. \end{aligned}$$

The Frobenius endomorphism Frob_E, also denoted Frob_q, for an elliptic curve $E/\mathbb{F}_q$ is the endomorphism inherited from $\mathrm{Frob}_{\mathbb{P}^2}$, and it allows us to characterize $\mathbb{F}_q$-rational points.

Proposition 1.6.1 ([25, §4.2])**.** *Let E be defined over $\mathbb{F}_q$, and let $P \in E(\overline{\mathbb{F}}_q)$; then $P \in E(\mathbb{F}_q)$ if and only if $\mathrm{Frob}_E(P) = P$.*

Example 1.6.1. *Let α be the generator of $\mathbb{F}_9$ over $\mathbb{F}_3$. Consider $E\colon y^2 = x^3 + x$ over $\mathbb{F}_9$. For $P = (1, \alpha+1) \in E(\mathbb{F}_9)$ the Frobenius endomorphism gives $\mathrm{Frob}_E(1, \alpha+1) = (1^9, (\alpha+1)^9) = (1, \alpha+1)$, thus $\phi_9(P) = P$, but for $Q = (\sqrt{\alpha}, \sqrt{(\sqrt{\alpha})^3 + \sqrt{\alpha}}) \in E(\overline{\mathbb{F}}_9)$, the image of this point by the Frobenius endormorphism is $\phi_9(\sqrt{\alpha}, \sqrt{(\sqrt{\alpha})^3 + \sqrt{\alpha}}) = (2\sqrt{\alpha}, (\alpha+1)\sqrt{(\alpha+1)\sqrt{\alpha}}) \neq Q$, which illustrates Proposition 1.6.1.*

There are many other important features of the Frobenius endomorphism; some of these are explained later when we have defined integer multiplication on a curve in Section 2.3.

Chapter 2

Isogenies

2.1 What Are Isogenies?

In this chapter we introduce the main object of study of this thesis: isogenies. The first section focuses on their definition and characterization. Isogenies are certain K-morphisms (see Definition A.5.3) of elliptic curves.

Definition 2.1.1. *Let E and E' be elliptic curves over K. A K-isogeny $\varphi\colon E \to E'$ is a surjective K-morphism such that $\varphi(\mathcal{O}_E) = \mathcal{O}_{E'}$. This is denoted $E \sim E'$.*

Given elliptic curves over K, $\overline{K}$-morphisms of elliptic curves are either constant or surjective and non-constant $\overline{K}$-morphisms are finite; see [11, Ch II, Prop 6.8] for a proof of these claims. Given the group structure of elliptic curves (see Section 1.4), it follows, that the definition above is equivalent to: a K-morphism of elliptic curves $\varphi\colon E \to E'$ is an isogeny if it is finite and surjective.

A non constant K-isogeny $\varphi\colon E_1 \to E_2$ of elliptic curves over K can be written using rational functions (see Section A.5). Given the affine equations of E_1 and E_2 (see Section 1.3), φ can be written as $\varphi(x, y) = (r_1(x), yr_2(x))$, where $r_1(x), r_2(x)$ are rational functions with coefficients in K, with $r_1(x) = \frac{p(x)}{q(x)}$ and $r_2(x) = \frac{s(x)}{t(x)}$, for $p(x), q(x), s(x), t(x) \in K[x]$ and $\gcd(p(x), q(x)) = 1 = \gcd(s(x), t(x))$.

Definition 2.1.2. *Given φ written as a rational function as above, we define its* degree *by* $\deg(\varphi) = \max\{\deg(p(x)), \deg(q(x))\}$.

Note that since $r_2(x)$ is determined by $r_1(x)$ and the Weierstrass equation of the elliptic curves, only $r_1(x)$ is considered when defining the degree of an isogeny.

It follows from composition of polynomials, that $\varphi \mapsto \deg(\varphi)$ is multiplicative,

$$\deg(\varphi \circ \psi) = \deg(\varphi) \cdot \deg(\psi).$$

Given a surjective K-morphism of elliptic curves $\varphi\colon E \to E'$, this morphism can be carried to the affine part of these curves giving $\varphi\colon E_{\text{aff}} \to {E_{\text{aff}}}'$. φ induces an injection of function fields fixing K (see Section 1.3 for how to compute the function field of an elliptic curve):

$$\varphi^*\colon K(E') \to K(E)$$
$$\varphi^* f = f \circ \varphi.$$

Morphisms of functions fields are field homomorphisms. For more details on what is presented in this section see [11, I§6 and II§6.8].

Proposition 2.1.1 ([19, II§2])**.** *Let E_1 and E_2 be elliptic curves over K.*

1. *Let $\varphi\colon E_1 \to E_2$ be a surjective K-morphism. Then $K(E_1)$ is a finite extension of $\varphi^* K(E_2)$.*
2. *Let $\iota\colon K(E_2) \to K(E_1)$ be an injection of function fields fixing K. Then there exist a unique surjective K-morphism $\varphi\colon E_1 \to E_2$ such that $\varphi^* = \iota$.*

The above gives us an anti equivalence between the category of elliptic curves and the category of function fields of elliptic curves, which is obtained by:

$$E \rightsquigarrow K(E)$$
$$\varphi\colon E_1 \to E_2 \rightsquigarrow \varphi^*\colon K(E_2) \to K(E_1).$$

The definition above gives an alternate definition of the degree of an isogeny:

$$\deg \varphi = [\overline{K}(E_1) : \varphi^* \overline{K}(E_2)];$$

see [19, §3.4] for more details.

Definition 2.1.3. *An isogeny $\varphi\colon E_1 \to E_2$, φ is separable if the corresponding field extension $\overline{K}(E_1)/\varphi^*\overline{K}(E_2)$ is separable.*

In the case $\mathrm{char}(K) = p$, if $\overline{K}(E_1)/\varphi^*\overline{K}(E_2)$ is a purely inseparable extension, then φ is a *purely inseparable isogeny.* Recall that a purely inseparable field extension L/K is when for all $\beta \in L$, the minimal polynomial of β is of the form $x^{p^n} - \alpha$, where $n \in \mathbb{N}$ and $\alpha \in K$.

Proposition 2.1.2 ([25, §2.9])**.** *For an elliptic curve E over K and a separable isogeny $\varphi\colon E(\overline{K}) \to E(\overline{K})$, $\deg \alpha = \#\ker(\alpha)$.*

Using the group structure, multiplication by $m \in \mathbb{Z}$ with $m \neq 0$ gives a very important isogeny of elliptic curves. For any elliptic curve E:

$$[m]\colon E \to E \qquad \text{is defined by} \qquad P \mapsto P + P + \cdots + P \quad m\text{-times.} \tag{2.1}$$

This is a non-constant isogeny of degree m^2, and this is a separable isogeny for $m \neq 0$, a proof of these claims can be found in [19, III§4].

Example 2.1.1. *Given the affine equation; $E\colon y^2 = x^3 + 1$ over $\mathbb{F}_5$, the multiplication by 3 map, $[3] : E \to E$ can be represented by the following rational functions:*

$$(x, y) \mapsto \left(\frac{x^9 - x^6 - 2x^3 - 1}{-x^8 + 2x^5 - x^2}, y\frac{-2x^{12} + 2x^6 - 1}{x^{12} + 2x^9 - 2x^6 - x^3} \right).$$

This is an isogeny of degree 9 by Definition 2.1.2. As we did above, Sage can be used to find the rational functions describing $[m] : E \to E$ for elliptic curves defined over number fields and for larger m; generally the resulting functions have very large defining polynomials. When denoting these polynomial $p(x), q(x), s(x), t(x)$, as earlier in this section, remark that one of $p(x)$ or $q(x)$ has degree m^2.

Proposition 2.1.3 ([19, §3.4])**.** *For every isogeny $\varphi\colon E_1 \to E_2$ of degree n there exists a unique isogeny $\hat{\varphi}\colon E_2 \to E_1$ such that $\varphi \circ \hat{\varphi} = [n]$ and $\hat{\varphi} \circ \varphi = [n]$.*

The isogeny $\hat{\varphi}\colon E_2 \to E_1$ for elliptic curves over K, determined by $\varphi\colon E_1 \to E_2$ is called the *dual isogeny* of φ. Note that with the dual isogeny of $\varphi\colon E_1 \to E_2$, comes an injection of function fields $\hat{\varphi}^*\colon K(E_1) \to K(E_2)$, given the equivalence with function fields mentioned earlier in Proposition 2.1.1.

Example 2.1.2. *Consider the degree-2 isogeny $\varphi\colon E_1 \to E_2$ with*

$$E_1\colon y^2 = x^3 - x \qquad \text{and} \qquad E_2\colon y^2 = x^3 + 4x$$

over $\mathbb{Q}$, given by the following rational functions:

$$\varphi : (x, y) \mapsto \left(\frac{x^2 - 1}{x}, \frac{x^2 y + y}{x^2}\right).$$

The dual isogeny, $\hat{\varphi} : E_2 \to E_1$, which is also a degree-2 isogeny, is given by the rational functions:

$$(x, y) \mapsto \left(\frac{x^2 + 4}{4x}, \frac{x^2 y - 4y}{8x^2}\right).$$

The composition of these two isogenies is the isogeny of degree 4 given by

$$[2] : (x, y) \mapsto \left(\frac{x^4 + 2x^2 + 1}{4x^3 - 4x}, \frac{8x^6 y - 40x^4 y - 40x^2 y + 8y}{64x^6 - 128x^4 + 64x^2}\right).$$

Remark 2.1.1. *For the isogeny $[2]$, which given P a point on an elliptic curve E, produces $[2]P = P + P$, the rational functions of $[2](x, y) = (r_1(x), y r_2(x)) = \left(\frac{p_1(x)}{q_1(x)}, y r_2(x)\right)$, with $\deg(p_1(x)) = 4$ and $\deg(p_2(x)) = 3$. Since multiplication by m is a succession of additions, for $[m](x, y) = \left(\frac{p(x)}{q(x)}, y r(x)\right)$, one always obtains $|\deg(p(x)) - \deg(q(x))| = 1$.*

2.2 Torsion Points and Tate Module

In this section we define torsion points of an elliptic curve E defined over K and the Tate module of E in Definition 2.3. The Tate module is important since it carries an action of the Galois group $\mathrm{Gal}(\overline{K}/K)$.

Let E be an elliptic curve defined over K and m a non-zero integer. The *subgroup of m-torsion points* $E[m]$ is defined by

$$E[m] := \{P \in E(\overline{K}) \mid [m]P = 0\}.$$

The *torsion subgroup* of E, denoted E_{tors}, is the set of points of finite order:

$$E_{\text{tors}} := \bigcup_{m=1}^{\infty} E[m]. \tag{2.2}$$

Proposition 2.2.1 ([19, §III.6])**.** *If E is an elliptic curve over K, and ℓ is a prime such that $\ell \nmid \operatorname{char}(K)$ then*

$$E[\ell^n] \cong \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z}$$

for every positive integer n.

Proof. Since $[\ell]$ is a separable isogeny of degree ℓ^2, combing this fact to Proposition 2.1.2 gives that $\#\ker([\ell]) = \ell^2$. By definition of $E[\ell]$, if $P \in \ker([\ell])$, then $P \in E[\ell]$, and the converse is also true. Therefore $\#\ker([\ell]) = \#E[\ell]$ and $E[\ell]$ has order ℓ^2. $E[\ell]$ is a subgroup of points of order dividing ℓ. Since $[\ell]$ is represented by a rational function $r(x)$ of degree ℓ^2 and torsion points are solutions over $\overline{K}$, $r(x)$ has ℓ^2 solutions, where only one of these is of order 1, $\mathcal{O}_E$, and the others are of order ℓ. Since $E[\ell]$ has a point of order ℓ, by the structure theorem of finitely generated abelian groups (see [4, §5.2]), $E[\ell]$ can either be $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ or $\mathbb{Z}/\ell^2\mathbb{Z}$, but $E[\ell]$ has no point of order ℓ^2, this it has to be isomorphic to the first one. Since $\#E[\ell] < \#E[\ell^2]$, one obtains a point of order ℓ^2 in $E[\ell^2]$, and using the same argument as in the proof above, $E[\ell^2] \cong \mathbb{Z}/\ell^2\mathbb{Z} \times \mathbb{Z}/\ell^2\mathbb{Z}$. Induction on n gives the generalization $E[\ell^n] \cong \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z}$. □

Proposition 2.2.2 ([19, §III.6])**.** *If E is an elliptic curve over K and* $\operatorname{char}K = p$ *then for all $e = 1, 2, 3, \ldots$ either*

1. *$E[p^e] \cong \{0\}$, or*
2. *$E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z}$.*

For every elliptic curve E/K and prime ℓ, the groups $E[\ell^n]$, as n ranges over positive integers, come equipped with group homomorphisms

$$[\ell^{m-n}] : E[\ell^m] \to E[\ell^n], \qquad m > n.$$

This allows us to form the *ℓ-adic Tate module* $T_\ell(E)$ of an elliptic curve E/K:

$$T_\ell(E) := \varprojlim_{n\in\mathbb{N}} E[\ell^n]. \tag{2.3}$$

Note that the Tate module sees torsion points of E over $\overline{K}$. By Proposition 2.2.1, if ℓ is coprime to $\mathrm{char}(K)$ then each $E[\ell^n]$ has a $\mathbb{Z}/\ell^n\mathbb{Z}$ module structure, and taking the inverse limit of these gives $T_\ell(E)$ a $\mathbb{Z}_\ell$-module structure.

Proposition 2.2.3 ([19, §3.7])**.** *$T_\ell(E)$ has a $\mathbb{Z}_\ell$-module structure, more specifically:*

1. *If ℓ is prime to $\mathrm{char}(K)$ then $T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$, where $\mathbb{Z}_\ell := \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/\ell^n\mathbb{Z}$.*
2. *If $\ell = \mathrm{char}(K)$ then $T_\ell(E) \cong \{0\}$ or $\mathbb{Z}_\ell$.*

Let X be a topological space and π a topological group, a group action of π on X is continuous if the map: $\pi \times X \to X$ is continuous.

Proposition 2.2.4 ([19, §3.7])**.** *Given an elliptic curve E over $\mathbb{Q}$, the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts continuously on $T_\ell(E)$.*

Proof. To see this, first one needs to define the topology on both these pro-finite spaces. $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = \varprojlim_{L} \mathrm{Gal}(L/\mathbb{Q})$, where the limit is taken over finite extensions L of $\mathbb{Q}$. The points in this space are in some $\mathrm{Gal}(L/\mathbb{Q})$ for a finite extensions L. The open sets come from the extensions such that $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(L/\mathbb{Q})$ is continuous. Similarly, the profinite topology on $T_\ell(E)$ makes the maps $T_\ell(E) \to E[\ell^n]$ continuous, for every positive integer n. For $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, consider the restriction $\sigma|_L = \sigma_L$, where L is the finite extension of $\mathbb{Q}$ such that $E(L)[\ell^n] = E[\ell^n]$ to obtain the following continuous action:

$$\begin{aligned} \mathrm{Gal}(L/\mathbb{Q}) \times E(L)[\ell^n] &\to E(L)[\ell^n] \\ (\sigma_L, P) &\mapsto \sigma_L(P). \end{aligned}$$

(Here we write $E(L)[\ell^n]$ for $\{P \in E(L) \mid [\ell^n]P = \mathcal{O}_E\}$.) This actions is continuous since the extension $L/\mathbb{Q}$ is finite, and finite unions and intersections of finite extensions are also finite. For $n < m$, one can obtain the following commutative diagram using projection maps:

$$\begin{array}{ccccc} \mathrm{Gal}(L_n/\mathbb{Q}) & \times & E(L_n)[\ell^n] & \longrightarrow & E(L_n)[\ell^n] \\ \downarrow & & \downarrow & & \downarrow \\ \mathrm{Gal}(L_m/\mathbb{Q}) & \times & E(L_m)[\ell^m] & \longrightarrow & E(L_m)[\ell^m]. \end{array}$$

Given the construction of inverse limits, one can obtain the commutative diagram:

$$\begin{array}{ccccc} \mathrm{Gal}(L_n/\mathbb{Q}) & \times & E(L_n)[\ell^n] & \longrightarrow & E(L_n)[\ell^n] \\ \downarrow & & \downarrow & & \downarrow \\ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) & \times & T_\ell(E) & \longrightarrow & T_\ell(E) \end{array}$$

for all $n \in \mathbb{N}$. Since the actions is continuous at each level and the topology of both pro-finite spaces was defined using continuous maps, this gives a continuous action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $T_\ell(E)$. □

2.3 Trace of Frobenius

Now we are ready to investigate more about the Frobenius endomorphism that was introduced in Chapter 1. In particular, we show in this section that the integer called trace of Frobenius allows to detect if E_1, E_2 defined over $\mathbb{F}_p$ are isogenous. The first propositions are there to help us determine which isogenies are separable or not and to then use the result from Proposition 2.1.2. For the remainder of this chapter, $q = p^n$ where p is a prime and $n \in \mathbb{N}$.

Proposition 2.3.1 ([19, §2.3])**.** *The Frobenius endomorphism is a non separable isogeny of degree q.*

Proposition 2.3.2 ([25, §2.9])**.** *Given an elliptic curve E defined over $\mathbb{F}_q$ and $r, s \in \mathbb{Z}$, $s \neq 0$, the endomrphism $r\mathrm{Frob}_q + s$ is separable if and only if $p \nmid s$.*

Let us now define the trace of Frobenius that links the Tate module to the Frobenius endomorphism. Since the Frobenius endomorphism of an elliptic curve $\mathrm{Frob}_E\colon E \to E$ is an isogeny (recall Proposition 2.3.1), this gives a map on the torsion subgroups $\mathrm{Frob}_q\colon E[\ell^n] \to E[\ell^n]$. Given the inverse limit structure of $T_\ell(E)$, the previous map induces a $\mathbb{Z}_\ell$-linear map, $\mathrm{Frob}_\ell\colon T_\ell(E) \to T_\ell(E)$. The set of $\overline{\mathbb{F}}_q$-morphism $E \to E$, is denoted $\mathrm{End}_{\overline{\mathbb{F}}_q}(E)$, and for the Tate modules one can obtain $\mathrm{End}_{\overline{\mathbb{F}}_q}(T_\ell(E))$. From the previous $\mathbb{Z}_\ell$-linear map, one can obtain a homomorphism,

$$\mathrm{End}_{\overline{\mathbb{F}}_q}(E) \to \mathrm{End}_{\overline{\mathbb{F}}_q}(T_\ell(E))$$
$$\psi \mapsto \psi_\ell,$$

and by Proposition 2.2.3, $T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ when $\ell \neq p$. See [19, 3§7] for more details. By choosing a $\mathbb{Z}_\ell$-basis for $T_\ell(E)$, ψ_ℓ can be written as a 2×2 matrix with coefficients in $\mathbb{Z}_\ell$.

Proposition 2.3.3 ([19, §2.3])**.** *Let* $\psi \in \mathrm{End}_{\overline{\mathbb{F}}_q}(E)$. *Then* $\det(\psi_\ell) = \deg(\psi)$ *and* $tr(\psi_\ell) = 1 + \deg(\psi) - \deg(1 - \psi)$.

(The proof is not tedious but requires an introduction to pairings so it was omitted from this thesis.)

Using Proposition 2.3.2 (setting $r = -1$ and $s = 1$), and Proposition 2.1.2 we obtain $\#\ker(1 - \mathrm{Frob}_E) = \deg(1 - \mathrm{Frob}_E)$. From Proposition 1.6.1, $P \in E(\mathbb{F}_q)$ if and only if $\mathrm{Frob}_E(P) = P = 1(P)$, hence if and only if $P \in \ker(1 - \mathrm{Frob}_E)$. One obtains that $\ker(1 - \mathrm{Frob}_E) = E(\mathbb{F}_q)$, hence $\#E(\mathbb{F}_q) = \#\ker(1 - \mathrm{Frob}_E) = \deg(1 - \mathrm{Frob}_E)$. From the above proposition, the characteristic polynomial of Frob_ℓ, which is the matrix corresponding to Frob_E, has coefficients in $\mathbb{Z}$. Thus, one can factor this characteristic polynomial over $\mathbb{C}$ and obtain

$$\det(T - \mathrm{Frob}_\ell) = T^2 - tr(\mathrm{Frob}_\ell)T + \det(\mathrm{Frob}_\ell) = (T - \alpha)(T - \beta).$$

Therefore, $\det(T - \mathrm{Frob}_\ell)$ has a complex conjugate or a double root, and $|\alpha| = |\beta|$. From $q = \det \mathrm{Frob}_\ell = \deg \mathrm{Frob}_E = \alpha\beta$, one can obtain $|\alpha| = |\beta| = \sqrt{q}$. By taking $T = 1$ and

applying $1 - \text{Frob}_E$ to Proposition 2.3.3, one can obtain that the number of points on E satisfies

$$\#E(\mathbb{F}_q) = \deg(1 - \text{Frob}_E) = \det(1 - \text{Frob}_\ell) = 1 - (\alpha + \beta) + q,$$
$$tr(\text{Frob}_\ell) = 1 - \deg(\text{Frob}_E) - \deg(1 - \text{Frob}_E) = \alpha + \beta,$$

$tr(\text{Frob}_\ell)$ is an integer, that does not depend on ℓ and can be used to find the number of points of an elliptic curve E defined over $\mathbb{F}_q$.

Definition 2.3.1. *Given E defined over $\mathbb{F}_q$, $tr(\text{Frob}_\ell)$ corresponding to the Frobenius endomorphism, is called the trace of Frobenius and is denoted by $a_p(E)$.*

Example 2.3.1. *Given the affine equation $E\colon y^2 = x^3 + 1$ defined over $\mathbb{F}_5$. The Frobenius endomorphism acts on the affine points of E in the following way $\text{Frob}_5(x, y) = (x^5, y^5)$. The matrix associated to Frob_5 is $\left[\begin{smallmatrix} 0 & 1 \\ -5 & 0 \end{smallmatrix}\right]$,this matrix has trace 0, therefore $a_5(E) = 0$. This matrix was obtained using Sage, which finds the trace of Frobenius of a curve by computing the number of points on the elliptic curve using Schoof, Elkies, Atkin's [15] method and then determines more about the Frobenius endomorphism. Given this matrix of Frobenius one can see that $\det(1 - Frob_\ell) = \det\left(\left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right] - \left[\begin{smallmatrix} 0 & 1 \\ -5 & 0 \end{smallmatrix}\right]\right) = \det\left(\left[\begin{smallmatrix} 1 & -1 \\ 5 & 1 \end{smallmatrix}\right]\right) = 6 = \#E(\mathbb{F}_5)$, and by listing all the solution over $\mathbb{F}_5$ to the above equation one actually obtains six of them.*

Definition 2.3.2. *The curve E is called* supersingular *if $a_p(E) \equiv 0 \pmod{p}$.*

E supersingular is equivalent to saying that $E[p] \cong \{0\}$ recalling Propostion 2.2.2, for a proof see [19, V§3]. In the case that $E[p] \cong \mathbb{Z}/p\mathbb{Z}$ then we say that E is *ordinary*.

Example 2.3.2. *The curve E from Example 2.3.1 has $a_5(E) = 0$, thus is a supersingular curve. Note that it's only $[5]$-torsion point is $\mathcal{O}_E$, hence $E[5] \cong \{0\}$, agreeing with the above.*

The following result allows us to detect when two curves are $\mathbb{F}_q$-isogenous.

Proposition 2.3.4 ([23, §3 Theorem 1])**.** *Let E_1, E_2 be elliptic curves over $\overline{\mathbb{F}}_q$ and $\rho_{E_1}(\text{Frob}_{E_1})$, $\rho_{E_2}(\text{Frob}_{E_2})$ be the characteristic polynomials of their Frobenius over $\mathbb{F}_q$, then the following are equivalent:*

1. $E_1,\ E_2$ *are* $\mathbb{F}_q$*-isogenous.*

2. $\rho_{E_1}(\mathrm{Frob}_{E_1}) = \rho_{E_2}(\mathrm{Frob}_{E_2})$*, i.e. they have the same trace of Frobenius.*

Chapter 3

From Global to Local and Vice Versa

3.1 Isogenies Over $\mathbb{Q}$

In Chapter 2, we saw a way to detect when two curves over a finite field are isogenous. This section shows how to use the techniques we have developed over finite fields to verify if two curves over $\mathbb{Q}$ are $\mathbb{Q}$-isogenous. The result is needed to prove the main result of this thesis, in Chapter 6.

Since we do not want to eliminate characteristic 2 and 3 fields, we return to elliptic curves E in general Weierstrass form. In fact, we now turn our attention to the affine Weierstrass equation

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with $a_1, \ldots a_6 \in \mathbb{Z}$; this is called an *integral Weierstrass equation.* Given any elliptic curve defined over $\mathbb{Q}$, it is always possible to obtain an integral Weierstrass equation using a proper change of variables. The change of variables

$$x \mapsto u^2x$$

$$y \mapsto u^3y$$

gives an elliptic curve where the coefficients $a_i \mapsto a_iu^i$ and it is possible to find a suitable u that will make this equation integral. Elliptic curves that are equal modulo a change of variables are equivalent. More details about this process can be found in [3, Chapter 8 §3].

Example 3.1.1. *Given the elliptic curve* $E\colon y^2 = x^3 + \frac{1}{5}x^2 + \frac{1}{3}x + 1$ *over* $\mathbb{Q}$*, using the change*

of variables

$$x \mapsto \frac{x}{15^2}$$
$$y \mapsto \frac{y}{15^3}$$

then one obtains $\frac{y^2}{15^6} = \frac{x^3}{15^6} + \frac{1}{5} \cdot \frac{x^2}{15^4} + \frac{1}{3} \cdot \frac{x}{15^2} + 1$*, multiplying the equation by* 15^6 *gives* $y^2 = x^3 + 45x^2 + 5 \cdot 15^3 x + 15^6$*, which is an integral Weierstrass equation.*

Given an integral Weierstrass equation over $\mathbb{Q}$, we define the *reduction* of our curve over $\mathbb{F}_p$ by E_p:

$$E_p \colon y^2 + \overline{a}_1 xy + \overline{a}_3 y = x^3 + \overline{a}_2 x^2 + \overline{a}_4 x + \overline{a}_6$$

with $\overline{a}_1, \dots \overline{a}_6 \in \mathbb{F}_p$ and $\overline{a}_i = a_i \pmod{p}$. This reduction might not give an elliptic curve, which can be checked by looking at the discriminant of E and of E_p, the discriminant of E_p is 0 when p divides the discriminant of E.

For $r \in \mathbb{Q}$, let $\nu_p(r)$ be the power of p appearing in r, which is the p-adic valuation, where $\nu_p(0) = +\infty$. Given an elliptic curve E over $\mathbb{Q}$, $\nu_p(E)$ denotes the smallest power of p appearing in the discriminant of any equivalent integral Weierstrass equation, that is:

$$\nu_p(E) = \min\{\nu_p(\Delta(E')) \mid E' \text{ integral equivalent to } E\}.$$

The global minimal discriminant of E is defined by:

$$\Delta_{\min}(E) = \prod_{p \text{ prime}} p^{\nu_p(E)}.$$

This is a finite product since $\nu_p(E) = 0$ for all $p \nmid \Delta(E)$.

Through a proper change of variable, the p-adic valuation of the discriminant can be minimized to $\nu_p(E)$ simultaneously for all p, more details about this procedure can be found in [19, §7.2]. From the above an elliptic curve E is $\mathbb{Q}$-isomorphic to an integral equation E' with discriminant $\Delta(E') = \Delta_{\min}(E)$. The equation of E' is defined to be a *minimal Weierstrass equation* of E.

For any elliptic curve E in minimal Weierstrass form, if $p \mid \Delta$, then E has bad reduction. When looking at the possible values that the dirscriminant of an integral Weierstrass equation can take, one obtains that $\Delta \neq \pm 1$, thus there is no elliptic curve over $\mathbb{Q}$ that has good reduction for all primes.

Given E, a Weierstrass equation of an elliptic curve over K, singular curves can be classified and one can figure out the type of singular points the curve has. E has

(a) a *cusp* if $\Delta = 0$ and $c_4 = 0$ (recall Section 1.3),

(b) a *node* if $\Delta = 0$ and $c_4 \neq 0$.

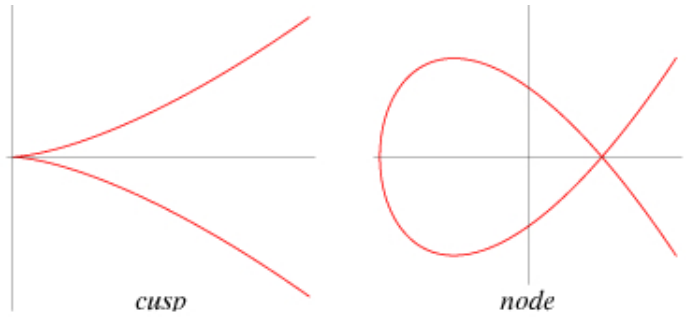


Figure 3.1: Types of Singular Points

Definition 3.1.1. *A minimal Weierestrass equation has:*

(a) good reduction *at p if E_p is smooth, in this case E_p has non zero discriminant;*

(b) multiplicative reduction *at p if E_p has a node;*

(c) additive reduction *at p if E_p has a cusp.*

For the two last cases E is said to have bad reduction at p.

Remark 3.1.1. *The names additive and multiplicative reduction can be explained by looking at the non-singular part of the reduction of E at p, denoted $(E_p)_{ns}$. In the case of E having multiplicative reduction $(E_p)_{ns}(\overline{\mathbb{F}}_p) \cong \overline{\mathbb{F}}_p^*$, a multiplicative group and in the case of E having additive reduction $(E_p)_{ns}(\overline{\mathbb{F}}_p) \cong \overline{\mathbb{F}}_p^+$, an additive group. A proof of these claims can be found in [19, VII§5].*

Recalling Propositon 2.2.4, the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts continuously on the Tate module of E. For a prime p there is a surjective map $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ the kernel of this map is called the *inertia group* of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ at p and is denoted I_p. More details about this can be found in [9, §7].

Definition 3.1.2. *Given a prime p, such that $p \neq \ell$, the ℓ-adic Tate module of an elliptic curve E over $\mathbb{Q}$ is* unramified *at p if the action of I_p on $T_\ell(E)$ is trivial.*

Proposition 3.1.1 ([19, VII§7])**.** *Let E be an elliptic curve over $\mathbb{Q}$. The ℓ-adic Tate module $T_\ell(E)$ is unramified at p if p is a prime of good reduction for E and $p \neq \ell$.*

Elliptic curves over $\mathbb{Q}$ can also be compared by looking at their L-series, which contain a large amount of information concerning the reduction of the curves. For an elliptic curve E over $\mathbb{Q}$ and a prime $p \nmid \ell$ an L factor is defined in the following way

$$L_p(s, E) := (1 - a_p(E)p^{-s} + p \cdot p^{-2s})^{-1},$$

the L-series of E is

$$L(s, E) := \prod_{p \text{ prime}} L_p(s, E).$$

A good reference for L-series is [20, II, §10].

Attached to the L-series of a curve is the notion of conductor of a curve that is introduced next. Similar to the discriminant, the conductor is an integer that measures the arithmetic of E defined over $\mathbb{Q}$. When two curves are $\mathbb{Q}$-isogenous, they have the same conductor. This is part of what is used in practice by computational algebra software such as Sage to verify if two curves are $\mathbb{Q}$-isogenous. For a more detailed description of the properties of the conductor, one can look at [20, IIV, §10].

Before defining the conductor, the *exponent of the conductor* f_p for E at p needs to be

introduced:

$$f_p = \begin{cases} 0 & \text{if E has good reduction at } p \\ 1 & \text{if E has multiplicative reduction at } p \\ 2 & \text{if E has additive reduction at } p \text{ and } p \notin \{2,3\} \\ 8 & \text{if E has additive reduction at } p \text{ and } p = 2 \\ 5 & \text{if E has additive reduction at } p \text{ and } p = 3. \end{cases}$$

Definition 3.1.3. *N_E the conductor of E over $\mathbb{Q}$ is following integer:*

$$N_E = \prod_{p \text{ prime}} p^{f_p}.$$

We remark that N_E and $\Delta_{\min}(E)$ have the same primes in their decomposition.

3.2 Faltings' Result

Proposition 3.2.1 ([8, Chapter II])**.** *E and E' are $\mathbb{Q}$-isogenous if and only if for all primes p where E, E' have good reduction, E_p is $\mathbb{F}_p$-isogenous to E'_p.*

The above was obtained in 1983, by Faltings, in the context of his proof of Tate's conjecture, which is a more general result that requires more algebraic geometry knowledge in order to be understood. A english version of Falting's proof can be found in [8]; more details about the general result are in the notes from this number theory seminar [13]. This result is important for Theorem 6.0.1 since it allows is to determine if two elliptic curves are $\mathbb{Q}$-isogenous using methods defined in the previous chapters.

Example 3.2.1. *Let $E_1 \colon y^2 = x^3 + x$ and $E_2 \colon y^2 = x^3 + x + 2$, over $\mathbb{F}_3$, $a_3(E_1) = 0 = a_3(E_2)$, thus E_1 and E_2 are $\mathbb{F}_3$-isogenous. Similarly, over $\mathbb{F}_5$, $a_5(E_1) = 2 = a_5(E_2)$, thus E_1 and E_2 are $\mathbb{F}_5$-isogenous. But E_1 and E_2 are not $\mathbb{Q}$-isogenous, they are not $\mathbb{F}_{11}$-isogenous, this can be seen through $a_{11}(E_1) = 0$ and $a_{11}(E_2) = -4$, illustrating Proposition 3.2.1. The conductors also indicate this, since they have different prime factors, the conductor of E_1 is 2^4 and the conductor of E_2 is $7 \cdot 8$.*

Chapter 4

Quadratic Twists

4.1 What are Quadratic Twists?

The main result of this thesis, given in Chapter 6, concerns when elliptic curves are $\mathbb{Q}$-isogenous to their quadratic twist. The objective of this chapter is to define quadratic twists and how to determine the quadratic twist of an elliptic curve.

Definition 4.1.1. *A* twist *of an elliptic curve E over a field K is an elliptic curve E' over K which is $\overline{K}$-isomorphic to E.*

Note that Proposition 1.5.1 implies that an elliptic curve and its twist have the same j-invariant (see Section 1.5).

Instead of working in the algebraic closure of K, we restrict ourselves to the quadratic extension $K(\sqrt{d})$, for a square free integer d. Note that for the main theorem in Chapter 6 only negative square free integers will be considered. Similar to Definition 4.1.1, given an elliptic curve E over $\mathbb{Q}$, a *quadratic twist* is defined to be a curve E^d over $\mathbb{Q}$ such that E is $\mathbb{Q}(\sqrt{d})$-isomorphic to E^d.

Let K be a field with $\text{char}(K) \neq 2$, then one can look at a simpler Weierstrass equation than the one from Section 1.3. Let

$$E: \quad y^2 = x^3 + a_2x^2 + a_4x + a_6$$

be an elliptic curve over K. For each $d \in K\backslash K^2$ and $d \neq 0$, let E^d be the elliptic curve defined by

$$E^d: \quad dy^2 = x^3 + a_2x^2 + a_4x + a_6.$$

More details on how to find twists in greater generality can be found in [19][X §2 and 5].

Example 4.1.1. *Here are some examples of curves over $\mathbb{Q}$ such that $E \sim E^d$. We will see later that these curves also admit complex multiplication by the ring of integers in the quadratic extension $\mathbb{Q}(\sqrt{d})$ (see Definition 5.1.1):*

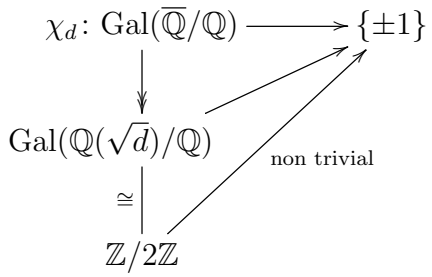
$$\mathbb{Z} \subsetneq \mathrm{End}_{\overline{\mathbb{Q}}}(E) \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}.$$

These are all examples of curves satisfying Theorem 6.0.1 and Theorem 6.0.2. The elliptic curves below were obtained using Sage, using an algorithm that, given an elliptic curve E over $\mathbb{Q}$ and d, returns the minimal integral Weierstrass equation of quadratic twist E^d (recall Section 3.1). Sage was also used to verify that E has complex multiplication by $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$.

Extension	*Curve*	*$\mathbb{Q}$-isogenous Twist*
$\mathbb{Q}(\sqrt{-1})$	$y^2 = x^3 + x$	$y^2 = x^3 + x$
$\mathbb{Q}(\sqrt{-2})$	$y^2 = x^3 + 4x^2 + 2x$	$y^2 = x^3 + x^2 - 13x - 21$
$\mathbb{Q}(\sqrt{-3})$	$y^2 + y = x^3$	$y^2 + y = x^3 - 7$
$\mathbb{Q}(\sqrt{-7})$	$y^2 + xy = x^3 - x^2 - 2x - 1$	$y^2 + xy = x^3 - x^2 - 107x + 552$
$\mathbb{Q}(\sqrt{-7})$	$y^2 = x^3 - 35x - 98$	$y^2 = x^3 - 1715x - 33614$
$\mathbb{Q}(\sqrt{-11})$	$y^2 + y = x^3 - x^2 - 7x + 10$	$y^2 + y = x^3 - x^2 - 887x - 10143$
$\mathbb{Q}(\sqrt{-19})$	$y^2 + y = x^3 - 38x + 90$	$y^2 + y = x^3 - 13718x - 619025$
$\mathbb{Q}(\sqrt{-43})$	$y^2 + y = x^3 - 860x + 9707$	$y^2 + y = x^3 - 1590140x - 771794326$
$\mathbb{Q}(\sqrt{-67})$	$y^2 + y = x^3 - 7370x + 243528$	$y^2 + y = x^3 - 33083930x - 73244287055$
$\mathbb{Q}(\sqrt{-163})$	$y^2 + y = x^3 - 2174420x + 1234136692$	$y^2 + y = x^3 - 57772164980x - 5344733777551611$

4.2 Quadratic Character

Consider the quadratic character $\chi_d : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \{\pm 1\}$, where d is a square free integer, defined below.



Thus $\chi_d\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \{\pm 1\}$ and is actually given by $\chi_d(\sigma) = (\sqrt{d})^\sigma/\sqrt{d}$. If $p \nmid d$, then $\chi_d(\mathrm{Frob}_p)$ is equal to $\left(\frac{d}{p}\right)$, the Legendre symbol.

4.3 Tate module of a twist

Proposition 4.3.1 ([19, X§2])**.** *For a prime $\ell \neq p$, the ℓ-Tate module of E^d is unramified (recall Definition 3.1.2) at p. If p is a prime of good reduction for $E/\mathbb{Q}$, and p is prime to d then for such p,*

$$\rho_{E^d,\ell}(\mathrm{Frob}_p) = \chi_d(\mathrm{Frob}_p)\rho_{E,\ell}(\mathrm{Frob}_p).$$

Remark 4.3.1. *Instead of looking at the character acting on the characterstic polynomials, one can distribute the character to every term of the characterstic polynomials and look only at the traces of Frobenius and obtain $a_p(E^d) = \chi_d(\mathrm{Frob}_p)a_p(E)$.*

Chapter 5

Complex Multiplication

The goal of this chapter is to describe the interesting phenomenon known as complex multiplication. The main result of this thesis links complex multiplication for elliptic curves to the property of having a $\mathbb{Q}$-isogenous quadratic twist, as defined in Chapter 4.

5.1 What is Complex Multiplication?

Integer multiplication on an elliptic curve was introduced in Section 2.1. Complex multiplication identifies when an elliptic curve E has more endomorphisms than multiplication by integers.

Recall that an *imaginary quadratic field* is a field extension of the form

$$K = \mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D} \mid a, b \in \mathbb{Q}\},$$

where D is a square-free negative integer. The ring of integers of this field $\mathcal{O}_K$ is the set of α with minimal polynomials in $\mathbb{Z}[x]$. These elements are called integral elements. This ring actually takes the form:

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\frac{1+\sqrt{D}}{2}], & \text{if } D \equiv 1 \pmod 4 \\ \mathbb{Z}[\sqrt{D}], & \text{if } D \equiv 2, 3 \pmod 4. \end{cases}$$

An *order in a quadratic imaginary field* is a subring $R \subseteq \mathcal{O}_K$ such that $R \otimes_{\mathbb{Z}} \mathbb{Q} = K$. Note that in this case $R \ncong \mathbb{Z}$.

Example 5.1.1. *For $K = \mathbb{Q}(\sqrt{-3})$ and as indicated above $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$. Then $\mathcal{O}_K$ is an order in K, as is the proper subring*

$$\mathbb{Z} + 2\mathbb{Z}[\sqrt{-3}] = \{a + 2b\sqrt{-3} \mid a, b \in \mathbb{Z}\}.$$

Given $a, b \in \mathbb{Q}^\times$, a *quaternion algebra* is the $\mathbb{Q}$-algebra of dimension 4, denoted $\mathcal{Q}$, with basis $1, i, j, k$, such that $i^2 = a$, $j^2 = b$ and $ij = -ji = k$. As for quadratic imaginary fields, one can define orders in a quaternion algebra, but first one needs to define what are the integral elements in the algebra. Using the $\mathbb{Q}$-linear automorphism

$$x = (1, i, j, k) \mapsto \hat{x} = (1, -i, -j, -k),$$

the trace of $x \in \mathcal{Q}$ is $T(x) = x + \hat{x}$ and the norm of x is $N(x) = x\hat{x}$. Note that both $T(x)$ and $N(x)$ lie in $\mathbb{Q}$. Given a quaternion algebra $\mathcal{Q}$, $x \in \mathcal{Q}$ is integral if $T(x)$ and $N(x)$ actually lie in $\mathbb{Z}$. An order in $\mathcal{Q}$ is a subring $\mathcal{O}_\mathcal{Q} \subset \mathcal{Q}$ such that $\mathcal{O}_\mathcal{Q} \otimes_\mathbb{Z} \mathbb{Q} = \mathcal{Q}$. Note that all elements of $\mathcal{O}_\mathcal{Q}$ are integral. For more information see Chenevier [1].

In both the case of imaginary quadratic fields and quaternion algebras, an order that is not properly contained in any other order is called a *maximal* order.

Example 5.1.2. *One of the most famous examples of quaternion algebras are the Hamiltonian quaternions, denoted* $\mathbb{H}$*:*

$$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R},\ i^2 = j^2 = k^2 = ijk = -1\}.$$

A subalgebra of these is the Hurwitz quaternions, denoted $\mathcal{H}$*:*

$$\mathcal{H} = \{a + bi + cj + dk \in \mathbb{H} \mid a, b, c, d \in \mathbb{Z} \text{ or } a, b, c, d \in \mathbb{Z} + \frac{1}{2}\}.$$

A proper order in $\mathcal{H}$ *is:*

$$\mathcal{O}_\mathcal{H} = \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k + \frac{\mathbb{Z}(1 + i + j + k)}{2}.$$

Proposition 5.1.1. *Let* E *be an elliptic curve over* K*. Then the ring* $\mathrm{End}_K(E)$ *of* K*-endomorphisms of* E *is isomorphic to either:*

1. $\mathbb{Z}$*,*
2. *an order in an imaginary quadratic field, or*

3. *an order in a quaternion algebra.*

In the case that $\mathrm{char}(K) = 0$*, only the two first cases are possible.*

Proof. This proof uses a result from ring theory, given the characteristics of the endomorphism ring of an elliptic curve. Many of these characteristics are obtained through the dual isogeny which was introduced in Proposition 2.1.3. A complete proof if this proposition can be found in [19, §3.9]. □

Definition 5.1.1. *Given an elliptic curve* E *over* K*,* E *is said to have* complex multiplication *if* $\mathrm{End}_K(E) \ncong \mathbb{Z}$*. The curve is said to have complex multiplication by the order isomorphic to* $\mathrm{End}_K(E)$*.*

Proposition 5.1.2. *Let* E *be an elliptic curve over a finite field* $\mathbb{F}_q$ *of characteristic* p*.*

1. *If* E *is ordinary (see Definition 2.3.2), then* $\mathrm{End}_{\mathbb{F}_q}(E)$ *is an order in an imaginary quadratic field.*
2. *If* E *is supersingular (see Definition 2.3.2), then* $\mathrm{End}_{\mathbb{F}_q}(E)$ *is a maximal order in a quaternion algebra.*

Proof. This proof was written in German by Deuring in [2], an English version of the proof can be found in [25, 10.2]. □

Given a quadratic imaginary field $K = \mathbb{Q}(\sqrt{D})$, a prime p is said to be:

1. ramified if the quotient $\mathcal{O}_K/p\mathcal{O}_K \cong \mathbb{F}_p[x]/(x)$,
2. split if $\mathcal{O}_K/p\mathcal{O}_K \cong \mathbb{F}_p[x]$ or,
3. inert if $\mathcal{O}_K/p\mathcal{O}_K \cong \mathbb{F}_{p^2}$, which can also be referred to as remaining prime.

These can be characterized using quadratic reciprocity.

Proposition 5.1.3 ([7, §4.4])**.** *For* $\mathbb{Q}(\sqrt{D})$*, prime* p *is said to be:*

1. *ramified if and only if* $\left(\frac{D}{p}\right) = 0$,
2. *split if and only if* $\left(\frac{D}{p}\right) = 1$ *or,*
3. *inert if and only if* $\left(\frac{D}{p}\right) = -1$.

Proposition 5.1.4 ([12, 13,§4])**.** *Let E be an elliptic curve defined over $\mathbb{Q}$ for which $\mathrm{End}_{\mathbb{Q}}(E) \cong \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$, where D is a square-free negative integer and $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ is a maximal order in $\mathbb{Q}(\sqrt{D})$. Then E_p, the good reduction of E over $\mathbb{F}_p$ (recall Definition 3.1.1), is supersingular if p ramifies or remains prime in $\mathbb{Q}(\sqrt{D})$.*

Combining both Proposition 5.1.2 and Propositon 5.1.4, it follows that an elliptic curve E over K with good reduction at a prime p is supersingular if and only if it has complex multiplication by an order that is ramified at p and split at all other primes.

Proposition 5.1.5. *Given an elliptic curve E over $\mathbb{Q}$ that does not admit complex multiplication, the primes for which the reduction E_p (recall Definition 3.1.1) is a supersingular elliptic curve are of density 0.*

Proof. This is a consequence of Serre's irreducibility theorem, [17, IV,§2] or [18, 2]. □

Chapter 6

Main Result

At this point in this thesis, we have seen all the necessary notions in order to understand the proof of the main theorem. We now see how complex multiplication is connected to $\mathbb{Q}$-isogenous quadratic twists.

Theorem 6.0.1. *Given an elliptic curve E over $\mathbb{Q}$, if E has complex multiplication (see Definition 5.1.1) by an order in $\mathbb{Q}(\sqrt{D})$, where D is negative and square-free, then E is $\mathbb{Q}$-isogenous to the quadratic twist E^D, see Section 4.1 for details about E^D.*

Proof. Let S to be the set of "bad" primes; that is, let S be the set of primes that divide the conductor of E and of E^D (recall Definition 3.1.3), note that the conductor of E^D will be a multiple of D. Since E^D is a quadratic twist, for all $p \notin S$, $\chi_D(\text{Frob}_p)a_p(E) = a_p(E^D)$ by Proposition 4.3.1. As seen in Section 4.2, χ_D is a Galois representation such that for $p \nmid D$, $\chi_D(\text{Frob}_p) = 1$ if and only if $\left(\frac{D}{p}\right) = 1$. Combining this with Proposition 5.1.4, it follows that, for every $p \notin S$, if $\left(\frac{D}{p}\right) = -1$ then the good reduction E_p (see Definition 3.1.1) is supersingular and $a_p(E_p) = a_p(E_p^D)$. The case $\left(\frac{D}{p}\right) = 1$ also gives $a_p(E_p) = a_p(E_p^D)$. Thus for all $p \notin S$, $a_p(E) = a_p(E^D)$ which implies that E_p is $\mathbb{F}_p$-isogenous to E_p^D (see Proposition 2.3.4). Using Proposition 3.2.1, if the two curves are locally isogenous for all $p \notin S$, then they are $\mathbb{Q}$-isogenous. □

Theorem 6.0.2. *If E is an elliptic curve over $\mathbb{Q}$ and E is $\mathbb{Q}$-isogenous to its quadratic twist E^D, for a negative square-free integer D, then E has complex multiplication.*

Proof. Taking S to be the same set of bad primes as in the above proof, the reductions E_p, E_p^D are $\mathbb{F}_p$-isogenous for all $p \notin S$, and $a_p(E_p) = a_p(E_p^D)$ by Proposition 2.3.4. As seen in Section 4.2, $\chi_D(\text{Frob}_p)a_p(E_p) = a_p(E_p^D)$, thus $a_p(E_p) = 0$ for all p inert in $\mathbb{Q}(\sqrt{D})$ and these

primes have density 1/2. From Proposition 5.1.5, this density is 0, when the curve does not have complex multiplication. Therefore E has complex multiplication. □

By joining both Theorem 6.0.1 and Theorem 6.0.2, one can obtain the following, which is the main result of this thesis:

Corollary 6.0.1. *An elliptic curve E over $\mathbb{Q}$, is $\mathbb{Q}$-isogenous to a quadratic twist if and only if it has complex multiplication.*

Remark 6.0.1. *As part of further work, the aim is to take Theorem 6.0.2, and obtain a more specific result, which is the converse of Theorem 6.0.1. This would make Theorem 6.0.2 more specific by proving that E has complex multiplication by an order in $\mathbb{Q}(\sqrt{D})$.*

6.1 Conclusion

The main result of this thesis demonstrates a different approach to complex multiplication of elliptic curves, namely, through isogenous quadratic twist. Further results as mentioned in Remark 6.0.1, would not only give a sufficient condition for a curve to have complex multiplication, but would also find the order to which the endomorphism ring of the curve is isomorphic to.

This project can be expanded by generalizing the main result to elliptic curves over number fields, not only $\mathbb{Q}$. Some numerical tests have been performed to confirm that such a generalization might be possible. In particular, when testing with a curve defined over $\mathbb{Q}(\sqrt{-1})$, and with 40000 primes, we obtain that the super singular primes have density 1/2, confirming that the curve has complex multiplication by Serre's Theorem 5.1.5. However, certain elements of the main proof, for example, Lang's Theorem 5.1.4, would require a more thorough investigation in order to be generalized.

Appendix A

A Little Algebraic Geometry

The goal of this section is to provide some of the necessary background to understand the category of schemes.

We begin by explaining that the category of affine schemes is anti-equivalent to the category of commutative rings with identity (these are denoted by "cring"). This allows us to start with the abstract notion of schemes and pass to ring theory which is usually well known. Then using the notion of schemes we define varieties, which are needed to define elliptic curves.

A.1 Sheaves of Crings and Ringed Spaces

Definition A.1.1. *A* presheaf $\mathcal{F}$ *on a topological space* X *is a contravariant functor from the category of open sets in* X *to* (***cring***)*. A morphism of presheaves is a natural transformation between presheaves.*

We use the notation $U \mapsto \mathcal{F}(U)$. Elements of $\mathcal{F}(U)$ are called the *sections* of $\mathcal{F}$ over U. Every inclusion of open sets $U_2 \supseteq U_1$ determines a ring homorphism of sections $\rho_{U_2,U_1} \colon \mathcal{F}(U_2) \to \mathcal{F}(U_1)$ such that $\rho_{U_1,U_1} = \text{identity}_{U_1}$ and for all $U_1 \subseteq U_2 \subseteq U_3 \subseteq X$, $\rho_{U_2,U_1} \circ \rho_{U_3,U_2} = \rho_{U_3,U_1}$.

Definition A.1.2. *A presheaf is a* sheaf *if its satisfies the two following axioms for every open covering* $U = \bigcup_{i \in I} U_i$ *of every open set* $U \subset X$*:*

Identity: *if* $f_1,\ f_2 \in \mathcal{F}(U)$ *and* $\rho_{U,U_i} f_1 = \rho_{U,U_i} f_2$ *for all* i*, then* $f_1 = f_2$*, and*

Gluability: *given* $f_i \in \mathcal{F}(U)$ *for all* i*, such that* $\rho_{U_i,U_i \cap U_j} f_i = \rho_{U_i,U_i \cap U_j} f_j$ *for all* i *and* j*, then there is some* $f \in \mathcal{F}(U)$ *such that* $\rho_{U,U_i} f = f_i$ *for all* i*.*

A *morphism of sheaves* is just a morphism of the underlying presheaves.

A *ringed space* is a pair $(X, \mathcal{O}_X)$ where X is a topological space and $\mathcal{O}_X$ is a sheaf of crings on X. Ringed spaces form a category where morphisms $f : (X, \mathcal{O}_X) \to (X, \mathcal{O}_Y)$ are defined as pairs $(|f|, f^{\#})$ where $|f|\colon X \to Y$ is a continuous function and $f^{\#}\colon \mathcal{O}_Y \to |f|_*\mathcal{O}_X$ is a sheaf homomorphism such that for any $x \in X$ the composition of $\mathcal{O}_{Y,y} \to (|f|_*\mathcal{O}_X)_y$ with $(|f|_*\mathcal{O}_X)_y \to \mathcal{O}_{X,x}$ is a morphism of local rings, for every $f(x) = y$. Here, $|f|_*$ is the push forward of $\mathcal{O}_X$, defined by $|f|_*\mathcal{O}_X(V) = \mathcal{O}_X(f^{-1}V)$ for every open $V \subseteq Y$ and $\mathcal{O}_{X,x} = \varinjlim_{V \ni x} \mathcal{O}_X(V)$, where the limit is taken over open subsets. See [24, Chapters 2,3,4].

A.2 Schemes

Objects in the category **(cring)** are crings and the morphisms are ring homomorphisms.

For any cring A, let $|\mathrm{Spec}(A)|$ be the set of prime ideals in A. The rule $A \mapsto |\mathrm{Spec}(A)|$ determines a contravariant functor from (**cring**) to (**set**) as follows. If $\varphi : A \to B$ is a ring homomorphism then $|\mathrm{Spec}(\varphi)|\colon |\mathrm{Spec}(A)| \to |\mathrm{Spec}(B)|$ is defined by $\mathfrak{p} \mapsto \varphi^{-1}(\mathfrak{p})$.

We give $|\mathrm{Spec}(A)|$ the *Zarisky topology*, by declaring that

$$V(S) := \{\mathfrak{a} \in |\mathrm{Spec}(A)| \mid S \subset \mathfrak{a}\}$$

is a closed set, for every subset $S \subseteq A$. The Zariski topology for $|\mathrm{Spec}(A)|$ admits a basis of open sets

$$X_f := \{\mathfrak{a} \in |\mathrm{Spec}(A)| \mid f \notin \mathfrak{a}\}$$

where $f \in A$. Elements of X_f may be understood as prime ideals in the localization

$$A_f := \left\{ \frac{a}{f^n} \mid a \in A \text{ and } n \in \mathbb{N} \right\}$$

because there is a one-to-one correspondence between prime ideals of A_f and the prime ideals of A that do not contain f. The set $|\mathrm{Spec}(A)|$, together with its Zariski topology, is denoted by $\mathrm{Spec}(A)$. One can show that, for every ring homomorphism $\varphi : A \to B$, the function

$|\mathrm{Spec}(\varphi)|\colon |\mathrm{Spec}(A)| \to |\mathrm{Spec}(B)|$ is continuous, with reference to the Zariski topology. This way, the rule $A \mapsto \mathrm{Spec}(A)$ determines a contravariant functor from $(\mathbf{cring})$ to the category of topological spaces.

The topological space $X = \mathrm{Spec}(A)$ is naturally equipped with a sheaf of crings, defined on the basis for the Zariski topology, by

$$\mathcal{O}_X(X_f) := A_f$$

and by

$$\begin{array}{ccc} X_{fg} \to X_f & \longmapsto & A_{fg} \leftarrow A_f \\ \mathfrak{p} \mapsto \mathfrak{p} & & \dfrac{ag^n}{f^n g^n} \leftarrow\!\shortmid \dfrac{a}{f^n}. \end{array}$$

Definition A.2.1. *An* affine scheme *is a ringed space isomorphic to* $(\mathrm{Spec}(A), \mathcal{O}_A)$*, for some cring* A*.*

Definition A.2.2. *A* scheme $(X, \mathcal{O}_X)$ *is a ringed space for which there is an open covering* $X = \cup_{i\in I} X_i$ *such that* $(X_i, \mathcal{O}_X|_{X_i})$ *is an affine scheme for every* $i \in I$*.*

Note that it is common notation to refer to X, when mentioning the scheme $(X, \mathcal{O}_X)$.

Proposition A.2.1 ([24, 3.7.1])**.** *The contravariant functor* $A \mapsto (\mathrm{Spec}(A), \mathcal{O}_A)$ *from* $(\boldsymbol{cring})$ *to the category of rings spaces is an equivalence from* $(\boldsymbol{cring})$ *to the category of affine schemes. The inverse functor from affine schemes to* $(\boldsymbol{cring})$ *is given by* $(X, \mathcal{O}_X) \to \mathcal{O}_X(X)$*.*

Definition A.2.3. *Given two schemes* $X = \cup_{i\in I} X_i$ *and* $Y \cup_{i\in I} Y_i$*, a morphism of schemes* $\varphi\colon X \to Y$*, is a morphism that satisfies the following on the underlying affine parts. For all* i, j*, where* $X_i \cong \mathrm{Spec}(A)$ *and* $Y_j \cong \mathrm{Spec}(B)$*, there exist a restriction* $\varphi_{X_i}\colon X_i \to Y_j$*, such that there is* $B \to A$ *is a ring homomorphism ,such that* $\mathfrak{p} \mapsto (\varphi^{\#}_{X_i})^{-1}(\mathfrak{p})$*.*

A.3 Some Morphisms

Definition A.3.1. *A morphism of schemes* $f\colon X \to Y$ *is* of finite type *if for each* $y \in Y$*, there exists an open affine subset* $V = \mathrm{Spec}(A)$ *containing* y *such that*

$$f^{-1}(V) = \bigcup_{i=1}^{n} \mathrm{Spec}(B_i)$$

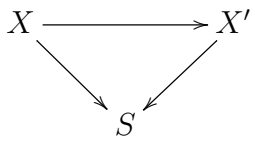
and for each i *the composite map*

$$A = \mathcal{O}_Y(V) \xrightarrow{f^\#} \mathcal{O}_X(f^{-1}(V)) \xrightarrow{restr} B_i$$

makes B_i *a finitely generated* A*-algebra. We say that* f *is* finite *if instead* $f^{-1}(V) = \mathrm{Spec}(B)$ *for some ring* B *and* $f^\#$ *makes* B *a finitely generated* A*-module.*

A.4 Relative Schemes and Rational Points

Fix a scheme S. Then a scheme over S (also referred to as a S scheme) is a scheme X together with a morphism of schemes $X \to S$, which is then called the structure morphism for X. A morphism of schemes over S is a morphism $X \to X'$ which makes the following diagram commute.



In the special case that $S = \mathrm{Spec}(R)$ for some cring R, a scheme over $\mathrm{Spec}(R)$ is called an R-scheme or a scheme over R.

Definition A.4.1. *Given a scheme* X *over a field* K*, a* K-rational point *of* X *is a morphism* $\mathrm{Spec}(K) \to X$*. The set of* K *rational points is denoted* $X(K)$*.*

A.5 Varieties

Since the aim is to work with varieties, only reduced schemes are considered; these are schemes $(X, \mathcal{O}_X)$ such that $\mathcal{O}_X(U)$ has no nonzero nilpotents for every open set U of X.

Definition A.5.1. *Let K be a field. A K-variety Y, is a finite type K-scheme $Y = \cup_{i\in I} Y_i$, where each Y_i is isomorphic to $K[x_1, x_2, \ldots, x_n]/I$ for some non-negative integer n and for some ideal $I \triangleleft K[x_1, x_2, \ldots, x_n]$ such that $\sqrt{I} = I$ (here, $\sqrt{}$ denotes the Jacobson radical of an ideal).*

In the case $Y \cong K[x_1, x_2, \ldots, x_n]/I$, Y is said to be an *affine variety.*

Definition A.5.2. *Let Y be a variety. Y is* nonsingular *at a point $P \in Y$ if the local ring $\mathcal{O}_{Y,P}$ defined in Section A.1, is a regular local ring, which is a ring where the localization at every prime ideal is local. Y is said to be* smooth *(or nonsingular) if it is nonsingular at every point.*

Definition A.5.3. *Let $X \cong K[x_1, x_2, \ldots, x_n]/I$ and Y be affine K-varieties. A K-morphism of affine varieties is a morphism of schemes (see Definition A.2.3), $f\colon X \to Y$ is a map such that $f \in K(x_1, x_2, \ldots, x_n)/I$ and the image $f(X)$ is in Y.*

Morphisms of K-varieties are defined by looking at the underlying affine varieties and taking K-morphisms of these.

A.6 Group Schemes

This section explains what are multiplicative group schemes, this is needed to define the group law of an elliptic curve in Section 1.4.

In the category of algebraic varieties over K, terminal objects are $\mathrm{Spec}(K)$. Note that every variety X comes equipped with a structure map $\sim\colon X \to \mathrm{Spec}(K)$. We define a *group scheme* to be an object X equipped with three morphisms:

1. Multiplication $m\colon X \times X \to X$.
2. Identity element $e\colon \mathrm{Spec}(K) \to X$, which does not have to be the identity map.

3. Inverse $\iota\colon X \to X$.

These morphisms also need to satisfy the following conditions:

(a) Associativity axiom, we want the following diagram to commute:

$$\begin{array}{ccc} X \times X \times X & \xrightarrow{id \times m} & X \times X \\ \downarrow{\scriptstyle m \times id} & & \downarrow{\scriptstyle m} \\ X \times X & \xrightarrow[m]{} & Y \end{array}$$

Where $id\colon X \to X$ is such that $x \mapsto x$.

(b) Identity axiom, we want both of the following to be the identity map:

$$X \xrightarrow{\sim} \mathrm{Spec}(K) \times X \xrightarrow{e \times id} X \times X \xrightarrow{m} X$$

$$X \xrightarrow{\sim} X \times \mathrm{Spec}(K) \xrightarrow{id \times e} X \times X \xrightarrow{m} X$$

(c) Inversion axiom, we want the following diagram to commute:

$$\begin{array}{ccccc} X \times X & & \xrightarrow{\iota \times id} & & X \times X \\ \uparrow{\scriptstyle diag} & & & & \downarrow{\scriptstyle m} \\ X & & \xrightarrow[id]{} & & Y \\ & \searrow^{proj} & & \nearrow_{\sim} & \\ & & \mathrm{Spec}(K) & & \end{array}$$

where $diag\colon X \to X \times X$ is simply the map $x \mapsto (x, x)$. Note that we also need a similar diagram for $id \times \iota$.

Appendix B

Cardinality of Isogeny Classes

Given an elliptic curve E defined over $\mathbb{F}_q$, it is an interesting problem to calculate how many other curves lie in its $\mathbb{F}_q$-isogeny class. In [16] Schoof gives an algorithm to compute the cardinality of $\mathbb{F}_q$-isogeny classes by breaking down in classes of isomorphic curves within the isogeny class, and then counting the projectively inequivalent curves. I have implemented this algorithm in Sage as an earlier part of my project, which is not needed for the proof main theorem of Chapter 6 but demonstrates an interesting aspect of isogenies. A proof of why the algorithm is correct can be found in [16]. Schoof's algorithm takes as input an elliptic curve over $\mathbb{F}_q$, and then finds its trace of Frobenius, denoted t here. Let $I(t)$ be the class of elliptic curves that have exactly $q+1-t$ points defined over $\mathbb{F}_q$. Hence curves in this class are $\mathbb{F}_q$-isogenous. The algorithm outputs the following values:

$N(t)$ The number of $\mathbb{F}_q$-isomorphism classes in $I(t)$.

$M(t)$ The number of projectively inequivalent curves over $\mathbb{F}_q$, that have exactly $q+1-t$ points.

Two curves are said to be projectively equivalent if there is a projective transformation mapping an equation of a curve to another. A projective transformation is a linear transformation of points of a projective variety.

The most significant task of this algorithm is to compute $N(t)$ which tells us the number of $\mathbb{F}_q$-isomorphisms classes of curves $\mathbb{F}_q$-isogenous to E. Two curves $E_1,\ E_2$ are in the same $\mathbb{F}_q$-isomorphism class if $E_1 \cong E_2$ and both of these are $\mathbb{F}_q$-isogenous to E, elliptic curves in different isomorphism classes are not isomorphic. Each isomorphism class gives at least one projectively inequivalent curve in the isogeny class of E. But there might be

more projectively inequivalent curves which are those obtained by non invertible projective transformations within an isogeny class, which is what $M(t)$ represents.

In [16] Schoof gives tables of values that the algorithm produces. He fixed a field and inputed various traces of Frobenius to the algorithm. The first thing done was to make sure that our implementation agreed with Schoof's values. Some examples are listed below. In particular, for Example B.0.1 and Example B.0.2 the fields have small cardinality and it was possible to test for every elliptic curve and actually obtain and list the $\mathbb{F}_q$-isogeny classes. This was achieved using Sage's built-in methods that can determine if two elliptic curves are $\mathbb{F}_q$-isogenous or $\mathbb{F}_q$-isomorphic.

Example B.0.1. *For the curve $E\colon y^2 = x^3 + x$ over $\mathbb{F}_3$, we have $M(t) = N(t) = 2$. Here is a list of all curves $\mathbb{F}_3$-isogenous to E:*

1. $y^2 = x^3 + x$
2. $y^2 = x^3 + x + 1$
3. $y^2 = x^3 + x + 2$
4. $y^2 = x^3 + 2x$.

The first 3 curves are all also $\mathbb{F}_3$-isomorphic to E, which explains why $M(t) = 2$. Elliptic curves 1 and 4 are projectively inequivalent.

Example B.0.2. *For $E\colon y^2 = x^3 + x$ over $\mathbb{F}_5$, we have $M(t) = N(t) = 2$. Here is a list of all curves $\mathbb{F}_5$-isogeneous to E:*

1. $y^2 = x^3 + x$
2. $y^2 = x^3 + x + 2$
3. $y^2 = x^3 + x^2 + 3x$
4. $y^2 = x^3 + x^2 + 3x + 2$
5. $y^2 = x^3 + x^2 + 3x + 3$
6. $y^2 = x^3 + 2x^2 + 4x$
7. $y^2 = x^3 + 2x^2 + 4x + 1$
8. $y^2 = x^3 + 2x^2 + 4x + 3$
9. $y^2 = x^3 + 3x^2 + 4x$
10. $y^2 = x^3 + 3x^2 + 4x + 2$
11. $y^2 = x^3 + 3x^2 + 4x + 4$
12. $y^2 = x^3 + 4x^2 + 3x$
13. $y^2 = x^3 + 4x^2 + 3x + 2$
14. $y^2 = x^3 + 4x^2 + 3x + 3.$

Here we have that curves 1, 3, 8, 10 and 12 are $\mathbb{F}_5$-isomorphic to E, the remaining curves are $\mathbb{F}_5$-isomorphic to each other.

Example B.0.3. *Over $\mathbb{F}_7$ we also have $M(t) = N(t) = 2$, in this case 42 curves are $\mathbb{F}_7$-isogenous to E and 21 are $\mathbb{F}_7$-isomorphic to E.*

Example B.0.4. *Over $\mathbb{F}_{11}$ we also have $M(t) = 8$ and $N(t) = 4$, in this case 220 curves are $\mathbb{F}_{11}$-isogenous to E and 55 are $\mathbb{F}_{11}$-isomorphic to E.*

Below are the main computations of Schoof's algorithm.

Input: t the trace of Frobenius of an elliptic curve. $q = p^n$ the order of the field where E is defined.

Output: $M(t)$

$$M(t) = N(t) + N_3(t) + 3N_{3\times 3}(t) - \epsilon(t),$$

where:

$\mathbf{N(t)}$	**if**
$H(t^2 - 4q)$	$t^2 < 4q$ and $p \nmid t$
H(-4p)	$t = 0$,and q is not a square
1	$t^2 = 2q$, p=2 and q is not a square
1	$t^2 = 3q$, p=3 and q is not a square
$\frac{1}{12}(p + 6 - 4(\frac{-3}{p}) - 3(\frac{-4}{p}))$	$t^2 = 4q$ and q is a square
$1 - (\frac{-3}{p})$	$t^2 = q$ and q is a square
$1 - (\frac{-4}{p})$	$t = 0$ and q is a square
0	otherwise

Where $\left(\frac{a}{p}\right)$, for $a \in \mathbb{Z}$, is the Legendre symbol, this method is implemented in Sage. $H(a)$, for $a \in \mathbb{Z}$, is the Kronecker class number, which is defined in [16, §2] and is implemented in Sage.

$\mathbf{N_3(t)}$	**if**
$N(t)$	$t \equiv q + 1 \pmod 3$
0	otherwise

$\mathbf{N_{3\times 3}(t)}$	**if**
$H\left(\frac{t^2-4q}{9}\right)$	$q \equiv 1 \pmod 3$, $p \nmid t$ and $t \equiv q + 1 \pmod 3$
$N(t)$	q is a square, $p \neq 3$ and $t = 2\left(\frac{\sqrt{q}}{3}\right)\sqrt{q}$
0	otherwise

$\epsilon(\mathbf{t})$	**if**
2	$(t = t_0$ or $t = t_1)$ and $t_0 \neq t_1$
3	$t = t_0 = t_1$ and $p = 2$
3	$t = t_0 = t_1$ and $p \neq 2$
0	otherwise

The numbers t_0 and t_1 are defined as follows:

$\mathbf{t_0}$, only defined if $q \equiv 1 \pmod 3$	**if**
the unique solution $t \in \mathbb{Z}$ to: $t \equiv q + 1 \pmod 9$ $p \nmid t$ $t^2 + 3x^2 = 4q$ for some $x \in \mathbb{Z}$	$p \equiv 1 \pmod 3$
$2\left(\frac{\sqrt{q}}{3}\right)\sqrt{q}$	$p \not\equiv 1 \pmod 3$

$\mathbf{t_1}$, only defined if $q \equiv 1$ or $\pmod{12}$	**if**
the unique solution $t \in \mathbb{Z}$ to: $t \equiv q + 1 \pmod 9$ $p \nmid t$ $t^2 + 4x^2 = 4q$ for some $x \in \mathbb{Z}$	$p \equiv 1 \pmod 4$
$2\left(\frac{\sqrt{q}}{3}\right)\sqrt{q}$	$p \not\equiv 1 \pmod 4$

Bibliography

[1] Chenevier, G. *Quaternion Algebras* Electronic edition available at: http://www.math.polytechnique.fr/ chenevier/coursIHP.

[2] Deuring, M. *Die Typen der Multiplikatorenringe Elliptischer Funktionenkörper.* Abh. Math. Sem. Hansischen Univ., 14:197272, 1941.

[3] Diamond F., Shurman J. *A First Course in Modular Forms.* Springer, 2001.

[4] Dummit D., Foote R. *Abstract Algebra.* John Wileys and Sons, third edition, 2004.

[5] Edixhoven, B., Groot, A., Top, J. *Elliptic curves over the rationals with bad reduction at only one prime* Springer, 2000.Mathematics of Computation, vol. 54, no. 189, January 1990.

[6] Eisenbud, D., Harris, J. *The Geometry of Schemes.* Springer, 2000.

[7] Everest, G., Ward, T. *An Introduction to Number Theory.* Springer, 2005.

[8] Faltings, G. *Finiteness Theorems for Abelian Varieties over Number Fields* Arithmetic Geometry, Cornell-Silverman, 1985.

[9] Fröhlich, A. *Local fields* In Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), pages 141. Thompson, Washington, D.C., 1967.

[10] Garling, D.J.H. *A Course in Galois Theory* Cambridge University Press, 1986.

[11] Hartshorne, R. *Algebraic Geometry* Springer, University of California Berkeley,1977.

[12] Lang, S. *Elliptic Functions* Springer-Verlag, Yale University, 1987.

[13] Levin, B. *Stanford University: Seminar on Falting's Proof of the Mordell Conjecture - Tate Conjecture.* Electronic edition available online at: http://math.stanford.edu/ akshay/ntslearn.html, 2010.

[14] Milne, J.S. *Abelian Varieties.* Electronic edition available online at: http://www.jmilne.org/math/CourseNotes/AV110.pdf, 1998.

[15] Schoof, R. *Counting Points on Elliptic Curves Over Finite Fields.* J. Théorie des nombres. 1995, pages 219–264.

[16] Schoof, R. *Nonsingular Plane Cubic Curves over Finite Fields* J. Combin. Theory Ser. A, volume 46, 1987, number 2, pages183–211.

[17] Serre, J. *Abelian ℓ-Adic Representation and Elliptic Curves* Research notes in mathematics, 1968.

[18] Serre, J. *Quelques Applications du Théorème de Densité de Chebotarev* Publications Mathémagiques de L'I.H.É.S., 1981.

[19] Silverman, J. H. *The Arithmetic of Elliptic Curves* Springer, 1986.

[20] Silverman, J. H. *Advanced Topics in the Arithmetic of Elliptic Curves* Springer, Brown University, 1996.

[21] Silverman, J. H., Tate, J. *Rational points on elliptic curves* Springer-Verlag 1994.

[22] Stichtenoth, H. *Algebraic Function Fields and Codes* Springer 2008.

[23] Tate, J. *Endomorphisms of Abelian Varieties over Finite Fields* Inventiones math., volume 2, 1966, 134–144.

[24] Vakil, R. *Foundations of Algebraic Geometry* Electronic edition available online at: http://math216.wordpress.com, 2013

[25] Washington, L. C. *Elliptic Curves Number Theory and Cryptography* CRC Press, University of Maryland, 2008.