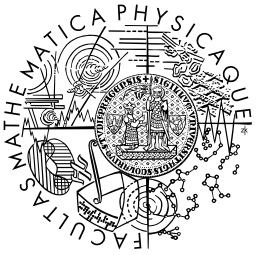


FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

MASTER THESIS

Jan Oupický

Theoretical foundations of cryptosystems based on isogenies of supersingular elliptic curves

Department of Algebra

Supervisor of the master thesis: prof. RNDr. Aleš Drápal, CSc., DSc.

Study programme: Mathematics

Study branch: Mathematics for Information Technologies

Prague 2022

I declare that I carried out this master thesis independently, and only with the cited sources, literature and other professional sources. It has not been used to obtain another or the same degree.

I understand that my work relates to the rights and obligations under the Act No. 121/2000 Sb., the Copyright Act, as amended, in particular the fact that the Charles University has the right to conclude a license agreement on the use of this work as a school work pursuant to Section 60 subsection 1 of the Copyright Act.

In ..... date ....

Author's signature

I would like to thank my supervisor prof. RNDr. Aleš Drápal, CSc., DSc. for his help and advice. Also, I would like to thank my family and friends who had helped me enormously during my studies. At last, I would like to thank Andrew V. Sutherland for his willingness to explain some details of his texts to me.

Title: Theoretical foundations of cryptosystems based on isogenies of supersingular elliptic curves

Author: Jan Oupický

Department: Department of Algebra

Supervisor: prof. RNDr. Aleš Drápal, CSc., DSc., Department of Algebra

Abstract: The thesis is focused on the theory behind post-quantum key exchange algorithms CSIDH and SIDH. We assume basic knowledge of elliptic curves although, at the beginning, we briefly present the theory of elliptic curves and isogenies. After that, we build on that theory to understand the endomorphism rings of elliptic curves. We also present the ideal class group action over the complex numbers and how it relates to elliptic curves over finite fields. At the end, we present the two mentioned algorithms and explain why and how they work with the help of the presented theory and examples. Also, we include a brief security analysis of some aspects of the algorithms. Throughout the thesis we have also modified or expanded proofs of essential statements.

Keywords: function field, elliptic curve, supersingular elliptic curve, isogeny, elliptic curve cryptography, CSIDH

Contents

Introduction

Cryptographic algorithms built on isogenies between supersingular elliptic curves have, for the past 10 years, become one direction in which we can go to achieve post-quantum cryptographic algorithms i.e., cryptographic algorithms that do not have efficient attacks against them using potential quantum computers.

The algorithms CSIDH[1] and SIDH[2] are meant to be post-quantum alternatives for the famous Diffie-Hellman key exchange. Both of these algorithms are built on the theory of supersingular curves and utilize walks on a specific supersingular isogeny graph. Although CSIDH and SIDH have very similar names, the theory behind them is quite different.

SIDH was developed first in 2011 by De Feo, Jao and Plût ([FJP11]) as a practically usable post-quantum key exchange algorithm inspired by the work of Rostovtsev and Stolbunov ([RS06]).

In 2018, Castryck et al. presented an alternative to SIDH called CSIDH ([Cas+18]). CSIDH is also inspired by the work of Rostovtsev and Stolbunov ([RS06]).

A standardized version of SIDH named "SIKE" is also a Round 3 finalist of NIST's Post-Quantum Cryptography Standardization project. CSIDH did not participate because the standardization project started in 2017.

The goal of this thesis is to present the necessary theory to understand how and why these two algorithms work, including a few examples. The understanding of the theory is crucial because, unless you are an expert in that field, after reading the above-mentioned papers [Cas+18] and [FJP11], you probably have a plethora of unanswered questions. This is because the authors mention only the necessary statements and do not provide proofs in many instances. Therefore, a non-expert in the theory of isogeny graphs has to go through an exhaustive number of references, which most of the time use different notation, to find answers.

In the first chapter, we first present a brief summary of number theory and ring theory that we are going to use later on. In the second part of the first chapter, we introduce the basics of the theory of elliptic curves focused mainly on isogenies between elliptic curves. Note that we assume the reader is familiar with most of the theory presented. For details, we recommend the books of Galbraith [Gal12], Washington [Was08] or Silverman [Sil09].

The second chapter builds on this theory to closely explore the theory of supersingular/ordinary curves and their endomorphism rings. We also present a few technical statements that are going to be useful in the final chapters.

The third chapter is supposed to inform the reader about where does the ideal class group action come from. The ideal class group action is the building block of the algorithm CSIDH. Note that the theory is presented using elliptic curves over $\mathbb{C}$. Therefore, we only present the necessary minimum and do not go into detail. This is because we are mainly interested in elliptic curves over finite fields.

That is where the fourth chapter comes into play. In this chapter, we show how can we define the ideal class group action on elliptic curves over finite fields.

In the fifth chapter, we focus on the isogeny graphs of elliptic curves. We

[1] Stands for "Commutative Supersingular Isogeny Diffie-Hellman".
[2] Stands for "Supersingular Isogeny Diffie-Hellman".

present some of their properties that are useful for understanding CSIDH and SIDH. We also present statements about ordinary and supersingular curves that are specific to CSIDH and SIDH.

At the end, we finally present the algorithms for which we were building the theory. We start with CSIDH because it utilizes most of the presented theory and after understanding CSIDH we believe SIDH is easier to comprehend. We briefly state the overview of the algorithm and then we go into detail with the help of an example. We mention a few security aspects that are not mentioned in the paper ([Cas+18]).

Then, we present the algorithm SIDH in the similar manner with comparisons to CSIDH.

The thesis is nearly self-contained. Besides basic facts about ring, modules and elliptic curves there are some facts from number theory which are mostly contained in Chapter 3 and were taken from [Sut19] and [Cox13].

Statements concerning elliptic curves and their endomorphism ring are proved nearly completely with notable exceptions like Hasse's theorem (Theorem 31), the classification of the endomorphism algebra (Theorems 26, 41), Theorem 45 and Schoof's theorem about the structure of the group of points of supersingular curves elliptic curves (Theorem 33).

1. Preliminaries

First, we introduce a few terms and theorems from number theory which we are going to utilize later. We define these because across literature the terminology could be a bit different. The number theory follows mainly [Cox13].

In the second part of this chapter, we present the basic theory of elliptic curves and isogenies.

Note, we use the notation $|G : H|$ for the index of a subgroup group H in a group G and the notation $|G|$ for the order of a group G.

1.1 Quadratic fields, tensors and orders

Definition 1. *Let R be a commutative ring and let A, B be R-modules. We define a tensor product of A, B over R (denoted $A \otimes_R B$) as*

$$A \otimes_R B = F(A \times B)/G$$

where $F(A \times B)$ is the free R-module generated by all elements $(a, b) \in A \times B$ and G is the R-submodule generated by all elements of the form

1. $-(a_1 + a_2, b) + (a_1, b) + (a_2, b)$
2. $-(a, b_1 + b_2) + (a, b_1) + (a, b_2)$
3. $-(ra, b) + (a, rb)$
4. $-r(a, b) + (a, rb)$

where $a, a_1, a_2 \in A$, $b, b_1, b_2 \in B$ and $r \in R$. The equivalence class $[(a, b)], a \in A, b \in B$ is denoted as $a \otimes b \in A \otimes_R B$.

If A, B are R-algebras, then we define the product on elements of the form $a \otimes b \in A \otimes_R B$ as

$$(a_1 \otimes b_1)(a_2 \otimes b_2) = (a_1 a_2 \otimes b_1 b_2)$$

where $a_1, a_2 \in A, b_1, b_2 \in B$. We then extend this product linearly to all elements of $A \otimes_R B$ making it an R-algebra.

Definition 2. *Let $\mathcal{R}$ be a $\mathbb{Q}$-algebra of dimension $r \in \mathbb{N}$ (as a $\mathbb{Q}$-vector space). We call $\mathcal{O} \subseteq \mathcal{R}$ an order in $\mathcal{R}$ if $\mathcal{O}$ is a subring which is $\mathbb{Z}$-module of rank r.*

An order $\mathcal{O}$ in $\mathcal{R}$ is maximal if there does not exist a different order $\mathcal{O}'$ in $\mathcal{R}$ s.t. $\mathcal{O} \subseteq \mathcal{O}'$.

Remark. An alternative definition of an order using a tensor product is: $\mathcal{O} \subseteq \mathcal{R}$ is a subring which is finitely generated as a $\mathbb{Z}$-module and $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q} = \mathcal{R}$.

A quadratic field is a field extension of $\mathbb{Q}$ of degree 2. Every quadratic field can be uniquely expressed as $\mathbb{Q}(\sqrt{D})$ where $D \in \mathbb{Z}$, D square free.

Definition 3. *Let $K = \mathbb{Q}(\sqrt{D})$ be a quadratic field and let $D \in \mathbb{Z}$ be square free. The discriminant of K denoted as d_K is defined as*

$$d_K = \begin{cases} D & D \equiv 1 \mod 4 \\ 4D & D \text{ otherwise.} \end{cases}$$

Remark. Note that $d_K \mod 4 \in \{0,1\}$ and $K = \mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{d_K})$ so K is uniquely determined by its discriminant.

Assume K is a quadratic field. If $d_K < 0$, then we say that K is an imaginary quadratic field and if $d_K > 0$, then K is a real quadratic field. In our work we will only work with imaginary quadratic fields therefore from now on we will only focus on them.

Theorem 1. *Let K be an imaginary quadratic field. Denote $\mathcal{O}_K$ its ring of integers. Let $\mathcal{O}$ be an order in K. Then*

(a) $\mathcal{O}_K$ is a unique maximal order in K of rank $r = [K : \mathbb{Q}]$.

(b) $\mathcal{O}_K = \mathbb{Z}\left[\frac{d_K+\sqrt{d_K}}{2}\right]$.

(c) $\exists! f > 0 \in \mathbb{Z}$ s.t. $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ (as a ring).

(d) f from (c) is equal to $|\mathcal{O}_K : \mathcal{O}|$.

(e) $\mathcal{O}_K$ is a Dedekind domain.

Proof. [Cox13] Lemma 7.2 and discussion before the lemma. For (e) see Theorem 5.5. □

Remark. Let $\mathcal{O}$ be an order in K. The index $|\mathcal{O}_K : \mathcal{O}| = f > 0 \in \mathbb{Z}$ from (d) is called the conductor of $\mathcal{O}$

We will now introduce a lattice. We will work with this term mainly in the third chapter but it is useful to define it here.

Definition 4. *A lattice is an additive subgroup of $\mathbb{C}$ generated by two complex numbers $\alpha, \beta \in \mathbb{C}$ s.t. α, β are linearly independent over $\mathbb{R}$.*

A lattice L generated by α, β is usually denoted as $L = [\alpha, \beta] = \alpha\mathbb{Z} + \beta\mathbb{Z}$.

From Theorem 1 we can deduce that $\mathcal{O}_K = [1, \alpha_K]$ where $\alpha_K = \frac{d_K+\sqrt{d_K}}{2}$. Also, from point (c) we get that every order $\mathcal{O}$ in K is a lattice $\mathcal{O} = [1, f\alpha_K]$.

From now on if $\mathcal{O} = [1, \alpha]$, then we assume $\alpha = f\alpha_K$ for some $f \in \mathbb{N}$.

Definition 5. *Let $\mathcal{O} = [1, \alpha]$ be an order in an imaginary quadratic field. The discriminant of $\mathcal{O}$ is the discriminant of the minimal polynomial of α over $\mathbb{Q}$. We denote it as* $\mathrm{disc}(\mathcal{O})$.

Remark. Since $\alpha \notin \mathbb{R}$ and $\alpha^2 \in \mathbb{Q}$, the minimal polynomial of α over $\mathbb{Q}$ is of the form $x^2 + ax + b \in \mathbb{Z}[x]$ where the discriminant is $a^2 - 4b < 0$ because $\alpha \notin \mathbb{R}$. We can compute is as

$$\mathrm{disc}(\mathcal{O}) = (\alpha - \overline{\alpha})^2.$$

Since $\mathrm{disc}(\mathcal{O}) = a^2 - 4b$ for some $a, b \in \mathbb{Z}$, then $\mathrm{disc}(\mathcal{O})$ is a square modulo 4 i.e., $\mathrm{disc}(\mathcal{O}) \mod 4 \in \{0, 1\}$.

Definition 6. *Let $D \in \mathbb{Z}, D < 0$ s.t. $D \mod 4 \in \{0, 1\}$. Such D is called a discriminant.*

Let D be a discriminant. If D cannot be written as $D = f^2 D'$ where $f \in \mathbb{Z}, f > 1$ and D' a discriminant then we call D a fundamental discriminant.

Corollary. Let D be discriminant. There exists a unique order $\mathcal{O}$ in an imaginary quadratic field K s.t. $\text{disc}(\mathcal{O}) = D = f^2 D_K$, where D_K is a fundamental discriminant s.t. $\text{disc}(\mathcal{O}_K) = D_K$, $K = \mathbb{Q}(\sqrt{D_K}) = \mathbb{Q}(\sqrt{D})$ and $f = |\mathcal{O}_K : \mathcal{O}|$. Also, clearly $d_K = D_K$ where d_K is the discriminant of K.

Proof. Follows from Theorem 1. □

Definition 7. *Let $\mathcal{O}$ be an order in an imaginary quadratic field. We call a set L an $\mathcal{O}$-ideal if L is an ideal of $\mathcal{O}$.*

Remark. This definition makes sense since an order is a subring of an imaginary quadratic field.

Definition 8. *Let $\mathcal{O}$ be an integral domain with a fraction field K. We call the set $I \subset K$ a fractional ideal of $\mathcal{O}$ if there exists an $\mathcal{O}$-ideal J and $\alpha \in K \setminus \{0\}$ s.t. $I = \alpha J = \{\alpha\beta : \beta \in J\}$.*

Let $\alpha I, \beta J$ be fractional $\mathcal{O}$-ideals. The product of αI and βJ is defined as

$$\alpha I \cdot \beta J = (\alpha \times \beta)(I \cdot' J) = (\alpha\beta) IJ$$

where $\times$ is product in K and $\cdot'$ is product of $\mathcal{O}$-ideals.

Remark. If K in the previous definition is an imaginary quadratic field (the case we are interested in), we can always write a fractional ideal of $\mathcal{O}$ in the form $\frac{1}{n} I$ where $n \in \mathbb{Z}, n > 0$ and I an $\mathcal{O}$-ideal.

If I is a fractional $\mathcal{O}$-ideal and $I \subseteq \mathcal{O}$, then I is an $\mathcal{O}$-ideal. Every $\mathcal{O}$-ideal is a fractional $\mathcal{O}$-ideal.

Definition 9. *Let I be a fractional $\mathcal{O}$-ideal. If there exists a fractional $\mathcal{O}$-ideal J s.t. $IJ = \mathcal{O}$ then I is said to be invertible.*

Remark. Let $\mathcal{O}$ be an order in an imaginary quadratic field K. If I is an invertible $\mathcal{O}$-ideal, then the inverse ideal J s.t. $IJ = \mathcal{O}$ is unique and we can use the notation $I^{-1} = J$. Because if J' is another fractional ideal s.t. $IJ' = \mathcal{O}$, then due to commutativity $J = J\mathcal{O} = J(IJ') = (JI)J' = (IJ)J' = \mathcal{O}J' = J'$.

Note that we are assuming an embedding of K in $\mathbb{C}$ thus for $\alpha \in K : \mathrm{N}(\alpha) = \alpha\overline{\alpha}$.

Definition 10. *Let $\mathcal{O}$ be an order in an imaginary quadratic field K and I be a non-zero $\mathcal{O}$-ideal. The norm of I is defined as*

$$\mathrm{N}(I) = |\mathcal{O} : I| \in \mathbb{N}.$$

Also define the norm of a non-zero fractional $\mathcal{O}$-ideal $J = \frac{1}{b} I$, where $b \in \mathbb{Z}, b > 0$, as

$$\mathrm{N}(J) = \frac{\mathrm{N}(I)}{\mathrm{N}(b)} \in \mathbb{Q} > 0.$$

Remark. The norm of a fractional ideal does not depend on the choice of I and b.

Definition 11. *Let $\mathcal{O}$ be an order in an imaginary quadratic field K and I an $\mathcal{O}$-ideal. Denote*

$$\mathcal{O}(I) = \{\alpha \in K : \alpha I \subseteq I\}.$$

Definition 12. *Let $\mathcal{O}$ be an order in an imaginary quadratic field, let I be an $\mathcal{O}$-ideal. We call I a proper $\mathcal{O}$-ideal if $\mathcal{O}(I) = \mathcal{O}$.*

1.2 Elliptic curves and isogenies

In this section we introduce the essentials needed to understand what isogenies are. We assume the reader is familiar with basics of algebraic geometry, divisors, elliptic curves and the group structure of an elliptic curve. Nonetheless we will start with some basic definitions which are used throughout the whole text.

In the following we assume a curve is always irreducible (i.e., a curve is a variety) over K. We also assume the reader is familiar with the correspondence between affine and projective curves. Therefore, in some cases we will not specifically say if by a curve we mean a subset of $\mathbb{P}^2$ (a projective space of dimension 2) or $\mathbb{A}^2$ (an affine space of dimension 2).

Throughout the whole work we assume that K is a perfect field. If we work with a finite field ($K = \mathbb{F}_q$), we automatically assume $q = p^e$ for some $p \in \mathbb{N}$ prime and $e \in \mathbb{N}$.

Definition 13. *Let K be a field. A Weierstrass curve over K is a curve defined a Weierstrass equation:*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.1}$$

where $\forall a_i \in K$.

Remark. If $\mathrm{char}(K) \neq 2$, then (1.1) is K-equivalent by substitution

$$(x, y) \mapsto \left(x, y - \frac{a_1x + a_3}{2}\right)$$

to a short Weierstrass equation is of the form

$$y^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4} \tag{1.2}$$

where

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= 2a_4 + a_1a_3 \\ b_6 &= a_3^2 + 4a_6. \end{aligned}$$

If $\mathrm{char}(K) \notin \{2, 3\}$, then (1.2) is also K-equivalent by substitution

$$(x, y) \mapsto \left(\frac{x - 3b_2}{36}, \frac{y}{216}\right)$$

to a simpler form

$$y^2 = x^3 + px + q \tag{1.3}$$

where

$$\begin{aligned} p &= -27(b_2^2 - 24b_4) \\ q &= -54(36b_2b_4 - b_2^3 - 216b_6). \end{aligned}$$

In this text we will not work with fields of characteristic 2 or 3 so we will not focus on these special cases. Therefore, from now on assume K to be a field s.t. $\mathrm{char}(K) \notin \{2, 3\}$.

Definition 14. *Let C be a Weierstrass curve over K (1.1). Define additional terms as follows*

$$b_8 = 4a_2a_6 + a_2a_3^2 + a_1^2a_6 - a_4^2 - a_1a_3a_4$$
$$c_4 = b_2^2 - 24b_4$$
$$\Delta(C) = -8b_4^3 - 27b_6^2 + 9b_2b_4b_6 - b_2^2b_8$$

and if $\Delta(C) \neq 0$, then also

$$j(C) = \frac{c_4^3}{\Delta(C)}.$$

Call $\Delta(C)$ the discriminant of C and $j(C)$ the j-invariant of C.

This following theorem formulates the basic properties of the j-invariant.

Theorem 2. *Let C, C' be Weierstrass curves over K.*

(a) C is smooth $\iff$ $\Delta(C) \neq 0$.

(b) If C, C' are smooth curves, then $j(C) = j(C') \iff$ C and C' are $\overline{K}$-equivalent.

In addition, if $j(C) \notin \{0, 1728\}$, then C and C' are L-equivalent where $[L : K] \leq 2$.

(c) $\forall \lambda \in K$ there exists a Weierstrass curve C' over K s.t. $j(C') = \lambda$.

Proof. [Sil09] Chapter III, Proposition 1.4. □

j-invariant gives us a tool for checking if curves are equivalent or not and subsequently if their functions fields are isomorphic. It also helps with checking the smoothness of a curve.

Definition 15. *We say E is an elliptic curve if E is smooth and is of genus one.*

Definition 16. *Let E, E' be elliptic curves over K. If $j(E) = j(E')$ and E, E' are not K-equivalent but are L-equivalent where $L \geq K$, we call E, E' twisted or we say E is a twist of E' (and vice versa).*

More specifically if $[L : K] = 2$ then we say E is a quadratic twist of E'.

Usually there is a fixed point on the curve (which corresponds to a place of degree one) which is called the base point or point at infinity denoted by ∞ or $\mathcal{O}$. We will mainly use $\mathcal{O}$ to denote the base point but sometimes we will use ∞ in cases where there might be a confusion since $\mathcal{O}$ is also the notation for an order.

Remark. Let E be an elliptic curve and $\mathcal{O} \in E$. Often an elliptic curve is denoted as a pair $(E, \mathcal{O})$.

We say E is an elliptic curve over K if E is a curve defined over K and $\mathcal{O} \in E$ is K-rational.

The term "point at infinity" is sometimes used to describe the projective points of a curve which cannot be mapped upon affine points. In our case we work only with Weierstrass curves which have a unique point at infinity so we use this term interchangeably.

As we know every elliptic curve can be considered a group. More specifically the points of an elliptic curve form an abelian group with an operation $\oplus$ and the neutral element being $\mathcal{O}$. In the case of Weierstrass curve $\mathcal{O} = (0 : 1 : 0) \in \mathbb{P}^2$.

From now on we will assume that an elliptic curve is given by a Weierstrass equation. The following claims can be applied upon any elliptic curve since every function field of an elliptic curve is isomorphic to a function field given by a Weierstrass equation.

Theorem 3. *Let* $\mathrm{char}(K) \neq 2, 3$, $E : y^2 = x^3 + Ax + B, E' : y^2 = x^3 + A'x + B'$ *be elliptic curves over* K.

(a) If $j(E) \neq 0, 1728$ *then define* $\gamma(E) = \frac{B}{A} \mod (K^*)^2 \in K^*/(K^*)^2$ *(as an element of the quotient group of the group* K^**) and similarly* $\gamma(E')$,

(b) if $j(E) = 0$ *then define* $\gamma(E) = B \mod (K^*)^6 \in K^*/(K^*)^6$ *and similarly* $\gamma(E')$,

(c) if $j(E) = 1728$ *then define* $\gamma(E) = A \mod (K^*)^4 \in K^*/(K^*)^4$ *and similarly* $\gamma(E')$.

Then E *and* E' *are* K*-equivalent (*K*-isomorphic) if and only if* $j(E) = j(E')$ *and* $\gamma(E) = \gamma(E')$.

Proof. Follows from the same as Theorem 2 with steps listed in [Sil09] Chapter X, Exercise 10.21. □

Remark. In the previous theorem the definitions for $\gamma(E)$ can be reworded in maybe simpler way. For example, in the case $j(E) \neq 0, 1728$ we need to check if $\frac{B}{A}$ is a square in K and $\frac{B'}{A'}$ is a square in K. If they are both squares or both non-squares we have a K-isomorphism.

Definition 17. *Let* $(E, \mathcal{O})$ *be an elliptic curve over* K. *By* $E(K)$ *we mean the set of all points* $P \in E$ *s.t.* P *are* K*-rational. The elliptic curve group is then denoted as a pair* $(E(K), \oplus)$ *where* $\mathcal{O}$ *is the neutral element.*

Since we have defined the elliptic curve group, we can finally define what an isogeny is.

Definition 18. *Let* $(E_1, \mathcal{O}_1), (E_2, \mathcal{O}_2)$ *be elliptic curves over* K. *Let* $\psi : E_1 \to E_2$ *be a* K*-rational map. We say* ψ *is an isogeny over* K *if* $\psi(\mathcal{O}_1) = \mathcal{O}_2$.

Isogeny over $\overline{K}$ *is called an isogeny.*

We say E_1, E_2 *are isogenous (over* K*) if there exists an isogeny* $E_1 \to E_2$ *(over* K*).*

The set of all isogenies $E_1 \to E_2$ *over* K *is denoted as* $\mathrm{Hom}_K(E_1, E_2)$.

Since we are working with (projective) elliptic curves E_1, E_2 (smooth and irreducible) over K every K-rational map ψ between them is a morphism over K

i.e., $\mathrm{Dom}(\psi) = E_1$. Also, every non-constant morphism over K between smooth curves is surjective.

From that we can conclude that every non-constant isogeny between elliptic curves is surjective. There exists only one constant morphism between elliptic curves that maps base point upon base point. This isogeny is called a zero isogeny.

Definition 19. *Let $\psi : E_1 \to E_2$ be a non-zero isogeny (over K) between elliptic curves over K. By degree of ψ (as an isogeny) we mean the degree of ψ as a rational map i.e., $\deg(\psi) = [K(E_1) : \mathrm{Im}(\psi^*)]$ where $\psi^* : K(E_2) \to K(E_1)$ is the K-homomorphism induced by ψ.*

Define the degree of a zero isogeny as 0.

Remark. Every isogeny is of finite degree.

Remark. Sometimes you might see an isogeny being referred to as a n-isogeny for some $n \in \mathbb{Z}$. This is an abbreviation to saying that the degree of the isogeny is n.

Definition 20. *We say that elliptic curves E_1, E_2 over K are isomorphic (over K) if there exist isogenies $\psi : E_1 \to E_2$ and $\phi : E_2 \to E_1$ (over K) s.t. $\phi \circ \psi = id_{E_1}$ and $\psi \circ \phi = id_{E_2}$. These isogenies are necessarily of degree 1. An isogeny of degree 1 is called an isomorphism.*

Remark. Sometimes we use the term "K-isomorphic" instead of "isomorphic over K".

Note that isomorphism between elliptic curves is "almost" the same as birational equivalence between curves except there is one more condition that those maps have to map base points upon base points.

Theorem 4. *Let ψ be a non-zero isogeny over K between elliptic curves over K.*

(a) There exist polynomials $p, q, r, s \in K[x]$ s.t. $\gcd_{K[x]}(p, q) = 1, \gcd_{K[x]}(r, s) = 1$ and $\psi(x, y) = \left(\frac{p(x)}{q(x)}, y\frac{r(x)}{s(x)}\right)$.

(b) $\deg(\psi) = \max(\deg(p), \deg(q))$.

(c) ψ is separable $\iff \left(\frac{p}{q}\right)' \neq 0$.

Proof. Follows from [Was08] section 2.9 and from the definitions of degree of a rational map and its separability. □

Remark. The rational functions in the previous claim are sometimes called the standard form of an isogeny.

Definition 21. *Let $\psi : E_1 \to E_2$ be a non-zero isogeny (over K) between elliptic curves over K. Define the separability degree of ψ (denoted as $\deg_s(\psi)$) as the degree of separability of the field extension $K(E_1)/\mathrm{Im}(\psi^*)$.*

Similarly define the inseparability degree of ψ (denoted as $\deg_i(\psi)$) as the degree of inseparability of the field extension $K(E_1)/\mathrm{Im}(\psi^*)$.

For a zero isogeny the separability degree and the inseparability degree are defined as 0.

We call ψ separable if $K(E_1)/\mathrm{Im}(\psi^*)$ is a separable field extension. We call ψ inseparable if it is not separable. We call ψ purely inseparable if $K(E_1)/\mathrm{Im}(\psi^*)$ is a purely inseparable field extension.

Remark. Let $\psi : E_1 \to E_2$ be an isogeny (over K) between elliptic curves over K. Then $\deg(\psi) = \deg_s(\psi)\deg_i(\psi)$.

Theorem 5. *Let E_1, E_2 be elliptic curves over K. Let $\phi, \psi \in \mathrm{Hom}_K(E_1, E_2)$. Then a map $\phi \oplus \psi$: $E_1 \to E_2$ defined as:*

$$\forall P \in E_1 : (\phi \oplus \psi)(P) = \phi(P) \oplus_2 \psi(P)$$

where ($\oplus_2$ denotes the binary group operation of E_2) is also an isogeny $E_1 \to E_2$ over K.

Let $\rho \in \mathrm{Hom}_K(E_1, E_1)$ then a map $\ominus\rho : E_1 \to E_1$ defined as:

$$\forall P \in E_1 : (\ominus\rho)(P) = \ominus_1\rho(P)$$

where ($\ominus_1$ denotes the unary group operation of E_1) is also an isogeny $E_1 \to E_1$ over K.

Proof. [Drá21] Theorem T.8. □

Remark. Theorem 5 allows us to interpret isogenies between elliptic curves as a group.

Let $(E, \mathcal{O})$ be an elliptic curve over K. Denote $\mathrm{End}_K(E) = \mathrm{Hom}_K(E, E)$ (endomorphisms of E over K). Due to Theorem 5 we know $\mathrm{End}_K(E)$ is a group and by definition of isogenies $\forall \phi_1, \phi_2 \in \mathrm{End}_K(E) : \phi_1 \circ \phi_2 \in \mathrm{End}_K(E)$. In conclusion $\mathrm{End}_K(E)$ is a ring with operations $(\oplus, \circ)$ and neutral elements $([0], [1])$. An element of this ring is called an endomorphism of E over K.

The set of invertible elements of $\mathrm{End}_K(E)$ forms the automorphism group of E denoted as $\mathrm{Aut}_K(E)$.

Also denote $\mathrm{End}(E) = \mathrm{End}_{\overline{K}}(E)$ and similarly for $\mathrm{Aut}(E)$.

Theorem 6. *Let E_1, E_2 be elliptic curves over K where $\mathrm{char}(K) \notin \{2, 3\}$. Every isomorphism $\phi : E_1 \to E_2$ defined over $\overline{K}$ is of the form:*

$$\phi(x, y) = (u^2x, u^3y)$$

where $u \in \overline{K}$. If $u \in K$, then ϕ is defined over K.

Proof. [Was08] Theorem 2.19. □

Definition 22. *Let E be an elliptic curve over K and $n \in \mathbb{Z}$. By $[n]$ we denote the endomorphism of E over K defined as*

$$n \geq 0 : \forall P \in E : [n](P) = P \oplus \cdots \oplus P \text{ (n times)}$$
$$n < 0 : [n](P) = \ominus([-n](P)).$$

Remark. Using the definition above $[0]$ is the unique zero isogeny of E and $[1]$ is the identity map of E.

We will often use notation $m, n \in \mathbb{Z} : [n + m] = [n] \oplus [m]$ and $[n \cdot m] = [n] \circ [m] = [n][m]$.

Corollary. Let E be an elliptic curve over K. The map

$$\mathbb{Z} \to \mathrm{End}_K(E) : n \mapsto [n]$$

is a ring homomorphism.

Theorem 7. *Let $(E, \mathcal{O})$ be an elliptic curve over $K, m \in \mathbb{Z}$. $[m] = [0] \iff m = 0$ i.e., if $m \neq 0$, then $[m]$ is a non-constant map.*

Proof. [Sil09] Chapter III, Proposition 4.2 (a). □

Corollary. Let E be an elliptic curve over K. Then $\mathrm{End}_K(E)$ is a domain and its characteristic is 0.

Definition 23. *Let $(E, \mathcal{O})$ be an elliptic curve over K and let $m \in \mathbb{N}$. The set of points of E of order which divides m is called the m-torsion subgroup of E. It is denoted by $E[m]$ i.e., $E[m] = \{P \in E : [m](P) = \mathcal{O}\}$.*

Also the torsion subgroup of E is defined and denoted as

$$E_{tors} = \cup_{m=1}^{\infty} E[m].$$

$E[m](K), E_{tors}(K)$ denote the subsets of points of $E[m], E_{tors}$ which are K-rational.

Theorem 8. *Let E_1, E_2 be elliptic curves and let $\psi \in \mathrm{Hom}(E_1, E_2)$ non-constant. Then $\forall P \in E_2 : |\mathrm{Ker}(\psi)| = |\psi^{-1}(P)| = \deg_s(\psi)$.*

Proof. [Drá21] Theorem T.15. □

Corollary. Under the assumptions from Theorem 8. If ψ is separable then $|\mathrm{Ker}(\psi)| = \deg(\psi)$.

Theorem 9. *Let A, B, C be elliptic curves, $\psi \in \mathrm{Hom}(A, B), \phi \in \mathrm{Hom}(A, C)$ non-constant, ψ separable and $\mathrm{Ker}(\psi) \subseteq \mathrm{Ker}(\phi)$. There exists a unique isogeny $\rho \in \mathrm{Hom}(B, C)$ s.t. $\phi = \rho \circ \psi$.*

Proof. [Drá21] Theorem T.18. □

If $\mathrm{char}(K) = 0$ then every isogeny is separable over K. For the other case there is Theorem 10 which decomposes an isogeny into a separable part and a Frobenius map.

Let K be a field s.t. $\mathrm{char}(K) = p$ s.t. p is a prime and E be an elliptic curve over K. Let ϕ be the Frobenius endomorphism of K i.e., $\phi : K \to K : \alpha \mapsto \alpha^p$. We extend this endomorphism to a K-endomorphism Φ of $K[X, Y, Z]$. For $e \in \mathbb{N}$ define $\phi^e = \phi \circ \cdots \circ \phi$ (e times), similarly for Φ. If $E = V_F$ for some $F \in K[X, Y, Z]$ then by $E^{(e)}$ we mean the curve given by $\Phi^e(F)$ i.e., $E^{(e)} = V_{\Phi^e(F)}$. Since Φ is a K-endomorphism we can easily check that $E^{(e)}$ is smooth since E is smooth. Especially in our case if E is a Weierstrass curve, then $j(E^{(e)}) = j(E)^{p^e}$.

Naturally we can define a K-rational map $\boldsymbol{\phi}^e : E \to E^{(e)}, e \in \mathbb{N}$

$$\boldsymbol{\phi}^e = (\Phi^e(X), \Phi^e(Y), \Phi^e(Z)) = (X^{p^e}, Y^{p^e}, Z^{p^e}).$$

We call $\boldsymbol{\phi}^e$ a Frobenius map. Since we assume E to be an elliptic curve (and therefore smooth), then $\boldsymbol{\phi}$ is a morphism.

Theorem 10. *Let $\mathrm{char}(K) = p > 0$, E_1, E_2 elliptic curves over K and $\psi \in \mathrm{Hom}_K(C_1, C_2)$. There exists $e \geq 0 \in \mathbb{Z}$ and $\rho \in \mathrm{Hom}_K(E_1^{(e)}, E_2)$, ρ separable s.t. $\psi = \rho \circ \boldsymbol{\phi}^e$.*

Proof. [Drá21] Theorem T.13. □

Theorem 11. *Let E_1, E_2 be elliptic curves over K, $\psi \in \mathrm{Hom}_K(E_1, E_2)$, ψ non-constant. There exists a unique isogeny $\widehat{\psi} \in \mathrm{Hom}_K(E_2, E_1)$ s.t. $\widehat{\psi} \circ \psi = [\deg(\psi)]$.*

Proof. [Sil09] Chapter III, Theorem 6.1 (a). □

Definition 24. *Under the assumptions from Theorem 11, the isogeny $\widehat{\psi}$ is called the dual isogeny of ψ. It is denoted as $\widehat{\psi}$.*

This next theorem sums up the basic properties of dual isogenies.

Theorem 12. *Let E_1, E_2 be elliptic curves over K, $\psi \in \mathrm{Hom}_K(E_1, E_2), m = \deg(\psi)$, ψ non-constant. Then*

(a) $\widehat{\widehat{\psi}} = \psi$.

(b) $\deg(\psi) = \deg(\widehat{\psi}) = m$.

(c) $\widehat{\psi} \circ \psi = [m] \in \mathrm{End}_K(E_1)$.

(d) $\widehat{[m]} = [m]$.

(e) $\deg([m]) = m^2$.

(f) Let E_3 be another elliptic curve over K and $\phi \in \mathrm{Hom}_K(E_2, E_3)$ non-constant. Then $\widehat{\phi \circ \psi} = \widehat{\psi} \circ \widehat{\phi} \in \mathrm{Hom}_K(E_3, E_1)$.

(g) Let $\rho \in \mathrm{Hom}_K(E_1, E_2)$ be non-constant. Then $\widehat{\phi \oplus \rho} = \widehat{\phi} \oplus \widehat{\rho}$.

Proof. [Sil09] Chapter III, Theorem 6.2. □

Next theorem gives us the structure of m-torsion subgroups.

Theorem 13. *Let $(E, \mathcal{O})$ be an elliptic curve over K and let $m \in \mathbb{N}$. If $\mathrm{char}(K) = 0$ or $\mathrm{char}(K) = p > 0$ s.t. $p \nmid m$, then*

$$E[m] \cong \mathbb{Z}_m \times \mathbb{Z}_m.$$

If $char(K) = p > 0$, then

$$\forall e \in \mathbb{N} : E[p^e] \cong \mathbb{Z}_{p^e}$$
$$or$$
$$\forall e \in \mathbb{N} : E[p^e] = \{\mathcal{O}\}.$$

Proof. [Drá21] Theorem D.5. and Corollary D.6. □

Corollary. Let $H \leq E(\overline{K})$ be a finite subgroup of order $n \in \mathbb{N}$. Let $\mathrm{char}(K) = p$. Then there exist $k, l \in N$ s.t. $k \mid l$ and $p \nmid k$ and $H \cong \mathbb{Z}_k \times \mathbb{Z}_l$.

Proof. Clearly $H \leq E[n]$ (order of every element of H is at most n). If $p \nmid n$ then it is the first case of Theorem 13. Subgroups of $\mathbb{Z}_n \times \mathbb{Z}_n$ can be expressed as $\mathbb{Z}_k \times \mathbb{Z}_l$ with the assumed properties.

Now if $p \mid n$: $n = mp^e$ where $p \nmid m$ and $e \geq 1$. Then using basic properties of abelian groups we have $E[n] \cong E[m] \times E[p^e]$ since $p \nmid m$. Now, we can use Theorem 13 for both cases. $E[m] \cong \mathbb{Z}_m \times \mathbb{Z}_m$ and $E[p^e] \cong \mathbb{Z}_{p^e}$ or $E[p^e] \cong \{\mathcal{O}\}$. In the first case we have

$$E[n] \cong \mathbb{Z}_m \times \mathbb{Z}_m \times \mathbb{Z}_{p^e} \cong \mathbb{Z}_m \times \mathbb{Z}_{mp^e}.$$

If $E[p^e] \cong \{\mathcal{O}\}$, then $E[n] \cong \mathbb{Z}_m \times \mathbb{Z}_m$. □

Definition 25. *Let E_1, E_2, E_2' be elliptic curves over K and let $\psi \in \mathrm{Hom}(E_1, E_2)$, $\phi \in \mathrm{Hom}(E_1, E_2')$. We say ψ and ϕ are K-isomorphic if there exists an isomorphism (an isogeny of degree 1) $\rho \in E_2 \to E_2'$ defined over K s.t.*

$$\rho \circ \psi = \phi.$$

Example 1. Isogenies $[n], [-n] \in \mathrm{End}_K(E)$ are K-isomorphic. In this case $E_1 = E_2 = E_2'$ and $\rho = [-1]$. $[-1]$ is clearly a K-rational map.

Definition 26. *Let E be an elliptic curve over K. Let $H \leq E$ be a subgroup. We say H is defined over K if H is $\mathrm{Gal}(\overline{K}/K)$-invariant i.e., $\forall \rho \in \mathrm{Gal}(\overline{K}/K), \forall P \in H : \rho(P) \in H$.*

Theorem 14. *Let E be an elliptic curve over K and let $H \subseteq E$ be a finite subgroup. Then there exists a unique elliptic curve E' (up to $\overline{K}$-isomorphism) and a unique separable isogeny $\phi \in \mathrm{Hom}(E, E')$ (up to $\overline{K}$-isomorphism) s.t. $\mathrm{Ker}(\phi) = H$. The curve and the isogeny are defined over a finite extension of K.*

If H is defined over K then E' is defined over K and $\phi \in \mathrm{Hom}_K(E, E')$. In this case E' and ϕ are unique up to K-isomorphism.

Proof. We only provide the proof of uniqueness. The proof of existence can be done by verifying Vélu formulae presented in Theorem 16.

Uniqueness: Let $\psi : E \to \widehat{E}$ be another separable isogeny s.t. $\mathrm{Ker}(\psi) = H$. Applying Theorem 9 we get a unique isogeny $\rho : E' \to \widehat{E}$ s.t. $\psi = \rho \circ \phi$. This isogeny must be of degree 1 since ψ and ϕ have the same degree (due to separability and same kernel). In other words, ρ is an isomorphism.

If H is defined over K then so are ψ, ϕ, E' and $\widehat{E}$ and subsequently ρ must be also defined over K i.e., it is a K-isomorphism. □

Remark. The elliptic curve E' from Theorem 14 is often denoted as E/H.

Theorem 15. *Let E, E' be elliptic curves over $K, \psi \in \mathrm{Hom}_K(E, E')$. There exist $n \in \mathbb{N}$ and $1 \leq i \leq n : \lambda_i$ isogenies of degree p_i where p_i is prime s.t.*

$$\psi = \lambda_1 \circ \cdots \circ \lambda_n.$$

Proof. This is an expanded version of the proof in [Gal12], Theorem 25.1.2.

We can assume that ψ is separable because if $\mathrm{char}(K) = 0$ then every isogeny is separable. If $\mathrm{char}(K) = p > 0$ then by Theorem 10 we can decompose $\psi = \psi' \circ \boldsymbol{\phi}^e$

for some $e \geq 0$ where ψ' is separable and defined over K since $\boldsymbol{\phi}^e$ is defined over K and $\deg(\boldsymbol{\phi}) = p$.

By Theorem 14 ψ is determined by its kernel. Let $G = \mathrm{Ker}(\psi)$. If there exists $n \in \mathbb{Z}$ s.t. $E[n] \leq G$ then by Theorem 9 we can decompose $\psi = \psi' \circ [n]$.

$[n]$ can be decomposed into isogenies of prime degree in the following way since n can be factored into primes. Let l be a prime, $[l]$ has a kernel $G \geq E[l] \cong \mathbb{Z}_l \times \mathbb{Z}_l$. We can take a point of order l from $E[l]$ which will define a separable isogeny ψ with $\mathrm{Ker}(\psi) \leq E[l]$. By Theorem 9 we get ψ' s.t. $[l] = \psi' \circ \psi$ where ψ is clearly defined over K and of degree l (same for ψ').[1]

From now on assume there doesn't exist an $n \in \mathbb{N}$ s.t. $E[n] \leq G$.

Let l be a prime s.t. $l \mid |G|$. There exists $P \in G$ of order l which forms a subgroup $\langle P \rangle$ of order l.

First, we want to show that $\langle P \rangle$ is defined over K. G is assumed to be defined over K i.e., for any $\sigma \in \mathrm{Gal}(\overline{K}/K) : \sigma(P) \in G$. But clearly by properties of σ the point $\sigma(P)$ also has an order l i.e., $\sigma(P) \in E[l] \cong \mathbb{Z}_l \times \mathbb{Z}_l$. If $l = \mathrm{char}(K)$, then we have a contradiction because either $E[l] = \mathbb{Z}_l$ which would mean that $E[l] \leq G$ or $E[l] = \{\mathcal{O}\}$.

Therefore $E[l] \nleq G$ and $\mathbb{Z}_l \cong \langle P \rangle \leq G$. Thus $\sigma(P)$ (which also generates a subgroup of prime order) must generate the same as P i.e., $\sigma(P) \in \langle P \rangle$.

Now we use Theorem 14 to get an isogeny $\psi_1 : E \to E_1 = E/\langle P \rangle$ s.t. $\mathrm{Ker}(\psi_1) = \langle P \rangle$. This isogeny is defined over K due to our previous paragraph. Consider the image of $G \leq E(\overline{K})$ under ψ_1. Since isogeny is (more precisely induces) a group homomorphism, we can see that by first isomorphism theorem $\psi_1(G) \leq E_1(\overline{K})$ and $\psi_1(G) \cong G/\langle P \rangle$.

Consider another isogeny $\psi_2 : E_1 \to E_2$ s.t. $\mathrm{Ker}(\psi_2) = \psi_1(G) \cong G/\langle P \rangle$. Let's look at $\psi_2 \circ \psi_1$. By definition $\mathrm{Ker}(\psi_2 \circ \psi_1) = G$ thus by Theorem 14 there must exist a K-isomorphism $\lambda : E_2 \to E'$ s.t. $\psi = \lambda \circ \psi_2 \circ \psi_1$. This can be also seen with a little bit of abusing the notation:

$$\begin{gathered}
\psi_2 \circ \psi_1 : E \to E_1 \to E_2 \\
E_1 = E/\langle P \rangle \\
E_2 = E_1/\psi_1(G) = (E/\langle P \rangle)/\psi_1(G) \cong (E/\langle P \rangle)/(G/\langle P \rangle) \cong E/G \\
\iff \\
\psi_2 \circ \psi_1 \cong \psi : E \to E/G.
\end{gathered}$$

ψ_1 has prime degree. Repeat the steps for $\lambda \circ \psi_2$. This process will eventually end since we always lower the degree. □

Since every isogeny can be decomposed into isogenies of prime degree, we present only a simplified version of Vélu formulae concerning only kernels of odd order. Note that there exist formulae also for a kernel of order 2. For details see [Sut19], Lecture 6, Theorem 6.13 (we present the Theorem 6.15).

Note that these formulae are specific to the model of the elliptic curve. In our case we use the short Weierstrass form but these formulae can be modified to work, for example, for Montgomery curves.

[1] This part is a proof of the existence of a dual isogeny.

Theorem 16 (Vélu). *Let E be an elliptic curve over K given by $y^2 = x^3 + Ax + B$ and let $G \leq E(\overline{K})$ be a subgroup of an odd order. For any $P \in E(\overline{K})$ denote by x_P its affine x-coordinate and similarly for y_P. $\forall P = (x_P, y_P) \in G$ define:*

$$t_P = 3x_P^2 + A,$$
$$u_P = 2y_P^2,$$
$$w_P = u_P + t_P x_P,$$

and also define:

$$t = \sum_{P \in G \setminus \{\mathcal{O}\}} t_P,$$
$$w = \sum_{P \in G \setminus \{\mathcal{O}\}} w_P,$$
$$r(x) = x + \sum_{P \in G \setminus \{\mathcal{O}\}} \left(\frac{t_P}{x - x_P} + \frac{u_P}{(x - x_P)^2} \right).$$

Then the rational map $\psi = (r(x), r'(x)y)$, where $r'(x)$ is the derivative of $r(x)$, defines a separable isogeny $E \to E'$ s.t. $\mathrm{Ker}(\psi) = G$ where E' is given by $y^2 = x^3 + A'x + B'$, where $A' = A - 5t, B' = B - 7w$.

Proof. A modified version of [Gal12] Theorem 25.1.6. □

Remark. Since y_P^2 can be expressed as a combination of x_P, during the computation we only need to work with x-coordinates of points of G.

In the following claim we automatically assume (as stated at the beginning of this chapter) that $q = p^e$ for some p prime and $e \in \mathbb{N}$.

Claim 17. *Under the assumptions of Theorem 16. If $K = \mathbb{F}_q$ and $\boldsymbol{\phi}^e(G) = G$, then E' and ψ are defined over $\mathbb{F}_q$.*

Proof. Since $\boldsymbol{\phi}^e$ permutes the coordinates of points in G, then we can see that the formulae for $t, w, r(x)$ are the same when the order of points is changed. From that we can see that the coefficients A', B' and also the rational functions of ϕ are fixed by $\boldsymbol{\phi}^e$ i.e., they are elements of $\mathbb{F}_q$. □

Example 2 (Isogeny computation with predefined kernel). Let $E : y^2 = x^3 + x + 1$ ($A = 1 = B$) and $K = \mathbb{F}_{101}$. Assume we know a point $P = (46, 25) \in E(\mathbb{F}_{101})$ is of order 5 i.e., $G = \langle P \rangle \leq E(\mathbb{F}_{101})$ is a subgroup of order 5.

We want to compute the isogeny $\psi : E \to E'$ with kernel G using Theorem 16 where $E' : y^2 = x^3 + A'x + B'$.

First, we compute G:

$$G = \{\mathcal{O}, P, 2P, 3P, 4P\} = \{\mathcal{O}, P, 2P, -2P, -P\}$$
$$= \{(0, 1), (46, 25), (86, 67), (86, 34), (46, 76)\}.$$

Next let's calculate $t, w, r(x)$:

Point P	t_P	u_P	w_P
P	87	38	0
$2P$	70	90	50
$3P$	70	90	50
$4P$	87	38	0

$$t = 2(87 + 70) = 11, w = 2(0 + 50) = 100 = -1$$
$$\Longrightarrow$$
$$A' = 47, B' = 8,$$
$$r(x) = x + 2\left(\frac{87}{x - 46} + \frac{38}{(x - 46)^2}\right) + 2\left(\frac{70}{x - 86} + \frac{90}{(x - 86)^2}\right).$$

After transforming $r(x)$ into the standard form (s.t. the numerator and the denominator are coprime) we get a form:

$$r(x) = \frac{x^5 + 39x^4 + 97x^3 + 81x^2 + 88x + 75}{x^4 + 39x^3 + 86x^2 + 57x + 87},$$
$$r(x)' = \frac{x^6 + 8x^5 + 95x^4 + 89x^3 + 37x^2 + 31x + 86}{x^6 + 8x^5 + 5x^4 + 74x^3 + 85x^2 + 90x + 65}.$$

We have completed the calculation. Now we have an explicit form of $\psi = (r(x), yr(x)')$. This is an isogeny between curves $y^2 = x^3+x+1$, $y^2 = x^3+47x+8$ and is of degree 5 with kernel G.

2. Supersingular curves and endomorphism ring

Most of this chapter follows [Sut19], Lectures 6, 13, 14. We provide some paraphrased proofs from these lectures because we feel they are needed to paint a better picture of the theory.

Definition 27. *Let $(E, \mathcal{O})$ be an elliptic curve over K, $\mathrm{char}(K) = p > 0$. We say E is supersingular if $\exists e \in \mathbb{N}$ s.t. $E[p^e] = \{\mathcal{O}\}$. If E is not supersingular we say E is ordinary.*

Remark. Due to Theorem 13 if $\exists e \in \mathbb{N}$ s.t. E is supersingular, then $\forall n \in \mathbb{N}$: $E[p^n] = \{\mathcal{O}\}$.

Theorem 18. *Let $(E_1, \mathcal{O}_1), (E_2, \mathcal{O}_2)$ be elliptic curves over K s.t. they are isogenous by $\psi \in \mathrm{Hom}_K(E_1, E_2)$. Then E_1 is supersingular iff E_2 is supersingular.*

Proof. This proof is a paraphrased version of [Sut19], Lecture 14, Theorem 14.2.

By definition E_1 is supersingular iff $\mathrm{Ker}([p]_1) = \{\mathcal{O}_1\} \iff \deg_s([p]_1) = 1$ by Theorem 8. Since all of the following maps are isogenies, we have:

$$\begin{gathered}
[p]_2 \circ \psi = \psi \circ [p]_1 \implies \\
\deg_s([p]_2 \circ \psi) = \deg_s(\psi \circ [p]_1) \\
\iff \\
\deg_s([p]_2)\deg_s(\psi) = \deg_s(\psi)\deg_s([p]_1) \\
\iff \\
\deg_s([p]_2) = \deg_s([p]_1).
\end{gathered}$$

Thus $\deg_s([p]_2) = 1$ as well. □

Theorem 19. *Let E be an elliptic curve over K, $\psi \in \mathrm{End}_K(E)$. Then*

$$\psi \oplus \hat{\psi} = [1] \oplus [\deg(\psi)] \ominus [\deg([1] \ominus \psi)].$$

Proof. This proof is an expanded version of [Sut19], Lecture 7, Lemma 7.16.

Using Theorem 12 (c) and (f) we have $[\deg([1] \ominus \psi)] = (\widehat{[1] \ominus \psi}) \circ ([1] \ominus \psi) = (\widehat{[1]} \ominus \hat{\psi}) \circ ([1] \ominus \psi) = ([1] \ominus \hat{\psi}) \circ ([1] \ominus \psi)$. Now only using the arithmetic of $\mathrm{End}_K(E)$ and (c) we get:

$$\begin{gathered}
([1] \ominus \hat{\psi}) \circ ([1] \ominus \psi) = ([1] \circ [1]) \ominus ([1] \circ \psi) \ominus (\hat{\psi} \circ [1]) \oplus (\hat{\psi} \circ \psi) = \\
= [1] \ominus \psi \ominus \hat{\psi} \oplus [\deg(\psi)] = [1] \ominus (\psi \oplus \hat{\psi}) \oplus [\deg(\psi)] \implies \\
[\deg([1] \ominus \psi)] = [1] \ominus (\psi \oplus \hat{\psi}) \oplus [\deg(\psi)] \\
\iff \\
\psi \oplus \hat{\psi} = [1] \oplus [\deg(\psi)] \ominus [\deg([1] \ominus \psi)].
\end{gathered}$$

□

Corollary. There exists a unique $n \in \mathbb{N}$ s.t. $\psi \oplus \widehat{\psi} = [n]$. Specifically, $n = 1 + \deg(\psi) - \deg([1] \ominus \psi)$.

Definition 28. *Let E be an elliptic curve over K, $\psi \in \mathrm{End}_K(E)$. Then the trace of ψ (denoted as $\mathrm{Tr}(\psi)$) is defined as $\mathrm{Tr}(\psi) = 1 + \deg(\psi) - \deg([1] \ominus \psi)$.*

Remark. Using Theorem 12 (d), (f) we get that $\mathrm{Tr}(\psi) = \mathrm{Tr}(\widehat{\psi})$ because $\psi \oplus \widehat{\psi} = [\mathrm{Tr}(\psi)] = \widehat{[\mathrm{Tr}(\psi)]} = \widehat{\psi \oplus \widehat{\psi}} = \widehat{\psi} \oplus \widehat{\widehat{\psi}} (= \widehat{\psi} \oplus \psi)$.

Also let $\tau \in \mathrm{End}_K(E)$, then $\mathrm{Tr}(\psi \oplus \tau) = \mathrm{Tr}(\psi) + \mathrm{Tr}(\tau)$ because $[\mathrm{Tr}(\psi \oplus \tau)] = (\psi \oplus \tau) \oplus \widehat{(\psi \oplus \tau)} = \psi \oplus \tau \oplus \widehat{\psi} \oplus \widehat{\tau} = \psi \oplus \widehat{\psi} \oplus \tau \oplus \widehat{\tau} = [\mathrm{Tr}(\psi)] \oplus [\mathrm{Tr}(\tau)] = [\mathrm{Tr}(\psi) + \mathrm{Tr}(\tau)]$.

We have shown that $\mathrm{End}_K(E)$ is a ring. It can be looked at as a $\mathbb{Z}$-algebra with operations $(\oplus, \circ)$. We will now extend this algebra into a $\mathbb{Q}$-algebra using a tensor product of algebras.

Remark. If R is an integral domain, A is a R-algebra and B is the fraction field of R, then every element of $A \otimes_R B$ can be expressed as $a \otimes b$ for some $a \in A, b \in B$.

Definition 29. *Let E be an elliptic curve over K. The endomorphism algebra of E is $\mathrm{End}^0_K(E) = \mathrm{End}_K(E) \otimes_{\mathbb{Z}} \mathbb{Q}$.*

Using the previous remark, we can see that every element of $\mathrm{End}^0_K(E)$ can be expressed as $\psi \otimes a$ where $\psi \in \mathrm{End}_K(E), a \in \mathbb{Q}$. $\mathrm{End}^0_K(E)$ is also clearly a $\mathbb{Q}$-algebra.

Lemma 20. *$\mathrm{End}^0_K(E)$ is a domain.*

Proof. Assume $(\psi \otimes a)(\tau \otimes b) = 0$ and ψ, τ non-zero in $\mathrm{End}_K(E)$ and $a, b \neq 0 \in \mathbb{Q}$.

$$(\psi \otimes a)(\tau \otimes b) = (\psi \circ \tau) \otimes (ab).$$

So, either $\psi \circ \tau = [0] \in \mathrm{End}_K(E)$ or $ab = 0 \in \mathbb{Q}$. Since all of them are assumed to be non-zero and $\mathbb{Q}$ is clearly a domain and so is $\mathrm{End}_K(E)$ by Theorem 7 we have a contradiction. □

Because $\mathbb{Q}$ and $\mathrm{End}_K(E)$ are torsion-free $\mathbb{Z}$-algebras, there exist injective homomorphisms which identify elements of $\mathrm{End}_K(E)$ and $\mathbb{Q}$ with elements of $\mathrm{End}^0_K(E)$:

$$\begin{aligned} \boldsymbol{\alpha} : \mathrm{End}_K(E) &\to \mathrm{End}^0_K(E), \\ \psi &\mapsto \psi \otimes 1, \\ \boldsymbol{\beta} : \mathbb{Q} &\to \mathrm{End}^0_K(E), \\ a &\mapsto [1] \otimes a. \end{aligned}$$

Note that since $\mathrm{End}_K(E)$ is a $\mathbb{Z}$-algebra we have an overlap of images of these two injective maps. For example $\boldsymbol{\alpha}([2]) = [2] \otimes 1 = (2[1]) \otimes 1 = [1] \otimes 2 = \boldsymbol{\beta}(2)$.

From now on we will use a simplified notation for elements of $\mathrm{End}^0_K(E)$. For $a \in \mathbb{Q}, \psi \in \mathrm{End}_K(E)$: $a\psi$ corresponds to the element $\psi \otimes a$. Also, we extend the definition of a dual isogeny on these elements as follows: $\widehat{a\psi} = a\widehat{\psi}$. Also, since we have an embedding of $\mathbb{Q}$ and $\mathrm{End}_K(E)$ into $\mathrm{End}^0_K(E)$, we consider them subsets of $\mathrm{End}^0_K(E)$.

Claim 21. *Let $a \in \mathbb{Q}$. Consider a as an element of $\mathrm{End}_K^0(E)$ i.e., $a = a[1] = \beta(a)$ in the notation above. Then for every $x \in \mathrm{End}_K^0(E)$: $xa = ax$.*

Proof. $x = b\psi, b \in \mathbb{Q}, \psi \in \mathrm{End}_K(E)$. Then using the fact that $[n] \circ \psi = \psi \circ [n]$ for $n \in \mathbb{N}, \psi \in \mathrm{End}_K(E)$:

$$xa = (\psi \otimes b)([1] \otimes a) = (\psi \circ [1]) \otimes (ba) = ([1] \circ \psi) \otimes (ab) = \\ = ([1] \otimes a)(\psi \otimes b) = ax.$$

□

We will also extend the definition of Tr and define the norm N.

Definition 30. *Let $x = a\psi \in \mathrm{End}_K^0(E)$. Define the norm of x as the element $\mathrm{N}(x) = x \cdot \widehat{x}$. Define the trace of x as the element $\mathrm{Tr}(x) = x + \widehat{x}$.*

Lemma 22. *Let $x \in \mathrm{End}_K^0(E)$. Then:*

(a) $\mathrm{N}(x) \geq 0 \in \mathbb{Q}$.

(b) $\mathrm{N}(x) = 0 \iff x = 0$.

(c) $\mathrm{N}(x) = \mathrm{N}(\widehat{x})$.

(d) $y \in \mathrm{End}_K^0(E) : \mathrm{N}(xy) = \mathrm{N}(x)\mathrm{N}(y)$.

Proof. This proof is an expanded version of [Sut19], Lecture 13, Lemma 13.7.

$x = a\psi$ for some $a \in \mathbb{Q}, \psi \in \mathrm{End}_K(E)$ then using the definitions and Theorem 12 (c)

$$x \cdot \widehat{x} = a\psi \cdot a\widehat{\psi} = (\psi \otimes a)(\widehat{\psi} \otimes a) = (\psi \circ \widehat{\psi}) \otimes a^2 = \\ = [\deg(\psi)] \otimes a^2 = [1] \otimes (a^2 \deg(\psi)).$$

So, we identify $\mathrm{N}(x)$ with the rational number $a^2 \deg(\psi)$, which is always non-negative. This proves (a) and (b) follows using $\deg(\psi) = 0 \iff \psi = [0]$.

Consider the element $x \cdot \mathrm{N}(\widehat{x})$ and use Claim 21:

$$x \cdot \mathrm{N}(\widehat{x}) = (\psi \otimes a)\mathrm{N}(\widehat{x}) = (\psi \otimes a)(\widehat{\psi} \otimes a)(\psi \otimes a) = \mathrm{N}(x)(\psi \otimes a) = \\ = (\psi \otimes a)\mathrm{N}(x).$$

Now, thanks to $\mathrm{End}_K^0(E)$ being a domain, we get $x \cdot \mathrm{N}(\widehat{x}) = x \cdot \mathrm{N}(x) \iff \mathrm{N}(\widehat{x}) = \mathrm{N}(x)$. This proves (c).

For the rest, we use Theorem 12 (f) and Claim 21:

$$\mathrm{N}(xy) = xy \cdot \widehat{xy} = xy \cdot \widehat{y}\widehat{x} = x \cdot \mathrm{N}(y) \cdot \widehat{x} = x\widehat{x} \cdot \mathrm{N}(y) = \mathrm{N}(x)\mathrm{N}(y).$$

□

Tr has similar properties. We list them without proof since the proof uses the same techniques as the previous claim.

Lemma 23. *Let $x \in \mathrm{End}_K^0(E)$. Then:*

(a) $\mathrm{Tr}(x) \in \mathbb{Q}$.

(b) $\mathrm{Tr}(x) = \mathrm{Tr}(\widehat{x})$.

(c) $y \in \mathrm{End}^0(E) : \mathrm{Tr}(x+y) = \mathrm{Tr}(x) + \mathrm{Tr}(y)$.

(d) $a \in \mathbb{Q} : \mathrm{Tr}(ax) = a\mathrm{Tr}(x)$.

Lemma 24. $\mathrm{End}_K^0(E)$ *is a division ring i.e.,* $\forall x \in \mathrm{End}_K^0(E) : \exists! x^{-1} \in \mathrm{End}_K^0(E) : x^{-1}x = xx^{-1} = 1$.

Proof. This proof is a paraphrased version of [Sut19], Lecture 13, Lemma 13.8.
Let $x \in \mathrm{End}_K^0(E)$. Set $y = \frac{1}{\mathrm{N}(x)}\widehat{x}$. Then using Claim 21:

$$xy = x\frac{1}{\mathrm{N}(x)}\widehat{x} = \frac{1}{\mathrm{N}(x)}x\widehat{x} = \frac{1}{\mathrm{N}(x)}\mathrm{N}(x) = 1 = yx.$$

□

Definition 31. *Let* $\psi \in \mathrm{End}_K^0(E)$. *The characteristic polynomial of* ψ *is the polynomial:*

$$x^2 - \mathrm{Tr}(\psi)x + \mathrm{N}(\psi) \in \mathbb{Q}[x].$$

Remark. If $\psi \in \mathrm{End}_K(E)$ then the characteristic polynomial of ψ is a polynomial in $\mathbb{Z}[x]$ due to the way that ψ is embedded into $\mathrm{End}_K^0(E)$.

Remark. If $\psi \in \mathrm{End}_K(E)$ then the characteristic polynomial of ψ can be written as:

$$x^2 - \mathrm{Tr}(\psi)x + \deg(\psi) \in \mathbb{Z}[x].$$

since $\mathrm{N}(\psi) = \psi\widehat{\psi} = [\deg(\psi)]$.

Lemma 25. *Let* $\psi \in \mathrm{End}_K^0(E)$. *Then* $\psi, \widehat{\psi}$ *are the roots of the characteristic polynomial of* ψ *in* $\mathrm{End}_K^0(E)$.

Proof. This proof is a paraphrased version of [Sut19], Lecture 13, Lemma 13.10.
Using the arithmetic of $\mathrm{End}_K^0(E)$:

$$0 = (\psi - \psi)(\psi - \widehat{\psi}) = \psi^2 - \psi\widehat{\psi} - \psi^2 + \psi\widehat{\psi} =$$
$$= \psi^2 - \psi(\widehat{\psi} + \psi) + \mathrm{N}(\psi) = \psi^2 - \psi\mathrm{Tr}(\psi) + \mathrm{N}(\psi) = \psi^2 - \mathrm{Tr}(\psi)\psi + \mathrm{N}(\psi).$$

For $\widehat{\psi}$ the proof is similar because the trace and norm are the same for dual isogenies. □

Definition 32. *An algebra* $\mathcal{Q}$ *over a field* K *is a quaternion algebra if there exist* $i, j \in \mathcal{Q}$ *s.t.* $\{1, i, j, ij\}$ *is a basis of* $\mathcal{Q}$ *and* $i^2, j^2 \in \mathbb{Q}^*$, $-ij = ji$.

Consider the subspace Q_0 of $\mathcal{Q}$ generated by $\{1\}$ and let Q_1 be the subspace of $\mathcal{Q}$ generated by $\{i, j, ij\}$. Every element $\alpha \in \mathcal{Q}$ can be decomposed into $\alpha = \alpha_0 + \alpha_1$ where $\alpha_0 \in Q_0, \alpha_1 \in Q_1$. Define $\widehat{\alpha} = \alpha_0 - \alpha_1$ and call it the conjugate of α. Using this conjugate map, we can similarly define a trace and a norm on $\mathcal{Q}$.

For $\alpha \in \mathcal{Q}$ define $\mathrm{Tr}(\alpha) = \alpha + \widehat{\alpha}$ and $\mathrm{N}(\alpha) = \alpha\widehat{\alpha}$. It can be shown that they have the same properties as their counterparts in $\mathrm{End}_K^0(E)$. Let $\alpha, \beta \in \mathcal{Q}$, then $\mathrm{Tr}(\alpha), \mathrm{N}(\alpha) \in K$ and $\mathrm{Tr}(\alpha + \beta) = \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta), \mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta)$.

Theorem 26. *Let E be an elliptic curve over K. $\mathrm{End}_K^0(E)$ is isomorphic to one of the following:*

(a) The field $\mathbb{Q}$.

(b) An imaginary quadratic field $\mathbb{Q}(i), i^2 < 0$.

(c) A quaternion algebra $\mathbb{Q}(i,j), i^2 < 0, j^2 < 0$.

Proof. [Sut19] Lecture 13, Theorem 13.17. □

Theorem 27. *Let E be an elliptic curve over K. $\mathrm{End}_K(E)$ is a free $\mathbb{Z}$-module of rank r where $r = \dim_{\mathbb{Q}}(\mathrm{End}_K^0(E))$ and $r \in \{1, 2, 4\}$.*

Proof. [Sut19] Lecture 13, Corollary 13.20. □

Corollary. $\mathrm{End}_K(E)$ is an order in $\mathrm{End}_K^0(E)$.

Proof. By definition $\mathrm{End}_K^0(E)$ is $\mathbb{Q}$-algebra and Theorem 26 tells us its dimension is finite. $\mathrm{End}_K(E)$ is clearly is subring of $\mathrm{End}_K^0(E)$ (more precisely the image of $\boldsymbol{\alpha}$). Using Theorem 27 we get that $\mathrm{End}_K(E)$ is a $\mathbb{Z}$-module of the same rank (as the dimension). □

For practical purposes we have to work with finite fields $\mathbb{F}_q$ where $q = p^e$ where p is prime and $e \in \mathbb{N}$. We will introduce a few properties specific to curves over finite fields.

From now on, assume $q = p^e$ where p is prime and $e \in \mathbb{N}$.

Since $K = \mathbb{F}_q$ is a perfect field, then $\boldsymbol{\phi}^e$ is an identity on K which implies $E = E^{(e)}$ for any elliptic curve E over K.

Remark. Let E be an elliptic curve over $\mathbb{F}_q$. Then $\boldsymbol{\phi}^e$ (as defined above) is an element of $\mathrm{End}(E)$.

This does not necessarily mean that $\mathrm{End}(E)$ cannot be isomorphic to $\mathbb{Z}$.

Theorem 28. *Let E be an elliptic curve over $K = \mathbb{F}_q$, $n \in \mathbb{Z}$. Then $[n] \in \mathrm{End}_K E$ is inseparable $\iff p \mid n$.*

Proof. [Sil09] Chapter III, Corollary 5.5. □

Theorem 29. *Let E_1, E_2 be elliptic curves over $K = \mathbb{F}_q$ and $\psi, \rho \in \mathrm{Hom}_K(E_1, E_2)$. Assume ψ is inseparable, then $\psi \oplus \rho$ is inseparable $\iff$ ρ is inseparable.*

In other words, the sum of two inseparable isogenies is inseparable. The sum of an inseparable isogeny and separable is separable.

Proof. Applying Theorem 10 we get that there exist $n_1, n_2 \in \mathbb{Z} : n_1 > 0, n_2 \geq 0$, $\lambda_1 \in \mathrm{Hom}_K(E_1^{(n_1)}, E_2)$ and $\lambda_2 \in \mathrm{Hom}_K(E_1^{(n_2)}, E_2)$ s.t. λ_1, λ_2 separable:

$$\begin{gathered}\psi = \lambda_1 \circ \boldsymbol{\phi}^{n_1}, \\ \rho = \lambda_2 \circ \boldsymbol{\phi}^{n_2} \\ \Longrightarrow \\ \psi \oplus \rho = (\lambda_1 \circ \boldsymbol{\phi}^{n_1}) \oplus (\lambda_2 \circ \boldsymbol{\phi}^{n_2}).\end{gathered}$$

If ρ is inseparable then $n_2 > 0$ and

$$\psi \oplus \rho = ((\lambda_1 \circ \boldsymbol{\phi}^{n_1-1}) \oplus (\lambda_2 \circ \boldsymbol{\phi}^{n_2-1})) \circ \boldsymbol{\phi}$$

which is clearly inseparable (for example because the degree of a composition is a product of degrees).

If $\psi \oplus \rho$ is inseparable then $\ominus(\psi \oplus \rho)$ is also inseparable. Then $\psi \oplus (\ominus(\psi \oplus \rho)) = \ominus\rho$ is inseparable (since it's a sum of two inseparable isogenies which we have just proved). Also $\ominus\rho$ is inseparable $\iff$ ρ is inseparable. □

Theorem 30. *Let E be an elliptic curve over $\mathbb{F}_q$. E is supersingular iff* $\mathrm{Tr}(\boldsymbol{\phi}^e) \equiv 0 \mod p$.

Proof. This proof is an expanded version of [Sut19], Lecture 14, Theorem 14.3.

It can be easily shown that $[p] = \widehat{\boldsymbol{\phi}} \circ \boldsymbol{\phi}$. E is supersingular iff $\deg_s([p]) = 1$ (proof of Theorem 18) also $\deg(\widehat{\boldsymbol{\phi}}) = \deg(\boldsymbol{\phi}) = p$. Therefore, E is supersingular $\implies$ $\deg_s([p]) = \deg_s(\widehat{\boldsymbol{\phi}}) = 1 \implies \deg_i(\widehat{\boldsymbol{\phi}}) > 1$ i.e., $\widehat{\boldsymbol{\phi}}$ is inseparable. By definition and using properties of dual isogenies $[\mathrm{Tr}(\boldsymbol{\phi}^e)] = \boldsymbol{\phi}^e \oplus \widehat{\boldsymbol{\phi}}^e \iff [\mathrm{Tr}(\boldsymbol{\phi}^e)] \ominus \boldsymbol{\phi}^e = \widehat{\boldsymbol{\phi}}^e$. If $\widehat{\boldsymbol{\phi}}$ is inseparable, then also $\widehat{\boldsymbol{\phi}}^e$ is inseparable. Therefore, $[\mathrm{Tr}(\boldsymbol{\phi}^e)] \ominus \boldsymbol{\phi}^e$ is inseparable and, by Theorem 29, it must be that $[\mathrm{Tr}(\boldsymbol{\phi}^e)]$ is inseparable since $\ominus\boldsymbol{\phi}^e$ is inseparable. Finally, by Theorem 28, it must be that $p \mid \mathrm{Tr}(\boldsymbol{\phi}^e) \iff \mathrm{Tr}(\boldsymbol{\phi}^e) \equiv 0 \mod p$.

On the other hand, $p \mid \mathrm{Tr}(\boldsymbol{\phi}^e) \implies \widehat{\boldsymbol{\phi}}^e$ inseparable $\implies \widehat{\boldsymbol{\phi}}$ inseparable $\iff \deg_i(\widehat{\boldsymbol{\phi}}) > 1 \implies \deg_s(\widehat{\boldsymbol{\phi}}) = 1$ and $\boldsymbol{\phi}$ is always inseparable so $\deg_s(\boldsymbol{\phi}) = 1$. This leaves the only option for $\deg_s([p]) = 1$ which is equivalent to saying E is supersingular. □

Theorem 31. *Let E be an elliptic curve over $\mathbb{F}_q$. Then $|E(\mathbb{F}_q)| = q + 1 - \mathrm{Tr}(\boldsymbol{\phi}^e)$ and $|\mathrm{Tr}(\boldsymbol{\phi}^e)| \leq 2\sqrt{q}$.*

Proof. [Sil09] Chapter V, Theorem 1.1. □

Claim 32. *Let E be an elliptic curve over $\mathbb{F}_p$, $p > 3$. E is supersingular $\iff$* $\mathrm{Tr}(\boldsymbol{\phi}) = 0 \iff |E(\mathbb{F}_p)| = p + 1$.

Proof. The equivalence $\mathrm{Tr}(\boldsymbol{\phi}) = 0 \iff |E(\mathbb{F}_p)| = p + 1$ is a straight up consequence of Theorem 31 in case $q = p$.

If $\mathrm{Tr}(\boldsymbol{\phi}) = 0$ then by Theorem 30 E is supersingular.

On the other hand, assume E is supersingular. Again, Theorem 30 tells us that $\mathrm{Tr}(\boldsymbol{\phi}) \equiv 0 \mod p$ i.e., $\mathrm{Tr}(\boldsymbol{\phi}) = kp$ for some $k \in \mathbb{Z}$. The other result of Theorem 31 gives us that $|kp| \leq 2\sqrt{p} \iff |k|\sqrt{p} \leq 2$. Clearly for any $p > 5$ this does not hold unless $k = 0 \iff \mathrm{Tr}(\boldsymbol{\phi}) = 0$. □

The structure of the group of $E(\mathbb{F}_q)$ for a supersingular elliptic curve is given by the following theorem.

Theorem 33. *Let E be a supersingular elliptic curve over $\mathbb{F}_q$. Then*

(a) If $\mathrm{Tr}(\boldsymbol{\phi}^e)^2 \in \{q, 2q, 3q\}$, then $E(\mathbb{F}_q)$ is cyclic.

(b) If $\mathrm{Tr}(\boldsymbol{\phi}^e)^2 = 4q$, then we have two possible cases.

(a) If $\mathrm{Tr}(\boldsymbol{\phi}^e) = 2\sqrt{q}$, then $E(\mathbb{F}_q) \cong \mathbb{Z}_{\sqrt{q}-1} \times \mathbb{Z}_{\sqrt{q}-1}$.

(b) If $\mathrm{Tr}(\boldsymbol{\phi}^e) = -2\sqrt{q}$*, then* $E(\mathbb{F}_q) \cong \mathbb{Z}_{\sqrt{q}+1} \times \mathbb{Z}_{\sqrt{q}+1}$.

(c) If $\mathrm{Tr}(\boldsymbol{\phi}^e) = 0$*, then either* $E(\mathbb{F}_q)$ *is cyclic or* $E(\mathbb{F}_q) \cong \mathbb{Z}_2 \times \mathbb{Z}_{\frac{q+1}{2}}$.

Proof. [Sch87] Lemma 4.8. □

Lemma 34. *Let* $\alpha, \beta \in \mathrm{End}_K^0(E), \alpha \notin \mathbb{Q}$ *where* E *is an elliptic curve over* K*. If* $\alpha\beta = \beta\alpha$*, then* $\beta \in \mathbb{Q}(\alpha)$*. Also, if* α *and* $\mathrm{Tr}(\alpha) = 0$*, then* $\alpha^2 = -\mathrm{N}(\alpha) < 0$.

Proof. This proof is an expanded version of [Sut19], Lecture 13, Corollary 13.11 and Lemma 13.18.

α is a root of its characteristic polynomial by Claim 25 i.e., $\alpha^2 - \mathrm{Tr}(\alpha)\alpha + \mathrm{N}(\alpha) = 0 \iff \alpha^2 = -\mathrm{N}(\alpha)$. α^2 is non-zero because $\mathrm{End}_K^0(E)$ is a division ring and α is non-zero (because $\alpha \notin \mathbb{Q}$). By Lemma 22 $-\mathrm{N}(\alpha) < 0$ since α is non-zero.

W.l.o.g. we can assume that $\mathrm{Tr}(\alpha) = 0 = \mathrm{Tr}(\beta)$ because we can replace α with $\alpha - \frac{\mathrm{Tr}(\alpha)}{2}$ and by properties of the trace:

$$\mathrm{Tr}\left(\alpha - \frac{\mathrm{Tr}(\alpha)}{2}\right) = \mathrm{Tr}(\alpha) - \frac{\mathrm{Tr}(\mathrm{Tr}(\alpha))}{2}$$
$$\mathrm{Tr}(\mathrm{Tr}(\alpha)) = \mathrm{Tr}(\alpha + \widehat{\alpha}) = 2(\alpha + \widehat{\alpha}) = 2\mathrm{Tr}(\alpha) \implies$$
$$\mathrm{Tr}\left(\alpha - \frac{\mathrm{Tr}(\alpha)}{2}\right) = \mathrm{Tr}(\alpha) - \frac{2\mathrm{Tr}(\alpha)}{2} = 0.$$

Also, we can w.l.o.g. replace β (already chosen s.t. $\mathrm{Tr}(\beta) = 0$) with $\gamma = \beta - \frac{\mathrm{Tr}(\alpha\beta)}{2\alpha^2}\alpha$ and get $\mathrm{Tr}(\alpha\gamma) = 0$ because

$$\mathrm{Tr}(\gamma) = \mathrm{Tr}(\beta) - \frac{\mathrm{Tr}(\alpha\beta)}{2\alpha^2}\mathrm{Tr}(\alpha) = 0 - \frac{\mathrm{Tr}(\alpha\beta)}{2\alpha^2} \cdot 0 = 0$$
$$\alpha\gamma = \alpha\beta - \frac{\mathrm{Tr}(\alpha\beta)}{2} \implies$$
$$\mathrm{Tr}(\alpha\gamma) = \mathrm{Tr}(\alpha\beta) - \frac{\mathrm{Tr}(\mathrm{Tr}(\alpha\beta))}{2} = \mathrm{Tr}(\alpha\beta) - \frac{\mathrm{Tr}(\alpha\beta + \widehat{\alpha\beta})}{2} =$$
$$\mathrm{Tr}(\alpha\beta) - \frac{\mathrm{Tr}(\alpha\beta) + \mathrm{Tr}(\widehat{\alpha\beta})}{2} = \frac{\mathrm{Tr}(\alpha\beta)}{2} - \frac{\mathrm{Tr}(\widehat{\alpha\beta})}{2} = 0.$$

To sum up we have $\mathrm{Tr}(\alpha) = 0 = \mathrm{Tr}(\gamma)$ and also $\mathrm{Tr}(\alpha\gamma) = 0$. This implies that $\alpha = -\widehat{\alpha}, \gamma = -\widehat{\gamma}$ and $\alpha\gamma = -\widehat{\alpha\gamma} = -\widehat{\gamma}\widehat{\alpha} \implies \alpha\gamma = -\gamma\alpha$.

Now, we use our assumption $\alpha\beta = \beta\alpha$. Let $t = \frac{\mathrm{Tr}(\alpha\beta)}{2\alpha^2} \in \mathbb{Q}$:

$$0 = \alpha\gamma + \gamma\alpha = \alpha(\beta - t\alpha) + (\beta - t\alpha)\alpha = \alpha\beta - t\alpha^2 + \beta\alpha - t\alpha^2$$
$$\iff$$
$$0 = 2\alpha\beta - 2t\alpha^2 \iff 2t\alpha^2 = 2\alpha\beta \implies \beta \in \mathbb{Q}(\alpha).$$

□

Theorem 35. *Let* E *be an elliptic curve over* $K = \mathbb{F}_q$*. If* $\boldsymbol{\phi}^e \notin \mathbb{Z}$ *(using the identification of* $\mathbb{Z}$ *and* $\mathrm{End}_K(E)$ *in* $\mathrm{End}_K^0(E)$ *i.e., there does not exist* $m \in \mathbb{Z}$ *s.t.* $[m] = \boldsymbol{\phi}^e$*) then* $\mathrm{End}_K^0(E) \cong \mathbb{Q}(\boldsymbol{\phi}^e) \cong \mathbb{Q}(\sqrt{D})$ *is an imaginary quadratic field where* $D = (\mathrm{Tr}(\boldsymbol{\phi}^e))^2 - 4q < 0$.

Proof. This proof is a paraphrased version of [Sut19], Lecture 14, Theorem 14.6.

The characteristic polynomial of $\boldsymbol{\phi}^e$ is:

$$x^2 - \mathrm{Tr}(\boldsymbol{\phi}^e)x + \deg(\boldsymbol{\phi}^e) \in \mathbb{Z}[x].$$

The discriminant of this quadratic polynomial is $D = (\mathrm{Tr}(\boldsymbol{\phi}^e))^2 - 4\deg(\boldsymbol{\phi}^e)$. We know $\deg(\boldsymbol{\phi}^e) = p^e = q$ i.e., $D = (\mathrm{Tr}(\boldsymbol{\phi}^e))^2 - 4q$. Therefore, $\mathbb{Q}(\sqrt{D}) \cong \mathbb{Q}(\boldsymbol{\phi}^e)$.

Since we assume $\boldsymbol{\phi}^e \notin \mathbb{Z}$ and $\boldsymbol{\phi}^e$ is an algebraic integer then it must be $\boldsymbol{\phi}^e \notin \mathbb{Q}$. This implies $D \neq 0 \iff (\mathrm{Tr}(\boldsymbol{\phi}^e))^2 \neq 4q$ and by Theorem 31 it must be $D < 0$. We have shown that $\mathbb{Q}(\boldsymbol{\phi}^e)$ is an imaginary quadratic field.

Take $\alpha \in \mathrm{End}_K^0(E)$ using our definitions we have $\alpha = a\psi$ where $a \in \mathbb{Q}, \psi \in \mathrm{End}_K(E)$. Since $K = \mathbb{F}_q$ we have $\psi\boldsymbol{\phi}^e = \boldsymbol{\phi}^e\psi$ (for details see the proof of Theorem 42). Applying lemma 34 and 21 we get $\alpha \in \mathbb{Q}(\boldsymbol{\phi}^e)$. This completes the proof. □

Lemma 36. *Let E be an elliptic curve over $K = \mathbb{F}_q$. If E is ordinary then $\boldsymbol{\phi}^e \notin \mathbb{Z}$.*

Proof. This proof is inspired by [Sut19], Lecture 14, Corollary 14.7.

Assume $\boldsymbol{\phi}^e \in \mathbb{Z}$. Consider the characteristic polynomial of $\boldsymbol{\phi}^e$:

$$x^2 - \mathrm{Tr}(\boldsymbol{\phi}^e)x + \mathrm{N}(\boldsymbol{\phi}^e) \in \mathbb{Z}[x].$$

The discriminant of the polynomial is $D = \mathrm{Tr}(\boldsymbol{\phi}^e)^2 - 4\mathrm{N}(\boldsymbol{\phi}^e) = \mathrm{Tr}(\boldsymbol{\phi}^e)^2 - 4\deg(\boldsymbol{\phi}^e) = \mathrm{Tr}(\boldsymbol{\phi}^e)^2 - 4q$.

If $D > 0$, then $\mathrm{Tr}(\boldsymbol{\phi}^e)^2 > 4q$ which contradicts Theorem 31. So, it must be that $D \leq 0$.

If $D < 0$, then the roots of the polynomial are $\frac{-\mathrm{Tr}(\boldsymbol{\phi}^e) \pm \sqrt{D}}{2}$ and one of the roots is $\boldsymbol{\phi}^e$ which we assume to be an element of $\mathbb{Z}$. This is a contradiction since $-\mathrm{Tr}(\boldsymbol{\phi}^e) \pm \sqrt{D} \notin \mathbb{Q}$.

It must be that $D = 0 \iff \mathrm{Tr}(\boldsymbol{\phi}^e)^2 = 4q \implies \pm\mathrm{Tr}(\boldsymbol{\phi}^e) = 2\sqrt{q}$. $\mathrm{Tr}(\boldsymbol{\phi}^e) \in \mathbb{Z}$ so $\sqrt{q} = \sqrt{p^e} \in \mathbb{Z} \implies e \equiv 2 \mod p$ and $\pm\mathrm{Tr}(\boldsymbol{\phi}^e) = 2p^{\frac{e}{2}} \implies \mathrm{Tr}(\boldsymbol{\phi}^e) \equiv 0 \mod p \iff E$ supersingular by Claim 32 which is a contradiction. □

Claim 37. *Let E be a supersingular elliptic curve over $K = \mathbb{F}_p$, $p > 3$. Then $\mathrm{End}_K^0(E) \cong \mathbb{Q}(\boldsymbol{\phi}) \cong \mathbb{Q}(\sqrt{-4p}) \cong \mathbb{Q}(\sqrt{-p})$.*

Proof. Using Claim 32 we know that $\mathrm{Tr}(\boldsymbol{\phi}) = 0 \in \mathbb{Z}$. We want to apply Theorem 35 so we will use the same argument as in Lemma 36.

To contrary assume $\boldsymbol{\phi} \in \mathbb{Z}$. The characteristic polynomial of $\boldsymbol{\phi}$:

$$x^2 - \mathrm{Tr}(\boldsymbol{\phi})x + \mathrm{N}(\boldsymbol{\phi}) \in \mathbb{Z}[x].$$

The discriminant of the polynomial in this case is $D = \mathrm{Tr}(\boldsymbol{\phi})^2 - 4p = -4p$. The roots of the polynomial are $\frac{\pm\sqrt{D}}{2}$. Since $\boldsymbol{\phi}$ is one of the roots and both roots are clearly not in $\mathbb{Z}$ we have a contradiction.

Thus $\boldsymbol{\phi} \notin \mathbb{Z}$ and applying Theorem 35 we get the desired result. □

Theorem 38. *Let E be an elliptic curve over $K = \mathbb{F}_q$, and $\mathrm{End}_K^0(E) \cong \mathbb{Q}(\boldsymbol{\phi}^e)$ where $\boldsymbol{\phi}^e \notin \mathbb{Z}$ (i.e., $\mathrm{End}_K^0(E)$ is an imaginary quadratic field). Denote $\mathcal{O}_E$ the ring of integers of $\mathrm{End}_K^0(E)$. Then*

$$\mathbb{Z}[\boldsymbol{\phi}^e] \subseteq \mathrm{End}_K(E) \subseteq \mathcal{O}_E$$

where $|\mathcal{O}_E : \mathrm{End}_K(E)| \mid |\mathcal{O}_E : \mathbb{Z}[\boldsymbol{\phi}^e]|$.

Proof. The inclusions are clear since we have shown that $\mathrm{End}_K(E)$ is an order in $\mathrm{End}_K^0(E)$ but since it is an imaginary quadratic field, $\mathcal{O}_E$ is its unique maximal order therefore it contains all other orders.

$\mathbb{Z}[\boldsymbol{\phi}^e]$ is an order in $\mathrm{End}_K^0(E)$ which is assumed to be a $\mathbb{Q}$-algebra of dimension 2 and $\mathbb{Z}[\boldsymbol{\phi}^e]$ is clearly its subring which is a $\mathbb{Z}$-module of rank 2 since $\boldsymbol{\phi}^e \notin \mathbb{Z}$. □

Theorem 39. *Let E be a supersingular curve over $\mathbb{F}_p$ where $p > 3$. Then*

(a) $\mathrm{End}_{\mathbb{F}_p}(E) = \mathbb{Z}[\boldsymbol{\phi}] = \mathcal{O}_K$ *if* $p \equiv 1 \mod 4$.

(b) $\mathrm{End}_{\mathbb{F}_p}(E) \in \{\mathbb{Z}[\boldsymbol{\phi}], \mathcal{O}_K\}$ *if* $p \equiv 3 \mod 4$.

where K is an imaginary quadratic field s.t. $K \cong \mathrm{End}_{\mathbb{F}_p}^0(E)$.

Proof. By Claim 37 we already know that $\mathrm{End}_{\mathbb{F}_p}^0(E)$ is an imaginary quadratic field. We know $\mathrm{End}_{\mathbb{F}_p}(E)$ is an order in this field and by Theorem 38 we know

$$\mathbb{Z}[\boldsymbol{\phi}] \subseteq \mathrm{End}_{\mathbb{F}_p}(E) \subseteq \mathcal{O}_K.$$

By Theorem 1 (b) we know $\mathcal{O}_K = \mathbb{Z}\left[\frac{d_K + \sqrt{d_K}}{2}\right]$.

First assume $p \equiv 1 \mod 4$. Then by the definition of d_K we get $d_K = -4p$.

$$\mathbb{Z}\left[\frac{d_K + \sqrt{d_K}}{2}\right] = \mathbb{Z}\left[\frac{-4p + \sqrt{-4p}}{2}\right] = \mathbb{Z}\left[\frac{-4p + 2\sqrt{-p}}{2}\right] = \mathbb{Z}\left[\sqrt{-p}\right].$$

Note that we always identify $\boldsymbol{\phi}$ (the Frobenius endomorphism of the elliptic curve) with the element $\sqrt{-p}$ of K due to the isomorphisms from Theorem 35 and Claim 37. Thus $\mathcal{O}_K = \mathbb{Z}[\boldsymbol{\phi}]$ and the only option for $\mathrm{End}_{\mathbb{F}_p}(E)$ is that its equal (isomorphic) to $\mathbb{Z}[\boldsymbol{\phi}]$. This proves (a).

Now $p \equiv 3 \mod 4$. $d_K = -p \implies \mathcal{O}_K = \mathbb{Z}\left[\frac{-p + \sqrt{-p}}{2}\right]$. Clearly the conductor of $\mathbb{Z}[\boldsymbol{\phi}] = \mathbb{Z}[\sqrt{-p}]$ is 2 in $\mathcal{O}_K$. The only possibilities for $\mathrm{End}_{\mathbb{F}_p}(E)$ by Theorem 38 are $\mathbb{Z}[\boldsymbol{\phi}]$ or $\mathcal{O}_K$. □

Theorem 40. *Let E be a supersingular elliptic curve over K s.t. $\mathrm{char}(K) = p > 0$. Then $j(E) \in \mathbb{F}_{p^i}$ where $i \in \{1, 2\}$.*

Proof. This proof is an expanded version of [Sut19], Lecture 14, Theorem 14.16.

E supersingular $\implies [p] = \widehat{\boldsymbol{\phi}} \circ \boldsymbol{\phi}$ is inseparable $\implies \widehat{\boldsymbol{\phi}}$ inseparable. Note that $\widehat{\boldsymbol{\phi}} : E^{(1)} \to E$. By Theorem 10 we have $n \in \mathbb{N}$ and $\lambda \in \mathrm{Hom}_K((E^{(1)})^{(n)}, E)$ separable:

$$\widehat{\boldsymbol{\phi}} = \lambda \circ \boldsymbol{\phi}^n.$$

Since $\deg(\boldsymbol{\phi}) = \deg(\widehat{\boldsymbol{\phi}})$ it must be that $n = 1$ and $\deg(\lambda) = 1$. By definition of the curve $E^{(i)}$ we see that $(E^{(1)})^{(n)} = E^{(n+1)}$ so $\lambda : E^{(2)} \to E$ is an isogeny of degree 1. This means $K(E^{(2)}) \cong K(E)$ i.e., the curves E^2 and E are isomorphic. Using Theorem 2 (b) we have $j(E) = j(E^{(2)})$. Using the definitions of the j-invariant and curves $E^{(i)}$ we get $j(E) = j(E^{(2)}) = j(E)^{p^2}$. Since $j(E) \in K$ and $j(E) = j(E)^{p^2}$ it must be that $j(E) \in \mathbb{F}_{p^i}, i \in \{1, 2\}$ depending on the structure of K. □

One of the consequences of the claim above is that for K s.t. $\text{char}(K) = p > 0$ there exist only finitely many non-isomorphic supersingular elliptic curves over K.

In the case of $K = \mathbb{F}_q$ this is clear since for ordinary or supersingular curve E its j-invariant $j(E) \in \mathbb{F}_q$ and curves with the same j-invariant are isomorphic.

Theorem 41. *Let E be a supersingular elliptic curve over K s.t. $\text{char}(K) = p > 0$. Then $\text{End}^0_{\overline{K}}(E)$ is a quaternion algebra.*

Proof. [Sut19] Lecture 14, Theorem 14.18. □

We can summarize the structure of the endomorphism algebra for finite fields into this corollary.

Corollary. Let E be an elliptic curve over $K = \mathbb{F}_q$. Then

(a) E is supersingular $\iff$ $\text{End}^0_{\overline{\mathbb{F}_q}}(E)$ is a quaternion algebra.

(b) E is ordinary $\iff$ $\boldsymbol{\phi}^e \notin \mathbb{Z}$ and $\text{End}^0_{\overline{\mathbb{F}_q}}(E)$ is an imaginary quadratic field.

Remark. Consider an elliptic curve E over $\mathbb{F}_p$. Although by Theorem 41 we know that $\text{End}^0(E) = \text{End}^0_{\overline{\mathbb{F}_p}}(E)$ is a quaternion algebra, its $\mathbb{F}_p$-rational subset $\text{End}^0_{\mathbb{F}_p}(E)$ is an imaginary quadratic field by Claim 37.[1]

Definition 33. *Let E be an elliptic curve over K. If $\text{End}_{\overline{K}}(E)$ is not isomorphic to $\mathbb{Z}$ (which is equivalent to saying $\text{End}^0_{\overline{K}}(E)$ is not isomorphic to $\mathbb{Q}$) we say that E has complex multiplication.*

Remark. If $K = \mathbb{F}_q$ then using the previous theorem we get that every elliptic curve over a finite field has complex multiplication.

Theorem 42. *Let E be an elliptic curve over $\mathbb{F}_q$, $\alpha \in \text{End}_{\overline{\mathbb{F}_q}}(E)$. $\alpha \circ \boldsymbol{\phi}^e = \boldsymbol{\phi}^e \circ \alpha \iff \alpha \in \text{End}_{\mathbb{F}_q}(E)$.*

Proof. First let's recall the definition of an endomorphism being defined over $\mathbb{F}_q$. Every endomorphism can be expressed as (we will use the affine representation for simplicity) a pair of rational functions defined over $\mathbb{F}_q$ i.e., if β is our endomorphism then $\beta = \left(\frac{A(x,y)}{B(x,y)}, \frac{C(x,y)}{D(x,y)}\right)$ where $A, B, C, D \in \mathbb{F}_q[x, y]$.

Let $\alpha = \left(\frac{A(x,y)}{B(x,y)}, \frac{C(x,y)}{D(x,y)}\right)$ where $A, B, C, D \in \overline{\mathbb{F}_q}[x, y]$. We know $\boldsymbol{\phi}^e = (x^q, y^p)$ so

$$\alpha \circ \boldsymbol{\phi}^e = \left(\frac{A(x^q, y^q)}{B(x^q, y^q)}, \frac{C(x^q, y^q)}{D(x^q, y^q)}\right).$$

Let's focus on the polynomial A (for others the reasoning is the same). On the LHS we have $A(x^q, y^q) \in \overline{\mathbb{F}_q}[x, y]$ i.e., if $A(x, y) = \sum_i \sum_j a_{i,j} x^i y^j$ then $A(x^q, y^q) = \sum_i \sum_j a_{i,j} x^{iq} y^{jq}$.

On the RHS $\boldsymbol{\phi}^e \circ \alpha$ we have $A(x, y)^q = (\sum_i \sum_j a_{i,j} x^i y^j)^q$. Since we are in a field of characteristic p then $A(x, y)^q = \sum_i \sum_j (a_{i,j})^q x^{iq} y^{jq}$.

This means $a_{i,j} = (a_{i,j})^q$. The Frobenius endomorphism of $\overline{\mathbb{F}_q}$ fixes exactly $\mathbb{F}_q$ i.e., $\forall i, j : a_{i,j} \in \mathbb{F}_q$. In other words $A(x, y) \in \mathbb{F}_q[x, y]$.

Same goes for B, C, D and we get that α is defined over $\mathbb{F}_q$.

The converse is clear. □

[1] This property is crucial to the cryptosystem CSIDH since the $\mathbb{F}_p$-rational endomorphism ring is commutative unlike the "whole" $\text{End}(E)$

Corollary. Let E be an elliptic curve over $\mathbb{F}_q$. If E is ordinary then $\mathrm{End}_{\mathbb{F}_q}(E) = \mathrm{End}_{\overline{\mathbb{F}_q}}(E)$.

Proof. E being ordinary means $\mathrm{End}_{\overline{\mathbb{F}_q}}(E)$ is an order in a quadratic imaginary field which is commutative. Applying Theorem 42 we get the desired result. □

Theorem 43. *Let $\psi : E \to E'$ be an isogeny defined over $\mathbb{F}_q$ between elliptic curves E, E' over $\mathbb{F}_q$. Then $|E(\mathbb{F}_q)| = |E'(\mathbb{F}_q)|$.*

Proof. Denote the Frobenius endomorphism of E as $\boldsymbol{\phi}^e$ and the Frobenius endomorphism of E' as $\boldsymbol{\phi'}^e$. Because $\boldsymbol{\phi}^e$ fixes exactly the $\mathbb{F}_q$-rational points we get $E(\mathbb{F}_q) = \mathrm{Ker}(\boldsymbol{\phi}^e \oplus [-1]), E'(\mathbb{F}_q) = \mathrm{Ker}(\boldsymbol{\phi'}^e \oplus [-1])$.

By Theorem 29, the isogenies $\boldsymbol{\phi}^e \oplus [-1], \boldsymbol{\phi'}^e \oplus [-1]$ are separable (because $[-1]$ is always separable). That means $\mathrm{Ker}(\boldsymbol{\phi}^e \oplus [-1]) = \deg(\boldsymbol{\phi}^e \oplus [-1])$ and $\mathrm{Ker}(\boldsymbol{\phi'}^e \oplus [-1]) = \deg(\boldsymbol{\phi'}^e \oplus [-1])$.

Using the same reasoning as in the proof of Theorem 42 we can prove that ψ being defined over $\mathbb{F}_q$ implies

$$\begin{gathered}\boldsymbol{\phi'}^e \circ \psi = \psi \circ \boldsymbol{\phi}^e \\ \Longrightarrow \\ (\boldsymbol{\phi'}^e \oplus [-1]) \circ \psi = \psi \circ (\boldsymbol{\phi}^e \oplus [-1]).\end{gathered}$$

If we compare degree of these isogenies, we get the desired result.

$$\begin{gathered}\deg((\boldsymbol{\phi'}^e \oplus [-1]) \circ \psi) = \deg(\psi \circ (\boldsymbol{\phi}^e \oplus [-1])) \\ \Longrightarrow \\ \deg(\boldsymbol{\phi'}^e \oplus [-1]) \deg(\psi) = \deg(\psi) \deg(\boldsymbol{\phi}^e \oplus [-1]) \\ \Longrightarrow \\ \deg(\boldsymbol{\phi'}^e \oplus [-1]) = \deg(\boldsymbol{\phi}^e \oplus [-1]) \implies \\ |E'(\mathbb{F}_q)| = |E(\mathbb{F}_q)|.\end{gathered}$$

□

Remark. The other implication that arises from Theorem 43 is also true. If $|E(\mathbb{F}_q)| = |E'(\mathbb{F}_q)|$, then there exists an isogeny defined over $\mathbb{F}_q$ between E, E'. This is known as the Tate's isogeny theorem.

Claim 44. *Let E be a supersingular curve over $\mathbb{F}_q$. Then E is $\overline{\mathbb{F}_q}$-isomorphic to a supersingular elliptic curve defined over $\mathbb{F}_{p^i}, i \in \{1, 2\}$.*

Proof. E is supersingular therefore by Theorem 40 $j(E) \in \mathbb{F}_{p^i}$. By Theorem 2 there exists an elliptic curve E' defined over $\mathbb{F}_{p^i}$ s.t. $j(E') = j(E)$ and using the same theorem we get they are $\overline{\mathbb{F}_q}$-isomorphic which implies supersingularity. □

Thus, over $\mathbb{F}_q$ we can only work with curves over a smaller field $\mathbb{F}_{p^2}$ and they are going to have the same properties.

Next, we present a theorem which gives us the exact number of different supersingular elliptic curves over $\overline{\mathbb{F}_q}$.

Theorem 45. *Let $p > 3$ a prime s.t. $\mathbb{F}_q$ is a finite field of characteristic p. Then the number of supersingular elliptic curves over $\overline{\mathbb{F}_q}$ (up to $\overline{\mathbb{F}_q}$-isomorphism) is*

$$\left\lfloor \frac{p}{12} \right\rfloor + \begin{cases} 0 & \text{if } p \equiv 1 \mod 12 \\ 1 & \text{if } p \equiv 5 \mod 12 \text{ or } p \equiv 7 \mod 12 \\ 2 & \text{if } p \equiv 11 \mod 12. \end{cases}$$

Proof. [Sil09], Chapter V, Theorem 4.1 (c). □

Claim 46. *Let $l \in \mathbb{Z}$ be a prime s.t. $\gcd(p, l) = 1$ and E an elliptic curve over $K = \mathbb{F}_q$. There exist exactly $l + 1$ isogenies of degree l (up to $\overline{K}$-isomorphism) from E to other elliptic curves over $\overline{K}$. All of these isogenies are separable.*

Proof. First, we note that every isogeny of degree l is separable. If there was an isogeny τ of degree l that is inseparable then by Theorem 10 we get $e > 0 \in \mathbb{N}$: $\tau = \psi \circ \boldsymbol{\phi}^e$ and $l = \deg(\tau) = \deg(\psi)\deg(\phi)^e = \deg(\psi)p^e$. That is a contradiction since $p \nmid l$.

Let τ be an isogeny of degree l from E. Now we use Theorem 14 and the fact that for separable isogenies $\deg(\tau) = |\mathrm{Ker}(\tau)|$. Since l is a prime then $\mathrm{Ker}(\tau) \leq E$ is a subgroup of prime order thus cyclic. This means $\mathrm{Ker}(\tau) \leq E[l]$.

Theorem 13 states $E[l] \cong \mathbb{Z}_l \times \mathbb{Z}_l$. The problem is therefore equivalent to finding out how many subgroups of order l the group $G = \mathbb{Z}_l \times \mathbb{Z}_l$ has. Every non-identity element of G has order l. Thus, there are $l^2 - 1$ elements of order l and every such element "goes over" $l - 2$ other elements, which are of order l, and the identity element. Looking at the number of equivalence classes we have $\frac{l^2-1}{l-2+1} = l + 1$ equivalence classes which correspond to different subgroups of $E[l]$ which correspond to different isogenies. □

3. Ideal class group action

In this chapter we will be working with elliptic curves over $\mathbb{C}$ to develop a what is called the ideal class group action upon elliptic curves. In the next chapter we will translate this theory to elliptic curves over finite fields.

Working with elliptic curves over $\mathbb{C}$ requires a knowledge of complex analysis. We will present only the most important results. The point of this chapter is to introduce the reader to the origin of the ideal class group action.

This chapter mainly follows [Sut19], Lectures $15-18, 21$.

3.1 Elliptic curves over $\mathbb{C}$

Definition 34. *Let L, L' be lattices. We say L, L' are homothetic if there exists $z \in \mathbb{C} \setminus \{0\}$ s.t. $L = zL'$.*

Remark. Being homothetic is clearly an equivalence relation. Also, if $L = [\alpha, \beta]$, $L' = [\gamma, \delta]$, then L, L' are homothetic iff there exists $z \in \mathbb{C} \setminus \{0\}$ s.t. $\alpha = z\gamma, \beta = z\delta$.

Definition 35. *Let L be a lattice. The Weierstrass $\wp$-function of a lattice L is defined as*

$$\forall z \in \mathbb{C} : \wp(z, L) = \frac{1}{z^2} + \sum_{\alpha \in L \setminus \{0\}} \left(\frac{1}{(z-\alpha)^2} - \frac{1}{\alpha^2} \right).$$

Remark. Usually the lattice L in the definition of its Weierstrass $\wp$-function is known so we usually write $\wp(z)$ instead of $\wp(z, L)$. The symbol "$\wp$" is a curly letter "p". Because of that it is also sometimes called the Weierstrass p-function.

Definition 36. *Let L be a lattice, $k \in \mathbb{Z}, k > 2$. The weight-k Eisenstein series for L is defined as*

$$G_k(L) = \sum_{\alpha \in L \setminus \{0\}} \frac{1}{\alpha^k}.$$

Remark. For any lattice L and $k \in \mathbb{Z}, k > 2$ the series $G_k(L)$ converges absolutely. This means $G_k(L)$ has always a defined value.

Theorem 47. *Let L be a lattice. The function $\wp(z)$ satisfies the differential equation*

$$\wp'(z)^2 = 4\wp(z)^3 - g_2(L)\wp(z) - g_3(L)$$

where $g_2(L) = 60G_4(L)$ and $g_3(L) = 140G_6(L)$.

Proof. [Sut19] Lecture 15, Theorem 15.29. □

Notice the familiarity between the Weierstrass equation of an elliptic curve and this differential equation. If we set $x = \wp(z), y = \wp'(z)$ then we have

$$y^2 = 4x^3 - g_2(L)x - g_3(L)$$

Define $A = -\frac{g_2(L)}{4}, B = -\frac{g_3(L)}{4}$ then we get

$$y^2 = 4x^3 + 4Ax + 4B$$

which is a curve $\mathbb{C}$-equivalent to the Weierstrass equation

$$y^2 = x^3 + ax + b$$

where $a, b \in \mathbb{C}$.

Now we need to find out under what circumstances is this actually an equation defining an elliptic curve over $\mathbb{C}$ i.e., when is this curve smooth. We know that a general Weierstrass curve is smooth iff its discriminant is not 0. This process yields the condition that $\Delta(L) = g_2(L)^3 - 27g_3(L)^2$ must not be zero.

Definition 37. *Let L be a lattice. The discriminant of L is defined as*

$$\Delta(L) = g_2(L)^3 - 27g_3(L)^2$$

Theorem 48. *Let L be a lattice. The discriminant of L is non-zero.*

Proof. [Sut19] Lecture 15, Lemma 15.32. □

Consequence of Theorem 48 is that every lattice L corresponds to an elliptic curve over $\mathbb{C}$.

Definition 38. *A torus is a quotient group $\mathbb{C}/L$ where L is a lattice.*

Remark. More specifically, the quotient group $\mathbb{C}/L$ is the quotient group of the additive group $\mathbb{C}$ and its additive subgroup L.

The Weierstrass $\wp$-function (and its derivative as well) is what's called an elliptic function. Simply stated it means that it is a complex function differentiable almost[1] everywhere and it is periodic on L i.e., $\forall z \in \mathbb{C}, \forall \alpha \in L : \wp(z) = \wp(z + \alpha)$.

Due to the periodicity, we can look at $\wp$ as a function of a torus. Using the substitutions described above, we can formulate the correspondence between lattices and elliptic curves as follows.

Theorem 49. *Let L be a lattice and $(E_L, \mathcal{O})$ be an elliptic curve over $\mathbb{C}$ given by: $y^2 = 4x^3 - g_2(L)x - g_3(L)$. Define a map $\Phi : \mathbb{C}/L \to E_L(\mathbb{C})$ as follows:*

$$\Phi(z) = \begin{cases} (\wp(z), \wp'(z)) & z \notin L \\ \mathcal{O} & z \in L. \end{cases}$$

The map Φ is a group isomorphism.

Proof. [Sut19] Lecture 16, Theorem 16.1. □

Now we know that for every lattice there exists an elliptic curve over $\mathbb{C}$ and that elliptic curve group is isomorphic to the corresponding torus. Let L be a lattice. From now on the corresponding elliptic curve to a lattice L is going to be denoted as E_L and it is given by the equation: $y^2 = 4x^3 - g_2(L)x - g_3(L)$.

[1] This "almost" has a clear definition. The term is "a meromorphic function".

Definition 39. *Let L be a lattice. Define the j-invariant of L as*

$$j(L) = 1728\frac{g_2(L)^3}{\Delta(L)}.$$

Remark. It holds that $j(L) = j(E_L)$ i.e., the j-invariant of a lattice is equal to the j-invariant of the corresponding elliptic curve E_L.

It would be nice to know if there exists a lattice for every elliptic curve over $\mathbb{C}$. This is also true.

Theorem 50. *Let L, L' be lattices and let $E_L, E_{L'}$ be the corresponding elliptic curves. L, L' are homothetic iff E_L, E'_L are $\mathbb{C}$-isomorphic.*

Proof. [Sut19] Lecture 16, Theorem 16.5. □

Theorem 51. *Let E be an elliptic curve over $\mathbb{C}$. There exists L s.t. E is the corresponding curve to the lattice L.*

Proof. [Sut19] Lecture 16, Corollary 16.12. □

This theorem clears up our doubts about the correspondence between elliptic curves over $\mathbb{C}$ and lattices. We can now look at elliptic curves over $\mathbb{C}$ as lattices.

We would like to translate isogenies into this framework. The following theorem characterizes morphisms between tori. We will again not give a precise definition of what a morphism between tori is but simply put: it is a restriction of a complex differentiable function upon tori that is also a group homomorphism.

For example choose $\alpha \in \mathbb{C}$ consider the map $f_\alpha : \mathbb{C} \to \mathbb{C}$ s.t. $f_\alpha(z) = \alpha z$. Add two lattices L, L' and denote the restriction of f_α as ϕ_α i.e., it is the map:

$$\begin{aligned} \mathbb{C}/L &\to \mathbb{C}/L' \\ z + L &\mapsto \alpha z + L'. \end{aligned}$$

For ϕ_α to be a group homomorphism we need $\phi_\alpha(0_L) = 0_{L'}$ i.e., $\alpha L \subseteq L'$. Thus, if α, L, L' satisfy this condition, then ϕ_α is a morphism of tori. The following theorem characterizes all possible morphism and states all of them have this form.

Denote $\mathrm{Hom}(\mathbb{C}/L, \mathbb{C}/L') = \{\text{morphisms } \mathbb{C}/L \to \mathbb{C}/L'\}$.

Theorem 52. *Let L, L' be lattices. Define a map τ as*

$$\begin{aligned} \{\alpha \in \mathbb{C} : \alpha L \subseteq L'\} &\to \mathrm{Hom}(\mathbb{C}/L, \mathbb{C}/L') \\ \alpha &\mapsto \phi_\alpha \end{aligned}$$

where ϕ_α is defined as above ($\phi_\alpha(z + L) = \alpha z + L'$). Then τ is an isomorphism of additive groups and if $L = L'$, then τ is an isomorphism of commutative rings.

Proof. [Sut19] Lecture 17, Corollary 17.2. □

Theorem 53. *Let L, L' be lattices, let $E_L, E_{L'}$ be the corresponding elliptic curves over $\mathbb{C}$ and let $\alpha \in \mathbb{C}$. Then the following are equivalent:*

(a) $\alpha L \subseteq L'$.

(b) *There exists a unique* $\lambda_\alpha \in \mathrm{Hom}_{\mathbb{C}}(E_L, E_{L'})$ *(*λ_α *is an isogeny over* $\mathbb{C}$*) s.t. this diagram commutes:*

$$\begin{array}{ccc} \mathbb{C}/L & \xrightarrow{\phi_\alpha} & \mathbb{C}/L' \\ \Phi \downarrow & & \downarrow \Phi' \\ E_L(\mathbb{C}) & \xrightarrow{\lambda_\alpha} & E_{L'}(\mathbb{C}) \end{array}$$

where ϕ_α *denotes the morphism described above Theorem 52 and* Φ, Φ' *denote the isomorphisms described in Theorem 49.*

In addition, for every $\lambda \in \mathrm{Hom}_{\mathbb{C}}(E_L, E_{L'})$ *there exists a unique* $\alpha_\lambda \in \mathbb{C}$ *s.t.* $\alpha_\lambda L \subseteq L'$*. The maps* $\alpha \mapsto \lambda_\alpha$ *and* $\lambda \mapsto \alpha_\lambda$ *are inverse group isomorphisms between* $\{\alpha \in \mathbb{C} : \alpha L \subseteq L'\}$ *and* $\mathrm{Hom}_{\mathbb{C}}(E_L, E_{L'})$*.*

Proof. [Sut19] Lecture 17, Theorem 17.4. □

Theorem 53 states that every isogeny between elliptic curves over $\mathbb{C}$ corresponds to a morphism between tori which correspond to certain elements of $\mathbb{C}$. This can remind us of the previous correspondence between elements of $\mathrm{End}_K(E)$ and elements of the tensor product $\mathrm{End}_K^0(E) = \mathrm{End}_K(E) \otimes \mathbb{Q}$. To investigate this further we need to focus more on the special case when $L = L'$.

Theorem 54. *Let* L *be a lattice. The following statements hold:*

(a) *The maps* $\alpha \mapsto \lambda_\alpha$ *and* $\lambda \mapsto \alpha_\lambda$ *are inverse ring isomorphisms between* $\{\alpha \in \mathbb{C} : \alpha L \subseteq L\}$ *and* $\mathrm{Hom}_{\mathbb{C}}(E_L, E_L) = \mathrm{End}_{\mathbb{C}}(E_L)$*.*

(b) *The map* $\phi \mapsto \hat{\phi}$ *(the dual isogeny map) corresponds to the complex conjugation* $\alpha \mapsto \overline{\alpha}$*.*

(c) $\mathrm{Tr}(\alpha) = \alpha + \overline{\alpha} = \mathrm{Tr}(\lambda_\alpha)$ *(the trace on left is in* $\mathbb{C}$ *and the trace on the right is in* $\mathrm{End}_{\mathbb{C}}(E_L)$*).*

(d) $\mathrm{N}(\alpha) = \alpha\overline{\alpha} = \mathrm{N}(\lambda_\alpha)$ *(the norm on left is in* $\mathbb{C}$ *and the norm on the right is in* $\mathrm{End}_{\mathbb{C}}(E_L)$ *which corresponds to the isogeny degree).*

Proof. [Sut19] Lecture 17, Corollary 17.5. □

Remark. The term complex multiplication comes from this. The endomorphisms of an elliptic curve which are not in $\mathbb{Z}$ correspond to certain complex numbers (specifically $\mathbb{C} \setminus \mathbb{R}$).

Theorem 55. *Let* E *be an elliptic curve over* $\mathbb{C}$*. Then* $\mathrm{End}_{\mathbb{C}}(E)$ *is isomorphic to either* $\mathbb{Z}$ *or an order in an imaginary quadratic field.*

Alternatively, $\mathrm{End}_{\mathbb{C}}^0(E)$ *is isomorphic to* $\mathbb{Q}$ *or* $\mathbb{Q}(\sqrt{D})$ *for some* $D \in \mathbb{Z}, D < 0$*.*

Proof. [Sut19] Lecture 17, Corollary 17.7. □

Remark. Notice the difference between $\mathbb{C}$ and a field of positive characteristic. In the positive characteristic we allow one more option, the quaternion algebra.

From now on we assume that the elliptic curve we work with in this section has complex multiplication. Every imaginary quadratic field can be embedded into $\mathbb{C}$. We can thus embed $\mathrm{End}^0_{\mathbb{C}}(E)$ into $\mathbb{C}$ naturally and as stated above, we have an isomorphism between $\mathrm{End}_{\mathbb{C}}(E)$ and an order in an imaginary quadratic field. We also assume that we have used an embedding for which $\mathrm{End}_{\mathbb{C}}(E)$ is equal to the order from Theorem 55.

An order is by definition a lattice (and a ring). We will now study the relationship between lattices, which define elliptic curves, and the elliptic curves' endomorphism rings, which are also lattices.

Consider an order $\mathcal{O}$ and define $L = \mathcal{O}$. What is $\mathrm{End}_{\mathbb{C}}(E_L)$? We know that $\mathrm{End}_{\mathbb{C}}(E_L) = \mathcal{O}' = \{\alpha \in \mathbb{C} : \alpha L \subseteq L\} = \{\alpha \in \mathbb{C} : \alpha\mathcal{O} \subseteq \mathcal{O}\}$. By the definition of an order, we get that $\alpha \in \mathcal{O}' \implies \alpha \in \mathcal{O}$ i.e., $\mathcal{O}' \subseteq \mathcal{O}$.

On the other hand, take $\alpha \in \mathcal{O}$. Since $\mathcal{O}$ is a ring, clearly $\alpha\mathcal{O} \subseteq \mathcal{O}$ i.e., also $\mathcal{O} \subseteq \mathcal{O}'$. In the end $\mathcal{O} = \mathcal{O}'$.

If L, L' are homothetic, then $\mathrm{End}_{\mathbb{C}}(E_L) = \mathrm{End}_{\mathbb{C}}(E_{L'})$. This is clear from the definition.

Now another question arises: Is there any non-homothetic lattice L' to $L = \mathcal{O}$ for which $\mathrm{End}_{\mathbb{C}}(E_{L'}) = \mathcal{O}$? W.l.o.g. we can assume every lattice to be of the form $L = [1, \alpha]$, since we only care about non-homothetic lattices. This is because any lattice $L = [\alpha, \beta] = \alpha\mathbb{Z} + \beta\mathbb{Z}$ is homothetic to a lattice $L' = [1, \frac{\beta}{\alpha}] = \mathbb{Z} + \frac{\beta}{\alpha}\mathbb{Z} = \frac{1}{\alpha}(\alpha\mathbb{Z} + \beta\mathbb{Z}) = \frac{1}{\alpha}L$.

Note that any order $\mathcal{O}$ we can express as a lattice $\mathcal{O} = [1, \xi]$ where ξ is an algebraic integer. For a lattice (as mentioned above) we assume $L = [1, \alpha]$ and $\alpha \in \mathbb{C} \setminus \mathbb{R}$.

Claim 56. *Let L be a lattice and $\mathcal{O}$ be an order in an imaginary quadratic field and let E_L be the corresponding elliptic curve to L. If $\mathrm{End}_{\mathbb{C}}(E_L) = \mathcal{O}$, then L is homothetic to an $\mathcal{O}$-ideal.*

Proof. Let $L = [1, \alpha]$ and $\mathcal{O} = [1, \xi]$ as above.

$\{\beta \in \mathbb{C} : \beta L \subseteq L\} = \mathrm{End}_{\mathbb{C}}(E_L) = \mathcal{O}$ implies that $\xi \in \mathcal{O}$ is an element of L. Thus, there exist $m, n \in \mathbb{Z}, n \neq 0$ s.t. $\xi = m + n\alpha$. Consider the lattice $nL = [n, n\alpha]$. We know $n\alpha = \xi - m$ thus $nL = [n, \xi - m]$ but also clearly $[n, \xi - m] \subseteq [1, \xi] = \mathcal{O}$. In other words, $nL \subseteq \mathcal{O}$ and L is homothetic to nL.

Now we just need to show that nL is an $\mathcal{O}$-ideal. nL is a lattice and it is a subset of $\mathcal{O}$ i.e., it is an additive subgroup of $\mathcal{O}$. We know $\mathcal{O} = \{\beta \in \mathbb{C} : \beta L \subseteq L\}$ but this set is the same for homothetic lattices so we get

$$\mathcal{O} = \{\beta \in \mathbb{C} : \beta L \subseteq L\} = \{\beta \in \mathbb{C} : \beta nL \subseteq nL\}.$$

In other words, nL is closed under multiplication by elements of $\mathcal{O}$ therefore an $\mathcal{O}$-ideal. □

Claim 57. *Let $\mathcal{O}$ be an order in an imaginary quadratic field K and let L be an $\mathcal{O}$-ideal. Then L is lattice, the set*

$$\mathcal{O}(L) = \{\beta \in \mathbb{C} : \beta L \subseteq L\}$$

is an order in K and $\mathcal{O} \subseteq \mathcal{O}(L) = \mathrm{End}_{\mathbb{C}}(E_L)$.

Proof. First we show that $\mathcal{O}(L) = \{\beta \in \mathbb{C} : \beta L \subseteq L\}$. Note that $\mathcal{O}(L)$ means the set from Definition 11 and we need to prove the equality. One inclusion is clear. By assumption $L \subseteq \mathcal{O} \subseteq K$. Take $\beta \in \mathbb{C} : \beta L \subseteq L \subseteq K$, take $\delta \in L$, then by assumption $\beta\delta \in L \subseteq K \implies \beta \in K$ since $\delta \in K$.

Next, we show that L is a lattice i.e., an additive subgroup of $\mathbb{C}$ of rank 2. Take $\delta \in L$, since L is an $\mathcal{O}$-ideal, then $\delta\mathcal{O} \subseteq L \subseteq \mathcal{O}$. $\delta\mathcal{O}$ and $\mathcal{O}$ are both additive subgroups of $\mathbb{C}$ of rank 2 therefore L is as well i.e., L is a lattice.

Because L is a lattice, then $\mathcal{O}(L) = \{\beta \in \mathbb{C} : \beta L \subseteq L\} = \mathrm{End}_{\mathbb{C}}(E_L)$ is an order in an imaginary quadratic field $K' \subseteq \mathbb{C}$. $\mathcal{O}(L)$ is a subring of K and $\mathcal{O}(L)$ is an order in K' therefore it must be also an order in K.

Take $\beta \in \mathcal{O}$, L is an $\mathcal{O}$-ideal therefore $\beta L \subseteq L$ i.e., $\beta \in \mathcal{O}(L) \implies \mathcal{O} \subseteq \mathcal{O}(L)$. □

Definition 40. *Let $\mathcal{O}$ be an order in an imaginary quadratic field. Let I, J be $\mathcal{O}$-ideals. We call I, J equivalent $\mathcal{O}$-ideals if they are homothetic as lattices. This definition make sense since in Claim 57 we have proven that every $\mathcal{O}$-ideal is a lattice.*

Equivalently we can define I, J to be equivalent $\mathcal{O}$-ideals if there exist $\alpha, \beta \in \mathcal{O}$ s.t. $\alpha I = \beta J \iff (\alpha)I = (\beta)J$.

Same as with $\mathcal{O}$-ideals, we define the set $\mathcal{O}(I)$ for a fractional $\mathcal{O}$-ideal as

$$\mathcal{O}(I) = \{\alpha \in K : \alpha I \subseteq I\}.$$

Definition 41. *Let I be a fractional $\mathcal{O}$-ideal. We call I proper if $\mathcal{O}(I) = I$.*

Theorem 58. *Let $\mathcal{O}$ be an order in an imaginary quadratic field K, let $L = [\alpha, \beta]$ be an $\mathcal{O}$-ideal and let $I = \frac{1}{b}L$ be fractional $\mathcal{O}$-ideal where $b \in \mathbb{Z}, b > 0$. Then:*

(a) I is proper iff L is proper.

(b) I is invertible iff L is invertible.

(c) L is invertible iff L is proper.

(d) If L is invertible, then $L\overline{L} = (\mathrm{N}(L))$ (a principal $\mathcal{O}$-ideal generated by an integer) where $\overline{L} = [\overline{\alpha}, \overline{\beta}]$. Also, the inverse of L is $L^{-1} = \frac{1}{\mathrm{N}(L)}\overline{L}$.

Proof. [Sut19] Lemma 18.9 and Theorem 18.10. □

Corollary. Let $\mathcal{O}$ be an order in an imaginary quadratic field K and let I, J be invertible fractional $\mathcal{O}$-ideals. Then $\mathrm{N}(IJ) = \mathrm{N}(I)\mathrm{N}(J)$.

3.2 Definition of the action

Definition 42. *Let $\mathcal{O}$ be an order in an imaginary quadratic field. Denote the set of invertible (proper) fractional $\mathcal{O}$-ideals as $I(\mathcal{O})$ and denote the set of principal invertible fractional $\mathcal{O}$-ideals as $P(\mathcal{O})$. Clearly $P(\mathcal{O}) \subseteq I(\mathcal{O})$.*

Define the ideal class group of $\mathcal{O}$ as the quotient group $\mathrm{cl}(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O})$.

Remark. We can also look at the ideal class group of $\mathcal{O}$ as the set of equivalence classes of proper $\mathcal{O}$-ideals where the equivalence is defined as an equivalence of $\mathcal{O}$-ideals.

Theorem 59. *Let $\mathcal{O}$ be an order in an imaginary quadratic field. Every class $[I] \in \mathrm{cl}(\mathcal{O})$ contains infinitely many ideals of prime norm.*

Proof. [Cox13] Theorem 7.7 (iii) and Theorem 9.12 □

Theorem 60. *Let $\mathcal{O}$ be an order in an imaginary quadratic field. $\mathrm{cl}(\mathcal{O})$ is a finite abelian group.*

Proof. [Cox13] Theorem 3.9 and Theorem 7.7 (ii). □

Definition 43. *Let K be an imaginary quadratic field and $\mathcal{O}_K$ its maximal order. Denote the cardinality of $\mathrm{cl}(\mathcal{O}_K)$ as $\underline{h(D)}$ where $D = \mathrm{disc}(\mathcal{O}_K)$.*

Definition 44. *Let $\mathcal{O}$ be an order in an imaginary quadratic field and let K be a field. Denote by $\mathrm{Ell}_{\mathcal{O}}(K)$ the set*

$$\mathrm{Ell}_{\mathcal{O}}(K) = \{j(E) \in K : \mathrm{End}_{\overline{K}}(E) = \mathcal{O}\}$$

If we fix an order $\mathcal{O}$ in an imaginary quadratic field, we can now say there is a bijection between the sets $\mathrm{cl}(\mathcal{O})$ and $\{E/\mathbb{C} : \mathrm{End}_{\mathbb{C}}(E) = \mathcal{O}\}$. We can also state that $\{E/\mathbb{C} : \mathrm{End}_{\mathbb{C}}(E) = \mathcal{O}\}$ is in bijection with the set $\{L \text{ a lattice} : \mathcal{O}(L) = \mathcal{O}\}$.

Let $\mathcal{O}$ be an order in an imaginary quadratic field. We know that every $\mathcal{O}$-ideal is a lattice. Let I be an $\mathcal{O}$-ideal and denote by E_I the elliptic curve over $\mathbb{C}$ which corresponds to I as a lattice. Every elliptic curve E s.t. its endomorphism ring is $\mathcal{O}$ corresponds to a curve E_L where L is a proper (invertible) $\mathcal{O}$-ideal. Its existence is guaranteed by the discussion at the start of this chapter. Also as stated above, we can look at elements of $\mathrm{cl}(\mathcal{O})$ as equivalence classes proper of $\mathcal{O}$-ideals.

Now we can finally define the ideal class group action.

Theorem 61. *Let $\mathcal{O}$ be order in an imaginary quadratic field K. The ideal class group $\mathrm{cl}(\mathcal{O})$ acts freely and transitively on the set $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ via the action*

$$\begin{aligned} \mathrm{cl}(\mathcal{O}) \times \mathrm{Ell}_{\mathcal{O}}(\mathbb{C}) &\to \mathrm{Ell}_{\mathcal{O}}(\mathbb{C}) \\ ([I], j(E_J)) &\mapsto j(E_{I^{-1}J}) \end{aligned}$$

Proof. First, we will prove it is a group action. We need to prove that for any non-zero principal invertible fractional $\mathcal{O}$-ideal P it holds that $j(E_J) = j(E_{P^{-1}J})$ where J is a non-zero invertible $\mathcal{O}$-ideal. This is easy because for P we have $P = (\alpha), \alpha \in K$ and clearly $P^{-1} = \left(\frac{1}{\alpha}\right)$.

Therefore, if we compare invertible fractional $\mathcal{O}$-ideals J and $\left(\frac{1}{\alpha}\right) J$ as lattices we can see that they are homothetic which means they define the same elliptic curves. We can consider invertible fractional $\mathcal{O}$-ideals as lattices since every one of them can be written as $J = \left(\frac{1}{n}\right) J', n \in \mathbb{Z}, n > 0, J'$ an $\mathcal{O}$-ideal. Thus, this does not change homothety.

We have proven the identity of the action.

Now we will prove compatibility i.e., for any I, J, L proper $\mathcal{O}$-ideals (we look at $\mathrm{cl}(\mathcal{O})$ as equivalence classes of proper $\mathcal{O}$-ideals) we have

$$[I]([J]j(E_L)) = [IJ]j(E_L) \text{ (using group action notation).}$$

Therefore

$$[I]([J]j(E_L)) = [I](j(E_{J^{-1}L})) = j(E_{I^{-1}J^{-1}L}) = j(E_{(JI)^{-1}L}) = [JI]j(E_L) = [IJ]j(E_L).$$

We have only used properties of fractional ideals and commutativity. We have completed the proof for the group action part.

Now we will show that it is free i.e., if there exists $[I] \in \mathrm{cl}(\mathcal{O})$ s.t. $[I]j(E_J) = j(E_J)$ then $[I]$ is the identity element, in our case I is principal. If $[I]j(E_J) = j(E_J)$ then $I^{-1}J$ and J must be homothetic since they define the same elliptic curve. By definition there exists a non-zero $\alpha \in K$ s.t. $I^{-1}J = \alpha J \implies I^{-1} = (\alpha)$ i.e., I^{-1} is principal which is equivalent to I being principal.

Next up is transitivity. This one is clear since we have shown before there is bijection between the finite sets $\mathrm{cl}(\mathcal{O})$ and $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$, the action must be transitive because if we take $j(E_J) \in \mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ and apply the action for all elements of $\mathrm{cl}(\mathcal{O})$ the images must be distinct because we have proven that the action is free. In other words the orbit of $j(E_J)$ is $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$. □

Definition 45. *Let X be a set and G be an abelian group. We say that X is a principal homogenous space for a group G if G acts freely and transitively on X. Alternatively, we can say that X is a G-torsor.*

Remark. For a G-torsor X we have that for all $x, y \in X$ there exists a unique $g \in G$ s.t. $gx = y$.

Corollary. Let $\mathcal{O}$ be order in an imaginary quadratic field. $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ is a $\mathrm{cl}(\mathcal{O})$-torsor.

Let's now investigate the relationship between the $\mathrm{cl}(\mathcal{O})$-action on $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ and isogenies between elliptic curves over $\mathbb{C}$ s.t. their endomorphism ring is $\mathcal{O}$ for some fixed $\mathcal{O}$ order. Recall Theorem 53, which basically characterizes how every isogeny between two elliptic curves over $\mathbb{C}$ looks like in terms of maps between tori.

Consider elliptic curves E_{L_1}, E_{L_2} over $\mathbb{C}$ where L_1, L_2 are their corresponding lattices and take $\lambda \in \mathrm{Hom}_{\mathbb{C}}(E_{L_1}, E_{L_2})$. By Theorem 53 there exists a unique $\alpha \in \mathbb{C}$ s.t. $\alpha L_1 \subseteq L_2$ and the following diagram commutes

$$\begin{array}{ccc} \mathbb{C}/L_1 & \xrightarrow{\phi_\alpha} & \mathbb{C}/L_2 \\ \Phi_1 \downarrow & & \downarrow \Phi_2 \\ E_{L_1}(\mathbb{C}) & \xrightarrow{\lambda} & E_{L_2}(\mathbb{C}) \end{array}$$

where ϕ_α is the induced morphism by α. For quite a while we have been looking at lattices and elliptic curves in terms of homothety and isomorphism classes, we will apply this approach to this diagram as well. We can extend the diagram as follows

$$\begin{array}{ccccc} \mathbb{C}/L_1 & \xrightarrow{\phi'_\alpha} & \mathbb{C}/\alpha L_1 & \xrightarrow{\phi_1} & \mathbb{C}/L_2 \\ \Phi_1 \downarrow & & \Phi'_1 \downarrow & & \downarrow \Phi_2 \\ E_{L_1}(\mathbb{C}) & \xrightarrow{\psi} & E_{\alpha L_1}(\mathbb{C}) & \xrightarrow{\lambda'} & E_{L_2}(\mathbb{C}) \end{array}$$

where $\phi_\alpha = \phi_1 \circ \phi'_\alpha, \lambda = \lambda' \circ \psi$ and Φ'_1 is the corresponding isomorphism. In more detail:

$$\begin{array}{rl} \phi'_\alpha : & \mathbb{C}/L_1 \to \mathbb{C}/\alpha L_1 \\ & \beta + L_1 \mapsto \alpha\beta + \alpha L_1 \\ \phi_1 : & \mathbb{C}/\alpha L_1 \to \mathbb{C}/L_2 \\ & \beta + \alpha L_1 \mapsto \beta + L_2 \end{array}$$

and ψ is the isomorphism between elliptic curves E_{L_1} and $E_{\alpha L_1}$ which we know exists since the corresponding lattices are homothetic. Then $\lambda' = \lambda \circ \psi^{-1}$ i.e., λ, λ' are isomorphic isogenies. If we now set $L' = \alpha L_1$ we get a diagram

$$\begin{array}{ccc} \mathbb{C}/L' & \xrightarrow{\phi_1} & \mathbb{C}/L_2 \\ \Phi'_1 \downarrow & & \downarrow \Phi_2 \\ E_{L'}(\mathbb{C}) & \xrightarrow{\lambda'} & E_{L_2}(\mathbb{C}) \end{array}$$

In other words, the isogeny λ' is induced by the inclusion $L' \subseteq L_2$. This means that looking at lattices up to homothety, elliptic curves up to isomorphism and isogenies up to isomorphism, every element of $\mathrm{Hom}_{\mathbb{C}}(E_{L_1}, E_{L_2})$ arises from an inclusion of lattices $L' \subseteq L_2$, since up to isomorphism $\mathrm{Hom}_{\mathbb{C}}(E_{L_1}, E_{L_2}) = \mathrm{Hom}_{\mathbb{C}}(E_{L'}, E_{L_2})$.

Since isomorphism between elliptic curves is an isogeny of degree 1, it must be that $\deg(\lambda) = \deg(\lambda')$ and since we are in $\mathbb{C}$, then λ is clearly separable. Therefore we have $\deg(\lambda) = |\mathrm{Ker}(\lambda)| = |\mathrm{Ker}(\lambda')|$. Looking at the diagram above, we can easily see the relationship between the kernel and the index of lattices (as groups).

Since $L' \subseteq L_2$ and the definition of Φ_2, we see that $\beta \in \mathbb{C} : \Phi_2(0) = 0 \iff \beta \in L_2$. By the inclusion then automatically we see that $\beta \in L' \implies \Phi_2(\beta + L_2) = \Phi_2(0) = 0$. By the commutativity of the diagram we see that the points of $\mathbb{C}_1/L'$, which map to 0 (more precisely the point ∞) in $E_{L_2}(\mathbb{C})$, are precisely the points of L_2. All of the points of L' are reduced by Φ'_1 to 0 in $E_{L'}(\mathbb{C})$ and since λ' is an isogeny, clearly $\forall \beta \in L' : \lambda'(\Phi'(\beta)) = \lambda'(0) = 0$. Because L' is a normal subgroup of L_2, we can look at the other points of L_2 as elements of the quotient L_2/L', which has the size $|L_2/L'| = |L_2 : L'|$.

We have shown that $\deg(\lambda) = |L_2/L'| = |L_2 : L'|$. For example if we take an elliptic curve E_L and its endomorphism ring, the inclusion $nL \subseteq L$ ($|L : nL| = n$) corresponds to the isogeny $[n]$ (multiplication by n endomorphism).

Now we combine this knowledge with our previous discussion about the $\mathrm{cl}(\mathcal{O})$ action. Let's consider $\mathcal{O}$ be an order in an imaginary quadratic field and E_L to

be an elliptic curve over $\mathbb{C}$ s.t. $\mathrm{End}_{\mathbb{C}}(E) = \mathcal{O}$. We know L is homothetic to I where I is a proper (invertible) $\mathcal{O}$-ideal. So up to homothety we can take E_L to be E_I. Take a proper $\mathcal{O}$-ideal J. Since $IJ \subseteq I$ and J invertible $\implies I \subseteq J^{-1}I$. This is also an inclusion of lattices (up to homothety) thus it induces an isogeny $\lambda_J : E_I \to E_{J^{-1}I}$. This exactly corresponds to how our $\mathrm{cl}(\mathcal{O})$-action by J to E_I behaves.

Theorem 62. *Let $\mathcal{O}$ be an order in an imaginary quadratic field. Let E_1, E_2 be elliptic curves over $\mathbb{C}$ s.t. $\mathrm{End}_{\mathbb{C}}(E_1) = \mathcal{O} = \mathrm{End}_{\mathbb{C}}(E_2)$. Then there exists an isogeny $E_1 \to E_2$.*

For every isogeny $E_1 \to E_2$ there exists a proper $\mathcal{O}$-ideal J s.t. $E_1 \cong E_I$ and $E_2 \cong [J]E_I$ where I is a proper $\mathcal{O}$-ideal. Isomorphic isogenies correspond to the same element of $\mathrm{cl}(\mathcal{O})$.

Proof. As usual let L_1 be the corresponding lattice to E_1 and same for L_2. Using the endomorphism ring assumption, we know that L_1 is homothetic to a proper $\mathcal{O}$-ideal I and L_2 is homothetic to a proper $\mathcal{O}$-ideal J. Denote these curves $E_I \cong E_1$ and $E_J \cong E_2$.

Define another elliptic curve isomorphic to E_I as $E_{(\mathrm{N}(J))I}$ i.e., the curve corresponding to the proper $\mathcal{O}$-ideal $(\mathrm{N}(J))I$. By Theorem 58 $(\mathrm{N}(J))I = J\overline{J}I \iff J \mid \mathrm{N}(J))I \iff \mathrm{N}(J))I \subseteq J$. We can apply the same argument as in the paragraph above. We have the inclusion $(\mathrm{N}(J))I = (J\overline{J})I \subseteq J$.

Having an inclusion means that there is an isogeny $\lambda : E_{(\mathrm{N}(J))I} \to E_J$. If we set $M = (\mathrm{N}(J))IJ^{-1}$, which is an invertible $\mathcal{O}$-ideal, and look at the action of M upon $E_{(\mathrm{N}(J))I}$ we get

$$[M]E_{(\mathrm{N}(J))I} = E_{M^{-1}(\mathrm{N}(J))I} = E_{((\mathrm{N}(J))IJ^{-1})^{-1}(\mathrm{N}(J))I} = E_{JI^{-1}(\mathrm{N}(J))^{-1}(\mathrm{N}(J))I} = E_J.$$

We have an isogeny between two elliptic curves which is induced by an inclusion of lattices and also, we have found an element of $\mathrm{cl}(\mathcal{O})$ which acts in the same way. We have constructed an isogeny between E_1 and E_2 (λ together with a few isomorphisms, which is still an isogeny).

Every isogeny arises from an inclusion and we can always craft a proper ideal in the same way as we did s.t. the isogeny between the curves corresponds to an action by that ideal. □

Definition 46. *Let E be an elliptic curve over $\mathbb{C}$ s.t. $\mathrm{End}_{\mathbb{C}}(E) = \mathcal{O}$ where $\mathcal{O}$ is an order in an imaginary quadratic field K and let I be an $\mathcal{O}$-ideal. The I-torsion subgroup of $E(\mathbb{C})$ is*

$$E[I] = \{P \in E(\mathbb{C}) : \forall \alpha \in I \ \alpha(P) = 0\}$$

Theorem 63. *Let E be an elliptic curve over $\mathbb{C}$ s.t. $\mathrm{End}_{\mathbb{C}}(E) = \mathcal{O}$ where $\mathcal{O}$ is an order in an imaginary quadratic field K and let I be a proper $\mathcal{O}$-ideal. Let λ_I be the corresponding isogeny $E \to [I]E$ from Theorem 62. Then $\deg(\lambda_I) = \mathrm{N}(I)$ and $\mathrm{Ker}(\lambda_I) = E[I]$.*

Proof. [Sut19] Lecture 18, Theorem 18.14. □

Which all can be summed up to:

Theorem 64. *Let $\mathcal{O}$ be an order in an imaginary quadratic field and let I be a proper $\mathcal{O}$-ideal. Let E be an elliptic curve s.t.* $\mathrm{End}_{\mathbb{C}}(E) = \mathcal{O}$ *then there exists an isogeny* $\lambda_I : E \to [I]E$ *s.t.* $\deg(\lambda_I) = \mathrm{N}(I)$.

Proof. This is basically a rephrased Theorem 63. □

Recall that $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ is a $\mathrm{cl}(\mathcal{O})$-torsor, this means that between any two elliptic curves with $\mathcal{O}$ as an endomorphism ring there exists an element of $\mathrm{cl}(\mathcal{O})$ which means there exists an isogeny of some degree (depends on the norm of the element).

4. The road from $\mathbb{C}$ to $\mathbb{F}_q$

In the last chapter, we have been exclusively working with elliptic curves over $\mathbb{C}$ but in practice we want to work with elliptic curves over finite fields.

In this chapter we show that we can transfer the most important results from $\mathbb{C}$ to a finite field.

Definition 47. *Let $\mathcal{O}$ be an order in an imaginary quadratic field s.t.* $\operatorname{disc}(\mathcal{O}) = D$. *The Hilbert class polynomial of $\mathcal{O}$ is a polynomial of the form:*

$$H_{\mathcal{O}}(x) = H_D(x) = \prod_{j(E)\in \mathrm{Ell}_{\mathcal{O}}(\mathbb{C})} (x - j(E)).$$

Theorem 65. *Let $\mathcal{O}$ be an order in an imaginary quadratic field. $H_{\mathcal{O}}(x) \in \mathbb{Z}[x]$.*

Proof. [Sut19] Lecture 21, Theorem 21.12. □

Corollary. Let $\mathcal{O}$ be an order in an imaginary quadratic field. Let E be an elliptic curve over $\mathbb{C}$ s.t. $\mathrm{End}_{\mathbb{C}}(E) = \mathcal{O}$. Then $j(E)$ is an algebraic integer.

Let $\mathcal{O}$ be an order in an imaginary quadratic field $K = \mathbb{Q}(\sqrt{D})$. We will for a while work with the splitting field of $H_{\mathcal{O}}(x)$ over K which we will call L. L/K is a finite Galois extension because L is a splitting field of a separable polynomial (by definition $H_{\mathcal{O}}(x)$ is separable).

Then $\forall j(E) \in \mathrm{Ell}_{\mathcal{O}}(\mathbb{C}) \implies j(E) \in L$. Also, since $j(E)$ is an algebraic integer, then $j(E) \in \mathcal{O}_L$.

Using Theorem 2 we can construct an elliptic curve given by a Weierstrass equation where the coefficients lie in $\mathcal{O}_L$ i.e., the elliptic curve is defined over L.

$\mathcal{O}_K, \mathcal{O}_L$ (clearly $\mathcal{O}_K \subseteq \mathcal{O}_L$ because $K \leq L$) are Dedekind domains which means that every proper ideal has a unique factorization into prime ideals and every prime ideal is maximal.

Let $P \subseteq \mathcal{O}_L$ be a prime ideal. The quotient ring $\mathcal{O}_L/P$ is field since P is a maximal ideal and it is a finite field since $\mathrm{N}(P) = |\mathcal{O}_L : P| \in \mathbb{N}$. All finite fields have cardinality of the form p^n for a prime p and $n \in \mathbb{N}$, this shows that the norm of a prime ideal is also of the form p^n.

Take a prime ideal P in $\mathcal{O}_K$ and consider the ideal $P\mathcal{O}_L \subseteq \mathcal{O}_L$. Since $\mathcal{O}_L$ is a Dedekind domain we have a unique decomposition of $P\mathcal{O}_L$ into prime ideals: $P\mathcal{O}_L = Q_1 \dots Q_n$ where $n \in \mathbb{N}, \forall 1 \leq i \leq n : Q_i$ is a prime ideal in $\mathcal{O}_L$.

Remark. For a prime P in $\mathcal{O}_K$ denote as $Q|P$ the set of Q_is where $P\mathcal{O}_L = Q_1 \dots Q_n$ is the prime decomposition.

Definition 48. *Let L/K be a finite Galois extension where K is an imaginary quadratic field and let P be a prime ideal of $\mathcal{O}_K$. If the prime ideals of $\mathcal{O}_L$ of the prime decomposition of the ideal $P\mathcal{O}_L$ are distinct, we say that P is unramified in L.*

Remark. Let L/K be a finite Galois extension where K is an imaginary quadratic field. There are only finitely many prime ideals of $\mathcal{O}_K$ that are not unramified in L. For proof see [Mar18] Chapter 3, Theorem 24 and Corollary 3.

Definition 49. *Let L/K be a finite Galois extension where K is an imaginary quadratic field. Let $p \in \mathbb{Z} \subset K$ be a prime. We say that*

(a) p is unramified in L, if $Q|(p)$ are distinct prime ideals.

(b) p splits completely in L, if $Q|(p)$ are distinct prime ideals of norm p.

If we take $\sigma \in \mathrm{Gal}(L/K)$ and apply it to our prime decomposition we get on the left side

$$\sigma(P\mathcal{O}_L) = \sigma(P)\sigma(\mathcal{O}_L) = P\mathcal{O}_L$$

because σ fixes elements of K and also must map algebraic integers of L to algebraic integers of L (it is an automorphism of L). On the left side we get

$$\sigma(Q_1 \dots Qn) = \sigma(Q_1) \dots \sigma(Qn) = Q_{\sigma'(1)} \dots Q_{\sigma'(n)}.$$

In other words, σ maps prime ideals upon prime ideals and, since we have a unique factorization, the worst it can do is permute them.

From now on we consider only σ s.t. σ' is an identity (the permutation is trivial). Fix a prime ideal P in $\mathcal{O}_K$ and fix an ideal $Q \in Q|P$. Since $\sigma(Q) = Q$ we have an induced automorphism $\overline{\sigma}$ of the quotient ring $\mathcal{O}_L/Q$ that is defined as $\overline{\sigma}(\phi_Q(x)) = \phi_Q(\sigma(x))$ where ϕ_Q is the canonical map $\mathcal{O}_L \to \mathcal{O}_L/Q$ for all $x \in \mathcal{O}_L$.

As mentioned before, $\mathcal{O}_L/Q$ is a finite field. If we take a look at the image of $\mathcal{O}_K \subseteq \mathcal{O}_L$ by ϕ_Q we have

$$\phi_Q(\mathcal{O}_K) = \mathcal{O}_K/(\mathcal{O}_K \cap Q) = \mathcal{O}_K/P.$$

This comes from the definiton of Q, since Q contains the ideal P. Because $\mathcal{O}_K/P \subseteq \mathcal{O}_L/Q$ are both finite fields we also get that $\mathcal{O}_K/P$ is a subfield of $\mathcal{O}_L/Q$. Denote these finite fields as $\mathbb{F}_P$ and $\mathbb{F}_Q$. They must have the same characteristic p which comes from the norm of the ideals.

Let's get back to elliptic curves. Consider an elliptic curve E over $\mathbb{C}$ s.t. $\mathrm{End}_{\mathbb{C}}(E) = \mathcal{O}$ where $\mathcal{O}$ is an order in an imaginary quadratic field K. Let L be the splitting field $H_{\mathcal{O}}(x)$. At the start of the chapter, we noted that $j(E)$ is an algebraic integer and by definition of L it means that $j(E) \in \mathcal{O}_L$. Using Theorem 2 we know that E can be given by a Weierstrass equation in the form $y^2 = x^3 + Ax + B$ where $A, B \in \mathcal{O}_L$ as well.

Assuming $\Delta(E) \notin Q$ ($\Delta(E)$ is also an element of $\mathcal{O}_L$), there is nothing preventing us from defining a new elliptic curve $\overline{E}$ over the finite field $\mathbb{F}_Q$ given by the polynomial $y^2 = x^3 + \phi_Q(A)x + \phi_Q(B)$.

Definition 50. *Let E be an elliptic curve over $\mathbb{C}$ s.t. $\mathrm{End}_{\mathbb{C}}(E) = \mathcal{O}$ where $\mathcal{O}$ is an order in an imaginary quadratic field K. Let L be the splitting field $H_{\mathcal{O}}(x)$ and Q a prime ideal of $\mathcal{O}_L$. We that that E has good reduction modulo Q if $\Delta(E) \notin Q$.*

Remark. There are only finitely many prime ideals Q of $\mathcal{O}_L$ s.t. the curve from previous definition does not have good reduction modulo Q. This is a consequence of $(\Delta(E))$ being divisible only by finitely many prime ideals in $\mathcal{O}_L$.

The following theorem tells us that in our use case we do not have to consider curves over $\mathbb{C}$ but only over L.

Definition 51. *Let L, K be field extensions over a field k. We say $L.K$ is a compositum of L, K where $L.K = k(K \cup L)$. In other words, the compositum of L, K is the smallest field containing L and K.*

Theorem 66. *Let $\mathcal{O}$ be an order in an imaginary quadratic field K and let E be an elliptic curve over $L \subseteq \mathbb{C}$ s.t. $\mathrm{End}_{\overline{L}}(E) = \mathcal{O}$. Then $\mathrm{End}_{\overline{L}}(E) = \mathrm{End}_{L.K}(E)$.*

Proof. [Sil94] Theorem 2.2 (b). □

Corollary. Let $\mathcal{O}$ be an order in an imaginary quadratic field K and let E be an elliptic curve over L where L is the splitting field of $H_{\mathcal{O}}(x)$ over K. Then $\mathrm{End}_{\overline{L}}(E) = \mathrm{End}_L(E)$.

Corollary. Let $\mathcal{O}$ be an order in an imaginary quadratic field K and let E be an elliptic curve over L where L is the splitting field of $H_{\mathcal{O}}(x)$ over K. Then $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C}) = \mathrm{Ell}_{\mathcal{O}}(L)$.

Proof. The inclusion $\mathrm{Ell}_{\mathcal{O}}(L) \subseteq \mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ is clear since $L \subseteq \mathbb{C}$ and $\mathrm{End}_{\overline{L}}(E) \subseteq \mathrm{End}_{\mathbb{C}}(E)$.

The other inclusion comes from Theorem 65 and Theorem 66. Let $j(E) \in \mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ i.e., E is an elliptic curve defined over $\mathbb{C}$ and $\mathrm{End}_{\mathbb{C}}(E) = \mathcal{O}$. By Theorem 65 this curve is actually defined over L thus it must be $\mathrm{End}_{\mathbb{C}}(E) = \mathrm{End}_{\overline{L}}(E)$. By Theorem 66 we have $\mathrm{End}_{\overline{L}}(E) = \mathrm{End}_L(E)$. □

Theorem 67. *Let E, E' be elliptic curves defined over $K \subseteq \mathbb{C}$. Then there exists a finite extension K'/K s.t. $\mathrm{Hom}_{\overline{K}}(E, E') = \mathrm{Hom}_{K'}(E, E')$.*

Proof. [Sil94] Theorem 2.2 (c). □

Definition 52. *Let p be a prime and D be an integer. If $p = 2$, then define the Kronecker symbol denoted as $\left(\frac{D}{p}\right)$ as*

$$\left(\frac{D}{2}\right) = \begin{cases} 0 & 2 \mid D \\ 1 & D \equiv \pm 1 \mod 8 \\ -1 & D \equiv \pm 3 \mod 8. \end{cases}$$

For $p > 2$ define it as

$$\left(\frac{D}{p}\right) = \begin{cases} 0 & D \equiv 0 \mod p \\ 1 & D \text{ is a quadratic residue modulo } p. \\ -1 & D \text{ is not a quadratic residue modulo } p. \end{cases}$$

Remark. For $p > 2$ we can define the Kronecker symbol as

$$\left(\frac{D}{p}\right) = |\{x \in \mathbb{F}_p : x^2 = (D \mod p)\}| - 1.$$

Remark. The Kronecker symbol is the Legendre symbol for $p > 2$. The only difference is that Kronecker is defined also for $p = 2$.

Definition 53. *Let $K = \mathbb{Q}(\sqrt{D})$ be an imaginary quadratic field and let $p \in \mathbb{Z}$ be a prime. We say that*

(a) *p splits in K* if $(p)\mathcal{O}_K$ *factors into 2 distinct prime ideals.*

(b) *p ramifies in K* if $(p)\mathcal{O}_K$ *factors into a square of a prime ideal.*

(c) *p is inert in K* if $(p)\mathcal{O}_K$ *is a prime ideal.*

Theorem 68. *Let $\mathcal{O}$ be an order with discriminant D in an imaginary quadratic field K and let p be a prime. If $p \mid |\mathcal{O}_K : \mathcal{O}|$, then there are no proper $\mathcal{O}$-ideals of norm p. Otherwise the number of such ideals is $1 - \left(\frac{D}{p}\right) \in \{0, 1, 2\}$. More specifically:*

(a) $1 - \left(\frac{D}{p}\right) = 0 \iff p$ *is inert in* K.

(b) $1 - \left(\frac{D}{p}\right) = 1 \iff p$ *is ramified in* K.

(c) $1 - \left(\frac{D}{p}\right) = 2 \iff p$ *splits in* K.

Corollary. Let $\mathcal{O}$ be an order with discriminant D in an imaginary quadratic field K, let p be a prime and let L be the splitting field of $H_D(x)$ over K. If $p \nmid D$, then p is unramified in L.

Proof. [Sut19] Lecture 22, the discussion before Corollary 22.8. □

Lemma 69. *Let $K = \mathbb{Q}(\sqrt{D})$ be an imaginary quadratic field, let q be a prime and $\mathcal{O} = [1, \alpha], \alpha \notin \mathbb{Z}$ s.t. $|\mathcal{O}_K : \mathcal{O}| = f$. Every $\mathcal{O}$-ideal of norm q is of the form $Q = [q, \alpha - \delta]$ where δ is a root of $\min_{\mathbb{Q}}(\alpha) \mod q$. The number of such ideals is $1 - \left(\frac{D}{q}\right) \in \{0, 1, 2\}$ and the factorization of the $\mathcal{O}$ ideal (q) into prime ideals is*

$$(q) = \begin{cases} Q\overline{Q} & \text{if } \left(\frac{D}{q}\right) = 1 \\ Q^2 & \text{if } \left(\frac{D}{q}\right) = 0 \\ (q) & \text{if } \left(\frac{D}{q}\right) = -1 \end{cases}$$

where in the first case $Q \neq \overline{Q}$.

Proof. This Lemma is a generalized version of [Sut19], Lecture 22, Lemma 22.6.

The minimal polynomial of α over $\mathbb{Q}$ is $f(x) = x^2 - (\alpha + \overline{\alpha})x + \alpha\overline{\alpha} \in \mathbb{Z}[x]$. Let Q be a $\mathcal{O}$-ideal of norm q. By Lagrange theorem we have $\mathrm{N}(Q) \cdot (1 + Q) = 0 + Q$ (in the quotient group $\mathcal{O}/Q$) which is equivalent to saying $\mathrm{N}(Q) = q \in Q \implies (q) \subseteq Q$.

Every integer in Q must be a multiple of q because otherwise we would have $Q = \mathcal{O}$. That would be a contradiction with Q being of norm q.

Thus $Q \cap \mathbb{Z} = (q)$. From that we can assume that Q is of the form $[q, a\alpha - \delta]$ for some $a, \delta \in \mathbb{Z}$ but since $[\mathcal{O} : Q] = q$ we get $a = 1$.

By properties of Q being an $\mathcal{O}$-ideal we get that

$$(\alpha - \delta)(\overline{\alpha} - \delta) = \alpha\overline{\alpha} - (\alpha + \overline{\alpha})\delta + \delta^2 = f(\delta) \in Q.$$

$f(\delta)$ is an integer that is an element of Q which implies $\delta \in (q)$. This also shows that δ is a root of $f(x) \mod q$.

On the other hand, if δ is a root of $f(x) \mod q$, then $[q, \alpha - \delta]$ is a $\mathcal{O}$-ideal of norm q. If $f(x) \mod q$ has distinct roots δ, λ modulo q, then $[q, \alpha - \delta], [q, \alpha - \lambda]$ define different ideals.

We have shown that the number of different ideals of $\mathcal{O}$ of norm q corresponds to the number of distinct roots of $f(x) \mod q$. The discriminant of $f(x)$ is $(\alpha+\overline{\alpha})^2 - 4\alpha\overline{\alpha} = (\alpha-\overline{\alpha})^2 = \text{disc}(\mathcal{O}) = f^2 D$.

Thus, the number of distinct roots of $f(x) \mod q$ corresponds to the value $1 - \left(\frac{D}{q}\right)$ if $q > 2$. For $q = 2$ this can be shown similarly but, in our applications, we will work with $q > 2$ so we omit the proof. □

Theorem 70. *Let $\mathcal{O}$ be an order with discriminant D in an imaginary quadratic field K, let L be the splitting field of $H_D(x)$ over K and let $p \in \mathbb{Z}, p > 2$ be a prime s.t. $p \nmid D$. Then the following are equivalent:*

(a) There exists a principal $\mathcal{O}$-ideal of norm p.

(b) $\left(\frac{D}{p}\right) = 1$ and $H_D(x)$ splits into linear factors in $\mathbb{F}_p[x]$.

(c) p splits completely in L.

(d) There exists $t, v \in \mathbb{Z}$ s.t. $t \not\equiv 0 \mod p$ and $4p = t^2 - v^2 D$.

Proof. [Sut19] Lecture 22, Theorem 22.5. □

Theorem 70 gives us characterization when p splits completely in L. Assume we have $p \nmid D$ where D is the discriminant of some order $\mathcal{O}$ in an imaginary quadratic field K and assume there exist such t and v. We know that there exists a prime ideal Q in $\mathcal{O}_L$ and $\text{N}(Q) = p$. This means that $\mathcal{O}_L/Q \cong \mathbb{F}_p$. We can reduce every root of $H_D(x)$ to an element of $\mathbb{F}_p$ by our canonical map.

Choose an elliptic curve E s.t. $j(E)$ is one of the roots of $H_D(x)$. By definition $\text{End}_L(E) = \mathcal{O}$ (since $\text{Ell}_{\mathcal{O}}(L) = \text{Ell}_{\mathcal{O}}(\mathbb{C})$). We also get a reduction modulo Q i.e., an elliptic curve $\overline{E}$ over $\mathbb{F}_p$.

A non-zero element $\psi \in \text{End}_L(E)$ can be always expressed as a rational function with coefficients in $\mathcal{O}_L$ due to L being the fraction field of $\mathcal{O}_L$. We can reduce these coefficients by our map $\mathcal{O}_L \to \mathbb{F}_p$. Denote this reduced endomorphism by $\overline{\psi}$. It is actually an endomorphism of $\overline{E}$ because if we consider E in the projective sense and look at the rational points $\forall P \in E(L) \iff F(P) = 0$ where $F \in \mathcal{O}_L[X, Y, Z]$. The curve $\overline{E}/\mathbb{F}_p$ is defined by $\overline{F} \in \mathbb{F}_p[X, Y, Z]$ where $\overline{F}$ is the reduction of F. Then $\forall P \in E$ we have $F(\psi(P)) = 0$ since ψ is an endomorphism. This equality still holds if we apply the reduction map. Only issue could be with points which have coordinates that are all reduced upon $(0:0:0)$ i.e., all divisible by p. In that case we can always consider another point representation where all points are not divisible by p.

We know that $\forall P \in E : \psi^2(P) \ominus [\text{Tr}(\psi)]\psi(P) = \ominus[\deg(\psi)](P)$. Applying the reduction map we get $\overline{\psi^2}(\overline{P}) \ominus [\text{Tr}(\psi)]\overline{\psi}(\overline{P}) = \ominus[\deg(\psi)](\overline{P})$. Note that the maps $[n]$ still present the n-point addition on elliptic curves. In the first one we have addition on E and in the second one we have addition on $\overline{E}$.

Therefore, $\overline{\psi}$ is a non-zero isogeny (the map $[\deg(\psi)]$ has only finitely many points in its kernel) and it must be that $\text{Tr}(\psi) = \text{Tr}(\overline{\psi})$ and $\deg(\psi) = \deg(\overline{\psi})$.

We have now shown that the reduction map of endomorphisms is an injective (because non-zero endomorphisms map to non-zero endomorphisms) homomorphism between rings $\text{End}_L(E) \hookrightarrow \text{End}_{\mathbb{F}_p}(\overline{E})$.

Note, this reduction is somewhat loosely stated but helps in understanding what is going on. For details refer to [Lan12] or [Sil94].

We can sum this up in a theorem.

Theorem 71. *Let $\mathcal{O}$ be an order with discriminant D in an imaginary quadratic field K, let L be the splitting field of $H_D(x)$ over K and let $p \in \mathbb{Z}$ be an odd prime s.t. $p \nmid D$ and $4p = t^2 - v^2 D$ for some $t, v \in \mathbb{Z}, t \not\equiv 0 \mod p$. If E is an elliptic curve over L s.t. $\mathrm{End}_L(E) = \mathcal{O}$, then E has good reduction $\overline{E}$ modulo Q where Q is a prime ideal of $\mathcal{O}_L$ of norm p. The reduction $\overline{E}$ is also an ordinary curve and the Frobenius endomorphism $\boldsymbol{\phi}$ of $\overline{E}/\mathbb{F}_p$ satisfies $\mathrm{Tr}(\boldsymbol{\phi}) = \pm t \not\equiv 0 \mod p$.*

Proof. The discussion before together with [Sut19] Lecture 22, Corollary 22.9. □

Using what we have learned we have now a way how to construct an elliptic curve over $\mathbb{F}_p$ with a preset number of rational points. We won't present it here but it can be found in literature under the name CM method or see the discussion in [Sut19] Lecture 22 after Corollary 22.9.

Next up are one of the most important theorems which proves that the injective homomorphism $\mathrm{End}_L(E) \hookrightarrow \mathrm{End}_{\mathbb{F}_p}(\overline{E})$ is an isomorphism.

Theorem 72. *Let $\overline{E}$ be an elliptic curve over $\mathbb{F}_q$ and let $\overline{\psi} \in \mathrm{End}_{\overline{\mathbb{F}_q}}(\overline{E})$ be non-zero. Then there exists an elliptic curve E over a number field L and an endomorphism $\psi \in \mathrm{End}_{\overline{L}}(E)$ s.t. E has good reduction modulo Q, where Q is a prime ideal of $\mathcal{O}_L$ of norm q, $\overline{E}$ is the reduction of E and the reduction of ψ is $\overline{\psi}$.*

Proof. [Lan12] Chapter 13, Theorem 14. □

Theorem 72 is called "The Deuring lifting theorem". The Deuring lifting theorem is the main reason why we can transfer the ideal class group action to elliptic curves over finite fields.

5. Isogeny graphs

Now we can finally define an isogeny graph. In this chapter we assume that K is a field and l is a prime s.t. $l \nmid \mathrm{char}(K)$.

Definition 54. *The K-rational l-isogeny graph is denoted by $G_l(K)$. $G_l(K) = (V, \mathcal{E})$ is a directed multigraph where V is the set of different elliptic curves over K. The edge (E_1, E_2) is present in $\mathcal{E}$ if there exists an l-isogeny $E_1 \to E_2$ defined over K. The edge (E_1, E_2) has multiplicity equal to the number of different l-isogenies $E_1 \to E_2$ defined over K. By "different" in the context of elliptic curves and isogenies we mean up to K-isomorphism.*

Remark. One might be eager to set $V = K$ since every $j \in K$ is a j-invariant of an elliptic curve over K by Theorem 2 (c). The only issue with this is that we would lose some vertices because j-invariant defines a curve up to $\overline{K}$-isomorphism but in our case, we need a finer distinction.

Remark. Considering K s.t. $\mathrm{char}(K) > 0$ then $G_l(K)$ has 2 disjoint subgraphs. The supersingular one and ordinary one. This is due to Theorem 18.

For every isogeny $E_1 \to E_2$ defined over K there exists its dual isogeny which is also defined over K. This means $(E_1, E_2) \in \mathcal{E} \iff (E_2, E_1) \in \mathcal{E}$. The multiplicities of both edges are the same if $j(E_1), j(E_2) \notin \{0, 1728\}$.

In case $j(E_1)$ or $j(E_2)$ is equal to 0 or 1728 the multiplicities might not match. This exceptional case is caused by extra automorphisms of curves with these j-invariants. Every curve has the automorphism $[-1]$ which does not change the kernel.

If $j(E_1) = 0$, then $\sqrt{-3} \in K$ (this is equivalent to saying that the 3rd root of unity is in K) and if $j(E_2) \notin \{0, 1728\}$, then E_1 has 2 extra automorphisms that do not fix the kernel. Therefore, every isogeny $E_1 \to E_2$ can be composed with one of these automorphisms and make a different isogeny. The corresponding dual isogenies have the same kernel i.e., they represent the same isogeny.

If $j(E_1) = 1728$ and the 4th root of unity is in K (i.e., $\sqrt{-1} \in K$) then we have one extra automorphism (technically there are 2 extra automorphisms, see the example below for details) which does not fix the kernel.

In our case we will work with fields where even if j-invariants are of values $0, 1728$ the automorphisms are not defined over K so the compositions with them are not K-rational i.e., they don't represent an edge and the multiplicities are the same.

Example 3. Let $E : y^2 = x^3 + x$ over $\mathbb{F}_q$. Assume we have a finite subgroup $H \leq E(\mathbb{F}_q)$ that induces an l-isogeny $\psi_H : E \to E'$ s.t. $j(E') \notin \{0, 1728\}$.

We calculate $j(E) = 1728$ which means we have 4 distinct automorphisms of E. Denote by $i \in \mathbb{F}_q$ the fourth root of unity. The automorphisms correspond to the values $\{i, i^2, i^3, 1\}$ by Theorem 6:

$$\begin{aligned}
\rho_1(x, y) &= (i^2 x, i^3 y) = (-x, -iy) \\
\rho_2(x, y) &= ((i^2)^2 x, (i^2)^3 y) = (x, -y) \\
\rho_3(x, y) &= ((i^3)^2 x, (i^3)^3 y) = (-x, iy) \\
\rho_4(x, y) &= ((i^4)^2 x, (i^4)^3 y) = (x, y)
\end{aligned}$$

Note that $\rho_2 = [-1], \rho_3 = [-1] \circ \rho_1, \rho_4 = [1]$.

As we noted before, the isogenies $[-1], [1]$ clearly do not change the kernel because if we compose ψ_H with them we get $\psi_H \circ [1] = \psi_H$ and $\psi_H \circ [-1]$. If $P \in \mathrm{Ker}(\psi_H) : \psi_H(P) = \mathcal{O}$ and $(\psi_H \circ [-1])(P) = \psi_H(-P) = -\psi_H(P) = -\mathcal{O} = \mathcal{O}$ because ψ_H is an isogeny and therefore a group homomorphism $E \to E'$.

The isogeny $\phi_H \circ \rho_1$ has a different kernel but the kernel has the same size because ρ_1 is an automorphism. To be precise, the kernel is $\rho_1^{-1}(H)$. The isogeny $\phi_H \circ \rho_3$ has the same kernel because $\rho_3 = [-1] \circ \rho_1$.

Assuming $\phi_H, \phi_H \circ \rho_1$ are the only two l-isogenies $E \to E'$ over $\mathbb{F}_q$, the edge (E, E') in $G_l(\mathbb{F}_q)$ has multiplicity 2 but the edge (E', E) has only multiplicity 1. This is because the dual isogeny $\widehat{\phi_H}$ has the same kernel as the dual isogeny $\widehat{\phi_H \circ \rho_1} = \widehat{\rho_1} \circ \widehat{\phi_H}$. Clearly $\widehat{\rho_1} = \rho_3$.

Claim 73. *$\sqrt{-1}, \sqrt{-3} \notin \mathbb{F}_p$ if and only if $p \equiv 11 \mod 12$.*

Proof. We want to know when $-1, -3$ are not quadratic residues modulo p. From number theory we know that a is not a quadratic residue modulo p iff $\left(\frac{a}{p}\right) = -1$ (using Legendre symbol). It is also well known that $\left(\frac{-1}{p}\right) = -1 \iff p \equiv 3 \mod 4$. Thus, we have one condition on p. We also want $\left(\frac{-3}{p}\right) = -1$. Using the properties of Legendre symbol we get

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right).$$

If $p \equiv 3 \mod 4$, then we want $\left(\frac{3}{p}\right) = 1$. This happens iff $p \equiv 1 \mod 12$ or $p \equiv 11 \mod 12$. The first case does not satisfy $p \equiv 3 \mod 4$ therefore the only option is $p \equiv 11 \mod 12$.

□

Theorem 74. *Let E_1, E_2 be elliptic curves over K and let $\psi \in \mathrm{Hom}(E_1, E_2)$ of degree l. Then $\mathrm{End}^0(E_1) \cong \mathrm{End}^0(E_2)$. If $\mathrm{End}^0(E_1) = K'$ is an imaginary quadratic field, then $\mathrm{End}(E_1) = \mathcal{O}_1, \mathrm{End}(E_2) = \mathcal{O}_2$. Both $\mathcal{O}_{1,2}$ are orders in K' and one of the following holds:*

(a) $\mathcal{O}_1 = \mathcal{O}_2$.

(b) $|\mathcal{O}_1 : \mathcal{O}_2| = l$.

(c) $|\mathcal{O}_2 : \mathcal{O}_1| = l$.

Proof. [Sut19] Lecture 23, Theorem 23.3. □

Using the previous theorem, we can characterize isogenies of degree l between two ordinary elliptic curves E_1, E_2.

Definition 55. *Under the assumptions of Theorem 74 we say that ψ is*

(a) *Horizontal* *if* $\mathcal{O}_1 = \mathcal{O}_2$.

(b) *Descending* *if* $|\mathcal{O}_1 : \mathcal{O}_2| = l$.

(c) *Ascending* *if* $|\mathcal{O}_2 : \mathcal{O}_1| = l$.

Descending and ascending isogenies are sometimes referred to as vertical isogenies.

Now we present a bit of graph theory which is essential to the understanding of the security of cryptographic algorithms which use isogeny graphs. Loosely speaking, we want random walks on these graphs to end up in random vertices.

Definition 56. *Let $n \in \mathbb{N}$. A random walk of length n on a graph $G = (V, \mathcal{E})$ is a path $v_1 \to \cdots \to v_n$ defined by a random process that selects v_i uniformly at random from the set of neighbors of v_{i-1} for all $2 \leq i \leq n$.*

Recall from graph theory that a degree of a vertex is the number of edges that this vertex is a part of. Let $k \in \mathbb{N}$, a k-regular graph is a graph where every vertex has a degree of k.

The adjacency matrix A^G of a graph $G = (V, \mathcal{E})$ is a $n \times n$ matrix where $n = |V|$ and $A^G_{i,j} = 1$ if there is an edge (v_i, v_j) and 0 otherwise. For an undirected graph this matrix is clearly symmetric which implies there are n real eigenvalues $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$.

If G is a k-regular graph, then $\lambda_1 = k$ and $\lambda_n \geq -k$.

Definition 57. *Let $G = (V, \mathcal{E})$ be a k-regular undirected multigraph and let $\epsilon \in \mathbb{R}, \epsilon > 0$. We say G is an ϵ-expander if $\lambda_2 \leq (1-\epsilon)k$ and $\lambda_n \geq -(1-\epsilon)k$.*

Theorem 75. *Let $G = (V, \mathcal{E})$ be a k-regular ϵ-expander and let $V' \subseteq V$ s.t. $|V'| \geq 1$. Then a random walk on G of length at least*

$$\frac{\log\left(\frac{2|V|}{\sqrt{|V'|}}\right)}{\log(1+\epsilon)} = \log_{1+\epsilon}\left(\frac{2|V|}{\sqrt{|V'|}}\right)$$

ends in V' with probability between $\frac{|V'|}{2|V|}$ and $\frac{3|V'|}{2|V|}$.

Proof. [JMV09] Lemma 2.1. □

Theorem 76. *Let $\mathcal{O}$ be an order in an imaginary quadratic field s.t. $\mathrm{disc}(\mathcal{O}) = D$, let $\delta > 0$, let q be a prime power and define a set $S = \{l \in \mathbb{Z} : l \text{ prime s.t. } l \leq (\log(|D|))^{2+\delta}\}$. Denote by $G_S(\mathbb{F}_q)$ the union of graphs $\{G_l(\mathbb{F}_q) : l \in S\}$. Then, assuming the Generalized Riemann Hypothesis, there exists $\epsilon > 0$ s.t. the subgraph G of $G_S(\mathbb{F}_q)$, which consists of vertices in $\mathrm{Ell}_{\mathbb{F}_q}(\mathcal{O})$[1], is an ϵ-expander as $q \to \infty$.*

Proof. [JMV09] Theorem 3.2. □

Remark. The value of ϵ is dependent on the value of δ. For details refer to [JMV09].

The previous 2 theorems are very technical. To rephrase them more "practically": they show that if we pick a vertex v and a walk of logarithmic length (in the number of vertices of G) on G then we end up in a vertex v' with a probability close to uniform. And that the union of $G_{l_i}(\mathbb{F}_q)$ for specific set of l_is has this property.

[1] We take the subgraph of $G_S(\mathbb{F}_q)$ with only horizontal isogenies and curves that have the endomorphism ring $\mathcal{O}$.

5.1 Ordinary curves

This section provides theory about the structure of isogeny graphs of ordinary curves and defines the class group action on $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$.

Note that we are working with ordinary curves but the theory can be applied also to special cases. For example, in CSIDH we work with supersingular curves but only with the $\mathbb{F}_p$-rational subset of the endomorphism ring which is isomorphic to an order in an imaginary quadratic field. For details refer to the end of the Section 5.2.

We now present a theorem which tells us how many isogenies of what type are there between curves with complex multiplication.

Theorem 77. *Let E be a curve over $\mathbb{F}_q$ and let $\mathrm{End}(E) = \mathcal{O}$ where $\mathcal{O}$ is an order in an imaginary quadratic field K s.t. $\mathrm{disc}(\mathcal{O}) = D$ and $\gcd(D, q) = 1$.*

(a) If $l \nmid |\mathcal{O}_K : \mathcal{O}|$, then there exist $1 - \left(\frac{D}{l}\right)$ different horizontal isogenies of degree l and 0 ascending isogenies of degree l.

(b) If $l \mid |\mathcal{O}_K : \mathcal{O}|$, then there exist 0 horizontal isogenies of degree l and a 1 ascending isogeny of degree l.

(c) Let $\mathcal{O}'$ be the order of index l in $\mathcal{O}$. If $\mathrm{Ell}_{\mathcal{O}'}(\mathbb{F}_q)$ is non-empty, then there exist $l + \left(\frac{D}{l}\right)$ different descending isogenies of degree l. Otherwise there are 0 descending isogenies of degree l.

Proof. [Sut19] Lecture 23, Corollary 23.7. □

Remark. By different (isogenies) we mean up to $\mathbb{F}_q$-isomorphism because if E is ordinary, then $\mathrm{End}_{\mathbb{F}_q}(E) = \mathrm{End}_{\overline{\mathbb{F}_q}}(E) = \mathrm{End}(E)$.

The following definition has already been introduced but only in the context of curves over $\mathbb{C}$. We are going to generalize it.

Definition 58. *Let E be an elliptic curve over K s.t. $\mathrm{End}(E) = \mathcal{O}$ where $\mathcal{O}$ is an order in an imaginary quadratic field and let I be a proper $\mathcal{O}$-ideal. The I-torsion subgroup of $E(\overline{K})$ is*

$$E[I] = \{P \in E(\overline{K}) : \forall \psi \in I, P \in \mathrm{Ker}(\psi)\}.$$

Note that as in the previous definition we have $\psi \in I \subseteq \mathcal{O} \cong \mathrm{End}(E)$ (we usually write "=" for simplicity) i.e., we automatically assume that ψ is the element of $\mathrm{End}(E)$ which is isomorphic to an element of I. We can show that $|E[I]| = N(I)$ using the same steps in the proof of Theorem 63 and using reduction of isogenies.

Assume $\overline{E}$ is an elliptic curve over $\mathbb{F}_q$ s.t. $\mathrm{End}(\overline{E}) = \mathcal{O}$ where $\mathcal{O}$ is an order in an imaginary quadratic field K. Let $D = \mathrm{disc}(\mathcal{O})$ and let I be a proper $\mathcal{O}$-ideal of norm $\mathrm{N}(I) = l$ where l is a prime s.t. $\gcd(D, q) = 1 = \gcd(q, l)$.

$\overline{E}[I]$ is a finite subgroup of $\overline{E}(\overline{\mathbb{F}_q})$ thus by Theorem 14 there exists a separable isogeny $\overline{\psi_I} : \overline{E} \to \overline{E}/\overline{E}[I]$. By definition $\mathrm{Ker}(\overline{\psi_I}) = \overline{E}[I] = \mathrm{N}(I) = l$ and because $\overline{\psi_I}$ is separable (because of the prime degree), we have $\deg(\overline{\psi_I}) = |\mathrm{Ker}(\overline{\psi_I})| = l$. This isogeny is unique up to $\overline{\mathbb{F}_q}$-isomorphism by Theorem 14.

We can then use Theorem 72 to lift $\overline{E}$ and $\overline{\psi_I}$ to its corresponding elliptic curve E and isogeny ψ_I defined over a number field $L \subseteq \mathbb{C}$. Since $\gcd(l, q) = 1$ we must

have $\deg(\psi_I) = \deg(\overline{\psi_I}) = l$. Also, since $\overline{E}[l] \cong E[l]$ (due to the reduction and $\gcd(l, q) = 1$) we must have $\mathrm{Ker}(\psi_I) \cong \mathrm{Ker}(\overline{\psi_I})$.

The lifted isogeny corresponds to the action of $[I] \in \mathrm{cl}(\mathcal{O})$ on $\mathrm{Ell}_{\mathcal{O}}(L)$ (the kernel of the lifted isogeny is $E[I]$). This also shows that $\mathrm{End}(\overline{E}/\overline{E}[I]) = \mathcal{O}$. In other words, $\overline{\psi_I}$ is a horizontal isogeny.

Using Theorem 59 we can always find an ideal of prime norm l s.t. $\gcd(l, q) = 1 = \gcd(q, D)$. We have now basically shown that we can define the action of $\mathrm{cl}(\mathcal{O})$ on $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$.

Theorem 78. *Let $\mathcal{O}$ be an order in an imaginary quadratic field s.t. $\mathrm{disc}(\mathcal{O}) = D$ and let q be a prime power s.t. $\gcd(q, D) = 1 = \gcd(l, q)$. If $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$ is non-empty, then it is a $\mathrm{cl}(\mathcal{O})$-torsor where the action of the ideal class of a proper $\mathcal{O}$-ideal of prime norm l is given by a horizontal isogeny of degree l, the inverse of the action is given by the inverse ideal which corresponds to the dual isogeny.*

Proof. Follows from the discussion before. □

5.2 Supersingular curves

This section provides theory about the structure of isogeny graphs of supersingular curves. This chapter mainly contains theorems crucial to the CSIDH algorithm.

Theorem 79. *Let E be an elliptic curve over $\mathbb{F}_q$, let l be a prime s.t. $\gcd(l, q) = 1$. The number of $\mathbb{F}_q$-rational l-isogenies from E can be characterized as follows:*

1. *If $\boldsymbol{\phi}^e$ (as a linear map on $E[l]$ over $\mathbb{F}_l$) has no eigenvalues, then there are no $\mathbb{F}_q$-rational l-isogenies.*
2. *If $\boldsymbol{\phi}^e$ has one eigenvalue of geometric multiplicity 1, then there is one $\mathbb{F}_q$-rational l-isogeny.*
3. *If $\boldsymbol{\phi}^e$ has one eigenvalue of geometric multiplicity 2, then there are $l + 1$ $\mathbb{F}_q$-rational l-isogenies.*
4. *If $\boldsymbol{\phi}^e$ has 2 eigenvalues (of geometric multiplicity 1), then there are 2 $\mathbb{F}_q$-rational l-isogenies.*

Proof. We know $E[l] \cong \mathbb{Z}_l \times \mathbb{Z}_l$ by Theorem 13 i.e., $E[l]$ a vector space over $\mathbb{F}_l$ of dimension 2. $\boldsymbol{\phi}^e$ is an isogeny so we can look at it as a linear map on $E[l]$. As a linear map on $E[l]$, $\boldsymbol{\phi}^e$ can have $0, 1$ or 2 eigenvalues.

Every isogeny is uniquely determined by its kernel. If there is a $\mathbb{F}_q$-rational l-isogeny, then there must be a cyclic (because l is prime) subgroup of $E[l]$. If there is a subgroup $G = \langle P \rangle \leq E[l]$ s.t. $\boldsymbol{\phi}^e(G) = G$, then there exists $\lambda \in \mathbb{F}_l$ s.t. $\boldsymbol{\phi}^e(P) = \lambda P$ i.e., λ is an eigenvalue of $\boldsymbol{\phi}^e$.

If the geometric multiplicity of λ is 1, then its eigenspace is G i.e., λ corresponds to one isogeny. If there is another μ eigenvalue, then we have a different eigenspace which is a kernel of another isogeny. Similarly, if the geometric multiplicity of λ is 2, then we have $l + 1$ different subgroups corresponding to different isogenies.

The case when there is no eigenvalue is also clear (if there is a $\mathbb{F}_q$-rational l-isogeny, then there must be a cyclic subgroup which would give us an eigenvalue). □

Theorem 80. *Let $p \equiv 3 \mod 4$ and let E be a supersingular curve over $\mathbb{F}_p$. Then $\mathrm{End}_{\mathbb{F}_p}(E) \cong \mathbb{Z}[\phi]$ or $\mathrm{End}_{\mathbb{F}_p}(E) \cong \mathbb{Z}\left[\frac{-p+\phi}{2}\right]$. Specifically $\mathrm{End}_{\mathbb{F}_p}(E) \cong \mathbb{Z}\left[\frac{-p+\phi}{2}\right]$ if and only if E has 2 distinct $\mathbb{F}_p$-rational points of order 2.*

Proof. Since E is supersingular, then $\mathrm{Tr}(\phi) = 0$ by Claim 32. A consequence of that is that its endomorphism algebra is isomorphic to $K = \mathbb{Q}(\sqrt{-p})$ by Claim 37 and the endomorphism ring is isomorphic to an order $\mathcal{O}$ in $\mathbb{Q}(\sqrt{-p})$. By Corollary 1.1 we know that $\mathrm{disc}(\mathcal{O}) = D = f^2 D_K$ where $D_K = \mathrm{disc}(\mathcal{O}_K)$ and $f = |\mathcal{O}_K : \mathcal{O}|$.

We have $p \equiv 3 \mod 4$ which implies $D_K = -p$. By theorems 1 and 38 we have $\mathbb{Z}[\phi] \subseteq \mathrm{End}_{\mathbb{F}_p}(E) \subseteq \mathbb{Z}\left[\frac{-p+\sqrt{-p}}{2}\right] = \mathbb{Z}\left[\frac{-p+\phi}{2}\right]$. Clearly, the conductor $f = 2$, so $\mathrm{End}_{\mathbb{F}_p}(E) \in \{\mathbb{Z}[\phi], \mathbb{Z}\left[\frac{-p+\phi}{2}\right]\}$.

This proves the first part of the theorem.

Assume we have $P, Q \in E[2]$ and $P \neq Q$ are $\mathbb{F}_p$-rational i.e., $\phi(P) = P, \phi(Q) = Q$. This implies that $\mathrm{Ker}([2]) \subseteq \mathrm{Ker}(\phi - [1])$. By theorems 29 and 28 both isogenies $[2], \phi - [1]$ are separable which means we can use Theorem 9 to obtain a unique isogeny ψ s.t. $[2]\psi = \phi - [1]$. This isogeny is $\mathbb{F}_p$-rational because $\phi - [1], [2]$ are $\mathbb{F}_p$-rational. This equality also shows that ψ cannot be expressed as an element of $\mathbb{Z}[\phi]$ i.e., it must be that $\mathbb{Z}[\phi] \subsetneq \mathrm{End}_{\mathbb{F}_p}(E) \iff \mathrm{End}_{\mathbb{F}_p}(E) \cong \mathbb{Z}\left[\frac{-p+\phi}{2}\right]$.

On the other hand, assume $\psi \in \mathbb{Z}\left[\frac{-p+\phi}{2}\right] \setminus \mathbb{Z}[\phi] \iff \psi = a + b\frac{-p+\phi}{2}$ for some $a, b \in \mathbb{Z}, b \not\equiv 0 \mod 2$. W.l.o.g. assume $b > 0$. We can rewrite the equality as (now in "isogeny notation") $[2]\psi = [2][a] + [b][-p] + \phi \iff \psi[2] = [a][2] + [b][-p] + \phi$. Take $P \in E[2], P \neq \mathcal{O}$ and plug it into the equation.

On the left-hand side, we get $\mathcal{O}$ because P is in the kernel of $[2]$ and ψ is an isogeny and therefore maps $\mathcal{O}$ to $\mathcal{O}$.

On the right-hand side, we can omit the $[a][2]$ part for the same reason. Since P is of order 2, $b \not\equiv 0 \mod 2, p$ is prime we get $[b][-p](P) = [-1](P) = -P$. The RHS is $-P + \phi(P)$.

To sum it up, we get $\phi(P) = P$ i.e., P is $\mathbb{F}_p$-rational. Since $|E[2]| = 4$, we always have 3 $\mathbb{F}_p$-rational points of order 2. □

Theorem 81. *Let $p \geq 5$ be a prime s.t. $p \equiv 3 \mod 8$ and let E be a supersingular elliptic curve over $\mathbb{F}_p$. Then $\mathrm{End}_{\mathbb{F}_p}(E) \cong \mathbb{Z}[\phi]$ iff there exists $A \in \mathbb{F}_p$ s.t. E is $\mathbb{F}_p$ isomorphic to the curve $E_A : y^2 = x^3 + Ax^2 + x$. Such A is unique. In addition, if E is isomorphic to a curve E_A, then E has only one $\mathbb{F}_p$-rational point of order 2.*

Proof. [Cas+18] Proposition 8. □

The following definition can be extended to ordinary curves or to different fields but in our case, we are only interested in supersingular curves over $\mathbb{F}_p$.

Definition 59. *Let E be a supersingular curve over $\mathbb{F}_p$. We say E is <u>on the surface</u> (resp. <u>on the floor</u>) if $\mathrm{End}_{\mathbb{F}_p}(E) \cong \mathbb{Z}\left[\frac{-p+\phi}{2}\right]$ (resp. $\mathrm{End}_{\mathbb{F}_p}(E) \cong \mathbb{Z}[\phi]$).*

Remark. The previous definition is connected to ascending/descending/horizontal isogenies. Generally, the isogeny graph forms a what is called a volcano which has a surface, a floor and levels between.

Theorem 82. *Let $p \geq 5$ be a prime s.t. $p \equiv 3 \mod 8$ and let $l > 2$ be a prime s.t. $\left(\frac{-p}{l}\right) = 1$. The supersingular subgraph of the graph $G_l(\mathbb{F}_p)$ has two levels (the surface and the floor). From each vertex there are two horizontal l-isogenies. On the surface there are $h(-p)$ vertices and on the floor there are $3h(-p)$ vertices. The surface and the floor are connected $1:3$ with 2-isogenies (descending/ascending) and there are no horizontal 2-isogenies.*

Proof. [DG13] Theorem 2.7 $(2)(b)$. □

The following theorem and corollary is a modification of Theorem 78 which takes into account supersingular curves over $\mathbb{F}_p, p \geq 5$.

Theorem 83. *Let $p \geq 5$ be a prime, let $K = \mathbb{Q}(\sqrt{-p})$ and let l be a prime s.t. $\gcd(l, p) = 1$. There is one to one correspondence between the sets*

$$\{\textit{supersingular elliptic curves over } \mathbb{F}_p\}$$
$$\leftrightarrow$$
$$\{\textit{elliptic curves } E \textit{ over } \mathbb{C} \textit{ s.t. } \mathrm{End}_{\mathbb{C}}(E) \in \{\mathbb{Z}[\sqrt{-p}], \mathcal{O}_K\}\}$$

and there is one to one correspondence also between the sets

$$\{l\textit{-isogenies defined over } \mathbb{F}_p \textit{ between supersingular curves over } \mathbb{F}_p\}$$
$$\leftrightarrow$$
$$\{l\textit{-isogenies defined over } \mathbb{C} \textit{ between elliptic curves } E \textit{ over } \mathbb{C} \textit{ s.t. } \mathrm{End}_{\mathbb{C}}(E) \in \{\mathbb{Z}[\sqrt{-p}], \mathcal{O}_K\}\}.$$

Proof. [DG13] Proposition 2.5 and the discussion after. □

Corollary. Let $p \geq 5$ be a prime, let $K = \mathbb{Q}(\sqrt{-p})$ and let l be a prime s.t. $\gcd(l, p) = 1$. Let $\mathcal{O} \in \{\mathbb{Z}[\sqrt{-p}], \mathcal{O}_K\}$. If the set of supersingular curves over $\mathbb{F}_p$ is non-empty, then it is a $\mathrm{cl}(\mathcal{O})$-torsor where the action of the ideal class of a proper $\mathcal{O}$-ideal of prime norm l is given by a horizontal isogeny of degree l. The inverse of the action is given by the inverse ideal which corresponds to the dual isogeny.

Proof. It is a rephrased Theorem 83 in the terminology we have used for ordinary curves. □

Next, we present a similar theorem to Theorem 76 which tells us that the supersingular isogeny graph over $\overline{\mathbb{F}_p}$ is also an ϵ-expander.

Theorem 84. *Let l be a prime different from p s.t. $l < \frac{p}{4}$. Then, there exists $\epsilon > 0$ s.t. the supersingular component of $G_l(\overline{\mathbb{F}_p})$ is a $l+1$-regular ϵ-expander. Specifically, $\epsilon = 1 - \frac{2\sqrt{l}}{l+1}$.*

Proof. [Piz90] Theorem 1. □

6. CSIDH

This is the algorithm which utilizes all of our presented theory. CSIDH is a public-key cryptography algorithm. To be precise, CSIDH is a key exchange algorithm which means it allows 2 parties to negotiate a shared secret key while communicating over an open channel.

CSIDH uses supersingular curves over a prime field $\mathbb{F}_p$ and works with the $\mathbb{F}_p$-rational subset of the endomorphism ring which is, by Claim 37, an order in an imaginary quadratic field. This means we can work with the class group action on $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p)$. This explains the acronym CSIDH[1] which stands for "Commutative Supersingular Isogeny Diffie-Hellman" where "commutative" represents the commutativity of the class group.

Generally speaking, CSIDH is an instance of what is called a "hard homogenous space". It is a principal homogenous space (introduced in Chapter 3) with a few conditions on complexity of operations.

The following definition is taken from [Cas+18].

Definition 60. *Let X be G-torsor s.t. the following operations are "easy" i.e., their complexity is polynomial:*

1. *All group operations in G.*
2. *Getting a random sample from G (uniformly distributed).*
3. *Evaluating the validity of elements of X and equality of their representation.*
4. *Computing the group action.*

The following operations are "hard" i.e., their complexity is not polynomial:

1. *Given $x, y \in X$ find $g \in G : g \cdot x = y$.*
2. *Given $x, x', y \in X, g \in G$ s.t. $g \cdot x = x'$ find $y' \in X$ s.t. $g \cdot y = y'$.*

We call (G, X) a hard homogenous space.

This definition might sound too abstract but in reality, we are already probably familiar with a hard homogenous space. The classic Diffie-Hellman key exchange is a hard homogenous space where $G = \mathbb{Z}_{p-1}^*$ and $X = \{g \in \mathbb{Z}_p^* : g \text{ is a generator of } \mathbb{Z}_p^*\}$ and the group action is given by exponentiation.

Now we are going to present how does CSIDH key exchange work on a high level and subsequently we are going to go into more detail using the presented theory.

We assume that Alice and Bob want to compute a shared key without anyone else knowing the key.

[1] Pronounced as "seaside".

6.1 What are the global parameters?

The global parameters of the CSIDH scheme is a finite set of small primes $\{l_i \in \mathbb{P} : 1 \leq i \leq n, l_i > 2\}$ s.t. $p = -1 + 4\prod_{i=1}^{n} l_i$ is a prime. This prime determines a finite field $\mathbb{F}_p$ s.t. an elliptic curve $E_0 : y^2 = x^3 + x$ over $\mathbb{F}_p$ is supersingular with $\mathrm{End}_{\mathbb{F}_p}(E_0) = \mathcal{O}$ for an order $\mathcal{O}$ in an imaginary quadratic field.

Also we pick a security parameter $m \in \mathbb{N}$ where m is chosen as the minimal m s.t. $(2m+1)^n \geq \sqrt{p}$.

6.2 What are the public and private keys?

The private keys for Alice and Bob are integer vectors of dimension n with values in $\{-m, \ldots, m\}$.

Let $\mathbf{a} = (a_1, \ldots, a_n)$ be such vector for Alice and $\mathbf{b} = (b_1, \ldots, b_n)$ for Bob. These vectors represent an element of $\mathrm{cl}(\mathcal{O})$ which is constructed from ideals of "small" norm. Every such ideal is uniquely determined by chosen primes l_i. Alice and Bob apply the group action determined by their secret vector to the elliptic curve E_0 and get elliptic curves E_A (for Alice) and E_B (for Bob). These curves can be uniquely represented by a parameter which is an element of $\mathbb{F}_p$.

To sum it up, the private key for Alice is the vector $\mathbf{a}$ and her public key is the coefficient $A \in \mathbb{F}_p$.

6.3 What is the shared key and how it's computed?

Denote the public keys of Alice and Bob as $A, B \in \mathbb{F}_p$. These values uniquely determine an elliptic curve with the same endomorphism ring. Therefore, they can both apply the action of $\mathrm{cl}(\mathcal{O})$ determined by their secret key to compute an elliptic curve E'. This elliptic curve is the shared secret, more specifically, the parameter, which uniquely determines the curve, is.

How do they arrive at the same curve? The answer is simple if we use the group action notation. Assume $[I_A] \in \mathrm{cl}(\mathcal{O})$ is the secret group action element of Alice determined by $\mathbf{a}$.

First, Alice computes the elliptic curve $[I_A]E_0 = E_A$ and Bob does the same (using his private key) $[I_B]E_0 = E_B$. This is the step (the computation of the public key) that can be done before the communication begins.

Now Alice and Bob share the parameters $A, B \in \mathbb{F}_p$ (which correspond to unique elliptic curves) and compute their action upon them. Alice computes $[I_A]E_B = E'$ and Bob computes $[I_B]E_A = E''$. Does $E' = E''$?

$$E' = [I_A]E_B = [I_A][I_B]E_0 = [I_B][I_A]E_0 = [I_B]E_A = E''$$

The third equality comes from the commutativity of the ideal class group.

6.4 More in depth

The previous presentation of the algorithm was very high level. Now we dive deep into why all the steps make sense.

Considering the choice of global parameters there is nothing to explain except that only the primes $l_1, \ldots, l_n$ and m need to be published. These parameters can be chosen once by the designers of the scheme based on the required security level. More on that in Section 6.7.

We have already mentioned that the $\mathbb{F}_p$-rational endomorphism ring of a supersingular curve is an order, denoted as $\mathcal{O}$, in an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-p})$.

By Theorem 81 we get that the elliptic curves[2] can be uniquely represented as one element of $\mathbb{F}_p$. Therefore, the public keys are just elements of $\mathbb{F}_p$ but note that not every elliptic curve $y^2 = x^3 + Ax^2 + x$, for some $A \in \mathbb{F}_p$, is supersingular. This can be verified easily using an algorithm presented in Section 6.5. This means we can detect invalid keys.

A few questions arise when looking at the private keys. How does a prime l_i uniquely determine an element of $\mathrm{cl}(\mathcal{O})$? This all comes down to the choice of p and to the elliptic curve.

Theorem 80 shows that the $\mathbb{F}_p$-rational endomorphism ring is isomorphic to $\mathbb{Z}[\boldsymbol{\phi}]$ because, by Theorem 81, a supersingular curve $E : y^2 = x^3 + Ax^2 + x, A \in \mathbb{F}_p$ always has only one $\mathbb{F}_p$-rational point of order 2.

Now we apply Lemma 69. Using the lemma notation, we have $D = -p, q = l_i, \alpha = \sqrt{D} = \sqrt{-p} = \boldsymbol{\phi}, f = 2$. $\left(\frac{-p}{l_i}\right) = 1$ because $-p \equiv 1 \mod l_i$ and 1 is a quadratic residue. Therefore, $(l_i) = L\overline{L}$ s.t. $L = [l, \sqrt{-p} - \delta]$ where δ is a root of $\min_{\mathbb{Q}}(\sqrt{-p})$.

The minimal polynomial of $\sqrt{-p}$ over $\mathbb{Q}$ is $x^2 + p$ and $x^2 + p \equiv x^2 - 1 \mod l_i$. W.l.o.g. $L = [l, \sqrt{-p} - 1], \overline{L} = [l, \sqrt{-p} + 1]$[3]. The choice of ± 1 is obviously arbitrary. In CSIDH, $a_i \in \mathbf{a}$ represents the ideal $L^{|a_i|}$ if $a_i > 0$, and $\overline{L}^{|a_i|}$ if $a_i < 0$.

The only thing left is to show how do we actually use these keys to arrive at a shared key. We explain this process in detail using a concrete example in Section 6.6.

6.5 Public key validation

We briefly introduce the algorithm for verifying the validity of a public key. This is considered a benefit because it narrows down the possibilities for a potential attacker. This section follows from [Cas+18], Section 5.

By Claim 32, we know that for every supersingular curve E over $\mathbb{F}_p$ the order of its $\mathbb{F}_p$-rational group of points is $p + 1$. In our case we have $|E(\mathbb{F}_p)| = p + 1 = 4\prod_{i=1}^{n} l_i$, where l_i are all different primes. Since $E(\mathbb{F}_p)$ is a finite abelian group, we know the group structure of $E(\mathbb{F}_p) \cong \mathbb{Z}_4 \times \prod_{i=1} \mathbb{Z}_{l_i}$.

By Theorem 31, we get a range of possible values of $E(\mathbb{F}_p)$ for an arbitrary elliptic curve over $\mathbb{F}_p$, that is $p + 1 - 2\sqrt{p} \leq E(\mathbb{F}_p) \leq p + 1 + 2\sqrt{p}$.

Let $P \in E(\mathbb{F}_p)$ and denote the order of P in $E(\mathbb{F}_p)$ by $k \in \mathbb{N}$. If $k > 4\sqrt{p}$, then there clearly exists only one $a \in \mathbb{N}$ s.t. $p + 1 - 2\sqrt{p} \leq ak \leq p + 1 + 2\sqrt{p}$ which means it must be that $ak = |E(\mathbb{F}_p)|$ because $k \mid |E(\mathbb{F}_p)|$.

If E is supersingular and $P \in E(\mathbb{F}_p)$ is chosen at random, then, due to the structure of $E(\mathbb{F}_p)$ described above, for each l_i P has the probability $\frac{l_i - 1}{l_i}$ (there

[2] The model in question is called the Montgomery model.

[3] This can be generalized for primes of other forms. 1 is actually the eigenvalue of $\boldsymbol{\phi}$ in $E[l]$.

are $l_i - 1$ generators of $\mathbb{Z}_{l_i}$) of having an order divisible by l_i.

We can thus estimate the average order of a random point of E. If we ignore the part $\mathbb{Z}_4$, then we get a lower bound estimate (an expected value). With probability $\frac{1}{l_i}$ the order of P does not increase but with probability $\frac{l_i-1}{l_i}$ the order gets multiplied by l_i. The expected value of the order of P is therefore: $\prod_{i=1}^{n} \left(l_i \frac{l_i-1}{l_i} + 1\frac{1}{l_i}\right)$.

As a lower estimate, we can see that the expected value of the order is at least $\prod_{i=1}^{n}(l_i - 1)$ which is almost p. We also only need a point of order $> 4\sqrt{p}$ to verify if its corresponding elliptic curve is supersingular. This heuristic leads to an algorithm for verifying the supersingularity.

Let (E, ∞) be an elliptic curve over $\mathbb{F}_p$ where p is of the form used in CSIDH. Then

1. Pick a random $P \in E(\mathbb{F}_p)$. Set $k = 1$ and $i = 1$.
2. While $i \leq n$ do:
   (a) Calculate $Q = \left[\frac{p+1}{l_i}\right] P$.
   (b) If $[l_i]Q \neq \infty$, then return "E is ordinary".
   (c) If $Q \neq \infty$, then set $k = k \cdot l_i$.
   (d) If $k > 4\sqrt{p}$, then return "E is supersingular".
   (e) Set $i = i + 1$.

In the step $2(b)$ if $[l_i]Q = \left[l_i \frac{p+1}{l_i}\right] P = [p+1]P \neq \infty$, then we can be sure that $E(\mathbb{F}_p) \neq p + 1$ because we have calculated that P is of order $> p + 1$.

In the step $2(c)$ we know that $\frac{p+1}{l_i} < k \leq p + 1$ and $l_i \mid k$. Therefore we increase our value of k accordingly.

In the step $2(d)$ if $k > 4\sqrt{p}$, then we calculated that the order of P is at least $4\sqrt{p}$ and the order is divisible by $l_1 \cdots l_i$. The only possibility for $E(\mathbb{F}_p)$ is that $E(\mathbb{F}_p) = p + 1$ due to Theorem 31 as explained above.

It may happen that the algorithm ends without deciding whether E is supersingular/ordinary due to the point P being of small order. This is very unlikely because the expected value of the order P above. Nonetheless, we can always repeat this process.

6.6 The graph

We have defined in Chapter 5 a K-rational l-isogeny graph. In CSIDH, we actually use a union of many such graphs. As mentioned before, the graph has 2 disjoint subgraphs (supersingular/ordinary). CSIDH, as the name suggests, works only with the supersingular subset.

By design, we have $p \equiv 11 \mod 12$ because $l_1 = 3$. Thus, we have the case where $\sqrt{-1}, \sqrt{-3} \notin \mathbb{F}_p$ by Claim 73 and the graph's edges between two vertices have the same multiplicity.

In most our theory of the ideal class group action we have assumed that the elliptic curve is ordinary but since we only work with $\mathbb{F}_p$-rational endomorphism ring which is isomorphic to an order in an imaginary quadratic field we can transfer this theory to supersingular curves over $\mathbb{F}_p$ due to Theorem 83.

Example 4. Set $p = 4 \cdot (3 \cdot 5) - 1 = 59$ i.e., $l_1 = 3, l_2 = 5$. Consider the supersingular subgraphs of graphs $G_3(\mathbb{F}_{59}), G_5(\mathbb{F}_{59})$. Note that this notation is not very precise because we are looking at only the subgraphs of $G_3(\mathbb{F}_{59}), G_5(\mathbb{F}_{59})$. To be precise, we only look at the floor parts of $G_3(\mathbb{F}_{59}), G_5(\mathbb{F}_{59})$ (see definition 59 and Theorem 82).

First, we need to determine the set of vertices which we can represent as the coefficients A in the Montgomery form of the curve due to Theorem 81. We include the Montgomery form (denoted as $E_{m,i}$) and also the short Weierstrass form (denoted as $E_{w,i}$). This is because CSIDH uses Montgomery forms but we have presented Vélu's formulae only for short Weierstrass form due to simplicity. We get 9 different elliptic curves.

i	$E_{m,i}$	$E_{w,i}$	A	$j(E_i)$
1	$y^2 = x^3 + x$	$y^2 = x^3 + x$	0	17
2	$y^2 = x^3 + 6x^2 + x$	$y^2 = x^3 + 22x + 54$	6	48
3	$y^2 = x^3 + 11x^2 + x$	$y^2 = x^3 + 29$	11	0
4	$y^2 = x^3 + 28x^2 + x$	$y^2 = x^3 + 29x + 41$	28	28
5	$y^2 = x^3 + 29x^2 + x$	$y^2 = x^3 + 8x + 28$	29	47
6	$y^2 = x^3 + 30x^2 + x$	$y^2 = x^3 + 8x + 31$	30	47
7	$y^2 = x^3 + 31x^2 + x$	$y^2 = x^3 + 29x + 18$	31	28
8	$y^2 = x^3 + 48x^2 + x$	$y^2 = x^3 + 30$	48	0
9	$y^2 = x^3 + 53x^2 + x$	$y^2 = x^3 + 22x + 5$	53	48

Note that we have "duplicate" elliptic curves in terms of j-invariants. These are pairs of elliptic curves and their quadratic twists.

Now we want to compute isogenies which correspond to ideals $[3, \boldsymbol{\phi} - 1], [5, \boldsymbol{\phi} - 1]$. We assume the isomorphism $\boldsymbol{\phi} \cong \sqrt{-p}$ in our notation, where $\boldsymbol{\phi}$ is the Frobenius endomorphism of the specific elliptic curve. There multiple approaches how to calculate these.

We know that the isogeny corresponding to ideal I has kernel $E[I]$. Since in our case I is generated by isogenies $[3], \boldsymbol{\phi} - [1]$, we can see that the points of the kernel have to be $\mathbb{F}_p$-rational because for any $P \in E[I] : \boldsymbol{\phi}(P) = P$. Thus, every point $P \in E[I]$ is a $\mathbb{F}_p$-rational point s.t. $[3]P = \infty$ and $\boldsymbol{\phi}(P) = P$. Also, since the curves are supersingular and defined over a prime field, then $|E(\mathbb{F}_p)| = p + 1 = 4 \prod_{i=1}^{n} l_i$. From group theory we know that there cannot be multiple subgroups of $E(\mathbb{F}_p)$ of prime order. CSIDH uses a random point sampling for getting such point, meaning it randomly selects a $\mathbb{F}_p$-rational point of E and checks if its order is 3.

Here are the points of such orders of our curves.

$E_{w,i}$	P_I
$y^2 = x^3 + x$	$(12, 18)$
$y^2 = x^3 + 22x + 54$	$(3, 41)$
$y^2 = x^3 + 29$	$(0, 41)$
$y^2 = x^3 + 29x + 41$	$(46, 57)$
$y^2 = x^3 + 8x + 28$	$(45, 2)$
$y^2 = x^3 + 8x + 31$	$(7, 31)$
$y^2 = x^3 + 29x + 18$	$(22, 34)$
$y^2 = x^3 + 30$	$(21, 21)$
$y^2 = x^3 + 22x + 5$	$(28, 34)$

Recall that our chosen ideal I is of prime norm i.e., $|E[I]|$ is of prime order thus since we have found a point which belongs into $E[I]$, we have the generator.

Now we can use Vélu's formulae from Theorem 16 to compute the isogenies which correspond to such ideals. Let's compute the isogeny given by I from $E_1 : y^2 = x^3 + x$.

$$P_1 = (12, 18), P_2 = 2P_1 = -P_1 = (12, 41)$$
$$t_{P_1} = t_{P_2} = 3 \cdot 12^2 + 1 = 20$$
$$u_{P_1} = u_{P_2} = 2 \cdot 18^2 = 2 \cdot 41^2 = 2 \cdot (-18)^2 = 58$$
$$w_{P_1} = w_{P_2} = u_{P_1} + t_{P_1} \cdot 12 = 3$$
$$\Longrightarrow$$
$$t = 40, w = 6$$

We get that this isogeny, denoted as $\lambda_{1,5}$, is from E_1 to $E' : y^2 = x^3 + 37x + 17$. The j-invariant of this curve is 47. Now we can use Theorem 3 to check which one (E_5 or E_6) is isomorphic to this elliptic curve. $\frac{17}{37} = 18 \in \mathbb{F}_{59}$ is non-square in $\mathbb{F}_{59}$ and so is $\frac{28}{8} = 33$, which means $E' \cong E_5$.

We also calculate the dual isogeny from $E_5 \to E_1$ given by $\overline{I} = [3, \boldsymbol{\phi} + 1]$. This isogeny's kernel is also generated by a point of order 3 but this point is not necessarily $\mathbb{F}_p$-rational. We have a condition $\forall P \in E[\overline{I}] : \boldsymbol{\phi}(P) = -P$.

In our model if $P = (x_P, y_P) \in E$, then $-P = (x_P, -y_P)$. From this we can conclude that the first coordinate of P is an element of $\mathbb{F}_p$ since the Frobenius endomorphism fixes exactly the elements of $\mathbb{F}_p$. The second coordinate satisfies $y^p = -y$ which means that if $y \neq 0$, then $y \notin \mathbb{F}_p$ but y must satisfy the curve equation $y^2 = x^3 + Ax + x$ and $x_P^3 + Ax_P + x_P = a \in \mathbb{F}_p$ for $x_P \in \mathbb{F}_p$. In other words, y is the square root of $a \in \mathbb{F}_p$. Thus $y \in \mathbb{F}_p(\sqrt{a}) \setminus \mathbb{F}_p \cong \mathbb{F}_{p^2} \setminus \mathbb{F}_p$.

The dual isogeny $\widehat{\lambda_{1,5}}$ of $\lambda_{1,5}$ is the isogeny with kernel generated by a $\mathbb{F}_{p^2}$-rational point of E_5 of order 3 with first coordinate in $\mathbb{F}_p$.

To find such point CSIDH uses the same sampling approach as for finding the $\mathbb{F}_p$-rational point. Combining these conditions, we get an algorithm for finding generators of $E[I]$ or $E[\overline{I}]$.

1. Choose a random $x \in \mathbb{F}_p$.
2. Calculate $a = x^3 + Ax + x \in \mathbb{F}_p$.
3. If a is a square in $\mathbb{F}_p$:
   (a) Calculate if the order of $(x, \sqrt{a}) \in E(\mathbb{F}_p)$ is l. If it is, then you have generator of $[l, \boldsymbol{\phi} - 1]$. If it's not, go to 1.
4. Else:
   (a) Calculate if the order of $(x, \sqrt{a}) \in E(\mathbb{F}_{p^2}) \setminus E(\mathbb{F}_p)$ is l. If it is, then you have generator of $[l, \boldsymbol{\phi} + 1]$. If it's not, go to 1.

We will again work with a short Weierstrass representation of $E_5 : y^2 = x^3 + 8x + 28$. Using the representation of $\mathbb{F}_{59^2} \cong \mathbb{F}_{59}[\alpha]/(\alpha^2 + 58\alpha + 2)$ and algorithm above we calculate the point of $E_5(\mathbb{F}_{59^2}) \setminus E_5(\mathbb{F}_{59})$ of order 3 which is

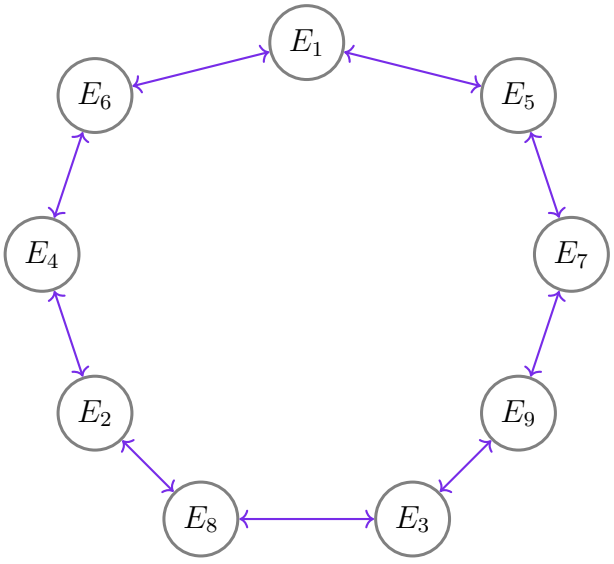
$P = (18 : 43\alpha + 8)$. Now we again use the Vélu formulae, the only difference is that we are now doing calculations in $\mathbb{F}_{59^2}$:

$$P_1 = (52, 25\alpha + 17), P_2 = 2P_1 = -P_1 = (52, 34\alpha + 42)$$
$$t_{P_1} = t_{P_2} = 3 \cdot 52^2 + 8 = 37$$
$$u_{P_1} = u_{P_2} = 2 \cdot (25\alpha + 17)^2 = 25$$
$$w_{P_1} = w_{P_2} = u_{P_1} + t_{P_1} \cdot 52 = 2$$
$$\Longrightarrow$$
$$t = 15, w = 4.$$

This shows us that the isogeny from E_5, determined by the kernel generated by $(52, 25\alpha + 17)$, is an isogeny to the curve $E'' : y^2 = x^3 + 51x + 0$. Again, by comparing j-invariants, we get that $E'' \cong E_1$ which makes sense since we have calculated the dual isogeny.

The dual isogeny computation requires computation in $\mathbb{F}_{p^2}$ (this can be prevented using Montgomery curves) but since I induces an action on the set of supersingular curves defined over $\mathbb{F}_p$, we always get a curve and an isogeny which can be defined over $\mathbb{F}_p$. Also note that in the Vélu formulae we do not need to do arithmetic in $\mathbb{F}_{p^2}$ since we can always substitute y_P^2 in terms of x_P. The only thing where in our case we need to do the arithmetic is to compute the order. This can be avoided by using the Montgomery model (which CSIDH actually uses), where the point addition can be done using only the x-coordinate which is always going to be in $\mathbb{F}_p$ as explained above.

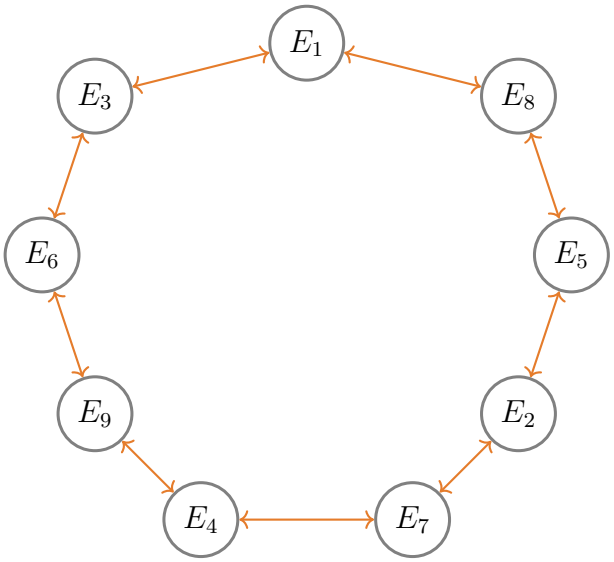
By proceeding doing the same for all listed curves we get this graph $G_3(\mathbb{F}_{59})$.



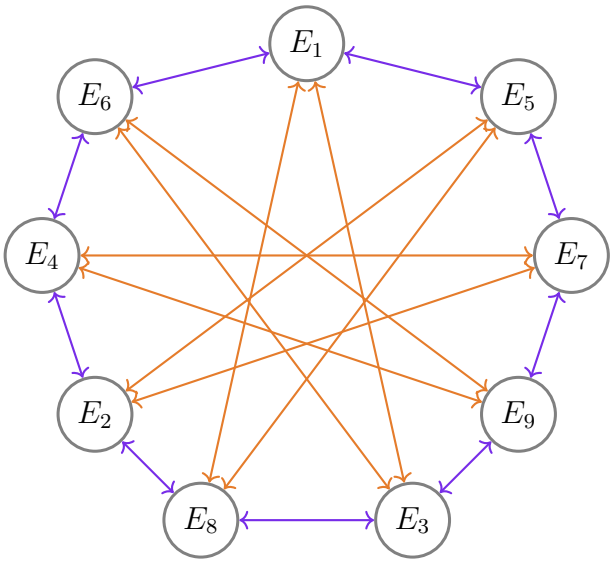
Going clockwise in the graph corresponds to applying the action $[l_i, \phi - 1]$, going counter-clockwise corresponds to the opposite action $[l_i, \phi{-}1]^{-1} = [l_i, \phi{+}1]$.

Similarly for $G_5(\mathbb{F}_{59})$.

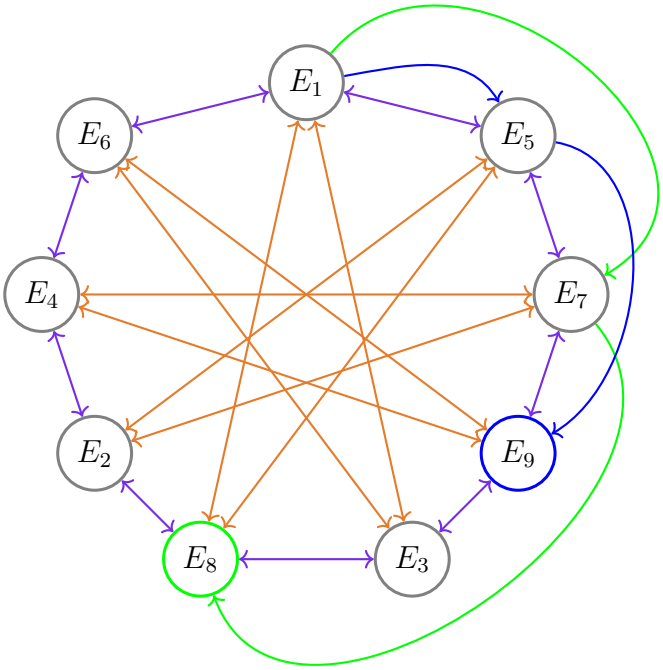
$E_{w,i}$	P_I
$y^2 = x^3 + x$	$(35, 28)$
$y^2 = x^3 + 22x + 54$	$(38, 40)$
$y^2 = x^3 + 29$	$(21, 26)$
$y^2 = x^3 + 29x + 41$	$(1, 37)$
$y^2 = x^3 + 8x + 28$	$(23, 44)$
$y^2 = x^3 + 8x + 31$	$(35, 36)$
$y^2 = x^3 + 29x + 18$	$(4, 32)$
$y^2 = x^3 + 30$	$(14, 1)$
$y^2 = x^3 + 22x + 5$	$(47, 14)$



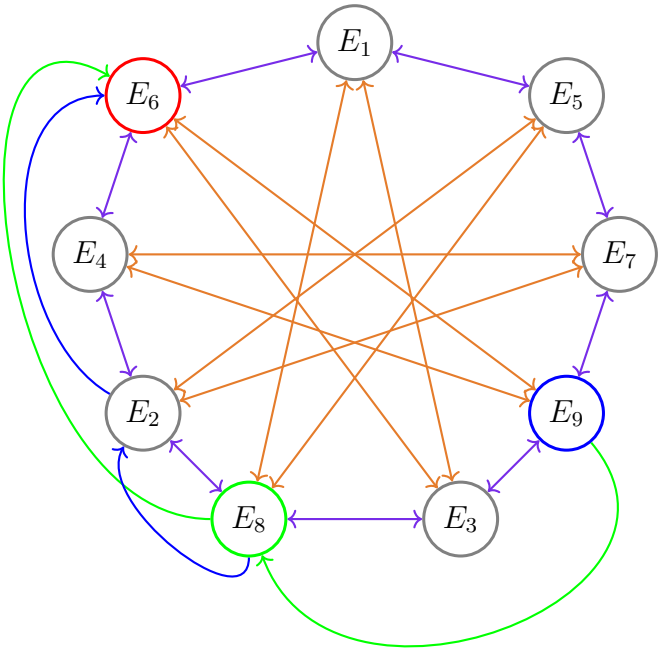
And now we combine $G_3(\mathbb{F}_{59}), G_5(\mathbb{F}_{59})$ into $G_{3,5}(\mathbb{F}_{59})$.



Let's say Alice's (green) private key is $\mathbf{a} = (2, -3)$ and Bob's (blue) private key is $\mathbf{b} = (1, 4)$. The keys correspond to public keys $E_A = E_8, E_B = E_9$ (technically the A parameters of the Montgomery curves which are $(E_8, E_9) = (48, 53)$). The public key computation in the graph can be visualized in this manner.



Thanks to the commutativity of the ideal class group, they should both arrive on the same shared secret $[L_3]^{a_1}[L_5]^{a_2}E_9 = [L_3]^{b_1}[L_5]^{b_2}E_8 = E_6$ as shown here.



This was an example how CSIDH works and how it computes a shared secret. Of course, in practice, the prime field $\mathbb{F}_p$ is much bigger which means that the graphs are huge.

One question that might arise is how can we be sure that the subgraph of $G_{l_i}(\mathbb{F}_p)$ is always a cycle with the same number of vertices. This is true due to Theorems 81 and 82. We are starting at the floor which has $3h(-p)$ vertices. We cannot "escape" from the floor because we are only using horizontal isogenies of degree at least 3. The graph is a cycle because we have 2 outgoing isogenies for every vertex and $\mathrm{Ell}_{\mathbb{F}_p}(\mathbb{Z}[\boldsymbol{\phi}])$ is a $\mathrm{cl}(\mathbb{Z}[\boldsymbol{\phi}])$-torsor by Theorem 83.

6.7 Security

In this section we will briefly discuss the security of CSIDH.

Theorem 82 states we have a graph with $3h(-p)$ vertices. We can roughly estimate that $h(-p) = h(D) \sim \sqrt{|D|}$ for any discriminant $D < 0$ due to [Cox13], page 135. In our case this means that we have roughly around $\sqrt{p}$ vertices.

Therefore, the (shared and public) key space grows proportionally to the size of $\sqrt{p}$, since $\sqrt{p}$ can be represented using roughly $\log_2(\sqrt{p}) = \frac{\log_2(p)}{2}$ bits.

The private key is a vector of n integers in the range $\{-m, \ldots, m\}$ i.e., the size of the private key space is $(2m+1)^n$. Note that these vectors represent ideal classes $[l_1^{e_1} \ldots l_n^{e_n}]$ and there exist different representatives of such classes.

The security of CSIDH is analyzed with respect to the key recovery problem. The key recovery problem is the problem of having curves E_0, E_1 s.t. $E_1 = [I]E_0$ for some $[I] \in \mathrm{cl}(\mathbb{Z}[\boldsymbol{\phi}])$ and the attacker wants to recover $[I]$. There is also an assumption that $[I]$ has to be represented in a way that the action of $[I]$ can be computed efficiently (i.e., polynomial time), for example, as product of ideals of small norm.

The importance of this problem to CSIDH security of obvious. The elliptic curves E_A, E_B are transmitted in plaintext. If an attacker is able to recover the ideal $[I_A]$ ($E_A = [I_A]E_0$) then, assuming he can evaluate the action by $[I_A]$ efficiently, he can just compute $[I_A]E_B$ and get the shared key. He also gets the private key because technically the vector of exponents (the private key) is just a representation of the ideal class.

6.7.1 Classical security

In classical security we consider non-quantum algorithms for attack.

The most obvious attack is the brute-force attack on the private keys. As mentioned, the "naive" key space is $(2m+1)^n$. This would hold if there were assurances that for a ideal class $[I]$ there is a unique short representation of $[I]$ using ideals of small norm. By small, we mean of norm less than l_n and by short we mean that all the exponents are in the range $\{-m, \ldots, m\}$.

In the paper ([Cas+18], Section 7.1) it is argued that under assumptions, that the ideal class group $\mathrm{cl}(\mathbb{Z}[\boldsymbol{\phi}])$ has a cyclic subgroup of order N where $N \approx h(-p)$, the number of small representations is $\frac{(2m+1)^n}{N}$.

This explains the motivation behind m being chosen as the minimal $m \in \mathbb{N}$ s.t. $(2m+1)^n \geq \sqrt{p}$. Since $h(-p) \approx \sqrt{p}$, we choose m so that the ratio $\frac{(2m+1)^n}{N} \approx$

$\frac{(2m+1)^n}{\sqrt{p}}$ is close to 1.

This means that the time complexity of the brute force search is exponential in the number of bits of p because $(2m+1)^n \approx \sqrt{p} = 2^{\frac{\log_2(p)}{2}}$.

Authors also mention that the meet-in-the-middle attack is possible with time complexity $O(\sqrt[4]{p})$, which is also exponential in the number of bits of p.

6.7.2 Quantum security

In this section, we briefly present an attack using quantum algorithm which is considered subexponential. We will not go into details of quantum computing because that is well beyond the scope of this work.

There exists a quantum algorithm which solves in subexponential time (and space) a what is called an "abelian hidden-shift problem".

The problem is fairly simple. Given an known abelian group G, a known finite set S and two black-box functions $f_0, f_1 : G \to S$, we say that f_0, f_1 hide a shift $s \in G$ if f_0 is injective and $\forall g \in G : f_0(x) = f_1(xs)$ ("f_1 is a shifted version of f_0"). The goal is to find s using queries to f_0, f_1.

It can be easily seen that solving this problem is equivalent to solving CSIDH (recovering the key).

Assume we have elliptic curves E_0, E_A. Set $G = \mathrm{cl}(\mathbb{Z}[\boldsymbol{\phi}]), S = \mathrm{Ell}_{\mathbb{F}_p}(\mathbb{Z}[\boldsymbol{\phi}])$. Technically this set is the set of j-invariants but in CSIDH this does not determine the elliptic curve uniquely due to quadratic twists. We omit this distinction for the sake of simplicity. Then f_0 represents the group action by $[I]$ and f_1 represents the group action by $[I_A][I]$ i.e., $s = [I_A]$ (the private key). f_0 is injective because $\mathrm{Ell}_{\mathbb{F}_p}(\mathbb{Z}[\boldsymbol{\phi}])$ is a $\mathrm{cl}(\mathbb{Z}[\boldsymbol{\phi}])$-torsor.

Note that solving the abelian hidden-shift problem doesn't necessarily imply that we get $[I_A]$ in a representation that can be efficient. But that can be done as shown in [CJS14] which presents an algorithm which computes an efficient representation of $[I_A]$.

The quantum security of CSIDH can be summed up to that there exist subexponetial quantum algorithms. The security of post-quantum algorithms is usually evaluated with comparison to the security of AES with $128, 192, 256$-bit keys.

Denote by CSIDH-$\log_2(p)$ an instance of the algorithm with p chosen to be a $\log_2(p)$-bit number. The corresponding security levels of CSIDH are.

AES	CSIDH
AES-128	CSIDH-$\log_2(512)$
AES-192	CSIDH-$\log_2(1024)$
AES-256	CSIDH-$\log_2(1792)$

6.8 Values of parameters in practice

In this section we will look at some concrete values of selected parameters of CSIDH for a 512-bit prime p.

Choosing p to be 512-bit number corresponds to having $n = 74$ where $l_1, \ldots, l_{73}$ are the smallest distinct primes greater than 2 and l_{74} is chosen as the smallest prime s.t. $-1+4\prod_{i=1}^{74} l_i$ is a prime and p is 512-bit number which gives $l_{74} = 751$[4].

[4] In the CSIDH paper the author chose $l_{74} = 587$ which gives a 511-bit number.

In this case

$$p = \texttt{0x821ed32c694fa08908391230eec2d67c5bd46f45b92843ccd37a36507ad38a40}$$
$$\texttt{adf3c8a9b259553bf3b3fe5257b0b4327d59bb18c5a5f1ce319564a4f73af0cb}.$$

We know that $n = 74$. Let's compute m. We know that m is the smallest integer s.t. $(2m+1)^n \geq \sqrt{p}$. To get an idea how big m is:

$$\log_2((2m+1)^n) = \log_2(\sqrt{p}) \iff n\log_2(2m+1) = \frac{\log_2(p)}{2} = 256$$
$$\implies$$
$$\log_2(2m+1) = \frac{256}{74} \approx 3.5$$
$$\iff$$
$$\lfloor \log_2(2m+1) \rfloor = 3 \iff \lfloor \log_2(2m+1) \rfloor + 1 = 4.$$

This shows that $2m+1$ should be a 4-bit number. If we calculate m as $m = \sqrt[2n]{p} - 1$ for our p, we get $m = 15$. Note that these are just rough estimates to give the reader an idea about practical sizes.

There is clearly a tradeoff between the number m and n. Choosing more primes (bigger n) we get a smaller m, which results in smaller private keys. In our case we have 74 4-bit numbers to store. This corresponds to private key size of 37 bytes. Public keys are numbers in $\mathbb{F}_p$ i.e., they are 512-bit numbers $\iff$ 64 bytes.

These key sizes are small compared to other post-quantum key exchange algorithms. For example, SIDH or NTRU have private and public key sizes in hundreds of bytes.

One thing that could be a little bit concerning is the assumption that the graph of $l_1, \ldots, l_{74}$ isogenies is a ϵ-expander for some $\epsilon > 0$. Recall Theorems 75 and 76. Assuming previously chosen values of l_i, we can see that our largest isogeny degree is $l_{74} = 751$. But Theorem 76 defines the set S as all primes $\leq B = \log(p)^2$ (we set $\delta = 0$ for this case). The value of B in this case for our p is about 125468, which is significantly larger than 751.

The number of different primes chosen (n in CSIDH) to fulfil this bound can be calculated using the standard prime number theorem: $\frac{\log(p)^2}{\log(2\log(p))} \approx 19117 = n$.

Assuming we would use these larger parameters for CSIDH, it would clearly make the private key sizes significantly larger and the algorithm would not be very practical in this sense.

In the CSIDH paper there is not explicitly stated much about the selection of the parameters with respect to the mixing properties of the graph, which imply that the shared key distribution is truly uniform. We suspect that CSIDH authors assume that the value of the exponent $2+\delta$ in Theorem 76 can be improved up to $1+\delta$. This is stated in the Section 7.2 of [JMV09], where the authors note that the value of $2+\delta$ is expected to be actually $1+\delta$.

If we assume this modification from $2+\delta$ to $1+\delta$, we get to the values < 100 for n and around 500 for B, depending on the choice of δ, which actually correspond to the chosen parameters by the authors.

7. SIDH

In this chapter, we present another algorithm for a key exchange utilizing isogenies between supersingular curves. This algorithm is called SIDH, which stands for "Supersingular Isogeny Diffie-Hellman" (almost the same as CSIDH). Although the names are almost the identical, these core theory behind them is quite different.

Note that you might have come across an algorithm called "SIKE". SIKE is a standardized version of SIDH (SIDH is the blueprint). SIKE is currently one of the Round 3 finalists of NIST's Post-Quantum Cryptography Standardization project.

We follow the same format as in the CSIDH chapter and we will mainly focus on the differences between these two algorithms.

7.1 What are the global parameters?

First, we choose distinct small primes l_A, l_B and exponents $e_A, e_B \in \mathbb{N}$. Together with a coefficient $f \in \mathbb{N}$ they form a prime $p = l_A^{e_A} l_B^{e_B} f \pm 1$. f is chosen s.t. $l_A^{e_A} l_B^{e_B} f \pm 1$ is a prime. e_A, e_B are chosen s.t. p is of the desired size and $l_A^{e_A} \approx l_B^{e_B}$.

We also calculate a supersingular curve E_0 over $\mathbb{F}_{p^2}$ s.t. $|E_0(\mathbb{F}_{p^2})| = (l_A^{e_A} l_B^{e_B} f)^2$ and calculate points $P_A, P_B,\ Q_A, Q_B$ s.t. $\langle P_A, Q_A \rangle = E_0[l_A^{e_A}]$ and $\langle P_B, Q_B \rangle = E_0[l_B^{e_B}]$.

To sum it up, the global parameters that need to be published are

$$(l_A, l_B, e_A, e_B, f, E_0, P_A, P_B, Q_A, Q_B).$$

We assume that Alice and Bob have pre-selected which one of them is A and which one of them is B. This can obviously be done by assuming that the side beginning communication is A and the other side is B. We only mention this because in CSIDH this is a non-issue.

7.2 What are the public and private keys?

We assume that Alice is "A" in this context. Alice's private key is a randomly generated pair of numbers $(m_A, n_A) \in \mathbb{Z}^2_{l_A^{e_A}}$ s.t. $l_A \nmid m_A$ or $l_A \nmid n_A$. This pair corresponds to an isogeny $\psi_A : E_0 \to E_A$ (more on that later).

The public key is a pair $(E_A, \psi_A(P_B), \psi_A(Q_B))$.

Bob does the same except his private key pair is an element of $\mathbb{Z}^2_{l_B^{e_B}}$.

7.3 What is the shared key?

Compared to the section in CSIDH chapter, we only mention here that the share key is a supersingular elliptic curve denoted as E_{AB}. By Claim 44, we can uniquely represent this curve by its j-invariant which is an element of $\mathbb{F}_{p^2}$. How do we arrive at E_{AB} is explained in the next section.

7.4 More in depth

The first question is, how do we calculate the elliptic curve E_0 over $\mathbb{F}_{p^2}$ with predefined set of points. We have already mentioned that this is indeed possible using the presented theory in Chapter 4. The full details for the general case and efficient algorithm can be found in [Bro06]. Nonetheless, the elliptic curve can be calculated once by the designers of SIDH. Same goes for the generators P_A, Q_A, P_B, Q_B.

W.l.o.g. assume that $p = l_A^{e_A} l_B^{e_B} f + 1$. By design, $|E_0(\mathbb{F}_{p^2})| = (p-1)^2 = (l_A^{e_A} l_B^{e_B} f)^2$ and . By Theorem 31, we have

$$|E_0(\mathbb{F}_{p^2})| = p^2 + 1 - \mathrm{Tr}(\boldsymbol{\phi}^e) \iff (p-1)^2 = p^2 + 1 - \mathrm{Tr}(\boldsymbol{\phi}^e)$$
$$\implies$$
$$\mathrm{Tr}(\boldsymbol{\phi}^e) = 2p.$$

For the case $p = l_A^{e_A} l_B^{e_B} f - 1$ we get $\mathrm{Tr}(\boldsymbol{\phi}^e) = -2p$.

We have calculated the value of the trace of Frobenius because we need to apply Theorem 33 to get the structure of $E_0(\mathbb{F}_{p^2})$. We get that $E_0(\mathbb{F}_{p^2}) \cong \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$.

This tells us that $E_0(\mathbb{F}_{p^2}) \leq E_0[l_A^{e_A} l_B^{e_B} f]$ but, by Theorem 13, $E_0[l_A^{e_A} l_B^{e_B} f] \cong \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$. Therefore, $E_0(\mathbb{F}_{p^2}) = E_0[l_A^{e_A} l_B^{e_B} f]$ i.e., the torsion group is $\mathbb{F}_{p^2}$-rational. Especially, $E_0[l_A^{e_A}], E_0[l_B^{e_B}] \leq E_0[l_A^{e_A} l_B^{e_B} f]$ are $\mathbb{F}_{p^2}$-rational.

By Theorem 13, the points P_A, Q_A have order $l_A^{e_A}$ and they are $\mathbb{F}_{p^2}$-rational. Similarly, the points P_B, Q_B have order $l_B^{e_B}$ and they are also $\mathbb{F}_{p^2}$-rational.

So, how does the pair $(m_A, n_A) \in \mathbb{Z}^2_{l_A^{e_A}}$ uniquely determine an isogeny ϕ_A? Alice calculates a point $R_A = [m_A]P_A + [n_A]Q_A \in E_0[l_A^{e_A}]$. The order of R_A in $E_0[l_A^{e_A}]$ is $l_A^{e_A}$ due to the following lemma.

Lemma 85. *Let E be an elliptic curve over $\mathbb{F}_q$, let P, Q be generators of $E[l^n]$, where l is a prime s.t. $\gcd(l, q)$ and $n \in \mathbb{N}$ i.e., $\langle P, Q\rangle = E[l^n]$, and let $a, b \in \mathbb{N}$ s.t. $l \nmid a$ or $l \nmid b$. Then the point $R = [a]P + [b]Q \in E[l^n]$ is of order l^n.*

Proof. W.l.o.g. assume $l \nmid a$. Point P is by definition of order l^n and because $l \nmid a$ the point $[a]P$ is also of order l^n due to Lagrange theorem. $[l^n]R = \mathcal{O}$ because $[l^n]R = [l^n]([a]P + [b]Q) = [a][l^n]P + [b][l^n]Q = [a]\mathcal{O} + [b]\mathcal{O} = \mathcal{O}$.

The only problem might arise if there exists $l^{n'}$, where $n' < n$, s.t. $[l^{n'}]R = \mathcal{O}$ i.e., if R was of order less than l^n. This would imply $[l^{n'}][a]P = [-1][l^{n'}][b]Q$. $[a]P$ is of order l^n therefore $[l^{n'}][a]P \neq \mathcal{O}$ and $[l^{n'}][a]P \in \langle P\rangle$. But the equality above implies that $[l^{n'}][a]P \in \langle Q\rangle$ which contradicts P, Q being the generators of $E[l^n]$ because $\langle P\rangle \cap \langle Q\rangle = \{\mathcal{O}\}$. □

Alice now has a point R_A of order $l_A^{e_A}$. Alice calculate the isogeny $\psi_A : E_0 \to E_A$ where $\mathrm{Ker}(\psi_A) = \langle R_A\rangle$ using Vélu formulae presented in Theorem 16. Note that we allow (and it is recommended for performance) for $l_A = 2$ and we have only presented Vélu formulae for a kernel of odd order. As mentioned before, there exist general formulae for an arbitrary kernel. For details refer to [Was08], Theorem 12.16.

By Claim 17, the isogeny ψ_A and E_A are defined over $\mathbb{F}_{p^2}$ because the kernel is as well. Because $|E_A(\mathbb{F}_{p^2})| = |E_0(\mathbb{F}_{p^2})|$, by Theorem 43, then also $E_A[l_A^{e_A}], E_A[l_B^{e_B}] \leq E_A(\mathbb{F}_{p^2})$ and $\deg(\psi_A) = l_A^{e_A}$.

If you take a look at the Vélu formulae, the calculation of an isogeny of degree $l_A^{e_A}$ (assuming $l_A^{e_A}$ is "big") is not very efficient. Specifically, we need to go over all $l_A^{e_A}$ points of its kernel to calculate this. But, we can use the same approach presented in the proof of Theorem 15 to calculate e_A isogenies of degree l_A. This approach is exponentially faster because we need to go over only $l_A e_A$ points.

The SIDH paper [FJP11] focuses a lot on the optimal approach how to calculate the isogeny efficiently. We only present this basic speedup. We can summarize the calculation in this algorithm which basically stems from the proof of Theorem 15.

1. Set $R_0 = R_A$, $i = 0$.
2. While $i < e$ do:
   (a) Calculate the isogeny $\psi_i : E_i \to E_{i+1}$ s.t. $\text{Ker}(\psi_i) = \langle [l_A^{e_A - i - 1}] R_i \rangle$.
   (b) Set $R_{i+1} = \psi_i(R_i), i = i + 1$.

At the end we get that $\psi_A = \psi_{e-1} \circ \dots \psi_0$ and $E_e = E_A$. In every iteration the point R_i has order l_A in $E_i(\mathbb{F}_{p^2})$ therefore every ψ_i has degree l_A.

In the next step, Alice exchanges public keys with Bob. Alice has received the elliptic curve E_B and the points $\psi_B(P_A), \psi_B(Q_A) \in E_B(\mathbb{F}_{p^2})$.

Alice then computes the isogeny $\psi'_A : E_B \to E_{AB}$ defined as $\text{Ker}(\psi'_A) = \langle [m_A]\psi_B(P_A) + [n_A]\psi_B(Q_A) \rangle$. It is not clear what the order of the kernel is. To clear things up we introduce this lemma.

Lemma 86. *Let $\psi : E \to E'$ be an isogeny between elliptic curves $(E, \mathcal{O}), (E', \mathcal{O}')$ and let $P \in E$ s.t. $\text{ord}(P) = n \in \mathbb{N}$. If $\forall a \in \mathbb{N}, a < n : [a]P \notin \text{Ker}(\psi)$, then $\text{ord}(\psi(P)) = \text{ord}(P)$.*

Proof. We know $[n]P = \mathcal{O}$ and $\forall a \in \mathbb{N}, a < n : [a]P \neq \mathcal{O}$. Denote $n' = \text{ord}(\psi(P))$.

If $n' < n$, then $[n']\psi(P) = \mathcal{O}' \iff \psi([n']P) = \mathcal{O}'$. This is a contradiction because that implies $[n']P \in \text{Ker}(\psi)$. □

Because ψ_B has kernel $\langle [m_B]P_B + [n_B]Q_B \rangle \leq E[l_B^{e_B}]$ and by definition $P_A, Q_A \notin E[l_B^{e_B}]$, applying Lemma 86 we get that $\psi_B(P_A), \psi_B(Q_A)$ have order $l_A^{e_A}$. It must be that $\langle \psi_B(P_A), \psi_B(Q_A) \rangle = E_B[l_A^{e_A}]$ and, by Claim 85, $[m_A]\psi_B(P_A) + [n_A]\psi_B(Q_A)$ has order $l_A^{e_A}$ in $E_B(\mathbb{F}_{p^2})$.

We have shown that $\deg(\psi_A) = \deg(\psi'_A) = l_A^{e_A}$ and $\deg(\psi_B) = \deg(\psi'_B) = l_B^{e_B}$. Assuming Bob follows the same steps as Alice, denote by E_{AB} and E_{BA} the elliptic curves that are the codomains of ψ'_A, ψ'_B. We need to check if $E_{AB} = E_{BA}$. This can be done by comparing the kernels of isogenies $\psi'_A \circ \psi_B$ and $\psi'_B \circ \psi_B$.

Let us validate that

$$\text{Ker}(\psi'_A \circ \psi_B) = \langle [m_A]P_A + [n_A]Q_A, [m_B]P_B + [n_B]Q_B \rangle = \text{Ker}(\psi'_B \circ \psi_A).$$

We will only prove one equality because the other one can be proven in the same way.

We know that $\text{Ker}(\psi_B) = \langle [m_B]P_B + [n_B]Q_B \rangle \leq E_0(\mathbb{F}_{p^2})$. The kernel of $\psi'_A : E_B \to E_{BA}$ is defined as $\langle [m_A]\psi_B(P_A) + [n_A]\psi_B(Q_B) \rangle \leq E_B(\mathbb{F}_{p^2})$.

Denote $\mathcal{S} = \{R \in E_0(\mathbb{F}_{p^2}) : \psi_B(R) \in \langle [m_A]\psi_B(P_A) + [n_A]\psi_B(Q_B)\rangle\}$ i.e., $\mathcal{S} = \psi_B^{-1}(\langle [m_A]\psi_B(P_A) + [n_A]\psi_B(Q_B)\rangle) = \psi_B^{-1}(\mathrm{Ker}(\psi'_A))$.

Let $R' \in \langle [m_A]\psi_B(P_A) + [n_A]\psi_B(Q_B)\rangle$, that means there exists $a \in \mathbb{N}$ s.t. $R' = [a][m_A]\psi_B(P_A) + [a][n_A]\psi_B(Q_A)$. There also must exist $R \in \mathcal{S}$ s.t. $\psi_B(R) = R' = [am_A]\psi_B(P_A) + [an_A]\psi_B(Q_A)$. Because isogenies $[n], n \in \mathbb{N}$ commute with other isogenies we get

$$\psi_B(R) = \psi_B([am_A]P_A + [an_A]Q_A).$$

Then clearly $\mathcal{S} = \langle [m_A]P_A + [n_A]Q_A, [m_B]P_B + [n_B]Q_B\rangle$ and $\mathrm{Ker}(\psi'_A \circ \psi_B) = \psi_B^{-1}(\mathrm{Ker}(\psi'_A)) = \mathcal{S}$.

We have shown that the algorithm works correctly.

In the language of isogeny graphs, we work with the supersingular subset of the union of $G_{l_A}(\mathbb{F}_{p^2})$ and $G_{l_B}(\mathbb{F}_{p^2})$. By Theorem 84, this graph is a ϵ-expander. From now on, for simplicity, when we refer to $G_l(\mathbb{F}_{p^2})$ we mean only the supersingular subset.

The theorem assumes isogenies and elliptic curves defined over $\overline{\mathbb{F}_p}$ but, as we have already mentioned, all supersingular curves over $\overline{\mathbb{F}_p}$ can be represented by an elliptic curve defined over $\mathbb{F}_{p^2}$ and l_A, l_B-isogenies, in our case, are defined over $\mathbb{F}_{p^2}$[1]. Therefore, it has "good mixing" properties in the similar way the isogeny graph in CSIDH has.

But, note that there is an unresolved problem with the walk length. For details, see the Security section below.

The graphs have the same number of points. The specific number is known due to Theorem 45 and it is roughly $\left\lfloor \frac{p}{12} \right\rfloor$. Note that, compared to CSIDH, the isogeny graphs have a more complicated structure. Although, by Theorem 84, the isogeny graph $G_l(\overline{\mathbb{F}_p})$ is $l+1$-regular, in the case of $G_l(\mathbb{F}_{p^2})$ there might be exceptional vertices which might have loops or the degree of the vertices is $< l+1$.

In the case there is a loop on a vertex in $G_l(\mathbb{F}_{p^2})$, that means there is an l-isogeny $E_1 \to E_2$, where $j(E_1) = j(E_2)$, but this isogeny is $\overline{\mathbb{F}_p}$-isomorphic to a $\overline{\mathbb{F}_p}$-isomorphism which means the loop disappears in $G_l(\overline{\mathbb{F}_p})$.

In the case there is a vertex in $G_l(\mathbb{F}_{p^2})$ with degree $< l+1$, that means at least 2 isogenies (defined by different kernels) go to elliptic curves with the same j-invariant.

7.5 Security

As we have already mentioned, SIDH works with the supersingular part of $G_{l_A}(\mathbb{F}_{p^2})$ and $G_{l_B}(\mathbb{F}_{p^2})$. Both of these parts have the same number of vertices which is about $\left\lfloor \frac{p}{12} \right\rfloor$. Therefore, the size of the public key space and the size of the shared key space is roughly the same as p.

The private key space little bit more complicated. The private key is basically the isogeny which is uniquely determined by its kernel. We need to know how many distinct kernels are there. This lemma answers the question.

Lemma 87. *Let l be a prime and $n \in \mathbb{N}$. The group $\mathbb{Z}_{l^n} \times \mathbb{Z}_{l^n}$ has $l^{n-1}(l+1)$ distinct cyclic subgroups of order l^n.*

[1] Note, this is not entirely correct. There are a few exceptions mentioned below.

Proof. From group theory we know that a cyclic subgroup of order k has exactly $\phi(k)$ different generators, where $\phi(\cdot)$ is the Euler's totient function.

We want to count the number of elements of $\mathbb{Z}_{l^n} \times \mathbb{Z}_{l^n}$ with order l^n. Let $(a, b) \in \mathbb{Z}_{l^n} \times \mathbb{Z}_{l^n}$. Clearly, $\text{ord}((a, b)) = \text{lcm}(\text{ord}(a), \text{ord}(b))$. Therefore, either a or b has to be of order l^n. We have $\phi(l^n)$ possibilities for a of order l^n and we can pair it with l^n other elements. Same for the case when b is of order l^n.

This gives us $\phi(l^n)l^n + l^n\phi(l^n) = 2\phi(l^n)l^n$ possible pairs, but we have counted some elements twice. Specifically, we have counted twice the pairs where both a and b are of order l^n. The number of such pairs is $\phi(l^n)^2$. To sum it up, the number of different pairs is $2\phi(l^n)l^n - (\phi(l^n))^2$.

Applying the fact we have stated at the beginning of this proof, we have

$$\frac{2\phi(l^n)l^n - (\phi(l^n))^2}{\phi(l^n)} = 2l^n - \phi(l^n) = 2l^n - (l^n - l^{n-1}) = l^{n-1}(l+1)$$

different cyclic subgroups of order l^n. □

This shows us that the group $E[l_A^{e_A}]$ has $l_A^{e_A-1}(l_A + 1)$ different subgroups of order $l_A^{e_A}$ which correspond to $l_A^{e_A}$ different $l_A^{e_A}$-isogenies.

We have briefly mentioned, in the previous section, that there is a problem with the walk length on the graphs used in SIDH. The problem is that Alice (similarly for Bob) makes a walk of length e_A on $G_{l_A}(\mathbb{F}_{p^2})$ to get her public key and then makes a walk of length e_B on $G_{l_B}(\mathbb{F}_{p^2})$.

We can roughly estimate the minimal walk length given by Theorem 75. For simplicity, assume $l_A = 2, l_B = 3, f = 1$ and $p = 2^{e_A}3^{e_B} + 1$. Then, by Theorem 84, we have $\epsilon = 1 - \frac{2}{3}\sqrt{3}$. Using the notation from Theorem 75 we have $|V| \approx p, |V'| = 1$

$$\frac{\log(2p)}{\log(2 - \frac{2}{3}\sqrt{3})} > \frac{\log(2p)}{\log(2)} =$$
$$= \log_2(2p) = \log_2(2(2^{e_A}3^{e_B} + 1)) > \log_2(2(2^{e_A}3^{e_B})).$$

Because we chose e_A, e_B s.t. $2^{e_A} \approx 3^{e_B}$, we get $\log_2(2(2^{e_A})3^{e_B}) \approx 2e_A + 1$. This means that, with generous estimates, the walks should be at least twice as long. Also, we do not know very well the mixing behavior of walking half of the total walk on $G_{l_A}(\mathbb{F}_{p^2})$ and the other half on $G_{l_B}(\mathbb{F}_{p^2})$.

The authors mention this non-uniformity but note that this is still a subject to further research.

Regarding complexities of attacks using classical and quantum computers, we only briefly mention the following. The best classical and quantum attacks against SIDH have exponential time complexities. Therefore, compared to CSIDH, SIDH is "more secure" against quantum computers. This is because we cannot exploit the commutativity of the endomorphism ring since it is an order in a quaternion algebra and not in an imaginary quadratic field.

Conclusion

In Chapter 1, we have presented the necessary theory to understand the subsequent chapters. We have provided a proof of uniqueness for Theorem 14, we have expanded the proof of Theorem 15, we have provided a proof for Claim 17 and then produced an example of how to apply Theorem 16.

In Chapter 2, we have focused on building the theory of supersingular and ordinary elliptic curve and the structure of their endomorphism rings. We have provided a proof for Theorems 29, 39, 42, 43 and for Claim 46. Mainly, our contribution in this chapter is the compilation of the necessary statements for CSIDH and SIDH from [Sut19], [Sil09], [Sch87], [Gal12] and presenting them in a united manner with expanded proofs. We especially focused on the required fields of definitions for some statements. For example, in most of the literature there is no mention of 42 which tells us that for ordinary elliptic curves all of their isogenies are defined over $\mathbb{F}_q$. This is necessary for implementations of the algorithms.

Chapter 3 was about the ideal class group action which was presented using the theory of elliptic curves over $\mathbb{C}$. This chapter is mainly compilation of [Sut19] and we have formulated and provided proofs for Claims 56, 57 and Theorems 61, 62.

Chapter 4 is supposed to give the reader an idea how and why can we use the theory of Chapter 3 for finite fields. We have provided an exhaustive commentary and collected necessary proofs from [Sut19], [Sil94] and [Lan12]. We have focused on the way how the reduction map works concretely which is usually in texts like [Sil94] or [Lan12] presented too abstractly. We have also presented and proven Lemma 69 which is crucial for understanding CSIDH.

In Chapter 5 we finally presented the isogeny graphs for supersingular and ordinary curves. We focused on the details regarding how automorphisms alter the graph structure and provided an example for better understanding. We also formulated and proved Claim 73 which is used in the next chapter to show correctness of CSIDH.

Then, we have provided some graph theory from [JMV09] and [Piz90] that is relevant to the security of CSIDH and SIDH. The theorems are not very well presented or mentioned in SIDH and CSIDH papers and we have followed up on them in the chapters 6, 7.

We also expanded the previous chapter and have shown why we have an ideal class group action on elliptic curves over finite fields with the help of [Sut19] and [DG13]. Additionally, we formulated and proved Theorem 80.

In the last two chapters (6, 7), we have presented CSIDH and SIDH as described in [Cas+18] and [FJP11]. In both cases, we have extensively explained the reasons why do the claims mentioned in the papers hold with references to the presented theory.

For CSIDH, we have created an example of the calculation of the shared key between two parties and provided a visual representation of the key exchange on the isogeny graphs. Additionally, we have briefly presented the security of the algorithm with relation to the chosen parameters. We have also analyzed a proposed version of the parameters by the authors and noted that the assumptions

of theorems from Chapter 5 are not met. We stated our hypothesis why the authors made such choice with relation to the open problems section of paper [JMV09].

In the chapter 7, we have followed the structure of the previous chapter and provided reasons behind the design choices of SIDH. We have formulated and proved Lemmas 85, 86 and 87. We have also touched on the security of SIDH with relation to the mixing properties of the graphs. We have noted that they also do not meet the assumptions of relevant theorems. Compared to CSIDH, the authors warn about this in their paper.

The last chapter could be expanded by creating an example similar to the one presented in CSIDH. Also, it would be beneficial to do an analysis of the size of parameters with comparison to CSIDH.

Furthermore, we have not focused much on the security analysis of these algorithms because they are fairly new (especially CSIDH) and at the time of writing the security is still being analyzed.

For further study of CSIDH and SIDH, we recommend the PhD thesis of Lorenz Panny (one of the authors of CSIDH) [Pan21] and lecture notes by Luca De Feo (one of the authors of SIDH) [Feo17]. For general study of isogeny graphs, we recommend the notable PhD thesis by David Kohel [Koh96] and the habilitation thesis by Luca De Feo [Feo18].

Bibliography

[FJP11] Luca De Feo, David Jao, and Jérôme Plût. "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies". In: (2011). https://ia.cr/2011/506.

[RS06] Alexander Rostovtsev and Anton Stolbunov. "PUBLIC-KEY CRYPTOSYSTEM BASED ON ISOGENIES". In: (2006). https://ia.cr/2006/145.

[Cas+18] Wouter Castryck et al. "CSIDH: An Efficient Post-Quantum Commutative Group Action". In: Lecture Notes in Computer Science 11274 (2018), pp. 395–427. DOI: 10.1007/978-3-030-03332-3_15. URL: https://csidh.isogeny.org/csidh-20181118.pdf.

[Gal12] S.D. Galbraith. *Mathematics of Public Key Cryptography*. Cambridge University Press, 2012. ISBN: 9781107013926.

[Was08] L.C. Washington. *Elliptic Curves: Number Theory and Cryptography, Second Edition*. 2nd ed. Discrete Mathematics and Its Applications. CRC Press, 2008. ISBN: 9781420071474.

[Sil09] J.H. Silverman. *The Arithmetic of Elliptic Curves*. 2nd ed. Graduate Texts in Mathematics. Springer New York, 2009. ISBN: 9780387094946.

[Sut19] Andrew Sutherland. *Lectures notes for 18.783 - Elliptic Curves*. 2019. URL: https://math.mit.edu/classes/18.783/2019/lectures.html.

[Cox13] D.A. Cox. *Primes of the Form X2 + Ny2: Fermat, Class Field Theory, and Complex Multiplication*. 2nd ed. Pure and Applied Mathematics: a Wiley Series of Texts, Monographs and Tracts Series. Wiley, 2013. ISBN: 9781118400722.

[Drá21] Aleš Drápal. *Skripta k předmětu (předběžná verze)*. 2021.

[DG13] Christina Delfs and Steven D. Galbraith. *Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$*. 2013. arXiv: 1310.7789 [math.NT]. URL: https://arxiv.org/pdf/1310.7789.

[Sch87] René Schoof. "Nonsingular plane cubic curves over finite fields". In: *Journal of Combinatorial Theory, Series A* 46.2 (1987), pp. 183–211. ISSN: 0097-3165. DOI: https://doi.org/10.1016/0097-3165(87)90003-3. URL: https://www.sciencedirect.com/science/article/pii/0097316587900033.

[Mar18] D.A. Marcus. *Number Fields*. Universitext. Springer International Publishing, 2018. ISBN: 9783319902333.

[Sil94] J.H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer New York, 1994. ISBN: 978-0-387-94328-2.

[Lan12] S. Lang. *Elliptic Functions*. 2nd ed. Graduate Texts in Mathematics. Springer New York, 2012. ISBN: 9781461247524.

[JMV09] David Jao, Stephen D. Miller, and Ramarathnam Venkatesan. "Expander graphs based on GRH with an application to elliptic curve cryptography". In: *Journal of Number Theory* 129.6 (June 2009), pp. 1491–1504. ISSN: 0022-314X. DOI: 10.1016/j.jnt.2008.11.006. URL: http://dx.doi.org/10.1016/j.jnt.2008.11.006.

[Piz90] Arnold K. Pizer. "Ramanujan graphs and Hecke operators". In: *Bulletin (New Series) of the American Mathematical Society* 23.1 (1990), pp. 127–137. URL: https://www.ams.org/journals/bull/1990-23-01/S0273-0979-1990-15918-X/S0273-0979-1990-15918-X.pdf.

[CJS14] Andrew Childs, David Jao, and Vladimir Soukharev. "Constructing elliptic curve isogenies in quantum subexponential time". In: *Journal of Mathematical Cryptology* 8.1 (Jan. 2014), pp. 1–29. ISSN: 1862-2984. DOI: 10.1515/jmc-2012-0016. URL: http://dx.doi.org/10.1515/jmc-2012-0016.

[Bro06] Reinier Broker. "Constructing elliptic curves of prescribed order". In: (Jan. 2006). URL: https://www.researchgate.net/publication/28641572_Constructing_elliptic_curves_of_prescribed_order.

[Pan21] Lorenz Panny. "Cryptography on Isogeny Graphs". Proefschrift. PhD thesis. Mathematics and Computer Science, Feb. 2021. ISBN: 978-90-386-5213-9.

[Feo17] Luca De Feo. "Mathematics of Isogeny Based Cryptography". In: *CoRR* abs/1711.04062 (2017). arXiv: 1711.04062. URL: http://arxiv.org/abs/1711.04062.

[Koh96] David R. Kohel. "Endomorphism rings of elliptic curves over finite fields". PhD thesis. University of California, Berkeley, 1996.

[Feo18] Luca De Feo. "Exploring Isogeny Graphs". HDR. Université de Versailles Saint-Quentin-en-Yvelines, Dec. 2018. URL: https://github.com/defeo/hdr/releases/download/defended/hdr.pdf.

[Sut13] Andrew Sutherland. "Isogeny volcanoes". In: *The Open Book Series* 1.1 (Nov. 2013), pp. 507–530. ISSN: 2329-9061. DOI: 10.2140/obs.2013.1.507. URL: http://dx.doi.org/10.2140/obs.2013.1.507.