Isogenies and Endomorphism Rings of Abelian Varieties of Low Dimension

Von der Fakultät für Mathematik und Naturwissenschaften der
Carl von Ossietzky Universität Oldenburg
zur Erlangung des Grades und Titels eines

Doktors der Naturwissenschaften (Dr. rer. nat.)

angenommene Dissertation von

Frau Christina Delfs

geboren am 04. April 1986 in Leer.

Gutachter:	**Prof. Dr. Andreas Stein**
Zweitgutachter:	**Prof. Dr. Florian Hess**
Tag der Disputation:	**16. Oktober 2015**

Zusammenfassung

Isogenien zwischen abelschen Varietäten über endlichen Körpern spielen sowohl bei theoretischen Betrachtungen in der modernen Zahlentheorie als auch bei kryptographischen Anwendungen dieses Gebietes häufig eine bedeutsame Rolle. Daher ist es interessant, bei gegebenen isogenen Varietäten A_0 und A_1 der selben Dimension g über einem Körper K effiziente Methoden zum Berechnen einer Isogenie $\phi : A_0 \to A_1$ zu finden. Die auftretenden Probleme werden mit zunehmender Dimension sehr komplex, daher konzentrieren wir uns zunächst auf den Fall von elliptischen Kurven über einem endlichen Körper.

Die bisherigen Algorithmen zum Berechnen von Isogenien bevorzugen gewöhnliche Kurven wegen der Struktur ihrer Endomorphismenringe und haben für supersinguläre Kurven eine schlechtere Laufzeit. In dieser Arbeit entwickeln wir theoretische Resultate, die insbesondere zu einem neuen Algorithmus führen. Dieser verbessert für supersinguläre elliptische Kurven über $\mathbb{F}_p$ die bisherigen Herangehensweisen deutlich und ist ebenso schnell wie die Algorithmen für Isogenien gewöhnlicher elliptischer Kurven. Dafür stellen wir mittels eingeschränkter Endomorphismenringe eine neuartige Verbindung von solchen Kurven und $\mathbb{F}_p$-rationalen Isogenien zu einer Idealklassengruppe her. Wir verwenden ähnliche Mittel wie bei dem bekannten Deuring Reduktionstheorem mit Endomorphismenringen gewöhnlicher elliptischer Kurven um dies zu erreichen. Außerdem zeigen wir, dass Isogenien unter dieser Reduktion immer über $\mathbb{F}_p$ definiert sind.

Diese Resultate liefern eine einfache Beschreibung des Aufbaus der $\mathbb{F}_p$-rationalen Isogeniegraphen supersingulärer elliptischer Kurven in eine levelartige Struktur, welche ähnlich der bereits bekannten gewöhnlichen Isogenievulkane die Grundlage der neuen Berechnungsmethode mit berechenbaren bidirektionalen Suchen ist. Implementationen des entstehenden Algorithmus und der klassischen Methode in `MAGMA` ergeben berechnete Ergebnisse, welche die vorhergehenden Komplexitätsanalysen bestätigen.

Zusätzlich zum elliptischen Fall untersuchen wir die möglichen Verallgemeinerungen auf höhere Dimension und vorallem die Situation von Jacobischen hyperelliptischer Kurven von Geschlecht zwei. Besonders supersinguläre abelsche Varietäten stellen sich dabei als schwierig heraus, da Ansätze aus dem gewöhnlichen Fall nicht greifen. Die verschiedenen theoretischen Hintergründe beeinflussen mögliche Lösungen von Problemen der Isogenieberechnung und liefern größere Hindernisse als bei elliptischen Kurven.

Abstract

Isogenies between abelian varieties defined over a finite field play an important role in theoretical considerations of modern number theory as well as in cryptographic applications of this area. Therefore it is interesting to find efficient methods for computing an isogeny $\phi : A_0 \to A_1$ for given isogenous varieties A_0 and A_1 of the same dimension g over a field K. The occurring problems become very complex with higher dimension, so we concentrate first on the case of elliptic curves defined over a finite field.

Existing algorithms for such elliptic curves so far favor ordinary curves due to their endomorphism ring structure and have a worse running time for supersingular curves. In this thesis we develop new structural results leading in particular to an algorithm which for supersingular elliptic curves defined over $\mathbb{F}_p$ improves the previous approaches notably and which is as fast as the algorithms for isogenies of ordinary elliptic curves. In order to achieve this, we find out how to use restricted endomorphism rings to establish a connection of such elliptic curves and $\mathbb{F}_p$-rational isogenies to an ideal class group, using means analogous to the famous Deuring Reduction Theorem for the endomorphism rings of ordinary elliptic curves. We also show that isogenies under this reduction are defined over $\mathbb{F}_p$.

These results yield a simple description of $\mathbb{F}_p$-rational supersingular isogeny graphs in an ordered level-structure, which provides the basis for the new computational method of feasible bi-directional searches like in the well-known ordinary isogeny volcanoes. `MAGMA` implementations of the emerging algorithm and the classical method reveal computational results which validate the preceding complexity analysis.

In addition to the elliptic case, we also investigate the possible generalizations to higher dimension where we focus on Jacobians of hyperelliptic curves of genus two. Especially supersingular abelian varieties prove to be more difficult in this setting since successful approaches of the ordinary case cannot be generalized directly. Diverging background theories affect the possible solution of problems concerning isogeny computation and present obstacles which appear much harder to access than for elliptic curves.

Contents

1 Introduction

Abelian varieties are important objects from algebraic geometry and number theory. They arise as algebraic varieties from a set of defining polynomials and at the same time they build an abelian group. Thus they have much structure that can be worked with and they turn out to be the basis of an interesting field of theory.

Elliptic curves are abelian varieties of genus one and have been of theoretical interest for many years before they were discovered for cryptographic applications. By now they are of great significance in many areas of recent research and play an important role in modern number theory and cryptography. They contribute a fundamental part in the proof of Fermat's Last Theorem and can be used for integer factorization and several public key cryptosystems. When regarded from different sides of theory, elliptic curves can be described with either algebraic elements or provide a connection to analytical objects, so they prove to be a many-faceted field of research. There are many standard references concerning the theory of elliptic curves (e.g. [38], [75], [91]) and their cryptographic applications (e.g. [13]) which provide a good overview.

Isogenies are rational maps between abelian varieties over a field K which have a finite kernel and are geometrically surjective. They appear in various applications of elliptic curves both in subjects of theoretical background and in cryptographic issues. Several properties of elliptic curves can be mapped to other elliptic curves via isogenies and thus problems for all elliptic curves in an isogeny class can be solved by showing them for a single representative.

It is easy to find out whether two given abelian varieties A_0 and A_1 which are defined over a finite field $\mathbb{F}_q$ lie in the same isogeny class; that is, whether there exists a non-constant isogeny between them. We will see from Tate's Isogeny Theorem in [86] that this is the case if and only if we have $\#A_0(\mathbb{F}_q) = \#A_1(\mathbb{F}_q)$. But explicitly and efficiently computing such an isogeny in terms of a rational map turns out to be a more difficult matter, even for low dimension.

Problem 1 (General Isogeny Problem). *Given two isogenous abelian varieties A_0 and A_1 of dimension g over a finite field K, compute an isogeny $\phi : A_0 \to A_1$.*

For $g = 1$ and ordinary elliptic curves there are algorithms based on an idea of Galbraith [27] which solve this task in $\widetilde{\mathcal{O}}(q^{1/4})$ field operations and storage[1], but for supersingular elliptic curves these ideas do not work due to different structures of their endomorphism rings.

[1] We will explain about complexity notation at the end of the Introduction chapter.

Even though supersingular elliptic curves over a finite field of prime characteristic p are always defined over $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$, the fastest method dealing with the problem of computing isogenies there has a running time of $\widetilde{\mathcal{O}}(p^{1/2})$ so far. There exist several cryptographic schemes – presented in SECTION 5 – supposedly relying on the hardness of computing such isogenies, so the question arises whether there are better methods for solving this problem. We explicitly pose this problem as follows.

PROBLEM 2 (Supersingular Elliptic Isogeny Problem). *Given two supersingular elliptic curves E_0 and E_1 over a finite field K, compute an isogeny $\phi : E_0 \to E_1$ with an algorithm that has complexity similar to the ones in the ordinary case.*

In this work we answer this question for the case where the supersingular elliptic curves E_0 and E_1 are defined over $\mathbb{F}_p$, that is for $K = \mathbb{F}_p$ in the situation of the problem. In order to accomplish this, we have to develop a modified version of the DEURING Reduction Theorem to establish a relation between the endomorphism rings of elliptic curves over certain number fields and the $\mathbb{F}_p$-rational endomorphism rings of supersingular elliptic curves defined over $\mathbb{F}_p$.

DEURING'S original theorem in [19] only preserves the endomorphism ring of ordinary elliptic curves after such a lifting and reduction process. We have shown with lifting theory, arithmetic of quadratic number fields and theory of ideal class groups that an analogous correspondence holds for supersingular curves when we restrict the endomorphism ring, see THEOREM 3.18 for the details and the proof.

RESULT. Let E be a supersingular elliptic curve defined over $\mathbb{F}_p$. Then there exists an elliptic curve $\widetilde{E}$ defined over a number field which reduces to E modulo p and we have

$$\operatorname{End} \widetilde{E} \;\cong\; \operatorname{End}_{\mathbb{F}_p} E.$$

The correspondence via lifting and reduction between those curves is uniquely defined up to isomorphism.

Furthermore we can also get a result as in PROPOSITION 3.19 about the isogenies connecting such supersingular elliptic curves and their behavior under reduction.

RESULT. Let $\widetilde{E}_0$ and $\widetilde{E}_1$ be elliptic curves over a number field such that their reductions E_0 and E_1 modulo p are supersingular elliptic curves defined over $\mathbb{F}_p$. Let further $\widetilde{\phi} : \widetilde{E}_0 \to \widetilde{E}_1$ be an isogeny. Then there is an isogeny $\phi : E_0 \to E_1$ which is defined over $\mathbb{F}_p$ such that $\widetilde{\phi}$ reduces to ϕ.

The resulting behavior can be used to introduce $\mathbb{F}_p$-rational isogeny graphs and examine their properties in SECTION 4. For primes $\ell \neq p$ we define the $\mathbb{F}_p$-rational supersingular ℓ-isogeny graph $G_0(\mathbb{F}_p, \ell)$ which has supersingular elliptic curves defined over $\mathbb{F}_p$ as nodes and $\mathbb{F}_p$-rational ℓ-isogenies as edges and investigate its behavior of in- and outgoing edges.

RESULT. Let $p > 3$ and ℓ be coprime primes and $G_0(\mathbb{F}_p, \ell)$ be the $\mathbb{F}_p$-rational supersingular isogeny graph. Then the structure of this graph can be explicitly determined as in THEOREMS 4.16 and 4.17 and resembles an ordinary ℓ-volcano with at most two levels.

The plotted graphs and the full supersingular isogeny graphs for several primes are given in the APPENDIX. It can be seen that in contrast to the full graph, the $\mathbb{F}_p$-rational graph has a more regular volcano-like structure but is not always connected. That reminds of the ordinary situation again and with the reduction results from above we can establish a connection to an ideal class group where the well-known result of BACH [1] gives us an upper bound for the norms of generators. Those norms comply with isogeny degrees and thus we have the analogous result.

RESULT. The $\mathbb{F}_p$-rational supersingular isogeny graph $G_0(\mathbb{F}_p, \mathcal{L})$ is fully connected when we use isogenies with degree $\ell \in \mathcal{L} := \{\ell \leq B\}$ as edges where B is the BACH bound.

Hence we are able to use results from graph theory on expander graphs, pose a bidirectional search algorithm as in the ordinary case, and expect the same complexity of $\widetilde{\mathcal{O}}(p^{1/4})$ field operations and storage of field elements. In fact, an complexity analysis proves those desired results. Thus this algorithm provides a considerable speedup of the previous methods which had a complexity of $\widetilde{\mathcal{O}}(p^{1/2})$. With that we get a positive answer to the SUPERSINGULAR ELLIPTIC ISOGENY PROBLEM above. The description of the algorithm and its complexity analysis can be found in SECTION 4.2.3.

RESULT. There is an algorithm which solves the above stated SUPERSINGULAR ELLIPTIC ISOGENY PROBLEM for $K = \mathbb{F}_p$ in a complexity of $\mathcal{O}(p^{1/4}(\log p)^5 \log\log p)$ running time and $O(p^{1/4})$ storage.

We implemented this algorithm in `MAGMA` and the computational results encourage the theoretical reflections. Both the source code and the computations for primes p up to a length of 32 bit can be found in the appendix.

When we return to the GENERAL ISOGENY PROBLEM, for arbitrary abelian varieties over a finite field or even only for JACOBIANS of hyperelliptic curves of genus $g > 1$, the situation is much more complicated. We will give an overview of some existing approaches for genus two and discuss what the problems are.

For ordinary JACOBIANS over a finite field many results can be generalized from the elliptic situation but there are still some open points. Horizontal isogenies between abelian varieties with isomorphic endomorphism ring can be handled, but the vertical structure is much more complicated than in the elliptic case. The distance from the surface no longer determines the endomorphism ring completely and there are also isogenies between varieties where the endomorphism rings are not contained in each other. When the real multiplication order is fixed as subset of the endomorphism rings though, some statements from the elliptic case can be generalized as in SECTION 4.3.2.

The supersingular case is in many respects more complex and thus there is not much theoretical knowledge yet. We will show the main obstacles for advanced theoretical results and algorithms there. A point which is a very prominent feature in that situation is that a supersingular abelian variety of dimension $g \geq 2$ does not have to be defined over a finite field. Even when regarding only such varieties defined over a fixed finite field, the endomorphism rings are orders in a sixteen-dimensional non-commutative algebra and difficult to treat. Consult SECTION 4.3.3 for a discussion of the implications.

This thesis is organized as follows. In SECTION 2 we introduce the background theory about the structure and the properties of the objects of peculiar interest we are dealing with. This provides the basics needed for our later work. The results which are used most frequently concern abelian varieties and especially supersingular elliptic curves, isogenies and the behavior of endomorphism rings of isogenous elliptic curves. A short excursus into graph theory gives us the terms to describe isogeny graphs and concepts concerning expander graphs. Those are used in complexity analyses of some presented algorithms.

SECTION 3 explains how endomorphism rings of certain elliptic curves defined over a number field behave towards each other. These relations supply the necessary tools for the definition and description of isogeny graphs. The structure and behavior of such endomorphism rings can be transferred to the ones of elliptic curves defined over a finite field.

In contrast to the case where the reduced elliptic curves are ordinary, the well-known lifting and reduction theorems of DEURING give no relation between the endomorphism rings of supersingular elliptic curves and their lifts. Therefore we develop a new version of those theorems which applies to the supersingular situation. This proven coherence is the reason why our later algorithms can work in the way they do.

Those algorithms are featured in SECTION 4 where also our main problem is addressed. First we present the ideas of the situation with ordinary elliptic curves where many results are known. We show how in the supersingular case those concepts cannot be employed. This leads us to the study of supersingular elliptic curves which are defined over the base field $\mathbb{F}_p$ for a prime p.

We illustrate how due to our adapted reduction theorem the restricted endomorphism rings of such elliptic curves provide a similar volcano-like structure as the full endomorphism rings in the ordinary case. Those structures show interesting regularities and relations with the full isogeny graphs, so we printed a number of those graphs in APPENDIX C. Based on that we can introduce a new algorithm which follows the lines of the ordinary algorithm and improves the running time of finding an isogeny between supersingular elliptic curves defined over $\mathbb{F}_p$ distinctly.

We implemented several algorithms in `MAGMA` in order to get a good comparison of the running time of the computations. All `MAGMA` codes can be found in APPENDIX A and the computational results in APPENDIX B.

The conclusion of SECTION 4 describes a few methods for the computation of isogenies between abelian varieties in general and their differences to the genus-one-case.

Eventually, in SECTION 5 we address cryptographic applications of elliptic curves and isogenies and briefly highlight their importance for the well-known ECDLP-problem.

In the end we examine two applications from cryptography where isogenies between supersingular elliptic curves are occurring, namely a cryptographic hash function and a key exchange protocol and cryptosystem. We analyze how our improved algorithm for computing isogenies in a subgraph of the full supersingular isogeny graph can affect the security of those schemes.

Part of this work can already be found on the `arXiv` ePrint archive referred to as DELFS-GALBRAITH [18], a publication which has been submitted and accepted to DESIGNS, CODES AND CRYPTOGRAPHY where it will appear shortly. This paper originated from a working collaboration started during a visit of the first author at the UNIVERSITY OF AUCKLAND which was partially funded by a DAAD scholarship for PhD students.

Used Notation in this Thesis. We will always denote the field of definition of an elliptic curve with K whereas the algebra containing orders which are isomorphic to the endomorphism ring of a given elliptic curve is called $\mathcal{K}$. Usually K is a number field or a finite field $\mathbb{F}_q$ of prime characteristic p such that $q = p^r$. $\mathcal{K}$ can be either a quaternion algebra or an imaginary quadratic field.

For any real number $x \in \mathbb{R}$ the notation $\log x$ always means the binary logarithm $\log_2 x$, any other logarithm to a basis b is written as $\log_b x$. The natural logarithm of such an element $x \in \mathbb{R}$ would be denoted with $\ln x$.

Complexity Notation. For comparing computational problems it is important to know how the running time and storage requirements of an algorithm grow with increasing data input. For that we regard weakly increasing functions which map the length of the problem input to the needed steps, arithmetic or binary operation or storage. Let $f : \mathbb{N} \to \mathbb{R}_{>0}$ be such a function, $0 < r, s \in \mathbb{Q}$ and $n_0, n, m \in \mathbb{N}$ in the following sets.

We define

$$
\begin{aligned}
\mathcal{O}(f) &:= \{g : \mathbb{N} \to \mathbb{R}_{>0} \mid \exists r, n_0\ \forall n > n_0 : \quad g(n) < rf(n)\}, \\
o(f) &:= \{g : \mathbb{N} \to \mathbb{R}_{>0} \mid \forall r, \exists n_0\ \forall n > n_0 : \quad g(n) < rf(n)\}, \\
\Omega_\infty(f) &:= \{g : \mathbb{N} \to \mathbb{R}_{>0} \mid \exists r, \text{ for infinitely many } n : \quad g(n) > rf(n)\}, \\
\omega(f) &:= \{g : \mathbb{N} \to \mathbb{R}_{>0} \mid \forall r, \text{ for infinitely many } n : \quad g(n) > rf(n)\}, \\
\Theta(f) &:= \{g : \mathbb{N} \to \mathbb{R}_{>0} \mid \exists r, s, n_0\ \forall n > n_0 : \quad rf(n) \leq g(n) \leq sf(n)\}.
\end{aligned}
$$

We also frequently use

$$
\widetilde{\mathcal{O}}(f) := \{g : \mathbb{N} \to \mathbb{R}_{>0} \mid \exists m : g \in \mathcal{O}(f(\log f)^m)\}
$$

when we want to ignore logarithmic terms.

The most important of those concepts for our work are $\mathcal{O}$ and $\widetilde{\mathcal{O}}$. We usually describe the complexity of our algorithms depending on the length $\log n$ of its input n and e.g. say the algorithm has a *complexity of $\mathcal{O}(f(\log n))$ in terms of field operations* or *storage requirements of $\mathcal{O}(f(\log n))$ field elements.* A field operation in $\mathbb{F}_q$ has an expected complexity of $\mathcal{O}((\log q)^2)$ in bit operations and a $\mathbb{F}_q$-element can be stored in $\mathcal{O}(\log q)$ bits.

For a *deterministic* algorithm we get the same output on the same way every time we apply it to a given input and thus always the same complexity. If an algorithm is *probabilistic*, we compute the expected value of its running time on a given input. When we consider the maximal value of this expected value on every possible input of the same length, we talk about *worst case complexity*. Analogously the *average complexity* is the average of all expected values.

As usual, an algorithm of input $n \in \mathbb{N}$ is *polynomial* in its length $\log n$ if it is in $\mathcal{O}((\log n)^k)$ for some integer $k \geq 1$ and *exponential* in $\log n$ if it lies in $\mathcal{O}(a^{\log n})$ for some real constant $a > 1$. When we define

$$L_n(u, v) := \exp((v + o(1)) \log(n)^u \log(\log(n))^{1-u})$$

for $u, v \in \mathbb{R}$, an algorithm with input as above having complexity $L_n(u, v)$ is *subexponential*.

2 Theoretical Foundations

In this thesis we will always work with a base field K which will be either a finite field or a number field with characteristic 0. In either case it is a perfect field[2], which will be needed in some of the proofs. We will regard *rational maps* between varieties in the projective space $\mathbb{P}^n(\bar{K})$ where $\bar{K}$ denotes an algebraic closure of K, so we will introduce the necessary background in Section 2.1 briefly.

Later in that section we will restrict to *algebraic curves*, that is, projective varieties of dimension one and most of the time to *elliptic curves* which are algebraic curves of genus one with rational points. We will be most interested in so-called *supersingular elliptic curves*, so we will describe their properties and several methods for determining whether a given elliptic curve is supersingular or not.

For our purposes the *endomorphism ring structure* of elliptic curves is important, thus we examine this concept in Section 2.2 for both ordinary and supersingular elliptic curves. Section 2.3 will give a very short introduction in graph theory and the concept of *expander graphs* which we will use for the analysis of our algorithms.

2.1 Basic Concepts

We will approach our objects of interest – *supersingular elliptic curves* and *isogenies of prime degree* ℓ – in this section via algebraic varieties and morphisms between them. Most of the theory is basic knowledge and can be found in Silverman [75], Mumford [62], Cohen [13] or Hartshorne [37].

Though elliptic curves as special projective varieties can be introduced independent of the general theory of varieties, in some points it is helpful to have a broader background and see which results work in a more general setting and which have to be explicitly restricted to elliptic curves. Hence it will be apparent that some of the occurring problems can also be stated in a more general situation. We will have a short look at such generalizations and why they cannot be handled with our methods in the Outlook.

Our regarded problems are mostly solved for ordinary elliptic curves, which we refer to as the *ordinary case*. The properties which distinguish supersingular elliptic curves from ordinary elliptic curves entail several complications of those well-known methods. Thus we will investigate supersingular elliptic curves and their properties thoroughly in the second part of this section.

[2] A field K is called *perfect* if every non-constant polynomial $f \in K[t]$ is separable.

2.1.1 Algebraic Varieties and Isogenies

Let K be a perfect field, $\mathbb{A}^n := \bar{K}^n$ be the *affine n-space over K* and I be a subset of the polynomial ring $\bar{K}[X_1, \cdots, X_n]$. Then we define an *affine algebraic set* through

$$\mathcal{V}(I) \quad := \quad \{x \in \mathbb{A}^n \mid f(x) = 0 \text{ for all } f \in I\}.$$

Especially if I is an ideal generated by a single polynomial f, we write $\mathcal{V}(f)$ for the algebraic set emerging through this construction.

Definition. An affine algebraic set $V \subseteq \mathbb{A}^n$ is called *reducible* if there are algebraic sets V_0, V_1 in $\mathbb{A}^n$ with $V = V_0 \cup V_1$ and $V_0 \neq V \neq V_1$. If no such sets exist, V is called *irreducible* or an *affine variety.*

The *ideal of an algebraic set V* is

$$\mathcal{I}(V) \quad := \quad \{f \in \bar{K}[X_1, \cdots, X_n] \mid f(x) = 0 \text{ for all } x \in V\}$$

which is a finitely generated ideal in $\bar{K}[X_1, \cdots, X_n]$ due to Hilbert's Basis Theorem. It can be shown that an affine algebraic set $V \neq \emptyset$ is an affine variety if and only if $\mathcal{I}(V)$ is a prime ideal.

We regard those structures restricted to K and get the *K-rational points* of $\mathbb{A}^n$

$$\mathbb{A}^n(K) \quad := \quad \{x = (x_1, \cdots, x_n) \in \mathbb{A}^n \mid x_i \in K\} = K^n.$$

When we define $x^\sigma := (\sigma(x_1), \cdots, \sigma(x_n))$ for all points $x = (x_0, \cdots, x_n) \in \mathbb{A}^n$ and $\sigma \in \mathrm{Gal}(\bar{K}/K)$, we get the equality

$$\mathbb{A}^n(K) \quad = \quad \{x \in \mathbb{A}^n \mid x^\sigma = x \text{ for all } \sigma \in \mathrm{Gal}(\bar{K}/K)\}.$$

Furthermore, an affine algebraic set V is said to be *defined over K* if $\mathcal{I}(V)$ has generators from $K[X_1, \cdots, X_n]$. In that case $V(K) := V \cap \mathbb{A}^n(K)$ will denote the set of *K-rational points of V*.

Let $V \subseteq \mathbb{A}^n$ be an affine variety. The set

$$\bar{K}[V] \quad \cong \quad {}^{\bar{K}[X_1, \cdots, X_n]}\!\big/_{\mathcal{I}(V)}.$$

is an integral domain and is called the *affine coordinate ring $\bar{K}[V]$ of V*. Elements in it can also be represented as functions $f : V \to \bar{K}$. Further we call its quotient field $\bar{K}(V)$ the *function field of V* and for an affine variety which is defined over K

we get $K[V]$ and $K(V)$ in an analogous way. Those are the subsets of $\bar{K}[V]$ resp. $\bar{K}(V)$ which are fixed by $\mathrm{Gal}(\bar{K}/K)$.

Let now $x \in V$ be a point on V. Then the localization

$$\bar{K}[V]_x \quad := \quad \{f \in \bar{K}(V) \mid f = g/h \text{ with } g, h \in \bar{K}[V] \text{ and } h(x) \neq 0\}$$

is called *local ring of V at x* and its elements f are *regular* or *defined at x*.

Definition. Let V be an affine variety, then we can define its *dimension* $\dim V$ to be the transcendence degree of $\bar{K}(V)$ over $\bar{K}$.

Particularly, we have $\dim \mathbb{A}^n = n$ and $\dim \mathcal{V}(f) = n - 1$ when f is a polynomial of degree $\deg f \geq 1$. Hartshorne [37] proposes an alternative description of the dimension of an affine variety in his Proposition I.1.7 as following.

Proposition 2.1. *For an affine variety V we have $\dim V = \dim \bar{K}[V]$ where $\dim \bar{K}[V]$ denotes the* Krull *dimension of the affine coordinate ring.*

Let V be an affine variety in $\mathbb{A}^n$ and let $f_1, \cdots, f_m \in \bar{K}[X_1, \cdots, X_n]$ generate $\mathcal{I}(V)$. Set

$$A_x \quad := \quad \left(\frac{\partial f_i}{\partial X_j}(x)\right)_{i,j} \in \bar{K}^{m \times n}.$$

Then V is said to be *smooth* or *non-singular* at a point $x \in V$ when we have $\mathrm{rk}\, A_x = n - \dim V$. If this condition holds for all $x \in V$, the affine variety V itself is called *smooth*, else it is called *singular*.

Now we introduce the projective analogues to the described concepts. The *projective n-space over K* is the set of all one-dimensional subspaces of $\mathbb{A}^{n+1}$ and denoted with $\mathbb{P}^n$. For $x, y \in \mathbb{A}^{n+1} \setminus \{0\}$ we have an equivalence relation defined through

$$x \sim y \quad \Longleftrightarrow \quad \exists \lambda \in \bar{K} : y = \lambda x$$

and the equivalence classes $[x] = \{\lambda x \mid \lambda \in \bar{K}^*\}$ of all $0 \neq x \in \mathbb{A}^{n+1}$ under this relation are just the elements of $\mathbb{P}^n$. Analogous to the affine n-space we define the *K-rational points of $\mathbb{P}^n$* as the set

$$\begin{aligned}\mathbb{P}^n(K) \quad &:= \quad \{[x] \in \mathbb{P}^n \mid x = (x_0, \cdots, x_n) \text{ with } x_i \in K\} \\ &= \quad \{[x] \in \mathbb{P}^n \mid [x]^\sigma = [x] \text{ for all } \sigma \in \mathrm{Gal}(\bar{K}/K)\}.\end{aligned}$$

Here $[x]^\sigma$ denotes the element $[x^\sigma] \in \mathbb{P}^n$ with $x^\sigma = (\sigma(x_0), \cdots, \sigma(x_n))$ as before and this is well-defined. We write $[x] = [x_0 : x_1 : \cdots : x_n]$.

A polynomial $f \in \bar{K}[X_0, \cdots, X_n]$ is *homogeneous of degree* d if it satisfies

$$f(\lambda X_0, \cdots, \lambda X_n) = \lambda^d f(X_0, \cdots, X_n)$$

for all $\lambda \in \bar{K}$. For such a homogenous polynomial f and equivalent $x, y \in \mathbb{A}^{n+1}$ with $y = \lambda x$ as above, we get $f(x) = 0$ if and only if $f(y) = 0$. Hence solutions of the equation $f([x]) = 0$ are well-defined.

Let I be an homogeneous ideal of $\bar{K}[X_0, \cdots, X_n]$, that is an ideal which is finitely generated by homogeneous polynomials. Then we can define a *projective algebraic set* through

$$\mathcal{V}(I) \quad := \quad \{[x] \in \mathbb{P}^n \mid f([x]) = 0 \text{ for all } f \in I\}$$

as well as the ideal of such a projective algebraic set V

$$\mathcal{I}(V) \quad := \quad \{f \in \bar{K}[X_0, \cdots, X_n] \text{ homogeneous} \mid f([x]) = 0 \text{ for all } [x] \in V\}.$$

V is *defined over* K if $\mathcal{I}(V)$ can be generated by homogeneous polynomials from $K[X_0, \cdots, X_n]$ and $V(K) = V \cap \mathbb{P}^n(K)$ is the set of K-rational points of V. Also the definition of *projective variety* is analogous to the affine case with the appropriate objects.

Let $f \in \bar{K}[X_1, \cdots, X_n]$ be a polynomial of degree d. Then the *homogenization of* f *with respect to* X_i for $i \in \{0, \cdots, n\}$ is given by

$$f^* \quad = \quad X_i^d f\left(\tfrac{X_0}{X_i}, \cdots, \tfrac{X_{i-1}}{X_i}, \tfrac{X_{i+1}}{X_i}, \cdots, \tfrac{X_n}{X_i}\right) \in \bar{K}[X_0, \cdots, X_n].$$

In the other direction the *dehomogenization of* $f \in \bar{K}[X_0, \cdots, X_n]$ *with respect to* X_i is

$$f_* \quad = \quad f\left(X_0, \cdots, X_{i-1}, 1, X_{i+1}, \cdots, X_n\right)$$

which can be interpreted as an polynomial in $\bar{K}[X_1, \cdots, X_n]$.

There are $n+1$ embeddings of $\mathbb{A}^n$ into $\mathbb{P}^n$ of the form

$$\begin{aligned} \varepsilon_i : \mathbb{A}^n \quad &\rightarrow \quad \mathbb{P}^n \\ (x_1, \cdots x_n) \quad &\mapsto \quad [x_1, \cdots, x_{i-1}, 1, x_i, \cdots x_n]. \end{aligned}$$

When we consider a projective variety V, we will always choose an embedding of $\mathbb{A}^n$ in $\mathbb{P}^n$ such that we have $\mathbb{A}^n \cap V \neq \emptyset$. This intersection will be an affine variety in $\mathbb{A}^n$.

With these concepts it is possible to define the *dimension*, *coordinate ring*, *function field* and *smoothness* of a projective variety V as the corresponding structures or properties of $V \cap \mathbb{A}^n$ as affine variety.

Maps between Projective Varieties. Let now V be a projective variety, $[x] \in V$ and $f \in \bar{K}(V)$. Then we call the function f *defined* or *regular* at $[x]$ if f can be evaluated at $[x]$, that is, it can be written as a fraction of functions from $\bar{K}[V]$ where the denominator g satisfies $g([x]) \neq 0$.

Let V_0 and V_1 be projective varieties in $\mathbb{P}^n$ and let $f_i \in \bar{K}(V_0)$ be functions which provide $[f_0([x]), \cdots, f_n([x])] \in V_1$ for all $[x] \in V_0$ where all f_i are defined. A map $\phi : V_0 \to V_1$ is called *rational map* if it is of the form $\phi = (f_0, \cdots, f_n)$ with such functions.

Such a rational map ϕ is *defined over* K or K*-rational* if there exists a scalar $\lambda \in K^*$ with $\lambda f_0, \cdots, \lambda f_n \in K(V_0)$, which due to Exercise 1.12 of Silverman [75] happens if and only if we have $\phi = \phi^\sigma = (f_0^\sigma, \cdots, f_n^\sigma)$ for all $\sigma \in \mathrm{Gal}(\bar{K}/K)$. Here f_i^σ denotes the image of the function f_i under the group action

$$\begin{array}{rcl} \mathrm{Gal}(\bar{K}/K) \times \bar{K}(V_0) & \to & \bar{K}(V_0) \\ (\sigma, f) & \mapsto & f^\sigma \end{array}$$

which is induced by the usual action of $\mathrm{Gal}(\bar{K}/K)$ on coefficients of polynomials; see page 4 of Silverman [75] for more details.

We also have that

$$\{f \in \bar{K}(V_0) \mid f^\sigma = f \text{ for all } \sigma \in \mathrm{Gal}(\bar{K}/K)\} \quad = \quad K(V_0)$$

(Remark 5.4.14 of Galbraith [28]) and thus $\phi^\sigma = \phi$ as above is equivalent to $f_i \in K(V_0)$ for all $i \in \{0, \cdots, n\}$.

Furthermore, ϕ is said to be *defined at* $[x] \in V_0$ if there is some $g \in \bar{K}(V_0)$ such that all gf_i are defined at $[x]$ but not all of them are 0 evaluated at $[x]$.

Definition. Let V_0 and V_1 be projective varieties. A rational map $\phi : V_0 \to V_1$ which is defined at every point $[x]$ of V_0 is called a *morphism of varieties*.

We will work mostly with *algebraic curves*, that is, projective varieties of dimension one. Especially when we deal with a smooth algebraic curve C, we have the advantage that any rational map from C into a projective variety V is a morphism, see Proposition II.2.1 of Silverman [75].

Now we will deal with morphisms between smooth algebraic curves C_0 and C_1. HARTSHORNE [37] shows in THEOREM II.6.8 that such morphisms are either constant or surjective. We want to introduce the *degree* of a morphism between smooth algebraic curves.

Let C_0 and C_1 be smooth algebraic curves defined over the field K. We start with defining the degree of a constant morphism $\phi : C_0 \to C_1$ to be 0. Let otherwise $\phi : C_0 \to C_1$ be a non-constant morphism. We get an injective map

$$\begin{array}{rcl} \phi^* : K(C_1) & \to & K(C_0) \\ f & \mapsto & f \circ \phi \end{array}$$

which fixes elements of K and provides a finite extension $K(C_0)$ of $\phi^*(K(C_1))$ and set the degree of ϕ to be

$$\deg \phi \quad := \quad [K(C_0) : \phi^*(K(C_1))] \, .$$

This extension can be separable or inseparable and we call ϕ a *separable* resp. *inseparable morphism* accordingly. The separable and inseparable degrees of ϕ are the corresponding degrees of the field extension and labeled with $\deg_s \phi$ resp. $\deg_i \phi$. For details of this construction see THEOREM II.2.4 and following of SILVERMAN [75].

Since a purely inseparable field extension can only occur in prime characteristic p and its degree is a power of p then, this means that the inseparable part of a morphism has to have a prime power degree. It can be shown that every morphism can be split in a product of a separable one and a special inseparable morphism which we describe below.

Let K be a field with characteristic $p > 0$ and let C be a smooth algebraic curve defined over K such that we have $C = \mathcal{V}(I)$ with $I := \langle f_1, \cdots, f_m \rangle$ being the ideal generated by the polynomials $f_i \in K[X_0, \cdots, X_n]$. Let q be a power of p and define the polynomials $f_i^{(q)}$ to arise from f_i through taking the q-th power of each coefficient.

DEFINITION. Let in this situation $C^{(q)} = \mathcal{V}(I^{(q)})$ be the smooth algebraic curve where $I^{(q)}$ is the ideal generated by $f_1^{(q)}, \cdots, f_m^{(q)}$. Then the morphism

$$\begin{array}{rcl} \pi_q : C & \to & C^{(q)} \\ [x_0 : \cdots : x_n] & \mapsto & [x_0^q : \cdots : x_n^q] \end{array}$$

is called the *q-th* FROBENIUS *morphism.*

The FROBENIUS morphism can be defined for an arbitrary algebraic variety defined over $\mathbb{F}_q$ in an similar way as $\pi_q : A \to A^{(q)}$ with $A^{(q)}$ constructed analogue. Further there exists a morphism

$$\rho_q : A^{(q)} \quad \to \quad A$$

with $\rho_q \pi_q = [q]_A$ and $\pi_q \rho_q = [q]_{A^{(q)}}$, the so-called *Verschiebung*.

SILVERMAN shows that the FROBENIUS morphism is purely inseparable and has degree q. It turns out to be quite useful when investigating arbitrary morphisms, because due to the following lemma (COROLLARY II.2.12 of SILVERMAN [75]) we can restrict to separable morphisms in many situations.

LEMMA 2.2. *Let C_0, C_1 be algebraic curves defined over a finite field of characteristic p and let $\phi : C_0 \to C_1$ be a morphism with $\deg_i \phi = q = p^r$. Then there exists a separable morphism $\psi : C_0^{(q)} \to C_1$ with $\phi = \psi \circ \pi_q$.*

$$\begin{tikzcd} C_0 \arrow[r, "\pi_q"] \arrow[rr, bend right, "\phi"'] & C_0^{(q)} \arrow[r, "\psi"] & C_1 \end{tikzcd}$$

For proving this lemma it is relevant that K is a perfect field as can be seen in SILVERMAN'S proof. We will not expand on this.

Now we want to restrict ourselves further to algebraic curves which are defined by a single homogeneous polynomial $f \in K[X_0, \cdots, X_n]$. Since the dimension of such a variety $\mathcal{V}(f)$ is $n-1$ but an algebraic curve has dimension 1, this yields $n = 2$.

DEFINITION. An algebraic curve in $\mathbb{P}^2$ is called a *plane projective curve.* If C is a non-singular plane projective curve over a field K with $C(K) = \mathcal{V}(f) \neq \emptyset$ and $\deg f = 3$, C is called an *elliptic curve* and often labeled E.

For a plane curve C which is defined by a polynomial f of degree d, we can define the *genus of* C as $g = \lfloor \frac{d-1}{2} \rfloor$. Thus, an elliptic curve is a curve of genus one. This term comes from the RIEMANN-ROCH-Theorem which can be found in SECTION I.5 of STICHTENOTH [82].

We can define an addition law on an elliptic curve E which provides an abelian group structure with identity element O on E. The K-rational points $E(K)$ are a subgroup of E for every field K where E can be defined. The precise addition formula can be looked up in SILVERMAN [75] or WASHINGTON [91].

More general, a smooth projective variety V where the structure of an abelian group can be defined with morphisms and a base point $O \in V(K)$, is called *abelian variety*. Such an abelian variety A is *defined over* K if it is defined over K as a projective variety and the morphisms for addition and inversion are also defined over K. A is *simple* if there is no non-trivial abelian varieties $B \subsetneq A$.

For an arbitrary smooth algebraic curve C we can construct the JACOBIAN *variety* $\mathrm{Jac}(C)$ which is an abelian variety such that C can be embedded in $\mathrm{Jac}(C)$. The dimension of $\mathrm{Jac}\, C$ is equal to the genus of C. For elliptic curves we have $\mathrm{Jac}(E) = E$. In particular, the JACOBIAN variety is isomorphic as a group to the divisor class group $\mathrm{Pic}^0 C$ which is the set of degree zero divisors of C modulo the principal divisors. Thus we can describe elements of $\mathrm{Jac}\, C$ as residue classes of divisors with degree zero. We will not extend much on this theory though since we will not need much of the concepts for our results. MILNE [60] addresses JACOBIAN varieties in more detail.

DEFINITION. Let A_0 and A_1 be abelian varieties with O_0 and O_1 being their respective identity elements. A morphism $\phi : A_0 \to A_1$ with $\phi(O_0) = O_1$ is called *isogeny*. If there exists an isogeny between A_0 and A_1 which is not constant, A_0 and A_1 are *isogenous*.

PROPOSITION 7.1 of MILNE [59] gives us a few nice properties of this general concept.

LEMMA 2.3. *A non-constant isogeny ϕ between abelian varieties A_0 and A_1 is surjective and has a finite kernel. Further,* $\dim A_0 = \dim A_1$ *has to hold.*

Let ϕ be a separable isogeny, then we know from the fundamental theorem of finitely generated abelian groups that there exist integers $\ell_1, \cdots, \ell_s \in \mathbb{N}$ satisfying $\ell_{i+1} \mid \ell_i$ for $i \in \{1, \cdots, s-1\}$ such that we get

$$\ker \phi \;\cong\; \mathbb{Z}/\ell_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/\ell_s\mathbb{Z}$$

and $\# \ker \phi = \prod_{i=1}^{s} \ell_i$. In that case we call ϕ a $(\ell_1, \cdots, \ell_s)$-*isogeny*. If we have $s = 1$, we see that the number $\ell := \ell_1$ is the degree of the isogeny and ϕ is called ℓ-isogeny.

Note that for genus $g > 1$ the term ℓ-*isogenies* is sometimes ambiguously used for either isogenies of degree ℓ or isogenies with kernel isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^g$. In the elliptic curve case these two concepts coincide, but for higher genus g the latter ones have degree ℓ^g. We will use the term for $(\ell, \cdots, \ell)$-isogenies.

A simple example of an isogeny from an abelian variety A over a field K to itself is the so-called *multiplication-by-m-map* for any $m > 0$ defined through

$$\begin{aligned} [m] \; := \; [m]_A : A \; &\to \; A \\ P \; &\mapsto \; mP = \underbrace{P + \cdots + P}_{m \text{ times}}. \end{aligned}$$

For $m < 0$ we set $[m](P) := [-m](-P)$ and $[0](P) := O_A$ for all $P \in A(\bar{K})$, so we actually can define multiplication by m for any integer m. MILNE [59] THEOREM 7.2 shows that this map has degree $\deg[m] = m^{2g}$ where g is the dimension of A. For positive m the kernel of the multiplication-by-m-map equals the m-torsion subgroup of A,

$$\ker[m] \; = \; A[m] \; := \; A(\bar{K})[m] \; = \; \{P \in A(\bar{K}) \mid mP = O_A\}.$$

We will use this connection and especially the p-torsion in characteristic p for elliptic curves later in SECTION 2.1.2.

We are able to determine the structure of such a torsion subgroup as shown in REMARKS 7.3 and 7.4 of MILNE [59]. For that we use the notation

$$\underbrace{\mathbb{Z}/m\mathbb{Z} \times \cdots \times \mathbb{Z}/m\mathbb{Z}}_{n \text{ times}} = (\mathbb{Z}/m\mathbb{Z})^n$$

for $n \in \mathbb{N}_0$ where we set $(\mathbb{Z}/m\mathbb{Z})^0 = \{0\}$.

LEMMA 2.4. *Let A be an abelian variety of dimension g defined over a field K.*

1. *Let $m \in \mathbb{Z}$ be an integer such that $\operatorname{char} K \nmid m$. Then we have*

$$A[m] \;\cong\; (\mathbb{Z}/m\mathbb{Z})^{2g}$$

as isomorphism of groups.

2. *Let $\operatorname{char} K = p > 0$ be a prime and m be a power of p. Then*

$$A[m] \;\cong\; (\mathbb{Z}/m\mathbb{Z})^{r_p(A)},$$

where $0 \le r_p(A) \le g$ is an integer called the p-rank of A. *Again, we mean group isomorphism.*

REMARK. The p-rank of an abelian variety A has a connection to the property of A being ordinary or supersingular as we will see in SECTION 2.1.2.

Definition. Let A_0 and A_1 be abelian varieties of dimension g defined over a field K. Then

$$\mathrm{Hom}(A_0, A_1) \quad := \quad \{\phi : A_0 \to A_1 \text{ isogeny}\}$$

denotes the set of isogenies between A_0 and A_1. $\mathrm{End}\, A_0 := \mathrm{Hom}(A_0, A_0)$ the so-called *endomorphism ring* of A_0.

Remark. We will see that $\mathrm{Hom}(A_0, A_1)$ is a free abelian group under addition of morphisms and $\mathrm{End}(A_0)$ is a ring with addition and composition of morphism.

When working with isogenies it is a natural question to ask how to determine whether two given abelian varieties over a field K are isogenous apart from having the same dimension. We will introduce the theory leading to a mighty theorem for this issue on the following pages.

Definition. Let q be a prime power and V be a projective variety defined over $\mathbb{F}_q$ and let $a_n := \#V(\mathbb{F}_{q^n})$. The *zeta function of V* is the power series defined through

$$Z_V \quad := \quad \exp\left(\sum_{n=1}^{\infty} \tfrac{a_n}{n} X^n\right).$$

Especially the zeta function is defined for abelian varieties and for algebraic curves where it is most often applied. Silverman [75] presents the so-called Weil Conjectures concerning the zeta function in Theorem V.2.2. as follows.

Theorem 2.5. *Let q be a prime power and V as above be a projective variety defined over $\mathbb{F}_q$. Let V be smooth and of dimension g. Then*

1. *The zeta function has rational coefficients, $Z_V \in \mathbb{Q}[[X]]$.*

2. *We have*

$$Z_V = \frac{P_1 \cdot P_3 \cdots P_{2g-1}}{P_0 \cdot P_2 \cdots P_{2g}}$$

with $P_i \in \mathbb{Z}[X]$ for $i \in \{0, \cdots, 2g\}$ such that we have

$$P_i = \prod_{j=1}^{d_i} (1 - \alpha_{ij} X)$$

with $|\alpha_{ij}| = \sqrt{q}$. This is also called the Riemann hypothesis.

Let A be an abelian variety over a field K and for a prime ℓ with $\operatorname{char} K \neq \ell$ consider the torsion subgroups $A[\ell^n] := A(\bar{K})[\ell^n]$ with $n \in \mathbb{N}$. Then an inverse limit with respect to the the multiplication-by-ℓ-map

$$[\ell] : A[\ell^n] \rightarrow A[\ell^{n-1}]$$

induces the TATE *module*

$$T_\ell A := \varprojlim_n A[\ell^n].$$

For abelian varieties A_0 and A_1 defined over K and prime $\ell \neq \operatorname{char} K$ this concept leads to a homomorphism

$$\begin{aligned} T_\ell : \operatorname{Hom}(A_0, A_1) &\rightarrow \operatorname{Hom}_{\mathbb{Z}_\ell}(T_\ell A_0, T_\ell A_1) \\ \phi &\mapsto T_\ell \phi, \end{aligned}$$

where $\mathbb{Z}_\ell$ denotes the usual ℓ-adic integers.

MUMFORD [61] uses this map in THEOREM 19.3 and the following COROLLARY 1 for the following results which can also be seen in MILNE [59], THEOREM 10.15.

PROPOSITION 2.6. *Let A_0 and A_1 be abelian varieties defined over a field K with dimension g_0 resp. g_1 and let ℓ be a prime with* $\operatorname{char} K \neq \ell$*.*

Then injective map

$$\operatorname{Hom}(A_0, A_1) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \hookrightarrow \operatorname{Hom}_{\mathbb{Z}_\ell}(T_\ell A_0, T_\ell A_1)$$

is induced by T_ℓ.

Especially $\operatorname{Hom}(A_0, A_1)$ *is a finitely generated free abelian group and a $\mathbb{Z}$-module with rank at most $4g_0g_1$.*

For a finite field K the map in PROPOSITION 2.6 is even bijective due to the MAIN THEOREM of TATE [86].

Let A be an abelian variety of dimension g defined over a field K and ℓ be a prime with $\operatorname{char} K \neq \ell$. Due to PROPOSITION 2.6 the endomorphisms ring $\operatorname{End} A$ is a free abelian group which is finitely generated of rank less than or equal to $4g^2$.

Let $\phi \in \operatorname{End} A$ be an isogeny from A to itself. Then we know from PROPOSITION 2.6 that the TATE module $T_\ell A$ is a $\mathbb{Z}_\ell$-module of rank $2g$. Thus when we regard the homomorphism $T_\ell \phi \in \operatorname{End} T_\ell A$, we can use standard linear algebra to construct the transformation matrix $M_{T_\ell \phi}$ and the characteristic polynomial $\chi_{T_\ell \phi} := \det(XI_{2g} - M_{T_\ell \phi})$.

Mumford [61] shows in Theorem 19.4 that the polynomial $\chi_{T_\ell \phi}$ is a monic polynomial of degree $2g$ with coefficients from $\mathbb{Z}$ and is surprisingly independent of ℓ. Furthermore, we have $\deg \phi = \det M_{T_\ell \phi}$ and $\deg(a \operatorname{id}_A - \phi) = \chi_{T_\ell \phi}(a)$ for all $a \in \mathbb{Z}$. Most importantly, the polynomial $\chi_{T_\ell \phi}$ is zero evaluated at ϕ.

With those results we can see that $\chi_{T_\ell \phi}$ is completely determined by ϕ and thus the next definition is justified.

Definition. Let A be an abelian variety of dimension g defined over a field K, let ℓ be any prime different from $\operatorname{char} K$ and let $\phi \in \operatorname{End} A$ be an isogeny. The polynomial $\chi_\phi := \chi_{T_\ell \phi}$ is called *characteristic polynomial* of ϕ.

When we write $\chi_\phi = \sum_{i=1}^{2g} a_i X^i$, we call a_0 the *norm* and $-a_{2g-1}$ the *trace of* ϕ.

Most important for our purposes is the characteristic polynomial of the Frobenius morphism which will play an prominent role in our investigations concerning endomorphisms of elliptic curves later. We often also call this characteristic polynomial χ_A.

Both the concepts of zeta functions and characteristic polynomial of the Frobenius are used in the fundamental result from Tate in Theorem 1c of [86] which gives us a very useful tool to determine whether two abelian varieties are isogenous.

Theorem 2.7 (Tate's Isogeny Theorem)**.** *Let q be a prime power and A_0 and A_1 be abelian varieties defined over the finite field $\mathbb{F}_q$. Let χ_0 and χ_1 be the characteristic polynomials of the respective q-*Frobenius *morphisms. Then we get*

$$\begin{aligned} A_0 \text{ and } A_1 \text{ are isogenous over } \mathbb{F}_q \quad &\iff \quad \chi_{A_0} = \chi_{A_1} \\ &\iff \quad Z_{A_0} = Z_{A_1} \\ &\iff \quad \#A_0(K) = \#A_1(K) \\ &\qquad\quad \text{for every finite extension } K \supseteq \mathbb{F}_q. \end{aligned}$$

Especially the last condition will turn out to be of great importance later.

Elliptic Curves. Now we will present some individual structures of elliptic curves which are much sore simple than in the general situation. Particularly for computations and applications it turns out that they can be handled much better than arbitrary varieties of higher dimension due to those properties.

✦ Silverman [75] shows how the generating polynomial for an elliptic curve defined over K can be written in a *projective* Weierstrass *form*

$$X_1^2 X_2 + a_1 X_0 X_1 X_2 + a_3 X_1 X_2^2 - X_0^3 - a_2 X_0^2 X_2 - a_4 X_0 X_2^2 - a_6 X_2^3$$

with $a_1, a_2, a_3, a_4, a_6 \in K$. When we apply dehomogenization with respect to X_2 we get the *affine* WEIERSTRASS *form*

$$Y^2 + a_1XY + a_3Y - X^3 - a_2X^2 - a_4X - a_6$$

in the variables $X := X_0/X_2$ and $Y := X_1/X_2$. The point $[0, 1, 0] \in \mathbb{P}^2$ is a solution of the first projective equation but cannot be displayed in the second affine situation. Such a point is called *point at infinity* and usually denoted by O. For an elliptic curve there is exactly one point at infinity.

✦ Let $F \in K[X_0, X_1, X_2]$ be the homogeneous defining polynomial of an elliptic curve in projective description as above and $f \in K[X, Y]$ be the dehomogenized one. The elliptic curve E can be written as

$$\begin{gathered}\{[x_0 : x_1 : x_2] \in \mathbb{P}^2 \mid F([x_0 : x_1 : x_2]) = 0\} \quad \text{or} \\ \{(x, y) \in \bar{K}^2 \mid f(x, y) = 0\} \cup \{O\}.\end{gathered}$$

We will prefer the affine notation and use the phrasing *E is represented by f*, always keeping the projective background in mind.

✦ For $\operatorname{char} K > 3$ we can simplify this WEIERSTRASS polynomial to

$$Y^2 - X^3 - aX - b$$

with $a, b \in K$. Since in our problems the cases $p = 2$ and $p = 3$ are of no interest, we will usually restrict to such an equation if we need an explicit description of the curve. For the forms in characteristic 3 and the conversion of the equations into each other see SILVERMAN [75], CHAPTER III.1.

✦ An elliptic curve E is a smooth algebraic curve, so we have to check the differentials $\frac{\partial f}{\partial X}$ and $\frac{\partial f}{\partial Y}$ not being both zero at a point of E.For $\operatorname{char} K > 3$ a cubic curve E is smooth if and only if the *discriminant of E*

$$\Delta \ := \ \Delta(E) := -16(4a^3 + 27b^2) \in K$$

is not zero.

✦ The *j-invariant* of an elliptic curve E is given through the equation

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

For every element of K there is an elliptic curve defined over K with this element as j-invariant and two elliptic curves E_0 and E_1 are isomorphic over $\bar{K}$ if and only if we have $j(E_0) = j(E_1)$. These j-invariants will play an important role in our investigation later. They further help to see where the elliptic curve can be defined.

Proposition 2.8. *An elliptic curve E can be defined over $\mathbb{F}_q$ if and only if its j-invariant lies in $\mathbb{F}_q$.*

Proof. The implication '$\Longrightarrow$' is a trivial computation since j is defined via the coefficients of the Weierstrass polynomial.

The other direction '$\Longleftarrow$' follows from Proposition 1.4.c of Silverman [75] as for given $j \in \mathbb{F}_q$ the curves given by Weierstrass polynomials

$$\begin{aligned} Y^2 + XY - X^3 + \tfrac{36}{j-1728}X + \tfrac{1}{j-1728} & \qquad \text{for } j \neq 0, 1728 \\ Y^2 + Y - X^3 & \qquad \text{for } j = 0 \\ Y^2 - X^3 - X & \qquad \text{for } j = 1728 \end{aligned}$$

are smooth and have j-invariant j. □

In characteristic $p > 0$ we have already seen for $q = p^r$ the q-th Frobenius which for an elliptic curve E defined over $\mathbb{F}_q$ can be expressed as a map

$$\begin{aligned} \pi_q : E &\rightarrow E^{(q)} \\ P := (x, y) &\mapsto (x^q, y^q) \\ O_E &\mapsto O_{E^{(q)}} \end{aligned}$$

which is also an isogeny and has degree $\deg \pi_q = q$. If E is defined over $K = \mathbb{F}_q$, we even get $E^{(q)} = E$ and hence an endomorphism with $\pi_q : E \rightarrow E$, the so-called Frobenius *endomorphism.* Furthermore, for any $s \in \mathbb{N}$ the Frobenius π_q generates the Galois group $\mathrm{Gal}(\mathbb{F}_{q^s}/\mathbb{F}_q)$ which is a cyclic group of order s (Galbraith [28], Theorem A.8.3).

This endomorphism π_q is very important in our work because it provides a simple way to check whether an isogeny between elliptic curves is defined over $\mathbb{F}_q$ as seen in Lemma 2.19. The resulting statement appears at several crucial points in our discussion and provides the possibility to regard supersingular isogeny graphs in the way we do in Section 4.2.2.

Remark. There are several nice properties of isogenies between elliptic curves over a field K which we will state without proof here. They can be found in Chapter III of Silverman [75].

- Every isogeny between two elliptic curves E_0 and E_1 over a field K is a homomorphism. $\operatorname{Hom}(E_0, E_1)$ is a torsion-free $\mathbb{Z}$-module with rank at most four.
- Every non-constant isogeny has a finite kernel and is *geometrically surjective*, which means that $\phi : E_0(\bar{K}) \to E_1(\bar{K})$ is surjective.
- We have already defined the degree of a morphism in a more general setting. Especially we have that $\deg : \operatorname{Hom}(E_0, E_1) \to \mathbb{Z}$ is a positive definite quadratic form. That means in particular that the degree is always non-negative, equal zero only for the trivial isogeny $[0]$, and we have $\deg \phi = \deg -\phi$. Further the pairing defined through $\langle \phi, \psi \rangle := \deg(\phi + \psi) - \deg \phi - \deg \psi$ is bilinear.

Let E be an elliptic curve defined over a field K. We already defined the *endomorphism ring* $\operatorname{End} E$ as $\operatorname{Hom}(E, E)$ and have seen that it is actually a ring with addition and composition of isogenies. We will investigate its structure in more detail in Section 2.2.3. When we regard only endomorphisms which are defined over K, we write $\operatorname{End}_K(E)$ for the respective set. Further the *automorphism group* $\operatorname{Aut}(E)$ of E is the set of isogenies from E to itself with degree 1, that is, isomorphisms.

Since we have at least $\pm \operatorname{id} \in \operatorname{Aut}(E)$, the number of automorphisms of an elliptic curve E has to be larger than one. Furthermore, $\# \operatorname{Aut}(E)$ divides 24 and we have

$$\# \operatorname{Aut}(E) = \begin{cases} 2 & \text{if } j(E) \notin \{0, 1728\}, \\ 4 & \text{if } j(E) = 1728 \text{ and } \operatorname{char} K > 3, \\ 6 & \text{if } j(E) = 0 \text{ and } \operatorname{char} K > 3, \\ 12 & \text{if } j(E) = 0 \text{ and } \operatorname{char} K = 3, \\ 24 & \text{if } j(E) = 0 \text{ and } \operatorname{char} K = 2 \end{cases}$$

as seen in Galbraith [28], Theorem 9.4.4. This will become important when we regard equivalent isogenies later in this section.

We have seen in Lemma 2.2 that any isogeny ϕ can be represented as the composition $\phi = \psi \circ \pi_q$ of a separable isogeny ψ and a Frobenius morphism. Therefore we often restrict to separable isogenies only which also have the advantage that the degree can be determined by the number of points in its kernel. We will see that our construction methods always yield separable isogenies, too.

A useful criterion for separability of some special isogenies can be found in Corollary III.5.5 of Silverman [75].

Corollary 2.9. *Let E be an elliptic curve over a finite field $\mathbb{F}_q$ of characteristic p. Let m, n be integers and define the isogeny $\phi : E \to E$ through $\phi := [m] + [n]\pi_q$. Then we have*

$$\phi \text{ is separable} \quad \Longleftrightarrow \quad p \nmid m.$$

Remark. In the situation of the corollary we can immediately see the following properties:

- $[m] : E \to E$ is separable $\iff m \not\equiv 0 \pmod{p}$,
- $\pi_q : E \to E$ is never separable.

The next result is Corollary III.4.11 of Silverman [75] and will be needed in a later part of this work.

Lemma 2.10. *Let K be a field, E_0, E_1 and E_2 be elliptic curves defined over K with non-constant isogenies $\phi_i : E_0 \to E_i$ for $i \in \{1, 2\}$. If ϕ_1 is separable and we have* $\ker \phi_1 \subseteq \ker \phi_2$, *then there exists an unique isogeny $\phi : E_1 \to E_2$ with $\phi_2 = \phi \circ \phi_1$.*

$$\begin{tikzcd} E_0 \arrow[r, "\phi_1"] \arrow[rr, bend right, "\phi_2"'] & E_1 \arrow[r, "\phi"] & E_2 \end{tikzcd}$$

Definition. Let E_0 and E_1 be elliptic curves defined over a field K with identity elements O_0 resp. O_1. Then E_1 is a *twist* of E_0 if there exists a $\bar{K}$-isomorphism $\phi : E_0 \to E_1$ which sends O_0 to O_1. If E_1 is also K-isomorphic to E_0, it is called a *trivial twist*.

If E_2 is another twist of E_0 which is K-isomorphic to E_1, the twists E_1 and E_2 are called *equivalent*. The set containing equivalence classes of twists of E_0 is denoted by $\mathrm{Twist}(E_0)$.

Twists will play an important role in our considerations later. In our case we only need them for elliptic curves defined over finite fields $\mathbb{F}_q$ where q is a power of the prime p with $p > 3$. There we can refine the definition mostly to the notion of *quadratic twists*.

Let E be an elliptic curve defined over $K = \mathbb{F}_q$ with $\operatorname{char} K = p > 3$ and let E be given by a Weierstrass equation $Y^2 = X^3 + aX + b$ with $a, b \in \mathbb{F}_q$. For any $d \in \mathbb{F}_q^*$ we define the elliptic curve $E^{(d)}$ through the Weierstrass equation

$Y^2 = X^3 + d^2aX + d^3b$ and regard the map

$$\begin{aligned} \phi : E &\to E^{(d)} \\ (x,y) &\mapsto (dx, d^{3/2}y). \end{aligned}$$

One can check that this is an isomorphism, so $E^{(d)}$ is a twist of E; but if $d^{1/2}$ is not an element of $\mathbb{F}_q$, the map ϕ is not defined over $\mathbb{F}_q$ but over the field extension $\mathbb{F}_q(d^{1/2})$. The other direction is also true, so we have

$$E \text{ and } E^{(d)} \text{ are not isomorphic over } \mathbb{F}_q \quad \Longleftrightarrow \quad \left(\frac{d}{q}\right) = -1.$$

Such an elliptic curve $E^{(d)}$ is called a *non-trivial quadratic twist of* E. We even have that $E^{(d_0)}$ and $E^{(d_1)}$ are isomorphic over $\mathbb{F}_q$ for two elements $d_0, d_1 \in \mathbb{F}_q^*$ which are not squares in $\mathbb{F}_q$, so there is exactly one equivalence class of non-trivial quadratic twists of E.

It can be shown that for $j(E) \notin \{0, 1728\}$ there are no other equivalence classes than the one of E itself and the one of the quadratic twists. For $j(E) = 1728$ or $j(E) = 0$ we have to add quartic resp. cubic twists in a similar manner, see Proposition X.5.4 of Silverman [75].

We obtain that if E is an elliptic curve defined over $\mathbb{F}_q$ with characteristic $p > 3$, we have

$$\#\,\mathrm{Twist}(E) = \begin{cases} 2 & \text{if } j(E) \notin \{0, 1728\}, \\ 4 & \text{if } j(E) = 1728, \\ 6 & \text{if } j(E) = 0. \end{cases}$$

We need this later to determine the $\mathbb{F}_p$-isomorphism classes of supersingular elliptic curves which are defined over $\mathbb{F}_p$, see Section 4.2.2 of this thesis.

When we regard elliptic curves over a given field K, the question arises whether we can determine if they are isogenous or not. We have seen in general from Theorem 2.7 that for $K = \mathbb{F}_q$ this property relies on the number of $\mathbb{F}_q$-rational points of the elliptic curves. It can also be determined with the characteristic polynomial of their Frobenius as well as their trace. We will briefly introduce the notation in the elliptic curve situation now.

PROPOSITION 2.11. *Let E be an elliptic curve defined over the field K and let $\phi \in \operatorname{End}_K E$ be a non-constant isogeny with $\deg \phi = d$. Then there exists some $t_\phi \in \mathbb{Z}$ with*

$$\phi^2 - [t_\phi] \circ \phi + [d] \quad = \quad [0].$$

This can be seen in THEOREM 9.9.3 of GALBRAITH [28]. The integer t_ϕ is the *trace of ϕ* and the polynomial $X^2 - t_\phi X + d \in \mathbb{Z}[X]$ the *characteristic polynomial of ϕ* as in the general version before.

We are mostly interested in the case where E is an elliptic curve defined over a finite field $\mathbb{F}_q$ and regard the FROBENIUS $\pi_q \in \operatorname{End}_{\mathbb{F}_q} E$. From now on $t := t_E$ will always denote the integer from the equation

$$\pi_q^2 - [t_E]\pi_q + [q] \quad = \quad 0$$

which is the *trace of* FROBENIUS and will appear often in our work. It can be shown that

$$t_E \quad = \quad q + 1 - \#E(\mathbb{F}_q)$$

and thus we can also talk about the *trace of the elliptic curve E*, which justifies the notation. A theorem from HASSE (for example proven in THEOREM V.1.1 of SILVERMAN [75]) says that we always have

$$|t_E| \leq 2\sqrt{q}.$$

Thus we have the following possibility for the cardinality of $E(\mathbb{F}_q)$.

PROPOSITION 2.12. *Let p be a prime and E be an elliptic curve defined over the finite field $\mathbb{F}_q$ of characteristic p. Then the number of $\mathbb{F}_q$-rational points of such an elliptic curve E is restricted through*

$$q + 1 - 2\sqrt{q} \quad \leq \quad \#E(\mathbb{F}_q) \quad \leq \quad q + 1 + 2\sqrt{q}.$$

In fact there are polynomial point-counting algorithms to explicitly determine this number like SCHOOF'S algorithm or an improvement of it called SEA algorithm by SCHOOF, ELKIES and ATKIN, both treated for example in SCHOOF [73].

Isogenies usually have non-trivial kernels, so they are not bijective. But it turns out that there is a way to return to the original curve via another isogeny which is related to the first. Namely for every non-constant isogeny $\phi : E_0 \to E_1$ there exists an unique isogeny $\widehat{\phi} : E_1 \to E_0$ with $\deg \widehat{\phi} = \deg \phi = m$ as well as $\widehat{\phi} \circ \phi = [m]_{E_0}$ and $\phi \circ \widehat{\phi} = [m]_{E_1}$. Further we define $\widehat{[0]} := [0]$. The isogeny $\widehat{\phi}$ is called the *dual isogeny of* ϕ and has some further nice computational properties (Theorem III.6.2 of Silverman [75]) like

- $\widehat{\psi \circ \phi} = \widehat{\phi} \circ \widehat{\psi}$ for isogenies $\phi : E_0 \to E_1$, $\psi : E_1 \to E_2$,
- $\widehat{\psi + \phi} = \widehat{\psi} + \widehat{\phi}$ for isogenies $\phi, \psi : E_0 \to E_1$,
- $\widehat{\widehat{\phi}} = \phi$ for every isogeny $\phi : E_0 \to E_1$.

Furthermore, $\widehat{\phi}$ has the same trace t_ϕ as ϕ and a short computation shows that we get $[t_\phi] = \phi + \widehat{\phi}$.

Remark. For an abelian variety A of dimension $g > 1$ the concept of dual isogenies cannot be applied completely analogous. It is true that for an isogeny $\phi : A_0 \to A_1$ of abelian varieties there exists an isogeny $\psi : A_1 \to A_0$ of the same degree d such that we have $\psi \circ \phi = [d]_{A_0}$ and $\phi \circ \psi = [d]_{A_1}$ ([34], Proposition 5.12). An example of this situation we have already seen with the Frobenius morphism and the Verschiebung. However, this isogeny ψ is usually not called dual isogeny to ϕ.

For the concept of what is generally understood as *dual isogeny* we need to introduce the *dual variety* $A^\vee$ as in Section 8 and 9 of Milne [59] which is also defined over K and has the same dimension but is usually different from A. An abelian variety A and its dual satisfy $A^{\vee\vee} \cong A$. Further A and $A^\vee$ are isogenous as seen in 16.2 of Oort [65] and an isogeny $\psi : A \to A^\vee$ is called *polarization*. If such an isogeny ψ is an isomorphism, we speak of a *principal polarization* and if such an isogeny exists, A is *principally polarized*. For example Jacobians of dimension two are always principally polarized.

The dual of an isogeny $\phi : A_0 \to A_1$ between abelian varieties A_0 and A_1 of dimension $g > 1$ can be seen as the morphism $\phi^\vee : A_1^\vee \to A_0^\vee$. Especially, for A as above and an isogeny $\phi \in \operatorname{End} A$ we get $\phi^\vee \in \operatorname{End} A^\vee$. For the case of an elliptic curve E we have the relation $E = E^\vee$ and there exists a $\psi : E \to E^\vee$ as a principal polarization. In this case both here described concepts coincide. That means that for elliptic curves the dual of the Frobenius morphism π_q equals the Verschiebung ρ_q which is not the case for arbitrary abelian varieties.

The concept of the dual isogeny on elliptic curves yields the symmetry of an equivalence relation given by

$$E_0 \sim E_1 \iff \exists \text{ isogeny } \phi : E_0 \to E_1.$$

The equivalence classes under this relation are called *isogeny classes.* The following theorem summarizes the fundamental result of TATE [86] for the elliptic curve situation as we will use it later and classifies the isogeny classes for the set of elliptic curves defined over a finite field $\mathbb{F}_q$.

THEOREM 2.13 (TATE'S ISOGENY THEOREM FOR ELLIPTIC CURVES). *Let E_0 and E_1 be elliptic curves defined over the finite field $\mathbb{F}_q$. Then we have*

$$\begin{aligned} E_0 \text{ and } E_1 \text{ are isogenous} \quad &\Longleftrightarrow \quad \#E_0(\mathbb{F}_q) = \#E_1(\mathbb{F}_q) \\ &\Longleftrightarrow \quad t_{E_0} = t_{E_1}. \end{aligned}$$

Due to the mentioned polynomial-time point counting algorithms it is now easy to determine whether two given elliptic curves are isogenous or not. Even determining for a fixed isogeny degree ℓ which elliptic curves are ℓ-isogenous to a given elliptic curve E can be done in a simple way as we see next.

PROPOSITION 2.14. *Let ℓ be an integer coprime to the characteristic of the field K in the case where the latter is nonzero. There exists a polynomial $\Phi_\ell \in \mathbb{Z}[X, Y]$ such that for elliptic curves E_0 and E_1 defined over K we have*

$$E_0 \text{ and } E_1 \text{ are } \ell\text{-isogenous} \quad \Longleftrightarrow \quad \Phi_\ell(j(E_0), j(E_1)) = 0.$$

REMARK.
- ✦ Although the statement is usually first formulated for K being a number field, it is also true for elliptic curves defined over a finite field $\mathbb{F}_q$ and the reduction of the polynomial in $\mathbb{F}_q[X, Y]$.
- ✦ The polynomial Φ_ℓ is called the *ℓ-modular polynomial* or *ℓ-th classical modular polynomial.*
- ✦ We will investigate the background of this polynomial in SECTION 3.2.1 and give a description of it.

Although we know how to determine whether two elliptic curves are isogenous and how to find ℓ-isogenous elliptic curves now, explicitly calculating such an isogeny turns out to be much more complicated and entails interesting applications in cryptography. Therefore we are going to deal with computational approaches to several variants of the following problem in the course of this work.

PROBLEM 3 (General Elliptic Isogeny Problem). *Given elliptic curves E_0, E_1 over $\mathbb{F}_q$ with $\#E_0(\mathbb{F}_q) = \#E_1(\mathbb{F}_q)$, explicitly compute an isogeny between them in terms of a rational map.*

Even when we look for separable isogenies only, it is not immediately clear how to proceed. We have to provide an explicit form of an isogeny $\phi : E_0 \to E_1$ in terms of a rational map to solve this problem.

One method to construct isogenies relies heavily on subgroups of a given order of the elliptic curve E_0 which become kernels of isogenies. Its correctness comes from the next statement as in Proposition 4.12 of Silverman [75].

Proposition 2.15. *Let E be an elliptic curve defined over a field K and let $G \subseteq E(\bar{K})$ be a finite subgroup. Then there exist a unique elliptic curve E_G and a separable isogeny $\phi_G : E \to E_G$ with $\ker \phi_G = G$.*

In particular this means that the sequence

$$0 \longrightarrow G \longrightarrow E \longrightarrow E_G \longrightarrow 0$$

is exact. According to this proposition isogenies are for the most part determined by their kernels. If G is defined over K – that means, it is a Galois invariant subgroup and thus we have the relation $\sigma(G) = G$ for all $\sigma \in \mathrm{Gal}(\bar{K}/K)$ – the elliptic curve E_G and the isogeny ϕ_G can be defined over K, too.

Recall that an isogeny is a rational map and we explained before what it means for a rational map to be defined over a given field. There are the explicit *formulae of* Vélu [90] which show how to compute such an isogeny and image curve in the following way.

Let E be an elliptic curve defined over a field K given by a Weierstrass polynomial $Y^2 - X^3 - aX - b$ with $a, b \in K$. For a point $P \neq \mathcal{O}$ from G we write $P = (x_P, y_P)$. The isogeny $\phi_G = (f_1, f_2)$ starting at E with

$$\begin{aligned} f_1(x,y) &= x + \sum_{\mathcal{O} \neq P \in G} \left(\frac{3x_P^2 + a}{x - x_P} + \frac{2y_P^2}{(x - x_P)^2} \right), \\ f_2(x,y) &= y - y \sum_{\mathcal{O} \neq P \in G} \left(\frac{3x_P^2 + a}{(x - x_P)^2} + \frac{4y_P^2}{(x - x_P)^3} \right) \end{aligned}$$

for all $(x, y) \in E(\bar{K})$ satisfies $\ker \phi_G = G$ as can be explicitly checked.

The image curve $\widetilde{E} := E_G$ of the isogeny will be defined by the Weierstrass polynomial $Y^2 - X^3 - \widetilde{a}X - \widetilde{b}$ where the values for $\widetilde{a}$ and $\widetilde{b}$ can be computed as

$$\begin{aligned} \widetilde{a} &= a - 5 \sum_{\mathcal{O} \neq P \in G} (3x_P^2 + a), \\ \widetilde{b} &= b - 7 \sum_{\mathcal{O} \neq P \in G} (5x_P^2 + 3ax_P + 2b). \end{aligned}$$

Example 2.16. *Let E be an elliptic curve defined over the finite field $K := \mathbb{F}_q$ of characteristic $p > 3$ which is given by a* Weierstrass *polynomial $Y^2 - f(X)$ with $f := X^3 + aX + b \in K[X]$. We want to show how to explicitly compute all outgoing 2-isogenies from E.*

Let $f \in K[X]$ have the three distinct roots $\alpha_0, \alpha_1, \alpha_2 \in \bar{K}$, so we get the points $P_i := (\alpha_i, 0) \in E(\bar{K})$ which we call Weierstrass points. *These are the only possible points of order two of E and thus the subgroups with exactly two elements are $\{P_i, \mathcal{O}\}$.*

Each of those subgroups defines the kernel of an 2-isogeny $\phi_i : E \to E_i$ with

$$\phi_i(x, y) \quad = \quad \left(x + \frac{3\alpha_i^2 + a}{x - \alpha_i}, y - y\frac{3\alpha_i^2 + a}{(x - \alpha_i)^2} \right)$$

where the image curve E_i is given by the Weierstrass *polynomial $Y^2 - X^3 - a_iX - b_i$ with $a_i := -4a - 15\alpha_i^2$ and $b_i := -13b - 35\alpha_i^2 - 21a\alpha_i$.*

We get all possible isogenies of degree two with this approach and the occurring equations are obviously easy to compute.

In Vélu [90] the formulae are slightly more complicated as they are stated not only for short Weierstrass polynomials, but the principle is the same. Although computing 2-isogenies like in the last example is fast, evaluating the equations gets harder with increasing degree of the isogeny since there are proportionally more terms in the sum. We get the following result, following Section 25.1.1 of Galbraith [28].

Proposition 2.17. *Let E be an elliptic curve defined over a field K and let $G \subseteq E(\bar{K})$ be a finite subgroup of order ℓ. Computing the elliptic curve E_G and the isogeny ϕ_G has expected $\widetilde{\mathcal{O}}(\ell)$ running time in field operations and needs expected $\mathcal{O}(\ell)$ storage in terms of field elements.*

This complexity does not include finding the appropriate subgroups which is another task and has to be considered independently. Furthermore, if we consider our general elliptic isogeny problem as stated above, we usually do not know the kernel of an isogeny $\phi : E_0 \to E_1$ at all. Elkies [22] presents a way to obtain it from the knowledge of the j-invariants of E_0 and E_1 using $\mathcal{O}(\ell^2)$ K-operations (see Section 25.2.1 of Galbraith [28]). This approach as well as an idea of Stark [81] are presented and analyzed in Bostan, Morain, Salvy, Schost [3] where also some fast alternatives for the Vélu formulae in certain situations are given.

Those methods do not apply well in small characteristic, where other algorithms have been invented as in Couveignes [15] or especially for characteristic two in Lercier [50].

There are other, even subexponential approaches for computing isogenies of large degree (Jao and Soukharev [44]) or on a quantum computer (Childs, Jao, Soukharev [11]).

The complexity of all those approaches depends heavily on the degree of the attained isogeny. However, since this number can be potentially large and, in particular, is not predictable when only the arbitrary isogenous elliptic curves E_0 and E_1 are given, this is seems to be a badly chosen measurement. Therefore in Section 4 we want to concentrate on algorithms which do not rely on the size of the kernel of the isogeny but only on the number of elements of the underlying field $\mathbb{F}_q$.

Note that the isogeny ϕ_G from the previous propositions is only determined up to *equivalence* in the following sense.

Definition. Let E_0 and E_1 be elliptic curves defined over a field K. Isogenies $\phi, \psi : E_0 \to E_1$ are called *equivalent* if they fulfill $\ker \phi = \ker \psi$.

Remark. Let E_0, E_1 be elliptic curves over a field K and $\phi : E_0 \to E_1$ be a separable isogeny.

- Obviously, ϕ and $-\phi$ are always equivalent.
- The isogeny $\lambda_1 \circ \phi$ is equivalent to ϕ for every $\lambda_1 \in \mathrm{Aut}(E_1)$ but the isogeny $\phi \circ \lambda_0$ does not have to be equivalent to ϕ for all $\lambda_0 \in \mathrm{Aut}(E_0)$ (see Exercise 25.1.1 of Galbraith [28]). This can only happen when we have $j(E_0) \in \{0, 1728\}$, though.

We have seen before that for $\mathrm{char}\, K > 3$ and $j(E_0) \notin \{0, 1728\}$ we always have exactly two automorphisms of E_0, so $\mathrm{Aut}(E_0) = \{\pm \mathrm{id}\}$. If we have $j(E_0) = 0$ or $j(E_0) = 1728$, there are additional automorphisms which can provide isogenies $\psi : E_0 \to E_1$ which are not equivalent to ϕ. Nevertheless, up to equivalence they can have the same dual as ϕ, since for an isogeny $\psi := \phi \circ \lambda_0 : E_0 \to E_1$ with $\lambda_0 \in \mathrm{Aut}(E_0)$ we have $\widehat{\psi} = \widehat{\lambda}_0 \circ \widehat{\phi}$ which – due to the second point of the previous remark – is usually equivalent to $\widehat{\phi}$ (except possibly in the case $j(E_1) \in \{0, 1728\}$).

Hence for j-invariants 0 and 1728 there can be several non-equivalent outgoing isogenies which have the same dual. We will see that this is a small inconvenience for isogeny graphs since we are not completely able to describe the graphs as undirected and apply theory of undirected graphs on them.

Let E_0 and E_1 be elliptic curves defined over K. We are interested in the question when an isogeny ϕ between them is also defined over K. If an isogeny ϕ is defined over K, this implies that the kernel of ϕ is Galois invariant (Exercise 9.6.5 of Galbraith [28]). Due to the discussion after Proposition 2.15 there is even the useful equivalence that K-rational ℓ-isogenies correspond to GALOIS invariant subgroups of order ℓ of elliptic curves as fixated in the next lemma.

LEMMA 2.18. *Let E_0 and E_1 be elliptic curves defined over K and $\phi : E_0 \to E_1$ be an isogeny of degree ℓ. ϕ is defined over K if and only if $\ker\phi$ is a GALOIS invariant subgroup of $E(\bar{K})$ with $\#\ker\phi = \ell$.*

For elliptic curves defined over the finite field $\mathbb{F}_q$ of characteristic p there is a simpler way to test whether an isogeny between them is also defined over $\mathbb{F}_q$. This is closely linked to the q-th FROBENIUS endomorphism $\pi_{q,i} \in \operatorname{End} E_i$ which for $i \in \{0, 1\}$ maps a point $P = (x, y) \in E_i(\bar{\mathbb{F}}_q)$ to the point (x^q, y^q).

Note that there is also the well-known FROBENIUS element in $\operatorname{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ which we also denote with π_q here. For $z \in \bar{\mathbb{F}}_q$ we have $\pi_q(z) = z^q$ and obviously π_q acts trivial on $\mathbb{F}_q$. This GALOIS automorphism induces the other version of the FROBENIUS on elliptic curves and for $P = (x, y) \in E_i$ we have

$$\pi_{q,i}(P) = (x^q, y^q) = P^{\pi_q} \in E_i^{(q)}.$$

This is used in the following result.

LEMMA 2.19. *Let E_0 and E_1 be elliptic curves defined over $\mathbb{F}_q$ and $\phi : E_0 \to E_1$ be an isogeny. Then we have*

$$\begin{aligned} \phi \textit{ is defined over } \mathbb{F}_q \quad &\iff \quad \phi^{\pi_q} = \phi \\ &\iff \quad \phi \circ \pi_{q,0} = \pi_{q,1} \circ \phi. \end{aligned}$$

PROOF. Let $\phi : E_0 \to E_1$ be an isogeny between elliptic curves defined over $\mathbb{F}_q$. We regard the description $\phi = (f_1, f_2)$ with functions $f_1, f_2 \in \bar{K}(E_0)$ and let $\mathbb{F}_{q^m}$ be an extension field of $K = \mathbb{F}_q$ where all coefficients of the polynomials from $K[E_0]$ defining the f_i live. Especially this field extension is finite.

Thus we deduce that ϕ is already defined over $\mathbb{F}_q$ if and only if we have $\phi^\sigma = \phi$ for all $\sigma \in \operatorname{Gal}(\mathbb{F}_{q^s}/\mathbb{F}_q)$ instead of $\operatorname{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$. Since this GALOIS group is generated by π_q, it is enough to check the equality of ϕ^{π_q} and ϕ. This proves the first equivalence.

In general, the equality $\phi^\sigma(P^\sigma) = (\phi(P))^\sigma$ is true for an isogeny $\phi : E_0 \to E_1$ and all $\sigma \in \operatorname{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ (SILVERMAN [75], CHAPTER I.3 on page 11). Hence we get for $P \in E_0$

$$\phi^{\pi_q}(\pi_{q,0}(P)) \;=\; \phi^{\pi_q}(P^{\pi_q}) \;=\; (\phi(P))^{\pi_q} \;=\; \pi_{q,1}(\phi(P))$$

and thus $\phi^{\pi_q} \circ \pi_{q,0} = \pi_{q,1} \circ \phi$. Thus we see immediately that the condition $\phi = \phi^{\pi_q}$ is equivalent to the wanted result $\phi \circ \pi_{q,0} = \pi_{q,1} \circ \phi$. □

Although the formulae of VÉLU give us a way to compute an isogeny between two elliptic curves over a field K, it turns out that they are harder to compute with more elements in the subgroup; thus the next observation which comes from THEOREM 25.1.2 of GALBRAITH [28] is crucial for computational performance.

PROPOSITION 2.20. *Let E_0 and E_1 be elliptic curves defined over a field K and $\phi : E_0 \to E_1$ be a separable isogeny. Then there exist separable isogenies $\phi_1, \cdots, \phi_n$ of prime degree between suitable elliptic curves such that*

$$\phi = \phi_n \circ \cdots \circ \phi_1 \circ [m]$$

where m is the largest integer such that $E[m] \subseteq \ker \phi$.

REMARK.

- ✦ If ϕ is defined over K, the ϕ_i can be defined over K, too.
- ✦ When ϕ is not guarantied to be separable, we have to add a FROBENIUS morphism like in LEMMA 2.2.

The degree of the isogeny ϕ in PROPOSITION 2.20 is the product of the degrees of the other isogenies. Hence, computing an isogeny with potentially large degree between two elliptic curves boils down to constructing a chain of isogenies with smaller and prime degree which are hopefully faster to compute. Still, the question remains how to find such a chain. We will deal with algorithms for that problem in SECTION 4.

Although we will see that for small degrees the formulae of VÉLU [90] give us a reasonable construction of an isogeny, they need the kernel of the resulting isogeny as input which usually is not known. When we have a starting elliptic curve E_0 defined over a field K and a prime ℓ different from $\operatorname{char} K$, we can compute the j-invariants of all image curves of ℓ-isogenies with the modular polynomial from PROPOSITION 2.14.

There are several ways to determine the subgroup which is the kernel of an unknown isogeny $\phi : E_0 \to E_1$ when only the j-invariants of E_0 resp. E_1 are given, see CHAPTER 25.2 of GALBRAITH [28] for a discussion. The algorithms are quite technical, so we refrain from a detailed description and concentrate on the following problem instead.

PROBLEM 4 (Isogeny Chain Problem). *Given elliptic curves E_0, E_1 over $\mathbb{F}_q$ with $\#E_0(\mathbb{F}_q) = \#E_1(\mathbb{F}_q)$, compute a chain of isogenies with small prime degrees between them.*

Such a chain of isogenies corresponds to a path in a certain isogeny graph as we will see later. In the case of ordinary elliptic curves defined over finite fields those graphs have a nice structure like a „volcano“. There are good-enough algorithms which are able to find a path between two arbitrary nodes in a component of one of them.

However, these methods cannot be applied on supersingular elliptic curves due to a different graph structure. In the course of this thesis we will investigate the alternatives for computing a chain of isogenies in the supersingular case. For the case where the elliptic curves in question are defined over the base field $\mathbb{F}_p$ we will provide an algorithm for this problem which is faster than the ones known before.

2.1.2 Supersingular Elliptic Curves

As we have seen, the multiplication-by-m-isogenies on an abelian variety A are strongly related to the m-torsion of A. For elliptic curves the structure of certain torsion subgroups turns out to have a big influence on the behavior of the elliptic curves themselves. The possible form of any m-torsion subgroup can be determined as in Lemma 2.4. Simplified to the case of elliptic curves it can be stated as in the following result which can also be found in Silverman [75, Theorem III.6.4].

Lemma 2.21. *Let E be an elliptic curve over a field K and $m \in \mathbb{N}$.*

1. *If* $\operatorname{char} K = 0$ *or* $\operatorname{char} K = p > 0$ *and $p \nmid m$, then*

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

2. *If* $\operatorname{char} K = p > 0$ *and m be a power of p, then*

$$E[m] = \{\mathcal{O}\} \quad \text{or} \quad E[m] \cong \mathbb{Z}/m\mathbb{Z}.$$

Both times the isomorphism means group isomorphism.

The second part of this proposition leads to the important differentiation between *ordinary* and *supersingular* elliptic curves. Note that this works only for elliptic curves defined over fields of positive characteristic.

Definition. Let E be an elliptic curve over a field K with $\operatorname{char} K = p > 0$. If E has no non-trivial p-torsion, so $E[p] = \{\mathcal{O}\}$, it is called *supersingular* and otherwise *ordinary*.

In particular this means that the multiplication-by-p-map has trivial kernel on supersingular elliptic curves in characteristic p and we have already seen that it is inseparable. There are several other ways of defining these terms through equivalent properties, some of them are needed in this work and listed below. The equivalences are shown in SILVERMAN [75, Theorem V.3.1].

THEOREM 2.22. *Let E be an elliptic curve defined over a finite field K with $\operatorname{char} K = p > 0$ and for $1 \leq r \in \mathbb{Z}$ let $\pi_{p^r} : E \to E^{(p^r)}$ denote the p^r-FROBENIUS morphism. The following concepts are equivalent.*

1. *$E[p^r] = \{\mathcal{O}\}$ for all $r \geq 1$,*
2. *$\widehat{\pi_{p^r}}$ is purely inseparable for all $r \geq 1$,*
3. *$[p] : E \to E$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$,*
4. *$\operatorname{End} E$ is an order in a quaternion algebra.*

For curves of higher genus and arbitrary abelian varieties the definition of supersingularity is based on the concept of elliptic curves being supersingular.

DEFINITION. Let A be an abelian variety of dimension g defined over $\mathbb{F}_q$. A is called *supersingular* if there exists a supersingular elliptic curve E defined over $\bar{\mathbb{F}}_q$ such that A is isogenous to $\underbrace{E \times \cdots \times E}_{g\text{-times}}$ over $\bar{\mathbb{F}}_q$.

Let C be an algebraic curve defined over $\mathbb{F}_q$. Then C is called *supersingular* when its JACOBIAN variety $\operatorname{Jac} C$ is supersingular.

As mentioned before, there is a connection between the supersingularity of an abelian variety A and its p-rank since from this definition we can immediately deduce that a supersingular abelian variety of dimension g defined over the finite field $\mathbb{F}_q$ of characteristic p has p-rank zero. For $g = 2$ this is even an equivalence as seen in EXERCISE 10.8.6 of GALBRAITH [28].

LEMMA 2.23. *Let A be an abelian variety of dimension $g = 2$ defined over the finite field $\mathbb{F}_q$ of characteristic p. Then we have*

$$A \text{ is supersingular} \iff r_p(A) = 0.$$

Matching to the elliptic case an abelian variety A of dimension g defined over the finite field $\mathbb{F}_q$ of characteristic p is called *ordinary* if it has p-rank $r(A) = g$.

In the remainder of this section we will deal with the genus one case. There are several nice properties of supersingular elliptic curves E defined over a finite field $\mathbb{F}_q$ of characteristic p. For example the restriction to j-invariants to maximal $\mathbb{F}_{p^2}$ from THEOREM 2.22.3 is quite helpful for handling supersingular elliptic curves in applications. Another one of them is an implication concerning the number of $\mathbb{F}_q$-rational points of E.

PROPOSITION 2.24. *Let E be an elliptic curve defined over the finite field $\mathbb{F}_q$ with $\operatorname{char} K = p > 0$ and let $t := t_E = q + 1 - \#E(\mathbb{F}_q) \in \mathbb{Z}$ be the trace of E as defined before. Then we have*

$$\begin{aligned} E \textit{ is supersingular} &\iff t \equiv 0 \pmod p \\ &\iff \#E(\mathbb{F}_q) \equiv 1 \pmod p. \end{aligned}$$

PROOF. First we observe that since the isogeny $[1] - \pi_q \in \operatorname{End} E$ is separable due to COROLLARY 2.9, we have

$$\begin{aligned} \#E(\mathbb{F}_q) &= \#\{P \in E \mid \pi_q(P) = P\} \\ &= \#\ker([1] - \pi_q) \\ &= \deg([1] - \pi_q). \end{aligned}$$

Therefore we can write $t = \deg \pi_q + 1 - \deg([1] - \pi_q)$ and after a short computation we obtain

$$[t] \quad = \quad \pi_q + \widehat{\pi}_q.$$

Because the FROBENIUS π_q is always purely inseparable and the set of inseparable endomorphisms on an elliptic curve form an ideal in the endomorphism ring (SILVERMAN [75], Corollary III.5.6), we obtain that $[t]$ is inseparable if and only if the so-called *Verschiebung* $\widehat{\pi}_q$ is inseparable. Using COROLLARY 2.9 again, we furthermore see that the inseparability of $[t]$ is equivalent to p dividing t.

So we achieve

$$\begin{aligned} E \text{ is supersingular} &\iff \widehat{\pi}_q \text{ is purely inseparable} \\ &\iff [t] = \pi_q + \widehat{\pi}_q \text{ is purely inseparable} \\ &\iff t \equiv 0 \pmod p. \end{aligned}$$

The second equivalence of the proposition is an obvious conclusion but often the more useful phrasing for applications. □

For most primes p this proposition can immediately be simplified to the case $q = p$ where we even get an equality.

Corollary 2.25. *If in the situation above we have $K = \mathbb{F}_p$ for $p > 3$, we get*

$$\begin{aligned} E \textit{ is supersingular} &\iff t = 0 \\ &\iff \#E(\mathbb{F}_p) = p + 1. \end{aligned}$$

Proof. The Hasse bound and the condition on p tell us that $|t| \leq 2\sqrt{p} < p$ has to hold, so $t = 0$ is the only possibility for $t \equiv 0 \pmod p$ to be true. □

The cases $p = 2$ and $p = 3$ are excluded in Corollary 2.25 not only because this kind of proof does not work here but because the statement does not hold for them. For example there are supersingular elliptic curves over $\mathbb{F}_2$ or $\mathbb{F}_3$ with only one $\mathbb{F}_2$-rational resp. $\mathbb{F}_3$-rational point as can be seen in tables in the proof of the next Lemma.

Lemma 2.26. *Let E be an elliptic curve over a field K with $\operatorname{char} K = p > 0$.*

1. *Case $p = 2$:*

$$\begin{aligned} E \textit{ is supersingular} &\iff j(E) = 0 \\ &\iff E \cong \mathcal{V}(Y^2 + Y - X^3). \end{aligned}$$

2. *Case $p = 3$:*

$$\begin{aligned} E \textit{ is supersingular} &\iff j(E) = 1728 \\ &\iff E \cong \mathcal{V}(Y^2 - X^3 - X). \end{aligned}$$

Proof. It is easy to compute a complete list of all elliptic curves over $\mathbb{F}_2$ resp. $\mathbb{F}_3$ as seen in Tables 1 and 2. Then we can determine the supersingular ones in it using Proposition 2.24 and checking for which curves the number of $\mathbb{F}_p$-rational points is 1 modulo p. We see that they all have the requested j-invariants 0 resp. 1728 (which is also 0 in $\mathbb{F}_3$). The second equivalence in each case of course means isomorphism over $\bar{\mathbb{F}}_p$ where the j-invariant classifies the isomorphism class.

Weierstrass Polynomial of E (with $a, b \in \mathbb{F}_2$)	$\#E(\mathbb{F}_2)$	$j(E)$
$Y^2 + Y \quad - \quad X^3 - aX^2 - (a+1)X - 1$	1	0
$Y^2 + Y \quad - \quad X^3 - a(X^2 + X) - b$	3	0
$Y^2 + Y \quad - \quad X^3 - aX^2 - (a+1)X$	5	0
$Y^2 + XY + Y \quad - \quad X^3 - aX^2 - bX - ab - 1$	2	1
$Y^2 + XY + aY \quad - \quad X^3 - aX^2 - bX - (a+1)(b+1)$	4	1

Table 1: $\mathbb{F}_2$-Isomorphism Classes of Elliptic Curves over $\mathbb{F}_2$

WEIERSTRASS Polynomial of E (with $a \in \mathbb{F}_3$)	$\#E(\mathbb{F}_3)$	$j(E)$
$Y^2 - X^3 - 2X - 2$	1	0
$Y^2 - X^3 - X - a$	4	0
$Y^2 - X^3 - 2X$	4	0
$Y^2 - X^3 - 2X - 1$	7	0
$Y^2 - X^3 - X^2 - aX - (a+1)^2 - 1$	3	1
$Y^2 - X^3 - 2X^2 - aX - 2(a+1)^2 - 2$	5	1
$Y^2 - X^3 - 2X^2 - aX - 2(a+1)^2$	2	2
$Y^2 - X^3 - X^2 - aX - (a+1)^2$	6	2

TABLE 2: $\mathbb{F}_3$-Isomorphism Classes of Elliptic Curves over $\mathbb{F}_3$

In these tables we can see again that the statement of COROLLARY 2.25 would be wrong for $p = 2$ and $p = 3$ since there are supersingular elliptic curves E with $\#E(\mathbb{F}_p) \neq p + 1$. □

Therefore the situation is particularly simple in these situations and thus we restrict to $p > 3$ in most of the following parts.

APPLICATION OF THE MODULAR POLYNOMIAL. Let E_0 and E_1 be supersingular elliptic curves defined over a finite field $\mathbb{F}_q$ of characteristic p. Recall from PROPOSITION 2.14 that the ℓ^{th} *modular polynomial* $\Phi_\ell \in \mathbb{F}_q[X, Y]$ has the property

$$E_0 \text{ and } E_1 \text{ are } \ell\text{-isogenous} \iff \Phi_\ell\big(j(E_0), j(E_1)\big) = 0.$$

Since we know from THEOREM 2.22 that in characteristic p all j-invariants of supersingular elliptic curves lie in $\mathbb{F}_{p^2}$, we get the following result.

THEOREM 2.27. *Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$ with characteristic p and $\Phi_\ell \in \mathbb{F}_q[X, Y]$ the ℓ^{th} modular polynomial. Then we have*

$$E \text{ is supersingular} \iff \begin{array}{l}\Phi_\ell\big(j(E), Y\big) \in \bar{\mathbb{F}}_q[Y] \text{ splits completely} \\ \text{over } \mathbb{F}_{p^2} \text{ for every } \ell \neq p.\end{array}$$

PROOF. The proof of this needs theory about isogeny volcanoes and can be found in SUTHERLAND [84]. □

We have already seen that elliptic curves with j-invariants 0 and 1728 often have slightly different properties from the other ones, so it is helpful to know whether such curves are supersingular or not. The following theorem provides a tool which can subsequently be used for that purpose as seen in COROLLARY 2.29.

Theorem 2.28. *Let E be an elliptic curve over $K := \mathbb{F}_q$ with $\operatorname{char} K = p > 2$ and $f \in K[X]$ be a cubic polynomial such that E is defined through the polynomial $Y^2 - f(X)$ in Weierstrass form. Further set $m := \frac{p-1}{2}$ and let c_{p-1} be the coefficient of X^{p-1} in $f(X)^m$. Then we get*

$$E \text{ is supersingular} \quad \Longleftrightarrow \quad c_{p-1} = 0.$$

Proof. We present a short sketch of proof as in Theorem V.4.1.(a) of Silverman [75] and neglect the technical details here.

- ✦ Show $\#E(\mathbb{F}_q) = 1 - c_{q-1}$ in $\mathbb{F}_q$ where c_{q-1} is the coefficient of X^{q-1} in $f(X)^{m'}$ with $m' = \frac{q-1}{2}$.
- ✦ Show $c_{q-1} = t$ in $\mathbb{F}_q$ where $[t] = \pi_q + \widehat{\pi}_q$, so $\widehat{\pi}_q = [t] + [-1]\pi_q$.
- ✦ With Corollary 2.9 we get the equivalence $(\star)$ in

$$\begin{aligned} c_{q-1} = 0 &\overset{t\in\mathbb{Z}}{\Longleftrightarrow} t \equiv 0 \pmod p \\ &\overset{(\star)}{\Longleftrightarrow} \widehat{\pi}_q \text{ is inseparable} \\ &\overset{\text{Def}}{\Longleftrightarrow} E \text{ is supersingular.} \end{aligned}$$

- ✦ Show $c_{p-1} = 0 \iff c_{q-1} = 0$ from $c_{p^{k+1}-1} = c_{p^k-1}c_{p-1}^{p^k}$ and induction on the positive integer k. □

The complexity of calculating the coefficient c_{p-1} from Theorem 2.28 is exponential in $\log p$ as for example explained in Section 2.1 of Sutherland [84]. But it is helpful to conclude the following statements.

Corollary 2.29. *Let E be an elliptic curve over K with $\operatorname{char} K = p \geq 5$. Then we have*

1. *in the case $j(E) = 0$, i.e. $E \cong \mathcal{V}(Y^2 - X^3 - 1)$:*

$$E \text{ is supersingular} \quad \Longleftrightarrow \quad p \equiv 2 \pmod 3.$$

2. *in the case $j(E) = 1728$, i.e. $E \cong \mathcal{V}(Y^2 - X^3 - X)$:*

$$E \text{ is supersingular} \quad \Longleftrightarrow \quad p \equiv 3 \pmod 4.$$

Note that it is easy to see that the appearing elliptic curves in this corollary have the indicated j-invariants 0 resp. 1728, so they can act as a representative of the respective isomorphism classes of elliptic curves which are given by their j-invariants.

PROOF.

1. Set $m := \frac{p-1}{2}$. For the first point we need to check with THEOREM 2.28 applied on $f := X^3+1$ if the coefficient c_{p-1} of X^{p-1} in

$$f(X)^m \;=\; (X^3+1)^m \;=\; \sum_{k=0}^{m} \tbinom{m}{k} X^{3k}$$

is zero, so – since binomial coefficients are nonzero – whether the X^{p-1}-term appears in the sum or not. We have $p > 3$, so p is either 1 or 2 modulo 3.

   - ✦ If $p \equiv 1 \pmod 3$, we see that we have $3k = p-1$ for $k := \frac{p-1}{3} \in \{0, \cdots, m\}$, so $c_{p-1} = \binom{m}{k} \not\equiv 0 \pmod p$ and the curve is not supersingular.
   - ✦ If $p \equiv 2 \pmod 3$, obviously $3k \neq p-1$ is true for all $k \in \{0, \cdots, m\}$, so $c_{p-1} = 0$ and the curve has to be supersingular.

2. Analogously we examine the coefficient c_{p-1} of X^{p-1} in

$$f(X)^m \;=\; (X^3+X)^m \;=\; \sum_{k=0}^{m} \tbinom{m}{k} X^{2k+m}.$$

   - ✦ If $p \equiv 1 \pmod 4$, it is $2k+m = p-1$ for $k := \frac{p-1}{4} \in \{0, \cdots, m\}$ so $c_{p-1} = \binom{m}{k} \not\equiv 0 \pmod p$ and the curve is ordinary.
   - ✦ If $p \equiv 3 \pmod 4$, we get $2k+m \neq p-1$ for all $k \in \{0, \cdots, m\}$ so $c_{p-1} = 0$ and the curve is supersingular. □

For an elliptic curve in LEGENDRE form as described below, the result of THEOREM 2.28 can be stated in a more directly applicable way which will help us to determine the number of supersingular elliptic curves in characteristic p. An elliptic curve defined over a field K is *in* LEGENDRE *form* if its WEIERSTRASS equation is written in the form

$$Y^2 \;-\; X(X-1)(X-\lambda)$$

with $\lambda \in \bar{K} \setminus \{0,1\}$. Such a curve is often denoted with E_λ and for characteristic $p > 2$ every elliptic curve is isomorphic to an elliptic curve in LEGENDRE form. This can be seen in PROPOSITION III.1.7 of SILVERMAN [75] along with the next related result.

Lemma 2.30. *An elliptic curve E_λ in* Legendre *form has j-invariant*

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

and the map

$$\begin{array}{rcl} \bar{K} \setminus \{0,1\} & \to & \bar{K} \\ \lambda & \mapsto & j := j(\lambda) \end{array}$$

is surjective and has six preimages for all $j \neq 0, 1728$ where it has two resp. three preimages.

Corollary 2.31. *Let E be an elliptic curve defined over $\bar{K}$ with $\operatorname{char} K = p > 2$, $m := \frac{p-1}{2}$ and $0, 1 \neq \lambda \in \bar{K}$ such that $E = E_\lambda$ is in* Legendre *form. Furthermore consider the polynomial*

$$H_p := \sum_{i=0}^{m} \binom{m}{i}^2 t^i \in \mathbb{Z}[t].$$

Then we get

$$E_\lambda \textit{ is supersingular} \iff H_p(\lambda) = 0.$$

Proof. This fact can be seen for instance in Theorem V.4.1.(b) of Silverman [75]. It is a direct conclusion from Theorem 2.28 applied on the cubic polynomial $f(X) = X(X-1)(X-\lambda)$ which apparently has distinct roots in $\bar{K}$.

Let c_{p-1} be the coefficient of X^{p-1} in $f(X)^m = X^m(X-1)^m(X-\lambda)^m$. Since $p - 1 = 2m$, this is the coefficient of X^m in

$$\begin{aligned} (X-1)^m(X-\lambda)^m &= \left(\sum_{i=1}^{m} \binom{m}{i} X^i (-1)^{m-i}\right) \cdot \left(\sum_{j=1}^{m} \binom{m}{j} X^{m-j} (-\lambda)^j\right) \\ &= \sum_{i=1}^{m} \sum_{j=1}^{m} \binom{m}{i}\binom{m}{j} X^{m+i-j} \lambda^j (-1)^{m-i+j}. \end{aligned}$$

So c_{p-1} is the sum of all coefficients of terms in this expression with $i = j$,

$$\begin{aligned} c_{p-1} &= \sum_{i=1}^{m} \binom{m}{i}^2 \lambda^i (-1)^m \\ &= (-1)^m H_p(\lambda), \end{aligned}$$

and thus we get

$$\begin{aligned} H_p(\lambda) = 0 \quad &\Longleftrightarrow \quad c_{p-1} = 0 \\ &\overset{2.28}{\Longleftrightarrow} \quad E_\lambda \text{ is supersingular} \end{aligned}$$

as we wanted to. □

Thus the set of supersingular elliptic curves E_λ corresponds to the roots λ of the polynomial H_p from the corollary. When we want to investigate the number of supersingular elliptic curves, we need to know if there can be multiple roots, but Theorem V.4.1.c) of Silverman [75] shows the following fact.

Proposition 2.32. *The polynomial H_p has m distinct roots in $\bar{K}$.*

With this result we are able to determine the number of supersingular elliptic curves in characteristic p. We call the j-invariants of supersingular elliptic curves *supersingular j-invariants.*

Theorem 2.33. *Let p be a prime and S_{p^2} be the set of all supersingular j-invariants in $\mathbb{F}_{p^2}$. Then*

$$\#S_{p^2} = \left\lfloor \frac{p}{12} \right\rfloor + \begin{cases} 0 & \text{if } p \equiv 1 \pmod{12} \\ 1 & \text{if } p \equiv 5 \pmod{12} \\ 1 & \text{if } p \equiv 7 \pmod{12} \\ 2 & \text{if } p \equiv 11 \pmod{12}. \end{cases}$$

Proof. This proof is along the lines of the one from part c) of Theorem V.4.1 of Silverman [75].

We know that every root λ of H_p yields the j-invariant of a supersingular elliptic curve through $\lambda \mapsto j(\lambda)$ as in Lemma 2.30. Further there are $m = \frac{p-1}{2}$ distinct roots of H_p according to Proposition 2.32. We have seen that if the j-invariant $j = 0$ is supersingular, there are two roots of H_p which lead to this j whereas for the case where $j = 1728$ is supersingular, there are three roots of H_p providing this j. These cases are easy to identify since we can check from Corollary 2.29 whether 0 and 1728 are supersingular or not dependent on the value of $p \pmod{12}$.

Furthermore we have seen that under this map every $j \notin \{0, 1728\}$ has six preimages, so the elliptic curves rising from those roots of H_p are isomorphic over $\bar{\mathbb{F}}_p$. When we denote the set of all roots of H_p which yield a j-invariant different from 0 or 1728 with R, there are $\frac{\#R}{6}$ different images of values from R.

Summed up there are the following results

$p \pmod{12}$	$0 \in S_{p^2}$	$1728 \in S_{p^2}$	$\#R$	$\#S_{p^2}$
1	no	no	$\frac{p-1}{2}$	$\frac{p-1}{12}$
5	yes	no	$\frac{p-1}{2} - 2 = \frac{p-5}{2}$	$\frac{p-5}{12} + 1$
7	no	yes	$\frac{p-1}{2} - 3 = \frac{p-7}{2}$	$\frac{p-7}{12} + 1$
11	yes	yes	$\frac{p-1}{2} - 2 - 3 = \frac{p-11}{2}$	$\frac{p-11}{12} + 2$

which conclude the proof. □

We have already seen that for $p \in \{2, 3\}$ there is always exactly one supersingular j-invariant in $\mathbb{F}_p$, namely $j \equiv 0 \pmod{p}$. For $p > 3$ it can be shown that this number of supersingular j-invariants is in relation to the so-called Hurwitz class number (see Cox [16], Theorem 14.18) although the proof goes beyond the scope of this work. Note that Cox talks about the actual number of supersingular elliptic curves, not just their number up to isomorphism, so there is a factor $\frac{p-1}{2}$ in his formula which vanishes when we regard $\mathbb{F}_p$-isomorphism classes. We gain another factor of $1/2$ when we regard $\bar{\mathbb{F}}_p$-isomorphism classes. Thus the number of j-invariants in $\mathbb{F}_p$ equals half the Hurwitz class number. This statement can be simplified to the following result with equations (1.8) and (1.11) from Gross [36].

Theorem 2.34. *Let $p > 3$ be a prime and let S_p be the set of all supersingular j-invariants in $\mathbb{F}_p$. Then*

$$\#S_p = \begin{cases} \frac{1}{2}h(-4p) & \text{if } p \equiv 1 \pmod{4} \\ h(-p) & \text{if } p \equiv 7 \pmod{8} \\ 2h(-p) & \text{if } p \equiv 3 \pmod{8} \end{cases}$$

where for any integer d we write $h(d)$ for the class number of the order with discriminant d.

Due to Proposition 2 of Galbraith [27] we can make the estimation

$$h(d) \quad \leq \quad \frac{1}{\pi}\sqrt{|d_{\mathcal{K}}|}\log|d_{\mathcal{K}}|$$

where $d_{\mathcal{K}}$ is the fundamental discriminant of $\mathcal{K} = \mathbb{Q}(\sqrt{d})$, and in our cases we have $d_{\mathcal{K}} \in \{-p, -4p\}$. This means that the number of supersingular j-invariants in $\mathbb{F}_p$ can be estimated with $\mathcal{O}(\sqrt{p}\log p)$. This is a lot smaller than the overall number of supersingular j-invariants in $\mathbb{F}_{p^2}$, which we have seen to be $\mathcal{O}(p)$. This consideration will turn out to be a starting point of our problem, since we will regard the graphs of those j-invariants as nodes and hope to find shorter paths in the smaller graph.

2.2 Endomorphism Rings of Abelian Varieties

In this section we want to investigate the structure of endomorphism rings of abelian varieties in general and then concentrate on the special properties of the endomorphism rings of ordinary and supersingular elliptic curves respectively. For that we deal with the full endomorphism ring as well as with the ring of endomorphisms restricted to the variety's field of definition. The concepts turn out to have a strong relation to the Frobenius morphism on the variety.

2.2.1 General Concepts

Let A be an abelian variety of dimension g defined over a finite field $K = \mathbb{F}_q$ with a prime power q. In this section we want to investigate the endomorphism ring $\operatorname{End} A$ which is a free $\mathbb{Z}$-module of rank at most $4g^2$ as stated in Proposition 2.6. Since for any $m \in \mathbb{Z}$ the multiplication-by-m-map is an element of $\operatorname{End} A$ and defined over K, we can embed $\mathbb{Z}$ into $\operatorname{End}_K A$. Further, the Frobenius π_q and the Verschiebung ρ_q are also elements of $\operatorname{End}_K A$ (see Theorem 3.5 of Waterhouse [92] or Remark 18.6 of Oort [65]), so we have

$$\mathbb{Z}[\pi_q, \rho_q] \quad \subseteq \quad \operatorname{End}_K A.$$

Let E be an elliptic curve defined over $\mathbb{F}_q$ and $t \in \mathbb{Z}$ be the trace of the Frobenius π_q. We have already seen that we get $\rho_q = \widehat{\pi}_q$ here and computed the identity $[t] = \pi_q + \widehat{\pi}_q$. Thus we obtain $\widehat{\pi}_q = [t] - \pi_q \in \mathbb{Z}[\pi_q]$ and have $\mathbb{Z}[\pi_q, \rho_q] = \mathbb{Z}[\pi_q]$ in this situation. Therefore we are able to work with the more simple subring

$$\mathbb{Z}[\pi_q] \quad \subseteq \quad \operatorname{End}_K A$$

here. For abelian varieties of dimension bigger than one, this is not true in general, so there we have the more complicated setting

$$\mathbb{Z}[\pi_q] \quad \subseteq \quad \mathbb{Z}[\pi_q, \rho_q] \quad \subseteq \quad \operatorname{End}_K A.$$

On the other hand when we take $\operatorname{End} A$ and tensor it with $\mathbb{Q}$, we get the algebra $\mathcal{A} := \operatorname{End}_K A \otimes_{\mathbb{Z}} \mathbb{Q}$. As an order in $\mathcal{A}$ we know that $\operatorname{End}_K A$ is contained in a maximal order of $\mathcal{A}$. We will investigate this algebra $\mathcal{A}$ and some important properties in this section. For that we first need to introduce some notation and background theory about quaternion algebras. We will see that the endomorphism rings play an important role for structures and even the sets of outgoing isogenies of abelian varieties. For more extensive discussions of this background theory we refer to SILVERMAN [75], SECTION 5 of KOHEL [45] or REINIER [67].

Let F be a field, $\mathcal{A}$ be a simple ring with operations $+$ and $*$ and $\varphi : F \to \mathcal{A}$ be a homomorphism of rings such that F is isomorphic to the center of $\mathcal{A}$ under φ. Then $\mathcal{A}$ can be regarded as a vector space over F with scalar multiplication $a \cdot \alpha := \varphi(a) * \alpha$ for any $a \in F$ and $\alpha \in \mathcal{A}$.

DEFINITION. When in the situation above the dimension $[\mathcal{A} : F] := \dim_F \mathcal{A}$ of this vector space is finite, $\mathcal{A}$ is a *central simple algebra over* F and a central simple algebra of dimension four over F is called *quaternion algebra over* F.

We will identify F with its image under φ and F will either be $\mathbb{Q}$ or one of its completions $\mathbb{Q}_p$ for some prime p or infinity where we set $\mathbb{Q}_\infty := \mathbb{R}$ and for p prime $\mathbb{Q}_p$ denotes the usual p-adic numbers. In this cases, R will be the notation for the ring $\mathbb{Z}$ or $\mathbb{Z}_p$, respectively. Recall that a subring $\mathcal{O}$ of $\mathcal{A}$ which is a full R-lattice is called *R-order of* $\mathcal{A}$ and satisfies $\mathcal{O} \otimes_R F = \mathcal{A}$. For convenience we will often drop the emphasis of the ring and only use the term *order* if no confusion seems possible.

A *division algebra over* F is an associative algebra $\mathcal{A}$ over F such that all elements $\alpha \in \mathcal{A}$ are invertible. For $n \in \mathbb{N}$ the *matrix algebra* $\mathbb{M}_n(F)$ is the algebra of $n \times n$ matrices with coefficients in F. Actually those two concepts are the only ones that occur for quaternion algebras.

PROPOSITION 2.35. *Let F be a field and $\mathcal{A}$ a quaternion algebra over F. Then there are the two possibilities*

- *$\mathcal{A}$ is a division algebra over F or*
- *$\mathcal{A} \cong \mathbb{M}_2(F)$.*

PROOF. From WEDDERBURN's Structure Theorem (REINIER [67], THEOREM 7.4) we know that every central simple algebra $\mathcal{A}$ is isomorphic to $\mathbb{M}_n(S)$ for some $n \in \mathbb{N}$ where S is a division ring with $F \subseteq S$, $[S : F] < \infty$ and that $[\mathcal{A} : F] = n^2[S : F]$.

In our case $\mathcal{A}$ is a quaternion algebra over F, so we have $[\mathcal{A} : F] = 4$ and the integer n must be 1 or 2.

Case $n = 1$: This implies $\mathcal{A} \cong M_1(S) \cong S$ and since S is a division ring with $F \subseteq S$, we can regard S as a F-division algebra.

Case $n = 2$: Here we get $[S : F] = 1$ and thus we have $S \cong F$, which leads to $\mathcal{A} \cong \mathbb{M}_2(F)$. □

We want to introduce *definite quaternion algebras* and for their definition we need the objects $\mathcal{A}_p := \mathcal{A} \otimes_{\mathbb{Q}} \mathbb{Q}_p$ for primes p or infinity. Those are quaternion algebras themselves as seen in REINIER [67] COROLLARY 7.8.

Proposition 2.36. *Let $\mathcal{A}$ be a quaternion algebra over $\mathbb{Q}$. Then we have that $\mathcal{A}_p$ is a quaternion algebra over $\mathbb{Q}_p$.*

This is needed for the following definition since we now know that $\mathcal{A}_p$ is either a division algebra or isomorphic to $\mathbb{M}_2(\mathbb{Q}_p)$ due to Proposition 2.35.

Definition. Let $\mathcal{A}$ be a quaternion algebra over $\mathbb{Q}$ and p be a prime or infinity. $\mathcal{A}$ is called *ramified at* p when $\mathcal{A}_p$ is a division algebra over $\mathbb{Q}_p$ and *split at* p when we have $\mathcal{A}_p \cong \mathbb{M}_2(\mathbb{Q}_p)$.

If $\mathcal{A}$ ramifies at infinity, it is called *definite quaternion algebra over* $\mathbb{Q}$, else *indefinite*.

The definite quaternion algebra over $\mathbb{Q}$ which is ramified exactly at a prime p and at infinity is denoted with D_p.

Remark.

- A *definite quaternion algebra over* $\mathbb{Q}$ is of the form

$$\mathcal{A} \;=\; \mathbb{Q} + \alpha\mathbb{Q} + \beta\mathbb{Q} + \alpha\beta\mathbb{Q}$$

  with $\alpha\beta := \alpha * \beta = -\beta * \alpha$ and $\alpha^2, \beta^2 \in \mathbb{Q}_{<0}$.

- The ring multiplication $*$ in $\mathcal{A}$ is obviously different from the commutative multiplication of α and β as elements in $\mathbb{C}$.

- $(1, \alpha, \beta, \alpha\beta)$ is a basis of $\mathcal{A}$ as $\mathbb{Q}$-vector space and we can embed $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$ into $\mathcal{A}$.

After introducing the basic concepts of quaternion algebras, we return to the endomorphism ring $\operatorname{End}_K A$ of an abelian variety A defined over a finite field K which contains the isogenies from A to itself which are defined over K. Theorem 2 of Tate [86] gives a strong statement about the algebra $\mathcal{A} = \operatorname{End}_K A \otimes_{\mathbb{Z}} \mathbb{Q}$ as seen below. Especially the following adaption on the case of an elliptic curve gives us useful facts about their structure and a connection between the characteristic polynomial of the Frobenius and the algebra containing the endomorphism ring.

Theorem 2.37. *Let A be an abelian variety of dimension g defined over the finite field $K = \mathbb{F}_q$ of characteristic $p > 0$. Then the center of $\mathcal{A}$ is $\mathbb{Q}(\pi_q)$ and we have the relation*

$$2g \;\leq\; [\mathcal{A} : \mathbb{Q}] \;\leq\; (2g)^2.$$

The extreme cases of this inequality yield the following situation

$$\begin{aligned}
[\mathcal{A}:\mathbb{Q}] = 2g \quad &\Longleftrightarrow \quad \chi_{\pi_q} \textit{ is squarefree},\\
&\Longleftrightarrow \quad \mathcal{A} = \mathbb{Q}(\pi_q),\\
&\Longleftrightarrow \quad \mathcal{A} \textit{ is commutative},
\end{aligned}$$

$$\begin{aligned}
[\mathcal{A}:\mathbb{Q}] = (2g)^2 \quad &\Longleftrightarrow \quad \exists a \in \mathbb{C}:\ \chi_{\pi_q} = (X-a)^{2g},\\
&\Longleftrightarrow \quad \mathbb{Q}(\pi_q) = \mathbb{Q},\\
&\Longleftrightarrow \quad \mathcal{A} \cong \mathbb{M}_g(D_p),\\
&\Longleftrightarrow \quad \exists \textit{ supersingular elliptic curve } E \textit{ with}\\
&\qquad\quad \operatorname{End}_K E = \operatorname{End} E \textit{ and an isogeny } \phi : A \to E^g
\end{aligned}$$

where D_p denotes the quaternion algebra which is ramified at p and infinity as defined before. Finally we have

$$\begin{aligned}
&\exists \textit{ simple abelian variety } B \textit{ and an isogeny } \phi : A \to B^u \textit{ for some } u \in \mathbb{N}\\
\Longleftrightarrow \quad &\exists h \in \mathbb{Z}[X] \textit{ irreducible over } \mathbb{Q} \textit{ and } u \in \mathbb{N} \textit{ such that } \chi_{\pi_q} = h^u\\
\Longrightarrow \quad &\mathcal{A} \textit{ is a central simple algebra over } \mathbb{Q}(\pi_q).
\end{aligned}$$

When we apply this theorem on the situation of an elliptic curve, we get the following results as consequences.

Corollary 2.38. *Let E be an elliptic curve defined over the finite field $K := \mathbb{F}_q$ of characteristic p and let $t \in \mathbb{Z}$ be the trace of the* Frobenius *endomorphism $\pi_q : E \to E$. Then the algebra $\mathcal{A} := \operatorname{End}_K E \otimes_{\mathbb{Z}} \mathbb{Q}$ is a central simple algebra with center $\mathbb{Q}(\pi_q)$. We have*

$$\begin{aligned}
\dim_{\mathbb{Q}} \mathcal{A} = 2 \quad &\Longleftrightarrow \quad X^2 - tX + q \textit{ is squarefree}\\
&\Longleftrightarrow \quad \mathcal{A} = \mathbb{Q}(\pi_q)\\
&\Longleftrightarrow \quad \mathcal{A} \textit{ is commutative},
\end{aligned}$$

$$\begin{aligned}
\dim_{\mathbb{Q}} \mathcal{A} = 4 \quad &\Longleftrightarrow \quad \exists a \in \mathbb{C}:\ X^2 - tX + q = (X-a)^2\\
&\Longleftrightarrow \quad \mathbb{Q}(\pi_q) = \mathbb{Q}\\
&\Longleftrightarrow \quad \mathcal{A} \cong D_p\\
&\Longleftrightarrow \quad E \textit{ is supersingular with } \operatorname{End}_K E = \operatorname{End} E.
\end{aligned}$$

We can make a more refined statement for these restricted endomorphism rings $\operatorname{End}_{\mathbb{F}_q} E$ as in RÜCK [72] or CHAPTER 4 of WATERHOUSE [92].

THEOREM 2.39. *Let p be a prime, $q = p^n$ and E be an elliptic curve defined over $\mathbb{F}_q$. Let $t = q + 1 - \#E(\mathbb{F}_q)$ be the trace of q-th* FROBENIUS π_q*. Then one of the following properties holds:*

a) $\gcd(t, p) = 1$,

b) n *even and* $t = \pm 2\sqrt{q}$,

c_1) n *even,* $p \not\equiv 1 \pmod 3$ *and* $t = \pm\sqrt{q}$,

c_2) n *even,* $p \not\equiv 1 \pmod 4$ *and* $t = 0$,

c_3) n *odd,* $p \in \{2, 3\}$ *and* $t = \pm p^{(n+1)/2}$,

c_4) n *odd and* $t = 0$.

Furthermore we have in the cases above

a) *E is ordinary, $\mathcal{A} = \mathbb{Q}(\pi_q) \cong \mathbb{Q}(\sqrt{t^2 - 4q})$ is an imaginary quadratic field over $\mathbb{Q}$ and $\operatorname{End}_{\mathbb{F}_q} E$ is isomorphic to an order in $\mathcal{A}$,*

b) *E is supersingular, $\mathcal{A}$ is a quaternion algebra over $\mathbb{Q}$, $\mathbb{Q}(\pi_q) = \mathbb{Q}$ and $\operatorname{End}_{\mathbb{F}_q} E$ is isomorphic to a maximal order in $\mathcal{A}$,*

c_i) *E is supersingular, $\mathcal{A} = \mathbb{Q}(\pi_q)$ is an imaginary quadratic field over $\mathbb{Q}$ and $\operatorname{End}_{\mathbb{F}_q} E$ is isomorphic to an order in $\mathcal{A}$ with conductor prime to p.*

This structure of the restricted endomorphism ring – especially the last case where a supersingular elliptic curve E will have $\operatorname{End}_{\mathbb{F}_q} E$ as an order in an imaginary quadratic field – will be central for our considerations and the basis for our algorithms.

On the other hand we are interested in quaternion algebras since for certain elliptic curves the full endomorphism ring is contained in one of them. This is due to the next theorem. Remember that an *anti-involution* on a $\mathbb{Z}$-module $\mathcal{M}$ is a $\mathbb{Z}$-linear and self-inverse map $\widehat{\cdot} : \mathcal{M} \to \mathcal{M}$ satisfying $\widehat{\alpha\beta} = \widehat{\beta}\widehat{\alpha}$ for any $\alpha, \beta \in \mathcal{M}$.

THEOREM 2.40. *Let $\mathcal{M}$ be an integral domain with $\operatorname{char} \mathcal{M} = 0$, $\operatorname{rk}_{\mathbb{Z}} \mathcal{M} \leq 4$ as $\mathbb{Z}$-module and an anti-involution $\widehat{\cdot} : \mathcal{M} \to \mathcal{M}$ with*

$$\alpha\widehat{\alpha} \in \mathbb{Z}_{\geq 0} \quad \textit{and} \quad \alpha\widehat{\alpha} = 0 \iff \alpha = 0$$

for all $\alpha \in \mathcal{M}$. Then we either get $\mathcal{M} = \mathbb{Z}$ or $\mathcal{M}$ is an order in either an imaginary quadratic extension of $\mathbb{Q}$ or in a definite quaternion algebra over $\mathbb{Q}$.

For a detailed analysis of the proof of this theorem see THEOREM III.9.3 of SILVERMAN [75]. Since the endomorphism ring of an elliptic curve E – with the anti-involution $\widehat{\cdot} : \operatorname{End} E \to \operatorname{End} E$ sending an endomorphism to its dual – fulfills all of the conditions of such a module $\mathcal{M}$, a direct conclusion of THEOREM 2.40 applied on endomorphism rings is the following statement.

COROLLARY 2.41. *Let E be an elliptic curve defined over the field K. Then we either have $\operatorname{End} E \cong \mathbb{Z}$ or $\operatorname{End} E$ is an order in either an imaginary quadratic field $\mathcal{A}$ or in a definite quaternion algebra $\mathcal{A}$ over $\mathbb{Q}$.*

EXERCISE III.3.18 of SILVERMAN [75] shows a way to see that if for an elliptic curve E over a field K the endomorphism ring $\operatorname{End} E$ is an order in a definite quaternion algebra $\mathcal{A}$, then K is a field of characteristic $p > 0$ and $\mathcal{A}$ ramifies exactly at p and ∞. Since two definite quaternion algebras are isomorphic if and only if they ramify at the same places, $\mathcal{A}$ is uniquely determined up to isomorphism. Further the exercise provides that $\operatorname{End} E$ is a maximal order in $\mathcal{A}$.

Therefore we can write $\mathcal{A}$ as $\mathbb{Q} + \alpha\mathbb{Q} + \beta\mathbb{Q} + \alpha\beta\mathbb{Q}$ with $\alpha\beta = -\beta\alpha$, $\alpha^2 = -p$ and $\beta^2 = -q$ with a prime q such that $(\frac{-q}{p}) = -1$ and thus we have $\beta \notin \mathbb{Q}(\alpha)$.

REMARK. Depending on the characteristic of the field K some cases can be excluded as in REMARK III.9.4.1 of SILVERMAN [75]:

- ✦ $\operatorname{char} K = 0 \implies \operatorname{End} E \otimes_{\mathbb{Z}} \mathbb{Q}$ is commutative, thus it is no quaternion algebra,
- ✦ $\operatorname{char} K = p > 0 \implies \mathbb{Z} \subsetneq \operatorname{End} E$.

Together with THEOREM 2.22 this implies that an elliptic curve E over a finite field $\mathbb{F}_q$ is

$$\begin{aligned} \text{ordinary} \quad &\iff \quad \operatorname{End} E \text{ is an order in an imaginary quadratic field,} \\ \text{supersingular} \quad &\iff \quad \operatorname{End} E \text{ is an order in a quaternion algebra.} \end{aligned}$$

Now we will regard endomorphism rings of ordinary resp. supersingular elliptic curves consecutively and particularly examine how endomorphism rings of isogenous elliptic curves are related to each other. In the ordinary case there are quite helpful relations which are the foundation of the known algorithms for computing isogenies between ordinary elliptic curves. For supersingular elliptic curves the structure is different, which is the reason those approaches do not work there. We will see how to fix that in a later section.

2.2.2 Ordinary Elliptic Curves

Let E be an ordinary elliptic curve defined over $\mathbb{F}_q$ with trace t. Then due to Theorem 2.39 $\operatorname{End} E$ is isomorphic to an order $\mathcal{O}$ in the imaginary quadratic field $\mathcal{K} = \mathbb{Q}(\sqrt{d})$ where $d = t^2 - 4q$ is a negative integer. It is standard number theory that when d_s is the square-free part of d, the *fundamental discriminant of* $\mathcal{K}$ is

$$d_{\mathcal{K}} = \begin{cases} d_s & \text{if } d_s \equiv 1 \pmod 4 \\ 4d_s & \text{if } d_s \equiv 2, 3 \pmod 4, \end{cases}$$

the *maximal order of* $\mathcal{K}$ is

$$\mathcal{O}_{\mathcal{K}} = \mathbb{Z}\left[\tfrac{d_{\mathcal{K}}+\sqrt{d_{\mathcal{K}}}}{2}\right]$$

and every other order of $\mathcal{K}$ is of the form $\widetilde{\mathcal{O}} = \mathbb{Z} + c\mathcal{O}_{\mathcal{K}}$ where $c := [\mathcal{O}_{\mathcal{K}} : \widetilde{\mathcal{O}}]$ is the *conductor of* $\widetilde{\mathcal{O}}$ and determines the order. We often denote such an order with $\mathcal{O}_c$ and its discriminant $d_{\mathcal{O}} = c^2 d_{\mathcal{K}}$ with d_c, or when the order is isomorphic to $\operatorname{End} E$ with $\mathcal{O}_E$ resp. d_E.

We usually fix an isomorphism $[\cdot] : \mathcal{O} \to \operatorname{End} E$ and identify the rings $\mathcal{O}$ and $\operatorname{End} E$ with each other. Since for every $m \in \mathbb{Z}$ the multiplication-by-m-map $[m]$ and also the q-th Frobenius π_q are elements of $\operatorname{End} E$ when E is defined over $\mathbb{F}_q$, we can in this case embed $\mathbb{Z}[\pi_q]$ into $\operatorname{End} E$ and interpret it also as a subring of $\mathcal{O}$. Thus we get the following statement.

Proposition 2.42. *Let E be an ordinary elliptic curve over $\mathbb{F}_q$ and π_q the q-th* Frobenius *morphism. Let $\mathcal{O}$ be an order in $\mathcal{K} = \mathbb{Q}(\sqrt{d})$ with $\mathcal{O} \cong \operatorname{End} E$. Then we have*

$$\mathbb{Z}[\pi_q] \subseteq \mathcal{O} \subseteq \mathcal{O}_{\mathcal{K}}.$$

Since on the other hand $\mathbb{Z}[\pi_q]$ contained in $\operatorname{End} E$ means that we have $E^{(q)} = E$, this provides that the Weierstrass polynomial of E is defined over $\mathbb{F}_q$ and thus per definition E is also $\mathbb{F}_q$-rational and we can state the next result.

Lemma 2.43. *Let E be an ordinary elliptic curve defined over a finite field of characteristic p. Then E is defined over $\mathbb{F}_q$ if and only if we have $\mathbb{Z}[\pi_q] \subseteq \operatorname{End} E$.*

It is slightly surprising that we can also make a statement about the relation of endomorphism rings of different ordinary elliptic curves which are isogenous to each other. This is a fundamental result from Proposition 21 of Kohel [45], which actually has a quite simple proof despite its importance for our further work.

Proposition 2.44. *Let E_0 and E_1 be ordinary elliptic curves defined over the finite field $\mathbb{F}_q$ of characteristic p and $\phi : E_0 \to E_1$ be an isogeny of prime degree $\ell \neq p$. Let $\mathcal{O}_0$ and $\mathcal{O}_1$ be orders in the imaginary quadratic field $\mathcal{K}$ with $\mathcal{O}_i \cong \operatorname{End} E_i$ for $i \in \{0, 1\}$. Then we have*

$$\mathcal{O}_i \subseteq \mathcal{O}_{1-i} \quad \textit{and} \quad [\mathcal{O}_{1-i} : \mathcal{O}_i] \mid \ell$$

for $i = 0$ or $i = 1$ where $[\mathcal{O}_{1-i} : \mathcal{O}_i]$ denotes the ring index.

Proof. Let $\phi : E_0 \to E_1$, $\mathcal{O}_0$ and $\mathcal{O}_1$ be defined as in the proposition. First we can show in a straightforward way that there are inclusions

$$\mathbb{Z} + \ell^2\mathcal{O}_0 \ \subseteq \ \mathbb{Z} + \widehat{\phi}\mathcal{O}_1\phi \ \subseteq \ \mathcal{O}_0$$

and that the index $[\mathcal{O}_0 : \mathbb{Z} + \ell^2\mathcal{O}_0]$ is ℓ^2. Since $\mathbb{Z} + \widehat{\phi}\mathcal{O}_1\phi$ is isomorphic to $\mathbb{Z} + \ell\mathcal{O}_1$, we get the following relation of rings

$$\begin{tikzcd}[arrows=-]
 & \mathcal{O}_{\mathcal{K}} & \\
\mathcal{O}_0 \arrow[ur, "c_0"] \arrow[rr, dashed, "x"] \arrow[d, "\ell"] \arrow[drr, "y"] & & \mathcal{O}_1 \arrow[ul, "c_1"'] \arrow[d, "\ell"] \\
\mathbb{Z} + \ell\mathcal{O}_0 \arrow[d, "\ell"] & & \mathbb{Z} + \ell\mathcal{O}_1 \arrow[d, "\ell"] \arrow[dll, "z"] \\
\mathbb{Z} + \ell^2\mathcal{O}_0 \arrow[dr, "r_0"] & & \mathbb{Z} + \ell^2\mathcal{O}_0 \arrow[dl, "r_1"'] \\
 & \mathbb{Z}[\pi_q] &
\end{tikzcd}$$

where $x, y, z, c_i, r_i \in \mathbb{N}$ are the unknown ring indices. In the case when $\mathcal{O}_0 = \mathbb{Z} + c_o\mathcal{O}_{\mathcal{K}}$ and $\mathcal{O}_1 = \mathbb{Z} + c_1\mathcal{O}_{\mathcal{K}}$ are contained in each other, x is the index of interest. We see in the diagram that we have $c_0r_0 = c_1r_1$ and because also $y \cdot z = \ell^2$ has to hold, we obtain the following three possibilities:

$y = 1$: This means $\mathcal{O}_0 \cong \mathbb{Z} + \ell\mathcal{O}_1$ and since the conductor determines an order in $\mathcal{K}$ uniquely, we have $\mathcal{O}_0 = \mathbb{Z} + \ell\mathcal{O}_1 \subseteq \mathcal{O}_1$ and $x = [\mathcal{O}_1 : \mathcal{O}_0] = \ell$.

$y = \ell$: Here we get $r_0 = r_1$ from the equation $[\mathcal{O}_0 : \mathbb{Z}[\pi_q]] = \ell^2 r_0 = y\ell r_1$ and thus also $c_0 = c_1$ which yields $\mathcal{O}_0 = \mathcal{O}_1 = \mathbb{Z} + c_0\mathbb{Z}$ and $x = [\mathcal{O}_1 : \mathcal{O}_0] = [\mathcal{O}_0 : \mathcal{O}_1] = 1$.

$y = \ell^2$: This tells us $r_0 = r_1\ell$ and thus $c_1 = c_0\ell$ which finally provides the equality $\mathcal{O}_1 = \mathbb{Z} + \ell\mathcal{O}_0 \subseteq \mathcal{O}_0$ and $x = [\mathcal{O}_0 : \mathcal{O}_1] = \ell$. □

We have concluded from Proposition 2.20 that instead of computing an isogeny of possibly large degree it is better to construct a chain of isogenies with small prime degree. Therefore we examine the relation of endomorphism rings of elliptic curves which are ℓ-isogenous with prime degree now. Let $\mathcal{O}_0$ and $\mathcal{O}_1$ be orders in $\mathcal{K}$ isomorphic to $\operatorname{End} E_0$ resp. $\operatorname{End} E_1$. According to the last two propositions we are in one of the following situations if we settle on prime degrees $\ell \neq p$.

$$
\begin{tikzcd}
\mathcal{O}_{\mathcal{K}} \arrow[d, dash, "c_1"] \arrow[dd, dash, bend left=60, "c_0"] \arrow[ddd, dash, bend right=60, "c"'] \\
\mathcal{O}_1 \arrow[d, dash, "\ell"] \\
\mathcal{O}_0 \arrow[d, dash] \\
\mathbb{Z}[\pi_q]
\end{tikzcd}
\qquad
\begin{tikzcd}
\mathcal{O}_{\mathcal{K}} \arrow[d, dash, "c_0"] \\
\mathcal{O}_0 \arrow[d, dash, "\ell"] \arrow[dd, dash, bend left=60, "\frac{c}{c_0}"] \\
\mathcal{O}_1 \arrow[d, dash] \\
\mathbb{Z}[\pi_q]
\end{tikzcd}
\qquad
\begin{tikzcd}
\mathcal{O}_{\mathcal{K}} \arrow[d, dash] \\
\mathcal{O}_0 \cong \mathcal{O}_1 \arrow[d, dash] \\
\mathbb{Z}[\pi_q]
\end{tikzcd}
$$

In the first case we call the isogeny $\phi : E_0 \to E_1$ *ascending* or *going up*, in the second one ϕ is *descending* or *going down* and in the last case it is *horizontal*. When ϕ is not horizontal, we see that ℓ has to divide $c = [\mathcal{O}_{\mathcal{K}} : \mathbb{Z}[\pi_q]]$.

Even more, if ϕ is ascending resp. descending, ℓ divides $c_0 = [\mathcal{O}_{\mathcal{K}} : \mathcal{O}_0]$ resp. $\frac{c}{c_0} = [\mathcal{O}_0 : \mathbb{Z}[\pi_q]]$. Thus, if $\ell \nmid c_0$, it is no longer possible to go up and E_0 is called *on the surface at* ℓ. Analogous, E_0 is *on the floor at* ℓ when $\ell \nmid \frac{c}{c_0}$ and it is not possible to go further down. Note that this is no global position since it can happen that an elliptic curve is on the surface or on the floor at some ℓ without having endomorphism ring $\mathcal{O}_{\mathcal{K}}$ or $\mathbb{Z}[\pi_q]$.

We will see in SECTION 3 how to determine the number of outgoing isogenies of each type on each level. The resulting structure leads us to so-called *isogeny graphs* which provide a good approach of finding isogeny chains between given isogenous ordinary elliptic curves.

2.2.3 Supersingular Elliptic Curves

If we take a supersingular elliptic curve E over $\mathbb{F}_p$ with $p > 3$, we know from THEOREM 2.22 that the full endomorphism ring of E is an order in a quaternion algebra. But when we regard the endomorphism ring of E restricted to endomorphisms defined over $\mathbb{F}_p$, we end up in case c_4) of THEOREM 2.39. Thus we obtain that $\operatorname{End}_{\mathbb{F}_p} E$ is an order in an imaginary quadratic field $\mathcal{K}$ and its conductor is prime to p. As this is analogous to the case of full endomorphism rings of ordinary elliptic curves, we can apply the results we constructed there to this situation.

Since we know that supersingular elliptic curves have trace $t = 0$, we get $d = -4p$ and $\mathcal{K} = \mathbb{Q}(\sqrt{-p}) \cong \mathbb{Q}(\pi_p)$ with fundamental discriminant

$$d_{\mathcal{K}} \quad = \quad \begin{cases} -p & \text{if } p \equiv 3 \pmod 4 \\ -4p & \text{if } p \equiv 1 \pmod 4. \end{cases}$$

In the first case the maximal order of $\mathcal{K}$ is $\mathcal{O}_{\mathcal{K}} = \mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$ and in the other one we have $\mathcal{O}_{\mathcal{K}} = \mathbb{Z}[\sqrt{-p}]$. Additionally, we get $\mathbb{Z}[\pi_p] \cong \mathbb{Z}[\sqrt{-p}]$, too.

It is useful to see that the proof of Proposition 2.42 needs nothing of the fact that the given elliptic curves are ordinary except for the structure of the orders in $\mathcal{K}$ which are isomorphic to the endomorphism rings. Therefore we can state an analogous result for supersingular elliptic curves defined over $\mathbb{F}_p$ and their restricted endomorphism rings and get

$$\mathbb{Z}\left[\pi_p\right] \;\subseteq\; \mathcal{O} \;\subseteq\; \mathcal{O}_{\mathcal{K}}$$

when we have $\mathrm{End}_{\mathbb{F}_p} E \cong \mathcal{O}$.

As for $p \equiv 1 \pmod 4$ the orders including and included in $\mathcal{O}$ coincide, there is no other choice for it but $\mathbb{Z}[\sqrt{-p}]$. This means that in this case all supersingular elliptic curves have the same $\mathbb{F}_p$-rational endomorphism ring with discriminant $d_{\mathcal{K}} = -4p$.

For $p \equiv 3 \pmod 4$ the conductor $[\mathcal{O}_{\mathcal{K}} : \mathbb{Z}[\sqrt{-p}]]$ is $c = 2$, so $\mathcal{O}$ can be either the maximal order $\mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$ with discriminant $d_{\mathcal{K}} = -p$ or the order $\mathbb{Z}[\sqrt{-p}]$ with discriminant $d_2 = -4p$.

Further the definitions of *ascending*, *descending* and *horizontal* isogenies can be stated analogously to the ordinary situation, too. Thus in all appearing cases we have only one or at most two possibilities for $\mathcal{O}$ and for the case $p \equiv 1 \pmod 4$ there can be only horizontal isogenies. We will see in Section 4.2.2 that this makes certain supersingular isogeny graphs even more assessable than most ordinary ones.

2.3 Graph Theory

We will consider so-called *isogeny graphs* later in this work, so we want to introduce the basic concepts of graph theory and special properties of certain types of graphs that we will need for our results. We mainly use the book of Diestel [20] and chapter 1.1 of Davidoff, Sarnak, Valette [17] for the introduction of concepts, section 25.3.2 of Galbraith [28] and Murty [63] for the definition of expander graphs. Many additional information can be found there.

2.3.1 Basic Concepts

A *graph* G consists of a set $V_G \neq \emptyset$ of *vertices* and a possibly empty set $E_G \subseteq {V_G}^2$ of *edges* and is often written as $G = (V_G, E_G)$. In a graphical interpretation we can draw the nodes as labeled dots. A directed edge $e \in E_G$ is of the form $e = (v_1, v_2)$ for $v_1, v_2 \in V_G$ which graphically means a connection in form of an arrow from v_1 to v_2. The edge from v_2 to v_1 which is the arrow of e run through in the other direction is sometimes labeled e^{-1}.

Often graphs are *undirected*, that means the edges (v_1, v_2) and (v_2, v_1) are considered the same. It is possible to have more than one edge between two given nodes, in that case G is often called a *multigraph*. We will not use this term and understand every graph as a potential multigraph. Note that for an edge (v_1, v_2) in a multigraph not every edge (v_2, v_1) equals e^{-1}.

When there is an edge from v_1 to v_2, the vertex v_2 is called a *neighbor of* v_1 and the edge (v_1, v_2) an *outgoing edge from* v_1. If every vertex in V_G has exactly $k \in \mathbb{N}$ outgoing edges, G is called a *k-regular graph*.

If the graph G has the nodes $v_1, \cdots, v_n$, we define the *adjacency matrix of* G as $A(G) = (a_{ij})_{i,j=1,\cdots,n}$ where a_{ij} denotes the number of edges from v_i to v_j. Obviously for a k-regular graph we have $\sum_{j=1}^{n} a_{ij} = k$ for every possible i. For an undirected graph this matrix is symmetric and we also have $\sum_{i=1}^{n} a_{ij} = k$ for every j.

For $m \leq n$ and pairwise distinct $v_i \in V_G$ we define a *path in* G as an ordered set $[v_0, v_1, \cdots, v_{m-1}, v_m]$ such that $P = (V_P, E_P)$ with

$$\begin{aligned} V_P &:= \{v_0, v_1, \cdots, v_{m-1}, v_m\} \quad \text{and} \\ E_P &:= \{(v_i, v_{i+1}) \mid 0 \leq i \leq m-1\} \end{aligned}$$

is a subgraph of G. We also say that P is a path from v_0 to v_m and has length $m \in \mathbb{N}$. The graph G is *connected* when between any two vertices of it there exists a path in G. For $v_1, v_2 \in V_G$ we define the *distance between* v_1 *and* v_2 *in* G as the length of the shortest possible path from v_1 to v_2. The *diameter of* G is the maximal distance of two vertices in G. A *circle of length* m is a path of length m in G which has the same start and end vertex $v_0 = v_m$. A graph without circles is called a *tree.*

Let now $G = (V_G, E_G)$ be an undirected, k-regular graph with vertex set $V_G = \{v_1, \cdots, v_n\}$. The adjacency matrix $A := A(G)$ of G is real and symmetric, so due to the spectral theorem it has n real eigenvalues

$$\lambda_{n-1} \leq \cdots \leq \lambda_1 \leq \lambda_0.$$

We say that λ is an *eigenvalue of* G if there is a function $f : V_G \to \mathbb{C}$ such that λ is an eigenvalue of A for some eigenvector

$$x := \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} f(v_1) \\ \vdots \\ f(v_n) \end{pmatrix}.$$

The next result concerning the eigenvalues is essentially Proposition 1.1.2 of Davidoff, Sarnak and Valette [17].

Proposition 2.45. *With the notation from above we deduce*

1. $|\lambda_i| \leq k$ *for all* $i \in \{1, \cdots, n\}$
2. $\lambda_0 = k$
3. $\lambda_1 < \lambda_0 \iff G$ *is connected*

Proof. 1. Let $\lambda \in \{\lambda_0, \cdots, \lambda_n\}$ be an eigenvalue of A with corresponding eigenvector x. Let x_i be the entry of x with $|x_i| = \max\{|x_1|, \cdots |x_n|\}$. We can assume without loss of generality that we have $x_i > 0$; if not we replace x with the negated vector $-x$.

From the eigenequation $Ax = \lambda x$ we get

$$\begin{aligned} |\lambda| x_i = |\lambda x_i| &= \left| \sum_{j=1}^{n} a_{ij} x_j \right| \\ &\leq \sum_{j=1}^{n} a_{ij} |x_j| \\ &\leq \sum_{j=1}^{n} a_{ij} x_i = k x_i \end{aligned}$$

and the statement follows.

2. Since G is k-regular, the sum of every row of A is k. Therefore

$$A\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix} = \begin{pmatrix}k\\ \vdots\\ k\end{pmatrix}$$

and thus k is an eigenvalue of A. Since all eigenvalues are less or equal to k, λ_0 as the largest one has to attain this value.

3. We show both implications separately.

"$\Longrightarrow$" Suppose that G is not connected. Show that there exists an eigenvector x for the eigenvalue $k = \lambda_0$ which is not a multiple of the vector $(1 \ \cdots \ 1)^T$. Since G is not connected, there must be a subset $U \subsetneq V_G$ such that no edges exist between any vertices $u \in U$ and $v \in V_G \setminus U$. Without loss of generality we can set $U := \{v_1, \cdots, v_r\}$ with $0 < r < n$. Then the adjacency matrix is of the form

$$A = \begin{pmatrix} A(U) & 0 \\ 0 & A(V_G \setminus U) \end{pmatrix}$$

and the vector $x := \begin{pmatrix}1 & \cdots & 1 & 0 & \cdots & 0\end{pmatrix}^T$ with $n-r > 0$ zero entries is an eigenvector for the eigenvalue k of A. and not a multiple of $(1 \ \cdots \ 1)^T$.

"$\Longleftarrow$" Let G be connected and x be an eigenvector of A to the eigenvalue k, so we have $Ax = kx$ and thus for every $i \in \{1, \cdots, n\}$

$$\sum_{j=1}^{n} a_{ij} x_j \quad = \quad k x_i.$$

We have to show that $x_1 = \cdots = x_n$. As above we choose x_i such that $|x_i| = \max\{|x_1|, \cdots |x_n|\}$. Then from the last equation we have a convex combination

$$x_i \quad = \quad \sum_{j=1}^{n} \tfrac{a_{ij}}{k} x_j \ \leq \ \sum_{j=1}^{n} \tfrac{a_{ij}}{k} x_i \quad = \quad x_i$$

since the non-negative integers a_{ij} summed up yield k. Therefore if we have $a_{ij} \neq 0$ – so when v_i and v_j are neighbors – we obtain $x_i = x_j$.

If now v_l is a neighbor of v_i, we have $|x_l| = |x_i| = \max\{|x_1|, \cdots |x_n|\}$ and thus the same argument holds for all neighbors of x_l, too. Since G is connected, we can reach every vertex in this way and get $x_j = x_i$ for all possible values of j. □

Definition. Let $G = (V_G, E_G)$ be a graph.

- A *walk in* G is a path in G where the condition is dropped that the v_i must be pairwise distinct. A path is a *self-avoiding* walk. The process of going to the vertex v_{i+1} from v_i via the edge e_i we call a *step*. A walk is *non-backtracking* if it is forbidden to reverse the last step along the same edge, that is, sequences like $v_{i+2} = v_i$ and $e_{i+1} = e_i^{-1}$ are not allowed. This condition is not as strong as being a path, though.
- A *random walk in* G is a walk in G where in each step the edge (v_i, v_{i+1}) and with it the vertex v_{i+1} is chosen uniformly at random from the possible outgoing edges of v_i.

A *bi-directional search in* G starts with two one-elemental subgraphs $X_0 = \{v_0\}$ and $X_1 = \{v_1\}$ of G and increases the sets X_i using some declared method (i.e. by adding the edge and vertex reached by the next step of a random walk starting at each of the v_i; or by adding all outgoing edges of X_i and their image vertices as in a breadth-first search). The bi-directional search ends when we have $X_0 \cap X_1 \neq \emptyset$ and any vertex occurring in the intersection is called a *collision*.

Under the assumption that during such a bi-directional search the elements in both X_i are chosen uniformly at random, we can estimate the size of the subgraphs until a collision occurs with an adapted version of the birthday attack.

Proposition 2.46 (Bi-directional Birthday Attack). *Let $G = (V_G, E_G)$ be a graph with $|V_G| = n$. Then the expected number of elements drawn from V_G during a bi-directional search until a collision occurs is roughly $\sqrt{\pi n}$.*

Remark. The proof we describe here follows the lines of the proof for Theorem 14.1.1 of Galbraith [28], although there the author describes the usual birthday attack where elements are sampled randomly from a n-element set. The modification of differentiation between two subsets X_0 and X_1 of V_G leads to the expected number $\sqrt{\pi n}$ instead of $\sqrt{\pi n/2}$ as in the normal case.

Proof. We define a random variable $\mathbb{X}$ which describes the number of elements of V_G which are selected until a collision occurs. Assume that m elements are already drawn from V_G, so roughly $m/2$ of them lie in X_0 and X_1 each. The probability that the next element (which is added to the side X_i) already appears on the other side in X_{1-i} is thus $\frac{m/2}{n}$.

Thus we can compute the expected value of $\mathbb{X}$ as

$$
\begin{aligned}
\mathbb{E}(\mathbb{X}) &= \sum_{m=1}^{\infty} m \cdot \Pr(\mathbb{X} = m) \\
&= \sum_{m=1}^{\infty} m \cdot \big(\Pr(\mathbb{X} > m-1) - \Pr(\mathbb{X} > m) \big) \\
&= \sum_{m=0}^{\infty} \big((m+1) \cdot \Pr(\mathbb{X} > m) - m \cdot \Pr(\mathbb{X} > m) \big) \\
&= \sum_{m=0}^{\infty} \Pr(\mathbb{X} > m) \\
&\overset{(1)}{\leq} 1 + \sum_{m=1}^{\infty} \exp(-\tfrac{(m-1)^2}{4n}) \\
&\overset{(2)}{\leq} 2 + \int\limits_{0}^{\infty} \exp(-\tfrac{x^2}{4n}) \mathrm{d}x \\
&\overset{(3)}{=} 2 + 2\sqrt{n} \int\limits_{0}^{\infty} \exp(-u^2) \mathrm{d}u \\
&= 2 + 2\sqrt{n} \cdot \sqrt{\pi}/2.
\end{aligned}
$$

Here the steps denoted with (1), (2) and (3) on the equal resp. less-than-or-equal signs arise due to the following considerations.

(1) With the estimate $1 - x \leq \exp(-x)$ for $0 \leq x \in \mathbb{R}$ we get

$$
\begin{aligned}
\Pr(\mathbb{X} > m) &= \prod_{i=0}^{m-1} (1 - \tfrac{i}{2n}) \\
&\leq \prod_{i=0}^{m-1} \exp(-\tfrac{i}{2n}) \\
&= \exp(-\sum_{i=0}^{m-1} \tfrac{i}{2n}) \\
&= \exp(-\tfrac{1}{2n} \cdot \tfrac{(m-1)m}{2}) \\
&\leq \exp(-\tfrac{(m-1)^2}{4n}).
\end{aligned}
$$

(2) The function $\exp(-\frac{x^2}{4n})$ is monotonically decreasing, so

$$\begin{aligned}
\sum_{m=1}^{\infty} \exp(-\tfrac{(m-1)^2}{4n}) &= \sum_{m=0}^{\infty} \exp(-\tfrac{m^2}{4n}) \\
&= 1 + \sum_{m=1}^{\infty} \int_{m-1}^{m} \exp(-\tfrac{m^2}{4n}) \mathrm{d}x \\
&\leq 1 + \sum_{m=1}^{\infty} \int_{m-1}^{m} \exp(-\tfrac{x^2}{4n}) \mathrm{d}x \\
&= 1 + \int_{0}^{\infty} \exp(-\tfrac{x^2}{4n}) \mathrm{d}x
\end{aligned}$$

explains the inequality between the sum and the integral here.

(3) A change of variables with $u := \frac{x}{2\sqrt{n}}$ yields this step. □

We will regard various bi-directional searches later, so this proposition helps determining the complexity of such algorithms.

2.3.2 Expander Graphs

Our isogeny graphs later will turn out to have the useful property of being *expander graphs* which we describe in this part of the work.

Definition. Let $G = (V_G, E_G)$ be a k-regular connected graph with $|V_G| = n \in \mathbb{N}$ and nontrivial eigenvalues $\lambda_1 \geq \cdots \geq \lambda_m$ for $m \leq n$. We define

$$\lambda(G) \;:=\; \max |\lambda_i|.$$

G is called a Ramanujan *graph* if we have $\lambda(G) \leq 2\sqrt{k-1}$.

Let $U \subseteq V_G$ be a subset of vertices. The *vertex boundary* $\partial_v(U)$ *of* U *in* V_G is the set of vertices which have distance one to U and is defined as

$$\partial_v(U) \;:=\; \{v \in V_G \setminus U \mid \exists u \in U \text{ such that } (u,v) \in E_G\}.$$

Similar the *edge boundary* $\partial_e(U)$ *of* U *in* V_G is the set of edges which lead out of U, namely

$$\partial_e(U) \;:=\; \{(u,v) \in E_G \mid u \in U \text{ and } v \in V_G \setminus U\}.$$

Let $c > 0$ be a real number. If for all subsets $U \subseteq V_G$ with $|U| \leq |V_G|/2$ we have the relation

$$|\partial_v(U)| \geq c \cdot |U|,$$

G is called a *c-expander graph* and c an *expander constant of G*.

This estimation can later be used in a complexity analysis concerning an expander graph; further expander graphs have the nice "mixing property" that random walks on them reach the uniform distribution quickly (page 533 of GALBRAITH [28] or SECTION 2.3 of CHARLES-GOREN-LAUTER [10]), that means that after a certain number of steps the end vertex v_m of a random walk in a graph with N vertices behaves like a vertex that is chosen uniformly at random.

Simple counting considerations show the following coherence.

LEMMA 2.47. *Let U be a subset of V_G. Then we obtain the relations*

$$|\partial_v(U)| \;\leq\; |\partial_e(U)| \;\leq\; k\;|\partial_v(U)|$$

between the cardinalities of the vertex- and edge-boundaries.

As we will show at the end of this section, this connection and the next proposition can be used to determine an expander constant for certain types of graphs.

PROPOSITION 2.48. *Let $G = (V_G, E_G)$ be a k-regular graph and $U \subseteq V_G$ be a subset of vertices with $|U| \leq |V|/2$. Then we get*

$$|\partial_e(U)| \geq \frac{k - \lambda_1}{2}|U|$$

where λ_1 is the maximal eigenvalue as before.

PROOF. MURTY shows on page 13 of [63] that the RAYLEIGH-RITZ-Theorem yields

$$k - \lambda_1 \quad = \quad \min_{\substack{f \neq 0 \\ \langle f, f_0 \rangle = 0}} \frac{\langle \Delta f, f \rangle}{\langle f, f \rangle}$$

where

- ✦ f is a real-valued function on V_G and f_0 is a constant function on V_G,
- ✦ the inner product $\langle \cdot, \cdot \rangle$ on the space of real-valued functions of V_G is defined as $\langle f, g \rangle := \sum_{v \in V_G} f(v)g(v)$,

- ✦ for the adjacency matrix A we have $(Af)(v) = \sum_{(v,u)\in E_G} f(u)$ where we take the sum over all outgoing edges $(v,u) \in E_G$ from V_G and
- ✦ $\Delta := k\,\mathrm{Id}_n - A$ has eigenvalues $k - \lambda_i$.

Now we choose the real-valued function f to be

$$f(v) = \begin{cases} |V_G \setminus U| & \text{if } v \in U \\ -|U| & \text{if } v \notin U \end{cases}$$

which satisfies the condition $\langle f, f_0 \rangle = 0$, so the inequation

$$k - \lambda_1 \quad \leq \quad \frac{\langle \Delta f, f \rangle}{\langle f, f \rangle}$$

holds for this f. Counting arguments yield

$$\begin{aligned}
\langle \Delta f, f \rangle &= k\langle f, f \rangle - \langle Af, f \rangle \\
&= k \sum_{v\in V_G} f(v)^2 - \sum_{v\in V_G} \sum_{(v,u)\in E_G} f(u)f(v) \\
&= \sum_{v\in V_G} \sum_{(v,u)\in E_G} f(v)^2 - \sum_{(v,u)\in E_G} f(u)f(v) \\
&= \tfrac{1}{2} \sum_{(v,u)\in E_G} f(v)^2 + f(u)^2 - \sum_{(v,u)\in E_G} f(u)f(v) \\
&= \tfrac{1}{2} \sum_{(v,u)\in E_G} (f(v) - f(u))^2 \\
&= \sum_{(v,u)\in E_G} (|V_G \setminus U| + |U|)^2 \\
&= |V_G|^2 \cdot |\partial_e(U)|,
\end{aligned}$$

$$\begin{aligned}
\langle f, f \rangle &= \sum_{v\in V_G} f(v)^2 \\
&= |V_G \setminus U| \cdot |V_G| \cdot |U|
\end{aligned}$$

and we conclude

$$\begin{aligned}
|\partial_e(U)| &\geq (k - \lambda_1)|U| \frac{|V_G \setminus U|}{|V_G|} \\
&\geq (k - \lambda_1)|U| \frac{|V_G|/2}{|V_G|} \\
&= \frac{k - \lambda_1}{2} |U|
\end{aligned}$$

since $|V_G \setminus U| \geq |V_G|/2$ follows from $|U| \leq |V_G|/2$. $\square$

Corollary 2.49. *With* Proposition *2.48 and* Lemma *2.47 we get*

$$\begin{aligned} |\partial_v(U)| &\geq \frac{|\partial_e(U)|}{k} \\ &\geq \frac{k-\lambda_1}{2k}|U|, \end{aligned}$$

so G is a c-expander graph with $c = \frac{k-\lambda_1}{2k}$ if we have $c > 0$.

Since we know $\lambda_1 < k$, the condition from Corollary 2.49 is always true. Especially this means that every Ramanujan graph is an expander graph since there $\lambda_1 < \lambda(G) \leq 2\sqrt{k-1}$ yields the constant c as above. We will see that for example supersingular isogeny graphs are Ramanujan graphs and thus we can use these results in our work with them.

3 Connection to Elliptic Curves over Number Fields

In this chapter we consider elliptic curves which are defined over a number field K and have special properties. For those curves we can develop a helpful set of results in Section 3.2 which describe their behavior and provide a nice picture of how the curves and their endomorphism rings are related to each other. Section 3.3 shows how the occurring structures can be transferred to elliptic curves defined over finite fields $\mathbb{F}_q$ at least when these reduced curves are ordinary. Further we show how to adapt this theory for curves whose reduction is supersingular, a result which is of fundamental value for our later work on supersingular isogeny graphs.

3.1 Complex Multiplication

In this part we sketch some basic theory we will need throughout this section. Let E be an elliptic curve defined over a number field $K \subseteq \mathbb{C}$. If we have that

- ✦ $\operatorname{End} E$ is a free $\mathbb{Z}$-module of rank two,
- ✦ there is an embedding $\iota : \operatorname{End} E \hookrightarrow \mathcal{K}$ for an imaginary quadratic field $\mathcal{K}$ and
- ✦ the image $\iota(\operatorname{End} E) =: \mathcal{O}$ is an order in $\mathcal{K}$,

E is said to have *complex multiplication with $\mathcal{O}$*.

Thus we can define an isomorphism $[\cdot] : \mathcal{O} \to \operatorname{End} E$. Note that hereby we can write any endomorphism of E as $[\alpha]$ with $\alpha \in \mathcal{O}$. For $\alpha = m \in \mathbb{Z}$ this is the same notation as for the usual multiplication-by-m-map $[m]$.

Two lattices Λ_0 and Λ_1 in $\mathbb{C}$ are called *homothetic* if there exists a complex number α with $\alpha\Lambda_0 = \Lambda_1$. It is a well-known fact (Silverman [75, Chapter VI]) that there is a bijection

$$\{E \text{ elliptic curve defined over } \mathbb{C}\}/_{\cong} \quad \longleftrightarrow \quad \{\Lambda \text{ lattice in } \mathbb{C}\}/_{\text{homothety}}$$

in the sense that every such elliptic curve E is given by the Weierstrass polynomial $Y^2 - 4X^3 + g_2(\Lambda)X + g_3(\Lambda)$ associated to[3] Λ in $\mathbb{C}$ and that the set $E(\mathbb{C})$ is isomorphic to the complex torus $\mathbb{C}/\Lambda$ as a group. The group law of the elliptic curve corresponds to the usual addition modulo a lattice on the torus.

[3]The modular functions g_2 and g_3 originate from the theory of elliptic functions and the existence of an appropriate lattice Λ is due to the *Uniformization Theorem* a lattice, see Silverman [75, Theorem VI.5.1].

Two elliptic curves E_0 and E_1 are isomorphic if and only if the associated lattices Λ_0 and Λ_1 are homothetic. Since we only regard lattices up to homothety, we can always assume such a lattice Λ to be of the form $\Lambda = \langle 1, \lambda \rangle$ with some λ from the upper half plane $\mathbb{H}$. Further another bijection occurs as

$$\{\phi : E_0 \to E_1 \text{ isogeny}\} \qquad \longleftrightarrow \qquad \{\alpha \in \mathbb{C} \mid \alpha\Lambda_0 \subseteq \Lambda_1\}$$

for given elliptic curves E_0 and E_1 where $\Lambda_i := \langle 1, \lambda_i \rangle \subseteq \mathbb{C}$ with $\lambda_i \in \mathbb{H}$ denotes the lattice such that we have $E_i(\mathbb{C}) \cong \mathbb{C}/\Lambda_i$. It can be shown that the left hand side is also a ring and actually the bijection holds in form of ring isomorphisms.

Let E be an elliptic curve defined over K and Λ be the associated lattice to E. Again we write $\Lambda = \langle 1, \lambda \rangle$ with some $\lambda \in \mathbb{C}$ having positive imaginary part. Husemöller [38, Proposition 12.4.7] shows that E has complex multiplication if and only if λ fulfills a quadratic equation (which can also be seen in the considerations below) and that in this case we have

$$\mathcal{K} \;=\; \mathbb{Q}(\lambda) \quad \text{and} \quad \operatorname{End} E \;\cong\; \mathcal{O} \;\subseteq\; \Lambda.$$

From now on we consider an elliptic curve E over K with complex multiplication by $\mathcal{O}$ and corresponding lattice $\Lambda = \langle 1, \lambda \rangle$. Due to the correspondence of isogenies to certain complex numbers as seen above we get

$$\operatorname{End} E \;\cong\; \{\alpha \in \mathbb{C} \mid \alpha\Lambda \subseteq \Lambda\}$$

with isomorphism of rings.

So the representation of Λ and the condition in the endomorphism ring leads to the existence of some $a, b, c, d \in \mathbb{Z}$ which fulfill

$$\begin{aligned} \alpha &= a + b\lambda \\ \alpha\lambda &= c + d\lambda \end{aligned}$$

for any $\alpha \in \operatorname{End} E$ such that in the end we get the quadratic equation

$$b\lambda^2 + (a-d)\lambda - c \;=\; 0.$$

Canceling out possible common divisors, λ satisfies a quadratic equation

$$A\lambda^2 + B\lambda + C \;=\; 0$$

with $\gcd(A, B, C) = 1$ and discriminant $D = B^2 - 4AC$. Theorem 8.1 from Lang [48] then tells us that under this circumstances we have

$$\operatorname{End} E \;\cong\; \left\langle 1, \tfrac{D+\sqrt{D}}{2} \right\rangle \;=:\; \mathcal{O}.$$

Note that we have $D = d_{\mathcal{O}}$. Thus we can determine the endomorphism ring of an elliptic curve E over a number field through calculating its discriminant when we know the lattice $\langle 1, \lambda \rangle$ by finding coprime $A, B, C \in \mathbb{Z}$ with $A\lambda^2 + B\lambda + C = 0$ and computing $D = B^2 - 4AC$. When we are able to determine the discriminant of the order $\mathcal{O}$ isomorphic to $\operatorname{End} E$ in some other way, we also have already found the order $\mathcal{O}$. This will be used in the next section.

3.2 The Characteristic Zero Picture

In this chapter we are interested in the relation of the endomorphism rings of isogenous elliptic curves which are defined over a number field $K \subset \mathbb{C}$. We will present an arrangement of those curves in a level structure and investigate how these levels are connected via isogenies of a given prime degree.

For this, the theory of complex multiplication as briefly described above can be used to characterize the number and type of outgoing isogenies for each elliptic curve defined over a number field depending on its endomorphism ring. We will analyze this behavior now.

Before we begin with the main part, we state two propositions which hold for elliptic curves over number fields with complex multiplication as well as for some defined over a finite field. The only requirement is the form of the endomorphism ring as an order in an imaginary quadratic field.

Proposition 3.1. *Let E_0 and E_1 be elliptic curves defined over a field K such that their endomorphism rings are isomorphic to orders $\mathcal{O}_0$ resp. O_1 in an imaginary quadratic field $\mathcal{K}$ and let $\phi : E_0 \to E_1$ be an isogeny of prime degree ℓ. Then we have*

$$\mathcal{O}_i \subseteq \mathcal{O}_{1-i} \text{ and } [\mathcal{O}_{1-i} : \mathcal{O}_i] \mid \ell$$

for $i = 0$ or $i = 1$.

Note that we already stated this result for ordinary elliptic curves as Proposition 2.44 which is attributed to Kohel [45]. The proof used only the structure of the endomorphism ring, so it works for elliptic curves with complex multiplication as well. The difference to the case of ordinary elliptic curves over finite fields is, that Proposition 2.42 cannot hold here since we do not have a distinct Frobenius endomorphism π_q which gives us a bottom level, so we have potentially more levels here than in the ordinary situation.

Analogue to isogenies between ordinary elliptic curves over finite fields like in Section 2.1.1 we call the isogeny $\phi : E_0 \to E_1$ between elliptic curves E_0, E_1 defined over a number field *ascending*, *descending* or *horizontal* depending on the relation of the endomorphism rings of E_0 and E_1, and elliptic curves with the same endomorphism ring are on the same *level*.

The *top level* which consists of elliptic curves with the maximal order of $\mathcal{K}$ as endomorphism ring will usually be denoted with V_0 and also called *crater*. The *distance* of a level from the surface is the power of ℓ dividing the conductor of curves on the level. The level with distance k to the top is labeled V_k. When we want to emphasize the order belonging to each level, we also talk about *the level* $\mathcal{O}$, so for instance the top level is labeled with $\mathcal{O}_K$.

Let E be an elliptic curve defined over some field K. We denote the set of isogenies starting at E with $\operatorname{Hom}(E, \cdot)$.

Proposition 3.2. *Let E be an elliptic curve defined over a field K so that* $\operatorname{End} E$ *is an order in an imaginary quadratic field and let ℓ be a prime that in the case of* $\operatorname{char} K = p > 0$ *is coprime to p.*

Then there are $\ell + 1$ non-equivalent isogenies of degree ℓ in $\operatorname{Hom}(E, \cdot)$.

Proof. Since these so-called *outgoing isogenies* correspond to cyclic subgroups of the ℓ-torsion group $E[\ell]$, we can determine how many of them exist by looking at the possible subgroups. We know from Proposition 2.21 that in our situation we have

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

and all subgroups of $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ are generated by $(1, 0)$ and $(i, 1)$ where i varies over all ℓ elements of $\mathbb{Z}/\ell\mathbb{Z}$. This yields exactly $\ell + 1$ subgroups and thus $\ell + 1$ outgoing isogenies from E, one for each subgroup. □

This result is very important for our work since the outgoing isogenies will be edges in our isogeny graphs and thus these graphs are $\ell + 1$-regular. We can also determine the form of the elliptic curves which are reached by those isogenies.

Remark. When write $\phi_i : E \to E_i$ with $i \in \{0, \cdots, \ell\}$ for the ℓ-isogenies arising from Proposition 3.2, the image curves E_i of them are called *ℓ-neighbors* of E.

When E is defined over a number field $K \subseteq \mathbb{C}$ with $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ for a lattice $\Lambda = \langle 1, \lambda \rangle$, the kernels of the outgoing isogenies have to be subgroups of order ℓ of

$$E[\ell] \cong \left\{ \tfrac{1}{\ell} (x + y\lambda) + \Lambda \mid x, y \in \mathbb{Z} \right\} =: M \subseteq \mathbb{C}/\Lambda.$$

If we use the isomorphism from $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ to $E[\ell]$ before that, we get an isomorphism

$$\begin{array}{rcl} Z/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z} & \to & M \\ (x, y) & \mapsto & \tfrac{1}{\ell} (x + y\lambda) + \Lambda \end{array}$$

and the generators of the possible subgroups of $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ from above yield the generators of order-ℓ-subgroups of $E[\ell]$ as the preimages of $\frac{1}{\ell} + \Lambda$ and $\frac{i+\lambda}{\ell} + \Lambda$ for $i \in \{1, \cdots, \ell\}$.

By the fundamental homomorphism theorem the image curves of the isogenies with those kernels are isomorphic to elliptic curves E_i with $E_i(\mathbb{C}) \cong \mathbb{C}/\Lambda_i$ where $\Lambda_0 = \langle 1, \ell\lambda \rangle$ and $\Lambda_i = \langle \ell, i + \lambda \rangle$ for $i \in \{1, \cdots, \ell\}$.

We will need the explicit descriptions of those image curves later.

Now that we have defined the levels of elliptic curves defined over number fields, we want to see how they are linked to each other with isogenies. Afterwards we will examine the connectedness within a single level in dependence of the given isogeny degree.

3.2.1 Vertical Connections Between Levels

In this section we want to show how the previously described levels are connected to each other. All elliptic curves are defined over a number field $K \subseteq \mathbb{C}$ if not stated otherwise. We will use the result described in the beginning of Section 3 about the order which is isomorphic to the endomorphism ring of an elliptic curve E being determined by its discriminant $D = d_E$. This can be computed by the coprime integers A, B and C from the equation $A\lambda^2 + B\lambda + C = 0$ where λ is the generator of the lattice corresponding to E.

Especially, this is also true for all ℓ-neighbors E_i of E, so that for finding their endomorphism rings it suffices to determine their discriminants in relation to the discriminant d_E. In particular, their discriminants are just the same as the discriminants d_{E_i} of the orders $\mathcal{O}_i$ in $\mathcal{K}$ which are isomorphic to $\operatorname{End} E_i$, so when one of the O_i has a discriminant D, $D \cdot \ell^2$ or D/ℓ^2, the ℓ-isogeny from E to this curve will be horizontal, descending resp. ascending due to our convention after Proposition 3.1.

This can be used to investigate the outgoing ℓ-isogenies from E like in the proof of Theorem 4 of Galbraith [27]. The kernel of such an isogeny has to be a subgroup of $E(\mathbb{C})$ with exactly ℓ elements and we have seen in the remark after Proposition 3.2 that the image curves from those isogenies are elliptic curves E_i with $E_0(\mathbb{C}) \cong \mathbb{C}/\Lambda_i$ and $\Lambda_0 = \langle 1, \ell\lambda \rangle$ resp. $\Lambda_i = \langle \ell, \lambda + i \rangle$ for $i \in \{1, \cdots, \ell\}$.

For each of the E_i we can use the generators of the lattice Λ_i to get a quadratic equation and based on the information on λ deduce the form of the discriminant from that. We will demonstrate the method for E_0 and refer to Galbraith [27] for the details of the lengthy calculations in the other cases.

We set $\lambda_0 := \ell\lambda$ and since we have $A\lambda^2 + B\lambda + C = 0$, we get

$$\underbrace{A}_{=:A_0}\lambda_0^2 + \underbrace{\ell B}_{=:B_0}\lambda_0 + \underbrace{\ell^2 C}_{=:C_0} = 0.$$

Note that we required the coefficients to be coprime to be able to use the theorem of Lang about the structure of the endomorphism ring. So in the situation with $\gcd(A_0, B_0, C_0) = 1$, $\ell \nmid A$ has to be true and we get the discriminant

$$\begin{aligned} D_0 &= B_0^2 - 4A_0C_0 \\ &= \ell^2 B^2 - 4\ell^2 AC \\ &= D \cdot \ell^2, \end{aligned}$$

so the isogeny ϕ_0 from E to E_0 is descending.

When the gcd-condition does not hold, $A = A_0$ has to be divisible by ℓ and we have $\gcd(A_0, B_0, C_0) \in \{\ell, \ell^2\}$. In the first case we divide ℓ out of the coefficients to attain $\gcd(\frac{A_0}{\ell}, \frac{B_0}{\ell}, \frac{C_0}{\ell}) = 1$, $\frac{A_0}{\ell}\lambda_0^2 + \frac{B_0}{\ell}\lambda_0 + \frac{C_0}{\ell} = 0$ and

$$\begin{aligned} D_0 &= \left(\tfrac{B_0}{\ell}\right)^2 - 4\tfrac{A_0}{\ell}\tfrac{C_0}{\ell} \\ &= B^2 - 4AC \\ &= D \end{aligned}$$

which implies that $\phi_0 : E \to E_0$ is a horizontal isogeny, whereas in the latter case we have to cancel ℓ^2 to get an analogous equation with coprime coefficients $\frac{A_0}{\ell^2}$, $\frac{B_0}{\ell^2}$ and $\frac{C_0}{\ell^2}$ which yields

$$\begin{aligned} D_0 &= \left(\tfrac{B_0}{\ell^2}\right)^2 - 4\tfrac{A_0}{\ell^2}\tfrac{C_0}{\ell^2} \\ &= \tfrac{B^2-4AC}{\ell^2} \\ &= D/\ell^2 \end{aligned}$$

and provides an ascending isogeny ϕ_0.

Let $\ell \mid A$. We want to emphasize that the ascending isogeny can only occur if ℓ also divides the conductor c with $d_E = c^2 d_{\mathcal{K}}$ and that in the other case a horizontal isogeny arises. If $\ell \nmid B$ this is due to the fact that $\left(\frac{c^2}{\ell}\right)\left(\frac{d_{\mathcal{K}}}{\ell}\right) = \left(\frac{d_E}{\ell}\right) = \left(\frac{B^2}{\ell}\right) = 1$, hence $\ell \nmid c$, ℓ splits in $\mathcal{K}$ and since we have $\gcd(A_0, B_0, C_0) = \ell$, we get a horizontal isogeny as shown above. When on the other hand $\ell \mid B$, we have the condition $\left(\frac{c^2}{\ell}\right)\left(\frac{d_{\mathcal{K}}}{\ell}\right) = \left(\frac{d_E}{\ell}\right) = 0$ so $\ell \mid c$ or $\ell \mid d_{\mathcal{K}}$ has to hold.

Let in this case $\ell \nmid c$ and $\ell > 2$ divide $d_{\mathcal{K}}$. Since $d_{\mathcal{K}}$ has no odd square factors,

ℓ^2 can neither divide $d_\mathcal{K}$ nor $c^2 d_\mathcal{K} = d_E = B^2 - 4AC$ and thus also $\ell^2 \nmid A$. This yields a horizontal isogeny with the described method. For $\ell = 2$ we know $\ell^2 \mid d_\mathcal{K}$ and the fundamental discriminant is $d_\mathcal{K} = 4d$ with $d \equiv 2, 3 \pmod 4$. Canceling the factor 4 out of the equation for d_E yields $c^2 d = \frac{B^2}{4} - AC$ and assuming $4 \mid A$ gives a contradiction to the form of d since then we had $c^2 d \equiv d \equiv \left(\frac{B}{2}\right)^2 \equiv 0, 1 \pmod 4$. Therefore $\ell^2 \nmid A$ and we have the same situation as for $\ell > 2$. So if ℓ ramifies in $\mathcal{K}$ and $\ell \nmid c$, the isogeny $\phi_0 : E \to E_0$ is horizontal.

Let now ℓ divide c, so it has also to divide $d_E = c^2 d_\mathcal{K}$ quadratically and thus for $\ell \neq 2$ we get $\ell^2 \mid A$ which leads to $\gcd(A_0, B_0, C_0) = \ell^2$ and an ascending isogeny in the way explained above. In the case $\ell = 2$ let $c = 2c'$ and consider the equation $c'^2 d_\mathcal{K} = \frac{B^2}{4} - AC$ again. This time we want an ascending isogeny, so suppose contradictorily that $4 \nmid A$. In that case $AC \equiv 2 \pmod 4$ and thus $c'^2 d_\mathcal{K} \equiv \left(\frac{B}{2}\right)^2 - 2 \equiv 2, 3 \pmod 4$ which is not possible since both c'^2 and $d_\mathcal{K}$ are 0 or 1 modulo 4. This concludes the investigation of the isogeny to the image curve E_0.

For the other ℓ image curves E_i we have to find quadratic equations for $\lambda_i := \frac{\lambda + i}{\ell}$ and investigate them in a similar way to see in which direction the isogeny from E to E_i leads. See Galbraith [27] for the details and results. Summed up we can make a case differentiation and gain the following theorem.

Theorem 3.3. *Let $\mathcal{K}$ be an imaginary quadratic field with maximal order $\mathcal{O}_\mathcal{K}$ and fundamental discriminant $d_\mathcal{K}$, E be an elliptic curve defined over a number field $K \subseteq \mathbb{C}$ whose endomorphism ring is isomorphic to an order with discriminant $d_E = c^2 d_\mathcal{K}$ for the conductor c in $\mathcal{K}$. Let ℓ be a prime.*

- *If $\ell \nmid c$, we have $\left(\frac{d_\mathcal{K}}{\ell}\right) = \left(\frac{d_E}{\ell}\right)$ and*
  - *two horizontal and $\ell - 1$ descending isogenies of degree ℓ which start at E if ℓ splits in $\mathcal{K}$,*
  - *ℓ descending isogenies and one horizontal outgoing isogeny from E if ℓ ramifies in $\mathcal{K}$,*
  - *$\ell + 1$ isogenies going down from E if ℓ is inert in $\mathcal{K}$.*
- *If $\ell \mid c$, we have ℓ descending isogenies and one ascending isogeny from E.*

If we arrange elliptic curves over K according to the levels of their endomorphism rings and connect them via ℓ-isogenies, the such arising graph is – apart from possible loops on the crater – almost a tree and quite large. However, we will see later that part of its structure can be transmitted to the corresponding graph in finite characteristic and that this tree can be cut off to become a slightly smaller graph.

Modular Functions And The Modular Polynomial. We mentioned the modular polynomial Φ_ℓ before and want to introduce its background briefly here. In this part we regard the *modular group* $\Gamma := \mathrm{SL}(2,\mathbb{Z})$ which acts transitively on the upper halfplane $\mathbb{H}$ through

$$\begin{array}{rcl} * : \Gamma \times \mathbb{H} & \to & \mathbb{H} \\ \left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), z \right) & \mapsto & \frac{az+b}{cz+d}. \end{array}$$

For fixed $A \in \Gamma$ we use the notation π_A to denote the function on $\mathbb{H}$ sending $z \in \mathbb{H}$ to $A * z$. Let ℓ be an integer, then we define

$$\Gamma_0(\ell) \quad := \quad \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \;\middle|\; c \equiv 0 \pmod{\ell} \right\}$$

which is a subgroup of Γ. Note that we have $\Gamma = \Gamma_0(1)$.

Definition. Let ℓ be an integer and $G := \Gamma_0(\ell)$ be a subgroup of Γ. A *modular function for* G is a function $f : \mathbb{H} \to \mathbb{C}$ which is invariant for G and meromorphic on $\mathbb{H}$ and on the cusps[4].

There exists a modular function $j : \mathbb{H} \to \mathbb{C}$ for Γ with

$$j(\lambda) \quad = \quad 1728 \frac{g_2^3(\lambda)}{g_2^3(\lambda) - 27 g_3^2(\lambda)}$$

where $g_2(\lambda)$ and $g_3(\lambda)$ are constants corresponding to the lattice $\Lambda := \langle 1, \lambda \rangle$. Since such lattices correspond to elliptic curves, $j(\lambda)$ can be interpreted as a constant for the elliptic curve E with $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ and in fact it is the j-invariant $j(E)$ of E. For more information on these objects consult Cox [16] or Lang [48].

This modular function j induces a bijection

$$j : \mathbb{H}/\Gamma \quad \to \quad \mathbb{C}$$

and thus we see

$$\begin{array}{rcll} j(\lambda_0) = j(\lambda_1) & \iff & \exists A \in \Gamma : & \lambda_1 = A * \lambda_0 \\ & \iff & \exists A \in \Gamma : & \Lambda_1 = \langle 1, A * \lambda_0 \rangle. \end{array}$$

[4] *meromorphic on the cusps* means that for all $A \in \Gamma$ the negative part of the Laurent expansion of $f \circ \pi_A$ does not have infinitely many coefficients, see Cox [16], Chapter 11.B.

Furthermore we have that every modular function for Γ is an element of $\mathbb{C}(j)$. If f is a modular function for Γ and ℓ is an integer, the function $g := f \circ \ell$ mapping z to $f(\ell z)$ is a modular function for $\Gamma_0(\ell)$. In fact, the set of all modular functions for $\Gamma_0(\ell)$ is $\mathbb{C}(j, j \circ \ell)$.

Proposition 3.4. *Let ℓ be an integer and $\Phi_{\ell,j} \in \mathbb{C}(j)[X]$ be the minimal polynomial of $j \circ \ell$. Then $\Phi_{\ell,j}$ is a polynomial in $\mathbb{C}[X, j]$ with degree $d := [\Gamma : \Gamma_0(\ell)]$. It can be written as*

$$\Phi_{\ell,j} = \prod_{i=1}^{d} (X - j \circ \ell \circ \pi_{A_i})$$

where for $A_i \in \Gamma$, $i \in \{1, \cdots, d\}$ the sets $\Gamma_0(\ell)A_i$ are representatives for the right cosets of $\Gamma_0(\ell)$ in Γ.

Hence there is a two-variable polynomial $\Phi_\ell \in \mathbb{C}[X, Y]$ with

$$\Phi_\ell(\cdot, j(\lambda)) = \prod_{i=1}^{d} (X - j(\ell \cdot (A_i * \lambda)))$$

for $\lambda \in \mathbb{H}$. This polynomial is called the *ℓ-modular polynomial* and is actually a symmetric polynomial from $\mathbb{Z}[X, Y]$. If ℓ is a prime, Φ_ℓ has degree $\ell + 1$ and fulfills

$$\Phi_\ell \equiv (X^\ell - Y)(X - Y^\ell) \pmod{\ell\, \mathbb{Z}[X, Y]}.$$

Let E_0 be an elliptic curve over a number field $K \subseteq \mathbb{C}$ such that we have $E(\mathbb{C}) \cong \mathbb{C}/\Lambda_0$ with $\Lambda_0 = \langle 1, \lambda_0 \rangle \subseteq \mathbb{C}$, so E_0 has j-invariant $j(\lambda_0)$. Let $z \in \mathbb{C}$ be a root of $\Phi_\ell(\cdot, j(\lambda_0))$, so we get due to the splitting of the polynomial in linear factors that $z = j(\ell \cdot (A * \lambda_0))$ is true with $A \in \Lambda$ being a representative of the right cosets of $\Gamma_0(\ell)$ in Γ.

We regard an elliptic curve defined over a number field $K \subseteq \mathbb{C}$ with analogous corresponding lattice Λ_1 and j-invariant $j(\lambda_1) = z$. Then we get

$$j(\lambda_1) = j(\ell \cdot (A * \lambda_0)) \iff \exists B \in \Gamma : \quad \Lambda_1 = \langle 1, \ell \cdot BA * \lambda_0 \rangle.$$

Due to the remark after Proposition 3.2 this is equivalent to E_1 being ℓ-isogenous to an elliptic curve E' given by the lattice $\Lambda' = \langle 1, BA * \lambda_0 \rangle =: \langle 1, \lambda' \rangle$. Since further $\lambda' = BA * \lambda_0$ is equivalent to $j(\lambda') = j(\lambda_0)$ this means that we get $E' \cong E_0$ and have an isogeny $\phi : E_0 \to E_1$ with degree $\deg \phi = \ell$. So in the end we get the following fundamental property.

Proposition 3.5. *Let E_0, E_1 be elliptic curves defined over a number field $K \subseteq \mathbb{C}$ with j-invariants j_0 resp. j_1 and let ℓ be a prime. Then there exists an isogeny $\phi : E_0 \to E_1$ of degree ℓ if and only if $\Phi_\ell(j_0, j_1) = 0$.*

This result is of great importance for our work with isogenies since it enables us to compute ℓ-neighbors of a given elliptic curve over a number field $K \subseteq \mathbb{C}$. It can also be found for example in Lang [48], Theorem 5.3.5.

3.2.2 Horizontal Links and the Ideal Class Group

Now we want to investigate single levels of this isogeny graph, that is, the set of elliptic curves defined over a number field $K \subseteq \mathbb{C}$ which have the same given endomorphism ring. Per definition, any isogeny between such curves has to be horizontal. We have seen in Theorem 3.3 that such isogenies only exist when their degree does not divide the conductor of the endomorphism ring and is not inert in the overlying imaginary quadratic field $\mathcal{K}$.

Even if there are horizontal isogenies of degree ℓ, it is not yet guarantied that the level is completely connected when we use them as edges in the graph. We will now see how we can achieve full connectedness of a given level. The essential knack is to regard isogenies of different degrees.

Let E_Λ denote the elliptic curve defined over K associated to a lattice Λ having complex multiplication by $\mathcal{O}$ which is an order in an imaginary quadratic field $\mathcal{K}$. Further let $\Lambda = \langle 1, \lambda \rangle$ where $A\lambda^2 + B\lambda + C = 0$ with coprime integers A, B, C is the equation like in the last part. We have seen in the beginning of the chapter that in this case we have $\mathcal{K} = \mathbb{Q}(\lambda)$ and $\mathcal{O} \subseteq \Lambda$. It is easy to show that $A\Lambda$ is an ideal in $\mathcal{O}$, so Λ can be regarded as a fractional ideal in $\mathcal{O}$. Since every fractional ideal in imaginary quadratic fields is a $\mathbb{Z}$-module of rank two, it is also a lattice and we will denote both concepts with Λ simultaneously.

Let now $\Theta = \theta\mathcal{O}$ with $0 \neq \theta \in \mathcal{O}$ be a principal ideal of $\mathcal{O}$. Then $\Theta\Lambda = \theta\Lambda$ is – as a lattice – homothetic to Λ and thus yields an elliptic curve in the same isomorphism class as E_Λ. On the other hand every elliptic curve which is isomorphic to E_Λ has an associated lattice that is homothetic to Λ and thus – as an ideal – emerges from multiplying Λ with a principal ideal.

Hence when regarding isomorphism classes of elliptic curves, principal ideals can be neglected and the isomorphism class of the elliptic curve E_Λ only depends on the ideal class $[\Lambda]$ in $\mathcal{C}\ell(\mathcal{O})$. Due to Corollary C.11.1.1. of Silverman [75], the set of isomorphism classes of elliptic curves defined over number fields with endomorphism ring isomorphic to $\mathcal{O}$ is finite. Thus K can be taken to be the maximal number field such that all elliptic curves with endomorphism ring $\mathcal{O}$ are defined over K and with this K we set

$$\mathcal{E}\ell\ell_K(\mathcal{O}) \quad := \quad \{\text{elliptic curves over } K \text{ with endomorphism ring } \mathcal{O}\}/_{\cong}.$$

Proposition C.11.1 of Silverman [75] and Proposition II.1.2 of Silverman [74] show the following result.

Proposition 3.6. *Let $\mathcal{O}$ be an order in the imaginary quadratic field $\mathcal{K}$. There is a one-to-one correspondence*

$$\mathcal{C}\ell(\mathcal{O}) \quad \longleftrightarrow \quad \mathcal{E}\ell\ell_K(\mathcal{O})$$

between ideal classes of $\mathcal{O}$ and isomorphism classes of elliptic curves over a number field with endomorphism ring isomorphic to $\mathcal{O}$. Moreover, the map

$$\begin{array}{rrcl} \star: & \mathcal{C}\ell(\mathcal{O}) \times \mathcal{E}\ell\ell_K(\mathcal{O}) & \to & \mathcal{E}\ell\ell_K(\mathcal{O}) \\ & ([\mathfrak{a}], E_\Lambda) & \mapsto & [\mathfrak{a}] \star E_\Lambda := E_{\mathfrak{a}^{-1}\Lambda} \end{array}$$

is well-defined and makes the ideal class group of $\mathcal{O}$ act simply transitive on the isomorphism classes of elliptic curves with fixed endomorphism ring $\mathcal{O}$.

We will see that in this setting isogenies can be represented as ideal classes, too, so $[\mathfrak{a}]$ corresponds to an isogeny $\phi_{[\mathfrak{a}]} : E_\Lambda \to E_{\mathfrak{a}^{-1}\Lambda}$. When we take an integral ideal $\mathfrak{a}$ from $[\mathfrak{a}]$, we always have $\Lambda \subseteq \mathfrak{a}^{-1}\Lambda$ since obviously $\mathfrak{a}\Lambda \subseteq \Lambda$ is true. Thus $\mathbb{C}/\Lambda$ can be embedded with a homomorphism into $\mathbb{C}/\mathfrak{a}^{-1}\Lambda$ and we get the following commutative diagram.

$$\begin{tikzcd} \mathbb{C}/\Lambda \arrow[r, "z \mapsto z"] \arrow[d, leftrightarrow] & \mathbb{C}/\mathfrak{a}^{-1}\Lambda \arrow[d, leftrightarrow] \\ E_\Lambda \arrow[r, "\phi_{[\mathfrak{a}]}"] & E_{\mathfrak{a}^{-1}\Lambda} = [\mathfrak{a}] \star E_\Lambda \end{tikzcd}$$

So we have an isogeny $\phi_{[\mathfrak{a}]} : E_\Lambda \to E_{\mathfrak{a}^{-1}\Lambda}$ and every isogeny $\phi : E_{\Lambda_0} \to E_{\Lambda_1}$ can be found this way since there exists an ideal $\mathfrak{a}$ such that $\Lambda_1 = \mathfrak{a}^{-1}\Lambda_0$. Proposition II.1.4 of Silverman [74] shows now that the kernel of this isogeny is

$$\ker \phi_{[\mathfrak{a}]} = E_\Lambda[\mathfrak{a}] \quad := \quad \{P \in E_\Lambda \mid [\alpha]P = O_{E_\Lambda} \text{ for all } \alpha \in \mathfrak{a}\}.$$

Remember that here $[\alpha]$ is the image of the element $\alpha \in \mathfrak{a} \subseteq \mathcal{O}$ under the fixed isomorphism $[\cdot] : \mathcal{O} \to \operatorname{End} E_\Lambda$ and thus an endomorphism of E_Λ whereas $[\mathfrak{a}]$ is the ideal class of $\mathfrak{a}$ in $\mathcal{C}\ell(\mathcal{O})$. Furthermore the same proposition tells us that this set is a free $\mathcal{O}/\mathfrak{a}$-module of rank 1. This implies $E_\Lambda[\mathfrak{a}] \cong \mathcal{O}/\mathfrak{a}$ and therefore we get

$$\deg \phi_{[\mathfrak{a}]} = \#E_\Lambda[\mathfrak{a}] = \#\mathcal{O}/\mathfrak{a} = \mathrm{N}(\mathfrak{a})$$

with the absolute ideal norm of $\mathfrak{a}$. So any isogeny of degree ℓ can be associated with an integral ideal of norm ℓ and we get the next result.

Proposition 3.7. *Let E_Λ be an elliptic curve defined over a number field K with endomorphism ring isomorphic to an order $\mathcal{O}$ in an imaginary quadratic field $\mathcal{K}$ and let ℓ be a prime. There is a correspondence*

$$\{\phi \in \operatorname{Hom}(E_\Lambda, \cdot) \mid \deg \phi = \ell\} \quad \longleftrightarrow \quad \{\mathfrak{a} \subseteq \mathcal{O} \text{ integral ideal} \mid \mathrm{N}(\mathfrak{a}) = \ell\}$$

where $\operatorname{Hom}(E_\Lambda, \cdot)$ denotes the set of outgoing isogenies from E_Λ with arbitrary image curves.

When we take two arbitrary elliptic curves E_Λ and $E_{\Lambda'}$ from $\mathcal{E}\ell\ell_K(\mathcal{O})$, we know that there exists an integral ideal $\mathfrak{a} \subseteq \mathcal{O}$ so that we have $E_{\Lambda'} = [\mathfrak{a}] \star E_\Lambda$. Let now B be a fixed positive integer such that $\mathcal{C}\ell(\mathcal{O})$ is generated by the ideal classes of all integral ideals with prime norm less or equal to B. Then we can write $[\mathfrak{a}] = [\mathfrak{a}_1] \cdots [\mathfrak{a}_n]$ where the integral ideals $\mathfrak{a}_i$ have prime norm $\ell_i \leq B$. With $\Lambda_0 := \Lambda$ we can now construct a sequence of lattices Λ_i for $i \in 1, \cdots, n$ with $\Lambda_i = \mathfrak{a}_i^{-1} \Lambda_{i-1}$ and $\Lambda_n = \Lambda'$.

Thereby we get elliptic curves $E_{\Lambda_i} \in \mathcal{E}\ell\ell_K(\mathcal{O})$ and isogenies $\phi_i : E_{\Lambda_{i-1}} \to E_{\Lambda_i}$. Due to the construction it is $\phi_i = \phi_{[\mathfrak{a}_i]}$, so we have $\deg \phi_i = \ell_i \leq B$. After all we found a chain of isogenies

$$E_\Lambda = E_{\Lambda_0} \xrightarrow{\phi_1} E_{\Lambda_1} \xrightarrow{\phi_2} \cdots \xrightarrow{\phi_n} E_{\Lambda_n} = E_{\Lambda'}$$

which provides an isogeny

$$\phi = \phi_n \circ \cdots \circ \phi_1 : \; E_\Lambda \to E_{\Lambda'}$$

with $\deg \phi = \ell_1 \cdots \ell_n$.

Thus when we take $\mathcal{L}$ to be the set of primes less or equal to B we can find an isogeny with $\mathcal{L}$-smooth degree between any two elliptic curves in $\mathcal{E}\ell\ell_K(\mathcal{O})$. This means that the graph consisting of such curves as nodes is fully connected if we allow all isogenies of prime degree less or equal to B as edges. This is an important result which we will use quite a few times in the course of this work.

Especially for complexity questions it is interesting how small the bound B can be chosen so that the classes of ideals with norm less or equal to B still generate the ideal class group $\mathcal{C}\ell(\mathcal{O})$. For $\mathcal{O} = \mathcal{O}_{\mathcal{K}}$ there are some theoretical estimations for that.

A theorem of MINKOWSKI (for instance see LANG [49, THEOREM V.4]) says that in every ideal class there is an integral ideal $\mathfrak{a}$ with $\mathrm{N}(\mathfrak{a}) \leq C_{\mathcal{K}}\sqrt{d_{\mathcal{K}}}$ where the constant $C_{\mathcal{K}}$ is in our quadratic case either $1/2$ or $2/\pi$. There have been endeavors to improve this constant like displayed in ZIMMERT [95] but nevertheless the implied unconditional bound is exponential in terms of $\log d_{\mathcal{K}}$.

A better bound which relies on a Generalized RIEMANN Hypothesis has been developed by BACH in [1] and makes use of *characters* χ which are functions on $\mathcal{O}_{\mathcal{K}}$-ideals. Such characters appear in *Hecke L-functions* along with the norm of ideals $\mathfrak{a}$ as

$$L_\chi \quad := \quad \sum_{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{\mathrm{N}(\mathfrak{a})}.$$

A form or the Generalized RIEMANN Hypothesis states that L_χ has no zeros on the halfplane with $\operatorname{Re} s > \frac{1}{2}$. Under this conjecture he can make explicit estimates and obtain bounds for ideals of least norm of with character different from 0 or 1. The analytical methods go beyond the topic of this thesis, but BACH concludes with a directly applicable conclusion from THEOREM 4 on page 376 of his work, which provides the following most useful statement.

THEOREM 3.8 (BACH'S Bound). *Let $\mathcal{K}$ be a field with discriminant $d_{\mathcal{K}}$ and $\mathcal{O}_{\mathcal{K}}$ be the maximal order of $\mathcal{K}$. Under the assumption of the Generalized* RIEMANN *Hypothesis the class group of $\mathcal{C}\ell(\mathcal{O}_{\mathcal{K}})$ is generated by the prime ideals of norm less or equal to $B = 12(\log|d_{\mathcal{K}}|)^2$.*

If $\mathcal{K}$ is a quadratic field, this bound can be improved to $B = 6(\log|d_{\mathcal{K}}|)^2$.

We will refer to this number B as *the* BACH *bound* later. In BELABAS - DIAZ Y DIAZ - FRIEDMANN [2] another bound is suggested which is asymptotically worse than the BACH bound but often better in practice. In our computations we usually take a much smaller bound (in most of the cases $B = 20$ suffices) to favor faster algorithms with the occasional chance of an error or endless loop over precise but slow algorithms.

REMARK. We will use the BACH bound to assert the existence of an isogeny between two elliptic curves over a finite field $\mathbb{F}_q$ with endomorphism ring isomorphic to the maximal order $\mathcal{O}_{\mathcal{K}}$ of an imaginary quadratic field $\mathcal{K}$. However, in some cases it would be useful to compute an isogeny between two such elliptic curves where the endomorphism ring is isomorphic to an order $\mathcal{O}$ in $\mathcal{K}$ which is not maximal. In practice and in some literature, this is done with the bound $B := 6(\log |d_{\mathcal{O}}|)^2$. To justify this bound, the ideals of norm less or equal to this B have to generate $\mathcal{C}\ell(\mathcal{O})$, which is not given by Bach's paper [1] though and – to the authors knowledge – nowhere else in literature, too.

3.3 Lifting and Reduction

It looks desirable to have similar structure of outgoing isogenies for elliptic curves defined over finite fields as the precise description of the ones defined over number fields. Fortunately at least for ordinary elliptic curves there is a connection between such curves through lifting and reduction theory which preserves the endomorphism ring and also the number and type of outgoing isogenies. We will explain the strategy here and point out why it does not work completely for supersingular elliptic curves. Afterwards we make a modification on the famous Deuring theorems which allow us to transfer their results to at least a subset of supersingular elliptic curves.

3.3.1 Deuring's Theorems

Let E be an elliptic curve defined over a number field $K \subseteq \mathbb{C}$ with endomorphism ring $\operatorname{End} E$ isomorphic to an order $\mathcal{O}$ in an imaginary quadratic field $\mathcal{K}$. By a change of variables and eliminating denominators we can assure that the coefficients of the Weierstrass equation are from the ring of integers R_K of K.

Let now p be a prime and $\mathfrak{P}$ be a place over p, so $\mathfrak{P}$ is one of the prime ideals of the factorization of the ideal generated by p in R_K. Since R_K as the maximal order in a number field is a Dedekind domain, every prime ideal is also maximal and hence $R_K/\mathfrak{P}$ is a field. Since we have

$$\# R_K/\mathfrak{P} = \mathrm{N}(\mathfrak{P})$$

and the norm is multiplicative, this field is finite with characteristic p. So we get $R_K/\mathfrak{P} = \mathbb{F}_q$ where q is a power of p. Thus we can introduce a reduction map

$$\bar{\cdot}_{\mathfrak{P}} : R_K \quad \to \quad \mathbb{F}_q$$

and by using it on the coefficients of E we get another cubic equation with coefficients from $\mathbb{F}_q$. If the discriminant of this equation is nonzero, this reduction provides an elliptic curve $\bar{E}$ defined over $\mathbb{F}_q$ and we say that *E has good reduction at $\mathfrak{P}$*. We mostly denote this reduction map only with $\bar{\cdot}$ when there can be no risk of confusion about the used place $\mathfrak{P}$.

Deuring [19] explains what happens to the endomorphism ring of the elliptic curve E under such a reduction. The notation and setting of this paper is kind of unusual and unfit for our situation, so we refer to proofs of both the following theorems in Lang [48] where they are Theorems 13.12 and 13.14.

Theorem 3.9 (Deuring Reduction Theorem)**.** *Let E be an elliptic curve defined over a number field K, $\operatorname{End} E$ isomorphic to an order $\mathcal{O}$ in an imaginary quadratic field $\mathcal{K}$ and $\mathfrak{P}$ be a place over some prime p such that E has good reduction $\bar{E}$ modulo this place. Then we get*

$$\bar{E} \text{ is ordinary} \iff p \text{ splits in } \mathcal{K}.$$

Let in this case $c = p^r c_0$ be the conductor of $\operatorname{End} E$ in $\mathcal{K}$ such that $p \nmid c_0$. Then we get $\operatorname{End} \bar{E} \cong \mathbb{Z} + c_0\mathcal{O}_{\mathcal{K}}$ and $c_0 = c$ implies that the map

$$\begin{array}{rccc} \bar{\cdot} : & \operatorname{End} E & \to & \operatorname{End} \bar{E} \\ & \phi & \mapsto & \bar{\phi} \end{array}$$

is an isomorphism.

Note that this theorem says nothing about the structure of the endomorphism ring if the reduced elliptic curve is supersingular. But as this turns out to be important for our approach of the restricted supersingular isogeny problem in Section 4.2.2, we investigate it in the next section. Before that we present the behavior when going in the other direction and lift an elliptic curve defined over a finite field to an elliptic curve over a number field K.

Theorem 3.10 (Deuring Lifting Theorem)**.** *Let $\mathcal{K}$ be an imaginary quadratic field, $\mathbb{F}_q$ be a finite field with $\operatorname{char} \mathbb{F}_q = p > 0$ and E_0 be an elliptic curve defined over $\mathbb{F}_q$ with endomorphism ring isomorphic to an order $\mathcal{O}$ in $\mathcal{K}$. Further, fix some non-trivial $\phi_0 \in \operatorname{End} E_0$.*

Then there exist an elliptic curve E over a number field K, an endomorphism $\phi \in \operatorname{End} E$ and a good reduction $\bar{E}$ of E at a place $\mathfrak{P}$ over p such that we get $E_0 \cong \bar{E}$ and ϕ_0 is mapped to $\bar{\phi}$ under this isomorphism.

So – at least for ordinary elliptic curves – it is possible to navigate between elliptic curves defined over a finite field and ones defined over a number field and preserve the endomorphism ring of the occurring elliptic curves. Note that lifting is no problem for supersingular elliptic curves defined over $\mathbb{F}_q$ but the reduction theorem yields no result for the behavior of the endomorphism rings of curves which reduce to such a supersingular one.

As a last point we want to examine the behavior of isogenies between elliptic curves under reduction. With the notation from above we can state Proposition II.4.4 from Silverman [74] in the following way.

Lemma 3.11. *For two elliptic curves E_0 and E_1 defined over a number field $K \subseteq \mathbb{C}$ with endomorphism rings isomorphic to orders in an imaginary quadratic field $\mathcal{K}$ the map*

$$\begin{array}{rcl} \bar{\cdot}\ :\ \mathrm{Hom}(E_0, E_1) & \to & \mathrm{Hom}(\bar{E}_0, \bar{E}_1) \\ \phi & \mapsto & \bar{\phi} \end{array}$$

is injective and preserves degree.

Especially when we regard all isogenies in $\mathrm{Hom}(E_0, \cdot)$ with degree ℓ, they are mapped injectively on ℓ-isogenies in $\mathrm{Hom}(\bar{E}_0, \cdot)$. Since in both cases there are $\ell + 1$ such isogenies as seen in Proposition 3.2, this mapping is bijective. We may fix this result in a lemma, too.

Lemma 3.12. *For an elliptic curve E_0 defined over a number field $K \subseteq \mathbb{C}$ whose endomorphism ring is an order in an imaginary quadratic field $\mathcal{K}$ and which reduces to an ordinary elliptic curve $\bar{E}_0$ defined over $\mathbb{F}_q$, the map*

$$\begin{array}{rcl} \bar{\cdot}\ :\ \mathrm{Hom}(E_0, \cdot) & \to & \mathrm{Hom}(\bar{E}_0, \cdot) \\ \phi & \mapsto & \bar{\phi} \end{array}$$

is bijective.

Furthermore it turns out that all of those isogenies are defined over $\mathbb{F}_q$ in this case.

Proposition 3.13. *Let $\bar{E}_0$ be an ordinary elliptic curve defined over the finite field $\mathbb{F}_q$ of characteristic p. Let $\ell \neq p$ be a prime.*

Then we have $\mathrm{End}\,\bar{E}_0 = \mathrm{End}_{\mathbb{F}_q}\bar{E}_0$ *and all ℓ-isogenies to ordinary elliptic curves defined over $\mathbb{F}_q$ which start at $\bar{E}$ are equivalent to ones which can be defined over $\mathbb{F}_q$, too.*

Proof. We have $\mathrm{End}\,\bar{E}_0 = \langle [1], \phi \rangle = \mathrm{End}_{\mathbb{F}_q}\bar{E}_0$ where ϕ is π_q or $\frac{1+\pi_q}{2}$ depending on whether the endomorphism ring is isomorphic to $\mathbb{Z}[\sqrt{-p}]$ or $\mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$. Proposition 23.3 of Kohel [45] and his discussion after that yield the second statement. $\square$

Thus when we take the ℓ-level structure of elliptic curves defined over a number field provided by Theorem 3.3 and reduce the whole picture to characteristic p, elliptic curves E are mapped bijectively to elliptic curves $\bar{E}$ with the same endomorphism ring and ℓ-isogenies from $\mathrm{Hom}(E, \cdot)$ also bijectively to respective ones in $\mathrm{Hom}(\bar{E}, \cdot)$. Hence the whole picture can be transferred from characteristic 0 to p.

Note that due to PROPOSITION 2.42 the reduced curves are defined over $\mathbb{F}_q$ if and only if we have $\mathbb{Z}[\pi_q] \subseteq \operatorname{End}\bar{E}$, so if we regard reduced elliptic curves over $\mathbb{F}_q$ the graph has to be truncated and the lower levels are cut off.

3.3.2 Reduction to Supersingular Elliptic Curves

The reduction and resulting bijection between elliptic curves over number fields resp. finite fields with same endomorphism ring and the one concerning their isogenies does only work in this form for the case where the reduced elliptic curves are ordinary. In this section we want to investigate the problems and describe a partly solution and reparation of the supersingular case. We will regard the set of supersingular elliptic curves which are defined over $\mathbb{F}_p$ and call them *$\mathbb{F}_p$-rational supersingular elliptic curves.*

Let p be a prime and E be an elliptic curve defined over a number field $K \subseteq \mathbb{C}$ so that its good reduction $\bar{E}$ at a place $\mathfrak{P}$ over p is supersingular. Because $\operatorname{End}\bar{E}$ is an order in a quaternion algebra, it has rank four as a $\mathbb{Z}$-module and the reduction

$$\begin{array}{rccc} \bar{\cdot}\ : & \operatorname{End}E & \to & \operatorname{End}\bar{E} \\ & \phi & \mapsto & \bar{\phi} \end{array}$$

as in the DEURING Reduction Theorem cannot be an isomorphism since $\operatorname{End}E$ is still an order in an imaginary quadratic field and thus a $\mathbb{Z}$-module of rank 2. For that reason we regard the *restricted endomorphism ring* $\operatorname{End}_{\mathbb{F}_p}\bar{E}$ consisting of all endomorphisms which are defined over $\mathbb{F}_p$, also called *$\mathbb{F}_p$-rational* endomorphisms. Analogously $\operatorname{Hom}_{\mathbb{F}_p}(\bar{E}_0, \bar{E}_1)$ contains all $\mathbb{F}_p$-rational isogenies between the supersingular elliptic curves $\bar{E}_0$ and $\bar{E}_1$.

We want to investigate the following situation. Let $p > 3$ be a prime and let $\bar{E}$ denote a supersingular elliptic curve which is defined over $\mathbb{F}_p$ and lifted via the DEURING Lifting Theorem to an elliptic curve E over a number field K. Then PROPOSITION 3.2 says that for a prime $\ell \neq p$ there are $\ell + 1$ isogenies $\phi_i : E \to E_i$ with degree $\phi_i = \ell$ and image curves E_i over K (or a finite extension of K) for $i \in \{0, \cdots, \ell\}$.

The endomorphism rings of all E_i have to be orders in $\mathcal{K} = \mathbb{Q}(\sqrt{-p})$, too, since they are isogenous to E. Thus p ramifies in $\mathcal{K}$ and from the DEURING Reduction Theorem we know that all E_i reduce to supersingular elliptic curves $\bar{E}_i$ in characteristic p, so the reduced curves have to be defined over $\mathbb{F}_{p^2}$. The situation is sketched in the following diagram.

$$\begin{tikzcd} E/K \arrow[r, "\phi_i"] & E_i/K \arrow[d] \\ \bar{E}/\mathbb{F}_p \arrow[u] & \bar{E}_i/\mathbb{F}_{p^2} \end{tikzcd}$$

FIGURE 1: Lifting a Supersingular Elliptic Curve over $\mathbb{F}_p$

Several problems arise while regarding this setting. We want to examine them in the remainder of this section.

The primary questions we will investigate for supersingular elliptic curves in this setting are listed below.

- ✦ Which of the $\bar{E}_i$ are defined over $\mathbb{F}_p$?
- ✦ What is the relation of the endomorphism rings of E_i and $\bar{E}_i$?
- ✦ What happens to the isogenies ϕ_i under this reduction?

For ordinary curves these issues over $\mathbb{F}_q$ can be answered easily as we have seen: The $\bar{E}_i$ are defined over $\mathbb{F}_q$ if and only if we have $\mathbb{Z}[\pi_q] \subseteq \operatorname{End} \bar{E}_i$ (LEMMA 2.43), $\operatorname{End} E_i \cong \operatorname{End} \bar{E}_i$ (THEOREM 3.9) and there exists an isogeny $\bar{\phi}_i : \bar{E} \to \bar{E}_i$ defined over $\mathbb{F}_q$ which is the reduction of ϕ_i for every $i \in \{0, \cdots, \ell\}$ (LEMMA 3.12). We want to show similar results in our case.

We deal with the first question at the beginning and show the following.

PROPOSITION 3.14. *Let E be an elliptic curve defined over a number field K and let $\mathfrak{P}$ be a place over a prime $p > 3$ such that E has good reduction $\bar{E}$ which is a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$. Then we get*

$$\bar{E} \text{ is defined over } \mathbb{F}_p \quad \Longleftrightarrow \quad \sqrt{-p} \in \operatorname{End} \bar{E}$$

in the sense that there exists an element $\phi \in \operatorname{End} \bar{E}$ with $\phi^2 = [-p]$.

PROOF. This follows PROPOSITION 2.4 of DELFS-GALBRAITH [18].

If $\bar{E}$ is defined over $\mathbb{F}_p$, we know that the FROBENIUS π_p lies in $\operatorname{End} \bar{E}$ and for supersingular elliptic curves fulfills the characteristic equation $\pi_p^2 + [p] = 0$ for $p > 3$, so we get $\pi_p = \sqrt{-p} \in \operatorname{End} \bar{E}$. To complete the equivalence, we have to show that if the endomorphism ring of a supersingular elliptic curve in characteristic p contains an element $\sqrt{-p}$, then the curve is already defined over $\mathbb{F}_p$.

So let $\phi \in \operatorname{End} \bar{E}$ be an endomorphism with $\phi^2 = [-p]$. Since the degree is multiplicative and p is prime, we get $\deg \phi = p$. $\bar{E}$ is supersingular, so it has no points of order p and the kernel of ϕ^2 is trivial. With this, it is also impossible for the kernel of ϕ to contain more than just the identity element O_E. The number of points in the kernel is just the separable degree of ϕ and thus from

$$p = \deg \phi = \deg_s \phi \cdot \deg_i \phi = 1 \cdot \deg_i \phi$$

we see that ϕ is inseparable.

Due to LEMMA 2.2 we can find a separable isogeny ψ such that ϕ factors as

$$\begin{tikzcd} E \arrow[r, "\pi_p"] \arrow[rr, bend right, "\phi"'] & E^{(p)} \arrow[r, "\psi"] & E_1 \end{tikzcd}$$

and, again, the multiplicativity of the degree yields $\deg \psi = 1$. So we have $E^{(p)} \cong E$ and therefore $j(E) = j(E^{(p)}) = j(E)^p$. That implies that $j(E) \in \mathbb{F}_p$ is true and thus E is defined over $\mathbb{F}_p$. □

For later use we define

$$\mathcal{E}\ell\ell_{\mathbb{F}_p,s} \quad := \quad \mathcal{E}\ell\ell_{\mathbb{F}_p}(\mathbb{Z}[\sqrt{-p}]) \cup \mathcal{E}\ell\ell_{\mathbb{F}_p}(\mathcal{O}_{\mathcal{K}})$$

as the set of all $\mathbb{F}_p$-isomorphism classes of supersingular elliptic curves defined over $\mathbb{F}_p$ and the corresponding set in characteristic 0 as

$$\mathcal{E}\ell\ell_{K,s} \quad := \quad \mathcal{E}\ell\ell_K(\mathbb{Z}[\sqrt{-p}]) \cup \mathcal{E}\ell\ell_K(\mathcal{O}_{\mathcal{K}}).$$

As in the beginning of SECTION 3.2.2, K is the maximal number field such that all elliptic curves with endomorphism ring either $\mathbb{Z}[\sqrt{-p}]$ or $\mathcal{O}_{\mathcal{K}}$ are defined over K.

We want to establish a one-to-one correspondence between those two sets, so first we show that they have the same number of elements. From THEOREM 2.34 we know the number of supersingular j-invariants in $\mathbb{F}_p$ to be

$$\#S_p = \begin{cases} \frac{1}{2}h(-4p) & \text{if } \ p \equiv 1 \pmod 4 \\ h(-p) & \text{if } \ p \equiv 7 \pmod 8 \\ 2h(-p) & \text{if } \ p \equiv 3 \pmod 8, \end{cases}$$

so we need to find out how many non-$\mathbb{F}_p$-isomorphic supersingular elliptic curves with the same j-invariant exist to determine the cardinality of $\mathcal{E}\ell\ell_{\mathbb{F}_p,s}$.

Proposition 3.15. *Let $p > 3$ be a prime. For every supersingular j-invariant in $\mathbb{F}_p$ there are – up to $\mathbb{F}_p$-isomorphism – exactly two supersingular elliptic curves defined over $\mathbb{F}_p$ with j-invariant j.*

Proof. Theorem 2.2 of Bröker [5] tells us that for $p > 3$ the number of elliptic curves over $\mathbb{F}_p$ with j-invariant j up to $\mathbb{F}_p$-isomorphism is

$$\begin{cases} 6 & \text{if } j = 0 \quad\quad \text{and } p \equiv 1 \pmod 3 \\ 4 & \text{if } j = 1728 \quad \text{and } p \equiv 1 \pmod 4 \\ 2 & \text{otherwise.} \end{cases}$$

Further we know from Corollary 2.29 that an elliptic curve with j-invariant 0 resp. 1728 is supersingular if and only if we have $p \equiv 2 \pmod 3$ resp. $p \equiv 3 \pmod 4$. So the cases of six or four such curves never arise in the supersingular case and thus we always have two different $\mathbb{F}_p$-isomorphism classes with given j-invariant there. □

Therefore we see that the number of elements in $\mathcal{E}\ell\ell_{\mathbb{F}_p,s}$ is just twice the number of possible j-invariants and thus equal to $2\#S_p$.

On the other hand, the cardinality of $\mathcal{E}\ell\ell_{K,s}$ can be simply calculated as

$$\begin{aligned} \#\mathcal{E}\ell\ell_{K,s} &= \begin{cases} \#\mathcal{E}\ell\ell_K(\mathbb{Z}[\sqrt{-p}]) & \text{if } p \equiv 1 \pmod 4 \\ \#\mathcal{E}\ell\ell_K(\mathbb{Z}[\sqrt{-p}]) + \#\mathcal{E}\ell\ell_K(\mathcal{O}_K) & \text{if } p \equiv 3 \pmod 4 \end{cases} \\ &= \begin{cases} h(-4p) & \text{if } p \equiv 1 \pmod 4 \\ h(-4p) + h(-p) & \text{if } p \equiv 3 \pmod 4 \end{cases} \\ &= \begin{cases} h(-4p) & \text{if } p \equiv 1 \pmod 4 \\ 2h(-p) & \text{if } p \equiv 7 \pmod 8 \\ 4h(-p) & \text{if } p \equiv 3 \pmod 8 \end{cases} \end{aligned}$$

which obviously also equals $2\#S_p$. So both sets are finite and equipotent. Actually, reduction of elliptic curves yields a bijection between them in the following sense. This is similar to Proposition 2.5 of Delfs-Galbraith [18].

Theorem 3.16. *Let $p > 3$ be a prime and K be a number field as before. There is a fixed place $\mathfrak{P}'$ over p such that the following reduction map is an isomorphism,*

$$\begin{aligned} \bar{\cdot}_{\mathfrak{P}'} : \mathcal{E}\ell\ell_{K,s} &\to \mathcal{E}\ell\ell_{\mathbb{F}_p,s} \\ [E] &\mapsto [\bar{E}]. \end{aligned}$$

PROOF. If E_0 and E_1 are isomorphic elliptic curves defined over a number field K, they have the same j-invariant, and when they are reduced the j-invariants of the reduced curves will equal, too. Thus, $\bar{E}_0$ and $\bar{E}_1$ are isomorphic and the map is well-defined. Since both sets are finite and have the same number of elements, it suffices to show surjectivity or injectivity of the map. We will show here that it is surjective.

Let E_0 be a supersingular elliptic curve defined over $\mathbb{F}_p$. We have shown previously that the restricted endomorphism ring $\operatorname{End}_{\mathbb{F}_p} E_0$ is either the order $\mathbb{Z}[\sqrt{-p}]$ or the maximal order $\mathcal{O}_\mathcal{K}$ in $\mathcal{K} = \mathbb{Q}(\sqrt{-p})$. Choosing the isogeny $\phi_0 \in \operatorname{End}_{\mathbb{F}_p} E_0$ as π_p or $\frac{1+\pi_p}{2}$ depending on the form of the restricted endomorphism ring with $\operatorname{End}_{\mathbb{F}_p} E_0 = \langle 1, \phi_0 \rangle$, we can perform a DEURING Lift on E_0 together with ϕ_0. With that we get an elliptic curve E over a number field K and $\phi \in \operatorname{End} E$ such that E has good reduction $\bar{E}$ at a place $\mathfrak{P}$, $\bar{E} \cong E_0$ and ϕ is mapped on ϕ_0 under this isomorphism.

In particular, this endomorphism ϕ has the same characteristic polynomial as ϕ_0, so $\operatorname{End} E = \langle 1, \phi \rangle$ is isomorphic to an order $\mathcal{O}$ in $\mathcal{K} = \mathbb{Q}(\sqrt{-p})$ with $\mathbb{Z}[\sqrt{-p}] \subseteq \mathcal{O}$. Hence, $[E] \in \mathcal{E}\ell\ell_{K,s}$ is true. Most importantly this also means $\operatorname{End} E \cong \operatorname{End}_{\mathbb{F}_p} \bar{E}$.

Usually though when we regard this reduction, the used place $\mathfrak{P}$ does not have to be the fixed place $\mathfrak{P}'$. But PROPOSITION 1.2 of TATE [87] tells us that for any two places $\mathfrak{P}$ and $\mathfrak{P}'$ over the same prime there exists some GALOIS automorphism σ with $\mathfrak{P}' = \mathfrak{P}^\sigma$. Thus the elliptic curve E^σ reduces to $\bar{E}$ modulo the fixed place $\mathfrak{P}'$ and the map $\bar{\cdot}$ is surjective. $\square$

In the proof we have even shown that the endomorphism ring of E is isomorphic to the restricted endomorphism ring of $\bar{E}$ under this reduction, which is fixed in the next PROPOSITION.

PROPOSITION 3.17. *Let $p > 3$ be a prime and E be an elliptic curve defined over a number field K such that there exists a good reduction $\bar{E}$ of E at a place $\mathfrak{P}$ over p which is supersingular and defined over the finite field $\mathbb{F}_p$. Then we have*

$$\operatorname{End} E \;\cong\; \operatorname{End}_{\mathbb{F}_p} \bar{E}.$$

The structure of an endomorphism ring of a supersingular elliptic curve defined over $\mathbb{F}_p$ has also the prominent attribute that it contains $\mathbb{Z}[\sqrt{-p}]$ as we have seen in PROPOSITION 3.14. Thus we even have

$$\begin{aligned} \bar{E} \text{ is defined over } \mathbb{F}_p \quad &\Longleftrightarrow \quad \sqrt{-p} \in \operatorname{End} \bar{E} \\ &\Longleftrightarrow \quad \sqrt{-p} \in \operatorname{End} E \end{aligned}$$

in the situation above and can already decide if the reduced curve is supersingular and defined over $\mathbb{F}_p$ when we look at the not-reduced curve's endomorphism ring. With these considerations the DEURING Reduction Theorem can be posed as follows.

THEOREM 3.18 (Supersingular DEURING Reduction Theorem). *Let E be an elliptic curve over a number field K, $\operatorname{End} E$ isomorphic to an order in an imaginary quadratic field $\mathcal{K}$ and $\mathfrak{P}$ be a place over some prime $p > 3$ such that E has good reduction $\bar{E}$ over $\mathbb{F}_p$ modulo this place. Then we get*

$$\begin{aligned} \bar{E} \text{ is supersingular} \quad &\Longleftrightarrow \quad p \text{ does not split in } \mathcal{K} \\ &\Longleftrightarrow \quad \mathcal{K} = \mathbb{Q}(\sqrt{-p}). \end{aligned}$$

Let in this case $\operatorname{End} E$ contain $\mathbb{Z}[\sqrt{-p}]$. Then the map

$$\begin{aligned} \bar{\cdot} \; : \; \operatorname{End} E \;&\to\; \operatorname{End}_{\mathbb{F}_p} \bar{E} \\ \phi \;&\mapsto\; \bar{\phi} \end{aligned}$$

is an isomorphism.

In our setting it is also interesting to see what happens to isogenies under reduction. The map $\operatorname{Hom}(E_0, E_1) \to \operatorname{Hom}(\bar{E}_0, \bar{E}_1)$ is an degree-preserving injection due to LEMMA 3.11, so the reduction of an ℓ-isogeny between E_0 and E_1 yields an ℓ-isogeny between the reduced curves. We want to show that in contrast to the ordinary case there is no immediate bijection but we have to restrict us – similarly as with the endomorphisms – to isogenies which are defined over $\mathbb{F}_p$.

PROPOSITION 3.19. *Let $\bar{E}_0$ and $\bar{E}_1$ be supersingular elliptic curves in characteristic p and E_0 and E_1 be elliptic curves defined over a number field such that E_i is reduced to $\bar{E}_i$. Let further $\phi \in \operatorname{Hom}(E_0, E_1)$ be an isogeny and $\bar{\phi} \in \operatorname{Hom}(E_0, E_1)$ its reduction.*

If $\bar{E}_0$ and $\bar{E}_1$ are defined over $\mathbb{F}_p$, then $\bar{\phi} : \bar{E}_0 \to \bar{E}_1$ is $\mathbb{F}_p$-rational.

PROOF. This is PROPOSITION 2.6 of DELFS-GALBRAITH [18]. Let π_p denote the FROBENIUS endomorphism in both of the $\operatorname{End}_{\mathbb{F}_p} \bar{E}_i$ and lift the curves E_i together with π_p. We have $\operatorname{End}_{\mathbb{F}_p} \bar{E}_i \cong \operatorname{End} E_i$ and take isogenies $\phi_i \in \operatorname{End} E_i$ which reduce to π_p. Further $\operatorname{End} E_i \cong \mathcal{O}_i$ is true where the $\mathcal{O}_i$ are orders in an imaginary quadratic field $\mathcal{K}$. We can assume that we have fixed those isomorphisms $[\cdot]_i : \mathcal{O}_i \to \operatorname{End} E_i$ with $\phi_i = [\sqrt{-p}]$ for the complex $\sqrt{-p} \in \mathcal{O}_i \subseteq \mathbb{C}$.

Let Λ_0 and Λ_1 be the lattices corresponding to E_1 resp. E_1, then the isogeny $\phi : E_0 \to E_1$ can be represented by an $\alpha \in \mathbb{C}$ with $\alpha\Lambda_0 \subseteq \Lambda_1$. In $\mathbb{C}$ we have the equality $\alpha \cdot \sqrt{-p} = \sqrt{-p} \cdot \alpha$, which leads to $\phi \circ \phi_0 = \phi_1 \circ \phi$, which can also be seen in COROLLARY II.1.1.1 of SILVERMAN [74]. Thus after reduction we get $\bar{\phi} \circ \pi_p = \pi_p \circ \bar{\phi}$. As shown in LEMMA 2.19, this already implies that $\bar{\phi}$ is defined over $\mathbb{F}_p$. □

Note that there can be isogenies between $\mathbb{F}_p$-rational elliptic curves $\bar{E}_0$ and $\bar{E}_1$ which are defined over an extension of $\mathbb{F}_p$, but those are not in the image of $\mathrm{Hom}(E_0, E_1)$ under reduction. Examples of that can be found in the graphs in APPENDIX C. But it can be shown that every $\mathbb{F}_p$-rational ℓ-isogeny between elliptic curves defined over $\mathbb{F}_p$ can be reached through reduction of an isogeny between the corresponding lifts.

PROPOSITION 3.20. *Let $p > 3$ be a prime, $E \in \mathcal{E}\ell\ell_{K,s}$ be an elliptic curve with good supersingular reduction $\bar{E} \in \mathcal{E}\ell\ell_{\mathbb{F}_p,s}$ and ℓ be a prime different from p. Then we get a one-to-one correspondence*

$$\left\{\phi \in \mathrm{Hom}(E, \cdot) \mid \deg \phi = \ell\right\} \quad \longleftrightarrow \quad \left\{\bar{\phi} \in \mathrm{Hom}_{\mathbb{F}_p}(\bar{E}, \cdot) \mid \deg \bar{\phi} = \ell\right\}.$$

PROOF. We have already shown that all reduced isogenies are defined over $\mathbb{F}_p$, so it remains to check that every $\mathbb{F}_p$-rational isogeny actually arises from the reduction of an isogeny in characteristic 0. The proof follows along the lines of page 7 of DELFS-GALBRAITH [18].

For an elliptic curve E in characteristic 0 with endomorphism ring $\mathrm{End}\, E$ we get from THEOREM 3.3 that isogenies between elliptic curves in $\mathcal{E}\ell\ell_{K,s}$ exist in the cases that

- $\ell > 2$ and ℓ splits in $\mathcal{K}$, then there are two outgoing horizontal isogenies from E to elliptic curves in $\mathcal{E}\ell\ell_{K,s}$ (the $\ell - 1$ descending isogenies have image curves outside of $\mathcal{E}\ell\ell_{K,s}$),
- $\ell = 2$ and $\mathrm{End}\, E = \mathbb{Z}\left[\sqrt{-p}\right]$, then there is one outgoing ascending or horizontal isogeny from E to an elliptic curve in $\mathcal{E}\ell\ell_{K,s}$ (the two descending isogenies lead to elliptic curves with smaller endomorphism rings),
- $\ell = 2$ and $\mathrm{End}\, E = \mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$, then there are three outgoing descending or horizontal isogenies from E to elliptic curves in $\mathcal{E}\ell\ell_{K,s}$.

We now want to show that the number of $\mathbb{F}_p$-rational between elliptic curves in $\mathcal{E}\ell\ell_{\mathbb{F}_p,s}$ is the same in the respective cases.

Let $\bar{E}$ be a supersingular elliptic curve defined over $\mathbb{F}_p$ and $\bar{\phi}$ be a $\mathbb{F}_p$-rational isogeny of prime degree ℓ starting at $\bar{E}$. As we have seen in LEMMA 2.18, $\bar{\phi}$ corresponds to a GALOIS-invariant subgroup G of $\bar{E}[\ell]$. Since ℓ is prime, this subgroup will also be cyclic. So let P be a point of $\bar{E}[\ell]$ such that $G = \langle P \rangle$ with $\pi_p(G) = G$. This yields the eigenequation $\pi_p(P) = [a]P$ for some integer a and thus the characteristic polynomial of π_p – which is $\pi_p^2 + p$ – has a root at $a \pmod{\ell}$.

Since we have $\bar{E}[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$, $\bar{E}[\ell]$ can be interpreted as 2-dimensional $\mathbb{Z}/\ell\mathbb{Z}$-vector space with chosen basis (P, Q). Let A_{π_p} denote the 2×2 matrix representing π_p with respect to this basis.

Let first $\ell > 2$ split in $\mathcal{K}$. Since we have $\left(\frac{-p}{\ell}\right) = 1$, the equation $\pi_p \equiv -p \pmod{\ell}$ is solvable, so the characteristic polynomial $\pi_p + p$ is not irreducible. It also does not have a repeated root at a, since the equation

$$\pi_p^2 + p \;\equiv\; (\pi_p - a)^2 \;\equiv\; \pi_p^2 - 2a\pi_p + a^2 \pmod{\ell}$$

is not solvable for $\ell \neq 2$. Thus the characteristic polynomial splits in a product of linear factors

$$\pi_p^2 + p \;\equiv\; (\pi_p - a)(\pi_p - b) \pmod{\ell} \quad \text{with } a \not\equiv b \pmod{\ell}.$$

This means that A_{π_p} is diagonalizable and can be represented as

$$A_{\pi_p} \;=\; \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}.$$

Therefore we have $\pi_p(P) = [a]P$ and $\pi_p(Q) = [b]Q$, which yields two cyclic GALOIS-invariant subgroups of $\bar{E}[\ell]$. The subgroup generated by any other non-trivial element $R := uP + vQ$ of $\bar{E}[\ell]$ is obviously not GALOIS-invariant.

Now take $\ell = 2$. Again, the equation $\pi_p^2 = -p \pmod{2}$ is solvable, so the characteristic polynomial is not irreducible. This time the assumption of two non-equal roots gives us a contradiction since

$$\pi_p^2 + p \;\equiv\; \pi_p(\pi_p + 1) \;\equiv\; \pi_p^2 + \pi_p \pmod{2}$$

cannot be true. Thus in this case the characteristic polynomial satisfies

$$\pi_p^2 + p \;\equiv\; (\pi_p - a)^2 \pmod{2}$$

and the representation matrix is

$$A_{\pi_p} \;=\; \begin{pmatrix} a & 0 \\ b & a \end{pmatrix}.$$

If the geometric multiplicity of a is two, the matrix will be diagonalizable and thus $b \equiv 0 \pmod 2$. In this case all the cyclic subgroups of $\bar{E}[2]$ generated by P, Q or $P+Q$ will be the GALOIS-invariant ones. Else we get $b \equiv 1 \pmod 2$ and only P generates a cyclic GALOIS-invariant subgroup of $\bar{E}[2]$.

It remains to be shown that the case $b \equiv 0 \pmod 2$ with the three subgroups occurs if and only if the restricted endomorphism ring of $\bar{E}$ is isomorphic to $\mathbb{Z}[\frac{1+\pi_p}{2}]$.

We have seen that $b \equiv 0 \pmod 2$ is true if and only if $\pi_p(P) = P$ and $\pi_p(Q) = Q$, so if P and Q are in the kernel of $\mathrm{id} + \pi_p$. Since P and Q generate $\bar{E}[2]$ and this is the same as $\ker([2])$, we get

$$\ker([2]) \quad \subseteq \quad \ker(\mathrm{id} + \pi_p).$$

The multiplication-by-2-map is separable, so we can use LEMMA 2.10 and find an $\phi \in \operatorname{End} \bar{E}$ with $\mathrm{id} + \pi_p = \phi \circ [2]$. The map

$$\phi \quad = \quad \frac{\mathrm{id} + \pi_p}{[2]} \in \operatorname{End} \bar{E}$$

is a $\mathbb{F}_p$-rational map and thus an element of $\operatorname{End}_{\mathbb{F}_p} \bar{E}$, but its interpretation $\frac{1+\pi_p}{2}$ in the isomorphic order of $\mathcal{K}$ is obviously not in $\mathbb{Z}[\sqrt{-p}]$. So $\operatorname{End}_{\mathbb{F}_p} \bar{E}$ has to be isomorphic to $\mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$ and since all of the steps in this argumentation are invertible, this brings the proposed equivalence. $\square$

Summed up, the level structure of elliptic curves and isogenies in characteristic 0 can be transferred to $\mathbb{F}_p$-rational isogenies between supersingular elliptic curves defined over $\mathbb{F}_p$. Since $\sqrt{-p} \in \operatorname{End} E$ is presumed for a supersingular elliptic curve E to be defined over $\mathbb{F}_p$, at most two levels occur in this reduced graph. The other descending isogenies lead to image curves which have endomorphism ring isomorphic to $\mathbb{Z}[\ell^r \sqrt{-p}]$ with some $r \geq 1$ and thus are not defined over $\mathbb{F}_p$.

We will investigate those graphs in more detail in the next section.

4 Arithmetic Isogeny Problems

In this section we will always regard elliptic curves E which are defined over a finite field $\mathbb{F}_q$ of characteristic p, their trace $t = q + 1 - \#E(\mathbb{F}_q)$ and the imaginary quadratic field $\mathcal{K} = \mathbb{Q}(\sqrt{d})$ with $d := t^2 - 4q$. After introducing the notation, basic definitions and problems to study, we will first cover the well-known ordinary case before explaining the difficulties of the supersingular situation. Then we will show how to adapt the approaches of the ordinary case to isogenies between supersingular elliptic curves which are defined over $\mathbb{F}_p$. The results from the last section will be of great importance there.

Definition. Let K be a field of characteristic $p > 0$ and $\mathcal{L}$ be a set of small primes with $p \notin \mathcal{L}$. The directed graph where

- the vertices are K-isomorphism classes of elliptic curves defined over K
- the edges are isogenies defined over K and of degree $\ell \in \mathcal{L}$ between the corresponding elliptic curves

is called *isogeny graph* and denoted with $G(K, \mathcal{L})$.

We will label the vertices with E or – especially in the explicit examples – with j when $j = j(E)$. Since for any isogeny $\phi : E_0 \to E_1$ there exists the dual isogeny $\hat{\phi} : E_1 \to E_0$, we usually treat the isogeny graph as an undirected graph. Exceptions only happen for $j = 0$ or $j = 1728$ as we have seen in the remark after Proposition 2.15 where we discussed equivalent isogenies.

Remark (and more refined Notation).

- For $\mathcal{L} = \{\ell\}$ we write $G(K, \ell)$.
- The isogeny graph $G(\mathbb{F}_q, \mathcal{L})$ is never fully connected since due to Theorem 2.13 isogenies can only exist between elliptic curves of same trace t (and for instance never between an ordinary and a supersingular one).
  Therefore we usually look only at possible *components* $G_t(\mathbb{F}_q, \mathcal{L})$.
- For $t \neq 0$ the graphs $G_t(\mathbb{F}_q, \mathcal{L})$ and $G_{-t}(\mathbb{F}_q, \mathcal{L})$ have the same structure since the curves in the one graph are twists of the curves in the other (see Exercise 25.3.8 of Galbraith [28]).
  Thus for ordinary graphs we usually regard only the case $t > 0$.
- Isogenies between ordinary elliptic curves over $\mathbb{F}_q$ are also defined over $\mathbb{F}_q$ (Proposition 3.13), so $G_t(\mathbb{F}_q, \mathcal{L})$ is always the whole picture.

✦ In the supersingular case we know from Theorem 2.22 that we always have $q \in \{p, p^2\}$ but isogenies are defined over $\bar{\mathbb{F}}_q$ in general. So here we usually regard the two situations $G_0(\mathbb{F}_p, \mathcal{L})$ and $G_0(\bar{\mathbb{F}}_p, \mathcal{L})$.

Finding paths between given vertices in an isogeny graph $G_t(\mathbb{F}_q, \mathcal{L})$ is a way to solve the general elliptic isogeny problem as introduced in Section 2.1.1, although an thus obtained isogeny has degree of a product of the primes in $\mathcal{L}$ and thus cannot be guarantied to exist. If need be, the set $\mathcal{L}$ has to be increased until a connection can be found. Therefore the following *isogeny graph problem* is phrased with a constraint.

Problem 5 (Elliptic Isogeny Graph Problem). *Let K be a finite field of characteristic p and $\mathcal{L}$ a set of small primes with $p \notin \mathcal{L}$. Given $j_0, j_1 \in G_t(K, \mathcal{L})$, compute a path between them (if possible).*

In this chapter we are going to describe the setting of this problem in different situations and some approaches to solve it.

4.1 The Ordinary Elliptic Isogeny Problem

Computing isogenies between ordinary elliptic curves is a problem that has been provided with a satisfying solution which we will investigate briefly in this chapter. To be explicit, we want to deal with the following problem.

Problem 6 (Ordinary Elliptic Isogeny Problem). *Let q be a prime power and E_0, E_1 ordinary elliptic curves over $\mathbb{F}_q$ with $\#E_0(\mathbb{F}_q) = \#E_1(\mathbb{F}_q)$. Compute an isogeny $\phi : E_0 \to E_1$.*

The first approach of Galbraith [27] is based on a bi-directional breadth-first search on ordinary isogeny graphs. This algorithm also guaranties to find the shortest path in the graph, but not necessarily an isogeny with smallest possible degree. Dropping the condition of finding the shortest path and using a random walk instead of the breadth-first search and *smoothing* ideals, Galbraith, Hess and Smart [29] developed a low-storage algorithm which can also be parallelized. This has further be improved by Galbraith and Stolbunov [31] through preferring isogenies with smaller degree in the computed chain of isogenies. The resulting isogeny's degree will probably be reasonably small after that, too.

We will see later that ideas from those approaches can also be used for an algorithm to compute isogenies between $\mathbb{F}_p$-rational supersingular elliptic curves. Therefore we will look into some of their details here.

4.1.1 Ordinary Isogeny Graphs

We have seen in Section 2.2 how the endomorphism rings of isogenous ordinary elliptic curves can be arranged in some kind of levels. This structure can be transferred to the ordinary isogeny graphs $G_t(\mathbb{F}_q, \ell)$. Even more, we can determine how many horizontal, ascending or descending isogenies a given elliptic curve in the graph has.

For this task we use the traits of elliptic curves defined over a number field developed in Section 3. There we deduced the number of outgoing isogenies in each direction and showed that this behavior is preserved under reduction. Thus we can transfer this structure to ordinary elliptic curves E defined over a finite field which have endomorphism ring isomorphic to an order $\mathcal{O}$ in an imaginary quadratic field $\mathcal{K}$. Since we have $\mathbb{Z}[\pi_q] \subseteq \mathcal{O} \subseteq \mathcal{O}_\mathcal{K}$, the ordinary isogeny graph is finite and we use the terms of an elliptic curve being on the *surface* or *floor* at ℓ as established before. The properties of outgoing isogenies for an ordinary elliptic curve over a finite field $\mathbb{F}_q$ are summarized in the next proposition, which can be deduced from Proposition 23 of Kohel [45].

Proposition 4.1. *Let E be an ordinary elliptic curve defined over $\mathbb{F}_q$ and ℓ be a prime not dividing* $\operatorname{char} \mathbb{F}_q$. *Let $\mathcal{K}$ be an imaginary quadratic field as before and $\mathcal{O}$ be an order in $\mathcal{K}$ with discriminant $d_\mathcal{O}$ which is isomorphic to the endomorphism ring of E. Further, let $(\frac{d_\mathcal{O}}{\ell})$ denote the* Kronecker *symbol.*

In the case where $\ell \mid [\mathcal{O}_\mathcal{K} : \mathbb{Z}[\pi_q]]$, we have more than just one level in the graph containing E and get the following behavior.

- *If E is on the surface at ℓ, there are $1+\left(\frac{d_\mathcal{O}}{\ell}\right)$ horizontal ℓ-isogenies and $\ell-\left(\frac{d_\mathcal{O}}{\ell}\right)$ descending ℓ-isogenies starting at E.*
- *If E is on the floor at ℓ, there is only one ascending ℓ-isogeny starting at E.*
- *If E is neither on the floor nor on the surface at ℓ, there is one ascending ℓ-isogeny and ℓ descending ones starting at E.*

In the case where floor and surface coincide we have

- $1 + \left(\frac{d_\mathcal{O}}{\ell}\right)$ *horizontal ℓ-isogenies starting E.*

The components of the resulting structure for $G_t(\mathbb{F}_q, \ell)$ are called volcanoes – a name introduced by Fouquet and Morain in [24] – and are easy to explore as we will see in the next section. Remember that we already defined distance in an isogeny graph in Section 3.2, a concept which can be used in the formal definition of levels in a volcano.

Definition. Let F_q be a finite field of characteristic p, $\ell \neq p$ be a prime and $0 < t \leq 2\sqrt{q}$ be a possible trace of ordinary elliptic curves defined over $\mathbb{F}_q$. A connected component of $G_t(\mathbb{F}_q, \ell)$ is called *ℓ-isogeny volcano* or *ℓ-volcano.* A *level* V_i of a volcano consists of all elliptic curves with distance i from the surface at ℓ.

As mentioned before, the ordinary isogeny graphs have finitely many nodes and thus we have a finite number of levels, too.

Those volcanoes provide useful arithmetic means in several areas, for example Bröker, Lauter and Sutherland [7] use them to compute modular polynomials and Sutherland [84] exploits their difference from the supersingular case to develop a fast algorithm to identify whether a given curve is ordinary or supersingular.

In Figure 2 is an example of an isogeny graph with two volcanoes of 2-isogenies. We used $p = 149$ and trace $t = 6$ where we get to work in $\mathcal{K} = \mathbb{Q}(\sqrt{-35})$ with fundamental discriminant $d_{\mathcal{K}} = -35$. Note that the conductor is $c = 4$, so the only vertical isogenies must have degree $\ell = 2$. We have $\left(\frac{d_{\mathcal{K}}}{2}\right) = -1$, so there are no horizontal 2-isogenies on the top level corresponding to elliptic curves with endomorphism ring isomorphic to $\mathcal{O}_{\mathcal{K}}$ but three descending ones. The reached image curves are not on the surface at 2, so the only possibilities for further outgoing isogenies are two more descending ones per node.

Remember that we regard the isogeny graph as an undirected graph, so each edge in this graph represents two isogenies which are dual to each other.

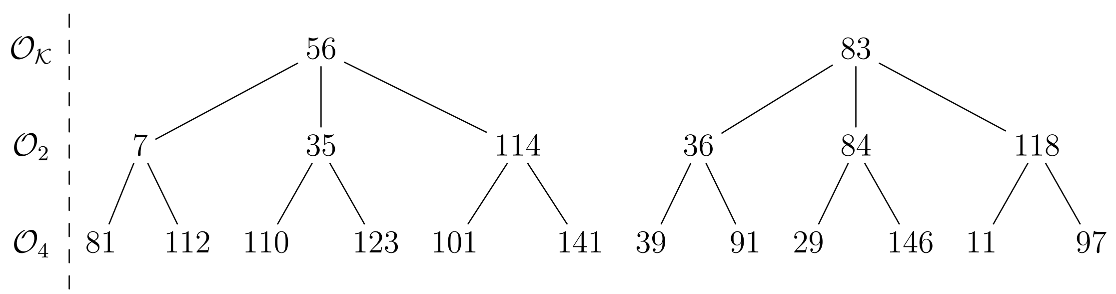


Figure 2: The Ordinary Isogeny Graph $G_6(\mathbb{F}_{149}, 2)$

With these concepts concerning isogeny graphs, solving the ordinary isogeny problem transmutes into finding a solution of the following question.

Problem 7 (Ordinary Isogeny Graph Problem). *Let $q = p^r$ be a prime power, $\mathcal{L}$ a set of small primes with $p \notin \mathcal{L}$ and $t \neq 0$. Given $j_0, j_1 \in G_t(\mathbb{F}_q, \mathcal{L})$, compute a path between them (if possible).*

Note that this problem is only equivalent to the original one if the set $\mathcal{L}$ is chosen *big enough* in the meaning that $G_t(\mathbb{F}_q, \mathcal{L})$ is fully connected with this $\mathcal{L}$. Otherwise we can only succeed for elliptic curves between which an isogenies with $\mathcal{L}$-smooth degree exists. In the example graph of FIGURE 2 for instance it is impossible to find a path from a node in the left volcano to a node in the right one. Only when we add 3-isogenies in the picture we get a fully connected graph, since there exist horizontal 3-isogenies connecting those components as can be seen in FIGURE 3.

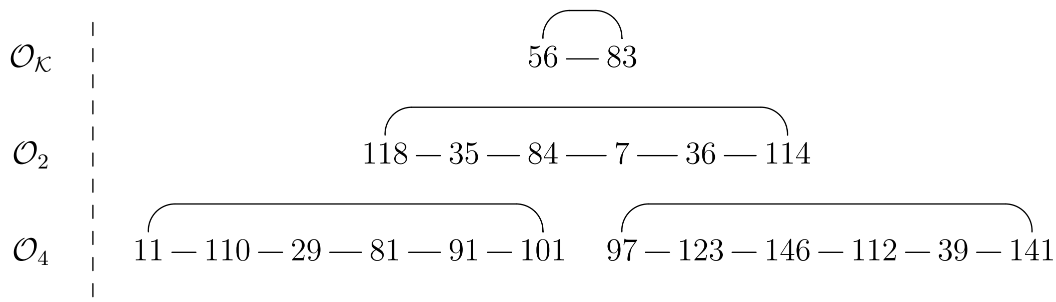


FIGURE 3: The Ordinary Isogeny Graph $G_6(\mathbb{F}_{149}, 3)$

Thus the main question is how many primes we have to add into the set $\mathcal{L}$ until the isogeny graph is fully connected. Here we can use the results from SECTION 3 and especially BACH'S bound again and apply them to the top level of the isogeny graph. We have seen that isogenies of degree ℓ correspond to ideals of norm ℓ and that ideals of norm $\leq B$ generate the full ideal class group $\mathcal{C}\ell(\mathcal{O}_{\mathcal{K}})$ which corresponds to the set of elliptic curves with endomorphism ring isomorphic to $\mathcal{O}_{\mathcal{K}}$. Thus the graph whose nodes are the elements of this set is fully connected when we take isogenies of degree $\leq B$ as edges. Especially the graph $G_t(\mathbb{F}_q, \mathcal{L})$ is connected when we use $\mathcal{L} = \{\text{primes } \ell < B\}$. To be even more precise, when we only regard elliptic curves on the crater we can restrict to $\mathcal{L} = \left\{\text{primes } \ell < B \mid \left(\frac{d_{\mathcal{K}}}{\ell}\right) \neq -1\right\}$ since those primes are the only ones where we can have horizontal isogenies at all. This result is useful for exploring the graph and developing algorithms for constructing isogenies as seen in the next section.

4.1.2 Resulting Algorithms and Complexity Analysis

In the following part we introduce several algorithms and present pseudocodes for them which can be used to investigate their running time and storage requirements. In APPENDIX A detailed `MAGMA` codes for those algorithms are shown which are the source of the computational results listed in APPENDIX B.

Computing Neighbors. Let E_0 be an ordinary elliptic curve defined over the finite field $\mathbb{F}_q$ of characteristic p, $\ell \neq p$ be a prime and j_0 the j-invariant of E_0. We have seen in Section 2.1.1 that all j-invariants of ℓ-neighbors of E_0 occur as roots of $\Phi_\ell(j_0, \cdot)$. In the case where this modular polynomial has at least one root, let j_1 be one of them. When there are only two elliptic curves with this j-invariant, they are quadratic twists of each other and one of them has trace t and the other trace $-t$. As mentioned before, the graphs $G_t(\mathbb{F}_q, \ell)$ and $G_{-t}(\mathbb{F}_q, \ell)$ look identical and there is an easy to compute isomorphism between those elliptic curves, so we regard them as being equivalent.

When there are more than two elliptic curves with this j-invariant though, they can have different positive trace, too, and this can lead to misunderstandings. Let for example be $q = p = 13$, then there are three different isomorphism classes of elliptic curves with positive trace and j-invariant 0. When we regard the modular polynomials for $\ell = 2$ and $\ell = 3$ we get

$$\begin{aligned}\Phi_2(0, Y) &= (Y+2)^3 \pmod{13}\\ \Phi_3(0, Y) &= Y(Y+10)^3 \pmod{13}\end{aligned}$$

so we would expect an elliptic curve E_0 with j-invariant 0 to have isogenous neighbors with j-invariant 11, 3 and 0. But we check that an elliptic curve E_1 with j-invariant 11 has trace $t = \pm 2$ and E_2 with j-invariant 3 has trace $t = \pm 5$, thus there cannot be an isogeny between them. The solution is, that there are elliptic curves with j-invariant 0 as well with trace 2 as with trace 5 and trace 7. The first one has three outgoing descending 2-isogenies to E_1 and one 3-isogeny to itself, the second one three descending 3-isogenies to E_2 and one horizontal one to itself, and the last one only one outgoing horizontal 3-isogeny to itself.

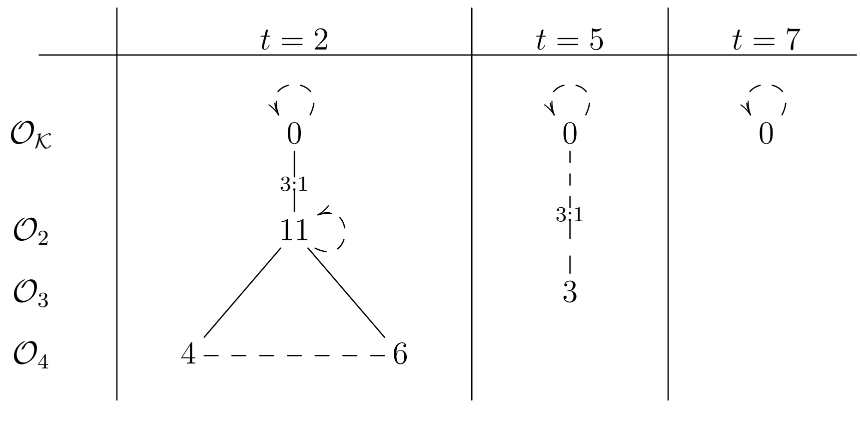


Figure 4: Ordinary Isogeny Graphs $G_t(\mathbb{F}_{13}, \{2, 3\})$ for $t \in \{2, 5, 7\}$

The behavior can be seen in FIGURE 4. There the 2-isogenies are drawn with solid lines and 3-isogenies with dashed ones. The undirected edges are understood to be a pair of dual isogenies each and the directed loops are single loops, that is, isogenies which are their own duals.

The label "3 : 1" on the arrows indicates that there are three outgoing isogenies from the node 0 which all have the same dual, so there is only one isogeny in the other direction. We verify that $\left(\frac{d_E}{\ell}\right)$ is -1 resp. 0 for $\ell = 2$ and $\ell = 3$, so there have to be none resp. one horizontal ℓ-isogenies.

BRÖKER, LAUTER and SUTHERLAND [7] have shown in their THEOREM 1 under assumption of the Generalized RIEMANN Hypothesis how for an odd prime ℓ and a positive integer q the classical modular polynomial $\Phi_\ell \in \mathbb{F}_q[X, Y]$ can be computed. We fix their complexity result below.

PROPOSITION 4.2. *Let ℓ be an odd prime. Assuming* GRH, *the ℓ modular polynomial $\Phi_\ell \in \mathbb{F}_q[X, Y]$ can be computed in expected $\mathcal{O}(\ell^3 (\log \ell)^3 \log\log \ell)$ bit operations and needs $\mathcal{O}(\ell^2 \log(\ell q))$ bits storage.*

However, because we can precompute all modular polynomials needed in our algorithms and `MAGMA` provides a sufficient database for them with $\ell \leq 60$, we will neglect the costs of computing Φ_ℓ and assume that the polynomial is given. Hence we will not count this step in the following complexity analyses but treat it as a independent precomputation.

As seen in TABLE 2.1 of GALBRAITH [28], finding the roots in $\mathbb{F}_q$ of a polynomial with degree d can be done in expected $\mathcal{O}(d^2 \log d \log q)$ field operations. It needs a storage of $\mathcal{O}(d)$ field elements. If ℓ is a prime, the ℓ-th modular polynomial has degree $\ell + 1$ in each variable and thus finding the roots of $\Phi_\ell(j, Y)$ can be achieved in $\mathcal{O}(\ell^2 \log \ell \log q)$ operations in $\mathbb{F}_q$ and the needed storage is $\mathcal{O}(\ell)$ field elements. This is dominated by the memory needed for storing the polynomial itself but probably has to be done for several values of j in course of the algorithms, thus it is no precomputation.

Summed up, the computation of all neighbors of a given vertex in $G_t(\mathbb{F}_q, \ell)$ can be achieved in the following expected complexity.

PROPOSITION 4.3. *Let $\mathbb{F}_q$ be a finite field and $\ell \neq \operatorname{char} \mathbb{F}_q$ be a prime. Let E be an elliptic curve defined over $\mathbb{F}_q$. Computing all ℓ-neighbors of E needs expected $\mathcal{O}(\ell^2 \log \ell \log q)$ running time and $\mathcal{O}(\ell)$ storage, both measured in operations resp. elements in $\mathbb{F}_q$.*

NAVIGATING THE GRAPH. The structure of the ordinary isogeny volcano and the connection to the ideal class group are of essential importance for computing isogenies between ordinary elliptic curves. At first we want to investigate some approaches about how to move in a single component volcano and how to detect the position of a given elliptic curve in this graph. This strategies have been developed by Kohel in his thesis [45].

For instance, it can immediately be determined if an elliptic curve is on the floor for a fixed isogeny degree ℓ. The usual situation can be seen in Figure 2 where we have more than one level in a volcano component. As there is only one outgoing isogeny for the elliptic curves E which are on the floor at $\ell = 2$, the ℓ-th modular polynomial $\Phi_2(j(E), Y)$ will only have a single root modulo q. Every other node E has three outgoing isogenies and thus the degree-3-polynomial $\Phi_2(j(E), Y)$ will split completely in linear factors.

However, this only works when floor and surface do not coincide. In the other cases like in Figure 3 all isogenies are horizontal and we have seen in Proposition 4.1 that the number of such isogenies of degree ℓ on the surface is $1 + \left(\frac{d_{\mathcal{K}}}{\ell}\right)$. Thus it is also possible to have two or none outgoing isogenies for an elliptic curve on the floor depending on how ℓ behaves in $\mathcal{K}$.

(a) ℓ splits in $\mathcal{K}$ (b) ℓ ramifies in $\mathcal{K}$ (c) ℓ is inert in $\mathcal{K}$

Figure 5: Possible Structures of One-Level Volcanoes

Every other ordinary elliptic curve which is not on the floor at some prime ℓ has $\ell+1 > 2$ outgoing isogenies. Summed up, being on the floor can be tested like in the following pseudocode. A working `MAGMA`-algorithm can be found in Appendix A as Algorithm A.1.

Algorithm 4.1 `IsOnFloor(E, q,` ℓ`)`

Input: `ordinary elliptic curve` E `defined over` $\mathbb{F}_q$, `prime number` ℓ `with` $\ell \nmid q$
Output: **true** `if` E `is on the floor at` ℓ, **false** `otherwise`

1: **return** `is` $(\#\{$`roots of` $\Phi_\ell(j(E), Y) \pmod q\} \leq 2)$

Since the main part of this algorithm is factorizing the precomputed ℓ-th modular polynomial and storing its roots, we have the complexity below.

Proposition 4.4. *Let E be an ordinary elliptic curve defined over the finite field $\mathbb{F}_q$ and let $\ell \neq \operatorname{char} \mathbb{F}_q$ be a prime. Testing whether E is on the floor at ℓ can be done in an expected running time of $\mathcal{O}(\ell^2 \log \ell \log q)$ $\mathbb{F}_q$-operations and $\mathcal{O}(\ell)$ storage of $\mathbb{F}_q$ elements.*

Another observation is that once we choose a descending isogeny in a non-backtracking path in a volcano, we keep going down until we reach the floor. This can be used to determine whether a given isogeny is descending or not. We start with two elliptic curves E_0 and E_1 and an isogeny $\phi : E_0 \to E_1$ with degree ℓ between them. When E_0 is on the floor, the isogeny is obviously either ascending, or horizontal if the volcano only consists of one level. When E is not on the floor, there are at least three outgoing isogenies including ϕ. Thus we can start three different paths of isogenies starting at E_0 where at least one of them has to begin with an descending isogeny and go straight down after that. The paths end when they reach an elliptic curve on the floor at ℓ and the length of the shortest one measures the distance of E_0 from the floor. If the path starting with ϕ is one of the shortest, ϕ is descending.

There are several small algorithms which can be deduced from those considerations. The first computes the length of a random path in an ℓ-volcano starting from an elliptic curve with j-invariant j_0 in direction of another one with j-invariant j_1 until a curve on the floor is reached. It is needed for the following procedures.

Algorithm 4.2 `LengthOfPathToFloor(`E_0`, `E_1`, q, `ℓ`, C)`

Input: ordinary elliptic curves E_0, E_1 defined over $\mathbb{F}_q$, prime number ℓ with $\ell \nmid q$, constant $C \leq \log c$ where $c = [\mathcal{O}_\mathcal{K} : \mathbb{Z}[\pi_q]]$
Output: 0 if E_0 is on the floor at ℓ; else length of a random path to a curve on the floor at ℓ, starting from E_0 to E_1

if E_0 is on the floor at ℓ **then**
    return 0
end if
$n \leftarrow 1$
while E_1 is not on the floor at ℓ and $n \leq C$ **do**
    $E_{tmp} \leftarrow E_1$
    $E_1 \leftarrow$ random ℓ-neighbor of E_{tmp}, different from E_0
    $E_0 \leftarrow E_{tmp}$
    $n \leftarrow n + 1$
end while
return n

The steps in this algorithm are randomly chosen and if it were not for the break condition $n \leq C$ we could take infinite paths by moving around the crater in circles. The maximal length of a resulting descending path is clearly dependent on the depth of the volcano which is the number of prime divisors of $c = [\mathcal{O}_\mathcal{K} : \mathbb{Z}[\pi_q]]$. If this conductor factors as $c = \prod_{i=1}^{r} \ell_i^{e_i}$, this number will be

$$\sum_{i=1}^{r} e_i = \sum_{i=1}^{r} e_i \log 2 \quad \leq \quad \sum_{i=1}^{r} e_i \log \ell_i = \log c$$

as used in the input condition. Note that still log denotes the binary logarithm, so we have $\log 2 = 1$.

If $C \leq \log c$ is the constant given in the algorithm, we get C steps where we have to compute all neighbors of a vertex. As we have seen, this is done in expected $\mathcal{O}(\ell^2 \log c \log q)$ each, thus the running time of this algorithm is expected $\mathcal{O}(C \cdot \ell^2 \log c \log q)$. In our applications we usually know the factorization of the conductor c and thus if the exact power of ℓ dividing c is ℓ^e, we can use $C = e$ which is the depth of the ℓ-volcano. Apart from the roots of the modular polynomial we only need to store two j-invariants from $\mathbb{F}_q$ at a time. The integer n which is at most $\log q$ and thus needs an expected storage of $\mathcal{O}(\log \log q)$ bits which is less than one $\mathbb{F}_q$-element.

Thus we can simplify this complexity for computing such a descending path to the following result.

Proposition 4.5. *Let E_0 and E_1 be elliptic curves defined over the finite field $\mathbb{F}_q$ and let $\ell \neq \operatorname{char} \mathbb{F}_q$ be a prime such that E_0 and E_1 are ℓ-isogenous and their endomorphism rings are orders in the imaginary quadratic field $\mathcal{K}$. For $e \in \mathbb{N}$ let ℓ^e be the exact power of ℓ dividing the conductor $c = [\mathcal{O}_\mathcal{K} : \mathbb{Z}[\pi_q]]$. Checking if the ℓ-isogeny $\phi : E_0 \to E_1$ is descending needs expected $\mathcal{O}(e \cdot \ell^2 \log \ell \log q)$ running time and $\mathcal{O}(\ell)$ storage in $\mathbb{F}_q$-operations resp. $\mathbb{F}_q$-elements.*

Another algorithm based strongly on this procedure – and with the same complexity – determines the distance of a given elliptic curve from the floor by comparing the length of three different paths. The shortest one has to be a straight descending path and thus its number of steps is the distance from the floor. Only choosing two different paths is not enough, for example if the curve is on the surface and there are two horizontal isogenies as in the following example.

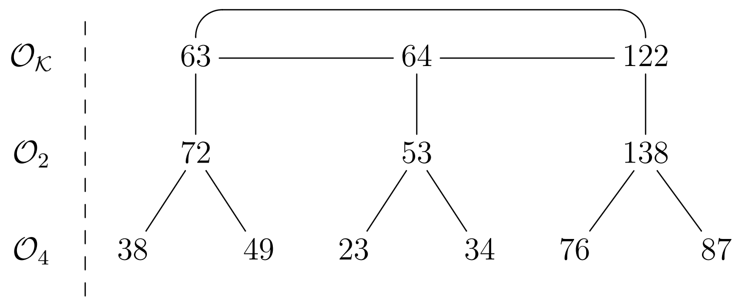


FIGURE 6: The Ordinary Isogeny Graph $G_{10}(\mathbb{F}_{149}, 2)$

If we want to determine the level of the node 64 and the two starting isogenies we take go to 63 and 122, we need at least three steps to reach the floor in each direction although the real distance is two. A path of length two will appear if we take a further starting isogeny to the third possible neighbor of 64. Note that the neighbors do not have to be pairwise distinct as long as the isogenies leading to them are different ones. As seen in FIGURE 3 between the nodes 56 and 83 it is possible that two non-equivalent isogenies have the same image curve.

A short pseudocode of this procedure can be written down as follows. As mentioned before, a working `MAGMA` code can be found in APPENDIX A.

ALGORITHM 4.3 `DistanceToFloor(E, q,` ℓ`)`

INPUT: ordinary elliptic curve E defined over $\mathbb{F}_q$, prime number ℓ with $\ell \nmid q$
OUTPUT: distance from E to the floor at ℓ

$E_1, E_2, E_3 \leftarrow$ random pairwise different neighbors of E
$n_1, n_2, n_3 \leftarrow$ length of random path to floor from E to E_i
return minimum of n_1, n_2 and n_3

This procedure only uses the one to compute the length of a random path to the floor as before, so it has the same time complexity but we have to store all the $e+1$ elements of the path to be able to reconstruct it. Thus the storage complexity here will be $\mathcal{O}(e)$.

PROPOSITION 4.6. *Let E be an ordinary elliptic curve defined over $\mathbb{F}_q$ and let $\ell \neq \operatorname{char} \mathbb{F}_q$ be a prime. Computing the distance of E to the floor in an ℓ-volcano needs expected $\mathcal{O}(e \cdot \ell^2 \log \ell \log q)$ running time and $\mathcal{O}(e)$ storage measured in $\mathbb{F}_q$-operations resp. $\mathbb{F}_q$-elements.*

This procedure is quite helpful for deciding if a given isogeny is descending. In that case a path in the ℓ-volcano starting with this isogeny goes straight down, thus its length is exactly the distance to the floor of the preimage curve.

Algorithm 4.4 `IsDescending(E`$_0$`, E`$_1$`, q,` ℓ`)`

Input: ℓ-isogeny ϕ between ordinary elliptic curves E_0, E_1 defined over $\mathbb{F}_q$ for a prime number ℓ with $\ell \nmid q$
Output: **true** if ϕ is descending, **false** otherwise

1: $n \leftarrow$ length of random non-backtracking path to the floor
2: starting from E_0 to E_1
3: $d \leftarrow$ distance of E to the floor
4: **return** is $(n = d)$

Considered in complexity notation, this obviously has the same running time as the last algorithms, so we get an analogous result here.

Proposition 4.7. *Let E_0 and E_1 be ordinary elliptic curves defined over $\mathbb{F}_q$ and let $\ell \neq \operatorname{char} \mathbb{F}_q$ be a prime such that E_0 and E_1 are ℓ-isogenous. Checking if an ℓ-isogeny $\phi : E_0 \to E_1$ is descending can be done in expected $\mathcal{O}(e \cdot \ell^2 \log \ell \log q)$ running time and $\mathcal{O}(e)$ storage measured in $\mathbb{F}_q$-operations resp. $\mathbb{F}_q$-elements.*

Analogously to that last procedure it is easy to construct an algorithm to see if a given isogeny from E_0 to E_1 is ascending by returning whether the dual isogeny from E_1 to E_0 is descending. An isogeny is horizontal if it is neither ascending nor descending. We have seen that when an ordinary elliptic curve E is on the surface at ℓ with endomorphism ring isomorphic to an order $\mathcal{O}$ of $\mathcal{K}$, the conductor $c_E := [\mathcal{O}_\mathcal{K} : \mathcal{O}]$ is not divisible by ℓ. Moreover, Proposition 4.1 tells us that there are $1 + \left(\frac{d_E}{\ell}\right)$ horizontal isogenies and we know that the number of elliptic curves in this level equals the class number $h := h(d_E)$.

The nodes on the surface correspond to the ideal class group $\mathcal{C}\ell(\mathcal{O})$ which is a group of order h. Thus every subgroup of $\mathcal{C}\ell(\mathcal{O})$ has an order dividing h. Let $\mathfrak{a}$ be a prime ideal of $\mathcal{O}$ which lies above ℓ and has order d in $\mathcal{C}\ell(\mathcal{O})$. Then Exercise 25.3.7 of Galbraith [28] shows that there are d elliptic curves which are connected via ℓ-isogenies in a big cycle. Thus we can deduce the possibilities of ℓ-volcanoes from the number of vertices on the surface.

We can proceed in the following way to find a path between two ordinary elliptic curves E_0 and E_1 in the same ℓ-volcano. We begin with constructing ascending paths of isogenies starting at each E_i until it is no longer possible to go up. After that we connect those paths with horizontal isogenies.

For a short example we use the graph from FIGURE 6 and show how to construct a path between the nodes 38 and 138. First we compute ascending isogenies $38 \rightsquigarrow 72$, $72 \rightsquigarrow 63$ and $138 \rightsquigarrow 122$ until we reach the surface at $\ell = 2$ on both sides of the path. Afterwards we take horizontal 2-isogenies from both sides until we create a connection between these two nodes on the crater. As there are no more than two of such isogenies and we assumed the volcano to be connected, the crater is arranged in a circle and it is not possible to get in a loop before reaching the other node. In our example the connection is made after only one step through the isogeny $63 \rightsquigarrow 122$ or its dual. Finally we have to append the descending duals of the ascending path from the image curve to get an end-to-end path between our nodes.

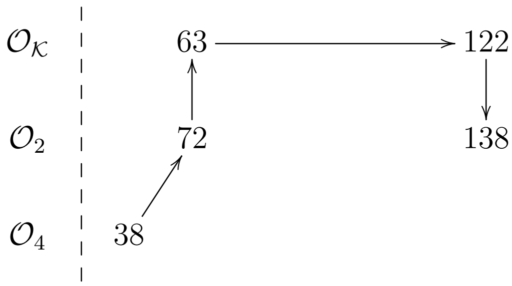


FIGURE 7: A Path in $G_{10}(\mathbb{F}_{149}, 2)$ between 38 and 138

Since this algorithm only works if E_0 and E_1 lie in the same volcano component and we construct a more general algorithm later, we will not implement it. But even there we need a procedure which computes a path to the surface of a ℓ-volcano, so we list a short pseudocode below.

ALGORITHM 4.5 `PathToCurveOnSurface(`E_0`, q, `ℓ`)`

INPUT: ordinary elliptic curve E_0 defined over $\mathbb{F}_q$, prime number ℓ with $\ell \nmid q$
OUTPUT: ordinary elliptic curve E_1 on the surface at ℓ and ascending path from E_0 to E_1

$X \leftarrow [E_0]$
repeat
  if exists an ascending isogeny starting from E_0 **then**
    append image curve E_1 to the list X
    $E_0 \leftarrow E_1$
  end if
until E_0 is on the surface at ℓ
return E_0, X;

Knowing the elliptic curves along the path from E_0 to E_1 we are able to construct an isogeny between them as a chain of ℓ-isogenies representing each step.

In contrast to the algorithm for constructing a path to the floor, this resulting path is deterministic, since in the case where an ascending isogeny exists, this isogeny is unique. If ℓ^e is the exact power of ℓ dividing c, in the worst case we have to compute roots of modular polynomials for every node in the tree beneath the node on the surface we want to reach. This tree has one node in its highest level which has ℓ children on the level below with ℓ children each in turn until the lowest level with ℓ^{e-1} nodes. Therefore the expected $\mathcal{O}(\ell^2 \log \ell \log q)$ operation of determining roots has to be performed

$$\sum_{i=0}^{e-1} \ell^i = \frac{\ell^e - 1}{\ell - 1} \in \mathcal{O}(\ell^{e-1})$$

times. In each step we have to compute the roots in $\mathbb{F}_q$ of the ℓ-modular polynomial but we only have to store the $e+1$ ones on the right path. Hence the overall complexity turns out to be as follows.

Proposition 4.8. *Let E be an elliptic curve defined over the finite field $\mathbb{F}_q$ and let $\ell \neq \operatorname{char} \mathbb{F}_q$ be a prime. Constructing and storing a path in a ℓ-volcano from E to the surface needs expected $\mathcal{O}(\ell^{e+1} \log \ell \log q)$ running time and $\mathcal{O}(e)$ storage in $\mathbb{F}_q$-operations resp. $\mathbb{F}_q$-elements.*

This path to the surface can be used for computing a path in a volcano component as we will describe now. When we have reached the surface on both sides, we have to add horizontal isogenies until we find a connection on the crater between those curves. But usually they do not live in the same volcano component of the graph $G_t(\mathbb{F}_q, \ell)$ and in that case it is impossible to find a path of ℓ-isogenies between them. Then we have to add more edges – that is, isogenies of different degree – and use the graph $G_t(\mathbb{F}_q, \mathcal{L})$ for a set of primes $\mathcal{L}$ to get a connection from E_0 to E_1.

Since it would destroy the nice volcano structure if we started with isogenies of all possible degrees as set of edges in the graph, in practice we successively use ascending isogenies in volcanoes of fixed degree until we reach a situation where we need to compute an isogeny between two elliptic curves with the same endomorphism ring $\mathcal{O}$. We emphasize that the important point is that the degree of the horizontal isogenies is not restricted to a single prime.

We have seen that the degree of any ascending isogeny has to divide the conductor $c = [\mathcal{O}_\mathcal{K} : \mathbb{Z}[\pi_q]]$. Thus we take each of the prime divisors $\ell_1, \cdots, \ell_r$ of c in turn and calculate ascending paths as in Algorithm A.6 of Appendix A. We start with the initial elliptic curves E_i and the first prime ℓ_1 and compute elliptic curves E_i'

which are on the surface at ℓ_1 and a path from E_i to E_{i1} in $G_t(\mathbb{F}_q, \ell_1)$. We repeat this with starting curves E_{ij} and the next degree ℓ_{j+1} for j from 1 to $r-1$.

Algorithm 4.6 `PathToGlobalSurface(E, q)`

Input: ordinary elliptic curve E defined over $\mathbb{F}_q$
Output: path to global surface

$c \leftarrow [\mathcal{O}_\mathcal{K} : \mathbb{Z}[\pi_q]]$
$X \leftarrow [E]$
for any prime divisor ℓ of c **do**
  $E \leftarrow$ elliptic curve on surface of ℓ reached by an
    ascending path starting at E
  append steps of that path to X
end for
return X

At the end we have two elliptic curves E_{ir} which are on the surface for all primes dividing c. Therefore it is no longer possible to go up in any way and the endomorphism ring of both E_{ir} has to be the maximal order $\mathcal{O}_\mathcal{K}$.

We have seen that for every path of ℓ-isogenies to the surface at ℓ we have an expected running time of $\mathcal{O}(\ell^{e+1} \log \ell \log q)$ where ℓ^e is the exact power of ℓ dividing c. Thus here we have the sum of this complexity for all divisors ℓ of c,

$$\begin{aligned} \mathcal{O}(\sum_{i=1}^{r} \ell_i^{e_i+1} \log \ell_i \log q) &\subseteq \mathcal{O}(\sum_{i=1}^{r} c^2 \log \ell_i \log q) \\ &\subseteq \mathcal{O}(c^2 \log q \sum_{i=1}^{r} \log \ell_i) \\ &\subseteq \mathcal{O}(c^2 \log c \log q) \end{aligned}$$

because $c = \prod \ell_i^{e_i}$ with $e_i \geq 1$ yields $\ell_i^{e_i+1} \in \mathcal{O}(c^2)$ and $\log c = \sum e_i \log \ell_i$ and thus $\sum \log \ell_i \in \mathcal{O}(\log c)$. We have to store every elliptic curve on the path which will have a length of $\sum e_i$ since for every ℓ_i we have a chain of e_i isogenies to the surface at ℓ_i. Thus we get for the algorithm of reaching the global surface the following complexity.

Proposition 4.9. *Let E be an ordinary elliptic curve defined over $\mathbb{F}_q$ such that $\operatorname{End} E$ is isomorphic to an order $\mathcal{O}$ in the imaginary quadratic field $\mathcal{K}$ with conductor $c := [\mathcal{O}_\mathcal{K} : \mathcal{O}]$. Finding a path of isogenies from E to an elliptic curve with endomorphism ring $\mathcal{O}_\mathcal{K}$ needs expected $\mathcal{O}(c^2 \log c \log q)$ running time and $\mathcal{O}(\log c)$ storage.*

This step includes factorizing the conductor which is another precomputation we make in addition to precomputing the modular polynomials. After those vertical steps both elliptic curves we deal with have endomorphism ring $\mathcal{O}_\mathcal{K}$ and we have to find a path between them. Hence we regard the subgraph of the used isogeny graph named $G_{t,\mathcal{O}_\mathcal{K}}(\mathbb{F}_q, \mathcal{L})$ which only consists of vertices of elliptic curves with endomorphism ring $\mathcal{O}_\mathcal{K}$. This graph corresponds to $\mathcal{C}\ell(\mathcal{O}_\mathcal{K})$ with the above-mentioned results from SECTION 3, so – assuming a form of the generalized RIEMANN hypothesis – it is fully connected due to THEOREM 3.8.

There are several general methods to find a path between two given vertices of a fully connected graph which can be used here. The first one is a bi-directional breadth first search and discussed in GALBRAITH [27]. That means we start with two single-node graphs with nodes E_0 resp. E_1 which are on the same level in the isogeny graph, usually the top level. We proceed to take random primes from the set $\mathcal{L}$, calculate all neighbors of all nodes in both graphs and add them and their edges to the corresponding graph until the two graphs connect.

ALGORITHM 4.7 `Path(E0, E1, q, B)`

INPUT: ordinary elliptic curves E_0, E_1 defined over $\mathbb{F}_q$ with $\operatorname{End} E_0 \cong \operatorname{End} E_1 \cong \mathcal{O}_\mathcal{K}$, bound B for isogeny degrees
OUTPUT: path in isogeny graph $G_{t,\mathcal{O}_\mathcal{K}}(\mathbb{F}_q, \mathcal{L})$ between E_0 and E_1 if possible, [ ] otherwise

$X_0 \leftarrow [E_0]$
$X_1 \leftarrow [E_1]$
$B \leftarrow \min\{6 \cdot (\log |d_\mathcal{K}|)^2, B\}$
$\mathcal{L} \leftarrow \{$primes $\ell \leq B \mid \left(\frac{d_\mathcal{K}}{\ell}\right) \neq -1\}$
choose random $\ell \in \mathcal{L}$
$i \leftarrow 0$
while X_0 and X_1 are disjoint **do**
    compute all ℓ-neighbors of all nodes of X_i
    append them to X_i
    if $X_i \cap X_{1-i} \neq \emptyset$ **then**
        reconstruct path in the graphs to the collision
        disjoint $\leftarrow$ **false**
    end if;
    $i \leftarrow 1 - i$
    choose a new isogeny degree ℓ different from the last
end while
return path from $j(E_0)$ to $j(E_1)$

Thus after the computation of the paths to the surface of which we already know the complexity, we take a random $\ell \in \mathcal{L}$ and have to determine the $\ell + 1$ neighbors of the latest E_0 in expected $\mathcal{O}(\ell^2 \log \ell \log q)$. In the worst case we have to check for ℓ of them if they are reached by a descending isogeny until we find an horizontal one. This check can by done in expected $\mathcal{O}(e \cdot \ell^2 \log \ell \log q)$ for each of the ℓ neighbors.

Assuming GRH, the graph is connected when we use $B = 6(\log |d_{\mathcal{K}}|)^2$, thus the while loop teminates. To see how many repetitions of this loop we have to expect, we use the fact that the crater of such an ordinary isogeny volcano is known to be an expander graph $G = (V_G, E_G)$ with h vertices, so there exists a constant $u \in \mathbb{R}_{>0}$ with $u \cdot |U| \leq \partial_v(U)$ for every subset U of V_G with $|U| \leq h/2$. We start with $X_0 = \{j(E_0)\}$ and $Y_0 = \{j(E_1)\}$ and add the next ℓ-neighbors in each step to get X_{i+1} from X_i and Y_{i+1} from Y_i.

We repeat that until there is a node which is as well in X_{i+1} as in Y_{i+1}. Each of the graphs X_i and Y_i fulfill that their number of nodes is less than $h/2$ if no connection is found yet. Thus we can iteratively get

$$\begin{aligned} |X_i| &= |X_{i-1}| + |\partial_v(X_{i-1})| \\ &\geq |X_{i-1}| + u \cdot |(X_{i-1})| \\ &\geq (1+u)^i \end{aligned}$$

and the same for every Y_i. Under the assumption that the new nodes behave like uniformly drawn vertices, the birthday paradox tells us that we expect the graph to be connected when we get

$$|X_i| + |Y_i| \geq \sqrt{\pi h}.$$

This is true for $i \geq \log_{1+u}(\sqrt{\pi h})$, thus we need expected

$$\begin{aligned} \mathcal{O}(\log_{1+u}(\sqrt{\pi h})) &= \mathcal{O}(\tfrac{1}{2}(\log_{1+u} \pi + \log_{1+u} h)) \\ &= \mathcal{O}(\log_{1+u} h) \\ &= \mathcal{O}(\log h) \end{aligned}$$

iterations in the while loop. The last step holds since logarithms for different bases only differ by a factor.

The pseudocode is quite vague since it is somewhat tedious to store all needed information like distance from the origin E_i and the predecessor node in an ordered manner, but in return this method guaranties to find the shortest path between two given isogenous ordinary elliptic curves in $G_t(\mathbb{F}_q, \mathcal{L})$. The degree of the resulting isogeny is $\mathcal{L}$-smooth, but there can be an isogeny with smaller degree between E_0 and E_1 which is not found by this algorithm.

For example the isogeny we found in FIGURE 7 is a chain of four 2-isogenies from an elliptic curve with j-invariant 38 to one with j-invariant 138 and thus has degree 2^4. But we can compute that there is a 5-isogeny from the elliptic curve with j-invariant 38 to an elliptic curve with j-invariant 87 and from there we can append a 2-isogeny to the image curve with j-invariant 138. This isogeny has degree $10 < 2^4$ but is not found if we only regard isogeny degrees less than five.

As in the case with only one volcano component we need expected $\mathcal{O}(\log h)$ iterations of the while loop to get a connection. In each step of the loop we have to compute all neighbors of all $\#X_i$ nodes in the graph. Since we know that the algorithm stops when $\#X_0 + \#X_1 \geq \sqrt{\pi h}$, we get $\#X_i \in \mathcal{O}(\sqrt{h})$. We have used several times before that computing the ℓ-neighbors of a node can be done in expected $\mathcal{O}(\ell^2 \log \ell \log q)$ and all isogeny degrees ℓ are bounded by $6(\log |t^2 - 4q|)^2$, so we can write $\ell \in \mathcal{O}((\log q)^2)$. For every new node in X_i we have to check if it already appeared in the other set of nodes X_{1-i}. Basic look-up algorithms achieve this in expected $\mathcal{O}(\log \#X_{1-i})$ when the elements are stored in a appropriate way, so this adds another $\mathcal{O}(\log h)$ in every step of the loop.

To construct a path from $j(E_0)$ to $j(E_1)$ out of the connected graphs X_0 and X_1 we have different possibilities. If we store some extra-information like the array index of the predecessor, this can be done with running back through the graph from the connection point to both starting points and write down the nodes along the path.

When we want no additional storage, in the worst case we have to visit every element of the graph. Both versions are not relevant for the overall complexity since they are bounded by $\mathcal{O}(\sqrt{h})$. We have to store all nodes in the sets X_0 and X_1 which will be up to $\mathcal{O}(\sqrt{h})$ field elements, although the returned chain of elliptic curves will only have a length of $\mathcal{O}(\log h)$. Summed up in this part we get the complexity below.

PROPOSITION 4.10. *Let E_0 and E_1 be isogenous elliptic curves defined over the finite field $\mathbb{F}_q$ having endomorphism rings isomorphic to the maximal order $\mathcal{O}_\mathcal{K}$ of the imaginary quadratic field $\mathcal{K}$. Further let $B \leq 6(\log |d_\mathcal{K}|)^2$ be a bound such that the ideal class $\mathcal{C}\ell(\mathcal{O}_\mathcal{K})$ is generated by ideals of norm less or equal to B.*

Assuming GRH, *computing an isogeny $\phi : E_0 \to E_1$ with the above described breadth-first search algorithm can be done in expected $\mathcal{O}(\sqrt{h} \log h((\log q)^5 \log \log q + \log h))$ running time and $\mathcal{O}(\sqrt{h})$ storage.*

It is also possible to only look for all ℓ-neighbors of the border $\partial_v(X_i)$ which are not elements of X_i themselves, that is, add only new nodes to the sets. This helps to avoid backtracking and counting different nodes more than once. In both variants we get the same complexity since still the number of nodes in the sets X_i has to become bigger than $\sqrt{\pi h}$ for them to connect and in terms of the $\mathcal{O}$-notation it also takes the same expected number of iterations.

Another possibility is to take two random walks in $G_{t,\mathcal{O}}(\mathbb{F}_q, \mathcal{L})$ starting at E_0 and E_1 and storing their steps in two separate lists instead of performing a breadth-first search. If one walk reaches an element which already appeared in the other list, we have a connection.

Algorithm 4.8 `RandomPath(`E_0`, `E_1`, q, B)`

Input: ordinary elliptic curves E_0, E_1 defined over $\mathbb{F}_q$ with $\operatorname{End} E_0 \cong \operatorname{End} E_1 \cong \mathcal{O}_\mathcal{K}$, bound B for isogeny degrees
Output: path in isogeny graph $G_{t,\mathcal{O}}(\mathbb{F}_q, \mathcal{L})$ between E_0 and E_1 if possible, [ ] otherwise

$X_0 \leftarrow [j(E_0)]$
$X_1 \leftarrow [j(E_1)]$
$B \leftarrow \min\{6 \cdot (\log |d_\mathcal{K}|)^2, B\}$
$\mathcal{L} \leftarrow \{$primes $\ell \leq B \mid \left(\frac{d_\mathcal{O}}{\ell}\right) \neq -1\}$
choose random $\ell \in \mathcal{L}$
$i \leftarrow 0$
while X_0 and X_1 are disjoint **do**
    $jE_i \leftarrow$ random ℓ-neighbor of E_i
    append $j(E_i)$ to X_i
    if $j(E_i) \in X_{1-i}$ **then**
        truncate X_{1-i}
        disjoint $\leftarrow$ **false**
    end if;
    $i \leftarrow 1 - i$
    choose a new isogeny degree ℓ different from the last
end while
return X_0 cat Reverse(X_1)

Again, the same considerations regarding complexity arising from the size of X_0 and X_1 hold, so the algorithm terminates when we have $\#X_0 + \#X_1 \geq \sqrt{\pi h}$. In every iteration we only get one new node on every side of the walk, have to check if it already appears in the other set of nodes which takes $\mathcal{O}(\log h)$ running time and have to compute its neighbors in expected $\mathcal{O}((\log q)^5 \log\log q)$. The resulting chain has length $\mathcal{O}(\sqrt{h})$ and the elements of it are exactly the ones we have to store. Thus we get a complexity as in the next result.

Proposition 4.11. *Let E_0 and E_1 be isogenous elliptic curves defined over the finite field $\mathbb{F}_q$ having endomorphism rings isomorphic to the maximal order $\mathcal{O}_\mathcal{K}$ in the imaginary quadratic field $\mathcal{K}$. Further let $B \leq 6(\log |d_\mathcal{K}|)^2$ be a bound such that the ideal class $\mathcal{C}\ell(\mathcal{O}_\mathcal{K})$ is generated by ideals of norm less or equal to B.*

Assuming GRH, *computing an isogeny $\phi : E_0 \to E_1$ with the above described random walk algorithm can be done in expected $\mathcal{O}(\sqrt{h}((\log q)^5 \log\log q + \log h))$ running time and $\mathcal{O}(\sqrt{h})$ storage.*

This time we also get the path immediately out of the returned graph since in every step we have a designated successor and predecessor and can return the combined chains obtained through the random walk. Another advantage of this variant of the algorithm is, that it can be parallelized. We will give a brief description of that concept along with some other improvements of the basic algorithm below.

Before that we still have to mention that although this algorithm gives us the way in the isogeny graph which provides a chain of isogenies between the given elliptic curves E_0 and E_1, it does not yet compute the isogenies. This can be done in expected $\mathcal{O}(\ell^3)$ at every step along the provided way.

The computed isogenies and image curves have to be combined to an isogeny $\phi' : E_0 \to E'$ where we have $j(E') = j(E_1)$. Note that this last image curve E' can be a quadratic twist of E_1 and in this case we have to append an isomorphism $\lambda : E' \to E_1$ to get our desired isogeny $\phi = \lambda \circ \phi' : E_0 \to E_1$.

Let us give a short summary of the steps necessary for computing a chain of isogenies between arbitrary isogenous ordinary elliptic curves defined over $\mathbb{F}_q$ and the expected complexity of each part.

1. Compute the modular polynomials Φ_{ℓ_i} for every ℓ_i dividing the conductor c.
   - ✦ **Running time:** $\mathcal{O}(c^3 \log c \log\log c)$
   - ✦ **Storage:** $\mathcal{O}(c^2)$
2. Find a chain of isogenies of degree dividing c from E_0 resp. E_1 to the global surface at E_0' resp. E_1'.
   - ✦ **Running time:** $\mathcal{O}(c^2 \log c \log q)$
   - ✦ **Storage:** $\mathcal{O}(\log c)$
3. Compute the modular polynomials Φ_ℓ for every $\ell \in \mathcal{L}$.
   - ✦ **Running time:** $\mathcal{O}((\log q)^8 \log\log\log q)$
   - ✦ **Storage:** $\mathcal{O}((\log q)^6 / \log\log q)$

4. Compute random walks starting at the nodes E_0' resp. E_1' until they connect and store a path between E_0' and E_1'.
   - ✦ **Running time:** $\mathcal{O}(\sqrt{h}((\log q)^5 \log\log q + \log h))$
   - ✦ **Storage:** $\mathcal{O}(\sqrt{h})$
5. Compute isogenies along the chains $E_0 \rightsquigarrow E_0' \rightsquigarrow E_1' \rightsquigarrow E_1$.
   - ✦ **Running time:** $\mathcal{O}(c^3 \log c + (\log q)^6 \log h)$
   - ✦ **Storage:** $\mathcal{O}(c^2 \log c + (\log q)^4 \log h)$

All together for computing an isogeny between given isogenous ordinary elliptic curves we have to execute all the above steps consecutively and get a running time of expected

$$\begin{aligned}\mathcal{O}(c^3 \log c \log\log c \quad &+ \quad c^2 \log c \log q \\ &+ \quad (\log q)^8 \log\log\log q \\ &+ \quad \sqrt{h}((\log q)^5 \log\log q + \log h) \\ &+ \quad c^3 \log c + (\log q)^6 \log h).\end{aligned}$$

These complexities are expressed in terms of q, c and h. We have seen at the end of Section 2.1.2 that in the worst cases we get $h \in \mathcal{O}(\sqrt{q} \log q)$. Thus the terms $(\log q)^8 \log\log\log q$ and $\log h \cdot (\log q)^6)$ under this condition are dominated by $\sqrt{h} \log h((\log q)^5 \log\log q + \log h)$ and since also $c^3 \log c$ can be dropped in favor of $c^3 \log c \log\log c$ we get

$$\mathcal{O}(c^2 \log c(\log\log c + \log q) \quad + \quad q^{1/4}(\log q)^{1/2}(\log q)^5 \log\log q)$$

Galbraith [27] says that usually the conductor c is $\log q$-smooth. Thus we assume $c \in \mathcal{O}((\log q)^v)$ for a positive integer v and all the terms containing c can be neglected against the $q^{1/4}$-term and we can simplify the overall running time further to the following result.

Theorem 4.12 (Computing Ordinary Isogeny – Running Time)**.** *Let E_0 and E_1 be isogenous elliptic curves defined over the finite field $\mathbb{F}_q$ with endomorphism rings isomorphic to the maximal order $\mathcal{O}_\mathcal{K}$ in the imaginary quadratic field $\mathcal{K}$. Further let $B \leq 6(\log|d_\mathcal{K}|)^2$ be a bound such that the ideal class $\mathcal{C}\ell(\mathcal{O}_\mathcal{K})$ is generated by ideals of norm less or equal to B.*

Assuming GRH*, $h \in \mathcal{O}(\sqrt{q}\log q)$ and $c \in \mathcal{O}((\log q)^v)$ for some $v \in \mathbb{N}$, computing an isogeny $\phi : E_0 \to E_1$ can be done in expected $\mathcal{O}(q^{1/4}(\log q)^{1/2}(\log q)^5 \log\log q)$ running time.*

With the same arguments concerning h and c the storage as collected in the steps above can be shrunk similarly.

Theorem 4.13 (Computing Ordinary Isogeny – Storage). *Let E_0 and E_1 be isogenous elliptic curves defined over the finite field $\mathbb{F}_q$ with endomorphism rings isomorphic to the maximal order $\mathcal{O}_\mathcal{K}$ in the imaginary quadratic field $\mathcal{K}$. Further let $B \leq 6(\log|d_\mathcal{K}|)^2$ be a bound such that the ideal class $\mathcal{C}\ell(\mathcal{O}_\mathcal{K})$ is generated by ideals of norm less or equal to B.*

Assuming GRH, *$h \in \mathcal{O}(\sqrt{q}\log q)$ and $c \in \mathcal{O}((\log q)^v)$ for some $v \in \mathbb{N}$, computing an isogeny $\phi : E_0 \to E_1$ needs expected $\mathcal{O}(q^{1/4}(\log q)^{1/2})$ storage.*

Thus we have a $\widetilde{\mathcal{O}}(q^{1/4})$ algorithm both in running time and storage. There have been some endeavors to improve the constants or logarithmic terms, or to parallelize the algorithm, but this is the main complexity class for computing isogenies at the moment.

Improvements Of the Basic Algorithm. During the time several modifications of this algorithm have been proposed to attain slightly better complexities although the complexity class does not change.

In 2002 Galbraith, Hess and Smart [29] developed a low-storage version of this algorithm which can be distributed to several processors. It uses pseudorandom walks in a Pollard-rho style algorithm with distinguished points. That means that the next step of the random walk is determined by the current node and thus when any walks meet at a point, they carry on identically afterwards. This can be used to distribute such pseudorandom walks on clients and let a server manage the walks and their output.

The GHS algorithm works on the ideal class side of the picture and computes ideals classes by multiplying the current with the ideal representing the isogeny in each step where the walk starts with the trivial ideal. When two walks collide with the ideals $\mathfrak{a}$ and $\mathfrak{b}$, the complete isogeny is represented by the ideal $\mathfrak{a}\mathfrak{b}^{-1}$ which usually has a large norm. The authors show how to reduce and smooth this ideal with index calculus methods to get an ideal corresponding to a shorted isogeny path in the graph.

For our work we restricted to the easier to implement basic version of the algorithm. Our later improvements in the $\mathbb{F}_p$-rational supersingular case are already a quite evident improvement there.

A further very plausible idea of Galbraith and Stolbunov [31] from 2011 makes use of the often mentioned fact that isogenies of smaller degree are faster to compute. They suggest to prefer small primes in the steps and thus draw the random primes from an uneven partitioning and not the uniform distribution on the set of possible primes. With this approach the length of the path obtained by the random walk increases, but eventually the running time is better when the isogenies are computed in that way.

Even though in our complexity analysis the step with computing isogenies is not dominant, the random prime ℓ also plays an important role in the most expensive part of constructing the path since there we have to factor the ℓ-th modular polynomial in every step. We estimated ℓ with the upper bound $(\log q)^2$ and used this number in the analysis. When smaller primes appear more often, the factorization is cheaper in more steps and thus the overall running time will be shorter in practice.

4.2 The Supersingular Isogeny Problem

Due to Theorem 2.33, for $\operatorname{char} \mathbb{F}_q = p < 11$ there is only a single j-invariant in $\mathbb{F}_q$ such that elliptic curves with this j-invariant are supersingular, so the question of finding a path is irrelevant. Especially we can exclude the cases of characteristic 2 and 3 from our considerations, which turns out to be comfortable in the next subsection. For now we deal with the general supersingular isogeny problem.

Problem 8 (Supersingular Isogeny Problem). *Let q be a prime power and E_0, E_1 supersingular elliptic curves over $\mathbb{F}_q$. Compute an isogeny $\phi : E_0 \to E_1$.*

As mentioned before, supersingular elliptic curves are always defined over $\mathbb{F}_p$ or over $\mathbb{F}_{p^2}$ but an isogeny between them can be defined over a higher field extension. Thus we often use the *full supersingular isogeny graph* $G_0(\bar{\mathbb{F}}_p, \mathcal{L})$ for general isogeny computations in the supersingular case, where $\mathcal{L}$ is a set of small primes with $p \notin \mathcal{L}$.

Such a graph $G_0(\bar{\mathbb{F}}_p, \mathcal{L})$ has the great advantage that it is always fully connected with $\mathcal{L} = \{\ell\}$ for every prime $\ell \neq p$ as can be seen in Mestre's work [57] or Corollary 78 of Kohel [45]. Therefore it is always possible to find a path between two arbitrary vertices in it, no matter what set $\mathcal{L}$ we use. Usually we choose $\mathcal{L} = \{2\}$ for computations since those isogenies of degree 2 are the fastest to compute. The simplest formulation of the problem in the setting of graphs is like follows.

Problem 9 (Supersingular Isogeny Graph Problem). *Let $p > 3$ be a prime. Given $j_0, j_1 \in G_0(\bar{\mathbb{F}}_p, 2)$, compute a path between them.*

In contrast to the ordinary case we have no immediate connection to a graph of elliptic curves over number fields and the ideal class group since Theorem 3.9 provides no isomorphism between endomorphism rings of arbitrary supersingular elliptic curves and their lifts since their endomorphism ring is too big. Thus we do not have the comfortable volcano structure of the graph and it is not as easy to explore. Especially, the ordinary algorithms we developed before are not applicable. We will investigate the supersingular graphs and possible algorithms for computing paths in them in the following part.

4.2.1 Supersingular Isogeny Graphs

We want to deal briefly with the full supersingular isogeny graphs in this section and demonstrate their irregular structure as well as the best currently known algorithm for finding a path in one of them. This is the foundation for being able to compare the properties we develop afterwards for supersingular elliptic curves defined over $\mathbb{F}_p$ with the general case.

Graph Structure and Algorithms. Let p be a prime and E be a supersingular elliptic curve with j-invariant $j \in \mathbb{F}_{p^2}$ and let $\ell \neq p$ be a prime. We have seen in Theorem 2.27 that the modular polynomial $\Phi_\ell(j, Y)$ splits completely over $\mathbb{F}_{p^2}$ and since every root of this polynomial yields a neighbor of E, there are $\ell + 1$ outgoing non-equivalent isogenies from every such supersingular elliptic curve E. Hence for every $\ell \neq p$ the graph $G_0(\bar{\mathbb{F}}_p, \ell)$ is $\ell + 1$-regular and we have already seen that it is a fully connected graph. Especially this is true for $\ell = 2$ and 2-isogenies are the fastest ones to compute. Therefore we usually attempt to find paths in $G_0(\bar{\mathbb{F}}_p, 2)$.

As we discussed in Section 2.2, endomorphism rings of supersingular elliptic curves in characteristic p are isomorphic to maximal orders in a quaternion algebra $\mathcal{A}$. In fact, $\mathcal{A}$ is the quaternion algebra over $\mathbb{Q}$ which is ramified at p and infinity. The full supersingular isogeny graph $G_0(\bar{\mathbb{F}}_p, \ell)$ can be shown to be a Ramanujan graph (e.g. page 535 of Galbraith [28]), so it is an expander graph.

Thus for finding a chain of 2-isogenies between two given nodes in $G := G_0(\bar{\mathbb{F}}_p, 2)$ we can use a simple bi-directional search with a random walk as in the next code.

Algorithm 4.9 `SupersingularPath(E`$_0$`, E`$_1$`, p)`

Input: `supersingular elliptic curves` E_0, E_1 `defined over` $\mathbb{F}_{p^2}$
Output: `path in full 2-isogeny graph between` E_0 `and` E_1

$X_0 \leftarrow [j(E_0)]$
$X_1 \leftarrow [j(E_1)]$
$i \leftarrow 0$
while X_0 `and` X_1 `are disjoint` **do**
    $E_i \leftarrow$ `random neighbor of` E_i `in` $G_0(\bar{\mathbb{F}}_p, 2)$
        `which is different from the one before`
    `append` $j(E_i)$ `to` X_i
    if $E_i \in X_{1-i}$ **then**
        `truncate` X_{1-i}
        `disjoint` $\leftarrow$ `false`
    end if
    $i \leftarrow 1 - i$
end while
return X_0 `joined with reversed` X_1

This works analogously to the approach on craters of ordinary isogeny volcanoes and the complexity analysis follows along the same lines. Since the size of the graph is bigger though, the algorithm is slower than the ordinary one, even though we are able to use only 2-isogenies. As in the ordinary case we have to compute the isogenies along the path afterwards and possibly combine them with another isogeny to the twist of the last elliptic curve in the chain to reach the right isomorphism class of the elliptic curve with j-invariant j_1.

Due to the analysis of the bi-directional birthday attack in PROPOSITION 2.46 we expect a collision in G when

$$\#X_0 + \#X_1 \geq \sqrt{\pi N}$$

where N is the number of vertices in the graph and X_0 resp. X_1 are the growing sets of nodes in the chain after the k-th iteration. Since for our graphs we have $N \approx p/12$ this means we expect to perform the operations in the while loop $\mathcal{O}(\sqrt{p})$ times. In each step of the loop we compute a random ℓ-neighbor of the last elliptic curve in the chain X_i like before in expected $\mathcal{O}(\ell^2 \log \ell \log q)$ and check if it already appears in the other chain X_{1-i}, what can be done in $\mathcal{O}(\log \#X_{1-i})$. Because we take $\ell = 2$ and have $\#X_{1-i} \in \mathcal{O}(\sqrt{p})$, this becomes the complexity below.

PROPOSITION 4.14. *Let E_0 and E_1 be supersingular elliptic curves defined over $\mathbb{F}_{p^2}$ where p is a prime. Computing an isogeny $\phi : E_0 \to E_1$ of 2-power degree can be done in expected $\mathcal{O}(p^{1/2} \log p)$ running time and $\mathcal{O}(p^{1/2})$ storage.*

To get a non-backtracking random walk we have to ensure that once we make a step from a node j_0 to a node j_1 the next step is not back to j_0. Since we determine neighbors of j_1 by roots of the modular polynomial $\Phi_2(j_1, Y)$, we can avoid j_0 by only regarding roots of $\Phi_2(j_1, Y)/(Y - j_0)$. If the modular polynomial evaluated at j_1 has a double root at j_0 though, it cannot be guarantied that j_0 is avoided. But if we exclude the node j_0 completely as next neighbor, we can happen to get stuck in a dead end if all outgoing isogenies from the node j_1 lead to j_0. For example, this always occurs for $j_1 = 0$ since we have

$$\begin{aligned} \Phi_2(0, Y) &= Y^3 - 162000Y^2 + 8748000000Y - 157464000000000 \\ &= (Y - 54000)^3 \end{aligned}$$

as a polynomial from $\mathbb{Z}[Y]$. Of course the same factorization holds when the coefficients are interpreted as elements from $\mathbb{F}_{p^2}$ and thus the three image curves reached by an outgoing 2-isogeny from a supersingular elliptic curve with j-invariant $j_1 = 0$ all have the same j-invariant $j_0 \equiv 54000 \pmod{p^2}$.

There are more subtle ways of regarding the concept of *non-backtracking* like trying to avoid short cycles as well, see GALBRAITH-ZHAO [32] for a discussion. Another approach is to completely forbid that a path intersects with itself but again we can get the problem that all three outgoing edges lead to nodes which have already been visited. Then we have to delete the vertex from the path and choose another neighbor from the vertex before. If the same situation arises there again, we have to repeat this procedure recursively.

4.2.2 Restriction to $\mathbb{F}_p$-rational Elliptic Curves

We know from THEOREM 2.33 that there are

$$\#S_{p^2} = \left\lfloor \frac{p}{12} \right\rfloor + \begin{cases} 0 & \text{if } p \equiv 1 \pmod{12} \\ 1 & \text{if } p \equiv 5 \pmod{12} \\ 1 & \text{if } p \equiv 7 \pmod{12} \\ 2 & \text{if } p \equiv 11 \pmod{12}. \end{cases}$$

supersingular j-invariants in $\mathbb{F}_{p^2}$, so the graph $G_0(\bar{\mathbb{F}}_p, 2)$ will have about $p/12$ nodes. When we want to compute the edges in this graph and draw the complete picture of it, we must know how these vertices are labeled, that is, which j-invariants are supersingular in this situation. The `MAGMA` command `SupersingularPolynomial(p)` yields a polynomial over $\mathbb{F}_p$ whose roots are just the supersingular j-invariants from $\mathbb{F}_{p^2}$. For big primes p though it is impractical to factor a polynomial of degree $\lfloor p/12 \rfloor$, so we need another method to find supersingular elliptic curves.

First we note that it is sufficient to determine one supersingular elliptic curve since from that one we can construct other ones through random walks on a supersingular isogeny graph. SUTHERLAND [84] gives a nice overview over classical strategies for solving that problem and introduces a new method for this issue as we will briefly describe. He states that given a random elliptic curve defined over $\mathbb{F}_{p^2}$, `Magma` uses a point counting method to verify if it is supersingular or not, using that supersingular elliptic curves E fulfill $E(\mathbb{F}_q) \equiv 1 \pmod{p}$. This approach has a complexity of $\widetilde{\mathcal{O}}((\log p)^4)$ whereas his new algorithm runs in $\widetilde{\mathcal{O}}((\log p)^3)$.

For it we use the structure of the ordinary resp. supersingular isogeny graph. We have seen that the supersingular graph $G_0(\bar{\mathbb{F}}_p, \ell)$ is a $\ell + 1$-regular graph, so every node has exactly $\ell + 1$ outgoing edges. This is not true for ordinary graphs, since the nodes on the floor of the volcano have only one outgoing edge which is ascending. Further we know that the depth d of the volcano is at most $\log_\ell \sqrt{4q}$.

Thus when we take descending paths in a volcano, we reach the floor after k steps for some integer $1 \leq k \leq \log_\ell \sqrt{4q}$.

Let us have an elliptic curve E_0 with $\ell+1$ outgoing edges where we do not know if it is ordinary or supersingular and start a non-backtracking random walk on the isogeny graph containing E_0. Let $e = (j_0, j_1)$ be the first edge in the path. When E_0 is ordinary and the edge is descending, it is not possible to construct a path with length $k > \log_\ell \sqrt{4q}$ without reaching the floor first. On the contrary, if E_0 is supersingular, we will reach no dead end for any length of path.

In practice we use 2-isogenies again since they are the fastest to compute. We factor the modular polynomial $\Phi_2(j(E_0), Y)$ and start paths in three directions. As soon as we find a node where the modular polynomial has only a single root, we know that E_0 is ordinary. If this does not happen after $\log \sqrt{4q}$ iterations, E_0 is supersingular. This is a nice application of the isogeny graph's structure.

Sutherland [84] also mentions a CM-method which he used to construct supersingular elliptic curves for testing his algorithm for known supersingular input. It is based on Bröker [5] where an algorithm is proposed to return a supersingular elliptic curve in characteristic p which has a complexity of $\widetilde{\mathcal{O}}((\log p)^3)$. We use this algorithm to construct random start and end points of our algorithms to test how fast the computation of an isogeny can be. It can be found in Algorithm A.8.

The subgraph of $G(\bar{\mathbb{F}}_p, \ell)$ which consists of nodes representing elliptic curves with j-invariants in $\mathbb{F}_p$ is much smaller than the whole graph – it has roughly $\sqrt{p}$ vertices instead of roughly $p/12$ as seen in Theorem 2.34.

Since we have seen that the complexity of finding a path in a fully connected graph like in Algorithm A.9 depends on the number of vertices, the idea is to use this smaller graph for an improved algorithm to solve at least the following restricted problem in a better running time than $\widetilde{\mathcal{O}}(\sqrt{p})$ with the algorithm in the full graph.

Problem 10 (Supersingular Isogeny Problem over $\mathbb{F}_p$)**.** *Let p be a prime and E_0, E_1 supersingular elliptic curves over $\mathbb{F}_p$. Compute an isogeny $\phi : E_0 \to E_1$.*

In contrast to the full supersingular isogeny graph though, such subgraphs do not have to be connected, so we cannot guaranty that a path of ℓ-isogenies exists between arbitrary supersingular elliptic curves over $\mathbb{F}_p$. The first example where this problem occurs is $G_0(\bar{\mathbb{F}}_{53}, 2)$ and is plotted below. In the picture α and $\bar{\alpha}$ are supposed to denote j-invariants in $\mathbb{F}_{53^2} \setminus \mathbb{F}_{53}$. There are three isogenies starting at the node 0 which have the same dual, a behavior we explained in Section 2.1. The isogeny displayed as single loop from 50 to itself can be checked to be its own dual.

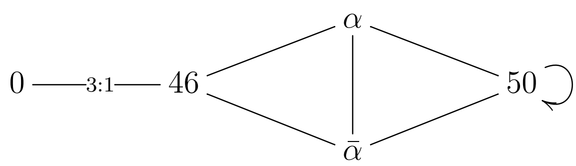


FIGURE 8: The Full Supersingular Isogeny Graph $G_0(\overline{\mathbb{F}}_{53}, 2)$

This graph is 3-regular and obviously the subgraph with nodes in $\mathbb{F}_{53}$ is not connected. Thus it is impossible to construct a path of 2-isogenies from 0 to 50 without going via j-invariants of $\mathbb{F}_{53^2} \setminus \mathbb{F}_{53}$. But as soon as we add the isogenies of degree 3 in this subgraph, it gets fully connected as displayed in the following picture. There the 2-isogenies are drawn as dashed lines and the 3-isogenies as solid lines.

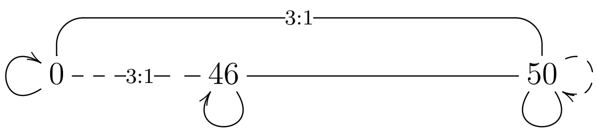


FIGURE 9: $\mathbb{F}_p$-rational Subgraph of $G_0(\bar{\mathbb{F}}_{53}, \{2, 3\})$

So the problem becomes a similar one as in the ordinary case – we have to find a set of small primes $\mathcal{L}$ such that the $\mathbb{F}_p$-rational subgraph of $G_0(\bar{\mathbb{F}}_p, \mathcal{L})$ is connected. We denote this $\mathbb{F}_p$-rational subgraph with $G_0(\bar{\mathbb{F}}_p, \mathcal{L}) \cap \mathbb{F}_p$ and stress that this is different from the $\mathbb{F}_p$-rational isogeny graph $G_0(\mathbb{F}_p, \mathcal{L})$ since the nodes represent $\bar{\mathbb{F}}_p$-isomorphism classes of supersingular elliptic curves defined over $\mathbb{F}_p$ and not $\mathbb{F}_p$-isomorphism classes.

In contrast to the ordinary isogeny volcano we do not have a nice and regular structure of the graph $G_0(\bar{\mathbb{F}}_p, \mathcal{L}) \cap \mathbb{F}_p$ though. So, even provided that we have such a set, it remains to be seen how the graph structure looks like and how it can be used to construct an algorithm to compute isogenies. To be explicit, we are interested in the next problem.

PROBLEM 11 (Supersingular Isogeny Graph Problem over $\mathbb{F}_p$)**.** *Let p be a prime and $\mathcal{L}$ a set of small primes with $p \notin \mathcal{L}$. Given $j_0, j_1 \in G_0(\bar{\mathbb{F}}_p, \mathcal{L}) \cap \mathbb{F}_p$, compute a path between them (if possible).*

The first noticeable difference between this graph problem and the arithmetic SUPERSINGULAR ISOGENY PROBLEM OVER $\mathbb{F}_p$ stated at the beginning of this section is that the vertices of the graph $G_0(\bar{\mathbb{F}}_p, \mathcal{L}) \cap \mathbb{F}_p$ represent $\bar{\mathbb{F}}_p$-isomorphism classes of supersingular elliptic curves over $\mathbb{F}_p$ and not $\mathbb{F}_p$-isomorphism classes.

In the ordinary case this makes no difference, since there an elliptic curve and its twists have a different number of points and hence are not isogenous to each other. Thus for $t \neq 0$ we are able to interpret $G_t(\mathbb{F}_p, \mathcal{L})$ as a proper subgraph of $G_t(\bar{\mathbb{F}}_p, \mathcal{L})$.

For $t = 0$ this is not possible as there are isogenous supersingular elliptic curves which are isomorphic over $\bar{\mathbb{F}}_p$ but not over $\mathbb{F}_p$. Therefore j-invariants – as in the graph $G_0(\bar{\mathbb{F}}_p, \mathcal{L}) \cap \mathbb{F}_p$ – are not a good representation of supersingular elliptic curves defined over $\mathbb{F}_p$ since they ignore any twists. It turns out to be useful to have a look at the rational supersingular isogeny graph $G_0(\mathbb{F}_p, \mathcal{L})$.

Relation of the Graphs. Firstly, we remark that the rational supersingular isogeny graph has exactly twice as many nodes as $G_0(\bar{\mathbb{F}}_p, \mathcal{L}) \cap \mathbb{F}_p$ and thus can under no circumstances be seen as a subgraph of the latter. This relation comes from the fact that the number of $\mathbb{F}_p$-isomorphism classes of elliptic curves defined over $\mathbb{F}_p$ with given j-invariant j can be deduced due to Proposition 3.15 as

$$\begin{cases} 6 & \text{if } j = 0 \qquad \text{and } p \equiv 1 \pmod 3 \\ 4 & \text{if } j = 1728 \quad \text{and } p \equiv 1 \pmod 4 \\ 2 & \text{else.} \end{cases}$$

Comparing those conditions with Corollary 2.29 we see that the cases with more than two isomorphism classes appear only for ordinary elliptic curves. Hence every j-invariant appears exactly twice for an $\mathbb{F}_p$-isomorphism class of supersingular elliptic curves. As a consequence, the nodes of $G_0(\mathbb{F}_p, \mathcal{L})$ cannot be stored as j-invariants but we have to consider some additional information to uniquely describe the isomorphism class.

Another observation is, that the edges of $G_0(\mathbb{F}_p, \mathcal{L})$ are $\mathbb{F}_p$-rational isogenies, so any isogeny from $G_0(\bar{\mathbb{F}}_p, \mathcal{L}) \cap \mathbb{F}_p$ which is defined over an extension of $\mathbb{F}_p$ will not appear in any form here. In the example above this applies to the double loop of 3-isogenies from 50 to itself. Corresponding edges to the other isogenies can be found in $G_0(\mathbb{F}_{53}, \{2, 3\})$ when we regard the following figure closely.

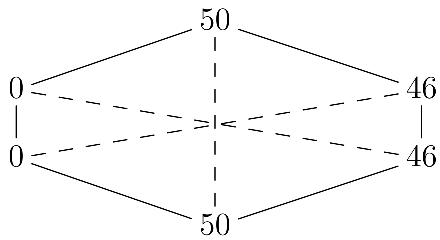


Figure 10: The $\mathbb{F}_p$-rational Isogeny Graph $G_0(\mathbb{F}_{53}, \{2, 3\})$

Again, 2-isogenies are drawn dashed and 3-isogenies with solid lines. We can see that single loops from FIGURE 9 evolve to isogenies from an elliptic curve to its quadratic twist in FIGURE 10 whereas double loops vanish. Single connections from a node j_0 to a node j_1 become isogenies between elliptic curves with just these j-invariants, although we have to explicitly compute which isomorphism class these curves lie in. There are several examples in APPENDIX C which show a similar behavior, so we conjecture a regularity in this behavior.

OBSERVATION 4.15. *We see that the edges in the graphs behave like follows when we have $j_0, j_1 \in \mathbb{F}_p$.*

1. ***Single connections.*** *Let j_0 and j_1 be different nodes in $G_0(\bar{\mathbb{F}}_p, \ell)$ such that there is a single edge from j_0 to j_1, so we have two nodes with j-invariant j_0 and j_1 each in the graph $G_0(\mathbb{F}_p, \ell)$. Then both of the nodes labeled with j_0 have a single edge to one of the nodes with j_1 and not to the same one. This means that the single isogeny in the full graph is a $\mathbb{F}_p$-rational isogeny.*

2. ***Single loops.*** *Let j_0 be a node in $G_0(\bar{\mathbb{F}}_p, \ell)$ such that there is a single loop from j_0 to itself. Then there is a single connection between the two different nodes labeled with j_0 in $G_0(\mathbb{F}_p, \ell)$. This means that the image curve of this isogeny is a twist of the original curve and the isogeny is defined over $\mathbb{F}_p$.*

3. ***Double connections.*** *Let j_0 and j_1 be nodes in $G_0(\bar{\mathbb{F}}_p, \ell)$ (possibly $j_0 = j_1$) such that there are two edges between them. Then those connections vanish in the $\mathbb{F}_p$-rational isogeny graph since they are defined over $\bar{\mathbb{F}}_p$ and duals of each other.*

STRUCTURE OF THE RATIONAL SUPERSINGULAR ISOGENY GRAPH. We can also construct the rational supersingular isogeny graph without going via the full isogeny graph. We have seen in SECTION 2.2.3 that the restricted endomorphism rings of $\mathbb{F}_p$-rational supersingular elliptic curves are of the same form as the full endomorphism rings in the ordinary case and that any such elliptic curve E fulfills

$$\mathbb{Z}[\sqrt{-p}] \;\subseteq\; \operatorname{End}_{\mathbb{F}_p} E \;\subseteq\; \mathcal{O}_{\mathcal{K}}.$$

Further we have observed that for $p \equiv 1 \pmod 4$ the only possible restricted endomorphism ring in this situation is $\operatorname{End}_{\mathbb{F}_p} E = \mathbb{Z}[\sqrt{-p}] = \mathcal{O}_{\mathcal{K}}$ and for $p \equiv 3 \pmod 4$ there are the alternatives $\operatorname{End}_{\mathbb{F}_p} E = \mathbb{Z}[\frac{1+\sqrt{-p}}{2}] = \mathcal{O}_{\mathcal{K}}$ as well as $\operatorname{End}_{\mathbb{F}_p} E = \mathbb{Z}[\sqrt{-p}] = \mathcal{O}_2$.

Analogous to the ordinary case we call a $\mathbb{F}_p$-rational supersingular elliptic curve E *on the surface* if its endomorphism ring is the maximal order and *on the floor* if it is $\mathbb{Z}[\sqrt{-p}]$. Note that for $p \equiv 1 \pmod 4$ floor and surface always coincide. Furthermore, in this situation the terms are used global and not with respect to different isogeny degrees ℓ since we only have two levels at most.

Since the proof of PROPOSITION 2.44 only uses the structure of the endomorphism ring, its result can also be applied to supersingular elliptic curves over $\mathbb{F}_p$ and their restricted endomorphism rings. Therefore we can observe that in the case where we have two levels, the degree of an isogeny connecting those levels has to divide $[\mathcal{O}_\mathcal{K} : \mathbb{Z}[\sqrt{-p}]] = 2$ and hence such *non-horizontal* isogenies can only occur for prime degree $\ell = 2$.

We want to establish a volcano-like structure of the graph $G_0(\mathbb{F}_p, \ell)$ with *ascending*, *descending* and *horizontal* isogenies like in the ordinary case. With our modified DEURING THEOREMS we have seen that the link between supersingular elliptic curves over $\mathbb{F}_p$ and elliptic curves over a number field is a similar one as for ordinary elliptic curves. Therefore we can transfer the well-known structure of the characteristic 0 picture as in SECTION 3 also to $G_0(\mathbb{F}_p, \ell)$.

Firstly, we can deduce the number of nodes in each level since due to this connection it equals the class number of $\mathcal{O}$ where $\mathcal{O} \in \{\mathcal{O}_\mathcal{K}, \mathcal{O}_2\}$ denotes the endomorphism ring on the respective level. Thus, for $p \equiv 1 \pmod 4$ we get $h(-4p)$ nodes in the graph which – as mentioned above – all represent supersingular elliptic curves over $\mathbb{F}_p$ with restricted endomorphism ring $\mathbb{Z}[\sqrt{-p}]$. For $p \equiv 3 \pmod 4$ and $p > 3$ there are two levels where the surface has $h(-p)$ nodes and the floor $h(-4p)$. Due to the formula

$$\frac{h(D)}{w(D)} = \frac{h(D_0)}{w(D_0)} \cdot c \cdot \prod_{\text{prime } r|c} \left(1 - \left(\tfrac{D_0}{r}\right) r^{-1}\right)$$

from page 233 of COHEN [12] in SECTION 5.3 with $D = c^2 D_0$ and $w(x) = 2$ for $x < -4$ we get for $p > 3$

$$\begin{aligned} \frac{h(-4p)}{2} &= \frac{h(-p)}{2} \cdot 2 \cdot \prod_{\text{prime } r|2} \left(1 - \left(\tfrac{-4p}{r}\right) r^{-1}\right) \\ &= \frac{h(-p)}{2} \left(2 - \left(\tfrac{-p}{2}\right)\right). \end{aligned}$$

Since the standard rule for computing KRONECKER symbols tells us that we have

$$\left(\frac{-p}{2}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1 & \text{if } p \equiv \pm 3 \pmod 8 \end{cases},$$

this yields for our situation

$$h(-4p) \;=\; \begin{cases} h(-p) & \text{if } p \equiv 7 \pmod 8 \\ 3h(-p) & \text{if } p \equiv 3 \pmod 8 \end{cases}$$

Hence we can make a refined statement and see, that for $p \equiv 7 \pmod 8$ floor and surface have the same number of nodes and for $p \equiv 3 \pmod 8$ there are trice as many nodes on the floor as on the surface. Summed up we obtain the following structure of the rational supersingular isogeny graph.

Theorem 4.16 (Node Structure of $G_0(\mathbb{F}_p, \ell)$).

- *For $p \equiv 1 \pmod 4$ there is only one level in $G_0(\mathbb{F}_p, \ell)$ with exactly $h(-4p)$ nodes.*
- *For $p \equiv 3 \pmod 8$ there are two levels in $G_0(\mathbb{F}_p, \ell)$, the upper one with $h(-p)$ and the lower one with $3h(-p)$ nodes.*
- *For $p \equiv 7 \pmod 8$ there are two levels with $h(-p)$ nodes each in $G_0(\mathbb{F}_p, \ell)$.*

Afterwards, we can determine how many isogenies of prime degree ℓ start at each of these nodes depending on their position in the graph. Again we use the connection to elliptic curves in characteristic 0 and the there obtained results to identify the number of outgoing isogenies in that situation. With help of Theorem 3.18 this structure can be preserved under reduction to supersingular elliptic curves over $\mathbb{F}_p$ and thus we get the following result.

Theorem 4.17 (Edge Structure of $G_0(\mathbb{F}_p, \ell)$).

- *For every node in $G_0(\mathbb{F}_p, \ell)$ with $\ell > 2$ and Kronecker-symbol $\left(\frac{-p}{\ell}\right) = 1$ there are exactly two horizontal ℓ-isogenies.*
- *The structure of $G_0(\mathbb{F}_p, 2)$ depends on the form of p.*
  - *For $p \equiv 1 \pmod 4$ there is exactly one outgoing horizontal 2-isogeny starting at each vertex.*
  - *For $p \equiv 3 \pmod 8$ there are three descending 2-isogenies for every vertex on the surface and one ascending 2-isogeny from every one on the floor.*
  - *For $p \equiv 7 \pmod 8$ there are two horizontal and one descending 2-isogeny for every vertex on the surface and one ascending 2-isogeny from every one on the floor.*

Note that for every isogeny in this picture there has to be a dual isogeny in the other direction, so for instance in the case $p \equiv 1 \pmod 4$ the nodes of the graph are grouped in pairs or single nodes and $G_0(\mathbb{F}_p, 2)$ cannot be connected when there are more than two nodes in it. This can be seen at the dashed lines representing 2-isogenies in the graph of FIGURE 10.

Similarly, for $p \equiv 3 \pmod 8$ we always have components of four vertices where one on the surface is connected with three ones on the floor via 2-isogenies. Only for $p \equiv 7 \pmod 8$ where we also have horizontal 2-isogenies, bigger components in $G_0(\mathbb{F}_p, 2)$ are possible. There are a number of examples in APPENDIX C where these structures can be seen nicely.

A nice result from BRILLHART-MORTON [4, PROPOSITION 8] helps us drawing the volcano in the two-level case since we can determine almost all elliptic curves which lie on the surface.

PROPOSITION 4.18. *Let $p > 3$ be a prime and E be a supersingular elliptic curve over $\mathbb{F}_p$ with $j(E) \neq 0, 1728$. Then we get*

$$\operatorname{End}_{\mathbb{F}_p} E = \mathbb{Z}\left[\tfrac{1+\sqrt{-p}}{2}\right] \quad \Longleftrightarrow \quad \left(\tfrac{j(E)-1728}{p}\right) = 1$$

where $\left(\frac{a}{p}\right)$ denotes the JACOBI-*Symbol.*

Thus we know for all nodes except for the ones labeled with 0 or 1728 on which level in the graph they are. From the examples we get an impression about a probable behavior of those nodes.

OBSERVATION 4.19. *In a graph $G_0(\mathbb{F}_p, \mathcal{L})$ both nodes labeled with 0 are always on the same level – in our examples always on the floor – and the situation where one node is on the floor and the other on the surface can happen only for nodes with label $1728 \pmod p$.*

The structures which can be conjectured from both OBSERVATION 4.15 and 4.19 are unproven yet, but they are also never used in any theoretical proof in this work.

4.2.3 Resulting Algorithm and Complexity Analysis

The bottleneck in the ordinary case algorithm was reaching the same level in the volcano when the conductor was not smooth. This problem cannot occur in the situation of $\mathbb{F}_p$-rational supersingular volcanoes since here the conductor is $c = 2$ and there are only less or equal to two levels in the graph at all. Considering this structure there are several strategies how to proceed with computing isogenies between supersingular elliptic curves E_0 and E_1 over $\mathbb{F}_p$.

- We can operate on single levels analogous as in the ordinary case. For that we have to determine the levels of E_0 and E_1 and calculate isogenies to elliptic curves E_0' and E_1' on the same level where necessary. For $p \equiv 1 \pmod 4$ this step can be omitted completely. For $p \equiv 7 \pmod 8$ both levels have the same cardinality and structure, so it does not matter on which level we work. In the case where $p \equiv 3 \pmod 8$ the upper level is smaller and as the length of the random walk depends on the graph size it probably is better to run the algorithm with starting curves E_0' and E_1' there.

- As for $p \equiv 3 \pmod 8$ and on the lower level of the graph for $p \equiv 7 \pmod 8$ no horizontal 2-isogenies exist but those are the fastest ones to compute, there is the possibility to allow vertical isogenies and not to restrict the nodes of the path to a single level. Then the steps of the path are averagely faster computable but on the other hand we expect longer paths since bigger graphs are used. This consideration does not apply for $p \equiv 1 \pmod 4$ where all isogenies are horizontal.

- Another approach is to completely ignore the level structure for an algorithm to compute isogenies between supersingular elliptic curves over $\mathbb{F}_p$ and just use the theoretically obtained result about the connectedness of the graph $G_0(\mathbb{F}_p, \mathcal{L})$. If this graph is fully connected with a suitable set $\mathcal{L}$, the smaller $\mathbb{F}_p$-rational subgraph of $G_0(\bar{\mathbb{F}}_p, \mathcal{L})$ will also be since the isogenies can be converted from one picture into the other.

Apart from the fact that there are less nodes in this graph, there is another computational advantage in that last approach, since in $G_0(\bar{\mathbb{F}}_p, \mathcal{L})$ a random neighbor of a node can be calculated through a root of a modular polynomial. When we use the rational isogeny graph $G_0(\mathbb{F}_p, \mathcal{L})$, we cannot use modular polynomial to compute neighbors since they only yield the j-invariant of the neighbor but we need more information to correctly identify it. Instead we have to take division polynomials ψ_ℓ as described at the beginning of Section 25.2 of Galbraith [28].

These polynomials depend on the starting curve E_0 thus they cannot be precomputed but have to be determined in each step. Their roots yield x-coordinates of the ℓ-torsion points of E_0 and such a point generates a subgroup of E_0 with order ℓ, thus it leads to an isogeny of degree ℓ. Since we are only interested in isogenies which are defined over $\mathbb{F}_p$, we need $\mathbb{F}_p$-rational subgroups of E_0. Such subgroups can only arise from roots of irreducible factors of degree less or equal to $(\ell - 1)/2$.

When we avoid these complications and only use the theoretical result about the connectedness of the graph $G_0(\mathbb{F}_p, \mathcal{L})$, we can adapt an algorithm which is similar to the one in the ordinary case we discussed in SECTION 4.1.2. In fact, the pseudocode is almost identical.

ALGORITHM 4.10 `RationalSupersingularPath(E_0, E_1, p, B)`

INPUT: supersingular elliptic curves E_0, E_1 defined over $\mathbb{F}_p$, bound B for isogeny degrees
OUTPUT: path in rational isogeny graph between E_0 and E_1

$X_0 \leftarrow [j(E_0)]$
$X_1 \leftarrow [j(E_1)]$
$B \leftarrow \min\{6 \cdot (\log |d_{\mathcal{K}}|)^2, B\}$
$\mathcal{L} \leftarrow \{2\} \cup \{$primes $\ell \leq B \mid \left(\frac{-p}{\ell}\right) = 1\}$
choose random $\ell \in \mathcal{L}$
$i \leftarrow 0$
while X_0 and X_1 are disjoint **do**
  $E_i \leftarrow$ random ℓ-neighbor of E_i
  append $j(E_i)$ to X_i
  if $j(E_i) \in X_{1-i}$ **then**
    truncate X_{1-i}
    disjoint $\leftarrow$ **false**
  end if;
  $i \leftarrow 1 - i$
  choose a new isogeny degree ℓ different from the last
end while
return X_0 joined with reversed X_1

In the complexity analysis we only have to bear in mind that the number of nodes in this graph is $\mathcal{O}(\sqrt{p})$ instead of $\mathcal{O}(h)$ as in the ordinary isogeny graph. Thus the resulting complexity is as following.

PROPOSITION 4.20. *Let E_0 and E_1 be supersingular elliptic curves defined over the finite field $\mathbb{F}_p$ where p is a prime and define $\mathcal{K} := \mathbb{Q}(\sqrt{-p})$. Further let $B \leq 6(\log |d_{\mathcal{K}}|)^2$ be a bound such that the ideal class $\mathcal{C}\ell(\mathcal{O}_{\mathcal{K}})$ is generated by ideals of norm less or equal to B.*

Computing an $\mathbb{F}_p$-isogeny $\phi : E_0 \to E_1$ can be done in expected running time of $\mathcal{O}(p^{1/4}(\log p)^5 \log\log p)$ and $\mathcal{O}(p^{1/4})$ storage.

So we have an algorithm with expected complexity $\widetilde{\mathcal{O}}(p^{1/4})$ which is a huge improvement to the previous $\widetilde{\mathcal{O}}(p^{1/2})$ algorithm for computing isogenies between supersingular elliptic curves. We implemented both algorithms and tested them on supersingular elliptic curves of various bit length. The computational results show an enormous speedup with the new algorithm and can be seen in TABLE 3 in APPENDIX B.

4.2.4 Application on Arbitrary Supersingular Curves

By now we have improved the algorithm to compute an isogeny between supersingular elliptic curves for the subset of those curves which are defined over $\mathbb{F}_p$. A natural question is whether this method can be used to find a better algorithm than the standard bi-directional search in $G_0(\bar{\mathbb{F}}_p, 2)$ for finding an isogeny between two *arbitrary* supersingular elliptic curves E_0 and E_1.

The first naive approach is to start with the usual random walks in the full supersingular isogeny graph at E_0 resp. E_1 using only 2-isogenies until we reach nodes which represent $\mathbb{F}_p$-rational supersingular elliptic curves. After that we connect those elliptic curves which can be represented as nodes in a $\mathbb{F}_p$-rational supersingular isogeny graph with the new algorithm. A pseudocode for this algorithm can have the following form.

Algorithm 4.11 `ArbitrarySupersingularPath(`E_0`, `E_1`, p, B)`

Input: `supersingular elliptic curves` E_0, E_1 `defined over` $\mathbb{F}_{p^2}$, `bound` B `for isogeny degrees`
Output: `path in full isogeny graph between` E_0 `and` E_1, `using a random walk of 2-isogenies and the` $\mathbb{F}_p$`-rational algorithm`

$X_0 \leftarrow [j(E_0)]$
$X_1 \leftarrow [j(E_1)]$
for $i = 0, 1$ **do**
  while $j(E_i) \notin \mathbb{F}_p$ **do**
    $E_i \leftarrow$ `random 2-neighbor of` E_i `different to the last`
    `Append` $j(E_i)$ `to` X_i
  end while
end for
$B \leftarrow \min\{6 \cdot (\log |d|)^2, B\}$
$\mathcal{L} \leftarrow \{2\} \cup \{$`primes` $\ell \leq B \mid \left(\frac{-p}{\ell}\right) = 1\}$
`choose random` $\ell \in \mathcal{L}$
$i \leftarrow 0$
while X_0 `and` X_1 `are disjoint` **do**
  $E_i \leftarrow$ `random` ℓ`-neighbor of` E_i
  `append` E_i `to` X_i
  if $E_i \in X_{1-i}$ **then**
    `truncate` X_{1-i}
    `disjoint` $\leftarrow$ **false**
  end if;
  $i \leftarrow 1 - i$
  `choose a new isogeny degree` ℓ `different from the last`
end while
return X_0 `joined with reversed` X_1

The first part uses the normal algorithm in the full isogeny graph $G_0(\bar{\mathbb{F}}_p, 2)$ where usually a path is found in expected $\widetilde{\mathcal{O}}(p^{1/2})$. Thus the complexity of this algorithm is dominated by finding a random walk to an elliptic curve with j-invariant from $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$ whereas the part of connecting the two $\mathbb{F}_p$-rational nodes with each other using our new algorithm is done in expected $\widetilde{\mathcal{O}}(p^{1/4})$ and thus neglectable in the overall complexity.

In this situation though we have to bear in mind that we do not fix both starting and ending point of the path but are satisfied when the path ends at any of the $\mathbb{F}_p$-rational nodes. If we can get an assertion about the distance of an arbitrary elliptic curve to the set of $\mathbb{F}_p$-rational elliptic curves it could improve the complexity analysis notably, but so far we know of no starting point for an approximation in such a way. Thus the following problem is still unsolved.

Problem 12 (Supersingular Isogeny Shortcut). *Let E_0 be a supersingular elliptic curve defined over $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$. Find an algorithm that computes a path from E_0 to an arbitrary supersingular elliptic curve E_1 defined over $\mathbb{F}_p$ which has an expected running time better than $\widetilde{\mathcal{O}}(p^{1/2})$.*

We implemented Algorithm 4.11 in `MAGMA`, too, and the results seem to support the theory of at least a small speedup of finding an isogeny path between two random supersingular elliptic curves with this method. They can be found in Table 4.

4.3 Isogenies between Abelian Varieties

In higher dimension it seems to be incomparably more difficult to compute an isogeny between arbitrary isogenous abelian varieties A_0 and A_1. Even when we restrict to Jacobians of hyperelliptic curves of genus $g = 2$, there are several problems. We will give a brief overview about some approaches for certain specific situations here.

First we will investigate attempts to generalize the formulae of Vélu, so we describe methods to obtain an isogeny having a specific subgroup of the Jacobian as kernel and discuss them and their image curves. Afterwards we deal with isogenous Jacobians with the same endomorphism ring and how to find isogenies between them if possible. Such isogenies are called *horizontal* as in the case of elliptic curves.

The analogy of *vertical isogenies* is not as easy since there does not have to be an inclusion relation between the endomorphism rings of isogenous Jacobians as in the elliptic case. However, some special cases can be examined. Finally we concentrate on the supersingular case where not much is known so far and state the relevant questions, problems and difficulties when dealing with that situation.

4.3.1 Computing Isogenies with Given Kernel

Recall Example 2.16 where we described how to compute all 2-isogenies starting at a given elliptic curve E defined over a field K. For that we needed a subgroup of order two of $E(\bar{K})$ to become the kernel of the isogeny. Such a group is generated by a point of order two which can be deduced from the zeros of the Weierstrass polynomial of the elliptic curve.

We introduce a generalization of this approach to $g = 2$ with similar tools. Smith [80] describes a way to determine $(2, 2)$-isogenies on the Jacobian of a hyperelliptic curve of genus two defined over a field K with $\operatorname{char} K \neq 2$. The presented Richelot formulae can be seen as an extension of the formulae of Vélu for 2-isogenies on elliptic curves. In order to accomplish that, let C be a hyperelliptic curve of genus two defined over a field K with $\operatorname{char} K \neq 2$ and denote its Jacobian with A. Remember that the points on A are represented by classes $[D]$ of divisors D with degree zero. The curve C is given by a Weierstrass polynomial

$$Y^2 \quad - \quad f(X)$$

where f is a polynomial of degree $d = 5$ or $d = 6$ with no multiple zeros. We call such polynomials f *hyperelliptic polynomials* and introduce the set of hyperelliptic polynomials

$$\mathcal{H} \; := \; \{f \in K[X] \mid \; f \text{ squarefree with } \deg f \in \{5,6\}\}.$$

We denote the roots of f in $\bar{K}$ with $\alpha_1, \cdots \alpha_d$ and the points $P_i := (\alpha_i, 0) \in C(\bar{K})$ for $i \in \{1, \cdots, d\}$ are called WEIERSTRASS *points of* C. In the case $d = 5$, the point at infinity $\mathcal{O}_C$ is also a WEIERSTRASS point and can be labeled P_6, so we always have six of those points.

LEMMA 8.1.1 of SMITH [80] implies that the kernels of $(2,2)$-isogenies correspond to proper non-trivial subgroups of $A[2]$ which are isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$ and which he calls $(2,2)$-*subgroups*. Thus we will need some 2-torsion points of A for the $(2,2)$-isogenies we want to construct and for that we examine how $A[2]$ behaves. SMITH [80] shows in LEMMA 8.1.3 that they are strongly related to the WEIERSTRASS points of C.

LEMMA 4.21. *Let C be a hyperelliptic curve of genus two, A be its* JACOBIAN *and $P \in A[2]$ be a non-zero point of order two. Then there are two uniquely determined* WEIERSTRASS *points P_i and P_j of C with $P =: P_{ij} = [P_i - P_j]$.*

Therefore all points P in $(2,2)$-subgroups can be represented by two WEIERSTRASS points P_i and P_j and thus comply with factors of degree two of the polynomial f having α_i and α_j as roots. We write g_P for a polynomial leading to the point P. For a whole $(2,2)$-subgroup we need three such polynomials which have to be coprime.

There are several ways to split f in quadratic factors (resp. in the case $d = 5$ in two quadratic and one linear factor). When we take the product of three such factors, we get a polynomial of degree 5 or 6. So we can interpret the possibilities of splitting $f \in \mathcal{H}$ as the set of preimages of the map

$$\begin{aligned} F : (K[X]_2)^3 \;&\rightarrow\; K[X] \\ (g_0, g_1, g_2) \;&\mapsto\; g_0 g_1 g_2 \end{aligned}$$

where we define

$$K[X]_2 := \{g \in K[X] \mid \deg g \leq 2\}$$

as usual. An element $(g_0, g_1, g_2) \in (K[X]_2)^3$ which is a preimage of some $f \in \mathcal{H}$ is called *quadratic splitting of* f. For a polynomial $f \in \mathcal{H}$ some of these splittings $F^{-1}(f)$ arise only by permuting the polynomials g_i or by allowing constant factors $c_i \in K^*$ in front of the respective g_i with $c_0 c_1 c_2 = 1$.

When we factor out relations given by the equivalence $\sim$ with

$$(c_0 g_1, c_1 g_1, c_2 g_2) \;\sim\; (g_0, g_1, g_2) \;\sim\; (g_1, g_2, g_0) \;\sim\; (g_2, g_0, g_1)$$

for g_i and c_i as before, we can define the *set of quadratic splittings*

$$\mathcal{S} \;:=\; F^{-1}(\mathcal{H})/\sim$$

which leads to a well-defined map

$$F : \mathcal{S} \;\to\; \mathcal{H}.$$

Further when we write the polynomials in the splitting as $g_i := a_{i0} + a_{i1}X + a_{i2}X^2$ and define the matrix $G := (a_{ij})$ containing their coefficients, we can get a map

$$\begin{aligned} \det : \mathcal{S} \;&\to\; K \\ [(g_0, g_1, g_2)] \;&\mapsto\; \det G \end{aligned}$$

which can also be checked to be well-defined.

We notice that the two splittings (g_0, g_1, g_2) and (g_0, g_2, g_1) are not considered equivalent under $\sim$. Since we can compute $\det[(g_0, g_2, g_1)] = -\det[(g_0, g_1, g_2)]$, the map det would not be well-defined with this permutation included in the equivalence relation. But we can consider those two elements as negative of each other and introduce a *negation*

$$\begin{aligned} \nu : \mathcal{S} \;&\to\; \mathcal{S} \\ [(g_0, g_1, g_2)] \;&\mapsto\; [(g_0, g_2, g_1)] \end{aligned}$$

and regard $\mathcal{S}/\langle\nu\rangle =: |S|$. The image of a splitting $\mathfrak{g}$ in $|S|$ is called *unsigned quadratic splitting* and denoted with $|\mathfrak{g}|$. This concept is closely related to $(2,2)$-subgroups of $\operatorname{Jac} C$ as seen in Proposition 8.2.3 of Smith [78].

Proposition 4.22. *Let C be a hyperelliptic curve of genus two represented by the polynomial $Y^2 - f(X)$ with $f \in \mathcal{H}$ and A be its* Jacobian. *There is a bijection*

$$\{\textit{kernels of } (2,2)\textit{-isogenies from } A\} \;\longleftrightarrow\; \{\textit{unsigned quadratic splittings of } f\}.$$

The above introduced determinant of a splitting helps to classify the splittings and eventually the images of the corresponding isogenies with kernels as in the last proposition.

Definition. Let $\mathfrak{g} := [(g_0, g_1, g_2)] \in \mathcal{S}$ be a quadratic splitting. Then $\mathfrak{g}$ is called *singular* if we have $\det G = 0$. The set of singular splittings we denote with $\mathcal{S}^0$ and the set of nonsingular splittings with $\mathcal{S}^+$.

Smith [78] explains how singular splittings produce $(2,2)$-isogenies to products of elliptic curves and nonsingular splittings $(2,2)$-isogenies to Jacobians of hyperelliptic curves of genus two. We will regard the latter case here.

Definition. For $\mathfrak{g} := [(g_0, g_1, g_2)] \in \mathcal{S}^+$ we define $\delta := \det G^{-1}$ and for any pair of i and j possible $[g_i, g_j] := g_i' g_j - g_j' g_i$ where $'$ is the first derivation. Then the Richelot *operator* is a map

$$\begin{aligned} \mathcal{R} : \mathcal{S}^+ &\to (K[X]_2)^3 \\ \mathfrak{g} &\mapsto (\delta[g_1, g_2], \delta[g_2, g_0], \delta[g_0, g_1]). \end{aligned}$$

The important fact about this map is that images from elements in $\mathcal{S}^+$ give rise to hyperelliptic polynomials again, that is, for all $\mathfrak{g} \in \mathcal{S}^+$ we have $F(\mathcal{R}(\mathfrak{g})) \in \mathcal{H}$. This can be seen in Lemma 8.4.2 of Smith [78]. He further shows a few easy-to-check rules of calculations which are satisfied by $\mathcal{R}$ and induce a well-defined involution $\mathcal{R} : \mathcal{S}^+ \to \mathcal{S}^+$. Thus every image of this map defines a hyperelliptic curve of genus two and we can make the following definition.

Definition. Let C be a hyperelliptic curve of genus two represented by the polynomial $Y^2 - f(X)$ with $f \in \mathcal{H}$ and let $\mathfrak{g} := [(g_0, g_1, g_2)] \in \mathcal{S}^+$ be a nonsingular quadratic splitting of f. Then we set $C_{\mathfrak{g}}$ as the hyperelliptic curve of genus two defined through $Y^2 - F(\mathcal{R}(\mathfrak{g}))$.

It can immediately be seen that $\mathcal{R}(\mathfrak{g}) := [(h_0, h_1, h_2)]$ is a nonsingular quadratic splitting of $F(\mathcal{R}(\mathfrak{g}))$ and we have $(C_{\mathfrak{g}})_{\mathcal{R}(\mathfrak{g})} = C$. Smith [78] develops a correspondence on $C \times C_{\mathfrak{g}}$ which can be used to prove the next statement from his Theorem 8.4.11 about the existence of an isogeny between the Jacobians of C and $C_{\mathfrak{g}}$ which is called Richelot *isogeny of* $\mathfrak{g}$.

Proposition 4.23. *Let C be a hyperelliptic curve of genus two represented by the polynomial $Y^2 - f(X)$ with $f \in \mathcal{H}$, A be its* Jacobian *and let $\mathfrak{g} \in \mathcal{S}^+$ be a nonsingular splitting of f. Let $C_{\mathfrak{g}}$ be the hyperelliptic curve constructed via the* Richelot *operator above and $A_{\mathfrak{g}}$ its* Jacobian.

Then there exists a well-defined $(2,2)$-isogeny $\phi_{\mathfrak{g}} : A \to A_{\mathfrak{g}}$ whose kernel is given by $|\mathfrak{g}|$ and the image of $A[2]$ is a $(2,2)$-subgroup of $A_{\mathfrak{g}}$ given by $|\mathcal{R}(\mathfrak{g})|$ both in accordance to Proposition *4.22.*

The isogenies $\phi_{\mathfrak{g}} : A \to A_{\mathfrak{g}}$ and $\phi_{\mathcal{R}(\mathfrak{g})} : A_{\mathfrak{g}} \to A$ behave as duals of each other as seen in COROLLARY 8.4.14 of SMITH [78].

PROPOSITION 4.24. *Let C and $\mathfrak{g}$ be as in the situation above. Then we have $\phi_{\mathcal{R}(\mathfrak{g})} \circ \phi_{\mathfrak{g}} = [2]_A$ and $\phi_{\mathfrak{g}} \circ \phi_{\mathcal{R}(\mathfrak{g})} = [2]_{A_g}$.*

An explicit computation of this RICHELOT isogeny is presented in SECTION 3.2 of TAKASHIMA, YOSHIDA [85].

PROPOSITION 4.25. *Let C be a hyperelliptic curve of genus two represented by the polynomial $Y^2 - f(X) \in K[X,Y]$ with $f \in \mathcal{H}$, $\mathfrak{g} := [(g_0, g_1, g_2)] \in \mathcal{S}^+$ be a nonsingular quadratic splitting of f and $\mathcal{R}(\mathfrak{g}) =: \mathfrak{h} = [(h_0, h_1, h_2)] \in \mathcal{S}^+$ be its image under the* RICHELOT *operator.*

Define the monic polynomials $\widetilde{g}_i$ and $\widetilde{h}_i$ as the normalized polynomials of g_i resp. h_i such that we have $g_0 g_1 g_2 = a\widetilde{g}_0\widetilde{g}_1\widetilde{g}_2$ and $h_0 h_1 h_2 = b\widetilde{h}_0\widetilde{h}_1\widetilde{h}_2$ with $a, b \in K^*$. Then we get

$$\begin{array}{rcl} \phi_{\mathfrak{g}} : A & \to & A_{\mathfrak{g}} \\ [(x,y) - P_0] & \mapsto & [(z_1, t_1) - (z_2, t_2)] \end{array}$$

where z_1, z_2 are the zeros of $\widetilde{g}_1(x)\widetilde{h}_1(Z) + \widetilde{g}_2(x)\widetilde{h}_2(Z)$ with respect to Z and t_1, t_2 satisfy $yt_i = a\widetilde{g}_1(x)\widetilde{h}_1(z_i)(x - z_i)$.

An analogous method for $(2,2,2)$-isogenies on the JACOBIAN of a hyperelliptic curve C of genus three can be found in SMITH [79]. It also uses WEIERSTRASS points and the fact that the subgroups of $A[2]$ which are isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3$ can be represented by four disjoint pairs of them. He uses trigonal construction to compute a curve $\widetilde{C}$ and an isogeny $\phi : A \to \widetilde{A}$ with given kernel although the image curve is usually not hyperelliptic.

A general computation of isogenies between higher genus curves – like the formulae of VÉLU in the elliptic case – is more complicated and needs profound and extensive theory of *theta functions* and *theta null points* which goes beyond the scope of this work. LUBICZ and ROBERT [52] present an algorithm for computing $(\ell, \cdots, \ell)$-isogenies of given kernel on abelian varieties defined over fields with odd characteristic. They use theta functions of different levels n and ℓn on the input and the image curve. COSSET and ROBERT [14] combine this method with an algorithm to convert between those theta coordinates and thus manage to get an algorithm for computing isogenies when the used theta coordinates are of the same level.

In the case of JACOBIANS of hyperelliptic genus two curves this approach yields separable ℓ-isogenies which have kernel isomorphic to $\mathbb{Z}/\ell\mathbb{Z}^2$ and therefore degree ℓ^2.

This is one way to interpret a generalization of the ℓ-isogenies from the elliptic case; another one is considering isogenies of degree ℓ instead. This is work in progress from Dudeanu, Jetchev and Robert and to appear soon, some notes can be found in Section 4 of Robert [69] or Section 2.3 of Robert [70].

4.3.2 Horizontal and Vertical Isogenies

Let C be a hyperelliptic curve of genus two defined over the finite field $K := \mathbb{F}_q$ of prime characteristic p and let $A := \operatorname{Jac} C$ its Jacobian which is a principally polarized abelian variety of dimension two.

We know from Section 2.2 that $\operatorname{End}_K A$ is isomorphic to an order in the usual algebra $\mathcal{A} := \operatorname{End}_K A \otimes_{\mathbb{Z}} \mathbb{Q}$ with

$$\mathbb{Z}[\pi_q, \rho_q] \;\subseteq\; \operatorname{End}_K A.$$

Furthermore, we get from Theorem 2.37 that the algebra $\mathcal{A}$ has center $\mathbb{Q}(\pi_q)$ and that we have

$$4 \;\leq\; [\mathcal{A} : \mathbb{Q}] \;\leq\; 16.$$

If A is simple, the theorem also tells us that A is ordinary and that we have $[\mathcal{A} : \mathbb{Q}] = 4$. We briefly examine the case where A is not a simple variety. Arbitrary abelian varieties can be written in the following way as seen in Proposition 10.1 and the following discussion on pages 42 and 43 of Milne [59].

Proposition 4.26. *Let A be an abelian variety of dimension g. Then there exist simple non-isogenous varieties $A_1, \cdots, A_s \subseteq A$ of dimension g_i and integers n_i with $\prod_{i=1}^{s} g_i^{n_i} = g$ such that*

$$A \text{ is isogenous to } A_1^{n_1} \times \cdots \times A_s^{n_s}.$$

Let further $\mathcal{A} := \operatorname{End} A \otimes_{\mathbb{Z}} \mathbb{Q}$ resp. $\mathcal{A}_i := \operatorname{End} A_i \otimes_{\mathbb{Z}} \mathbb{Q}$ be the algebras containing the respective endomorphism rings. Then we have

$$\mathcal{A} \;\cong\; \prod \mathbb{M}_{n_i}(\mathcal{A}_i).$$

Corollary 4.27. *Let A be an abelian variety of dimension $g = 2$. Then A is either simple or isogenous to the product of two not necessarily different elliptic curves E_1 and E_2.*

Several concepts are transmitted from the elliptic curves to the original abelian variety as we can check straightforwardly.

Lemma 4.28. *With the notation from above and A defined over the finite field $\mathbb{F}_q$ of characteristic p let E_1 and E_2 have p-rank r_1 resp. r_2. Then the p-rank of A is $r(A) = r_1 + r_2$.*

Further let $\mathcal{A}$, $\mathcal{A}_1$ and $\mathcal{A}_2$ be as above. Then we have

$$[\mathcal{A} : \mathbb{Q}] \quad = \quad [\mathcal{A}_1 : \mathbb{Q}] \cdot [\mathcal{A}_2 : \mathbb{Q}].$$

With these considerations we get the following classification of abelian varieties of dimension two in characteristic p according to their p-rank.

Proposition 4.29. *Let A be an abelian variety of dimension $g = 2$ defined over the finite field $\mathbb{F}_q$ of characteristic p. Let E_1 and E_2 be elliptic curves such that A is isogenous to $E_1 \times E_2$. Then we have*

$$\begin{aligned} r(A) = 2 \quad &\Longleftrightarrow \quad E_1, E_2 \textit{ ordinary} \\ &\Longleftrightarrow \quad [\mathcal{A} : \mathbb{Q}] = 4, \\[2ex] r(A) = 1 \quad &\Longleftrightarrow \quad E_i \textit{ ordinary, } E_{1-i} \textit{ supersingular for } i = 0 \textit{ or } i = 1 \\ &\Longleftrightarrow \quad [\mathcal{A} : \mathbb{Q}] = 8, \\[2ex] r(A) = 0 \quad &\Longleftrightarrow \quad E_1 = E_2 \textit{ supersingular} \\ &\Longleftrightarrow \quad [\mathcal{A} : \mathbb{Q}] = 16. \end{aligned}$$

Recall that an ordinary abelian variety has p-rank g whereas a supersingular one has p-rank 0 and that for $g = 2$ these conditions are even equivalences. Then from the previous discussion and Theorem 2.37 again, we get the *ordinary* and the *supersingular case* as following.

$$\begin{aligned} A \text{ is ordinary} \quad &\Longleftrightarrow \quad \dim_{\mathbb{Q}} \mathcal{A} = 4 \\ &\Longleftrightarrow \quad \chi_{\pi_q} \text{ is squarefree} \\ &\Longleftrightarrow \quad \mathcal{A} = \mathbb{Q}(\pi_q) \\ &\Longleftrightarrow \quad \mathcal{A} \text{ is commutative,} \end{aligned}$$

and on the other hand

$$\begin{aligned} A \text{ is supersingular} \quad &\Longleftrightarrow \quad \dim_{\mathbb{Q}} \mathcal{A} = 16 \\ &\Longleftrightarrow \quad \exists a \in \mathbb{C}:\ \chi_{\pi_q} = (X-a)^4 \\ &\Longleftrightarrow \quad \mathbb{Q}(\pi_q) = \mathbb{Q} \\ &\Longleftrightarrow \quad \mathcal{A} \cong \mathbb{M}_2(D_p) \\ &\Longleftrightarrow \quad \exists \text{ supersingular elliptic curve } E \\ &\qquad\qquad \text{with } \operatorname{End}_K E = \operatorname{End} E \\ &\qquad\qquad \text{and an isogeny } \phi : A \to E \times E. \end{aligned}$$

Those are quite important properties which can be used when handling ordinary resp. supersingular JACOBIANS of genus two hyperelliptic curves.

Let now A_0 and A_1 be principally polarized abelian varieties of dimension two so we know that they are isogenous if and only if the characteristic polynomials of their respective FROBENIUS endomorphisms are equal.

WESOLOWSKI [93] deals with computing horizontal isogenies in the ordinary situation, so where $\mathcal{A}$ is a totally imaginary extension of a real quadratic extension $\mathcal{A}_0$ of $\mathbb{Q}$, also called a *CM field*. He considers the situation where the abelian varieties already have maximal endomorphism ring isomorphic to the maximal order $\mathcal{O}_{\mathcal{A}}$ of $\mathcal{A}$ and uses them as vertices in an isogeny graph. An important point is that he takes isogenies of degree ℓ instead of (ℓ, ℓ)-isogenies as edges. In that case he can show that the graph is connected when using a set of primes $\ell \leq B$ as possible degrees where – similar to the elliptic case – B is a bound resulting from a connection to an ideal class group.

To build this connection, the varieties have to be lifted to abelian varieties over the ring $W := W(\mathbb{F}_q)$ of WITT vectors of $\mathbb{F}_q$. We do not want to enlarge upon the technical details of the construction here, but in this special situation the ring W has characteristic zero and is an extension of the p-adic integers $\mathbb{Z}_p$ with

$$[W : \mathbb{Z}_p] \quad = \quad [\mathbb{F}_q : \mathbb{F}_p]$$

and a surjective homomorphism $W \to \mathbb{F}_q$. For an abelian variety A defined over $\mathbb{F}_q$ we can now introduce the *canonical lift* $\widetilde{A}$ which is an abelian variety defined over W with same dimension as A and – most importantly – with

$$\operatorname{End} \widetilde{A} \quad \cong \quad \operatorname{End} A,$$

see SECTION 4 of OORT [64] or SECTION 3 of KOHEL [46].

They also state a theorem of SERRE and TATE which provides that for every ordinary abelian variety over a finite field such a canonical lift exists. The original notes about this topic can be found in LUBIN-SERRE-TATE [53]. We write the statement for our situation like follows.

PROPOSITION 4.30. *Let A be an ordinary abelian variety of dimension g defined over a finite field $K := \mathbb{F}_q$ of characteristic $p > 0$. Then there exists an abelian variety $\widetilde{A}$ of dimension g defined over the ring of* WITT *vectors $W := W(\mathbb{F}_q)$ and we have $\operatorname{End}\widetilde{A} \cong \operatorname{End} A$.*

After that the lifted abelian varieties over the WITT vectors can be embedded into other abelian varieties defined over a number field. Those varieties still have the same endomorphism rings as the original abelian varieties defined over $\mathbb{F}_q$ and are principally polarized if and only if the original ones are. Each of them is again isomorphic to $\mathbb{C}^2/\Lambda$ where Λ is a lattice in $\mathbb{C}^2$. This lattice only depends on an ideal $\mathfrak{a}$ and thus we can map the situation to an ideal class group again. To be precise, this connection can be described as on page 15 of WESOLOWSKI [93] and seen below.

PROPOSITION 4.31. *Let $\mathcal{A}$ be a CM field as above and let*

$$\begin{aligned} \nu : \mathcal{C}\ell(\mathcal{A}) &\to \mathcal{C}\ell^+(\mathcal{A}_0) \\ [\mathfrak{a}] &\mapsto [\mathrm{N}_{\mathcal{A}/\mathcal{A}_0}(\mathfrak{a})] \end{aligned}$$

where $\mathcal{C}\ell^+(\mathcal{A}_0)$ is the narrow class group of $\mathcal{A}_0$. Then there is a one-to-one connection

$$\left\{ \begin{array}{c} \textit{isomorphism classes of} \\ \textit{principally polarized abelian} \\ \textit{varieties defined over } \mathbb{C} \end{array} \right\} \longleftrightarrow \ker \nu.$$

Further there is a free and transitive action of $\ker \nu$ on the set of isomorphism classes of principally polarized abelian varieties. As in the elliptic case the map between the varieties corresponding to the ideal classes $[\mathfrak{a}]$ and $[\mathfrak{b}]$ is given by the ideal class $[\mathfrak{a}^{-1}\mathfrak{b}]$. This means that those ideals of norm ℓ still correspond to separable isogenies with degree ℓ and thus BACH'S theorem gives us a bound B for the degrees sufficient such that the isogeny graph is connected. We emphasize that these isogenies are different from ℓ-isogenies in genus two which have degree ℓ^2.

Proposition 4.32. *In the same situation as above, we have a one-to-one connection*

$$\left\{\begin{matrix}\textit{isogenies between principally polarized}\\ \textit{abelian varieties defined over } \mathbb{C}\end{matrix}\right\} \longleftrightarrow \ker \nu.$$

The similarities of the resulting structure to the elliptic situation are distinctive although the technical steps are more difficult. Details of this construction can be found in Section 2.1.2 of Wesolowski [93]. This approach provides a possibility to apply bi-directional searches and find a path between given vertices via a collision analogously to the discussed methods for the same problem with elliptic curves.

It is crucial for the occurring correspondences between ideal classes and abelian varieties defined over a number field that these varieties have to be principally polarized. Thus for dimension two where the Jacobians of hyperelliptic genus-two-curves are exactly the principally polarized abelian varieties, this construction provides us with a method to compute isogenies between abelian varieties with same endomorphism ring. For higher dimension $g > 2$ though, not all principally polarized varieties are Jacobians of hyperelliptic curves of genus g. Thus the method does not generalize immediately to that cases.

In contrast to those horizontal isogenies, vertical isogenies between Jacobians of genus two hyperelliptic curves defined over $K := \mathbb{F}_q$ prove to be a more difficult matter and cannot be generalized from the elliptic curve case without limitations. Ionica and Thomé [41] examine the situation when the real multiplication is maximal. This means that the endomorphism ring of the occurring abelian varieties has to be isomorphic to an order in $\mathcal{A}$ which has to contain the maximal order $O_{\mathcal{A}_0}$ of the real quadratic subfield $\mathcal{A}_0$ of $\mathcal{A}$. Further it is assumed that $\mathcal{A}_0$ has class number one, such that it is a principal ring and $\mathcal{O}_{\mathcal{A}}$ is a module over $\mathcal{O}_{\mathcal{A}_0}$.

These restrictions are necessary since the isogeny graph for Jacobians of hyperelliptic genus two curves does not have the useful volcano structure as the ordinary elliptic curve isogeny graph. In the elliptic case we had the property that the index of the endomorphism ring in the maximal order already determined the endomorphism ring uniquely, so we had only one single level of a given distance from the surface. For the genus two situation this does not need to be true as there can be different orders in $\mathcal{A}$ with the same index since the $\mathbb{Z}$-rank of the orders is four.

Furthermore, Ionica and Thomé [41] say that the result from Kohel about the endomorphism rings of ℓ-isogenous ordinary elliptic curves being contained in each other does not entirely hold, see Section 8 of Bröker, Gruenewald and Lauter [68]. It generalizes only in the following way.

PROPOSITION 4.33. *Let A_0 and A_1 be ordinary* JACOBIANS *of genus two hyperelliptic curves and $\phi : A_0 \to A_1$ be an isogeny such that their endomorphism rings are isomorphic to the orders $\mathcal{O}_0$ resp. $\mathcal{O}_1$ in the CM field $\mathcal{A}$. Then we have*

$$\ell\mathcal{O}_i \subseteq \mathcal{O}_{1-i} \qquad \textit{for } i = 0 \textit{ or } i = 1.$$

The proof is similar as KOHEL'S proof for genus one but taking in account that the $\mathbb{Z}$-rank of the orders is four. Thus endomorphism rings of isogenous JACOBIANS do not have to be contained in each other and there cannot be a simple volcano like structure as in the ordinary elliptic case.

But PROPOSITION 4 and 5 from IONICA and THOMÉ [41] show that under the given constraints on $\mathcal{A}$ and $\mathcal{A}_0$ and a prime $\ell \neq \operatorname{char} K$ there are $\ell+1$ cyclic kernels of isogenies starting at a given JACOBIAN A and that the endomorphism rings of the respective images contain $\mathcal{O}_{\mathcal{A}_0}$, too. We say that such isogenies *preserve the real multiplication*. In their PROPOSITION 12 is shown how many of those isogenies are ascending, descending or horizontal when $\mathcal{A} \neq \mathbb{Q}(\xi_5)$. In fact, the result is quite similar to the ordinary elliptic volcano structure. Again there is a connection to an ideal class group and the isogenies are given by ideals $\mathfrak{a} \subseteq \mathcal{O}_{\mathcal{A}_0}$ of norm ℓ. Those are called $\mathfrak{a}$-isogenies.

Subsequently in the case where we have $\ell\mathcal{O}_{\mathcal{A}_0} = \mathfrak{a}_1\mathfrak{a}_2$ with coprime ideals $\mathfrak{a}_1$ and $\mathfrak{a}_2$, they describe $\{\mathfrak{a}_1, \mathfrak{a}_2\}$-isogeny graph. This graph has edges which are either $\mathfrak{a}_1$ or $\mathfrak{a}_2$-isogenies and it turns out to be the graph of all rational isogenies of degree ℓ as edges which preserve the real multiplication.

Further it has the interesting form of a direct product of two graphs of the structure like an ordinary isogeny volcano. Remember that we have a circle as surface of a volcano when the prime splits and a single point when it is inert as can be deduced from PROPOSITION 4.1. Therefore the $\{\mathfrak{a}_1, \mathfrak{a}_2\}$-isogeny graph's surface is a torus, a circle or a single point depending on whether both, one or none of the respective primes split.

These are nice structural results but rely on some assumptions and restrictions as we have seen. Especially the containment of the real multiplication in the occurring orders is a prominent feature in this work. Avoiding this and describing the structure of the isogeny graph for JACOBIANS of genus two hyperelliptic curves without fixed real multiplication is work in progress by DAMIEN, IONICA and MARTINDALE and – to the authors knowledge [54] – will be treated by MARTINDALE in her PhD thesis.

4.3.3 The Supersingular Case

When we look back to the case of supersingular elliptic curves, we see that there are several central points which distinguish it from the ordinary situation and makes it easier to deal with. For example we have in characteristic $p > 0$ that

I. a supersingular elliptic curve E can always be defined over $\mathbb{F}_{p^2}$,

II. two supersingular elliptic curves are always isogenous,

III. for any prime $\ell \neq p$ the isogeny graph $G_0(\bar{\mathbb{F}}_p, \ell)$ is always fully connected,

IV. the restricted endomorphism ring $\operatorname{End}_{\mathbb{F}_p} E$ of a supersingular elliptic curve E which is defined over $\mathbb{F}_p$ is isomorphic to an order in an imaginary quadratic field.

In this part we want to take a look at supersingular Jacobians of genus two hyperelliptic curves defined over the finite field $K := \mathbb{F}_q$ of characteristic p and examine the questions above for them. We know that for such a Jacobian A the algebra $\mathcal{A} = \operatorname{End}_K A \otimes_{\mathbb{Z}} \mathbb{Q}$ is isomorphic to the 2×2-matrices over the quaternion algebra ramified at p and infinity and as $\mathbb{Q}$-vector space has dimension 16. Further there is a supersingular elliptic curve E such that A is isogenous to $E \times E$.

I. Already the first property of elliptic curves in the list above proves to be difficult to investigate or generalize.

Problem 13. *Let A be a supersingular abelian variety of genus two defined over a field of characteristic $p > 0$. Is there an integer $r > 1$ such that A can be defined over $\mathbb{F}_{p^r}$?*

For a hyperelliptic genus-two-curve C and its Jacobian $A := \operatorname{Jac} C$ we have

$$A \text{ can be defined over } \mathbb{F}_q \iff C \text{ can be defined over } \mathbb{F}_q$$

(see the discussion in Section 14 of Milne [60]) and thus for a given entity we can use the coefficients of the Weierstrass equation of C to find out where A is defined. This does not provide a general statement though.

In the elliptic curve case the above stated result is shown by asserting that the j-invariant lies in $\mathbb{F}_{p^2}$, but since the moduli space of genus-two-curves has dimension three, we need at least three invariants to determine such a curve up to isomorphism. For that purpose usually the Igusa *invariants* i_1, i_2, i_3 (for example described by Goren and Lauter in [35], based on Igusa [40]) are used. It is possible to construct a hyperelliptic curve of genus two in characteristic p from given IGUSA invariants with MESTRE's algorithm ([58]), but a statement analogous to PROPOSITION 2.8 cannot be made.

To be explicit, in general we have for a hyperelliptic curve C of genus two

$$i_1, i_2, i_3 \in \mathbb{F}_q \quad \not\Rightarrow \quad C \text{ defined over } \mathbb{F}_q,$$

see REMARK 14.3 of OORT [65]. Further, even if there were such a connection, to the authors knowledge no restriction of the field of definition of such invariants is known for supersingular curves.

Most importantly, it can be shown that a generalization of the property of supersingular elliptic curves is not possible as presented by OORT in [66]. First there is a general result about abelian varieties attributed to GROTHENDIECK as in the next proposition.

PROPOSITION 4.34. *Let A be an abelian variety defined over a field K of characteristic $p > 0$. Then there exist a finite field extension $\mathbb{F}_q \supseteq \mathbb{F}_p$ and an abelian variety $\widetilde{A}$ defined over K such that A and $\widetilde{A}$ are K-isogenous and $\widetilde{A}$ can be defined over $\mathbb{F}_q$.*

This means that any abelian variety A in characteristic $p > 0$ is *isogenous* to an abelian variety which can be defined over a finite field extension of $\mathbb{F}_p$ but it is not necessarily true that A can be defined over a finite field itself. OORT [66] explains on page 10 that this can be done for p-rank at least $\dim A - 1$, but not always for lower p-rank.

PROPOSITION 4.35. *Let A be an abelian variety of dimension g with p-rank $r \geq g - 1$. Then A can be defined over a finite field.*

Note that this also implies that all elliptic curves in positive characteristic can be defined over finite fields and – most relevant for our discussion here – this does not cover *supersingular abelian varieties of dimension two.* In particular EXAMPLE 3.4 of OORT [66] explicitly constructs supersingular abelian varieties of dimension $g = 2$ which cannot be defined over a finite field but are defined over a field of positive characteristic.

PROPOSITION 4.36. *In characteristic $p > 0$ there exist supersingular abelian varieties A of dimension $g = 2$ which cannot be defined over a finite field.*

Thus there is no way to construct an analogue of the fact that supersingular elliptic curves in characteristic $p > 0$ can always be defined over $\mathbb{F}_{p^2}$ for supersingular abelian varieties of dimension 2. This also holds for dimension $g \geq 3$ and varieties with p-rank less than $g - 1$.

II. The second point though proves easier to deal with and we are able to get a similar result as in the case of elliptic curves.

Problem 14. *Let A_0 and A_1 be supersingular abelian varieties of genus two defined over a field of characteristic $p > 0$. Is there an isogeny $\phi : A_0 \to A_1$?*

By Tate's Isogeny Theorem 2.7 we know for two such Jacobians A_0 and A_1 defined over a finite field $\mathbb{F}_q$ of characteristic p that they are $\mathbb{F}_q$-isogenous if and only if we have

$$\#A_0(K) = \#A_1(K)$$

for all finite extensions $K \supseteq \mathbb{F}_q$. Let E_0 resp. E_1 denote the supersingular elliptic curves such that there are isogenies

$$\phi_i : A_i \to E_i \times E_i,$$

then we obtain $\#E_i(K)^2 = \#A_i(K)$ from the same argument. Since as seen before all supersingular elliptic curves E_0 and E_1 have the same number of K-rational points and thus are isogenous, this means that also all supersingular Jacobians of genus-two-curves are isogenous and the following diagram commutes using isogenies and their duals.

$$\begin{tikzcd} A_0 \arrow[r] \arrow[d, "\phi_0"] & A_1 \arrow[d, "\phi_1"] \\ E_0 \times E_0 \arrow[r] & E_1 \times E_1 \end{tikzcd}$$

So we get the following result.

Proposition 4.37. *Let A_0 and A_1 be supersingular abelian varieties of dimension g defined over a finite field $\mathbb{F}_q$ of characteristic $p > 0$. Then there exists an $\mathbb{F}_q$-isogeny $\phi : A_0 \to A_1$.*

But as we have seen in the last point, a supersingular abelian variety A does not have to be defined over a finite field, so this argument is not always applicable.

Luckily, even if A is defined over a field K of characteristic p which is not a finite field, PROPOSITION 4.34 provides us with an abelian variety $\widetilde{A}$ defined over a finite field $\mathbb{F}_q$ and a $\mathbb{F}_q$-isogeny $A \to \widetilde{A}$. Thus also such varieties are isogenous to the ones defined over finite fields and the isogenies between them can be defined over a finite field, too.

PROPOSITION 4.38. *Let A_0 and A_1 be supersingular abelian varieties of dimension g defined over a field K of characteristic $p > 0$. Then there exists an isogeny $\phi : A_0 \to A_1$ which is defined over a finite field.*

Note that neither the degree nor the field of definition of the isogeny is specified and especially that this does not mean that every isogeny of any given degree has to be defined over a finite field, only that there exist some of them between any supersingular abelian varieties.

III. The next problem which arises in contrast to the elliptic situation is the question whether the graph of supersingular JACOBIANS is also fully connected for a single isogeny degree ℓ or not.

PROBLEM 15. *Regard the graph with supersingular abelian varieties of genus two defined over a field of characteristic $p > 0$ as nodes and with ℓ-isogenies as edges for a fixed prime $\ell \neq p$. Is this supersingular isogeny graph fully connected?*

MESTRE'S result which could be applied on supersingular elliptic curves is working with a connection between supersingular points and a model for the moduli space of supersingular elliptic curves and cannot be generalized immediately since again the moduli space of supersingular abelian varieties is not as simple[5]. So it is not even clear if a random walk algorithm with isogenies of given degree can always provide an isogeny between two arbitrary supersingular JACOBIANS.

We further investigate the question whether we can determine if we can stay in a certain subgraph by starting at a JACOBIAN of a genus-two-curve C defined over $\mathbb{F}_p$ for an odd prime p and simple isogenies of a given degree.

[5]The subset of the moduli space of principally polarized abelian varieties of dimension g which contains the supersingular ones – the so called *supersingular locus* – has dimension $\lfloor g^2/4 \rceil$ (LI-OORT [51]), so in this case we have a one-dimensional space.

Recall from SECTION 4.3.1 the definition of the RICHELOT isogeny from before: We split the defining degree-d-polynomial $f \in \mathbb{F}_p$ of C (where $d \in \{5,6\}$) into three polynomials g_0, g_1 and g_2 which have degree one or two and correspond to a two-torsion point of $A := \operatorname{Jac} C$ each.

Then we construct polynomials $\widetilde{g}_0$, $\widetilde{g}_1$ and $\widetilde{g}_2$ which can be computed directly from the coefficients of the g_i. The product of the $\widetilde{g}_i$ provides a defining polynomial $\widetilde{f}$ of a genus-two-curve $C_{\mathfrak{g}}$ and the RICHELOT isogeny a $(2,2)$-isogeny

$$\phi_{\mathfrak{g}} : A \to A_{\mathfrak{g}}$$

where $A_{\mathfrak{g}}$ is the JACOBIAN of the hyperelliptic curve $C_{\mathfrak{g}}$.

We can immediately see that

$$\begin{aligned} g_i \in \mathbb{F}_q[X] \quad &\Longrightarrow \quad \widetilde{g}_i \in \mathbb{F}_q[X] \\ &\Longrightarrow \quad \widetilde{f} \in \mathbb{F}_q[X] \\ &\Longrightarrow \quad C_{\mathfrak{g}} \text{ defined over } \mathbb{F}_q. \end{aligned}$$

The same is true for the field of definition of the RICHELOT isogeny $\phi_{\mathfrak{g}}$ since the coefficients of the polynomials in its representation as rational function can also be computed from the g_i, so

$$g_i \in \mathbb{F}_q[X] \quad \Longrightarrow \quad \phi_{\mathfrak{g}} \text{ defined over } \mathbb{F}_q.$$

Still, the field of definition of the g_i depends on the roots $\alpha_1, \cdots, \alpha_d$ of f and thus on the WEIERSTRASS points of C as we have for $g_i := c_i(X-\alpha_j)(X-\alpha_k)$ resp. $g_i := c_i(X-\alpha_j)$ with $c_i \in \mathbb{F}_p^*$

$$\alpha_j, \alpha_k \in \mathbb{F}_q \quad \Longrightarrow \quad g_i \in \mathbb{F}_q.$$

As we know the WEIERSTRASS points of C correspond with the 2-torsion of A and thus when the complete two-torsion group is defined over $\mathbb{F}_q$ all WEIERSTRASS points have already to be defined over this extension field,

$$A(\mathbb{F}_q)[2] \cong (\mathbb{Z}/2\mathbb{Z})^4 \quad \Longleftrightarrow \quad \alpha_1, \cdots, \alpha_d \in \mathbb{F}_q.$$

Taken as a whole we therefore get the following result.

Proposition 4.39. *Let C be a hyperelliptic curve of genus two defined over the finite field $\mathbb{F}_p$ and let A be its* Jacobian. *Let further $C_{\mathfrak{g}}$ be the image curve of the* Richelot *isogeny $\phi_{\mathfrak{g}}$ dependent on an unsigned quadratic splitting of the form $\mathfrak{g} := (g_0, g_1, g_2)$. Then we have*

$$A(\mathbb{F}_q)[2] \cong (\mathbb{Z}/2\mathbb{Z})^4 \quad \Longrightarrow \quad C_{\mathfrak{g}}, \phi_{\mathfrak{g}} \text{ defined over } \mathbb{F}_q$$

where $\mathbb{F}_q$ is a finite extension field of $\mathbb{F}_p$.

Unfortunately, the field of definition of the roots of f can be a large extension field of $\mathbb{F}_p$ so in general we cannot restrict to a given small q here. For a certain class of supersingular hyperelliptic curves of genus two though, Takashima and Yoshida [85] have found a restriction to $q = p^2$ resp. $q = p^4$ dependent on $p \pmod 5$.

For $p > 5$ they regard curves C defined over $\mathbb{F}_p$ given by the polynomial

$$Y^2 \quad - \quad X^5 + u$$

where $u \in \mathbb{F}_p$. Those curves are supersingular if and only if $p \not\equiv 1 \pmod 5$ due to Proposition 1.13 of Ibukiyama-Katsura-Oort [39].

If the Jacobian of a genus two curve C fulfills

$$A(\mathbb{F}_q) \cong (\mathbb{Z}/(q^{1/2}+1)\mathbb{Z})^4,$$

then we have $A(\mathbb{F}_q)[2] \cong (\mathbb{Z}/2\mathbb{Z})^4$ since p is odd. In Lemma 4.3 Takashima and Yoshida [85] show that for a curve of the above described form this condition is valid with $q = p^2$ resp. $q = p^4$ for the cases $p \equiv 4 \pmod 5$ resp. $p \equiv 2, 3 \pmod 5$. Thus we get the next result from the observations before.

Proposition 4.40. *Let $p > 5$ be a prime and $C := \mathcal{V}(Y^2 - X^5 + u)$ for $u \in \mathbb{F}_p$ be a hyperelliptic curve of genus two defined over $\mathbb{F}_p$ with* Jacobian *A. Then we have*

$$\begin{aligned} A(\mathbb{F}_{p^2}) &\cong (\mathbb{Z}/2\mathbb{Z})^4 \quad \text{if} \quad p \equiv 4 \pmod 5, \\ A(\mathbb{F}_{p^4}) &\cong (\mathbb{Z}/2\mathbb{Z})^4 \quad \text{if} \quad p \equiv 2, 3 \pmod 5 \end{aligned}$$

and thus $C_{\mathfrak{g}}$ and $\phi_{\mathfrak{g}}$ are defined over $\mathbb{F}_{p^2}$ resp. $\mathbb{F}_{p^4}$.

Moreover, we can show that the property $\widetilde{A}(\mathbb{F}_q) \cong (\mathbb{Z}/(q^{1/2}+1)\mathbb{Z})^4$ is also true for every Jacobian $\widetilde{A}$ of a hyperelliptic curve $\widetilde{C}$ which can be reached by a chain of RICHELOT isogenies starting at the JACOBIAN of such a C. Since all those RICHELOT isogenies are defined over $\mathbb{F}_q$ with appropriate q due to the reflections above, A and $\widetilde{A}$ are $\mathbb{F}_q$-isogenous and due to TATE'S Isogeny Theorem 2.7 their characteristic polynomials χ_A and $\chi_{\widetilde{A}}$ of the q-th FROBENIUS are the same.

For an abelian variety A defined over $\mathbb{F}_q$ the structure $A(\mathbb{F}_q)$ depends on the irreducible components of χ_A (see THEOREM 2 of XING [94]), hence we get $A(\mathbb{F}_q) \cong \widetilde{A}(\mathbb{F}_q)$ and thus $\widetilde{C}$ is also defined over $\mathbb{F}_{p^2}$ resp. $\mathbb{F}_{p^4}$.

If we start this procedure at a general supersingular curve C, this does not have to be true, even when we remain in the case where we only regard RICHELOT isogenies. As we have seen the field of definition of an image curve of such an isogeny depends on the field of definition of the roots of the starting curve's defining polynomial. Hence we are not able to determine a useful restriction of which sort of JACOBIANS can be attained from an arbitrary starting point via a given type of isogenies.

Thus we cannot make a refined statement about the structure of isogeny graphs of supersingular genus-two JACOBIANS. Even when we only regard the component of the full 2-RICHELOT isogeny graph which contains the JACOBIAN of the above investigated curve

$$C = \mathcal{V}(Y^2 - X^5 + u)$$

does not provide a well-explorable and predictable structure. Since we have seen that there are 15 RICHELOT isogenies starting at each hyperelliptic JACOBIAN, most often[6] those graphs are 15-regular. Even for the smallest possible primes we can investigate, the cardinality of the according component gets large and they cannot reasonably be drawn in a comprehensible way.

IV. Finally the result from WATERHOUSE or RÜCK as in THEOREM 2.39 provided the essential tools for our improved algorithm in the $\mathbb{F}_p$-rational supersingular elliptic situation.

PROBLEM 16. *Let A be a supersingular abelian variety of genus two defined over $\mathbb{F}_{p^r}$ for an integer $r > 0$ and let $\mathcal{A}$ be the algebra such that* $\operatorname{End} A$ *is isomorphic to a maximal order in $\mathcal{A}$. Is the a restriction on r such that $\mathcal{A}$ is a number field?*

[6] Only when there are nodes representing the cartesian product of two elliptic curves this does not have to apply. Such nodes appear if and only if $p \equiv 4 \pmod 5$ as seen in PROPOSITION 1.13 of IBUKIYAMA-KATSURA-OORT [39].

> THEOREM 2.39 is only stated for elliptic curves and relies on their special structure. We do not know if there is a restriction of endomorphism rings such that they are orders in a number field analogous to the elliptic case.
>
> If that were possible, we could try to generate a connection to an ideal class group again and adapt the appropriate algorithms. However, from a present-day perspective such a lifting-and-reduction correspondence preserving an endomorphism ring has not yet been established.

Thus we see that for the supersingular situation there are still a number of open problems even when we only regard genus two and several obstacles occur in contrast to the situation of supersingular elliptic curves. Difficulties to conclude parallel results arise among others since

- a supersingular variety of dimension $g > 1$ in characteristic $p > 0$ does not have to be defined over a finite field,
- when we start with simple RICHELOT isogenies at such a variety which is defined over $\mathbb{F}_p$, we cannot make a good restriction about where the image curve can be defined,
- even when we just regard the components of graphs with such isogenies as edges which contain the JACOBIAN of the special curve C as above – and thus all varieties in the graph are defined over $\mathbb{F}_{p^4}$ – the components become quite large and not easy to deal with,
- the endomorphism ring of such a variety is an order in a non-commutative algebra of dimension g^2 over $\mathbb{Q}$ and there is no known restriction to the endomorphism ring of the variety such that there exists a lift to an abelian variety in characteristic zero with the same endomorphism ring,
- thus no connection to an ideal class group can be formed yet and we know about no upper bound for the isogeny degree such that the supersingular isogeny graph in dimension $g > 1$ is fully connected.

These problems give rise to many significant questions and impulses for further proceeding in what seems to be a most interesting field of theory for future research.

5 Cryptography with Elliptic Curves and Isogenies

Elliptic curves have been discovered for cryptographic methods in the mid 1980s and are common use today. Basically every cryptosystem which relies on a group structure can be applied on the point group $E(K)$ of an elliptic curve E over a finite field K since this group is finite and the addition law is easy to compute. Especially this means that there is a Discrete Logarithm Problem (DLP) on elliptic curves as described later which is the foundation for many currently used systems. For group size $n \in \mathbb{N}$ generic attacks like Pollard Rho, Shanks BSGS and Pohlig-Hellman can solve the DLP in $\mathcal{O}(\sqrt{n})$ operations, which is exponential in the input size $\log n$. Such methods are therefore infeasible for solving DLPs.

Theoretically these cryptosystems also work for arbitrary abelian varieties where we also have a group structure, but usually the arithmetic is not as efficient as in the simple case of elliptic curves. Furthermore there are certain attacks working on them. Even when we only regard Jacobians of hyperelliptic curves defined over K there are methods to solve the DLP for certain higher genus curves in subexponential time as described by Enge in [23] or index calculus methods as presented in Thériault [89]. Thus we usually restrict to elliptic curve cryptography (ECC) where also isogenies tend to appear often.

In this section we will first regard the discrete logarithm problem on elliptic curves, ECDLP. For certain classes of elliptic curves there are better-than-general methods for solving this problem and we will briefly describe three of them. Other elliptic curves are actually used in important present cryptographic applications.

Afterwards we will discuss two cryptographic methods which rely on isogenies between supersingular elliptic curves instead of an ECDLP based scheme, so they are set in the area of the main result of this thesis. We will investigate how our improved algorithm for the computation of such isogenies will affect the security of these systems.

5.1 Cryptography Based on the ECDLP

Many public key cryptosystems build their security on the hardness of the well-known Discrete Logarithm Problem (DLP). Since this is a problem which can be investigated on any finite group, it can particularly be adapted on the setting of the group $E(K)$ where E is an elliptic curve defined over a finite field K. In this situation the DLP can be stated as following.

Problem 17 (Elliptic Curve Discrete Logarithm Problem). *Let E be an elliptic curve defined over a finite field $K = \mathbb{F}_q$ of characteristic $p > 0$. Let $P, Q \in E(K)$ be points such that $Q \in \langle P \rangle$ with $\#\langle P \rangle := n \in \mathbb{N}$. Find $m \in \{0, \cdots, n-1\}$ with $Q = [m]P$.*

This problem is abbreviated ECDLP. Its security is dependent on the size of the group $\langle P \rangle$, so it is usually tried to find elliptic curves with nearly prime order of $E(K)$ so the ECDLP has to be solved in the subgroup of big prime order $n \mid \#E(K)$.

We can use isogenies to transfer the ECDLP from an elliptic curve E_0 defined over $K = \mathbb{F}_q$ to another elliptic curve E_1 if they are isogenous. For that we consider $P, Q \in E_0(K)$ with $Q \in \langle P \rangle$ and want to know for which $m \in \mathbb{N}$ the relation $Q = [m]P$ is true. Let $\phi : E_0 \to E_1$ be an isogeny and denote the images of P and Q under ϕ with $\widetilde{P}$ and $\widetilde{Q}$, respectively. Applying ϕ on the problem equation yields an ECDLP on E_1 as

$$\begin{aligned} \widetilde{Q} = \phi(Q) &= \phi([m]P) \\ &= (\phi \circ [m])(P) \\ &= ([m] \circ \phi)(P) \\ &= [m]\widetilde{P} \end{aligned}$$

since the multiplication-by-m-maps commute with every other isogeny. Thus if we can solve ECDLPs on E_1 and if isogenies are fast enough to compute, we can solve ECDLPs also on every elliptic curve which is isogenous to E_1, that is, on the whole isogeny class.

There are several systems based on the ECDLP which appear in actual practice like in projects of the German government concerning for instance electronic health cards and passports. The security for these projects is provided by the Bundesamt für Sicherheit in der Informationstechnik (BSI) as in [9] based on their technical guideline [8]. Among other methods they use elliptic curve cryptography algorithms for signatures (ECDSA, ECGDSA and EC-Schnorr) and key agreements (Diffie-Hellman and ElGamal). We will not repeat the principles of these standard methods here.

However, there are several types of elliptic curves where good attacks on the ECDLP have been developed and thus they are not secure for cryptographic use of the above methods and should be avoided in this environment. We will describe the reasons for that in the following parts.

5.1.1 MOV Attack via Pairings

Menezes, Okamoto and Vanstone [55] developed a method for reducing an ECDLP from an elliptic curve E defined over a finite field $\mathbb{F}_q$ to a DLP on the multiplicative group of a finite field $\mathbb{F}_{q^k}$ where k is an integer. We know that for such groups there are subexponential algorithms like the number field sieve or the function field sieve for solving DLPs. Thus – if k is not too big – it is possible to solve this new DLP much faster than the original one on the elliptic curve.

This MOV attack on ECDLPs uses the Weil pairing to map the subgroup $\langle P \rangle$ into $\bar{\mathbb{F}}_q$, so we sketch it first. Frey and Rück [26] use a variant of the Tate pairing (also called Tate-Lichtenbaum pairing) for a similar approach.

Let E be an elliptic curve defined over the finite field $\mathbb{F}_q$ of characteristic $p > 0$ and $n \in \mathbb{N}$ with $\gcd(n, p) = 1$. Let μ_n be the group of n-th roots of unity in $\bar{\mathbb{F}}_q$. There exists a non-degenerate bilinear map

$$e_n : E[n] \times E[n] \;\; \to \;\; \mu_n$$

called the Weil *pairing* which can be defined with divisors as in Section 13 of Milne [59] or Section III.8 of Silverman [75]. We will not need the technical details of how to compute the actual value of the pairing, therefore we abstain from introducing the explicit formulas.

The Weil pairing has a number of practical properties as seen in Menezes, Okamoto and Vanstone [55] or Galbraith [28]. For $P, Q, R \in E[n]$ we have

1. identity: $e_n(P, P) = 1$,
2. non-degeneration: $e_n(P, \mathcal{O}) = 1$ and $e_n(P, Q) = 1$ for all $Q \in E[n]$ implies $P = \mathcal{O}$,
3. alternation: $e_n(P, Q) = e_n(Q, P)^{-1}$,
4. bilinearity: $e_n(P + Q, R) = e_n(P, R)e_n(Q, R)$ and $e_n(P, Q + R) = e_n(P, Q)e_n(P, R)$,
5. Galois invariance: $e_n(\sigma(P), \sigma(Q)) = \sigma(e_n(P, Q))$ for all $\sigma \in \mathrm{Gal}(\bar{\mathbb{F}}_q, \mathbb{F}_q)$,
6. $E[n] \subseteq E(\mathbb{F}_{q^k}) \implies e_n(P, Q) \in \mathbb{F}_{q^k}$.

Remark. For abelian varieties the Weil pairing can be introduced with the dual variety as a non-degenerate bilinear pairing

$$e_n : A[n] \times A^\vee[n] \;\; \to \;\; \mu_n,$$

also defined through divisors on A. When we take a polarization $\phi : A \to A^\vee$, we can adapt another pairing

$$\begin{array}{rcl} e_n^\phi : A[n] \times A[n] & \to & \mu_n \\ (P, Q) & \mapsto & e_n(P, \phi(Q)) \end{array}$$

although this may be degenerated.

An important fact concerning the question whether $E[n] \subseteq E(\mathbb{F}_{q^k})$ is true can be found in LEMMA 3 of MENEZES, OKAMOTO and VANSTONE [55].

LEMMA 5.1. *Let E be an elliptic curve defined over the finite field $\mathbb{F}_q$ of characteristic $p > 0$. For $n \in \mathbb{N}$ with $\gcd(n, q) = 1$ we have*

$$\begin{array}{rcl} E[n] \subseteq E(\mathbb{F}_{q^k}) & \iff & n^2 \mid \#E(\mathbb{F}_{q^k}) \\ & \iff & n \mid q^k - 1. \end{array}$$

COROLLARY III.8.1.1 of SILVERMAN [75] or THEOREMS 9 and 10 of MENEZES, OKAMOTO and VANSTONE [55] further show the following result.

LEMMA 5.2. *Let E be an elliptic curve as above and $P \in E(\mathbb{F}_q)$ with $\#\langle P \rangle = n \in \mathbb{N}$ and $\gcd(n, q) = 1$. Then there exists some $R \in E[n]$ such that $e_n(P, R) \in \mu_n$ is a primitive root of unity and for this fixed R the map*

$$\begin{array}{rcl} \langle P \rangle & \to & \mu_n \\ Q & \mapsto & e_n(Q, R) \end{array}$$

is an isomorphism of groups.

We still want to solve the ECDLP $Q = [m]P$ with $P, Q \in E(\mathbb{F}_q)$ such that $\#\langle P \rangle = n$ and $Q \in \langle P \rangle$. We now have to perform the following steps.

- ✦ Find minimal $k \in \mathbb{N}$ with $E[n] \subset E(\mathbb{F}_{q^k})$,
- ✦ find $R \in E[n]$ as in LEMMA 5.2 and compute $\alpha := e_n(P, R) \in \mathbb{F}_{q^k}$,
- ✦ further compute $\beta := e_n(Q, R) \in \mathbb{F}_{q^k}$,

then we have with the rules for computing of the WEIL pairing as above

$$\beta = e_n(Q, R) = e_n([m]P, R) = e_n(P, R)^m = \alpha^m$$

which is a DLP in $\mathbb{F}_{q^k}$. This integer k is also called *embedding degree.*

There are a few points in this procedure which have to be examined for finding out how fast the method is. First, computing the embedding degree k is equivalent to finding the minimal solution k of the equation

$$q^k \equiv 1 \pmod{n}$$

due to LEMMA 5.1. Second, we have to find an appropriate $R \in E[n]$ with $e_n(P, R)$ of order n. SILVERMAN [75] shows in PROPOSITION XI.6.1 how that can be done in polynomial time and explains in THEOREM XI.8.1 how the MILLER algorithm computes WEIL pairings also in polynomial time. Thus we have the following result.

PROPOSITION 5.3. *Let E be an elliptic curve defined over the finite field $\mathbb{F}_q$ of characteristic $p > 0$ and regard $P \in E(\mathbb{F}_q)$ with $\#\langle P\rangle = n$, $\gcd(n,p) = 1$ and $Q \in \langle P\rangle$. The* ECDLP *$Q = [m]P$ can be transferred to a* DLP *in $\mathbb{F}_{q^k}$ where $k \in \mathbb{N}$ is the embedding degree with a polynomial algorithm.*

Usually though the embedding degree is too large to improve the complexity of this new DLP in contrast to the original ECDLP. However, for supersingular elliptic curves we can show that always $k \leq 6$ has to be true and this is small enough for a significant difference in the running time as seen in COROLLARY 12 of MENEZES, OKAMOTO and VANSTONE [55].

PROPOSITION 5.4. *Let the elliptic curve E from* PROPOSITION *5.3 be supersingular. Then we have $k \leq 6$ and the obtained* DLP *can be solved in subexponential time.*

PROOF. First we know from THEOREM 2.39 that the trace of a supersingular elliptic curve E is $t = 0$, $t = \pm\sqrt{q}$, $t = \pm 2\sqrt{q}$ or $t = \pm q^{(r+1)/2}$ for $q = p^r$ with $p \in \{2, 3\}$ and $r \in \mathbb{N}$ odd.

When we have $P \in E(\mathbb{F}_q)$ with $\#\langle P\rangle = n \in \mathbb{N}$ this especially means

$$n \mid \#E(\mathbb{F}_q) = q + 1 - t$$

and since $p \mid t$ we get $\gcd(n, q) = 1$ and LEMMA 5.1 can be applied. It tells us that

$$E[n] \subseteq E(\mathbb{F}_{q^k}) \iff n \mid q^k - 1.$$

Thus we investigate the situation for all possible traces t.

- ✦ $t = 0$:
  This yields $n \mid q + 1$, so we get $n \mid q^2 - 1 = (q + 1)(q - 1)$ and thus obtain $k = 2$ or $k = 1$ when already $n \mid q - 1$.

- ✦ $t = \pm\sqrt{q}$:
  We have $n \mid q+1\pm\sqrt{q}$ and thus $n \mid q^3-1 = (q-1)(q+1+\sqrt{q})(q+1-\sqrt{q})$, so $k \leq 3$.

- ✦ $t = \pm 2\sqrt{q}$:
  Here we have $n \mid q+1\pm 2\sqrt{q} = (\sqrt{q}\pm 1)^2$ and thus $n \mid q-1 = (\sqrt{q}+1)(\sqrt{q}-1)$ which yields $k = 1$.

- ✦ $t = \pm p^{(r+1)/2}$ and $q = p^r$ with $p = 2$ and r odd:
  When we rearrange this form of the trace to $t = \pm\sqrt{2q}$, we get $n \mid q+1\pm\sqrt{2q}$ and thus $n \mid q^4-1 = (q+1)(q-1)(q+1+\sqrt{2q})(q+1-\sqrt{2q})$, hence $k \leq 4$.

- ✦ $t = \pm p^{(r+1)/2}$ and $q = p^r$ with $p = 3$ and r odd:
  Similarly we can write $t = \pm\sqrt{3q}$ for the trace here, get $n \mid q+1\pm\sqrt{3q}$, attain $n \mid q^6-1 = (q+1)(q-1)(q^2+q+1)(q+1+\sqrt{3q})(q+1-\sqrt{3q})$ and $k \leq 6$.

In all cases we clearly have $k \leq 6$ and thus the result follows. □

Due to these considerations it is not advisable to use supersingular elliptic curves for cryptographic schemes based on the ECDLP. The small embedding degree gives a good possibility for an attack which is not usually true for an ordinary elliptic curve.

5.1.2 Anomalous Elliptic Curves

In the MOV attack the situation with $\gcd(n, q) \neq 1$ were omitted. But there is another approach presented by SMART in [76] which shows that elliptic curves E defined over the finite field $\mathbb{F}_p$ with $\#E(\mathbb{F}_p) = p$ are not suited for cryptography based on the ECDLP either. There the problem can even be transferred on a DLP on an additive group which can be solved in linear time. We will briefly describe the idea here.

Let E be an elliptic curve defined over $\mathbb{F}_p$ with $\#E(\mathbb{F}_p) = p$ and take two points $P, Q \in E(\mathbb{F}_p) \setminus \{\mathcal{O}\}$ which obviously both have order p. Thus there exists an integer $0 \leq m \leq p-1$ with $Q = [m]P$ which we want to determine.

Since the problem is only interesting for large p, we can assume that E is given by a short WEIERSTRASS polynomial $Y^2 - X^3 - aX - b$. Now we consider the elliptic curve $\widetilde{E}$ defined over the p-adic numbers $\mathbb{Q}_p$ which has a short WEIERSTRASS equation $Y^2 - X^3 - \widetilde{a}X - \widetilde{b}$ with the coefficients a and b from E interpreted as elements $\widetilde{a}, \widetilde{b}$ of $\mathbb{Q}_p$.

Further we construct points $\widetilde{P}, \widetilde{Q} \in \widetilde{E}(\mathbb{Q}_p)$. For that let $P = (x, y) \in E(\mathbb{F}_p)$, then y is a root of the polynomial $t^2 - x^3 - ax - b \in \mathbb{F}_p[t]$ and $f'(y) \neq 0$ since P is not of order two. Therefore by Hensels Lemma there exists a $\widetilde{y} \in \mathbb{Q}_p$ such that $\widetilde{y}$ is a root of the polynomial $t^2 - \widetilde{x}^3 - \widetilde{a}\widetilde{x} - \widetilde{b} \in \mathbb{Q}_p[t]$ where $\widetilde{x} \in \mathbb{Q}_p$ is a lift of x.

Denote the reduction map from $\widetilde{E}$ to E with π. Then there exists an easily computable map

$$\log_E : \ker \pi \quad \to \quad p\mathbb{Z}_p$$

where $\mathbb{Z}_p$ are the p-adic integers and the operation on $p\mathbb{Z}_p$ is additive (see Chapter IV.5 of Silverman [75]). This map satisfies the usual calculation rules of a logarithm with respect to the additive group law of $\ker \pi$. Since $\widetilde{P}$ and $\widetilde{Q}$ both have order p, we get $[p]\widetilde{P}, [p]\widetilde{Q} \in \ker \pi$ and also $\widetilde{R} \in \ker \pi$ for $\widetilde{R} := \widetilde{Q} - [m]\widetilde{P}$. We label the images of $[p]\widetilde{P}, [p]\widetilde{Q}$ and $\widetilde{R}$ under $\log_E$ with $p\alpha$, $p\beta$ and $p\gamma$ respectively. Then we get

$$\begin{aligned} p\beta &= \log_E([p]\widetilde{Q}) \\ &= \log_E([p]([m]\widetilde{P} + \widetilde{R})) \\ &= m \log_E([p]\widetilde{P}) + p \log_E(\widetilde{R}) \\ &= mp\alpha + p^2\gamma \\ &\equiv mp\alpha \pmod{p^2\mathbb{Z}_p} \end{aligned}$$

and finally are able to compute

$$m \equiv \beta\alpha^{-1} \pmod{p\mathbb{Z}_p}.$$

Remark. The group $\ker \pi$ is a formal group often denoted with $E_1(\mathbb{Q}_p)$. For more information on that matter consult Silverman [75] Chapter IV, Section VII.2, Exercise VII.7.13 and Proposition XI.6.5.

There is also mentioned in Remark XI.6.6 and shown in Example XI.6.7 how it is only necessary to compute lifts modulo p^2, so the effort for the described method is low. Computing m transmutes to a DLP in an additive group and can thus be solved with one inversion and one multiplication.

5.1.3 Weil Decent Attack

The Weil descent was first introduced by Frey [25] in 1998 and Galbraith and SMART [30] used this approach to transfer the ECDLP on an elliptic curve defined over a finite field $\mathbb{F}_{q^r}$ with $r > 1$ to a DLP on a Jacobian of a hyperelliptic curve defined over $\mathbb{F}_q$ with genus $g \geq r$. We already mentioned that there are subexponential index calculus methods to solve such problems if the genus is high enough. Gaudry, Hess, Smart [33] examine this approach and the occurring curves more detailed, especially with regard to actual cryptographic applications. Thus the method is also often called GHS Weil *descent attack*.

Let E be an elliptic curve defined over $K := \mathbb{F}_{q^r}$ where $r > 1$ is an integer. In applications often $\operatorname{char} \mathbb{F}_q = 2$ is suggested as well as r rather small such that q^r is large. We regard the usual ECDLP $Q = [m]P$ for $P, Q \in E(K)$ and $Q \in \langle P \rangle$ with $\#\langle P \rangle =: n$. We want to transform this problem such that it suffices to solve a DLP on a hyperelliptic Jacobian $\operatorname{Jac} C$. For that we first construct an abelian variety A of dimension n or $n-1$ in the following way.

Since K is a field extension of $\mathbb{F}_q$ of dimension r, there are elements $\psi_1, \cdots, \psi_r$ providing a $\mathbb{F}_q$-basis of K. Thus we can display the coefficients a_i of the defining Weierstrass equation of E as sums $\sum\limits_{j=1}^{r} a_{ij}\psi_i$ with known coefficients $a_{ij} \in \mathbb{F}_q$ and introduce new variables x_j and y_j for $j \in \{1, \cdots, r\}$ to write

$$X = \sum_{j=1}^{r} x_j \psi_j \quad \text{and} \quad Y = \sum_{j=1}^{r} y_i \psi_i.$$

When we substitute these sums into the original Weierstrass equation of E, expand the products and sort the terms with respect to the ψ_i, we get r equations in the $2r$ variables $x_1, \cdots, x_r, y_1, \cdots, y_r$. We call the vanishing polynomials of these equations $f_1, \cdots, f_r$ and define the variety $W(E) := \mathcal{V}(f_1, \cdots, f_r)$ which is defined over $\mathbb{F}_q$ and has dimension r. It is also called Weil *restriction of scalars*.

Due to a Theorem of Frey [25] on page 9 we have $W(E)(\mathbb{F}_q) \cong E(K)$ as algebraic groups. Thus $W(E)$ is actually an abelian variety defined over $\mathbb{F}_q$ and the group law of E can be transferred to it via the relation

$$\begin{aligned} E(K) &\rightarrow W(E)(\mathbb{F}_q) \\ \left(\sum_{j=1}^{r} u_j \psi_j, \sum_{j=1}^{r} v_j \psi_j \right) &\mapsto (u_1, \cdots, u_r, v_1, \cdots, v_r). \end{aligned}$$

Moreover, if E itself is defined over $\mathbb{F}_q$, then $E(\mathbb{F}_q)$ is isomorphic to a subvariety of $W(E)$ and we get the following relation from Lemma 4 of Galbraith, Smart [30].

Lemma 5.5. *Let E be an elliptic curve defined over $K = \mathbb{F}_{q^r}$ as before and $W(E)$ be the* Weil *restriction defined over $\mathbb{F}_q$. Then there exists an abelian variety V defined over $\mathbb{F}_q$ of dimension $r-1$ such that we have*

$$W(E) \;\cong\; E(\mathbb{F}_q) \times V$$

as isomorphism of varieties.

Definition. Let $W(E)$ and V be as in the previous lemma. The abelian variety A defined over $\mathbb{F}_q$ is set as

- $A := W(E)$ if E is not defined over $\mathbb{F}_q$,
- $A := V$ if E is defined over $\mathbb{F}_q$.

In the first case A has dimension r, in the second one $r-1$. In particular, when we map the points $P, Q \in E(K)$ from our ECDLP to points in $W(E)$ we get images in A which are defined over $\mathbb{F}_q$. Thus A is the abelian variety where the corresponding DLP from E is transferred to and we have a map

$$E(K) \;\to\; A(\mathbb{F}_q).$$

Next we construct a curve C defined over $\mathbb{F}_q$ by intersecting A with $r-1$ resp. $r-2$ hyperplanes which provides a variety of dimension one with a $\mathbb{F}_q$-rational point at $\mathcal{O}_A$. This yields a map

$$\phi : C(\mathbb{F}_q) \;\to\; A(\mathbb{F}_q)$$

which will be used with the next proposition. Gaudry, Hess, Smart [33] study the curve C in more detail. Working with function fields and Artin-Schreier theory they determine the genus of C and thus the dimension of $\operatorname{Jac} C$ to be

$$g = 2^{b-1} \quad \text{or} \quad g = 2^{b-1} - 1$$

with $1 \leq b \leq r$. This is important to know for the DLP on $\operatorname{Jac} C$ we will maintain.

Milne [60] Proposition 6.1 gives the *universal property* of Jacobians as below which helps us getting a connection to the Jacobian of C.

Proposition 5.6. *Let C be a smooth curve of genus g defined over a field F with a F-rational point P. Further let A be an abelian variety of dimension r defined over F and $\phi : C \to A$ be a map sending P to $\mathcal{O}_A$. Then there exists a unique homomorphism*

$$\psi : \operatorname{Jac} C \to A \quad \textit{with} \quad \phi = \psi \circ f^P$$

where f^P is the canonical embedding of C into $\operatorname{Jac} C$ with $f^P(P) = O_{\operatorname{Jac} C}$.

Thus we have a homomorphism $\psi : \operatorname{Jac} C \to A$ in our situation[7] which is also surjective when A is simple since its image is a subvariety of A. Due to Corollary 3 of Galbraith, Smart [30] we also know in that case that $g \geq r$ has to hold and $g = r$ if and only if A and $\operatorname{Jac} C$ are isogenous.

Now we regard the images of P and Q in $A(\mathbb{F}_q)$ and want to be able to pull them back to $\operatorname{Jac} C$ via ψ. Note that preimages of those points have to exist according to the surjectivity of ψ. Galbraith, Smart [30] treat this issue in Section 4 where they use the connection of $\operatorname{Jac} C$ to the divisor class group $\operatorname{Pic}^0 C$. This group consists of the set of degree zero divisors on C defined over $\mathbb{F}_q$ modulo principal divisors and is isomorphic to $\operatorname{Jac} C$ as an abelian variety as seen in Milne [60][8].

We will refrain from the technical details concerning divisors and the above mentioned pullback from that section which show how exactly the original problem is transformed to the problem of solving the DLP $D_Q = mD_P$ in $\operatorname{Pic}^0 C$. When this is possible, the resulting integer m is the required solution. Section 6 of Galbraith, Smart [30] discusses an approach to the DLP in $\operatorname{Pic}^0 C$ yielding a heuristic subexponential algorithm with growing genus.

As apparent from the description of the GHS attack as presented above, it is crucial that the elliptic curve is not defined over a prime field. Further, Menezes and Qu [56] show that it infeasible for elliptic curves defined over $\mathbb{F}_{2^s}$ with $s \in \{160, \cdots, 600\}$ prime, thus systems using such elliptic curves are not endangered by the GHS attack. However, there are proposals for using elliptic curves defined over $\mathbb{F}_{2^{155}}$ or $\mathbb{F}_{2^{185}}$ in an IETF standard (see for example Section 4 of ECC Brainpool [21]). Several exploits were made to see how the GHS attack can be applied to those elliptic curves.

[7] If C is not smooth, we replace it with its *normalization*, a smooth curve defined over the same field as C and related to C via a rational map of degree one, see Hartshorne [37], Exercise II.3.8 or the beginning of Section 2 of Galbraith, Smart [30].

[8] The divisor class group of a singular curve is isomorphic to the one of its normalization, thus this is also working when C is not smooth

Since we have $155 = 5 \cdot 31$, the method from above can be applied with $q = 2^{31}$ and $r = 5$ or with $q = 2^5$ and $r = 31$. Smart [77] examined the first of these explicitly proposed cases and came to the conclusion that such curves are secure against that attack since he obtained a curve C defined over $\mathbb{F}_{2^{31}}$ of genus 16 where the index calculus method currently would take years.

Jacobson, Menezes, Stein [42] regarded the latter case with $q = 2^5$ and found the GHS method applicable for 2^{32} of the 2^{156} isomorphism classes of elliptic curves defined over $\mathbb{F}_{2^{155}}$ which – although this is only a small portion of all possible curves – already suggests that this case is not qualified for cryptographic uses.

Later Galbraith, Hess, Smart [29] extended this number of vulnerable isomorphism classes to 2^{104} out of 2^{156} by using isogenies due to the following fact. Let E_0 and E_1 be isogenous elliptic curves defined over $\mathbb{F}_q$, then the GHS approach on each of those curves does not yield DLPs on Jacobians of curves *of the same genus*. This is quite important since it means that when we can solve the ECDLP on an elliptic curve E_0 via the GHS attack, then we can also solve a corresponding ECDLP on every isogenous elliptic curve E_1 even if the GHS method does not work for E_1 itself. At this point it is crucial that we have a efficient construction method for computing isogenies between E_0 and E_1 like the algorithm from Galbraith or any of its adaptions. This is a very interesting application of isogenies in a cryptographic area.

Summed up it is not advisable to build cryptosystems based on the ECDLP of elliptic curves defined over a composite extension field $\mathbb{F}_{2^s}$ with characteristic two and non-prime integer s since the problem could be transferred to an easier problem on the Jacobian of a hyperelliptic curve.

5.2 Supersingular Isogenies in Cryptography

Isogenies have a number of applications in cryptography. In this section we will focus our attention mostly on isogenies between supersingular elliptic curves in cryptographic settings and describe on the one hand a hash function and on the other hand a encryption system which is supposed to be quantum resistant, both of which are based on isogenies between supersingular elliptic curves. Further we analyze if our improvements for calculating $\mathbb{F}_p$-rational isogenies yield any new approaches of attacking those structures.

5.2.1 A Cryptographical Hash Function

Charles, Goren and Lauter [10] propose cryptographic hash functions based on expander graphs which work especially on supersingular isogeny graphs and are supposed to be collision resistant since the computation of isogenies between supersingular elliptic curves is hard. We will briefly describe the method in the situation of supersingular isogenies and analyze if our improvement for computing isogenies between $\mathbb{F}_p$-rational supersingular elliptic curves can be used to attack this system.

Definition. A *cryptographic hash function* is a function

$$h : \{0,1\}^* \quad \to \quad \{0,1\}^m$$

mapping arbitrary bitstrings deterministically to bitstrings of length $m \in N$. A *family of hash functions* is a finite set of hash functions h_k for k from some index set I. The value k is called *key* of the hash function.

A hash function h is *preimage resistant* or *one way* if given some $y \in \{0,1\}^n$ it is impracticable to compute an $x \in \{0,1\}^*$ with $h(x) = y$.

It is *collision resistant* if it is infeasible to find different bitstrings $x, y \in \{0,1\}^*$ with $h(x) = h(y)$.

Note that a hash function is never injective since the image set is smaller than the input set. This is reasonable because hash functions are normally used to compress information. Nevertheless, this means that there will always be collisions, that is, different bitstrings that are mapped on the same output. A hash function should be easy to compute but hard to invert.

For the isogeny hash functions we take 2-isogenies which are fastest to compute and regard the full supersingular isogeny graph $G_0(\bar{\mathbb{F}}_p, 2)$ for some prime p of desired bit length. In Charles-Goren-Lauter [10] the authors restrict to primes

p which satisfy $p \equiv 1 \pmod{12}$ since then the j-invariants 0 and 1728 are not supersingular and we do not have to deal with multiple edges arising from non-trivial automorphisms as discussed before.

When we define the index set I as the set of supersingular j-invariants in $\mathbb{F}_{p^2}$, we can construct a hash function h_k for every $k \in I$ in the following way. Let E_0 be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$ with j-invariant k and let $x \in \{0,1\}^*$ be a bitstring of length $n \in \mathbb{N}$. From this bitstring x we create a non-backtracking path $E_0 \to E_1 \to \cdots \to E_n$ with length n in $G_0(\bar{\mathbb{F}}_p, 2)$ as described below.

The path has to be deterministic or h would not always yield the same output for a given input $x = b_1 b_2 \cdots b_n$ with $b_i \in \{0,1\}$. So when we are at the node in $G_0(\bar{\mathbb{F}}_p, 2)$ representing E_{i-1}, we have to use the bit b_i to deterministically choose one of the three neighbors of E_{i-1} to become the next curve E_i in the chain. Each of those neighbors correspond to a subgroup of E_{i-1} of order 2 which arise from 2-torsion points. When the defining polynomial of E_{i-1} is $Y^2 - f(X)$ with a polynomial f of degree 3, the three distinct roots x_1, x_2, x_3 of f give us the first coordinate of the 2-torsion points $(x_i, 0)$. We fix some order relation '$<$' such that we can compare x_1, x_2 and x_3 as elements in $\bar{\mathbb{F}}_p$. Then we choose the smallest possibility under this relation when $b_i = 0$ and the next biggest if we have $b_i = 1$. Usually we only have two possibilities since we want a non-backtracking path and cannot take the dual of the last isogeny as new outgoing isogeny, so this is no restriction. The only case where there are three reachable neighbors is for E_0, so there we disregard the neighbor corresponding to the largest value under '$<$' with this method. But eventually this procedure yields a deterministically constructed chain of 2-isogenies in $G_0(\bar{\mathbb{F}}_p, 2)$.

We have seen that there are roughly $p/12 < p$ nodes in $G_0(\bar{\mathbb{F}}_p, \ell)$, so we can injectively map them to $\mathbb{F}_p$ with some embedding ε. Let E_n be the elliptic curve reached at the end of the path and j_n be its j-invariant. Then h_k returns the image of j_n under this embedding ε as bitstring which has length $m := \log p$.

For an attack on such a hash function h_k we have given E_0 and E_n where y is the representation of $\varepsilon(j(E_n))$ as bitstring and want to find a bitstring x with $h(x) = y$. Note that to enforce a collision of h_k it is not necessary for the isogeny coming from x to have degree 2^n but any path length will be sufficient, although it depends on the application whether the length of the chain is preset or not. Due to our previous considerations it takes $\widetilde{\mathcal{O}}(p^{1/2})$ field operations to construct such an isogeny via a path in $G_0(\bar{\mathbb{F}}_p, 2)$. If we need an isogeny of given degree 2^n, we have to modify the algorithm slightly, but the overall complexity class does not change.

When we now include our new considerations about isogenies between supersingular elliptic curves defined over $\mathbb{F}_p$ we can find an isogeny from E_0 to E_n in $\widetilde{\mathcal{O}}(p^{1/4})$ when they are defined over $\mathbb{F}_p$. Although this isogeny is constructed in a different graph – namely in the rational supersingular isogeny graph $G_0(\mathbb{F}_p, \mathcal{L})$ for a set of primes $\mathcal{L}$ instead of in the full supersingular isogeny graph $G_0(\bar{\mathbb{F}}_p, 2)$ – every edge in that graph can be lifted to an edge in a full supersingular isogeny graph $G_0(\bar{\mathbb{F}}_p, \mathcal{L})$. The problem is, that in the resulting chain of elliptic curves we take isogenies of degree $\ell > 2$ and thus have more than two possibilities for the next neighbor curve. Therefore we cannot convert the choice of the neighbor into a bit b_i to obtain the bitstring $x = b_1 b_2 \cdots b_n$.

If there is a way to convert a given $\mathcal{L}$-smooth isogeny into an isogeny of ℓ-power degree, this can be applied to our obtained $\mathcal{L}$-smooth isogeny to get a chain of 2-isogenies between E_0 and E_n. The consecutive application of those two algorithms yields an isogeny which has degree of a power of 2 and thus provides a collision of the hash function h_k.

In the recent paper Kohel-Lauter-Petit-Tignol [47] there is a new approach about which introduces a probabilistic algorithm with expected polynomial running time to convert a left ideal in a maximal order of a quaternion algebra ramified at p and ∞ to such an ideal of ℓ-power norm. We have seen that those ideals correspond to isogenies between supersingular elliptic curves defined over $\mathbb{F}_{p^2}$ and that the degree of the isogeny equals the norm of the ideal. Unfortunately, it seems to be complicated to calculate this correspondence between ideals and isogenies explicitly so that the structure cannot be immediately transmitted. This problem is marked as future work in the paper. Likewise, in the ordinary case no such transmission from the ideals to isogenies is known.

When E_0 and E_n are not defined over $\mathbb{F}_p$, we do not get a better complexity for constructing an isogeny between them with our new algorithm, but the computational results seem to imply that it is slightly faster anyway when we use $\mathcal{L}$-smooth $\mathbb{F}_p$-rational isogenies in between. In this situation we have the same problem that we have to convert the resulting isogeny to a chain of 2-isogenies.

Hence once there is a way to split an isogeny into 2-isogenies, our algorithm provides an improvement for a possible attack on an isogeny hash function. To achieve the same security of the hash function, the size of the prime p has to be increased considerately or elliptic curves which are defined over $\mathbb{F}_p$ have to be excluded.

5.2.2 A Proposed Quantum Resistant Cryptosystem

There have been several approaches to construct cryptosystems which are based on isogenies, but mostly they take isogenies between ordinary elliptic curves. We will not go into details of those concepts here but concentrate on a supersingular variant later. It started with Rostovtsev-Stolbunov [71] in 2006 where the authors used so called *isogeny stars* on ordinary elliptic curves.

Later in 2010 Stolbunov [83] stated a Diffie-Hellman type of key exchange with computing isogenies between ordinary elliptic curves. The security is based on the fastest classical algorithms so far for computing isogenies, which as we have seen are exponential in $\log p$ (Galbraith-Stolbunov [31], which is based on Galbraith-Hess-Smart [29]). However, a paper of Childs, Jao and Soukharev [11] from 2011 shows that on a quantum computer this can be defeated in subexponential time.

The goal of Jao-De Feo [43] is to find a system that is more secure and much faster than Stolbunov's. They use supersingular elliptic curves of smooth order so that there are many small subgroups and thus a large number of isogenies that are fast to compute. The cryptosystem lets Alice and Bob make a random walk on a different isogeny graph. Since those isogenies correspond to ideal classes in a maximal order of a quaternion algebra which do not commute, some extra information is needed to reach the same elliptic curve in the end as we will sketch briefly below. The authors claim that the provided system is quantum resistant since at least the attack of Childs-Jao-Soukharev is not applicable here.

Key Exchange. Suppose that Alice and Bob want to securely exchange data through establishing a cryptosystem which uses a secret shared key k. First they have to agree on this key in a way that no attacker can access it. In this case the key will arise from a shared elliptic curve, for example computed from its j-invariant.

For that we have to make some precomputations as follows.

- choose a prime $p = \ell_A^{e_A} \ell_B^{e_B} \cdot u - 1$ of desired size where ℓ_A, ℓ_B are small primes, $e_A, e_B, u \in \mathbb{N}$
- find a supersingular elliptic curve E_0 over $\mathbb{F}_{p^2}$
- find generators $\{P_A, Q_A\}$ resp. $\{P_B, Q_B\}$ of $E_0[\ell_A^{e_A}]$ resp. $E_0[\ell_B^{e_B}]$

We will discuss later the difficulties of getting those objects.

Afterwards Alice and Bob have to perform a few calculations concerning isogenies starting at the known elliptic curve E_0.

Alice	**Bob**
✦ choose $m_A, n_A \in \mathbb{Z}/\ell_A^{e_A}\mathbb{Z}$ with $m_A \not\equiv 0 \pmod{\ell_A}$ or $n_A \not\equiv 0 \pmod{\ell_A}$	✦ choose $m_B, n_B \in \mathbb{Z}/\ell_B^{e_B}\mathbb{Z}$ with $m_B \not\equiv 0 \pmod{\ell_B}$ or $n_B \not\equiv 0 \pmod{\ell_B}$
✦ compute subgroup $K_A := \langle m_A P_A + n_A Q_A \rangle$ of E_0 and isogeny $\phi_A : E_0 \to E_0/K_A =: E_A$	✦ compute subgroup $K_B := \langle m_B P_B + n_B Q_B \rangle$ of E_0 and isogeny $\phi_B : E_0 \to E_0/K_B =: E_B$
✦ compute $P'_B := \phi_A(P_B)$ and $Q'_B := \phi_A(Q_B) \in E_A$	✦ compute $P'_A := \phi_B(P_A)$ and $Q'_A := \phi_B(Q_A) \in E_B$

✦ $E_A, \phi_A(P_B), \phi_A(Q_B) \quad \overset{\text{exchange}}{\longleftrightarrow} \quad E_B, \phi_B(P_A), \phi_B(Q_A)$

✦ compute subgroup $K'_A := \langle m_A P'_A + n_A Q'_A \rangle$ of E_B and isogeny $\phi'_A : E_B \to E_B/K'_A =: E_{BA}$	✦ compute subgroup $K'_B := \langle m_B P'_B + n_B Q'_B \rangle$ of E_A and isogeny $\phi'_B : E_A \to E_A/K'_B =: E_{AB}$

The isogenies are computed via the formulae of Vélu which we examined before. We will analyze the efficiency later. Figure 11 visualizes the line of action of those proceedings.

$$
\begin{tikzcd}
 & E_A \arrow[dr, "\phi'_B"] \arrow[dd, dashed, leftrightarrow] & \\
E_0 \arrow[ur, "\phi_A"] \arrow[dr, "\phi_B"'] & & E_{AB} \\
 & E_B \arrow[ur, "\phi'_A"'] &
\end{tikzcd}
$$

Figure 11: A Key Exchange Protocol using Supersingular Isogenies

It can be shown that after these steps the constructed isogenies reach the same image curve since the kernels of $\phi'_A \circ \phi_B$ and $\phi'_B \circ \phi_A$ are equal because

$$
\begin{aligned}
\ker \phi'_A \circ \phi_B &= \{P \in E_0 \mid \phi_B(P) \in \ker \phi'_A\} \\
&= \{P \in E_0 \mid \phi_B(P) \in \langle m_A \phi_B(P_A) + n_A \phi_B(Q_A) \rangle\}
\end{aligned}
$$

and we have

$$\begin{aligned} \langle m_A\phi_B(P_A) + n_A\phi_B(Q_A)\rangle &= \phi_B(\langle m_A P_A + n_A Q_A\rangle) \\ &= \phi_B(\ker\phi_A)\} \end{aligned}$$

which yields that

$$\begin{aligned} \ker\phi'_A\circ\phi_B &= \{P\in E_0 \mid \exists Q\in\ker\phi_A : \phi_B(P) = \phi_B(Q)\} \\ &= \{P\in E_0 \mid \exists Q\in\ker\phi_A : \phi_B(\underbrace{P-Q}_{=:R}) = O_{E_B}\} \\ &= \{P\in E_0 \mid \exists Q\in\ker\phi_A, R\in\ker\phi_B : P = Q+R\} \end{aligned}$$

and since these observations can also be taken for A and B interchanged, this leads to the desired equality

$$\ker\phi'_A\circ\phi_B = \ker\phi'_B\circ\phi_A.$$

The common j-invariant of E_{BA} resp. E_{AB} can be used to form a secret shared key in a pre-agreed manner.

Public-Key Cryptosystem. In addition to the key exchange this setting can be used to establish a cryptosystem as shown below. First we have to choose a prime $p = \ell_A^{e_A}\ell_B^{e_B}\cdot u - 1$, E_0, $\{P_A, Q_A\}$, $\{P_B, Q_B\}$ as in the key-exchange protocol above and a finite set I and family $\mathcal{H}$ of hash-functions $h_k : \{E\} \to \{0,1\}^w$ for any $k\in I$. Then we can make the following arrangements.

- **Key Agreement:**
  - choose $m_A, n_A \in \mathbb{Z}/\ell_A^{e_a}\mathbb{Z}$ like above
  - compute E_A, P'_B, Q'_B
  - choose $k\in I$
  - **Public Key:** (E_A, P'_B, Q'_B, k)
  - **Private Key:** (m_A, n_A)
- **Encryption:**
  - take message $m\in\{0,1\}^w$
  - choose $m_B, n_B \in \mathbb{Z}/\ell_B^{e_B}\mathbb{Z}$ like above
  - compute E_B, P'_A, Q'_A

- compute $h := h_k(E_{AB})$
- compute $c := h \oplus m$
- send (E_B, P'_A, Q'_A, c)

Decryption:

- compute $h := h_k(E_{BA}) = h_k(E_{AB}) = c \oplus m$
- compute $h \oplus c = c \oplus m \oplus c = m$

Concerning this key exchange and encryption protocol there are several questions of efficiency we can state.

1. If $\ell_A^{e_A}, \ell_B^{e_B}$ are fixed, how do we find some $u \in \mathbb{N}$ of desired size such that $p := \ell_A^{e_A} \ell_B^{e_B} \cdot u - 1$ is prime?
2. If p is fixed, how is a supersingular elliptic curve E_0 over $\mathbb{F}_{p^2}$ found?
3. How can we find a basis of $E_0[\ell_A^{e_A}]$?
4. How do we compute $\phi_A : E_0 \to E_A$ with $\ker \phi_A = K_A$?

We briefly summarize the answers on those questions given by Jao-De Feo [43] in Section 3.3.

1. Let $\ell_A^{e_A}, \ell_B^{e_B}$ be fixed, then we test random u of the right size until $\ell_A^{e_A} \ell_B^{e_B} u - 1$ is prime. We do not have to care about u being coprime to ℓ_A or ℓ_B when we increase e_A resp. e_B in that cases. According to the authors of Jao-De Feo [43] this is probable enough due to the prime number theorem.
2. We already discussed the algorithm of Bröker [6] which efficiently constructs supersingular elliptic curves in given prime characteristic p.
3. When we randomly take a point $P \in E_0(\mathbb{F}_{p^2})$ and calculate $P' := [m]P$ for $m := (\ell_B^{e_B} u)^2$, we eliminated all terms containing ℓ_B and u from the order of the point so that P' has order of a power of ℓ_A and at most $\ell_A^{e_A}$. If this order equals $\ell_A^{e_A}$, we set $P_A := P'$, else we choose another random point P.

   Analogously we construct Q_A with order $\ell_A^{e_A}$ and in order to get a basis of $E_0[\ell_A^{e_A}]$ we have to check if P_A and Q_A are independent. This can be done with the Weil-pairing. Jao-De Feo [43] claim that P_A and Q_A having the right order and not being dependent happens with high probability.

4. As we know, computing an isogeny with big kernel is slow, so JAO-DE FEO [43] show how to successively find a chain of e_A isogenies of degree ℓ_A which combine to an isogeny $\phi : E_0 \to E_A$ with kernel K_A. Since ℓ_A is chosen to be a small prime, those isogenies are fast to compute. We do not go into the technical details here.

The security of the above described systems is based on the conjectured hardness of the following problems.

PROBLEM 18 (Supersingular Isogeny (SSI)). *Given E_A, P'_B, Q'_B, find generator of K_A.*

PROBLEM 19 (Supersingular Computational DIFFIE-HELLMAN (SSCDH)). *Given $E_A, E_B, P'_A, Q'_A, P'_B, Q'_B$, find j-invariant of E_0/K_{AB}.*

PROBLEM 20 (Supersingular Decisional DIFFIE-HELLMAN (SSDDH)). *Given a tuple sampled with probability* 0.5 *either from*
$(E_A, E_B, P'_A, Q'_A, P'_B, Q'_B, E_{AB})$
or from
$(E_A, E_B, P'_A, Q'_A, P'_B, Q'_B, E_C)$,
decide from which distribution it is.

These problems can be used as a basis to examine the key-exchange and encryption scheme as in THEOREMS 4.4 and 4.5 of JAO-DE FEO [43].

THEOREM 5.7.

1. *The key-exchange protocol based on isogenies between supersingular elliptic curves as described above is session-key secure in the authenticated links adversarial model of* CANETTI-KRAWCZYK *when we assume SS-DDH.*

2. *The ensuing public-key cryptosystem is secure in terms of indistinguishability against chosen plaintext attack (IND CPA) under some assumptions on $\mathcal{H}$.*

Here a key-exchange protocol is called *session-key secure in the authenticated links adversarial model of* CANETTI-KRAWCZYK if the same key is produced on both sides of the agreement and the advantage of a polynomial-time attacker is negligible. If the protocols were not secure in that way, there would be a polynomial-time distinguisher for SSDDH with non-negligible advantage.

It is obvious that a SSI solver entails a SSCDH solver which in turn leads to a SSDDH solver, but the other direction is not known and assumed to be hard. For their work JAO-DE FEO [43] make the additional assumption that also a SSDDH solver implies a SSI solver, that is, they suppose that the three problems are equally hard to solve. Then they analyze possible ways of attack as provided sketchily below.

To break the cryptosystem we have to compute E_{AB} and thus the kernel of the isogeny ϕ'_A. This arises from the same integers m_A and n_A as the kernel of ϕ_A and these integers can be found easily once a generator of the kernel is known (Jao-De Feo [43] refer to Teske [88] for this fact). Thus we have to compute an isogeny from E_0 to E_A in order to solve this problem.

As we have seen finding isogenies between supersingular elliptic curves over $\mathbb{F}_{p^2}$ has a complexity of $\mathcal{O}(\sqrt{p}(\log p)^2)$. In this scheme elliptic curves with smooth order are used, but it is unknown if this helps in some way for computing isogenies between them. Also the distribution of isogenous elliptic curves with kernels $\langle m_A P_A + n_A Q_A \rangle$ is not uniform, but so far no use of this fact has been found.

A main question is whether the additional information $\phi_A(P_B)$ and $\phi_A(Q_B)$ help to determine ϕ_A. Although we can compute ϕ_A on $E_0[\ell_B^{e_B}]$ completely since any element therein is a known linear combination of P_B and Q_B (again due to extended DLP of Teske [88]), finding ϕ_A seems to be as difficult as before.

Further the authors discuss the possibilities of quantum computers for attacking this scheme and especially if the quantum algorithm of Childs-Jao-Soukharev can be established for supersingular instead of ordinary elliptic curves. This algorithm in build on the fact that ideal classes form an abelian group though; and in a quaternion algebra this is not the case. So far no adaption of this concept is found and thus the algorithm is supposed to be quantum resistant.

Our improvement for computing isogenies between supersingular elliptic curves defined over $\mathbb{F}_p$ implies that to obtain the same security of this system, the elliptic curve E_0 as well as the integers m_A and n_A should be chosen such that all elliptic curves in this scheme are defined over $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$. Also in the case when the elliptic curves were defined over $\mathbb{F}_p$ we have a correspondence to ideal classes in a commutative ideal class group again, so probably the quantum algorithm of Childs-Jao-Soukharev works in this situation and provides an attack on the protocol.

6 Conclusion and Outlook

In this thesis we gave an overview about algorithms to compute isogenies between given elliptic curves defined over finite fields. For that we described the necessary theoretical background of abelian varieties, their endomorphism rings and the concept of isogenies. A survey of complex multiplication theory as well as famous lifting and reduction theorems were presented.

Then we concentrated on supersingular elliptic curves defined over the finite field $\mathbb{F}_p$ for a prime $p > 3$ and established a connection between their $\mathbb{F}_p$-rational endomorphism rings and the full endomorphism rings of certain elliptic curves with complex multiplication. This relation arose from a modification of the Deuring Reduction Theorem which we extended to this $\mathbb{F}_p$-rational supersingular case. It was important to see that $\mathbb{F}_p$-rational isogenies behave well in this situation so we could get the one-to-one connections

$$\left\{\begin{array}{c}\text{elliptic curves } E \text{ defined over } \mathbb{C}\\ \text{with } \operatorname{End} E \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}(\sqrt{-p})\\ \text{and } \mathbb{Z}[\sqrt{-p}] \subseteq \operatorname{End} E\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{supersingular elliptic curves}\\ \text{defined over } \mathbb{F}_p\end{array}\right\}$$

for elliptic curves on the one hand and

$$\left\{\begin{array}{c}\ell\text{-isogenies between}\\ \text{elliptic curves } E \text{ defined over } \mathbb{C}\\ \text{with } \operatorname{End} E \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}(\sqrt{-p})\\ \text{and } \mathbb{Z}[\sqrt{-p}] \subseteq \operatorname{End} E\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\mathbb{F}_p\text{-rational } \ell\text{-isogenies between}\\ \text{supersingular elliptic curves}\\ \text{defined over } \mathbb{F}_p\end{array}\right\}$$

for isogenies of prime degree $\ell \neq p$ on the other hand.

With those discoveries we were able to build $\mathbb{F}_p$-rational supersingular isogeny graphs which turned out to have a structure that is quite similar to the volcano-like one of an ordinary isogeny graph. It became apparent that they are even more assessable than an ordinary isogeny volcanoes since they have at most two levels and the only vertical isogenies can have degree two.

Due to the correspondences above we were able to establish a connection from supersingular elliptic curves defined over $\mathbb{F}_p$ to an ideal class group of an order of the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$. There an important result from Bach gave us the possibility to determine a bound on the norms of generators which leads to maximal required isogeny degrees such that the rational supersingular isogeny graph can be proven to be fully connected.

We made use of this coherence to develop a proven faster than usual algorithm for computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$. We implemented our new algorithm in `MAGMA` and observed a notable improvement in the running time of our version in contrast to the previous algorithms for computing supersingular isogenies, confirming the complexity analysis which revealed a speedup from former $\widetilde{\mathcal{O}}(p^{1/2})$ algorithms to one of complexity $\widetilde{\mathcal{O}}(p^{1/4})$.

After these main results we dealt with the investigation of possible generalizations of the insights gained from the work with elliptic curves to JACOBIANS of curves with higher genus. We discerned that the structural differences provide many difficulties which did not arise in the case concerning genus one. The computation of isogenies with given kernel works to an extend but is expectably more complex. Whereas for ordinary JACOBIANS of genus-two-curves horizontal isogenies can be a handled with a connection to an ideal class group and isogenies between two JACOBIANS with different endomorphism ring can at least partly be described, the supersingular case is more or less uncharted. We identified and illustrated the problems in this area where several points for most interesting further research can be detected.

Finally we regarded cryptographic applications of elliptic curves ans isogenies in general and of our new algorithm for computing isogenies between supersingular $\mathbb{F}_p$-rational elliptic curves in special. The general concepts appear in many fields of interest and especially in studies of the ECDLP. We presented two occurrences of isogenies between supersingular elliptic curves in cryptographic schemes – a cryptographic hash function and a probably quantum resistant cryptosystem. Although our new algorithm provides no immediate attack on an arbitrary instance of neither of those systems, in certain cases it can bring an improvement and thus at least a new perspective to consider.

FURTHER WORK. A thesis can not even begin to cover the immense number of theoretical problems which appear along the way during writing and researching. There are a few quite interesting open points in this work for further research which we briefly want to mention here.

Although the structure of the $\mathbb{F}_p$-rational supersingular isogeny graph is mostly described, some details remain to be examined like CONJECTURE 4.15 where we tried to induce a pattern by which the full supersingular isogeny graphs $G_0(\bar{\mathbb{F}}_p, \ell)$ transmute into the $\mathbb{F}_p$-rational graphs $G_0(\mathbb{F}_p, \ell)$ but succeeded only partially. Another unproven statement is presented in CONJECTURE 4.19 saying that in the graph $G_0(\mathbb{F}_p, \ell)$ the two nodes with the label 0 are always on the same level. Both conjectures are heavily supported by our example graphs but not proven yet.

Our new algorithm does not cover the computation of an isogeny between elliptic curves when at least one of them is not defined over $\mathbb{F}_p$. Hence a natural question is whether this cases can be improved with another algorithm. Already the naive approach – taking random walks until a j-invariant in $\mathbb{F}_p$ is reached on both sides and applying the new algorithm on them – shows a small improvement in the computations, but it would be interesting to see if there is a way to find a "shortcut" in the full graph to go to the "nearest" $\mathbb{F}_p$-rational node.

Further the isogeny resulting from our algorithm has probably quite large degree, even if it is relatively smooth. Nevertheless it would be good to find a way of "smoothing" the isogeny to a chain of 2-isogenies. Firstly they are the fastest ones to compute and furthermore we have seen the for example in the CHARLES-GOREN-LAUTER hash function only 2-isogenies are used, so there we are also only allowed to take isogenies which are of degree two for an attack.

An important result would be a computational feasible way to transmit the above structure from the ideal class side to the sets of elliptic curves. Since the ideal class group is well-known and for example factoring an ideal in a chain of prime ideals with small norm is manageable, many problems would get much simpler with such a connection. But so far no method in that manner is known to the author.

Finally we have seen that for JACOBIANS of higher genus curves or general abelian varieties there are still a lot of open difficult problems. Even the situation of ordinary JACOBIANS with dimension two is not as well exploited as the elliptic case. Although computing horizontal isogenies between varieties with isomorphic endomorphism rings is mostly possible due to a connection to an ideal class group, a generalization of vertical isogenies is only partly applicable. The graph structure becomes much more complicated as the endomorphism rings of isogenous JACOBIANS do not have to be contained in each other. Fixing the real multiplication helps for building parts of the graphs, but the understanding of the whole structure without fixed subring in the endomorphism rings is still incomplete.

The supersingular case causes even more intricacies, starting with the fact that not all supersingular abelian varieties of dimension $g > 1$ do have to be defined over a finite field. That is already a major drawback in contrast to the elliptic case where the minimal field of definition was always either $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$. At least a result of GROTHENDIECK tells us that every supersingular abelian variety is isogenous to a supersingular abelian variety defined over a finite field, thus they are all connected via isogenies. Although thus all supersingular JACOBIANS of genus-two-curves are isogenous, we know nothing about the degrees or field of definitions of the connecting isogenies. Hence even basic random walk approaches turn out to be complicated as we do not know an upper bound for the used degrees.

Further a simplification to JACOBIANS defined over $\mathbb{F}_p$ as in the elliptic case does not immediately provide a starting point for a better algorithm since the algebra containing orders isomorphic to the endomorphism rings is not required to be a number field and thus no connection to an ideal class is known. Establishing a lifting-and-reduction theory of such varieties which preserves some restricted endomorphism ring could provide a leverage point for this problem. There are many interesting issues for further work and projects in this area and we will watch expectantly for future development and progress in this field of research.

List of Figures

List of Tables

List of Algorithms

References

[1] Bach, Eric: Explicit bounds for primality testing and related problems, in: *Mathematics of Computation*, **55** (1990), #191, pages 355–380.

[2] Belabas, Karim; Diaz y Diaz, Francisco and Friedman, Eduardo: Small generators of the ideal class group, in: *Mathematics of Computation*, **77** (2008), #262, pages 1185–1197.

[3] Bostan, Alin; Morain, François; Salvy, Bruno and Schost, Éric: Fast algorithms for computing isogenies between elliptic curves, in: *arXiv ePrint Archive*, (2006).
URL http://arxiv.org/abs/cs/0609020v1

[4] Brillhart, John and Morton, Patrick: Class numbers of quadratic fields, Hasse invariants of elliptic curves, and the supersingular polynomial, in: *Journal of Number Theory*, **106** (2004), #1, pages 79–111.

[5] Bröker, Reinier: *Constructing Elliptic Curves of Prescribed Order*, Ph.D. thesis, Universiteit Leiden (2006).

[6] Bröker, Reinier: Constructing Supersingular Elliptic Curves, in: *Journal of Combinatorics and Number Theory*, **1** (2009), #3, pages 269–273.

[7] Bröker, Reinier; Lauter, Kristin E. and Sutherland, Andrew V.: Modular polynomials via isogeny volcanoes, in: *arXiv ePrint Archive*, (2010).
URL http://arxiv.org/abs/1001.0402

[8] BSI: TR-03111 Elliptische-Kurven-Kryptographie (ECC) (2012).
URL http://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03111/index_htm.html

[9] BSI: TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung (2014).
URL http://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03116/index_htm.html

[10] Charles, Denis X.; Goren, Eyal Z. and Lauter, Kristin E.: Cryptographic hash functions from expander graphs, in: *Journal of Cryptology*, **22** (2009), #1, pages 93–113.

[11] Childs, Andrew M.; Jao, David and Soukharev, Vladimir: Constructing elliptic curve isogenies in quantum subexponential time, in: *arXiv ePrint Archive*, (2011).
URL http://arxiv.org/abs/math/1012.4019

[12] Cohen, Henri: *A course in computational algebraic number theory*, Springer, 1996.

[13] Cohen, Henri; Frey, Gerhard; Avanzi, Robero M.; Doche, Christophe; Lange, Tanja; Nguyen, Kim and Vercauteren, Frederik: *Handbook of elliptic and hyperelliptic curve cryptography*, Discrete Mathematics and its Applications. Boca Raton, FL: Chapman & Hall/CRC, 2006.

[14] Cosset, Romain and Robert, Damien: Computing (l,l)-isogenies in polynomial time on Jacobians of genus 2 curves, in: *International Association for Cryptologic Research. Cryptology ePrint Archive*, (2011).
URL http://eprint.iacr.org/2011/143

[15] Couveignes, Jean-Marc: Computing ℓ-Isogenies Using the p-Torsion, in: *Lecture Notes in Computer Science*, **1122** (1996), pages 59–66.

[16] Cox, David A.: *Primes of the form $x^2 + ny^2$*, Wiley, 1989.

[17] Davidoff, Giuliana; Sarnak, Peter and Valette, Alain: Elementary number theory, group theory, and Ramanujan graphs, in: *Cambridge University Press*, (2003).

[18] Delfs, Christina and Galbraith, Steven D.: Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$, in: *arXiv ePrint Archive*, (2013). To appear in *Designs, Codes and Cryptography.*
URL http://arxiv.org/abs/1310.7789

[19] Deuring, Max: Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, in: *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, **14** (1941), #1, pages 197–272.

[20] Diestel, Reinhard: *Graph Theory*, Graduate Texts in Mathematics, Volume 173, Springer, 2010, 4th.

[21] ECC Brainpool: Standard Curves and Curve Generation v. 1.0 (2005).
URL http://www.ecc-brainpool.org/ecc-standard.htm

[22] Elkies, Noam D.: Elliptic and modular curves over finite fields and related computational issues, in: *Computational perspectives on number theory: proceedings of a conference in honor of AOL Atkin, September 1995, University of Illinois at Chicago*, American Mathematical Society, 1997, volume 7, pages 21–76.

[23] Enge, Andreas: Computing discrete logarithms in high-genus hyperelliptic Jacobians in provably subexponential time, in: *Mathematics of Computation*, **71** (2002), #238, pages 729–742.

[24] Fouquet, Mireille and Morain, François: Isogeny volcanoes and the SEA algorithm, in: Fieker, Claus and Kohel, David R. (Editors) *Lecture Notes in Computer Science - ANTS-V 2002*, Springer, 2002, volume 2369, pages 276–291.

[25] Frey, Gerhard: How to disguise an elliptic curve (Weil Descent) (1998). Talk at Waterloo ECC workshop, slides at `http://cacr.uwaterloo.ca/conferences/1998/ecc98/slides.html`.

[26] Frey, Gerhard and Rück, Hans-Georg: A Remark Concerning m-divisibility and the Discrete Logarithm in the Divisor Class Group of Curves, in: *Mathematics of Computation*, **62** (1994), #206, pages 865–874.

[27] Galbraith, Steven D.: Constructing isogenies between elliptic curves over finite fields, in: *LMS Journal of Computation and Mathematics*, **2** (1999), pages 118–138.

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

[29] Galbraith, Steven D.; Hess, Florian and Smart, Nigel: Extending the GHS Weil descent attack, in: *Advances in Cryptology – EUROCRYPT 2002*, Springer, 2002, pages 29–44.

[30] Galbraith, Steven D. and Smart, Nigel P.: A Cryptographic Application of Weil Descent, in: *Cryptography and Coding, 7th IMA International Conference, Cirencester, UK, December 20-22, 1999, Proceedings*, 1999, pages 191–200.

[31] Galbraith, Steven D. and Stolbunov, Anton: Improved Algorithm for the Isogeny Problem for Ordinary Elliptic Curves, in: *arXiv ePrint Archive*, (2011). URL `http://arxiv.org/abs/1105.6331`

[32] Galbraith, Steven D. and Zhao, Chang-An: Low-Storage Algorithms for the supersingular isogeny problem (2012). Personal Communication.

[33] Gaudry, Pierrick; Hess, Florian and Smart, Nigel P.: Constructive and Destructive Facets of Weil Descent on Elliptic Curves, in: *Journal of Cryptology*, **15** (2002), #1, pages 19–46.

[34] van der Geer, Gerard and Moonen, Ben: Abelian Varieties (2014). Preliminary Version of the First Chapters.
URL `http://www.math.ru.nl/~bmoonen/research.html#bookabvar`

[35] Goren, Eyal Z. and Lauter, Kristin: Genus 2 Curves with Complex Multiplication, in: *arXiv ePrint Archive*, (2010).
URL `http://arxiv.org/abs/1003.4759`

[36] Gross, Benedict H.: Heights and special values of L-series, in: *CMS Conference Proceedings*, **7** (1987), pages 115–187.

[37] Hartshorne, Robin: *Algebraic geometry*, Springer, 1977.

[38] Husemöller, Dale: *Elliptic curves*, Springer, 2004.

[39] Ibukiyama, Tomoyoshi; Katsura, Toshiyuki and Oort, Frans: Supersingular curves of genus two and class numbers, in: *Compositio Mathematica*, **57** (1986), #2, pages 127–152.

[40] Igusa, Jun-Ichi: Arithmetic variety of moduli for genus two, in: *Annals of Mathematics*, **72** (1960), #3, pages 612–649.

[41] Ionica, Sorina and Thomé, Emmanuel: Isogeny graphs with maximal real multiplication, in: *arXiv ePrint Archive*, (2014).
URL `http://arxiv.org/abs/1407.6672`

[42] Jacobson, Michael; Menezes, Alfred and Stein, Andreas: Solving Elliptic Curve Discrete Logarithm Problems Using Weil Descent, in: *Journal of the Ramanujan Mathematical Society*, **16** (2001), pages 231–260.

[43] Jao, David and De Feo, Luca: Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies, in: *PQCrypto*, 2011, pages 19–34.

[44] Jao, David and Soukharev, Vladimir: A Subexponential Algorithm for Evaluating Large Degree Isogenies, in: Hanrot, Guillaume; Morain, François

and THOMÉ, Emmanuel (Editors) *Algorithmic Number Theory, 9th International Symposium, ANTS-IX, Nancy, France, July 19-23, 2010. Proceedings*, Springer, 2010, *Lecture Notes in Computer Science*, volume 6197, pages 219–233.

[45] KOHEL, David R.: *Endomorphism rings of elliptic curves over finite fields*, Ph.D. thesis, University of California at Berkeley (1996).

[46] KOHEL, David R.: Complex multiplication and canonical lifts, in: *Algebraic Geometry and Its Applications*, (2008), pages 67–83.

[47] KOHEL, David R.; LAUTER, Kristin; PETIT, Christophe and TIGNOL, Jean-Pierre: On the quaternion ℓ-isogeny path problem, in: *arXiv ePrint Archive*, (2014).
URL `http://arxiv.org/abs/1406.0981v1`

[48] LANG, Serge: *Elliptic functions*, Springer, 1987.

[49] LANG, Serge: *Algebraic Number Theory*, Springer, 1994.

[50] LERCIER, Reynald: Computing Isogenies in $\mathbb{F}_{2^n}$, in: *Lecture Notes in Computer Science*, **1122** (1996), pages 197–212.

[51] LI, Ke-Zheng and OORT, Frans: *Moduli of supersingular abelian varieties*, Lecture notes in mathematics, Springer, 1998.

[52] LUBICZ, David and ROBERT, Damien: Computing isogenies between abelian varieties, in: *arXiv ePrint Archive*, (2010).
URL `http://arxiv.org/abs/1001.2016`

[53] LUBIN, Jonathan; SERRE, Jean-Pierre and TATE, John: Elliptic curves and formal groups (1964). Lecture notes prepared in connection with the seminars held at the Summer Institute on Algebraic Geometry, Whitney Estate, Woods Hole, Massachusetts.
URL `http://www.ma.utexas.edu/users/voloch/LST/lst.pdf`

[54] MARTINDALE, CHLOE AND STRENG, MARCO: Email and Personal Discussion (2013).

[55] MENEZES, Alfred; OKAMOTO, Tatsuaki and VANSTONE, Scott: Reducing elliptic curve logarithms to logarithms in a finite field, in: *IEEE Transactions on Information Theory*, **39** (1993), #5, pages 1639–1646.

[56] MENEZES, Alfred and QU, Minghua: Analysis of the Weil Descent Attack of Gaudry, Hess and Smart (2000).

[57] MESTRE, Jean-François: La méthode des graphes. Exemples et applications, in: *Proceedings of the international conference on class numbers and fundamental units of algebraic number fields (Katata)*, 1986, pages 217–242.

[58] MESTRE, Jean-François: Construction de courbes de genre 2 à à partir de leurs modules, in: *Effective Methods in Algebraic Geometry, Proceedings of Symposium on Castiglioncello*, Birkhäuser, 1991, *Progress in Mathematics*, volume 94, pages 313–334.

[59] MILNE, James S.: Abelian Varieties (v2.00) (2008).
URL `http://www.jmilne.org/math/`

[60] MILNE, James S.: Jacobian Varieties (2012).
URL `http://www.jmilne.org/math/`

[61] MUMFORD, David B.: *Abelian Varieties*, Oxford University Press, 1970.

[62] MUMFORD, David B.: *The Red Book of Varieties and Schemes*, *Lecture Notes in Mathematics*, volume 1358, Springer, 1999.

[63] MURTY, Ram: Ramanujan graphs, in: *Journal of the Ramanujan Math. Society*, **18** (2003), #1, pages 1–20.

[64] OORT, Frans: Lifting algebraic curves, abelian varieties and their endomorphisms to characteristic zero, in: BLOCH, Spencer J. and CLEMENS, Charles H. (Editors) *Algebraic geometry Bowdoin*, American Mathematical Society, 1985, volume 46.2, pages 165–195.

[65] OORT, Frans: Abelian varieties over finite fields (2007). Higher-dimensional varieties over finite fields – Summer school in Göttingen.

[66] OORT, Frans: Moduli of abelian varieties in mixed and in positive characteristic, in: *Handbook of moduli*, **III** (2013), pages 75–134.

[67] REINER, Irving: *Maximal Orders*, Oxford University Press, 2003.

[68] REINIER BRÖKER, David Gruenewald and LAUTER, Kristin: Explicit CM-theory for level 2-structures on abelian surfaces, in: *arXiv ePrint Archive*, (2010).
URL `http://arxiv.org/abs/0910.1848v2`

[69] Robert, Damien: Computing cyclic isogenies using real multiplication (2014). Notes of a talk given for the ANR Peace project.
URL http://www.normalesup.org/~robert/pro/publications/notes/2013-04-Peace-Paris-Cyclic-Isogenies.pdf

[70] Robert, Damien: Isogenies between abelian varieties (2014). Notes of a talk given for the Conference *Effective moduli spaces and applications to cryptography* in Rennes.
URL http://www.normalesup.org/~robert/pro/publications/notes/2014-06-Rennes-Moduli.pdf

[71] Rostovtsev, Alexander and Stolbunov, Anton: Public-key cryptosystem based on isogenies, in: *International Association for Cryptologic Research. Cryptology ePrint Archive*, (2006).
URL http://eprint.iacr.org/2006/145

[72] Rück, Hans-Georg: A note on elliptic curves over finite fields, in: *Mathematics of Computation*, **49** (1987), #179, pages 301–304.

[73] Schoof, René: Counting points on elliptic curves over finite fields, in: *Journal de Théorie des Nombres de Bordeaux*, **7** (1995), #1, pages 219–254.

[74] Silverman, Joseph H.: *Advanced topics in the arithmetic of elliptic curves*, Springer, 1994.

[75] Silverman, Joseph H.: *The arithmetic of elliptic curves*, Springer, 2009.

[76] Smart, Nigel P.: The Discrete Logarithm Problem On Elliptic Curves Of Trace One, in: *Journal of Cryptology*, **12** (1999), pages 193–196.

[77] Smart, Nigel P.: How Secure Are Elliptic Curves over Composite Extension Fields?, in: Pfitzmann, Birgit (Editor) *EUROCRYPT*, Springer, 2001, *Lecture Notes in Computer Science*, volume 2045, pages 30–39.

[78] Smith, Benjamin: *Explicit endomorphisms and correspondences*, Ph.D. thesis, University of Sydney (2005).

[79] Smith, Benjamin: Isogenies and the Discrete Logarithm Problem on Jacobians of Genus 3 Hyperelliptic Curves, in: *International Association for Cryptologic Research. Cryptology ePrint Archive*, (2007).
URL http://eprint.iacr.org/2007/428

[80] Smith, Benjamin: Computing low-degree isogenies in genus 2 with the Dolgachev-Lehavi method, in: *Contemporary Mathematics*, **574** (2012), pages 159–170.

[81] Stark, Harold M.: Class-Numbers of Complex Quadratic Fields, in: Kuijk, Willem (Editor) *Modular Functions of One Variable I*, Springer Berlin Heidelberg, 1973, *Lecture Notes in Mathematics*, volume 320, pages 153–174.

[82] Stichtenoth, Henning: *Algebraic function fields and codes*, Springer, 2003.

[83] Stolbunov, Anton: Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves, in: *Advances in Mathematics of Communications*, **4** (2010), #2, pages 215–235.

[84] Sutherland, Andrew V.: Identifying supersingular elliptic curves, in: *arXiv ePrint Archive*, (2011).
URL `http://arxiv.org/abs/1107.1140`

[85] Takashima, Katsuyuki and Yoshida, Reo: An Algorithm for Computing a Sequence of Richelot Isogenies, in: *Bulletin of the Korean Mathematical Society*, **46** (2009), #4, pages 789–802.

[86] Tate, John T.: Endomorphisms of abelian varieties over finite fields, in: *Inventiones mathematicae*, **2** (1966), #2, pages 134–144.

[87] Tate, John T.: Global Class Field Theory, in: Cassels, John W. S. and Frölich, Albrecht (Editors) *Algebraic Number Theory*, Academic Press, 1967, pages 162–203.

[88] Teske, Edlyn: The Pohlig-Hellman Method Generalized for Group Structure Computation, in: *Journal of Symbolic Computation*, **27** (1999), #6, pages 521–534.

[89] Thériault, Nicolas: Index Calculus Attack for Hyperelliptic Curves of Small Genus, in: *Advances in Cryptology - ASIACRYPT 2003, 9th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, November 30 - December 4, 2003, Proceedings*, Springer, 2003, *Lecture Notes in Computer Science*, volume 2894, pages 75–92.

[90] Vélu, Jaques: Isogénies entre courbes elliptiques, in: *Comptes Rendus de l'Académie des Sciences Paris, Série 1*, **273** (1971), pages 238–241.

[91] WASHINGTON, Lawrence C.: *Elliptic curves: number theory and cryptography*, Chapman & Hall, 2008.

[92] WATERHOUSE, William C.: Abelian varieties over finite fields, in: *Annales Scientifiques de l'Ecole Normale Supérieure*, **2** (1969), #4, pages 521–560.

[93] WESOLOWSKI, Benjamin: *Walking on Isogeny Graphs of Genus 2 Hyperelliptic Curves*, Master's thesis, École Polytechnique Fédérale de Lausanne (2014).

[94] XING, Chaoping: On Supersingular Abelian Varieties of Dimension Two over Finite Fields, in: *Finite Fields and Their Applications*, **2** (1996), #4, pages 407–421.

[95] ZIMMERT, Rainer: Ideale kleiner Norm in Idealklassen und eine Regulatorabschätzung, in: *Inventiones mathematicae*, **62** (1981), pages 367–380.

A MAGMA Program Codes

We implemented the described methods in MAGMA so that we were able to compute examples and make comparisons of the actual running time of the algorithms. Note that these implementations are not optimized but work sufficiently fast for our input sizes. Also, to keep it simple, we provide no error catching lines to avoid wrong input or similar issues.

The first codes here (Algorithms A.1-A.7) concern the methods we presented already as pseudocodes in Section 4.1.2 for navigating in an ordinary isogeny volcano.

Algorithm A.1 IsOnFloor(j, q, l)

```
F := GF(q);
R<t> := PolynomialRing(F);
S<x, y> := PolynomialRing(F, 2);
Phi := S!ClassicalModularPolynomial(l);
m := 0;
M := Roots(R!UnivariatePolynomial(Evaluate(Phi, x, j)));
// if there are any roots, count their multiplicities
if not #M eq 0 then
    for i in {1..#M} do
        m +:= M[i, 2];
    end for
end if
return m le 2;
```

Algorithm A.2 LengthOfRandomPathToFloor(j0, j1, q, l)

```
if IsOnFloor(j0, q, l) then
    return 0;
end if
F := GF(q);
R<t> := PolynomialRing(F);
S<x, y> := PolynomialRing(F, 2);
Phi := S!ClassicalModularPolynomial(l);
n := 1;
while not IsOnFloor(j1, q, l) do
    jtmp := j1;
    // factor out root to ensure that path does not go back
    j1 := Random(Roots(R!(R!UnivariatePolynomial(
                        Evaluate(Phi, x, j1))/(t-F!j0));
    j0 := jtmp;
    n +:= 1;
end while
return n;
```

Algorithm A.3 DistanceToFloor(j, q, l)

```
F := GF(q);
R<t> := PolynomialRing(F);
S<x, y> := PolynomialRing(F, 2);
Phi := S!ClassicalModularPolynomial(l);
// choose three different isogenies starting at j
j1 := Random(Roots(R!UnivariatePolynomial(
            Evaluate(Phi, x, j))))[1];
j2 := Random(Roots(R!(R!UnivariatePolynomial(
            Evaluate(Phi, x, j))/(t-F!j1))))[1];
j3 := Random(Roots(R!(R!UnivariatePolynomial(
            Evaluate(Phi, x, j))/((t-F!j1)*(t-F!j2)))))[1];
n1 := LengthOfPath(j, j1, q, l);
n2 := LengthOfPath(j, j2, q, l);
n3 := LengthOfPath(j, j3, q, l);
return Minimum([n1, n2, n3]);
```

Algorithm A.4 IsDown(j0, j1, q, l)

```
return LengthOfPath(j0, j1, q, l)
       eq DistanceToFloor(j0, q, l);
```

Algorithm A.5 IsUp(j0, j1, q, l)

```
return IsDown(j1, j0, q, l);
```

Algorithm A.6 PathToSurface(j, q, l, X)

```
Phi := S!ClassicalModularPolynomial(l);
repeat
  isonsurface := true;
  M := Roots(R!UnivariatePolynomial(Evaluate(Phi, x, j)));
  for m in M do
    if IsUp(j, m, q, l) then
      Append(~X, m);
      j := m;
      isonsurface := false;
    end if
  end for
until isonsurface;
return j, X;
```

Algorithm A.7 `OrdinaryIsogeny(j0, j1, q)`

```
F := GF(q);
R<t> := PolynomialRing(F);
S<x,y> := PolynomialRing(F, 2);
E0 := EllipticCurveFromjInvariant(j0);
r0 := #RationalPoints(E0);
E1 := EllipticCurveFromjInvariant(j1);
if r0 ne #RationalPoints(E1) then
    return -1;
end if
t1 := q+1-r0;
d := t1^2-4*q;
dk := Discriminant(QuadraticField(d));
O := sub<OK| 1/2*(-t+Integers()!Sqrt(d/dk)*x)>;
c := Conductor(O);
C := Factorization(c);
// FIRST STEP: reaching the same level
X := [F!j0];
Y := [F!j1];
for g in C do
    l := g[1];
    j0, X := PathToSurface(j0, q, l, X);
    j1, Y := PathToSurface(j1, q, l, Y);
end for
// SECOND STEP: random walk on top level
B := Minimum([B, 60, Floor(6*Log(d)^2)])[1];
// list of possible isogeny degrees up to the bound B
L := Sort(SetToSequence({2} join
                          {l:  l in PrimesInInterval(3, B)
                          | LegendreSymbol(d, l) ne -1}));
l := Random(L);
Phi := S!ClassicalModularPolynomial(l);
// compute a first random neighbour of j0, store it in X
M := Roots(R!UnivariatePolynomial(Evaluate(Phi, x, j0)));
j0tmp := j0;
j0 := F!M[Random([1..#M])][1];
Append(~X, j0);
// compute a first random neighbour of j1, store it in Y
M := Roots(R!UnivariatePolynomial(Evaluate(Phi, x, j1)));
j1tmp := j1;
j1 := F!M[Random([1..#M])][1];
Append(~Y, j1);
```

```
disjoint := not (j0 in Y or j1 in X);
while disjoint do
   // choose a new isogeny degree different from the last
   l := Random(Exclude(L, l));
   Phi := S!ClassicalModularPolynomial(l);
   // compute a chain of l-isogenies which is stored in X
   if disjoint then
      M := Roots(R!UnivariatePolynomial(
                  Evaluate(Phi, x, j0)));
      j0 := F!M[Random([1..#M])][1];
      Append(~X, j0);
      // stop if the other chain Y is reached
      // cut Y to the right length
      if j0 in Y then
         Y := Y[1..Index(Y, j0)];
         disjoint := false;
      end if;
   end if;
   // compute a chain of l-isogenies which is stored in Y
   if disjoint then
      M := Roots(R!UnivariatePolynomial(
                  Evaluate(Phi, x, j1)));
      j1 := F!M[Random([1..#M])][1];
      Append(~Y, j1);
      // stop if the other chain X is reached
      // cut X to the right length
      if j1 in X then
         X := X[1..Index(X, j1)];
         disjoint := false;
      end if;
   end if;
end while;
return X cat Reverse(Y);
```

For our computational results we compute paths between random j-invariants to test how fast the respective algorithms are. For that we need a method to construct a set of supersingular j-invariants of $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$ from that we can draw the start and end points of our random walks. We use the mentioned CM-method from Bröker [5] in the following way to construct a set of cardinality m which contains supersingular j-invariants lying in $\mathbb{F}_{p^r}$.

Algorithm A.8 `GetjInvariants(p, m, r)`

```
F := GF(p^r);
R<t> := PolynomialRing(F);
if r eq 1 then
   s := NumberOfRationaljInvariants(p);
else
   s := NumberOfSupersingularCurves(p);
end if;
if m eq 0 then
   m := s;
else
   m := Minimum(m, s);
end if;
q := 2;
A := { };
repeat
   repeat
      q := NextPrime(q);
   until (q mod 4 eq 3 and LegendreSymbol(-q, p) eq -1);
   f := R!HilbertClassPolynomial(-q);
   S := Roots(f);
   for j in 1..#S do
      A := A join S[j,1];
   end for;
until #A ge m;
return Sort(SetToSequence(A)[1..m]);
```

The classical bi-directional search via random walks on the full supersingular isogeny graph is described in the next code and used for the comparisons against our new algorithm. The computational results arising from that are displayed afterwards in Appendix B.

Algorithm A.9 `SupersingularIsogeny(j0, j1, p)`

```
F := GF(p^2);
R<t> := PolynomialRing(F);
S<x,y> := PolynomialRing(F, 2);
Phi := S!ClassicalModularPolynomial(2);
X := [F!j0];
Y := [F!j1];
// compute a first random neighbor of j0, store it in X
M := Roots(R!UnivariatePolynomial(Evaluate(Phi, x, j0)));
j0tmp := j0;
j0 := F!M[Random([1..#M])][1];
Append(~X, j0);
// compute a first random neighbor of j1, store it in Y
M := Roots(R!UnivariatePolynomial(Evaluate(Phi, x, j1)));
j1tmp := j1;
j1 := F!M[Random([1..#M])][1];
Append(~Y, j1);
disjoint := not (j0 in Y or j1 in X)
while disjoint do
   if disjoint then
      M := Roots(R!(R!UnivariatePolynomial(
                     Evaluate(Phi, x, j0)) / (t-j0tmp)));
      j0tmp := j0;
      j0 := F!M[Random([1..#M])][1];
      Append(~X, j0);
      if j0 in Y then
         Y := Y[1..Index(Y, j0)];
         disjoint := false;
      end if
   end if
   if disjoint then
      M := Roots(R!(R!UnivariatePolynomial(
                     Evaluate(Phi, x, j1)) / (t-j1tmp)));
      j1tmp := j1;
      j1 := F!M[Random([1..#M])][1];
      Append(~Y, j1);
      if j1 in X then
         X := X[1..Index(X, j1)];
         disjoint := false;
      end if
   end if
end while
return #X-1 + #Y-1;
```

The code for our new algorithm working in the $\mathbb{F}_p$-rational isogeny graph $G_0(\mathbb{F}_p, \mathcal{L})$ for the set $\mathcal{L} = \{\text{primes } \ell \leq B \mid \left(\frac{-p}{\ell}\right) = 1\}$ where B is a chosen upper bound for the isogeny degrees is presented on the next pages. The input C is used to avoid endless loops when the graph is not connected for the appropriate set $\mathcal{L}$.

Algorithm A.10 `SupersingularRationalIsogeny(j0, j1, p, B, C)`

```
F := GF(p);
R<t> := PolynomialRing(F);
S<x,y> := PolynomialRing(F, 2);
B := Minimum(B, 60);
L := Sort(SetToSequence({2} join {l:  l in
          PrimesInInterval(3, Minimum(B,
          Floor(6*Log(4*p)^2)))
          | LegendreSymbol(-p, l) eq 1}));
// store the starting j-invariants
X0 := [F!j0];
X1 := [F!j1];
// store the degrees of used isogenies
D := [];
l := Random(L);
disjoint := j0 ne j1;
i := 0;
while disjoint do
   Phi := S!ClassicalModularPolynomial(l);
   Append(~D, l);
   // compute a chain of l-isogenous elliptic curves
   // starting at j0 which is stored in X0
   M := Roots(R!UnivariatePolynomial(
               Evaluate(Phi, x, j0)));
   j0 := F!M[Random([1..#M])][1];
   Append(~X0, j0);
   // stop if the other chain X1 is reached
   // cut X1 to the right length
   if j0 in X1 then
      c := Index(X1, j0) - 1;
      X1 := X1[1..c];
      D := D cat Reverse(D[1..c]);
      disjoint := false;
      break;
   end if;
```

```
    // compute a chain of l-isogenous elliptic curves
    // starting at j1 which is stored in X1
    M := Roots(R!UnivariatePolynomial(
                 Evaluate(Phi, x, j1)));
    j1 := F!M[Random([1..#M])][1];
    Append(~X1, j1);
    // stop if the other chain X1 is reached
    // cut X1 to the right length
    if j1 in X0 then
       c := Index(X0, j1) - 1;
       X0 := X0[1..c];
       D := D[1..c] cat Reverse(D);
       disjoint := false;
       break;
    end if;
    // choose a new isogeny degree
    // different from the last to avoid back-tracking
    // (mostly)
    if #L gt 1 then
       l := Random(Exclude(L, l));
    end if;
    // avoid going into an endless loop
    i +:=1;
    if i gt C then
       break;
    end if;
end while;
if not disjoint then
    X := X0 cat Reverse(X1);
else
    X := [];
    D := [];
end if;
return X, D, not disjoint;
```

Finally we examined the situation when we want to compute paths between j-invariants from $\mathbb{F}_{p^2}$. For that we need a procedure to reach a $\mathbb{F}_p$-rational node first and after that we combine the algorithms to attain a complete path between the original nodes.

Algorithm A.11 PathToRational(j, p)

```
F := GF(p^2);
R<t> := PolynomialRing(F);
S<x,y> := PolynomialRing(F, 2);
Phi := S!ClassicalModularPolynomial(2);
// store the starting j-invariant
X := [F!j];
if j notin GF(p) then
   compute a first random neighbor of j
   M := Roots(R!UnivariatePolynomial(
              Evaluate(Phi, x, j)));
   jtmp := j;
   Append ~X, j;
   while j notin GF(p) do
      // compute neighbor of the current j-invariant
      // which is not the previousone
      until a j-invariant in Fp is reached
      M := Roots(R!(R!UnivariatePolynomial(
                 Evaluate(Phi, x, j)) /
                 R!UnivariatePolynomial(x-jtmp)));
      jtmp := j;
      j := F!M[Random([1..#M])][1];
      Append(~X, j);
   end while
end if
return X
```

Algorithm A.12 SupersingularIsogeny(j0, j1, p, B)

```
X0 := PathToRational(j0, p);
X1 := PathToRational(j1, p);
X, D, success := SupersinuglarRationalIsogeny(
                 X0[#X0], X1[#X1], p, B);
return X0[1..#X0-1] cat X cat X1[1..#X1-1],
      [[#X0-1], D, [#X1-1]], success;
```

B Computational Results

We made some calculations using the above described `MAGMA` functions. For each bitlength we chose 20 random primes p, computed a set of supersingular j-invariants in $\mathbb{F}_p$ and draw 100 pairs out of this set. For each of those pairs we computed a chain of isogenies in the full supersingular graph $G_0(\bar{\mathbb{F}}_p, 2)$ with a classical random walk of 2-isogenies as well as with our new method in the $\mathbb{F}_p$-rational graph $G_0(\mathbb{F}_p, \mathcal{L})$ where we took $\mathcal{L}$ to be the set of non-inert primes ℓ less than 20. We counted the number of steps in those paths and measured the CPU time needed for computing them. The averages over all paths between j-invariants belonging to a b-bit prime are displayed in Table 3.

	path length (steps)		CPU time (seconds)	
p	new	old	new	old
16-bit	20	145	0.015	0.081
20-bit	39	587	0.028	0.391
24-bit	81	2284	0.065	1.812
28-bit	222	9506	0.242	21.275
32-bit	385	35878	0.677	270.056

Table 3: Comparing the Algorithms for j-Invariants from $\mathbb{F}_p$

Our algorithm improves the complexity of the computation of a path notably when the start and ending nodes represent j-invariants from $\mathbb{F}_p$. When we choose arbitrary elliptic curves and thus j-invariants from $\mathbb{F}_{p^2}$, we have to perform random walks on both sides until nodes in $\mathbb{F}_p$ are reached and add a chain computed with our new algorithm to connect them. We want to compare this procedure with the complete classical random walks. For that we repeated the above computations with the same parameters but with j-invariants from $\mathbb{F}_{p^2}$. The results can be seen in Table 4.

	path length (steps)		CPU time (seconds)	
p	new	old	new	old
16-bit	99	135	0.045	0.076
20-bit	331	561	0.177	0.382
24-bit	1313	2106	0.791	1.718
28-bit	4913	8638	7.108	19.193
32-bit	19772	36760	59.183	320.232

Table 4: Comparing the Algorithms for j-Invariants from $\mathbb{F}_{p^2}$

Note that this is only the algorithm of finding a path in the isogeny graphs and the resulting isogeny has not been computed yet. Since in the classical algorithm only 2-isogenies are used and we need ℓ-isogenies of degree less or equal to B, this step will probably take longer even though the chain is shorter and thus less isogenies have to be computed.

The choice of primes less than 20 in the set $\mathcal{L}$ for above calculations was indiscriminate and made since for that bound most of the graphs were connected. For higher bitlength we sometimes expect errors and have to repeat a computation or increase the set $\mathcal{L}$. The choice of the upper bound B for this set has an influence on the algorithm as seen in TABLE 5 for the case of 20-bit primes where the behavior can be seen nicely. We used the same number of paths as in the previous algorithms.

	B	successrate	path length (steps)	CPU time (seconds)
20-bit	3	37.2 %	374	0.075
	5	68.2 %	249	0.053
	7	81.2 %	185	0.045
	11	90.9 %	102	0.034
	13	96.8 %	78	0.033
	17	100.0 %	52	0.028

TABLE 5: The New Algorithm for Different Bounds on the Isogeny Degrees

We can see that with increasing isogeny degrees the paths get shorter and faster to compute and the probability that the graph is connected gets higher, too. But we keep in mind that for computing an isogeny along the path we prefer small degrees in every step, thus we should not choose the bound B too big.

C Example Graphs

We have seen that the structure of the $\mathbb{F}_p$-rational supersingular isogeny graph depends on the form of $p \pmod 8$. The only vertical isogenies have degree two, for other isogeny degrees we always have big horizontal circles on the levels. In this part we will print the graphs $G_0(\mathbb{F}_p, 2)$ for primes p between 5 and 101 to get a good overview about the occurring structures.

In the case $p \equiv 1 \pmod 4$, there is only one level and all isogenies are horizontal. There are always pairs of nodes connected with dual 2-isogenies. When we have $p \equiv 7 \pmod 8$, both levels have the same number of nodes and are connected one-to-one via 2-isogenies. Additionally there are two horizontal 2-isogenies at every node on the surface. For $p \equiv 3 \pmod 8$ the floor is thrice as big as the top level and every surface node has three neighbors on the floor. This behavior can be seen distinctly in the next table for the examples of the first three primes p we are regarding.

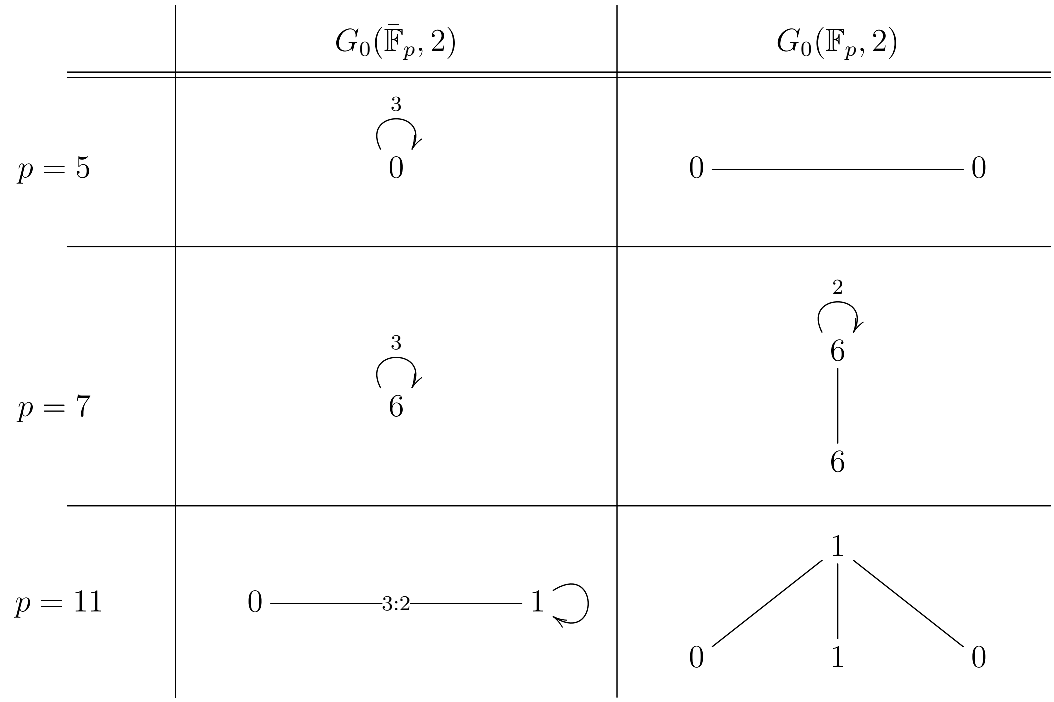
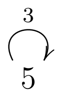
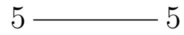
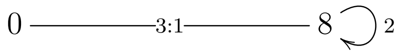
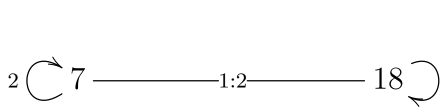
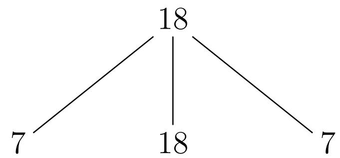
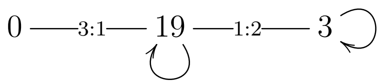
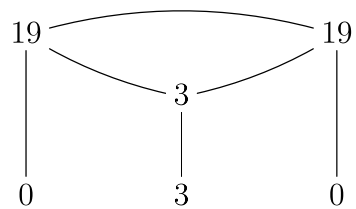
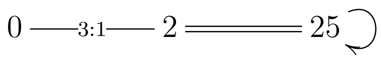
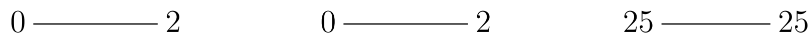
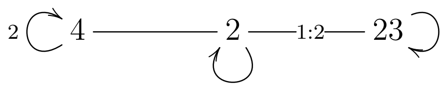
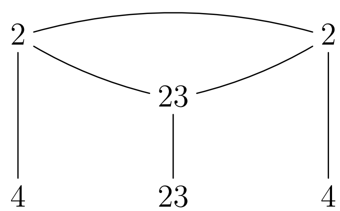
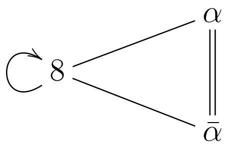
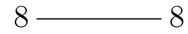
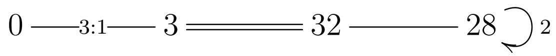
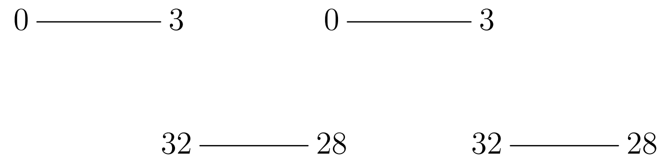
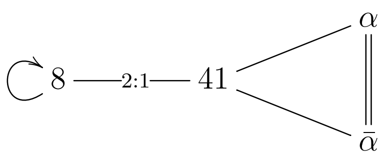
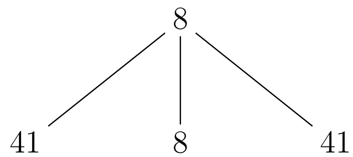
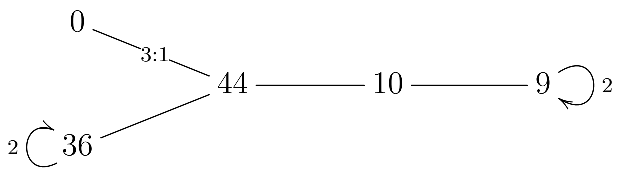
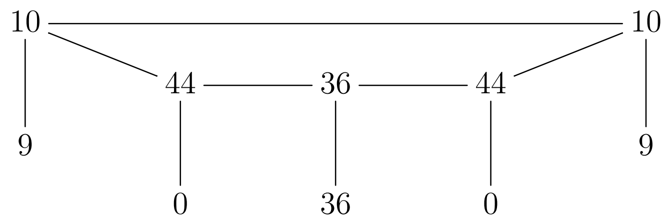
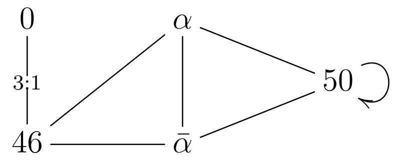
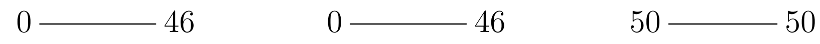
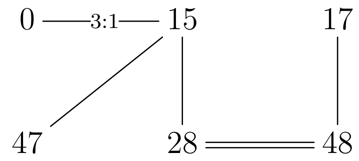
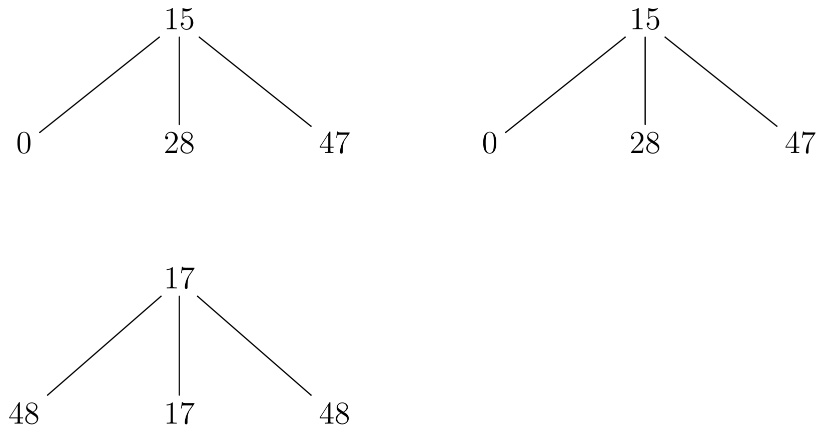
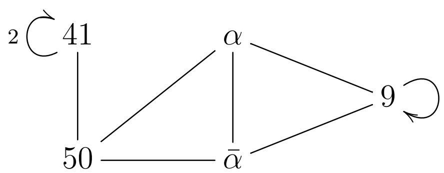
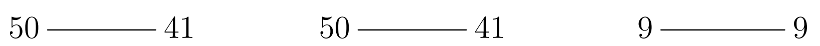


Table 6: Supersingular 2-isogeny graphs for $p \in \{5, 7, 11\}$

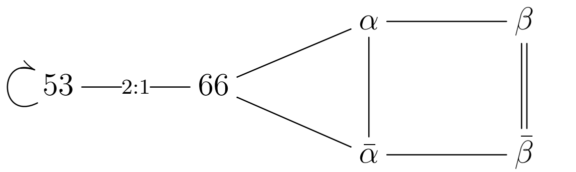
On the next pages are further examples. α, β and γ always denote j-invariants from $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$. Note that there are examples where neither the set of $\mathbb{F}_p$-rational j-invariants nor its complement in $G_0(\bar{\mathbb{F}}_p, 2)$ are connected.

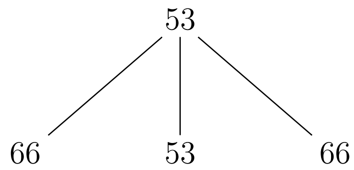
	$G_0(\bar{\mathbb{F}}_p, 2)$	$G_0(\mathbb{F}_p, 2)$
$p = 13$		
$p = 17$		
$p = 19$		
$p = 23$		
$p = 29$		
$p = 31$		

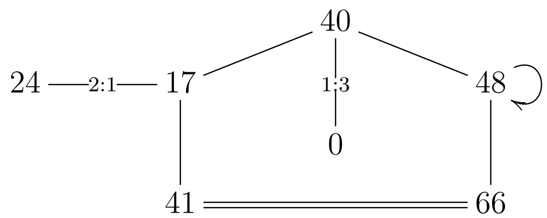
	$G_0(\bar{\mathbb{F}}_p, 2)$	$G_0(\mathbb{F}_p, 2)$
$p = 37$		
$p = 41$		
$p = 43$		
$p = 47$		

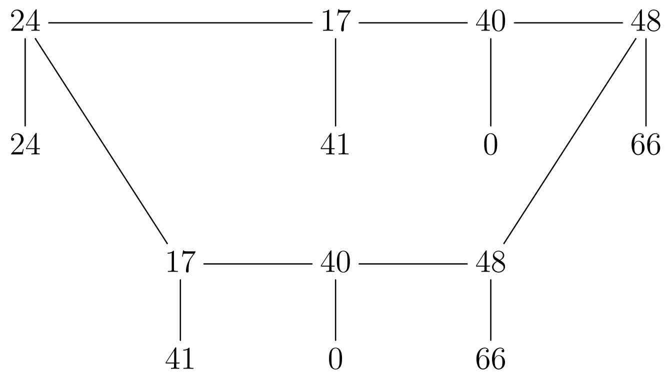
	$G_0(\bar{\mathbb{F}}_p, 2)$	$G_0(\mathbb{F}_p, 2)$
$p = 53$		
$p = 59$		
$p = 61$		

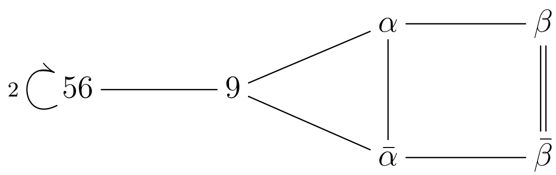
	$G_0(\bar{\mathbb{F}}_p, 2)$	$G_0(\mathbb{F}_p, 2)$
$p = 67$		
$p = 71$		
$p = 73$		

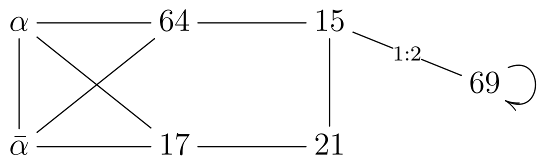
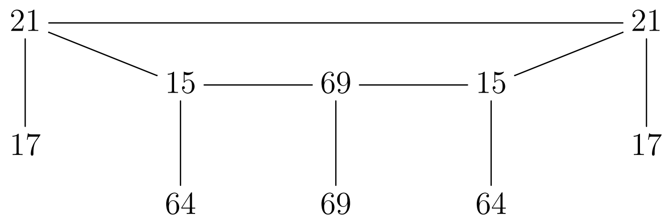
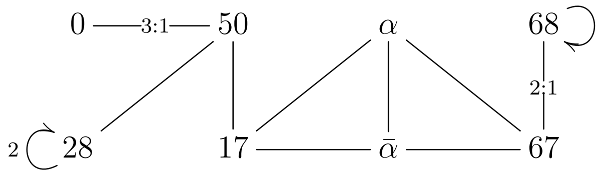
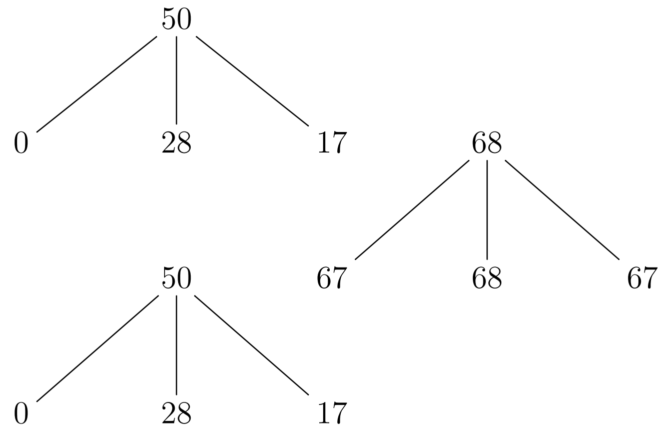
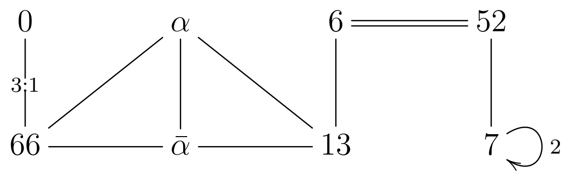
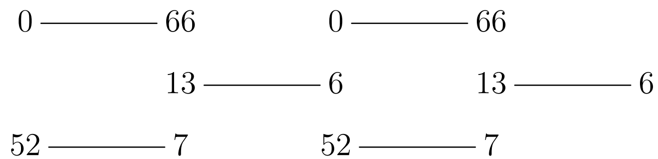


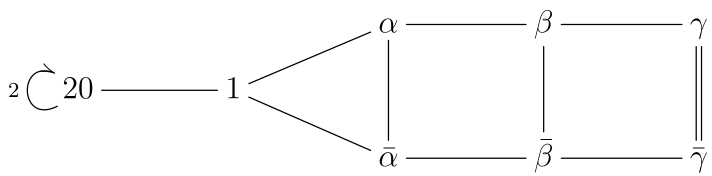
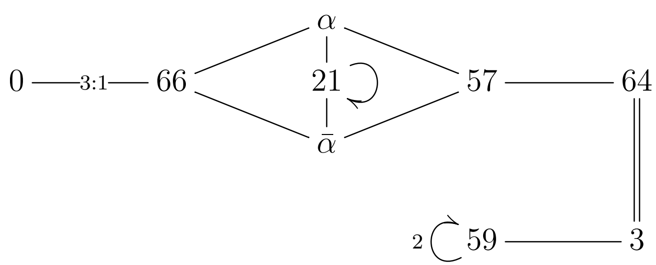
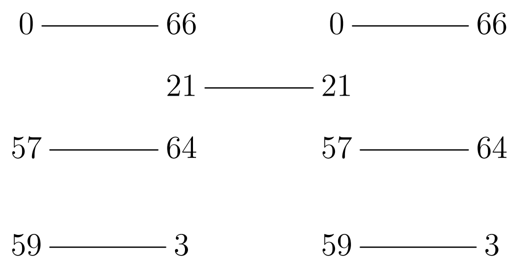








	$G_0(\bar{\mathbb{F}}_p, 2)$	$G_0(\mathbb{F}_p, 2)$
$p = 79$		
$p = 83$		
$p = 89$		

	$G_0(\bar{\mathbb{F}}_p, 2)$	$G_0(\mathbb{F}_p, 2)$
$p = 97$		
$p = 101$		

Those graphs were constructed with short straightforward `MAGMA` routines which provide adjacency matrices of the appropriate graphs and whose source codes can be found below. The methods work quite fast for moderately sized primes p but later the factorization of the *supersingular polynomial* – a monic polynomial over $\mathbb{F}_p$ implemented in `Magma` whose roots are the supersingular j-invariants – makes it slower. However, since the graphs for large primes p are much too big to draw in a comprehensible way, this is more than sufficient for our purposes.

To extract a comprehensive, neatly arranged picture of a graph from its adjacency matrix proves tedious. We drew three medium sized examples for full supersingular 2-isogeny graphs as well as for their rational correspondences which can be found after the source codes. The j-invariants which are not in $\mathbb{F}_p$ are denoted with greek letters for a better overall view. It is clear to see how the rational graphs arise from the full ones, supporting Conjecture 4.15.

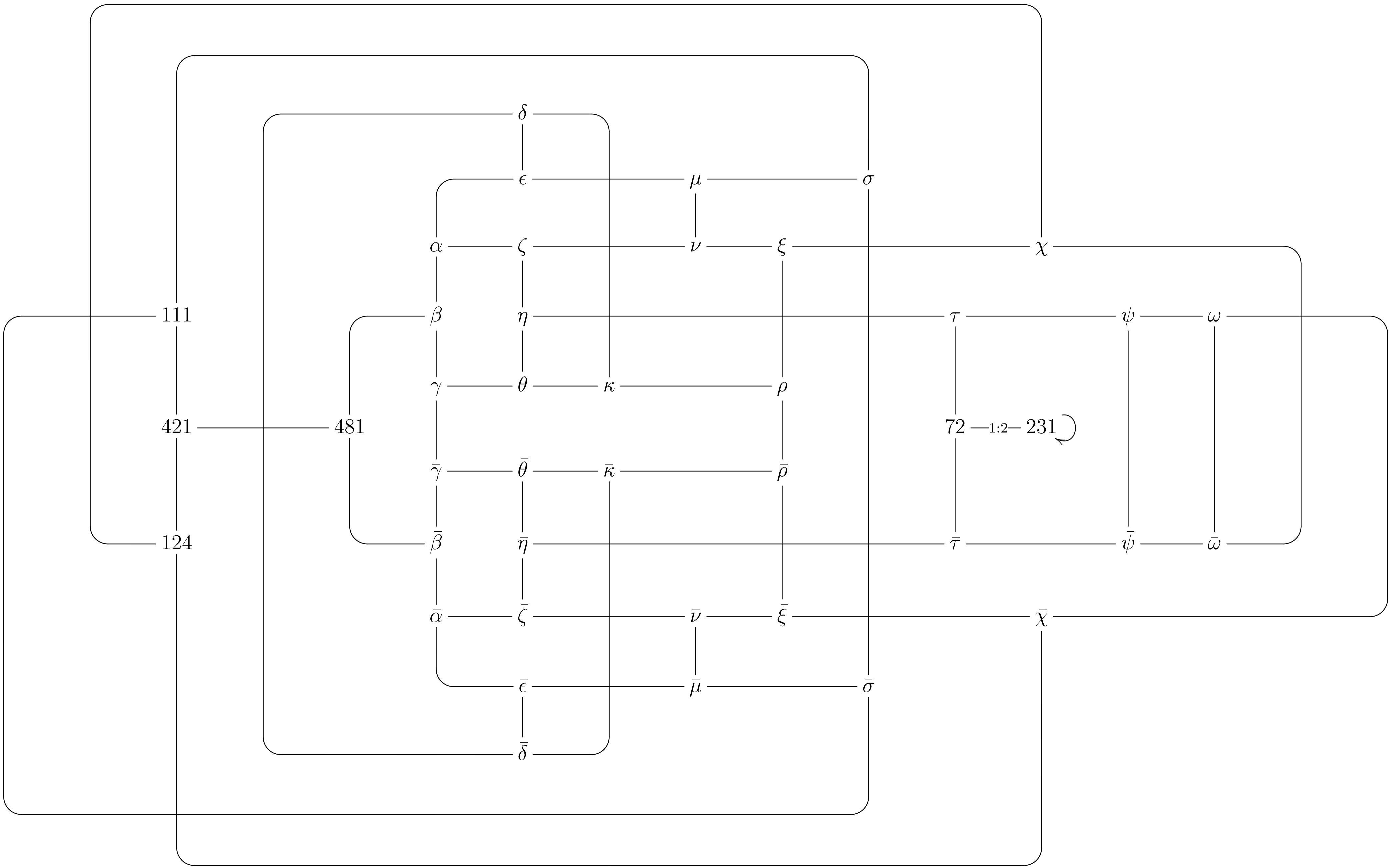
Input: `coprime primes p and l`
Output: `Adjacency matrix of full supersingular l-isogeny graph in characteristic p`

```
F := GF(p);
R<x> := PolynomialRing(GF(p^2));
S<x,y> := PolynomialRing(GF(p^2), 2);
Psi := S!ClassicalModularPolynomial(2);
T := Roots(SupersingularPolynomial(p), GF(p^2));
A := [];
for a in {1..#T} do
    j := GF(p^2)![T[a,1]];
    if j in GF(p) then
        A := [j] cat A;
    else
        A := A cat [j];
    end if
end for
N := ZeroMatrix(Integers(), #A, #A);
for i in {1..#A} do
    M := Roots(R!UnivariatePolynomial(
                Evaluate(Psi, x, A[i])));
    for  m in {1..#M} do
        k := Index(A, M[m,1]);
        N[i,k] := N[i,k] + M[m,2];
    end for
end for
return A, N;
```

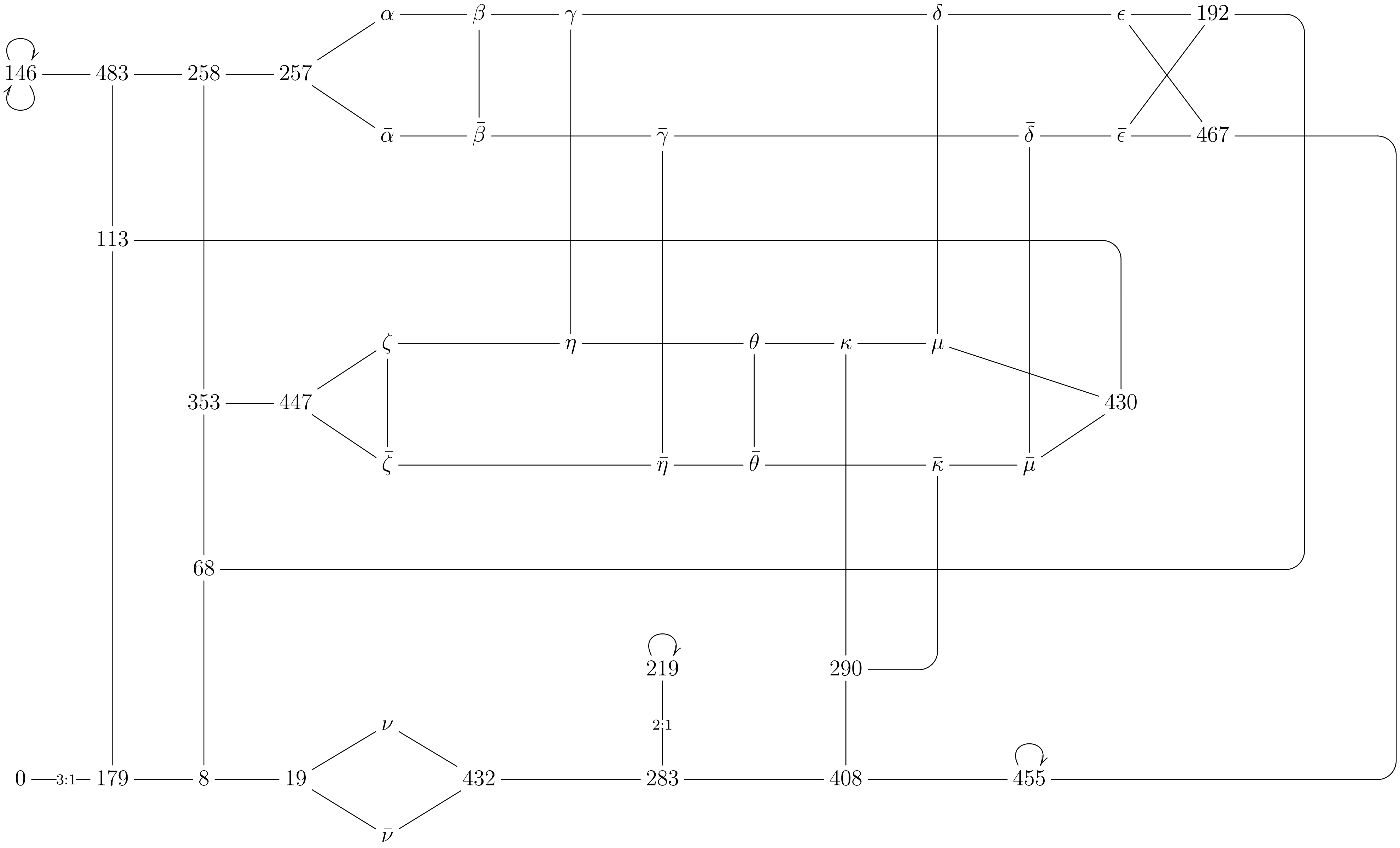
Input: coprime primes p and l
Output: Adjacency matrix of rational supersingular l-isogeny graph in characteristic p

```
F := GF(p);
T := Roots(SupersingularPolynomial(p), F);
Curves := [];
A := [];
for a in {1..#T} do
   E := EllipticCurveFromjInvariant(F!T[a,1]);
   Curves := Curves cat [E, QuadraticTwist(E)];
   A := A cat [jInvariant(E), jInvariant(E)];
end for
N := ZeroMatrix(Integers(), #A, #A);
for i in {1..#A} do
   E := Curves[i];
   M := Factorization(DivisionPolynomial(E, l));
   for m in {1..#M} do
      try
         EE := IsogenyFromKernel(E, Factorization
                (DivisionPolynomial(E, l))[m,1]);
         for  k in {1..#A} do
            if IsIsomorphic(EE, A[k]) then
               N[i,k] := N[i,k] + 1;
            end if
         end for
      catch e
         e‘Object;
      end try
   end for
end for
return A, N;
```

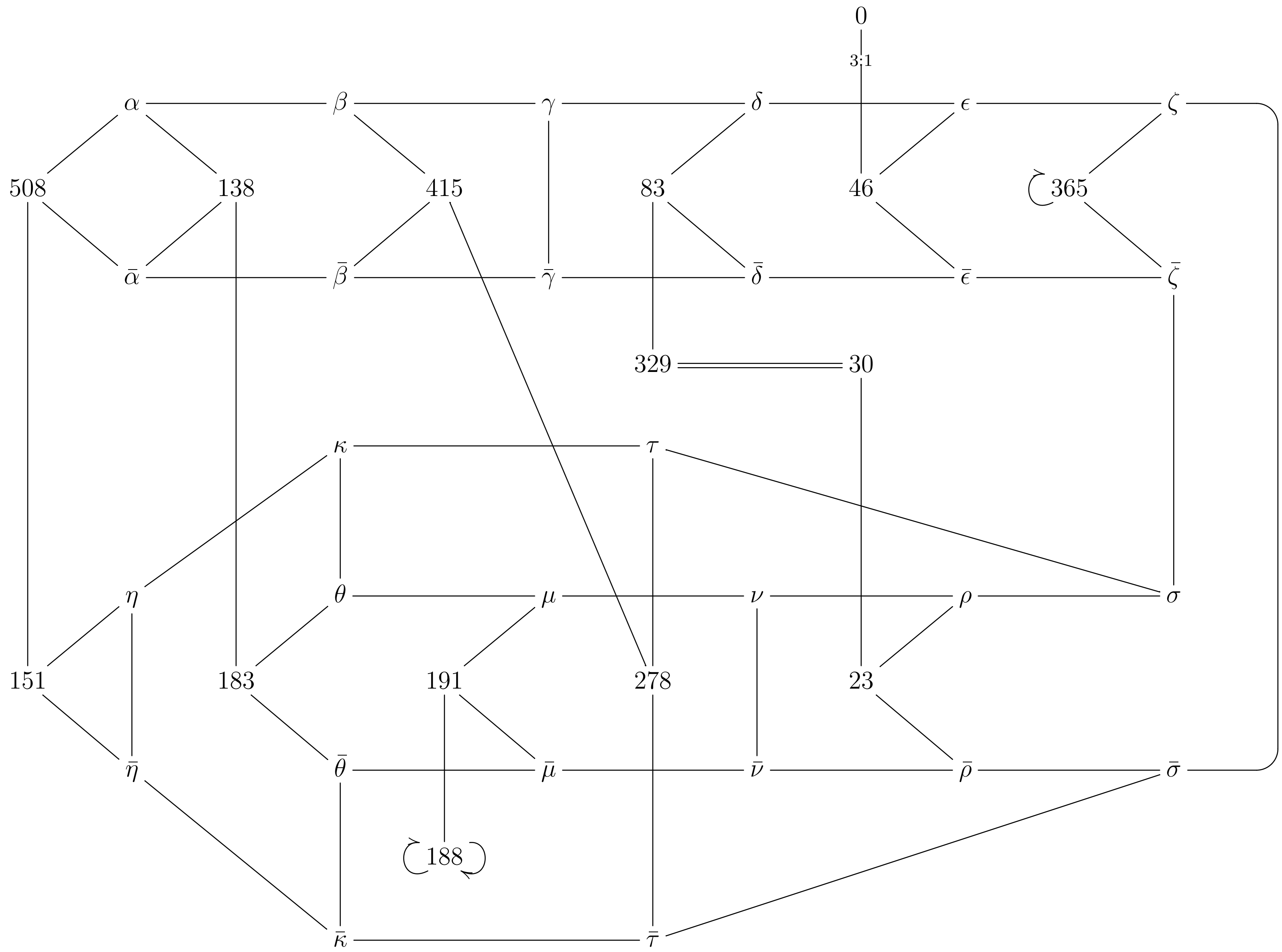
$p = 499$ $G_0(\bar{\mathbb{F}}_p, 2)$



$p = 503$ $G_0(\bar{\mathbb{F}}_p, 2)$



$p = 509$ $\qquad$ $G_0(\bar{\mathbb{F}}_p, 2)$



	$G_0(\bar{\mathbb{F}}_p, 2)$

$p = 499$

$$\begin{tikzcd}[column sep=small]
 & 421 \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & & & 421 \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & & & 231 \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
111 & 124 & 481 & 111 & 124 & 481 & 72 & 72 & 231
\end{tikzcd}$$

$p = 503$

$$\begin{tikzcd}
179 \arrow[r, dash] \arrow[d, dash] \arrow[rrrrrr, dash, bend left] & 113 \arrow[r, dash] \arrow[d, dash] & 483 \arrow[r, dash] \arrow[d, dash] & 258 \arrow[r, dash] \arrow[d, dash] & 353 \arrow[r, dash] \arrow[d, dash] & 68 \arrow[r, dash] \arrow[d, dash] & 8 \arrow[d, dash] \\
0 & 430 & 146 & 257 & 447 & 192 & 19
\end{tikzcd}$$

$$\begin{tikzcd}
179 \arrow[r, dash] \arrow[d, dash] \arrow[rrrrrr, dash, bend left] & 113 \arrow[r, dash] \arrow[d, dash] & 483 \arrow[r, dash] \arrow[d, dash] & 258 \arrow[r, dash] \arrow[d, dash] & 353 \arrow[r, dash] \arrow[d, dash] & 68 \arrow[r, dash] \arrow[d, dash] & 8 \arrow[d, dash] \\
0 & 430 & 146 & 257 & 447 & 192 & 19
\end{tikzcd}$$

$$\begin{tikzcd}
455 \arrow[r, dash] \arrow[d, dash] \arrow[rrrrrr, dash, bend left] & 408 \arrow[r, dash] \arrow[d, dash] & 283 \arrow[r, dash] \arrow[d, dash] & 219 \arrow[r, dash] \arrow[d, dash] & 283 \arrow[r, dash] \arrow[d, dash] & 408 \arrow[r, dash] \arrow[d, dash] & 455 \arrow[d, dash] \\
467 & 290 & 432 & 219 & 432 & 290 & 467
\end{tikzcd}$$

$p = 509$

$$\begin{tikzcd}
415 \arrow[r, dash] & 278 & 508 \arrow[r, dash] & 151 & 138 \arrow[r, dash] & 183 & 23 \arrow[r, dash] & 30 \\
415 \arrow[r, dash] & 278 & 508 \arrow[r, dash] & 151 & 138 \arrow[r, dash] & 183 & 23 \arrow[r, dash] & 30 \\
329 \arrow[r, dash] & 8 & 191 \arrow[r, dash] & 188 & 0 \arrow[r, dash] & 46 & 365 \arrow[r, dash] & 365 \\
329 \arrow[r, dash] & 8 & 191 \arrow[r, dash] & 188 & 0 \arrow[r, dash] & 46 & &
\end{tikzcd}$$

Acknowledgments

There have been a number of people who accompanied and supported me during my studies and I appreciate that a lot. Most notably I want to thank

- ✦ my supervisor Prof. Dr. Andreas Stein for guiding me, introducing this particularly interesting research topic to me and giving me the possibility to become acquainted with the academic world;
- ✦ the University of Oldenburg and all of its staff for the enjoyable years and the great working atmosphere;
- ✦ Prof. Dr. Steven Galbraith for enabling my visit at the University of Auckland and helping me with my studies;
- ✦ the DAAD for giving me this opportunity through funding the stay in Auckland, New Zealand with a PhD scholarship;
- ✦ Marco Streng for pointing out an easy solution to a problem I posed at the Intercity Number Theory Seminar in Groningen;
- ✦ everyone else who discussed questions concerning my work with me, gave me new ideas or proofread it;
- ✦ my family for unconditionally supporting me on my way and always being there for me;
- ✦ my friends for listening, making me laugh and relax and having a wonderful time during and beside the university life;
- ✦ and Max for all of the last points and for standing beside me the whole time.

Thank You!

Selbstständigkeitserklärung

Hiermit versichere ich, dass ich diese Dissertation selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Sie wurde weder in ihrer Gesamtheit noch in Teilen einer anderen wissenschaftlichen Hochschule zur Begutachtung in einem Promotionsverfahren vorgelegt.

Außerdem erkläre ich, dass ich die allgemeinen Prinzipien wissenschaftlicher Arbeit und Veröffentlichung, wie sie in den Leitlinien guter wissenschaftlicher Praxis der Carl von Ossietzky Universität Oldenburg festgelegt sind, befolgt habe.

Oldenburg, 23. Februar 2015.

Christina Delfs