Generating supersingular curves with modular polynomials

Simon Pohmann
St Hugh's College
University of Oxford

A thesis submitted for the degree of
Master of Science in Mathematics
2022

Contents

Chapter 1

Introduction

In recent years, much progress has been made in the construction of quantum computers that might be able to break currently used cryptographic schemes. Hence, the search for alternative schemes is currently in the center of attention. One approach is based on ideas of Couveignes, Rostovtsev and Stolbunov [12, 27, 30], but only became really practical with the introduction of the SIDH protocol [17].

The main difference to the previous protocols is that instead of ordinary Elliptic Curves, SIDH relies on supersingular curves. These have the advantage that the structure of their rational points is much more predictable, hence allowing efficient computations. While recent successes in the cryptoanalysis of SIDH [6] eliminate this scheme, there are already ideas about how it can be fixed [24, 19]. Furthermore, many other cryptosystems are based on supersingular Elliptic Curves, like variants of SIDH [7, 11] or hash functions [8]. All in all, it is fair to say that supersingular curves are a hot topic in cryptography.

It is thus a natural question how to computationally generate random supersingular curves for use in various protocols. The current approach, based on random walks in isogeny graphs (see Section 5.1), is very efficient, but has a drawback. Namely, the computation reveals an isogeny path to the starting curve, which usually has a small endomorphism ring, a weakness [15]. In the standard scenario, this is not a problem, since the person generating the curve will be one of the participants, and not an attacker. However, there are situations in which there are problems caused by this weakness. In particular, a various cryptographic primitives [18, 5] currently require a trusted setup step because of it.

It is currently an open problem if we can generate Elliptic Curves efficiently in a way that does not reveal such an isogeny, nor other information that might be used for attacks in certain scenarios. Up to now, the only solution is to involve a trusted third party that forgets about the additional information produced by generating a supersingular curve by one of the classical ways.

Some approaches to solve this problem have been proposed in [2], most of them trying to exploit special structure to find roots of very large polynomials. However, for each approach so far there are some serious obstacles before it might be practical. In this work, we focus on the second of these, which is proposed by Kate Stange. Basically, it relies on the observation that Elliptic Curves with fixed-degree isogenies to their Frobenius conjugate are supersingular with higher probability. In the case that one requires two isogenies of different, fixed degree, they also propose a resultant-based algorithm to find such curves. However, as mentioned in [2], there are two main problems with this approach.

First, it is not clear how strong the correlation between having fixed-degree isogenies to the conjugate and the supersingularity is. The paper contains an estimate under the assumption that the existence of different degree isogenies is in a certain sense independent. However, this estimate does not completely match their experimental data. Furthermore, in the case of taking two isogenies of different degree, the correlation seems to be too weak, i.e. there are still to many ordinary curves with such isogenies to make the method find a supersingular curve efficiently. According to their heuristic, this can be fixed by using three different isogenies, but this is also not proven, and computationally more expensive than the two-isogeny variant.

The second problem is that in order to avoid vulnerabilities, the algorithm has to work with modular polynomials of exponential degree. Currently, no way to exploit special structure is known that would allow us to do this efficiently.

In our research, we tried to address both problems. Namely, we were able to find a special cases involving two isogenies, in which the fraction of supersingular Elliptic Curves is provably big enough. More concretely, we present the following result.

Proposition 1.0.1 (First Result)**.** *Let l be a small prime, f be an odd integer and e an even integer such that l^f is polynomial in $\log(p)$ and $l^e = \Theta(p)$. Then a random Elliptic Curve over $\bar{\mathbb{F}}_p$ with a cyclic l^f-isogeny and any l^e-isogeny to its Frobenius conjugate is supersingular with exponentially high probability (in $\log(p)$).*

Taking the degrees of the isogenies to be prime powers might additionally have computational advantages, as it allows us to decompose the isogeny into a sequence of smaller ones. In particular, this holds for the possibly non-cyclic isogeny of degree l^e.

The second problem seems to be more difficult, and we did not find an algorithm that can compute the curves in practice. However, we also propose a variant of the original idea, and argue that the structure of the corresponding polynomials looks like it might make computations simpler. This new method is based on the following statement, which is our second main result.

Proposition 1.0.2 (Second Result)**.** *Let $l_1, ..., l_r$ be a small primes with $\prod l_i \geq \sqrt{p}$. Then a random Elliptic Curve over $\mathbb{F}_{p^2}$ such that there are three l_i-isogeneous curves over $\mathbb{F}_{p^2}$ for each i is supersingular with exponentially high probability.*

Finally, we also present some classical results from the theory underlying isogeny graphs, in the hope of making them more accessible to cryptographers. Most of the standard mathematical literature on the subject (e.g. [13]) usually focuses on the case of Elliptic Curves over $\mathbb{C}$, and the finite field setting used in cryptography introduces some additional subtleties. The finite field setting and its connection to the classical, complex setting are seldomly treated, and then in works like [14] or [33], which are quite challenging. For example, the work of Deuring [14] is quite old and written in German, while the work of Waterhouse [33] treats the much more general theory of abelian varieties, and uses a great deal more algebraic geometry than necessary for Elliptic Curves. To summarize, (relatively) elementary proofs for some classical results seem to be missing in the crypto literature, and we also want to bridge this gap in this work.

Chapter 2

Elliptic Curves and Isogenies

In this chapter, we will give a short overview on the basic theory of Elliptic Curves. However, since the details are mostly the theory of algebraic geometry and do not bear too much on the main content of our work, we will keep it brief and refer the reader to the excellent textbook [29].

2.1 Elliptic Curves and the group law

Consider a field k with algebraic closure $\bar{k}$. An *Elliptic Curve* is a nonsingular projective curve of genus 1 together with a special point O. If the characteristic of k is not 2 or 3, each Elliptic Curve E is isomorphic to a projective plane curve given by an affine equation of the form

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

such that the special point is the projective point at infinity $O = (0 : 1 : 1)$ [29, Prop. III.3.1]. Furthermore, an isomorphism class of Elliptic Curves is uniquely determined by its j-invariant [29, Prop. III.1.4], defined as

$$j(E) := -1728 \frac{(4A)^3}{-16(4A^3 + 27B^3)}$$

Since isomorphic curves have the same properties in all aspects that matter for this work, we will use the terms Elliptic Curves and isomorphism classes of Elliptic Curves interchangeably from now on. In particular, note that whenever we count Elliptic Curves with special properties, we only count isomorphism classes.

The reason that makes Elliptic Curves so important is that they are abelian varieties, i.e. become groups in a way compatible with the geometric structure. There are different characterizations of this group law, the most explicit being its representation by polynomials. More concretely, if the curve is given by an affine equation $y^2 = x^3 + Ax + B$, then the sum of two affine points $P = (x_1 : y_1 : 1)$ and $Q = (x_2 : y_2 : 1)$ is given as

$$P + Q = (\lambda^2\mu - x_1\mu^3 - x_2\mu^3 : \lambda(2x_1\mu^2 + x_2\mu^2 - \lambda^2) - y_1\mu^3 : \mu^3)$$

where

$$(\lambda, \mu) = \begin{cases} (y_2 - y_1, x_2 - x_1) & \text{if } x_1 \neq x_2 \\ (3x_1^2 + A, 2y_1) & \text{if } x_1 = x_2 \end{cases}$$

Moreover, we declare the special point O to be the identity element of the group. The nontrivial result is now that this defines a group law on the set of points of E [29, Prop. III.2.2]. A more theoretical characterization of the group law is given by [29, Prop. III.3.4], which states that the above operation $+$ is the same as the group law induced by a natural isomorphism $E \cong \mathrm{Pic}(E)$ from the points of E to its Picard group.

The two most important subgroups of the group E are now the n-torsion group

$$E[n] := \{P \in E \mid \underbrace{P + ... + P}_{n \text{ times}} = O\}$$

and the subgroup of k-rational points

$$E(k) := \{P \in E \mid P = (x : y : z) \text{ for some } x, y, z \in k\}$$

2.2 Isogenies

An *isogeny* between two Elliptic Curves E and E' is a morphism (in the sense of algebraic geometry) that maps O to O. The first important result is that an isogeny is automatically a group homomorphism [29, Thm III.4.8]. The simplest example of an isogeny is the multiplication-by-m map on an Elliptic Curve E

$$[m] : E \to E, \quad P \mapsto \underbrace{P + ... + P}_{m \text{ times}}$$

An isogeny $\psi : E \to E'$ is closely connected to the field extension $k[E]/\psi_* k[E']$, where $\psi_* : k[E'] \to k[E]$ is the associated map of k-algebras. The degree of ψ is then given by the degree of this field extension (it is always finite), and ψ is said to be separable, if $k[E]/\psi_* k[E']$ is. Similarly, we can define the separability degree of an isogeny. It is a fact of algebraic geometry that both degree and separability degree behave multiplicatively under composition. Furthermore, the separability degree of an isogeny is equal to the size of its kernel [29, Thm III.4.10]. It is common to call isogenies of degree m also m-isogenies.

Studying again the example of the multiplication-by-m isogeny $[m] : E \to E$, one can show that this has degree m^2. Its kernel is obviously the subgroup $E[m]$, and thus, if $[m]$ is separable, we see that $E[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$. We will explain what happens in the case that $[m]$ is inseparable in the next section.

A very important result on isogenies is that they can be classified by their kernel $\ker(\psi) \subseteq E$, which is always a finite group. More concretely, up to isomoprhism, there is a one to one correspondence

$$\begin{array}{rcl} \{\text{Pairs } (\psi, E') \text{ where } \psi : E \to E' \text{ is a separable isogeny}\} & \to & \{\text{Finite subgroups } G \leq E\} \\ (E', \psi) & \mapsto & \ker(\psi) \end{array}$$

In particular, for a finite subgroup $G \leq E$ there is a unique (up to isomorphism) Elliptic Curve E' and separable isogeny $\psi : E \to E'$ with kernel G. We also denote E' by E/G, as that is the group structure on E' by the isomorphism theorem (morphisms of projective irreducible curves are always surjective).

Furthermore, this correspondence is compatible with the inclusion of finite subgroups as follows. If $G_1 \leq G_2 \leq E$ are two finite subgroups, then the unique separable isogeny $\psi : E \to E/G_2$ with kernel G_2 factors through the isogeny $\phi : E \to E/G_1$, i.e. there is an isogeny $\rho : E/G_1 \to E/G_2$ with

$$\begin{tikzcd} E \arrow[r, "\phi"] \arrow[rr, bend left, "\psi"] & E/G_1 \arrow[r, "\rho"] & E/G_2 \end{tikzcd}$$

is commutative. An analogous statement also holds for inseparable isogenies. If $\mathrm{char}(k) = p$, then an inseparable isogeny $\psi : E \to E'$ always factors through the p-th power Frobenius $\pi : E \to E^{(p)}$ (which is of course purely inseparable), where $E^{(p)}$ is the Elliptic Curve with all coefficients of the defining equation raised to the p-th power. Note that can also define operation $\cdot^{(p)}$ on isogenies, by again raising each coefficient in the defining polynomials to the p-th power. This way, $\cdot^{(p)}$ becomes an endofunctor on the category of Elliptic Curves over $\bar{\mathbb{F}}_p$ and their isogenies.

The final notion we require in this context is the one of the dual isogeny. Since the kernel of an isogeny $\psi : E \to E'$ is a subgroup of size $\deg_s(\psi)$, we see that it is contained in $E[\deg(\psi)] = \ker[\deg(\psi)]$. Now the previous correspondence shows that ψ factors through through the multiplication map $[\deg(\psi)]$, via an isogeny $\hat{\psi}$

$$\begin{tikzcd} E \arrow[r, "\psi"] \arrow[rr, bend left, "{[\deg(\psi)]}"] & E' \arrow[r, "\hat{\psi}"] & E \end{tikzcd}$$

The isogeny $\hat{\psi} : E' \to E$ has then the same degree as ψ, and is called the *dual isogeny* of ψ.

2.3 The endomorphism ring

For an Elliptic Curve E, we write from now on $\mathrm{End}(E)$ for the set of isogenies $E \to E$. Via composition and pointwise addition, this becomes a (possibly noncommutative) unital ring. The existence of the multiplication-by-m isogeny implies that there is a ring homomorphism

$$\mathbb{Z} \to \mathrm{End}(E)$$

As it turns out, this is always injective [29, Prop. III.4.2], hence the endomorphism ring has characteristic 0. Much more is known about the endomorphism ring, though. In particular, there is the following theorem

Theorem 2.3.1. *Let E be an Elliptic Curve over k. Then* $\mathrm{End}(E)$ *is one of the following*

- *The ring of integers $\mathbb{Z}$.*
- *An order in a quadratic imaginary number field.*
- *An order in the quaternion algebra ramified exactly at p and ∞, where $p = \mathrm{char}(k)$.*

If $\mathrm{char}(k) = 0$*, only the first two are possible. Similarly, if* $\mathrm{char}(k) \neq 0$*, only the last two are possible.*

For a proof, see e.g. [29, Corollary III.9.4].

If $\mathrm{char}(k) \subseteq \bar{\mathbb{F}}_p$, we call the curve E *ordinary* in the second case and *supersingular* in the third case. There are some other fundamental differences between those two types, as displayed in the following table. Denote by π_E the q-th power Frobenius, where E is defined over $\mathbb{F}_q$.

ordinary	supersingular
$[p]$ has separability degree p	$[p]$ is totally inseparable
$E[p] \cong \mathbb{Z}/p\mathbb{Z}$	$E[p] = \{O\}$
$\mathrm{End}(E)$ is commutative	$\mathrm{End}(E)$ is not commutative
$\mathrm{Tr}(\pi_E) \not\equiv 0 \mod p$	$\mathrm{Tr}(\pi_E) \equiv 0 \mod p$
$\hat{\pi}_E$ separable	$\hat{\pi}_E$ totally inseparable
$p \nmid d(\mathrm{End}(E))$	$p \mid d(\mathcal{O})$ for some commutative subring $\mathcal{O} \subseteq \mathrm{End}(E)$

Note that the trace [1] of the Frobenius endomorphism $\mathrm{Tr}(\pi_E)$ is of some importance, as (in the ordinary case) it determines the quadratic imaginary number field that contains $\mathrm{End}(E)$. Furthermore, there is the relationship

$$\mathrm{Tr}(\pi_E) = q + 1 - \#E(\mathbb{F}_q)$$

There is also the famous theorem by Hasse [29, Thm V.1.1] which states that

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

In particular, this implies that $|\mathrm{Tr}(\pi_E)| \leq 2\sqrt{q}$. Furthermore, if $E/\mathbb{F}_q$ is ordinary, the discriminat of the order $\mathrm{End}(E)$ divides the discriminat $d(\mathbb{Z}[\pi_E])$, as $\mathbb{Z}[\pi_E] \subseteq \mathrm{End}(E)$. As $d(\mathbb{Z}[\pi_E]) = \mathrm{Tr}(\pi_E)^2 - 4q$, we see that $-4q < d(\mathrm{End}(E)) < 0$ in this case.

Finally, note that in a supersingular Elliptic Curve, we always have $[p] = \epsilon\pi^2$, where now $\pi : E \to E^{(p)}$ the the p-th power Frobenius and ϵ is an automorphisms of E. However, too hard to show [29, Thm III.10.1] that

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

in the case $\mathrm{char}(k) \neq 2, 3$. Thus we see that either $j(E) \in \{0, 1728\}$ or $[p] = \pm\pi^2$, and so in both cases that $j(E) \in \mathbb{F}_{p^2}$. In other words, every supersingular curve is isomoprhic to a curve over $\mathbb{F}_{p^2}$.

[1] By trace, we mean either the trace in the quadratic imaginary number field, or the reduced trace in the quaternion algebra. In particular, if $\pi_E = \pm p$ (the supersingular setting with $E/\mathbb{F}_{p^2}$), we have $\mathrm{Tr}(\pi_E) = \pm 2p$.

Chapter 3

Isogeny graphs

In cryptography, we are of course not just interested in abstract structure of Elliptic Curves and isogenies, but also in computing it. There are for example nice ways to compute the curve E and the isogeny $E \to E/G$ for a finite subgroup $G \leq E$ in time polynomial in $\#G$. However, in the general case, there is no way how one can represent or compute an isogeny of exponentially large degree. This is where we can do cryptography, since for smooth-degree isogenies ψ, we can factor them into a sequence of small degree isogenies, and evaluate them one after the other. However, if this factorization is not known, it seems very hard to evaluate the isogeny.

The underlying structure of this approach (and others) can now be captured by the l-isogeny graph $\Gamma_l(\mathbb{F}_q)$, for a prime $l \neq p$.

Definition 3.0.1. Denote by $\Gamma_l(\mathbb{F}_q)$ the graph whose vertices are isomorphism classes of Elliptic Curves over $\mathbb{F}_q$, and the edges are the degree l isogenies between them (with multiplicity).

Since there is never an isogeny between ordinary and supersingular curves, each connected component of $\Gamma_l(\mathbb{F}_q)$ contains either only ordinary or supersingular curves. Hence, we will call them ordinary and supersingular connected components, respectively. Furthermore, the existence of the dual isogeny shows that this graph is undirected, and we know that it is $(l+1)$-regular (if $l \perp p$), since there are exactly $l+1$ subgroups of order l in $E[l] \cong (\mathbb{Z}/l\mathbb{Z})^2$.

Note that when doing computations with this graph, we identify each vertex with the j-invariant of the corresponding curves. This makes it easy to work with isomorphism classes of Elliptic Curves. Furthermore, we observe that $\Gamma_l(\mathbb{F}_q)$ has exactly q vertices, since there are that many j-invariants $j \in \mathbb{F}_q$.

3.1 The ordinary case

We begin by analysing the structure of the ordinary part of $\Gamma_l(\mathbb{F}_q)$, which (as we will see), is quite different from the supersingular part. There is a very powerful description of this graph in terms of the endomorphism rings of the ordinary curves. Since these are (usually non-maximal) orders in quadratic imaginary number fields, whose theory is somewhat more complicated than the one of maximal orders (which are Dedekind domains), we first study them a little.

3.1.1 Imaginary quadratic orders

For this part, let $\mathcal{O}$ be an order in an imaginary quadratic number field K. What we will mainly do in this section is to show that ideal $\mathfrak{a} \leq \mathcal{O}$ with norm $\mathfrak{N}(\mathfrak{a}) := [\mathcal{O} : \mathfrak{a}]$ coprime to the index

$[\mathcal{O}_K : \mathcal{O}]$ behave "nicely", i.e. similar to ideals in a Dedekind domain. Furthermore, we will study the structure of the class group of $\mathcal{O}$. First, we state a version of the chinese remainder theorem.

Lemma 3.1.1. *Let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}$. Then*

$$\mathcal{O}/\mathfrak{a} \cong \bigoplus_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}/\mathfrak{a}\mathcal{O}_{\mathfrak{p}}$$

For a proof of this, see e.g. [25, Prop. I.12.3].

Lemma 3.1.2. *Let $\mathfrak{p} \leq \mathcal{O}_K$ be a prime with $\mathfrak{N}(\mathfrak{p}) \perp [\mathcal{O}_K : \mathcal{O}]$. Then $\mathfrak{p}$ has a set of generators in $\mathcal{O}$.*

Proof. Suppose $\mathfrak{p}$ is a prime over p, and let $\mathcal{O} = \mathbb{Z}[\phi]$. We use the decomposition law in Dedekind ring extensions. Since $\mathfrak{N}(\mathfrak{p}) \perp [\mathcal{O}_K : \mathcal{O}]$ are coprime, we can apply it with a generator ϕ of $\mathcal{O}$.

If $\mathrm{MiPo}(\phi) = f(X)g(X) \mod p$ splits, then have

$$p\mathcal{O}_K = (p, f(\phi))(p, g(\phi))$$

and so the prime ideals over p are $(p, f(\phi))$ and $(p, g(\phi))$. If $\mathrm{MiPo}(\phi) \mod p$ is irreducible, then have that $p\mathcal{O}_K$ is prime and thus the only prime ideal over p. Hence, all prime ideals over p (including $\mathfrak{p}$) have a set of generators in $\mathcal{O}$. □

Corollary 3.1.3. *Let $\mathfrak{a} \leq \mathcal{O}_K$ be an ideal with $\mathfrak{N}(\mathfrak{a}) \perp [\mathcal{O}_K : \mathcal{O}]$. Then $\mathfrak{a}$ has a set of generators in $\mathcal{O}$.*

Proposition 3.1.4. *Let $\mathfrak{p} \leq \mathcal{O}$ be a prime ideal with $\mathfrak{N}(\mathfrak{p}) \perp [\mathcal{O}_K : \mathcal{O}]$ and $\mathfrak{p}' = \mathfrak{p}\mathcal{O}_K$. Then $\mathcal{O}_{\mathfrak{p}} = (\mathcal{O}_K)_{\mathfrak{p}'}$.*

Proof. We have $\mathcal{O}_K = \mathbb{Z}[\alpha]$ and $\mathcal{O} = \mathbb{Z}[f\alpha]$ where $f = [\mathcal{O}_K : \mathcal{O}]$. Thus $f \notin \mathfrak{p}$ and so $f \in \mathcal{O}_{\mathfrak{p}}^*$. Therefore $\mathcal{O}_K \subseteq \mathcal{O}_{\mathfrak{p}}$ and thus $(\mathcal{O}_K)_{\mathfrak{p}'} \subseteq \mathcal{O}_{\mathfrak{p}}$. □

This already gives a somewhat nice description of most ideals of the order $\mathcal{O}$.

Proposition 3.1.5. *Let $\mathfrak{I}_f(\mathcal{O})$ resp. $\mathfrak{I}_f(\mathcal{O}_K)$ denote the monoid of invertible integral ideals of norm $\perp f := [\mathcal{O}_K : \mathcal{O}]$. Then*

$$\mathfrak{I}_f(\mathcal{O}) \to \mathfrak{I}_f(\mathcal{O}_K), \quad \mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_K$$

is a monoid isomorphism with inverse

$$\mathfrak{I}_f(\mathcal{O}_K) \to \mathfrak{I}_f(\mathcal{O}), \quad \mathfrak{a} \mapsto \mathfrak{a} \cap \mathcal{O}$$

Proof. Clearly, this is a well-defined monoid homomorphism. Hence, we have to show that it is bijective.

By Corollary 3.1.3, we know that any $\mathfrak{a} \leq \mathcal{O}_K$ with $\mathfrak{N}(\mathfrak{a}) \perp [\mathcal{O}_K : \mathcal{O}]$ has generators in $\mathcal{O}$, thus $(\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K = \mathfrak{a}$. This shows that $\mathfrak{a} \cap \mathcal{O}$ is a preimage of $\mathfrak{a}$, and so the map is surjective.

Assume now $\mathfrak{a}, \mathfrak{b} \leq \mathcal{O}$ with $\mathfrak{a}\mathcal{O}_K = \mathfrak{b}\mathcal{O}_K$ and $\mathfrak{N}(\mathfrak{a}), \mathfrak{N}(\mathfrak{b}) \perp f$. We show that $\mathfrak{a}_{\mathfrak{p}} = \mathfrak{b}_{\mathfrak{p}}$ for all primes $\mathfrak{p} \leq \mathcal{O}$. Note that if $\mathfrak{N}(\mathfrak{p}) \not\perp f$, this holds trivially, as $\mathfrak{a}_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}} = \mathfrak{b}_{\mathfrak{p}}$. Otherwise, note that

$$\mathfrak{a}_{\mathfrak{p}} = \mathfrak{a}_{\mathfrak{p}}\mathcal{O}_{\mathfrak{p}} = \mathfrak{a}(\mathcal{O}_K)_{\mathfrak{p}} = \mathfrak{a}\mathcal{O}_K(\mathcal{O}_K)_{\mathfrak{p}} = \mathfrak{b}\mathcal{O}_K(\mathcal{O}_K)_{\mathfrak{p}} = \mathfrak{b}_{\mathfrak{p}}(\mathcal{O}_K)_{\mathfrak{p}} = \mathfrak{b}_{\mathfrak{p}}$$

as $\mathcal{O}_{\mathfrak{p}} = (\mathcal{O}_K)_{\mathfrak{p}}$. This shows that $\mathfrak{a}_{\mathfrak{p}} = \mathfrak{b}_{\mathfrak{p}}$ at all primes, so $\mathfrak{a} = \mathfrak{b}$ and our map is injective. Furthermore, since $(\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K = \mathfrak{a}$, we see that it has the inverse

$$\mathfrak{I}_f(\mathcal{O}_K) \to \mathfrak{I}_f(\mathcal{O}), \quad \mathfrak{a} \mapsto \mathfrak{a} \cap \mathcal{O}$$

which must then be well-defined. □

Furthermore, we are really interested in the class group of $\mathcal{O}$, which is now the quotient of only the invertible ideals of $\mathcal{O}$ modulo the principal ideals. The following statements are special cases of the general theory in [25, Chapter I.§12].

Lemma 3.1.6. *Write $\mathfrak{I}(\mathcal{O})$ for the group of invertible fractional ideals in $\mathcal{O}$. Then there exists an isomorphism*

$$\iota : \bigoplus_{\mathfrak{p}} K^*/\mathcal{O}_{\mathfrak{p}}^* \to \mathfrak{I}(\mathcal{O})$$

with $\iota(a)\mathcal{O}_{\mathfrak{p}} = (a_{\mathfrak{p}})$ for all prime ideals $\mathfrak{p} \leq \mathcal{O}$ and $a = (a_{\mathfrak{p}})_{\mathfrak{p}}$.

Proof. Again, this is a special case of [25, Prop. I.12.9].

First, we show that for an invertible ideal $\mathfrak{a} = (a_1, ..., a_n)$ have that $\mathfrak{a}\mathcal{O}_{\mathfrak{p}}$ is principal. By assumption, have $\mathfrak{a}\mathfrak{b} = (1)$ with $\mathfrak{b} = (b_1, ..., b_m)$ and so have $1 = \sum a_i b_i c_i$ with $c_i \in \mathcal{O}_{\mathfrak{p}}$. Clearly, $1 \notin \mathfrak{p}\mathcal{O}_{\mathfrak{p}}$ and thus one $a_i b_i c_i \notin \mathfrak{p}\mathcal{O}_{\mathfrak{p}}$, so $a_i b_i c_i \in \mathcal{O}_{\mathfrak{p}}^*$ is a unit. Therefore, we find that $\mathfrak{a}\mathcal{O}_{\mathfrak{p}} = a_i\mathcal{O}_{\mathfrak{p}}$, because for all $x \in \mathfrak{a}\mathcal{O}_{\mathfrak{p}}$, have then $x b_i c_i \in \mathfrak{a}\mathfrak{b} = \mathcal{O}_{\mathfrak{p}}$, so

$$x = a_i \underbrace{x b_i c_i}_{\in \mathcal{O}_{\mathfrak{p}}} \in a_i \mathcal{O}_{\mathfrak{p}}$$

Now we can see that there is a well-defined homomorphism

$$\iota^{-1} : \mathfrak{I}(\mathcal{O}) \to \bigoplus_{\mathfrak{p}} K^*/\mathcal{O}_{\mathfrak{p}}^*$$

that maps an ideal $\mathfrak{a}$ to the class of generators of $\mathfrak{a}\mathcal{O}_{\mathfrak{p}}$.

Clearly, it is injective, since if $\mathfrak{a}\mathcal{O}_{\mathfrak{p}} \neq \mathfrak{b}\mathcal{O}_{\mathfrak{p}}$ for any prime $\mathfrak{p}$, then $\mathfrak{a} \neq \mathfrak{b}$.

It is thus left to show that ι^{-1} is also surjective. The following proof is taken with some modifications from [25, Prop. I.12.2].

Assume $(a_{\mathfrak{p}})_{\mathfrak{p}} \in \bigoplus_{\mathfrak{p}} K^*/\mathcal{O}_{\mathfrak{p}}^*$. Then set $\mathfrak{a} := \bigcap_{\mathfrak{p}} a_{\mathfrak{p}}\mathcal{O}_{\mathfrak{p}}$. Clearly we have $\mathfrak{a}\mathcal{O}_{\mathfrak{p}} \subseteq a_{\mathfrak{p}}\mathcal{O}_{\mathfrak{p}}$, so it is left to show the inclusion $\supseteq$.

First of all, all except finitely many $a_{\mathfrak{q}}$ are in $\mathcal{O}_{\mathfrak{q}}^*$, hence we can assume that those are $a_{\mathfrak{q}} = 1$. Let $c \in \mathcal{O}$ with $c a_{\mathfrak{q}}/a_{\mathfrak{p}} \in \mathcal{O}$ for all $\mathfrak{q}$ such that $a_{\mathfrak{q}} \neq 1$. Now the chinese remainder theorem gives us $b \in \mathcal{O}$ such that

$$b \equiv c \mod \mathfrak{p} \quad \text{and} \quad b \equiv c a_q / a_{\mathfrak{p}} \mod \mathfrak{q}^k \quad \text{for } \mathfrak{q} \neq \mathfrak{p} \text{ with } a_{\mathfrak{q}} \neq 1$$

where $k \geq 1$ is an integer such that $a_q \in \mathfrak{q}^k\mathcal{O}_k$.

This b is unique modulo $\bigcap_{a_{\mathfrak{q}} \neq 1} \mathfrak{q}^k$, and in particular, we can choose it such that $b a_{\mathfrak{p}}/c \in \mathcal{O}$. Now we have $b/c \in \mathcal{O}_{\mathfrak{p}}^*$. Furthermore, $a_{\mathfrak{p}} b/c \in \mathfrak{a}$, since

- $b/c \in \mathcal{O}_{\mathfrak{p}}^* \subseteq \mathcal{O}_{\mathfrak{p}}$, so $a_{\mathfrak{p}} b/c \in a_{\mathfrak{p}}\mathcal{O}_{\mathfrak{p}}$.
- $b \equiv c a_q/a_{\mathfrak{p}} \mod \mathfrak{q}^k$, so $a_{\mathfrak{p}} b/c \equiv a_{\mathfrak{q}} \mod \mathfrak{q}^k\mathcal{O}_{\mathfrak{q}}$, which implies $a_{\mathfrak{p}} b/c \in a_{\mathfrak{q}}\mathcal{O}_{\mathfrak{q}}$ for $\mathfrak{q} \neq \mathfrak{p}$ with $a_{\mathfrak{q}} \neq 1$.
- $b a_{\mathfrak{p}}/c \in \mathcal{O}$, so $b a_{\mathfrak{p}}/c \in a_{\mathfrak{q}}\mathcal{O}_{\mathfrak{q}}$ whenever $a_{\mathfrak{q}} = 1$.

Since $b/c \in \mathcal{O}_{\mathfrak{p}}^*$, we now find $a_{\mathfrak{p}} \in \mathfrak{a}\mathcal{O}_{\mathfrak{p}}^*$ and the claim follows. □

This lemma is a very useful characterization of invertible ideals. We are now ready for our first description of $\mathrm{Cl}(\mathcal{O})$.

Lemma 3.1.7. *Let $f = [\mathcal{O}_K : \mathcal{O}]$ and assume that $\mathcal{O}_K^* = \{\pm 1\}$. There is an exact sequence*

$$1 \to \bigoplus_{\mathfrak{p}} R_{\mathfrak{p}}^*/\mathcal{O}_{\mathfrak{p}}^* \to \mathrm{Cl}(\mathcal{O}) \to \mathrm{Cl}(\mathcal{O}_K) \to 1$$

where $\mathrm{Cl}(\mathcal{O})$ is the ideal class group of $\mathcal{O}$, i.e. the group of invertible, fractional ideals modulo principal ideals and $R_{\mathfrak{p}}$ is the localization of $\mathcal{O}_K$ at the multiplicative set $\mathcal{O} \setminus \mathfrak{p}$.

Proof. This proof is taken with some modifications from [25, Prop. I.12.11].

First, we show that every ideal class $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_K)$ has an integral representative of norm coprime to f. Let $m \mid \mathfrak{N}(\mathfrak{a})$ be maximal such that $m \mid f^e$ for some e. Then there is an element $\alpha \in m\mathfrak{a}^{-1}$, and we see that $\mathfrak{N}(\alpha^{-1}\mathfrak{a}) \mid \mathfrak{N}(\mathfrak{a})/m$, thus is coprime to f. Furthermore, $\alpha \in \mathfrak{a}^{-1}$, so $\alpha^{-1}\mathfrak{a}$ is integral. This shows our claim, and so by Corollary 3.1.3 that the natural map

$$\mathrm{Cl}(\mathcal{O}) \to \mathrm{Cl}(\mathcal{O}_K), \quad [\mathfrak{a}] \to [\mathfrak{a}\mathcal{O}_K]$$

is surjective.

Next, note that the isomorphism $\iota : \mathfrak{I}(\mathcal{O}) \to \bigoplus_{\mathfrak{p}} K^*/\mathcal{O}_{\mathfrak{p}}^*$ induces a map

$$\bigoplus_{\mathfrak{p}} R_{\mathfrak{p}}^*/\mathcal{O}_{\mathfrak{p}}^* \to \mathrm{Cl}(\mathcal{O})$$

where $R_{\mathfrak{p}}$ is the localization of $\mathcal{O}_K$ at the multiplicative subset $\mathcal{O} \setminus \mathfrak{p}$.

It is injective, as for an element $a = (a_{\mathfrak{p}})_{\mathfrak{p}}$ in the kernel, have that $\iota(a) = (\alpha)$. However, then $(a_{\mathfrak{p}}) = (\alpha)$ in $\mathcal{O}_{\mathfrak{p}}$. Hence, $\mathfrak{a}_{\mathfrak{p}} = \alpha\epsilon$ for $\epsilon \in \mathcal{O}_{\mathfrak{p}}^*$ and we can assume that the representatives $a_{\mathfrak{p}} \in R_{\mathfrak{p}}^*$ are chosen such that $a_{\mathfrak{p}} = \alpha$. This implies that $\alpha \in \bigcap_{\mathfrak{p}} R_{\mathfrak{p}}^* = \mathcal{O}_K^*$, and by the assumption $\mathcal{O}_K^* = \{\pm 1\}$, have then $\alpha = \pm 1$. The claim follows.

Now it is only left to show that the sequence is exact at $\mathrm{Cl}(\mathcal{O})$.

For $a = (a_{\mathfrak{p}})_{\mathfrak{p}} \in \bigoplus_{\mathfrak{p}} R_{\mathfrak{p}}^*/\mathcal{O}_{\mathfrak{p}}^*$, we know that

$$\iota(a)R_{\mathfrak{p}} = \iota(a)\mathcal{O}_{\mathfrak{p}}R_{\mathfrak{p}} = a_{\mathfrak{p}}R_{\mathfrak{p}} = R_{\mathfrak{p}}$$

and so $\mathrm{im}(f) \subseteq \ker(g)$. Now we show the converse.

Let $\mathfrak{a} \leq \mathcal{O}$ be integral and invertible with $\mathfrak{a}\mathcal{O}_K = (\alpha)$. Since $[\frac{1}{\alpha}\mathfrak{a}] = [\mathfrak{a}]$ are in the same ideal class, we can assume wlog that $\alpha = 1$.

Let $a = (a_{\mathfrak{p}})_{\mathfrak{p}} = \iota^{-1}(\mathfrak{a})$. Then

$$a_{\mathfrak{p}}R_{\mathfrak{p}} = a_{\mathfrak{p}}\mathcal{O}_{\mathfrak{p}}R_{\mathfrak{p}} = \iota(a)R_{\mathfrak{p}} = \mathfrak{a}R_{\mathfrak{p}} = \alpha R_{\mathfrak{p}} = R_{\mathfrak{p}}$$

This clearly implies that $a_{\mathfrak{p}} \in R_{\mathfrak{p}}^*$ and so $\mathfrak{a} \in \mathrm{im}(f)$. □

The expression $\bigoplus_{\mathfrak{p}} R_{\mathfrak{p}}^*/\mathcal{O}_{\mathfrak{p}}^*$ is still somewhat unwieldy, but fortunately, it has the following nice form.

Lemma 3.1.8. *We have*

$$(\mathcal{O}_K/f\mathcal{O}_K)^*/(\mathcal{O}/f\mathcal{O}_K)^* \cong \bigoplus_{\mathfrak{p}} R_{\mathfrak{p}}^*/\mathcal{O}_{\mathfrak{p}}^*$$

Note that $f\mathcal{O}_K \subseteq \mathcal{O}$ is the largest ideal of $\mathcal{O}_K$ contained in $\mathcal{O}$, and thus an ideal of $\mathcal{O}$ as well.

Proof. First, note that if $\mathfrak{N}(\mathfrak{p}) \perp f$, we know that $R_\mathfrak{p} = (\mathcal{O}_K)_{\mathfrak{p}\mathcal{O}_K}$ and so by Prop. 3.1.4 that $R_\mathfrak{p}^*/\mathcal{O}_\mathfrak{p}^*$ is trivial.

Note that for each prime $\mathfrak{p} \leq \mathcal{O}$ containing $f\mathcal{O}_K$ have a finite, positive number of primes $\mathfrak{q} \leq \mathcal{O}_K$ with $\mathfrak{q} \cap \mathcal{O} = \mathfrak{p}$. There is at least one, as $\mathfrak{p}\mathcal{O}_K$ is contained in a prime, and the number is finite, as $f\mathcal{O}_K$ factors into finitely many primes in the Dedekind ring $\mathcal{O}_K$. Hence, we have by the chinese remainder theorem

$$(\mathcal{O}/f\mathcal{O}_K)^* \cong \bigoplus_{\mathfrak{p} \supseteq f\mathcal{O}_K} (\mathcal{O}_\mathfrak{p}/f\mathcal{O}_K\mathcal{O}_\mathfrak{p})^* \cong \bigoplus_{\mathfrak{p} \supseteq f\mathcal{O}_K} (\mathcal{O}_\mathfrak{p}/f\mathcal{O}_K\mathcal{O}_\mathfrak{p})^* = \bigoplus_{\mathfrak{p} \supseteq f\mathcal{O}_K} (\mathcal{O}_\mathfrak{p}/fR_\mathfrak{p})^*$$

Furthermore, we have

$$(\mathcal{O}_K/f\mathcal{O}_K)^* \cong \bigoplus_{\mathfrak{q} \supseteq f\mathcal{O}_K} ((\mathcal{O}_K)_\mathfrak{q}/f(\mathcal{O}_K)_\mathfrak{q})^* \cong \bigoplus_{\mathfrak{p} \supseteq f\mathcal{O}_K} \bigoplus_{\mathfrak{q} \supseteq \mathfrak{p}\mathcal{O}_K} ((\mathcal{O}_K)_\mathfrak{q}/f(\mathcal{O}_K)_\mathfrak{q})^*$$

We claim that

$$R_\mathfrak{p}/fR_\mathfrak{p} \cong \bigoplus_{\mathfrak{q} \supseteq \mathfrak{p}\mathcal{O}_K} (R_\mathfrak{p})_\mathfrak{q}/f(R_\mathfrak{p})_\mathfrak{q} = \bigoplus_{\mathfrak{q} \supseteq \mathfrak{p}\mathcal{O}_K} (\mathcal{O}_K)_\mathfrak{q}/f(\mathcal{O}_K)_\mathfrak{q}$$

This isomorphism follows from the chinese remainder theorem and the fact that the prime ideals $\mathfrak{q}$ over $\mathfrak{p}\mathcal{O}_K$ give all prime ideals of $R_\mathfrak{p}$.

Both isomorphisms are compatible [1], and so have

$$(\mathcal{O}_K/f\mathcal{O}_K)^*/(\mathcal{O}/f\mathcal{O}_K)^* \cong \bigoplus_{\mathfrak{p} \supseteq f\mathcal{O}_K} (R_\mathfrak{p}/fR_\mathfrak{p})^*/(\mathcal{O}_\mathfrak{p}/fR_\mathfrak{p})^*$$

Finally, observe that the map $R_\mathfrak{p}^* \to (R_\mathfrak{p}/fR_\mathfrak{p})^*/(\mathcal{O}_\mathfrak{p}/fR_\mathfrak{p})^*$ has kernel $\mathcal{O}_\mathfrak{p}^*$. It also is surjective, since for $[a] \in (R_\mathfrak{p}/fR_\mathfrak{p})^*$ there is $b \in R_\mathfrak{p}$ with $ab \in 1 + fR_\mathfrak{p}$ and thus $ab \equiv 1 \mod \mathfrak{p}R_\mathfrak{p}$ (because we only consider $\mathfrak{p}$ with $f \in \mathfrak{p}$). In particular, $a \notin \mathfrak{q}$ for all primes $\mathfrak{q}$ of $R_\mathfrak{p}$ (these are all over $\mathfrak{p}R_\mathfrak{p}$), and so $a \in R_\mathfrak{p}^*$. □

Corollary 3.1.9. *Suppose $\mathcal{O}_K = \{\pm 1\}$. Then there is an exact sequence*

$$1 \;\to\; (\mathcal{O}_K/f\mathcal{O}_K)^*/(\mathcal{O}/f\mathcal{O}_K)^* \;\to\; \mathrm{Cl}(\mathcal{O}) \;\to\; \mathrm{Cl}(\mathcal{O}_K) \;\to\; 1$$

The condition $\mathcal{O}_K = \{\pm 1\}$ is very weak, as there are only two quadratic imaginary number fields such that the ring of integers has more units, namely $K = \mathbb{Q}[\sqrt{-3}]$ and $K = \mathbb{Q}[\sqrt{-1}]$. These correspond to the Elliptic Curves with j-invariants 0 and 1728 (if they are ordinary), and need a special treatment in many cases anyway. In [25], there is also a more general version of this statement without this assumption.

3.1.2 The class group action

Now we can come back to the study of Elliptic Curves and their isogeny graphs. The class group action which we will define in the following is the most important tool when working with isogeny graphs of ordinary curves. Because of this, it is mentioned in more or less all the literature dealing with the topic. For me, it was thus quite surprising that I could nowhere find a precise and relatively elementary proof for the statement in the case of finite fields.

[1] Meaning the inclusion $\mathcal{O}/f\mathcal{O}_K \subseteq \mathcal{O}_K/f\mathcal{O}_K$ commutes with the natural map

$$O/f\mathcal{O}_K \xrightarrow{\sim} \bigoplus_{\mathfrak{p}} (\mathcal{O}_\mathfrak{p}/f\mathcal{O}_K\mathcal{O}_\mathfrak{p}) = \bigoplus_{\mathfrak{p}} (\mathcal{O}_\mathfrak{p}/fR_\mathfrak{p}) \to \bigoplus_{\mathfrak{p}} (R_\mathfrak{p}/fR_\mathfrak{p}) \xrightarrow{\sim} \mathcal{O}_K/f\mathcal{O}_K$$

Most sources cite [33, Thm 4.5], however the statement there is not as explicit as one might wish, and the proof is done in the much more general theory of abelian schemes. Apart from that, there are many references to the corresponding statement for curves over $\mathbb{C}$, but these ignore some of the subtleties introduced by non-separable isogenies. Therefore, we now present a relatively simple proof of the class group action for ordinary curves defined over a finite field and explicitly handle the non-separable case.

For the whole section, let E and E' be Elliptic Curves defined over a finite field $k = \mathbb{F}_q$ with characteristic p. We write π_E for the q-th power Frobenius endomorphism of E.

Definition 3.1.10. For an integral ideal $\mathfrak{a} \leq \mathrm{End}(E)$ of an ordinary Elliptic Curve E, define the $\mathfrak{a}$-torsion

$$E[\mathfrak{a}] := \bigcap_{\alpha \in \mathfrak{a}} \ker(\alpha)$$

From now on, we will often compare endomorphism rings of isogeneous curves. To do so, we embed those rings into an imaginary quadratic number field K. However, the field K and its orders can have nontrivial automorphisms, which means the embedding $\mathrm{End}(E) \to K$ cannot be unique. Fortunately, we can choose a system of embeddings $\mathrm{End}(E) \to K$ jointly for all curves E in a canonical way as follows.

Lemma 3.1.11. *Let $\phi : E \to E'$ be an isogeny. Then there is an isomorphism*

$$\Phi : \mathrm{End}(E) \otimes \mathbb{Q} \to \mathrm{End}(E') \otimes \mathbb{Q}, \quad \tau \mapsto \frac{1}{\deg(\phi)} \phi \circ \tau \circ \hat{\phi}$$

Furthermore, if we assume E to be ordinary, then this is canonical in the sense that for any other isogeny $\psi : E \to E'$ have $\Phi = \Psi$.

Proof. It is clear that this is a morphism of ring, and its inverse is given by $\hat{\Phi}$ induced by the dual isogeny $\hat{\phi}$.

So it remains to show the last part. Let ϕ and ψ be two isogenies $E \to E'$. Then for each $\tau \in \mathrm{End}(E)$ have

$$\begin{aligned}
(\Phi \circ \hat{\Psi})(\tau) &= \frac{1}{\deg(\phi)} \phi \circ \left(\frac{1}{\deg(\psi)} \hat{\psi} \circ \tau \circ \psi \right) \\
&= \frac{1}{\deg(\phi)\deg(\psi)} (\phi \circ \hat{\psi}) \circ \tau \circ (\psi \circ \hat{\phi}) \\
&= \frac{1}{\deg(\phi)\deg(\psi)} (\phi \circ \hat{\psi}) \circ (\psi \circ \hat{\phi}) \circ \tau \\
&= \frac{1}{\deg(\phi)\deg(\psi)} (\deg(\phi)\deg(\psi))\tau = \tau
\end{aligned}$$

since $(\psi \circ \hat{\phi})$ and τ are elements of $\mathrm{End}(E)$, hence commute.

Now $\hat{\Psi}$ is the inverse of Ψ, and the claim follows. $\square$

In other words, we choose an arbitrary embedding $\mathrm{End}(E) \to K$ for one ordinary curve E, and then choose all further embeddings $\mathrm{End}(E') \to K$ for isogeneous curves E' as

$$\mathrm{End}(E') \to \mathrm{End}(E') \otimes \mathbb{Q} \xrightarrow{\Phi} \mathrm{End}(E) \otimes \mathbb{Q} \to K$$

From now on, whenever we identify $\mathrm{End}(E)$ with an approriate subring of K, this shall use that embedding. This will be used already in the next statement, which describes the relationship of endomorphism rings of isogeneous curves more concretely.

Proposition 3.1.12. *Let $\phi : E \to E'$ be an isogeny of prime degree p between (not necessarily ordinary) Elliptic Curves. Then (after embedding* $\mathrm{End}(E')$ *via* Φ *and* $\mathrm{End}(E)$ *into* $\mathrm{End}(E) \otimes \mathbb{Q}$*) exactly one of the following is the case.*

- $\mathrm{End}(E) = \mathrm{End}(E')$ *and we call* ϕ horizontal.
- $\mathrm{End}(E) \subseteq \mathrm{End}(E')$ *with* $[\mathrm{End}(E') : \mathrm{End}(E)] = p$*. We call* ϕ ascending.
- $\mathrm{End}(E) \supseteq \mathrm{End}(E')$ *with* $[\mathrm{End}(E) : \mathrm{End}(E')] = p$*. We call* ϕ descending.

Proof. Note that the map

$$l\Phi : \mathrm{End}(E) \to \mathrm{End}(E'), \quad \tau \mapsto \phi \circ \tau \circ \hat{\phi}$$

yields endomorphisms of $\mathrm{End}(E')$, and so we have $l\mathrm{End}(E) \subseteq \mathrm{End}(E')$. Similarly, find $l\mathrm{End}(E') \subseteq \mathrm{End}(E)$.

Now let α be a generator of the maximal order in $K = \mathrm{End}(E) \otimes \mathbb{Q}$. Then each order of K is of the form $\mathbb{Z} + f\alpha\mathbb{Z}$, and so

$$\mathrm{End}(E) = \mathbb{Z} \oplus f_1\alpha\mathbb{Z}, \quad \mathrm{End}(E')\mathbb{Z} \oplus f_2\alpha\mathbb{Z}$$

However, this implies that $f_1 \mid lf_2$ and $f_2 \mid lf_1$, so $f_1 \mid lf_2 \mid l^2 f_1$. Since l is prime, we find $f_2 \in \{f_1/l, f_1, lf_1\}$ and the claim follows. □

Furthermore, we will sometimes talk about horizontal or vertical isogenies *at a prime* l, which is defined by the next proposition. The advantage is that this is defined for all isogenies, not just those of prime degree.

Proposition 3.1.13. *Similarly, let $\phi : E \to E'$ be an isogeny of any degree n. Further, let l be a prime. Then (after embedding* $\mathrm{End}(E') \otimes \mathbb{Z}_{(l)}$ *via* Φ *and* $\mathrm{End}(E) \otimes \mathbb{Z}_{(l)}$ *into* $\mathrm{End}(E) \otimes \mathbb{Q}$*) exactly one of the following is the case.*

- $\mathrm{End}(E) \otimes \mathbb{Z}_{(l)} = \mathrm{End}(E') \otimes \mathbb{Z}_{(l)}$ *and we call* ϕ horizontal at l.
- $\mathrm{End}(E) \otimes \mathbb{Z}_{(l)} \subseteq \mathrm{End}(E') \otimes \mathbb{Z}_{(l)}$ *with* $[\mathrm{End}(E') \otimes \mathbb{Z}_{(l)} : \mathrm{End}(E) \otimes \mathbb{Z}_{(l)}] = l^r$ *for $r > 0$. We call* ϕ ascending at l.
- $\mathrm{End}(E) \otimes \mathbb{Z}_{(l)} \supseteq \mathrm{End}(E') \otimes \mathbb{Z}_{(l)}$ *with* $[\mathrm{End}(E) \otimes \mathbb{Z}_{(l)} : \mathrm{End}(E') \otimes \mathbb{Z}_{(l)}] = p$ *for $r > 0$. We call* ϕ descending at l.

Proof. Exactly as the previous proof. □

Now we can make a step towards the class group action and present how we assign isogenies to (integral, invertible) ideals of the endomorphism ring.

Definition 3.1.14. For an ordinary Elliptic Curve E and an integral, invertible ideal [2] $\mathfrak{a} = \mathfrak{b}(p, \pi_E)^r \leq \mathrm{End}(E)$ with $\mathfrak{b} \perp (p, \pi_E)$ define the isogeny

$$\phi_{E,\mathfrak{a}} : E \longrightarrow E/E[\mathfrak{b}] \xrightarrow{\pi_r} E_{\mathfrak{a}} := (E/E[\mathfrak{b}])^{(p^r)}$$

where $E \to E/E[\mathfrak{b}]$ is the unique separable isogeny with kernel $E[\mathfrak{b}]$ and $\pi_r : E/E[\mathfrak{b}] \to (E/E[\mathfrak{b}])^{(p^r)}$ is the r-th power Frobenius map.

[2] By Prop. 3.1.5, this representation of an ideal $\mathfrak{a}$ is well-defined and unique, as $\mathfrak{N}((p, \pi)) = p \nmid [\mathcal{O}_{\mathrm{End}(E) \otimes \mathbb{Q}} : \mathrm{End}(E)] \mid d(\mathrm{End}(E))$.

In order to define a group action later, we need to be able to chain such isogenies given by ideals. The obvious difficulty here is that the ideals are all in the same ring, but subsequent isogenies will have different curves as domain. Hence, we need to be able to view an ideal $\mathfrak{a} \leq \mathrm{End}(E)$ as an ideal of another endomorphism ring $\mathrm{End}(E')$. As it turns out, the endomorphism rings we consider are all isomorphic, and so this works out nicely.

Lemma 3.1.15. *Let E be an ordinary Elliptic Curve and $\mathfrak{a} \leq \mathrm{End}(E)$ an integral, invertible ideal. Then $\mathrm{End}(E) \cong \mathrm{End}(E_{\mathfrak{a}})$. In particular, $\phi_{E,\mathfrak{a}}$ is horizontal at every prime l.*

Proof. Let $\mathfrak{a} = \mathfrak{b}(p, \pi_E)^r$ with $\mathfrak{b} \perp (p, \pi_E)$. We show that $\mathrm{End}(E) \cong \mathrm{End}(E/E[\mathfrak{b}])$ and the claim follows, as for any Elliptic Curve E, have an isomorphism

$$\mathrm{End}(E) \to \mathrm{End}(E^{(p)}), \quad \alpha \mapsto \alpha^{(p)}$$

It suffices to show that the separable isogeny $\phi := \phi_{E,\mathfrak{b}}$ is horizontal at each prime l.

Assume for a contradiction that ϕ is descending at l. In other words, there is $\tau \in \mathrm{End}(E)$ such that $\phi \circ \tau \circ \hat{\phi}$ is not divisible by l. Hence, $E'[l] \not\subseteq \ker(\phi \circ \tau \circ \hat{\phi})$ and there is a point $P \in E'[l]$ with $\phi(\tau(\hat{\phi}(P))) \neq O$. This implies $\tau(\hat{\phi}(P)) \notin E[\mathfrak{a}]$ and thus there is $\alpha \in \mathfrak{a}$ with $\tau(\hat{\phi}(P)) \notin \ker(\alpha)$. Note that α factors through ϕ as

$$\begin{tikzcd} E \arrow[r, "\phi"] \arrow[rr, bend left, "\alpha"] & E' \arrow[r, "\psi"] & E \end{tikzcd}$$

We assume $l \mid n$, otherwise the claim is trivial. However, then we have the contradiction

$$\begin{aligned} \psi((\phi \circ \tau \circ \hat{\phi})(P)) &= (\psi \circ \phi \circ \tau \circ \hat{\phi})(P) = (\alpha \circ \tau \circ \hat{\phi})(P) \\ &= (\tau \circ \alpha \circ \hat{\phi})(P) = (\tau \circ \psi \circ [n])(P) = (\tau \circ \psi)(O) = O \end{aligned}$$

since $\tau \circ \alpha = \alpha \circ \tau$ ($\mathrm{End}(E)$ is commutative). □

For the next statement, we need to establish the relationship between separability of endomorphisms and properties of the endomorphism ring.

Lemma 3.1.16. *Let E be an ordinary curve and $\alpha \in \mathrm{End}(E)$. Then α inseparable if and only if $\alpha \in (p, \pi_E)$.*

Proof. First, consider

$$\mathfrak{b} := \{\beta \in \mathrm{End}(E) \mid \beta \text{ inseparable}\}$$

This is an ideal, as for two inseparable $\beta_1, \beta_2 \in \mathrm{End}(E)$ have that they factor as

$$\begin{tikzcd} E \arrow[r, "\pi_1"] \arrow[rr, bend left, "\beta_i"] & E^{(p)} \arrow[r, "\phi_i"] & E \end{tikzcd}$$

with the p-th power Frobenius $\pi_1 : E \to E^{(p)}$. Now $\beta_1 + \beta_2 = (\phi_1 + \phi_2) \circ \pi_1$ is inseparable, and clearly $\beta\gamma$ is inseparable for $\beta \in \mathfrak{b}$ and $\gamma \in \mathrm{End}(E)$ (just compare separability degrees).

Furthermore, p and π_E are inseparable, so $(p, \pi) \subseteq \mathfrak{b}$. Note that in the imaginary quadratic order $\mathrm{End}(E)$, every prime ideal is maximal. Since $\mathfrak{N}((p, \pi)) = p \perp d(\mathrm{End}(E))$, Prop. 3.1.5 shows that (p, π_E) is prime, and thus $(p, \pi_E) = \mathfrak{b}$ (clearly, $\mathfrak{b} \neq \mathrm{End}(E)$). □

Note now that for an isogeny $\phi : E \to E'$, have

$$\phi \circ \hat{\phi} \circ \Phi(\pi_E) = \frac{\deg(\phi)}{\deg(\phi)} \phi \circ \pi_E \circ \hat{\phi}$$

Comparing inseparability degrees, it follows that $\Phi(\pi_E)$ is totally inseparable as endomorphism on E'. Hence, E' is isomorphic to a curve such that $\Phi(\pi_E)$ becomes the Frobenius endomorphism of that curve. Since we only work with isomorphism classes, we assume from now on that $\Phi(\pi_E)$ is the Frobenius of E'.

Now we can prove that ideal multiplication is compatible with chaining of isogenies. Note that the condition $p \nmid d(\mathcal{O})$ is just equivalent to all curves E with $\mathrm{End}(E) \cong \mathcal{O}$ being ordinary.

Lemma 3.1.17. *Let $\mathcal{O}$ be a quadratic imaginary order with $p \nmid d(\mathcal{O})$ and two integral, invertible ideals $\mathfrak{a}, \mathfrak{b} \leq \mathcal{O}$. Let further E be an Elliptic Curve with $\mathrm{End}(E) \cong \mathcal{O}$. Identifying $\mathrm{End}(E_\mathfrak{a})$ with $\mathcal{O}$ by the canonical isomorphism $\Phi_{E,\mathfrak{a}} : \mathrm{End}(E) \xrightarrow{\sim} \mathrm{End}(E_\mathfrak{a})$, we have*

$$E_{\mathfrak{ab}} \cong (E_\mathfrak{a})_\mathfrak{b} \quad \text{and} \quad \phi_{E,\mathfrak{ab}} = \phi_{E_\mathfrak{a},\mathfrak{b}} \circ \phi_{E,\mathfrak{a}}$$

Proof. Write $\pi \in \mathcal{O}$ for the unique element of $\mathcal{O}$ that maps to the Frobenius of E under the maps $\mathcal{O} \xrightarrow{\sim} \mathrm{End}(E)$ for all E with $\mathrm{End}(E) \cong \mathcal{O}$.

We have $\mathfrak{a} = \tilde{\mathfrak{a}}(p,\pi)^r$ and $\mathfrak{b} = \tilde{\mathfrak{b}}(p,\pi)^s$ with $\tilde{\mathfrak{a}}, \tilde{\mathfrak{b}} \perp (p,\pi)$. It is now the case that

$$\phi_{E,\mathfrak{ab}} = \phi_{E,\tilde{\mathfrak{a}}\tilde{\mathfrak{b}}}^{(p^{r+s})}$$

and

$$\phi_{E_\mathfrak{a},\mathfrak{b}} \circ \phi_{E,\mathfrak{a}} = (\phi_{E_\mathfrak{a},\tilde{\mathfrak{b}}} \circ \pi_r \circ \phi_{E,\tilde{\mathfrak{a}}})^{(p^s)} = (\phi_{E_\mathfrak{a},\tilde{\mathfrak{b}}}^{(q/p^r)} \circ \phi_{E,\tilde{\mathfrak{a}}})^{(p^{r+s})}$$

where $\pi_r : E_{\tilde{\mathfrak{a}}} \to E_{\tilde{\mathfrak{a}}}^{(p^r)}$ is the p^r-th power Frobenius and we assume that $\phi_{E_\mathfrak{a},\tilde{\mathfrak{b}}}$ is defined over $\mathbb{F}_q$. Note that $\phi_{E_\mathfrak{a},\tilde{\mathfrak{b}}}$ is the separable isogeny with kernel $E_\mathfrak{a}[\tilde{\mathfrak{b}}]$ and thus $\phi_{E_\mathfrak{a},\tilde{\mathfrak{b}}}^{(q/p^r)}$ is the separable isogeny with kernel $E_\mathfrak{a}^{(q/p^r)}[\tilde{\mathfrak{b}}] = E_{\tilde{\mathfrak{a}}}[\tilde{\mathfrak{b}}]$. In other words, find

$$\phi_{E_\mathfrak{a},\tilde{\mathfrak{b}}}^{(q/p^r)} = \phi_{E_{\tilde{\mathfrak{a}}},\tilde{\mathfrak{b}}}$$

and so it suffices to show the claim in the case that $\mathfrak{a} = \tilde{\mathfrak{a}}$, $\mathfrak{b} = \tilde{\mathfrak{b}}$ are integral, invertible ideals coprime to (p,π). By Lemma 3.1.16, this means that the isogenies $\phi_{E,\mathfrak{a}}$ and $\phi_{E_\mathfrak{a},\mathfrak{b}}$ are separable.

Having reduced everything to the separable case, it now suffices to show that $\ker(\phi_{E_\mathfrak{a},\mathfrak{b}} \circ \phi_{E,\mathfrak{a}}) = E[\mathfrak{ab}]$. For simplicity of notation, write $\phi = \phi_{E,\mathfrak{a}}$ and $\psi = \phi_{E_\mathfrak{a},\mathfrak{b}}$. Hence, we want to show that $\ker(\psi \circ \phi) = E[\mathfrak{ab}]$.

The crucial point here is that our isomorphism $\mathrm{End}(E) \cong \mathrm{End}(E_\mathfrak{a})$ is given by Φ. Since the identification of $\mathrm{End}(E)$ and $\mathrm{End}(E_\mathfrak{a})$ would hide this, we will be explicit in this part and write

$$i : \mathcal{O} \to \mathrm{End}(E) \quad \text{and} \quad i' : \mathcal{O} \to \mathrm{End}(E')$$

for the isomorphisms. Note that $\Phi \circ i = i'$. We have

$$\begin{aligned}
\ker(\psi \circ \phi) =& \phi^{-1}(\ker \psi) = \phi^{-1}(E'[\mathfrak{a}]) = \phi^{-1}\Big(\bigcap_{\tau \in \mathfrak{a}} \ker(i'(\tau))\Big) \\
=& \bigcap_{\tau \in \mathfrak{a}} \phi^{-1}(\ker(i'(\tau))) = \bigcap_{\tau \in \mathfrak{a}} \ker(i'(\tau) \circ \phi) \overset{(*)}{=} \bigcap_{\tau \in \mathfrak{a}} \ker(\phi \circ i(\tau)) \\
=& \bigcap_{\tau \in \mathfrak{a}} i(\tau)^{-1}(\ker \phi) = \bigcap_{\tau \in \mathfrak{a}} i(\tau)^{-1}(E[\mathfrak{b}]) = \bigcap_{\tau \in \mathfrak{a},\ \rho \in \mathfrak{b}} i(\tau)^{-1}(\ker(i(\rho))) \\
=& \bigcap_{\tau \in \mathfrak{a},\ \rho \in \mathfrak{b}} \ker(\underbrace{i(\rho) \circ i(\tau)}_{= i(\rho\tau) \in i(\mathfrak{ab})}) = E[\mathfrak{ba}]
\end{aligned}$$

The equality at $(*)$ holds, since

$$i'(\tau) = (\Phi_* \circ i)(\tau) = \frac{1}{\deg(\phi)} \phi \circ i(\tau) \circ \hat{\phi} \qquad \square$$

What we have so far is already enough to establish a monoid action

$$\mathfrak{I}(\mathcal{O}) \times \mathrm{Ell}(\mathcal{O}) \to \mathrm{Ell}(\mathcal{O}), \quad \mathfrak{a} \mapsto E_{\mathfrak{a}}$$

where $\mathfrak{I}(\mathcal{O})$ stands for the monoid of integral invertible ideals of $\mathcal{O}$ and

$$\mathrm{Ell}(\mathcal{O}) := \{E \text{ isomorphism class of Elliptic Curves over } \bar{\mathbb{F}}_p \mid \mathrm{End}(E) \cong \mathcal{O}\}$$

denote the set of isomorphism classes of Elliptic Curves with endomorphism ring $\mathcal{O}$.

Next, we investigate the torsion of this action, i.e. for which $\mathfrak{a}$ we have $\mathfrak{a}.E = E$.

Lemma 3.1.18. *Let E be an ordinary curve and $\mathfrak{a}, \mathfrak{b} \leq \mathrm{End}(E)$ two integral, invertible ideals. Then $E_{\mathfrak{a}} \cong E_{\mathfrak{b}}$ if and only if $[\mathfrak{a}] = [\mathfrak{b}] \in \mathrm{Cl}(\mathrm{End}(E))$ are in the same ideal class.*

Proof. First, we show the direction $\Leftarrow$. By assumption, there are $\alpha, \beta \in \mathcal{O}$ such that $\alpha\mathfrak{a} = \beta\mathfrak{b}$. Thus $E_{\alpha\mathfrak{a}} = E_{\beta\mathfrak{b}}$ and it suffices to show that for any Elliptic Curve E and $\alpha \in \mathrm{End}(E)$, have $E_{(\alpha)} \cong E$.

Write $(\alpha) = (p, \pi)^r \mathfrak{a}$ and assume that E is defined over $\mathbb{F}_{p^s}$. Then $(\alpha)(p)^{\lceil r/s \rceil s - r} = (\pi)^{\lceil r/s \rceil}(\alpha')$ since $(p) = (p, \pi)(p, \pi - t)$ and $(p, \pi)^s = (\pi)$ by an easy computation. Furthermore, $\alpha' \notin (p, \pi)$. Now note that for any curve E, have $E_{(\pi)} = E^{(p^s)} \cong E$ and $E_{(p)} \cong E$, where the latter holds, since in the ordinary case, p factors as

$$\begin{tikzcd} E \arrow[r, "\pi_1"] \arrow[rr, bend left, "{[p]}"] & E^{(p)} \arrow[r, "\phi"] & E \end{tikzcd}$$

with the p-th power Frobenius π_1 and ϕ is separable with $\ker(\phi) = E[p] = \ker([p]) \cap \ker(\pi - t)$. Thus we see that $E_{(\alpha)} \cong E_{(\alpha')}$ and can assume wlog that $\alpha = \alpha' \notin (p, \pi)$.

By Lemma 3.1.16, we now see that α is separable, and so clearly $\ker(\alpha) = E[(\alpha)]$. Since $\alpha : E \to E$ is the separable isogeny on E with kernel $E[(\alpha)]$, we see that $E_{(\alpha)} = E/E[(\alpha)] \cong E$.

Now we consider the other direction $\Rightarrow$. Again, write $\mathfrak{a} = \tilde{\mathfrak{a}}(p, \pi)^r$ and assume that E is defined over $\mathbb{F}_{p^s}$. Then we have as before that $\mathfrak{a}(p)^{\lceil r/s \rceil s - r} = (\pi)^{\lceil r/s \rceil}\mathfrak{a}'$ for the ideal $\mathfrak{a}' = \tilde{\mathfrak{a}}(p, \pi - t)^{\lceil r/s \rceil s - r}$. Now clearly $[\mathfrak{a}] = [\mathfrak{a}']$ are in the same ideal class and $\mathfrak{a}' \perp (p, \pi)$. Furthermore, by the direction $\Leftarrow$, have $E_{\mathfrak{a}} \cong E_{\mathfrak{a}'}$. Doing the same with $\mathfrak{b}$, we can assume wlog that $\mathfrak{a} = \mathfrak{a}'$ and $\mathfrak{b} = \mathfrak{b}'$ are ideals coprime to (p, π).

Therefore, the isogenies $\phi_{E,\mathfrak{a}}$ and $\phi_{E,\mathfrak{b}}$ are separable. Write $E' := E_{\mathfrak{a}} = E_{\mathfrak{b}}$. Choose $N > 0$ such that $[N]^{-1}(E[\mathfrak{a}]) \supseteq E[\mathfrak{b}]$. Now the isogeny $[N] \circ \phi_{E,\mathfrak{a}}$ factors through $\phi_{E,\mathfrak{b}}$, i.e. we get a commutative diagram

$$\begin{tikzcd} & E' \arrow[dr, "{[N]}"] & \\ E \arrow[ur, "\phi_{E,\mathfrak{a}}"] \arrow[dr, "\phi_{E,\mathfrak{b}}"'] & & E' \\ & E' \arrow[ur, "\psi"'] & \end{tikzcd}$$

for some endomorphism $\psi : E' \to E'$. Clearly the isogenies $[N]$ and ψ are given by the ideals (N) resp. (ψ), and so we find

$$(N)\mathfrak{a} = (\psi)\mathfrak{b}$$

and the claim follows. □

Now we have proven almost everything we need. The final ingredient, from which it will then follow that the class group action is transitive, is a theorem of Tate. Since it uses much of the theory on general abelian varieties, we will present it without proof here. For a proof, the reader is referred to the work of Tate [32].

Theorem 3.1.19 (Isogeny theorem). *Let E, E' be Elliptic Curves defined over $\mathbb{F}_q$. Then there is an isogeny $E \to E'$ if and only if $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$.*

Note that this condition is also equivalent to $\mathrm{End}(E) \otimes \mathbb{Q} \cong \mathrm{End}(E') \otimes \mathbb{Q}$ or that the q-th power Frobenius endomorphisms have the same trace.

Theorem 3.1.20. *Let $\mathcal{O}$ be an imaginary quadratic order with $p \nmid d(\mathcal{O})$. Then there is a free and transitive group action*

$$\mathrm{Cl}(\mathcal{O}) \times \mathrm{Ell}(\mathcal{O}) \to \mathrm{Ell}(\mathcal{O}), \quad ([\mathfrak{a}], E) \mapsto E_{\mathfrak{a}}$$

where $\mathfrak{a}$ is an integral, invertible ideal representative of the ideal class $[\mathfrak{a}]$.

Proof. Well-definedness and freeness follow from all the previous lemmas. So it is left to derive the transitivity from Thm 3.1.19. Let E and E' be curves in $\mathrm{Ell}(\mathcal{O})$. Clearly, we then have $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$ and so there is a separable isogeny $\phi : E \to E'$. Everything we have to show is that $\phi = \phi_{E,\mathfrak{a}}$ for some ideal $\mathfrak{a} \leq \mathcal{O}$. Note that we can multiply $\mathfrak{a}$ by (p) and divide by π, and thus achieve that ϕ is separable.

Here we use the same approach as in [33, Thm 4.5]. In particular, we want to consider the problem locally at primes l. The usual way to achieve this is to consider the l-adic Tate module defined as the inverse limit

$$T_l E := \lim_{n} E[l^n]$$

Note that this is an $\mathcal{O}_l := \mathcal{O} \otimes \mathbb{Z}_l$-module. Furthermore, the isogeny ϕ induces a map

$$\phi_l : T_l E \to T_l E', \quad (P_n)_n \mapsto (\phi P_n)_n$$

By our choice of the canonical isomorphism $\mathrm{End}(E) \cong \mathcal{O} \cong \mathrm{End}(E')$, this becomes an $\mathcal{O}_l$-module homomorphism. Extending it linearly, we get the map

$$\phi_l : T_l E \otimes_{\mathbb{Z}_l} \mathbb{Q}_l \to T_l E' \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$$

We can now consider the $\mathcal{O}_l$-module $M := \phi_l^{-1}(T_l E') \subseteq T_l E \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$. Note that this is the only time we use the assumption $\mathrm{End}(E) \cong \mathrm{End}(E')$, which yields here that M is an $\mathcal{O}_l$-module.

The module M contains $T_l E$ and furthermore, $T_l E$ has finite index in M. Therefore M is a $\mathcal{O}_l$-submodule of $l^{-n} T_l E$ for some n.

So we see that M is a free rank-1 module over $\mathcal{O}_l$, and hence there is an element $\alpha_l \in \mathcal{O}_l$ with

$$\alpha_l M = T_l E$$

Note that we can write $\alpha_l = a \otimes l^n b$ with $a \in \mathcal{O}$ and $b \in \mathbb{Z}_l^*$. Then also $(a l^n) M = T_l E$ and thus we can assume wlog that $\alpha_l = a l^n \in \mathcal{O}$.

Now it is left to establish the connection between $\ker(\phi)$ and M. This is done by the map

$$\phi_l^{-1}(T_l E') = M \to \ker(\phi)_{(l)}, \quad \frac{1}{l^m}(P_n)_n \mapsto P_m$$

where an element of $T_l E'$ is $(P_n)_n$ with $P_n \in E[l^n]$ such that $[l]P_{n+1} = P_n$. Further

$$\ker(\phi)_{(l)} := \{P \in \ker(\phi) \mid [l]^n P = O \text{ for some } n \geq 0\}$$

is the power-of-l torsion part of $\ker(\phi)$, or equivalently the localization at the prime ideal (l) as $\mathbb{Z}$-module.

First, note that the map is well-defined, as for an element $1/l^m(P_n)_n$ in the domain, we have by assumption

$$\frac{1}{l^m}\phi_l((P_n)_n) = \frac{1}{l^m}(\phi(P_n))_n \in T_l E'$$

and thus $\phi(P_m) = O$, i.e. $P_m \in \ker(\phi)$.

Clearly, the map is also a morphism of $\mathcal{O}$-modules, where $\ker(\phi)_{(l)}$ becomes an $\mathcal{O}$-module in the obvious way.

It is also surjective, since for $P \in \ker(\phi)_{(l)}$ of order $\mathrm{ord}(P) = l^m$, we can lift it to an element $(P_n)_n$ with $P_m = P$. Then clearly $1/l^m(P_n)_n \in M$ with image P.

Finally, note that for $1/l^m(P_n)_n \in M$ have $P_m = O$ if and only if $P_0 = ... = P_m = O$, in which case we have that

$$1/l^m(P_n)_n = (P_{n+m})_n \in T_l E$$

Thus the kernel of above map is $T_l E$ and we get an isomorphism of $\mathcal{O}$-modules

$$\ker(\phi)_{(l)} \cong M/T_l E$$

Now let $\mathfrak{a} \leq \mathcal{O}$ be the invertible ideal such that $\mathfrak{a}\mathcal{O}_{\mathfrak{l}} = (\alpha_l)_{\mathfrak{l}}$ for every prime ideal $\mathfrak{l}$ under a prime number l (the α_l are the element from above with $\alpha_l M = T_l E$). This is possible by Lemma 3.1.6, as only finitely many $(\alpha_l) \neq (1)$ (namely for those l with $l \mid \deg(\phi)$).

Then for each primes l, we have

$$\ker(\phi)_{(l)} = \{P \in E_{(l)} \mid \alpha_l(P) = O\} = \{P \in E_{(l)} \mid \forall \alpha \in \mathfrak{a} : \alpha(P) = O\}$$

where again $E_{(l)}$ is the power-of-l torsion part of the group E. Thus $\ker(\phi) = E[\mathfrak{a}]$. □

A similar class group action exists in many other cases, since it is really founded in the theory of abelian varieties, see [33]. Notable examples are the CSIDH class group action for supersingular curves defined over $\mathbb{F}_p$ (see [7]), its generalization to so-called oriented curves (see [11]), and the very classical class group action of Elliptic Curves with complex multiplication (over $\mathbb{C}$). More concretely, if we consider an order $\mathcal{O}$ in a quadratic imaginary number field and write $\mathrm{Ell}(\mathcal{O})$ for the set of (isomorphism classes of) curves over $\mathbb{C}$ with endomorphism ring $\mathcal{O}$ (these are said to have *complex multiplication*), then there is a free and transitive class group action

$$\mathrm{Cl}(\mathcal{O}) \times \mathrm{Ell}(\mathcal{O}) \to \mathrm{Ell}(\mathcal{O}), \quad ([\mathfrak{a}], E) \to E/E[\mathfrak{a}]$$

where we choose $\mathfrak{a}$ to be an integral ideal representative of $[\mathfrak{a}]$. Note that for ideals $\mathfrak{a} \perp (p, \pi)$, this is analogous to our action defined above. However, since the Frobenius has trivial kernel, one needs some addition in the finite field case.

Note that one can still keep the simpler definition

$$\mathrm{Cl}(\mathcal{O}) \times \mathrm{Ell}(\mathcal{O}) \to \mathrm{Ell}(\mathcal{O}), \quad ([\mathfrak{a}], E) \to E/E[\mathfrak{a}]$$

also in the finite field case, if we require $\mathfrak{a}$ to be an (integral) ideal representative of $[\mathfrak{a}]$ that is coprime to (p, π). Clearly, every ideal class has such a representative, since we can multiply with the principal ideal $(p) = (p, \pi)(p, \pi - t)$ and divide out the principal ideal $(\pi) = (p, \pi)^s$. However, some sources do not explicitly mention that $\mathfrak{a}$ must be chosen coprime to (p, π), which caused me some confusion at the beginning.

3.1.3 Vulcanos

Once we have the class group action, we can derive a lot of information about the structure of the ordinary part of an isogeny graph.

Definition 3.1.21. For $l > 0, d \geq 0$, a graph G is called *l-vulcano of depth d*, if its vertices can be partitioned into a set C (the "crater") and a set L (the "lava flows") such that

- $G[C]$ is either a single vertex (possibly with one or two loops), two connected vertices or a cycle of at least two vertices[3]
- $G[V]$ is a forest of complete l-ary trees of depth d
- Every vertex $v \in C$ is connected to the roots of $l + 1 - \deg_{G[C]}(v)$ trees in $G[L]$

In particular, every vertex in G except the leaves of the trees has degree $l + 1$.

The term "vulcano" was introduced by [20], after Kohel had mostly determined the structure of ordinary connected components in his PhD thesis.

Theorem 3.1.22. *Let G be a connected component of $\Gamma_l(\mathbb{F}_q)$. Suppose that G is ordinary, i.e. its vertices are (isomorphism classes of) ordinary curves. Then G is an l-vulcano. Further, we have*

- *All curves on the crater have the same endomorphism ring $\mathcal{O}$ with $l \nmid [\mathcal{O}_{\mathcal{O}\otimes\mathbb{Q}} : \mathcal{O}]$.*
- *All curves on the i-th tree level of a lava flow have the endomorphism ring $\mathbb{Z} + l^i\mathcal{O}$.*
- *The size of the crater is the order of $\mathfrak{l}_1$ in $\mathrm{Cl}(\mathcal{O})$, where $(l) = \mathfrak{l}_1\mathfrak{l}_2$ in $\mathcal{O}$, or 1 if l is inert in $\mathcal{O}$.*

Proof. This follows from the class group action and the description of the class group of quadratic imaginary orders 3.1.9. For the remaining details, we refer the reader to Kohel's thesis [22, Prop. 23]. □

We remark that the crater of a vulcano is a single vertex with a loop, if (l) is inert in $\mathcal{O}$. Furthermore, the crater consists of two connected vertices, if (l) is ramified in $\mathcal{O}$, and is either a vertex with double loop or a cycle, if (l) splits.

3.2 The supersingular case

After studying the ordinary connected components of the l-isogeny graph $\Gamma_l(\mathbb{F}_q)$, we now come to the supersingular component(s). First, note that all supersingular j-invariants are defined over $\mathbb{F}_{p^2}$, and so we will assume $q = p^2$ for this section.

[3] A cycle of two vertices shall be two vertices with a double edge.

In the supersingular setting, the endomorphism ring is now non-commutative. There still exists a non-commutative analogue of the class group action, but using that structure is significantly harder. Mainly, because the theory of quaternion algebras is more complicated, and its class group structure is less studied.

Instead, there is the famous result of Pizer, which states that supersingular isogeny graphs (i.e. the supersingular part of $\Gamma_l(\mathbb{F}_q)$) are so called Ramajuan graphs, that is have excellent expander properties. We will introduce this result in this section, but without proof.

Definition 3.2.1. A d-regular graph G is called ϵ-expander, if the eigenvalues $\lambda_1 > ... > \lambda_n$ of its adjacency matrix satisfy

$$|\lambda_2|, |\lambda_n| \leq (1 - \epsilon)d$$

In the literature, expander graphs are often defined by the use of the expansion ration

$$h(G) := \min_{S \subseteq V,\ \#S \leq \frac{n}{2}} \frac{\#\partial S}{\#S}$$

of a graph $G = (V, E)$. Here ∂S is the edge boundary, i.e. the set of edges between a point in S and a point in $V \setminus S$.

The connection between those two definitions is then given by the Cheeger-inequality

Proposition 3.2.2. *Let G be a d-regular graph such that its adjacency matrix has eigenvalues $\lambda_1 > ... > \lambda_n$. Then*

$$\frac{d - \lambda_2}{2} \leq h(G) \leq \sqrt{2d(d - \lambda_2)}$$

Proof. See e.g. [9]. □

This inequality only correlates the so-called spectral gap $d - \lambda_2$ with $h(G)$, and does not bound $|\lambda_2|$. In many cases, bounds on the spectral gap or expansion ration already suffice to show properties of expanders. Because of this, expanders are usually defined as graphs for which only λ_2 or $h(G)$ are bounded. Our definition 3.2.1 is then sometimes called “two-sided expander”. However, we will never use one-sided expanders in this work, hence the above definition shall be sufficient.

The nice thing about the expansion ratio is that it gives more intuition on what the expander property means. In particular, an expander graph is densely connected, i.e. by deleting a small number of edges, it is impossible to make the graph split into two (or more) connected components of relatively large size.

Definition 3.2.3. A connected d-regular graph is called Ramajuan, if

$$|\lambda_2|, |\lambda_n| \leq 2\sqrt{d - 1}$$

where $\lambda_1 > ... > \lambda_n$ are again the eigenvalues of the adjacency matrix.

It is known that the bound $2\sqrt{d-1}$ is asymptotically optimal, i.e. for sufficiently large n, all d-regular graphs of n vertices have $\lambda_2 \geq 2\sqrt{d-1} - \epsilon$. In that sense, we can say Ramajuan graphs are graphs with asymptotically optimal expansion properties.

One of the main properties of expander graphs is random walks on them mix rapidly. That is, the final vertex of relatively short random walks is distributed almost uniformly among all vertices.

Theorem 3.2.4. *Let $G = (V, E)$ be a d-regular ϵ-expander graph and $v \in V$ a vertex. Then the distribution of the final vertex of a random walk starting from v of length t is close to uniform, in particular, the ℓ_2-statistical distance is bounded by $(1 - \epsilon)^t$.*

For a proof of this theorem, see e.g. Thm 3.3 in this excellent survey on expander graphs [21]. Note that expander graphs used in cryptography are usually of exponential size, so this theorem says that a random walk of polynomial length already reaches all vertices of the graph.

Now we come to the anticipated result, that supersingular isogeny graphs are expander graphs.

Definition 3.2.5. The *supersingular l-isogeny graph over $\mathbb{F}_{p^2}$* is the subgraph of $\Gamma_l(\mathbb{F}_{p^2})$ induced by all (isomorphism classes of) supersingular curves over $\mathbb{F}_{p^2}$.

Since the supersingular l-isogeny graph is disconnected from the rest of $\Gamma_l(\mathbb{F}_{p^2})$, we see that it is an $(l+1)$-regular graph. We also know its size exactly, which directly follows from a classical result on the number of supersingular curves over $\mathbb{F}_{p^2}$.

Proposition 3.2.6. *For $p \geq 5$, there are exactly*

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

supersingular Elliptic Curves over $\mathbb{F}_{p^2}$.

For a proof of this statement, see e.g. [29, Thm V.4.1].

In [26], Pizer has now shown that

Theorem 3.2.7. *The supersingular l-isogeny graph is Ramajuan.*

This means that there is a huge difference between the ordinary and supersingular graphs. For example, there is always a path of length $O(\log(p))$ between two curves in the supersingular graph, but in the ordinary graph, such a path does not exist in many cases. We will try to quantify this in the last section. The idea of our research is to utilize these differences in order to find random, supersingular curves.

3.3 Modular polynomials

If we want to work computationally with isogeny graphs, we need a way to explicitly compute them. The simplest way to find the m-isogeny neighbors of a curve E is to compute $E[m]$ and find the order-m-subgroups. While this works in many cases, it can happen that the torsion group $E[m]$ only lies in an extension of $\mathbb{F}_q$ of degree $O(m^2)$, in which it is very costly to work. Furthermore, there are many other applications where a torsion-based approach does not work at all.

In the ordinary case, the class group action might be also used to compute neighbors in the l-isogeny graph, provided we know the endomorphism ring of the start curve. However, finding the endomorphism ring is a hard problem in itself, and thus this method is not really practical. Furthermore, this does not work in the supersingular setting.

One solution to this problem is given by modular curves, which give a very useful algebraic structure to the l-isogeny graph. In particular, the existence of a nontrivial l-isogeny between curves is an algebraically closed condition, i.e. is given by an algebraic curve.

The classical way to study this is by using the theory of modular forms. Since this is out of the scope of this work, we refer to [13, §11] for an introduction of the topic. The basic result is the following.

Theorem 3.3.1. *For $m \geq 2$ there is an irreducible and monic polynomial*

$$\Phi_m(X, Y) \in \mathbb{Z}[X, Y]$$

such that for Elliptic Curves E, E' defined over $\mathbb{C}$, there is a cyclic m-isogeny $E \to E'$ if and only if $\Phi_m(j(E), j(E')) = 0$.

This polynomial is called the *(classical) modular polynomial of level m*. A proof of this theorem is e.g. given in [13, Thm 11.18]. A few corollaries of this theorem can easily be inferred.

Corollary 3.3.2. *Let $m \geq 2$. Then we have*

- *Φ_m is symmetric, i.e. $\Phi_m(X, Y) = \Phi_m(Y, X)$.*
- *Φ_m has degree $\psi(m)$ (as polynomial in X), where ψ is the Dedekind ψ-function*

$$\psi(m) = m \prod_{p \mid m} 1 + \frac{1}{p}$$

Proof. The first statement follows from the existence of the dual isogeny. For the second statement, note that for each Elliptic Curve E over $\mathbb{C}$, the degree of $\Phi_m(X, j(E))$ is the number of curves E' with an m-isogeny $E \to E'$, which is equal to the number of cyclic subgroups $G \leq E \cong (\mathbb{R}/\mathbb{Z})^2$ of size m. By the Chinese Remainder theorem, this is a multiplicative function, and for a prime power $m = p^k$, the number is

$$\begin{aligned}
&\#\big\{G \leq (\mathbb{Z}/m\mathbb{Z})^2 \;\big|\; \#G = m\big\} \\
=&\#\big\{\langle(1, \alpha)\rangle \;\big|\; \alpha \in \mathbb{Z}/m\mathbb{Z}\big\} + \#\big\{\langle(\alpha, 1)\rangle \;\big|\; \alpha \in (\mathbb{Z}/m\mathbb{Z}) \setminus (\mathbb{Z}/m\mathbb{Z})^*\big\} \\
=&p^k + \#\big\{\langle(\alpha, 1)\rangle \;\big|\; \alpha \in p(\mathbb{Z}/m\mathbb{Z})\big\} = p^k + p^{k-1} \\
=&m\left(1 + \frac{1}{p}\right)
\end{aligned}$$

□

Since we are mainly interested in the case of finite fields, we have to show that the modular polynomial behaves well under reductions mod p. This theory relies on Hensel lifting, and has been explored by [14].

Lemma 3.3.3. *Let $f \in \mathcal{O}_K[X]$ be a polynomial for some number field K with a prime $\mathfrak{p}$. If $f(X) \mod \mathfrak{p} \in \mathbb{F}_q[X]$ has a root α, then f has a root in $\mathcal{O}_L$ that reduces to α modulo a prime over $\mathfrak{p}$ for some finite field extension L/K.*

Proof. Follows by Hensel's Lemma. □

The next lemma allows us to lift curves connected by an isogeny over $\mathbb{F}_q$ to $\mathbb{C}$. This is very similar to the well-known lifting lemma of Deuring, which is about lifting a curve together with an endomorphism.

Lemma 3.3.4. *Let E and E' be curves over $\mathbb{F}_q$ and $\phi : E \to E'$ a cyclic m-isogeny. Then there exist curves E_0, E_0' with j-invariant in $\mathcal{O}_K$ for some number field K with a prime $\mathfrak{p}$ over $p = \mathrm{char}(K)$ and an isogeny $\phi_0 : E_0 \to E_0'$ such that*

$$\tilde{E}_0 = E, \; \tilde{E}_0' = E' \quad \textit{and} \quad \tilde{\phi}_0 = \phi$$

where $\tilde{\cdot}$ is the reduction modulo $\mathfrak{p}$.

Proof. This proof is somewhat technical, but the basic idea is simple. Having an isogeny $E \to E'$ is equivalent to the fact that the polynomial of the isogeny satisfy the defining equations of E'. In other words, we have to lift polynomials over $\mathbb{F}_q$ to a number field such that certain equations are satisfied. This however can be done by Hensel's lemma. The only difficulty is that we have to lift the correct coefficient in the correct order, to resolve all required dependencies.

Consider some arbitrary lift E_0 and E_0' of E resp. E' to a number field K such that $j(E_0), j(E_0') \in \mathcal{O}_K$. Assume that E_0' is defined by a homogeneous polynomial $f = Y^2Z - X^3 - AXZ^2 - BZ^3 \in \mathcal{O}_K[X, Y, Z]$. Finally, assume[4] $\phi = [u : Yv : w]$ with polynomials $u, v, w \in \mathbb{F}_q[X]$ and choose an arbitrary lift $v_0, w_0 \in \mathcal{O}_K[X]$ of v resp. w. Hence the coefficients $u^{(0)}, ..., u^{(n)}$ of $u \in \mathbb{F}_q[X]$ are a root of

$$f(\sum T_i X^i, Yv_0, w_0) = \sum_i a_i(T_0, ..., T_n)X^i \in \mathcal{O}_K[X][T_i]$$

modulo $\mathfrak{p}$. Note that the coefficient $a_j(T_0, ..., T_n)$ of X^j in $(\sum_i T_i X^i)^3$ contains the monomial $T_0^2 T_j$, and wlog we have chosen the lifts of A, B such that also the coefficient in $f(\sum T_i X^i, Yv, w)$ does. Furthermore, a_j is in $\mathcal{O}_K[T_0, ..., T_j]$, i.e. only depends on $T_0, ..., T_j$.

wlog $u_0 \neq 0$, otherwise we can just move E' in x-direction by some element in $\mathfrak{p}$, which preserves $\tilde{E}_0' = E'$.

We know that $u^{(0)}$ is a root of a_0 modulo $\mathfrak{p}$, and so Lemma 3.3.3 shows that there is a lift $u_0^{(0)}$ of $u^{(0)}$ in some number field L_0/K with $a_0(u_0^{(0)}) = 0$. Since $u_0^{(0)} \neq 0$, we see that $a_i(u_0^{(0)}, ..., u_0^{(i-1)}, T_i)$ contains the monomial T_i, and so applying the lemma inductively, we also find lifts $u_0^{(1)}, ..., u_0^{(n)} \in \mathcal{O}_L/K$ with $a_i(u_0^{(0)}, ..., u_0^{(i)}) = 0$. In other words, we found a lift u_0 of u in $\mathcal{O}_L[X]$ such that $f(u_0, Yv_0, w) = 0$. Now we can set $\phi_0 = [u_0 : Yv_0 : w_0] : E_0 \to E_0'$ and the claim follows. □

Using a little bit more Hensel lifting (don't worry, the ugly part is done), we now can pull down the properties of Φ_m to finite fields.

Proposition 3.3.5. *For $m \geq 2$ and Elliptic Curves E and E' over $\mathbb{F}_q$, have $\Phi_m(j(E), j(E')) = 0 \in \mathbb{F}_q$ if and only if there is a cyclic m-isogeny $E \to E'$.*

Proof. First, consider the direction $\Leftarrow$. Here the previous Lemma shows that we can lift the situation to m-isogeneous curves E_0 and E_0' over a number field K, and so have by Prop. 3.3.1 that

$$\Phi_m(j(E_0), j(E_0')) = 0$$

Furthermore we know that $j(E_0), j(E_0') \in \mathcal{O}_K$, and so we clearly have for the reduction modulo $\mathfrak{p}$ that

$$\Phi_m(j(E), j(E')) \equiv \Phi_m(j(E_0), j(E_0')) \equiv 0 \mod \mathfrak{p}$$

Now we show the direction $\Rightarrow$. We have $\Phi_m(j(E), j(E')) = 0 \in \mathbb{F}_q$, thus there is a number field K with a prime $\mathfrak{p}$ over $p = \mathrm{char}(\mathbb{F}_q)$ and $x, y \in \mathcal{O}_K$ such that

$$\Phi_m(x, y) \equiv 0 \mod \mathfrak{p} \quad \text{and} \quad x \equiv j(E),\ y \equiv j(E') \mod \mathfrak{p}$$

Now we can again use Lemma 3.3.3 to find x' in the completion $K_\mathfrak{p}$ such that $x' \equiv x \mod \mathfrak{p}$ and $\Phi_m(x', y) = 0 \in K_\mathfrak{p}$. Since x' is a root of $\Phi_m(X, y)$, it is algebraic and thus an algebraic integer. So there is a number field K' with a prime $\mathfrak{p}'$ over $\mathfrak{p}$ such that $x', y \in K'$ and $x' \equiv j(E)$, $y \equiv j(E')$ modulo $\mathfrak{p}'$. In particular, there are curves E, E' over K' with j-invariants x' resp. y, and thus by Prop. 3.3.1, there is a cyclic m-isogeny $E \to E'$. Therefore, there is also an m-isogeny between the curves $\tilde{E}$ and $\tilde{E}'$, which are the reductions of E resp. E' modulo $\mathfrak{p}'$. □

[4] It is a simple consequence of the geometry of Elliptic Curves that every isogeny is of such a form.

Some properties however cannot be transfered to the finite field case. For example, in the finite field case, Φ_m might not be irreducible anymore. In fact, it is easy to see that

$$\Phi_p(X, Y) \equiv -(X^p - Y)(Y^p - X) \mod p$$

since the only p-isogenies over a field of characteristic p are the Frobenius and its conjugate.

The modular polynomial is an indispensable tool when doing computations on the isogeny graph. In particular, when combined with an algorithm to factor polynomials over $\mathbb{F}_q$, it allows us to compute all the neighbors of a curve E in the l-isogeny graph. For example Sutherland's supersingular test [31] uses modular polynomials for walks in the isogeny graph, and distinguishes ordinary and supersingular curves by the structure of their isogeny graph neighborhoods. Another example is Shoof's algorithm [28] for counting $\mathbb{F}_q$-rational points on a curve, which also fundamentally relies on modular polynomials.

Therefore, computing modular polynomials is an important task. The most classical approach is to mimic to proof of Thm 3.3.1, i.e. view Elliptic Curves as lattices over $\mathbb{C}$ and compute the Fourier coefficients of the j-function. However, one main problem is that the coefficients in the modular polynomial become very large very fast. For example, Φ_5 has already the constant coefficient

$$141359947154721358697753474691071362751004672000$$

In many cases, we only need the value of Φ_m modulo a prime p, and thus other algorithms can easily be faster. A whole line of work tries to use isogeny graphs over finite fields to find such an algorithm, see e.g. [4] and [3]. Using the Chinese Remainder theorem, these algorithms can also be used to find Φ_m over $\mathbb{C}$ by collecting information modulo many different primes.

Chapter 4

Isogeny-based cryptography

Chapter 5

Generating supersingular curves

Since the advent of the SIDH scheme [17], supersingular curves are at the center of attention in isogeny-based cryptography. The most important hard problem in that context is the *(supersingular) isogeny path problem*, defined as finding an isogeny of smooth degree (or sometimes power-l degree) between two given supersingular curves. This problem is also equivalent [16] to the supersingular endomorphism ring problem, that is to compute a basis of the endomorphism ring of a supersingular curve. In many cryptographic application, it is helpful or even required that supersingular curves used to instantiate the scheme do not come with a trapdoor that might simplify solving one of these problems. More concretely, we want to instantiate the scheme with a random supersingular curve, for which nobody knows the endomorphism ring or a smooth isogeny to a previously fixed curve. Hence it is an important question how we can compute a random supersingular curve in a way that the computation does not reveal such information - or more precisely, that it is impossible to efficiently compute this information given the randomness used for finding the curve.

Up to now, the only attempt at solving this problem is in [2], who proposed several highly interesting ideas. However, each of them currently has some major obstacle that must be overcome before one can get a practical method. Three of the five presented ideas are based on defining polynomial systems whose roots are (overwhelmingly) supersingular, and then try to find a random root of the system. The main problem with those methods is that the considered polynomials are too large to work with efficiently. Furthermore, current tools to solve polynomial systems like resultants and in particular Groebner bases are often impractical even for moderately sized inputs.

Our research focused on the second idea of [2], which is based on modular polynomials. We found answers to some of the questions in the paper, as well as a variation of the method that has properties that might help with efficiently computing it. However, the algorithm is still not practical. In this chapter, we present those results, after first discussing some naive approaches.

5.1 Naive and classical approaches

First, we have a look at some simple approaches to the problem, to get a feeling for the challenges.

Random Sampling It is a folklore knowledge that all supersingular curves over $\bar{\mathbb{F}}_p$ have a j-invariant in $\mathbb{F}_{p^2}$, i.e. are isomorphic to a curve defined over $\mathbb{F}_{p^2}$. Hence, the most naive approach is to sample random $j \in \mathbb{F}_{p^2}$ and check if they define supersingular curves. It is clear that this algorithm does not reveal any information about isogenies or the endomorphism ring of the found curve, unless the information can be efficiently computed from the curve itself (in which case the cryptographic schemes are broken anyway). However, the number of supersingular curves over $\mathbb{F}_{p^2}$ is only approximately $p/12$, which means that the expected number of required samples (and supersingularity checks) is about $12p$, which is exponential in $\log(p)$.

Random Walk Opposed to that we have the way supersingular curves are currently generated: As discussed in Section 3.2, a random walk of length polynomial in $\log(p)$ in the supersingular l-isogeny graph is sufficient to find an (almost) uniformly distributed supersingular curve. As long as we know one fixed curve to start with, this is quite efficient. However, clearly this computation reveals a power-l degree isogeny to the fixed starting curve, which is exactly what we want to avoid.

Polynomial with supersingular roots An idea that is more similar to what we will do next, is to use the following theorem from [29, Thm V.4.1].

Theorem 5.1.1. *Let p be an odd prime and $m = (p-1)/2$. Then the Elliptic Curve given by $y^2 = x(x-1)(x-\lambda)$ over $\mathbb{F}_q$ is supersingular, if and only if*

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

In other words, we just have to find a random root of the polynomial $H_p(X)$, which then gives rise to a random supersingular curve. The obvious problem here is again that p is exponential in the input size $\log(p)$, thus the polynomial $H_p(X)$ also has exponential degree, and it is not clear if we can find a random root efficiently. In fact, the first idea in [2] is use a method similar to the Newton-Raphson algorithm to find a random root. However, that seems to be only moderately successful.

5.2 GCDs of modular polynomials

The second idea of [2], which we want to study in more detail, is based on the following intuition:

Since the supersingular isogeny graph is an expander, it is relatively likely that there is an n-isogeny between two random curves E and E' (for a fixed n). On the other hand, this is much less likely in the ordinary case. We expect that this still applies when we take not two random curves, but a random curve E and its Frobenius conjugate $E^{(p)}$, i.e. the curve with j-invariant $j(E)^p$. Hence, the roots of

$$\Phi_n(X, X^p)$$

should contain a relatively large fraction of supersingular roots over $\mathbb{F}_{p^2}$. More concretely, from the OSDIH class group action, see e.g. [10, Thm 4.3], we can derive the following corollary.

Corollary 5.2.1. *There are $\Theta(\sqrt{mp})$ supersingular curves E over $\mathbb{F}_{p^2}$ with an m-isogeny to $E^{(p)}$.*

Since it has degree np, it has in total np roots in $\bar{\mathbb{F}}_p$, which means that the fraction of supersingular roots is still exponentially small. Of course, it might be more interesting to find the number of roots over $\mathbb{F}_{p^2}$, but this turns out to be somewhat tricky. Another obvious problem with this polynomial is that it has exponential degree, so it is not clear how to compute its roots.

To tackle these two problems, [2] proposed to instead take the polynomial

$$f_{p,n,m} = \gcd(\Phi_n(X, X^p), \Phi_m(X, X^m))$$

The idea to find a root of this is to take a non-square $d \in \mathbb{F}_p$ and its square root $\delta \in \mathbb{F}_{p^2}$. Then $(a + b\delta)^p = a - b\delta$ and so we can equivalently look for $x, y \in \mathbb{F}_p$ such that

$$\Phi_n(x + \delta y, x - \delta y) = \Phi_m(x + \delta y, x - \delta y) = 0$$

Hence, we look for a root in $\mathbb{F}_p$ of the polynomial

$$\mathrm{res}_Y(\Phi_n(X + \delta Y, X - \delta Y), \Phi_m(X + \delta Y, X - \delta Y))$$

However, note that a solution to this system will have an endomorphism of degree nm. If we choose both n and m of size polynomial in $\log(p)$, this means the endomorphism ring has polynomial discriminant, which is a weakness (in particular, there are only polynomially many curves with such an endomorphism ring). Hence, at least one of n resp. m has to be of super-polynomial (or better exponential) degree in $\log(p)$.

This of course makes it very hard to even write down or compute some properties of Φ_n. Hence, we will study a slight modification and focus on the case that $n = l^e$ is a prime power.

5.2.1 The prime power case

First of all, we describe how the assumption $n = l^e$ might help us to work with Φ_n. Note that $\Phi_{l^e}(j(E), j(E'))$ is equivalent to there being a cyclic l^e-isogeny between E and E'. If we relax this to just any l^e-isogeny and note that an l^e-isogeny is equal to an l-isogeny path of length e, we can instead work with the condition

$$\exists x_1, ..., x_{e-1} : \ \Phi_l(x, x_1) = \Phi_l(x_1, x_2) = ... = \Phi_l(x_{e-1}, y)$$

In other words, we look for a solution to the polynomial system

$$F_{p,m,l^e} := \langle \Phi_m(x, y), \Phi_l(x, x_1), ..., \Phi_l(x_{e-1}, y) \rangle$$

The other advantage of this approach is that every supersingular curve E has an l^e-isogeny to $E^{(p)}$ if $e \geq O(\log_l(p))$. This follows from our results on expander graphs. More concretely, Thm 3.2.7 shows that the supersingular l-isogeny graph over $\mathbb{F}_{p^2}$ is an ϵ-expander for

$$\epsilon = 1 - \frac{2\sqrt{d-1}}{d} = 1 - 2\frac{\sqrt{l}}{l+1} \geq 1 - \frac{2}{\sqrt{l}}$$

Thus, a random walk of length at least

$$-\log_{2/\sqrt{l}}(p/12) = O(\log_l(p))$$

has a nonzero probability of ending in any fixed vertex, by Thm 3.2.4. Note further that for moderately large l, the constant approaches 2, i.e. we can choose $e \approx 2\log_l(p)$.

This leaves us with a polynomial system of $O(\log(p))$ unknowns and equations, which at least can be explicitly written down. Now we want to study how big the fraction of supersingular roots is. However, since by our choice of $e = \Theta(\log_l(p))$, we can assume that all supersingular j-invariants are roots of $\Phi_{l^e}(X, X^p)$, and so the number of supersingular roots is $O(\sqrt{mp})$, again by Corollary 5.2.1. Hence, we want to find instances of l, e and m such that above system has at most $O(\mathrm{poly}(\log(p)))$ ordinary roots.

5.2.2 Studying the number of ordinary roots

To estimate the number of ordinary roots, we will of course use the class group action. Thus, we need a bound on the class number of quadratic imaginary orders. The next theorem puts together some classical results, in particular the famous class number formula.

Theorem 5.2.2. *Let $\mathcal{O}$ be an order in a quadratic imaginary number field with discriminant $D = d(\mathcal{O})$. Assuming GRH, we then have for the class number $h(D) := \#\mathrm{Cl}(\mathcal{O})$ that*

$$\Theta\left(\frac{\sqrt{|D|}}{(\log\log|D|)^2}\right) \leq h(D) \leq \Theta\left(\sqrt{|D|}\log|D|\right)$$

Proof. wlog assume that $d_K := d(\mathcal{O}_K) < -4$. Then the Dirichlet class number formula has the form

$$h(\mathcal{O}_K) = \frac{\sqrt{|d_K|}}{2\pi}L(1,\chi)$$

where

$$\chi : \mathbb{Z} \to \mathbb{C}, \quad m \mapsto \left(\frac{d}{m}\right)$$

is a real Dirichlet character and $L(s,\chi)$ is its Dirichlet L-function. This follows from the general class number formula, as e.g. presented in [25, Korollar VII.5.11].

In [23, Thm 1], it was proven under GRH that $L(1,\chi) \geq \Theta(\sqrt{|d_K|}\log\log|d_K|)$, and the lower bound follows. The upper bound can easily be proven via partial summation, and does not require GRH. Hence, for a maximal order, we have

$$\Theta\left(\frac{\sqrt{|D|}}{\log\log|D|}\right) \leq h(D) \leq \Theta\left(\sqrt{|D|}\log|D|\right)$$

To transfer this result to all orders, we use Corollary 3.1.9, from which it follows that

$$h(\mathcal{O}) = h(\mathcal{O}_K)\frac{\#(\mathcal{O}_K/\mathfrak{f})^*}{\#(\mathcal{O}/\mathfrak{f})^*}$$

where $\mathfrak{f} \leq \mathcal{O}_K$ is the largest ideal contained in $\mathcal{O}$. For the conductor $f = [\mathcal{O}_K : \mathcal{O}]$ we know that $d(\mathcal{O}) = f^2 d_K$, and clearly $\mathfrak{f} = (f)$. Now $\mathcal{O}/\mathfrak{f} \cong \mathbb{Z}/f\mathbb{Z}$ and so $\#(\mathcal{O}/\mathfrak{f})^* = \phi(f)$. To find $\#(\mathcal{O}_K/\mathfrak{f})^*$, consider the factorization $f = \prod p_i^{e_i}$. Clearly $\mathcal{O}_K/\mathfrak{f} \cong \bigoplus \mathcal{O}_K/(p_i)^{e_i}$, and thus it suffices to consider the case that $f = p^e$ is a prime power.

We have

$$\begin{aligned}
\#(\mathcal{O}_K/\mathfrak{f})^* &= \#\{(a,b) \in (\mathbb{Z}/p^e\mathbb{Z})^2 \mid a^2 + d_K b^2 \in (\mathbb{Z}/p^e\mathbb{Z})^*\} \\
&= \#\{(a,b) \in (\mathbb{Z}/p^e\mathbb{Z})^2 \mid a^2 + d_K b^2 \not\equiv 0 \mod p\} \\
&= p^{2e-2}\#\{(a,b) \in \mathbb{F}_p \mid a^2 + d_K b^2 \neq 0\} \\
&= p^{2e-2} \cdot \begin{cases} p^2 - 1 & \text{if } \left(\frac{-d_K}{p}\right) \in \{-1, 0\} \\ (p-1)^2 & \text{otherwise} \end{cases} \\
&= \begin{cases} f\phi(f) & \text{if } \left(\frac{-d_K}{p}\right) \in \{-1, 0\} \\ \phi(f)^2 & \text{otherwise} \end{cases}
\end{aligned}$$

since in the case $\left(\frac{-d_K}{p}\right) = -1$, have that $a^2 + d_K b^2 = (a + \delta b)(a - \delta b)$. Hence the change of variables $(a, b) \mapsto (a + \delta b, a - \delta b)$ transforms the set into $(\mathbb{F}_p \setminus \{0\})^2$.

Thus, we find

$$\frac{\#(\mathcal{O}_K/\mathfrak{f})^*}{\#(\mathcal{O}/\mathfrak{f})^*} \in \{f, \phi(f)\}$$

Now note that $\phi(n)$ is lower bounded by $\Omega(n/\log\log(n))$ (and upper bounded by n), so the claim follows. $\square$

Note that the study of the class number of nonmaximal orders $h(\mathbb{Z} + f\mathcal{O}_K)$ in a quadratic imaginary number field K from the proof shows that

$$h(\mathbb{Z} + l^e\mathcal{O}_K) = \begin{cases} l^e h(\mathcal{O}_K) & \text{if } \left(\frac{-d_K}{l}\right) = -1, 0 \\ (l-1)l^{e-1}h(\mathcal{O}_K) & \text{if } \left(\frac{-d_K}{l}\right) = 1 \end{cases}$$

This is compatible with the structure of the l-isogeny vulcano 3.1.22, in particular

- If $l \mid d_K$, i.e. is ramified in $\mathcal{O}_K$, the crater consists of two vertices with a double edge (or a single vertex with a double loop). Since the whole graph is $(l+1)$-regular, a crater vertex has $l - 1$ neighbors outside the crater. Thus, the class number of the first level is $h(\mathbb{Z} + l\mathcal{O}_K) = (l-1)h(\mathcal{O}_K)$.
- If $-d_K$ is a quadratic residue mod l, then l splits in $\mathcal{O}_K$ and so the crater is a cycle. As above, a crater vertex thus has $l - 1$ neighbors outside the crater and the class number is $h(\mathbb{Z} + l\mathcal{O}_K) = (l-1)h(\mathcal{O}_K)$.
- If l is inert in $\mathcal{O}_K$, the crater is a single vertex with a single loop. Since the whole graph is $(l+1)$-regular, it has l neighbors outside the crater and as expected, the class number is $h(\mathbb{Z} + l\mathcal{O}_K) = lh(\mathcal{O}_K)$.

Furthermore, a non-crater vertex always has l children and one parent, and the class number of the children level is $h(\mathbb{Z} + l^e\mathcal{O}_K) = lh(\mathbb{Z} + l^{e-1}\mathcal{O}_K)$.

Now lets come back to our estimate of the number of ordinary roots of $f_{p,m,n}$ resp. our polynomial system F_{p,m,l^e}. First, we now explain why instead of (isomorphism classes of) curves it suffices to count endomorphism rings.

Whenever we have two ordinary curves E and E' with same endomorphism ring $\mathcal{O}$ in a quadratic imaginary number field K, then by the class group action, there is $\mathfrak{a} \leq \mathcal{O}$ with $[\mathfrak{a}].E = E'$. It is not too hard to see that there also must be an ideal $\tilde{\mathfrak{b}} \leq \mathcal{O}$ of norm coprime to l in the same ideal class $[\mathfrak{a}]$ and so $[\tilde{\mathfrak{b}}].E = E'$. By Prop. 3.1.5, there is now a unique $\mathfrak{b} \leq \mathcal{O}_K$ with $\mathfrak{b} \cap \mathcal{O} = \tilde{\mathfrak{b}}$.

Now this gives us a graph automorphism of the l-isogeny subgraph induced by $\mathrm{Ell}(\mathcal{O})$, given by

$$\mathrm{Ell}(\mathcal{O}) \to \mathrm{Ell}(\mathcal{O}), \quad E \mapsto [\mathfrak{b} \cap \mathrm{End}(E)].E$$

This is not just a graph automorphism (i.e. preserves the graph structure), but also preserves Frobenius conjugates and the property of being defined over $\mathbb{F}_p$. The latter follows, since being defined over $\mathbb{F}_p$ is a property of the endomorphism ring, namely equivalent to the ideal (p, π) being principal.

Since our approach only uses properties of the l-isogeny graph and Frobenius conjugates, this means that if E and E' have the same endomorphism ring, it holds

$$f_{p,n,m}(j(E)) = 0 \quad \Leftrightarrow \quad f_{p,n,m}(j(E')) = 0$$

and similar for the system F_{p,n,l^e}.

Hence, we determine the set of endomorphism rings such that any resp. all corresponding curves are roots of the polynomials. Then, the total number of curves is given by the sum over the class numbers $\sum_D h(D)$ where D runs through the discrimiannts of said endomorphism rings.

We mentioned before that $\Phi_m(X, X^p)$ has about mp ordinary roots over $\bar{\mathbb{F}}_p$, but the argument implicitly assumed that the polynomial is separable. With our new framework, is is now easy to properly compute the number of ordinary roots of $\Phi_m(X, X^p)$, as these correspond to the endomorphism rings with cyclic [1] elements of norm mp. The reason is that this is equivalent to there being a solution with $x \perp y$ of the diophantine equation

$$x^2 + Dy^2 = m$$

if $D \equiv 0 \mod 4$ and

$$x^2 + Dy^2 = m$$

For now we will only make a crude estimate, but note that everything can be made rigorous. We do that later with a very similar argument in 5.3.1. Neglecting log-factors, we now have

$$\begin{aligned}\#\{j \in \bar{\mathbb{F}}_p \mid \Phi_m(j, j^p) = 0\} &= \sum_{\substack{x^2 - Dy^2 = mp \text{ solvable} \\ \text{with } x \perp y}} h(D) \\ &\geq \sum_{0<x<\sqrt{mp}} \sqrt{mp - x^2} \approx \int_0^{\sqrt{mp}} \sqrt{mp - x^2} \approx \Theta(mp)\end{aligned}$$

None of the ways we consider to capture supersingularity by modular polynomials can completely exclude ordinary roots. This is because if we take m and l to be small, then an ordinary curve defined over $\mathbb{F}_p$ with endomorphisms of degree m and l will always be a root. Similar situations can occur with other polynomial systems, but it is always the case that these ordinary curves have very small endomorphisms. The next statement shows that thus this is not a problem, as those ordinary roots are very rare.

Proposition 5.2.3. *For $n > 0$, there are at most $O(n^{3/2}\log(n)^2)$ isomorphism classes of ordinary curves who have a nontrivial endomorphism of degree n.*

Proof. First, note that for an endomorphism ϕ of an Elliptic Curve E have

$$\phi \text{ cyclic} \quad \Leftrightarrow \quad \text{no } m \geq 2 \text{ divides } \phi$$

Hence, a curve E having a cyclic endomorphism of degree n implies that $\mathrm{End}(E)$ has a nontrivial element of norm n.

Now assume that $\mathcal{O}$ is an imaginary quadratic order with $p \nmid d(\mathcal{O})$ that has such an element $\beta \in \mathcal{O}$. The discriminant of the order $\mathbb{Z}[\beta]$ is $d(\mathbb{Z}[\beta]) = \mathrm{Tr}(\beta)^2 - 4\mathfrak{N}(\beta) \geq -4\mathfrak{N}(\beta)$. Hence $|d(\mathcal{O})| \leq 4n$, and we find that the number of isomorphism classes of ordinary curves with a cyclic n-endomorphism is bounded by

$$\sum_{\substack{-4n \leq D \leq 0 \\ D \text{ fundamental discriminant}}} h(D) \leq \sum_{1 \leq D \leq 4n} \sqrt{D}\log(D)^2 \in O(n^{3/2}\log(n)^2) \qquad \square$$

[1] An element $\alpha \in \mathcal{O}$ is cyclic if the corresponding endomorphisms of curves E with $\mathrm{End}(E) \cong \mathcal{O}$ are cyclic. This is equivalent to $n \nmid \alpha$ for all $n \geq 2$.

This is now as far as we can go with the general case. The main problem is that once we want to determine which endomorphism rings have nontrivial endomorphisms of two different degrees (e.g. m and l^e), there is no analogue of the simple statement

$$\{d(\mathcal{O}) \mid \mathcal{O} \text{ has cyclic endomorphism of degree } m\} \supseteq \{m - x^2 \mid 0 < x < \sqrt{m}\}$$

While the diophantine equation $x^2 + Dy^2 = m$ has been deeply studied (see e.g. [13]), the best characterization for it being solvable (assuming $m = p$ is prime) involves the so-called Hilbert class polynomial

$$h_D(x) = \prod_{d(\mathrm{End}(E))=D} (X - j(E))$$

In our case, D is variable, which makes working with Hilbert class polynomials very unwieldy. All in all, it seems like the general case is very hard to get a handle on.

5.2.3 A working example

While we are unlikely to get nice provable bounds on the number of ordinary roots in the general situation of F_{p,m,l^e}, there are special cases in which this is possible. Next we present one of those situations.

Proposition 5.2.4. *Let l be a prime and further f be odd and e be even. Then the system*

$$F_{p,l^f,l^e} := \langle \Phi_{l^f}(x, x^p), \Phi_l(x, x_1), ..., \Phi_l(x_{e-1}, x^p) \rangle$$

has $O(l^{3f} \log(l^f)^2)$ ordinary roots [2].

Proof. We show that every ordinary root $j \in \bar{\mathbb{F}}_p$ of F_{p,l^f,l^e} has an endomorphism of degree at most l^{2f} and the claim follows by Prop. 5.2.3.

For any ordinary curve E, denote now by E_R the root of the lava flow tree containing E in the l-isogeny vulcano. In other words, if E is on the i-th lava flow tree level, then there is a sequence of ascending l-isogenies

$$E = E_0 \to E_1 \to ... \to E_i = E_R$$

and $\mathrm{End}(E_R)$ is maximal at l (meaning $l \nmid [\mathcal{O}_{\mathrm{End}(E_R)\otimes\mathbb{Q}} : \mathrm{End}(E_R)]$).

Note further that $(E^{(p)})_R = E_R^{(p)}$ for all ordinary curves E.

Now assume a root j of F_{p,l^f,l^e} gives an ordinary curve E. We distinguish two cases.

If $j(E_R) \in \mathbb{F}_p$, i.e. the crater of the vulcano is defined over $\mathbb{F}_p$, then clearly $E_R = (E^{(p)})_R$. Now let k be minimal such that $j(E_k) \in \mathbb{F}_p$. Then every cyclic path $E \to E^{(p)}$ has the form

$$E \to E_1 \to ... \to E_k \xrightarrow{\phi} E_k = E_k^{(p)} \to E_{k-1}^{(p)} \to ... \to E^{(p)}$$

where ϕ is a power-of-l endomorphism of E_k.

If we apply this to the l-isogeny path $E \to E^{(p)}$ of length f, we see that ϕ is an l^{f-2i}-endomorphism of E_i. However, since $f - 2i$ is odd by assumption, $\deg(\phi)$ is not a square and so ϕ is nontrivial. This now gives a nontrival endomorphism

$$E \to E_1 \to ... \to E_i \xrightarrow{\phi} E_i \to E_{i-1} \to ... \to E$$

[2]It might be not totally clear what we mean by an ordinary root of the system. So let us define the number of ordinary roots as the number of $j \in \bar{\mathbb{F}}_p$ such that $F_{p,l^f,l^e}(j, x_1, ..., x_{e-1})$ has a solution. However, note that for a fixed j, the number of different solutions of the system is polynomial, hence it would not make a big difference if we counted all solution tuples $(x, x_1, ..., x_{e-1})$.

of E with degree l^f and we are done.

If $j(E_R) \notin \mathbb{F}_p$, then $E_R \not\cong E_R^{(p)}$. In particular, this means that the ideal (p, π) in $\mathcal{O} := \mathrm{End}(E_R)$ is non-principal. Now we consider the subcases how (l) splits in $\mathcal{O}$.

If $(l) = \mathfrak{l}_1\mathfrak{l}_2$ is split in $\mathcal{O}$, note that our cyclic l-isogeny path $E \to E^{(p)}$ of length f induces a path $E_R \to E_R^{(p)}$ of length $f - 2i$, for some $i \geq 0$. Since walking around the crater is given by the action of $\mathfrak{l}_1$, we see that $[(p, \pi)] = [\mathfrak{l}_1]^{f-2i}$ in the ideal class group. Thus $\mathfrak{l}_1^{2f-4i}$ is principal, and its generator gives a nontrival endomorphism ϕ of $\mathrm{End}(E_R)$ of degree l^{2f}. Now

$$E = E_0 \to E_1 \to ... \to E_i = E_R \xrightarrow{\phi} E_R = E_i \to E_{i-1} \to ... \to E$$

gives a nontrival endomorphism of E with degree l^{2f}, so we are done.

If (l) is inert in $\mathcal{O}$, the crater only has a single vertex. Since we have $E_R \not\cong E_R^{(p)}$ are both curves in a crater, we see that they must be in different l-isogeny vulcanos. Hence, this also holds for E and $E^{(p)}$ and there cannot be an l^f-isogeny $E \to E^{(p)}$, contradicting our assumption.

Finally, we are left with the case that $(l) = \mathfrak{l}^2$ is ramified in $\mathcal{O}$. This is the only case where we will use the fact there is also an l-isogeny path $E \to E^{(p)}$ of length e. Since (l) is ramified, we see that the crater of the vulcano has exactly two vertices, which then must be E_R and $E_R^{(p)}$.

We did not assume that the l-isogeny path $E \to E^{(p)}$ of length e does not backtrack. But we can still remove the backtracks, and get a cyclic path $E \to E^{(p)}$ of length $e - 2k$, where k is the number of backtracking steps in the original path. Now this new path must go through the crater, and thus is of the form

$$E = E_0 \to E_1 \to ... \to E_i = E_R \to E_R^{(p)} = E_i^{(p)} \to E_{i-1}^{(p)} \to ... \to E_0^{(p)} = E^{(p)}$$

However, now we get a contradiction, since above path has odd length $2i + 1$, while $e - 2k$ is even by assumption. $\square$

By choosing $e = \Theta(\log_l(p))$, we have $\Theta(\sqrt{l^f p})$ supersingular roots of above system. Thus, this theorem shows that the fraction of supersingular roots is not just noticable, i.e. $1/\mathrm{poly}(\log(p))$, but even exponentially large. Therefore an algorithm that is able to efficiently compute a random root of F_{p,l^f,l^e} can be used to generate a random supersingular curve with very high probability. We expect that this will not reveal a trapdoor, i.e. information about the endomorphism ring.

Note that we can choose f very small, e.g. $\log_l \log(p)$ and thus $n = l^f$ is polynomial in $\log(p)$. Therefore, we can indeed write down the system

$$F_{p,l^f,l^e} := \langle \Phi_{l^f}(x, x^p), \Phi_l(x, x_1), ..., \Phi_l(x_{e-1}, x^p) \rangle$$

explicitly. The only question is how to compute a random root. The standard approach using Groebner basis does not work, as we expect its complexity to be exponential in the number of variables, i.e. exponential in $\log_l(p)$. The original paper [2] thought it might be possible to use a "square-and-multiply" approach to compute the resultant

$$\mathrm{res}_Y(\Phi_n(X + \delta Y, X - \delta Y), \Phi_{l^e}(X + \delta Y, X - \delta Y))$$

but this means we will not represent Φ_{l^e} by the polynomial system anymore, hence we would need to get enough information about the exponential-degree modular polynomial Φ_{l^e} another way. This seems to be a very serious obstacle.

5.3 An idea based on Sutherland's supersingularity test

As an alternative to the above approach, we propose another set of polynomial equations, whose properties might make computations easier. In particular, our system does not consist of long dependency cycles, in the sense that we have equations $f_i(x_i, x_{i+1})$ and $f_n(x_n, x_0)$. Instead, our equations are of the form $f_i(x_i, x_{i+1})$ and $f_n(x_n)$, which seems to be easier to handle.

The basic idea is an observation by Sutherland [31], namely that the lava flows of an ordinary vulcano can only have a bounded number of levels defined over $\mathbb{F}_{p^2}$. Hence, we can consider the following algorithm, which is Sutherland's supersingularity test. Beginning from the input j-invariant j_0, consider three random walks $j_0 = j_0^{(i)}, j_1^{(i)}, ..., j_n^{(i)}$ with $i \in \{1, 2, 3\}$ in the l-isogeny graph of fixed length n such that $j_1^{(1)}, j_1^{(2)}$ and $j_1^{(3)}$ are distinct. Furthermore, assume the walks do not backtrack. If j_0 is now ordinary, then at least one $j_1^{(i)}$ must be in a lava flow, and since the walks do not backtrack, one of them must descend in the corresponding lava flow tree. For n large enough, this shows that one $j_n^{(i)} \notin \mathbb{F}_{p^2}$. On the other hand, the whole supersingular l-isogeny graph is defined over $\mathbb{F}_{p^2}$, so this will never happen.

It is easy to see that $n = \log_l(p)$ is sufficient, which is also Sutherland's original choice. However, a slightly better bound can achieved, as observed by [1]. In our case, we are also interested in how many ordinary curves we will accept if we choose n smaller than the optimal bound. All this is considered in the next proposition.

Theorem 5.3.1. *Let p be an odd prime and $m \geq 2$ an odd integer coprime to p. Consider the number n of endomorphism rings $\mathcal{O}$ of ordinary curves defined over $\mathbb{F}_{p^2}$ with $\pi \in \mathbb{Z} + m\mathcal{O}$, where π is the p^2-Frobenius endomorphism [3] of $\mathcal{O}$. Then*

$$\left\lfloor \frac{p}{m^2} \right\rfloor \leq n \leq \left\lfloor \frac{4p(p+1)}{m^3} \right\rfloor$$

Furthermore, consider the number N of ordinary j-invariants $j \in \mathbb{F}_{p^2}$ such that $\pi \in \mathbb{Z} + m\mathrm{End}(j)$. Under GRH, we then get

$$c_1 \left(\frac{p^2}{m^3 \log\log(p)^2} \right) \leq N \leq c_2 \left(\frac{p^2 \log(p)^2}{m^3} \right)$$

where $c_1, c_2 > 0$ are constants.

Proof. First, we show the lower bounds. Note that there are $\lfloor p/m^2 \rfloor$ different integers a with $0 < am^2 < p$ (clearly $m^2 \nmid p$). For each of them, consider $D = 4am^2(am^2 - p)$. Clearly D is a fundamental discriminant, as $D \equiv 0 \mod 4$. We have

$$(p - 2am^2)^2 - D \cdot 1^2 = p^2 - 4pam^2 + 4a^2m^4 - 4a^2m^4 + 4pam^2 = p^2$$

Thus the imaginary quadratic order $\mathcal{O}$ with discriminant D contains a nontrivial element of norm p^2, which must be the Frobenius π. In particular, the imaginary quadratic order $\mathcal{O}_0$ with discriminant $d := D/m^2$ satisfies $\mathcal{O} = \mathbb{Z} + m\mathcal{O}_0$ as $[\mathcal{O}_0 : \mathcal{O}]^2 = d(\mathcal{O})/d(\mathcal{O}_0) = m^2$ Therefore we see that $\pi \in \mathbb{Z} + m\mathcal{O}_0$. Note that each a gives rise to a distinct $\mathcal{O}_0$, and the first lower bound follows.

[3] With the p^2-th power Frobenius endomorphism of an order $\mathcal{O}$, we mean a nontrivial element of norm p^2. There are at most two of them, and they are Galois conjugates. Hence, for $\mathrm{End}(E) \cong \mathcal{O}$ we can choose an isomorphism such that π is indeed mapped to the Frobenius. Furthermore, by our study of the canonical isomorphism $\mathrm{End}(E) \cong \mathrm{End}(E')$ for isogeneous curves E and E', we know that the choice of the isomorphism $\mathcal{O} \cong \mathrm{End}(E)$ is compatible with all canonical isomorphisms.

To get a lower bound for the number of curves, note that for each $\mathcal{O}_0$, by the class group action, there are exactly $\#\mathrm{Cl}(\mathcal{O}_0)$ such curves. Under GRH, Thm 5.2.2 gives

$$h(d) \geq \frac{\sqrt{|d|}}{(\log\log|d|)^2}\Theta(1)$$

Hence, the total number of curves is lower bounded by

$$\begin{aligned}
&\Theta(1)\sum_{1\leq a\leq\lfloor p/m^2\rfloor} h(4a(am^2-p)) \geq \Theta(1)\sum_{1\leq a\leq\lfloor p/m^2\rceil}\frac{\sqrt{4a|am^2-p|}}{(\log\log|4a(am^2-p)|)^2}\\
=&\Theta(1)m\sum_{1\leq a\leq\lfloor p/m^2\rfloor}\frac{\sqrt{a}\sqrt{p/m^2-a}}{(\log(\log(4)+\log(am^2)+\log(p-am^2)))^2}\\
\geq&\Theta(1)\frac{m}{(\log(\log(4)+2\log(p/2)))^2}\sum_{1\leq a\leq\lfloor p/m^2\rfloor}\sqrt{a}\sqrt{p/m^2-a}\\
=&\Theta(1)\frac{m}{\log\log(p)^2}\int_0^{p/m^2}\sqrt{a}\sqrt{p/m^2-a}\;da\\
=&\Theta(1)\frac{p^2}{m^3\log\log(p)^2}\int_0^1\sqrt{x(1-x)}dx = \Theta\left(\frac{p^2}{m^3\log\log(p)^2}\right)
\end{aligned}$$

We assume that $p\geq m^2$ when estimating the sum by the integral.

Now to the upper bounds. Consider an endomorphism ring $\mathcal{O}_0$ such that $\mathcal{O} := \mathbb{Z}+m\mathcal{O}_0$ contains the p^2-Frobenius π. Then

$$\mathbb{Z}[\pi]\subseteq\mathcal{O}\subseteq\mathcal{O}_0$$

and so $D := d(\mathbb{Z}[\pi]) = a^2m^2d(\mathcal{O}_0)$. Furthermore, if t is the trace of π, we find $D = t^2-4p^2 = (t-2p)(t+2p)$. Hence

$$a^2m^2d(\mathcal{O}_0) = (t-2p)(t+2p)$$

Unless $m=2$ or $m=4$, m cannot divide both $t-2p$ and $t+2p$.

If $m^2 \mid t+2p$, then $t\in\{m^2-2p, 2m^2-2p, ..., km^2-2p\}$ where $k=\lfloor 2p/m^2\rfloor$.

If $m^2 \mid t-2p$, then $t\in\{2p-(k+1)m^2, 2p-(k+2)m^2, ..., 2p-(2k+1)m^2\}$.

In particular, there are at most $2k+1$ different choices for t. For a given t, there are now at most

$$\sqrt{\frac{|t^2-4p^2|}{m^2}} \leq \sqrt{\frac{4p^2}{m^2}} = \frac{2p}{m}$$

choices for a, which then uniquely determines $d(\mathcal{O}_0)$. The total number of possibilities for $d(\mathcal{O}_0)$ is thus

$$(2k+1)\frac{2p}{m} \leq \frac{4p(p+1)}{m^3}$$

To bound the number of curves, we again use the class group action and the following bound on the class number of a quadratic imaginary number field. Namely, if the discriminant is d, have

$$h(d)\leq\sqrt{|d|}\log(|d|)O(1)$$

This now gives us the following upper bound on the number of curves

$$
\begin{aligned}
&\sum_{1\le i\le k}\ \sum_{a^2 \ \mid\ ((im^2-2p)^2-4p^2)/m^2} h\left(\frac{(im^2-2p)^2-4p^2}{a^2m^2}\right)\\
&+\sum_{k+1\le i\le 2k+1}\ \sum_{a^2 \ \mid\ ((2p-im^2)^2-4p^2)/m^2} h\left(\frac{(2p-im^2)^2-4p^2}{a^2m^2}\right)\\
\le& O(\log(4p^2/m^2))\Bigg(\sum_{1\le i\le k}\sqrt{\frac{4p^2-(im^2-2p)^2}{m^2}}\sum_{a^2 \ \mid\ ((im^2-2p)^2-4p^2)/m^2}\frac{1}{a}\\
&+\sum_{k+1\le i\le 2k+1}\sqrt{\frac{4p^2-(2p-im^2)^2}{m^2}}\sum_{a^2 \ \mid\ ((2p-im^2)^2-4p^2)/m^2}\frac{1}{a}\Bigg)
\end{aligned}
$$

Note that

$$
\sum_{a^2 \ \mid\ x}\frac{1}{a}\le\sum_{a\le\sqrt{x}}\frac{1}{a}=O(\log(x))
$$

Thus we can upper bound the previous sum by

$$
\begin{aligned}
&O(\log(4p^2/m^2))\Bigg(\sum_{1\le i\le k}\sqrt{\frac{4p^2-(im^2-2p)^2}{m^2}}\quad\log\left(\frac{4p^2-(im^2-2p)^2}{m^2}\right)\\
&+\sum_{k+1\le i\le 2k+1}\sqrt{\frac{4p^2-(2p-im^2)^2}{m^2}}\quad\log\left(\frac{4p^2-(2p-im^2)^2}{m^2}\right)\Bigg)\\
\le&\frac{O(\log(p/m)^2)}{m}\left(\sum_{1\le i\le k}\sqrt{4p^2-(im^2-2p)^2}+\sum_{k+1\le i\le 2k+1}\sqrt{4p^2-(2p-im^2)^2}\right)\\
=&\frac{O(\log(p/m)^2)}{m}\left(\int_0^k\sqrt{4p^2-(xm^2-2p)^2}dx+\int_{k+1}^{2k+2}\sqrt{4p^2-(xm^2-2p)^2}dx\right)\\
\le&\frac{O(\log(p/m)^2)}{m}\left(\int_0^k\sqrt{4p^2-(xm^2-2p)^2}dx+\int_{k}^{2k}\sqrt{4p^2-(xm^2-2p)^2}dx+O(p)\right)\\
=&\frac{O(\log(p/m)^2)}{m}\left(\frac{1}{m^2}\int_0^{2p}\sqrt{4p^2-(x-2p)^2}dx+\frac{1}{m^2}\int_{2p}^{4p}\sqrt{4p^2-(2p-x)^2}dx+O(p)\right)\\
=&\frac{O(\log(p/m)^2)}{m}\left(\frac{1}{m^2}\int_{-2p}^{0}\sqrt{4p^2-x^2}dx+O(p)\right)\\
=&\frac{O(\log(p/m)^2)}{m}\left(\frac{4p^2}{m^2}\int_{-1}^{0}\sqrt{1-x^2}\right)=O\left(\frac{p^2\log(p/m)^2}{m^3}\right)
\end{aligned}
$$

This shows the claim. □

In particular, it follows that we can choose $m=l^r$ with $r=\lceil\frac{1}{2}\log_l(p)\rceil$ and can be sure never to accept an ordinary curve as supersingular. Furthermore, if we are ok with accepting $O(p)$ ordinary curves as supersingular, we can choose $r=\lceil\frac{1}{3}\log_l(p)\rceil$.

5.3.1 Generating curves

According to the above discussion, the obvious polynomial system we want to find a root of is

$$\langle \Phi_m(x, y_1), \Phi_m(x, y_2), \Phi_m(x, y_3),\ y_1^{p^2-1} - 1,\ y_2^{p^2-1} - 1,\ y_3^{p^2-1} - 1\rangle$$

Since m will be exponentially large, and we thus have no good description of Φ_m, we can instead consider the paths explicitly again. More concretely, consider the polynomial system

$$\begin{aligned}
&\langle \Phi_l(x, u_0), \Phi_l(x, v_0), \Phi_l(x, w_0),\\
&\ \Phi_l(u_0, u_1), \Phi_l(v_0, v_1), \Phi_l(w_0, w_1),\\
&\ ...\\
&\ \Phi_l(u_{n-1}, u_n), \Phi_l(v_{n-1}, v_n), \Phi_l(w_{n-1}, w_n),\\
&\ u_n^{p^2-1} - 1, v_n^{p^2-1} - 1, w_n^{p^2-1} - 1\rangle
\end{aligned}$$

We can explicitly write down that system.

However, a solution to this system might "collapse" nodes, e.g. have $u_i = u_{i+2}$. Then the corresponding l-isogeny path backtracks, and it is not guaranteed that one path reaches the n-th lava flow level. Hence, we can still get many ordinary curves.

Then condition $u_i \neq u_{i+2}$ is not algebraically closed, so we cannot write it as a polynomial directly. But we can use the structure of the vulcanos (in particular, they have at most one cycle), and the fact that Φ_m characterizes the existence of a *cyclic* isogeny. Hence, consider the polynomial system

$$\begin{aligned}
&\langle \Phi_l(x, u_0), \Phi_l(x, v_0), \Phi_l(x, w_0),\\
&\ \Phi_l(u_0, u_1), \Phi_l(v_0, v_1), \Phi_l(w_0, w_1),\\
&\ ...\\
&\ \Phi_l(u_{n-1}, u_n), \Phi_l(v_{n-1}, v_n), \Phi_l(w_{n-1}, w_n),\\
&\ u_n^{p^2-1} - 1, v_n^{p^2-1} - 1, w_n^{p^2-1} - 1,\\
&\ \Phi_{2l}(u_0, v_0), \Phi_{2l}(u_0, w_0), \Phi_{2l}(v_0, w_0),\\
&\ \Phi_{2l}(u_0, u_2), \Phi_{2l}(v_0, v_2), \Phi_{2l}(w_0, w_2),\\
&\ ...\rangle
\end{aligned}$$

The additional constraints $\Phi_2 l(u_i, u_{i+2})$ ensure that $u_i \neq u_{i+2}$, unless the curve of j-invariant u_i has a cyclic endomorphism of size $2l$. However, this means that its endomorphism ring has polynomially large discriminant, and by the class group action, there are only polynomially many such curves. Hence, a root of above system is supersingular with probability $1 - 1/\mathrm{poly}(\log(p))$.

Still, it seems pretty impossible to efficiently compute a random root of above system. We now present a way that looks like there is some hope to compute its roots, even though there are still some serious obstacles.

Proposition 5.3.2. *Let $\mathcal{O}$ be an order in a quadratic imaginary number field with p^2-power Frobenius π. Let $l_1, ..., l_r$ be distinct primes. Then*

$$\pi \in \mathbb{Z} + l_1 ... l_r \mathcal{O} \quad \Leftrightarrow \quad \forall i : \pi \in \mathbb{Z} + l_i \mathcal{O}$$

Proof. The direction $\Rightarrow$ is clear, as $\mathbb{Z} + l_1 ... l_r \mathcal{O} \subseteq \mathbb{Z} + l_i \mathcal{O}$. For the other direction, choose an integral generator α of $\mathcal{O}$, i.e. $\mathcal{O} = \mathbb{Z} + \alpha\mathbb{Z}$. Then $\mathbb{Z} + l_i \mathcal{O} = \mathbb{Z} + l_i \alpha \mathbb{Z}$. Furthermore, there is a unique representation $\pi = a + b\alpha$. Now the assumption

$$\pi \in \mathbb{Z} + l_i \mathcal{O} = \mathbb{Z} + l_i \alpha \mathbb{Z}$$

implies $l_i \mid b$, and so $l_1 ... l_r \mid b$. Thus

$$\pi \in \mathbb{Z} + l_1 ... l_r \mathcal{O} = \mathbb{Z} + l_1 ... l_r \alpha \mathbb{Z} \qquad \square$$

Hence, we can instead consider the sum of systems

$$\sum_i \quad \langle \Phi_{l_i}(x, u_i), \Phi_{l_i}(x, v_i), \Phi_{l_i}(x, w_i), \\ \Phi_{2l_i}(u_i, v_i), \Phi_{2l_i}(u_i, w_i), \Phi_{2l_i}(v_i, w_i), \\ u_i^{p^2-1} - 1, v_i^{p^2-1} - 1, w_i^{p^2-1} - 1 \rangle$$

for distinct primes l_i with $\prod_i l_i \geq \sqrt{p}$. Finally, we can still make it somewhat more explicit.

Lemma 5.3.3. *Assume that k is an algebraically closed field. Let $I \leq k[x, Y, B]$ be an ideal, where Y and B are vectors of unknowns. Then elimination and evaluation commute, i.e.*

$$\mathrm{ev}_{x,b}(I \cap k[x, B]) = \mathrm{ev}_{x,Y,b}(I) \cap k[x]$$

where $b \in k[x]^n$ is a vector and $\mathrm{ev}_{x,b}$ resp. $\mathrm{ev}_{x,Y,b}$ are evaluation homomorphisms.

Proof. Taking the point of view of varieties over the algebraically closed field k, we see that elimination corresponds to projection (the main theorem of elimination theory), and evaluation corresponds to the intersection with a linear subspace. Clearly, both of them commute in the above sense. $\square$

Lemma 5.3.4. *We have*

$$y^{p^2-1} - 1 \equiv \begin{pmatrix} y^l \\ \vdots \\ 1 \end{pmatrix}^T b - 1 \mod \Phi_l(x, y)$$

where

$$b = A^{p^2-l-1} \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

for an explicitly computable $(l+1) \times (l+1)$ matrix $A \in k[x]^{(l+1)\times(l+1)}$.

Proof. Just perform univariate polynomial division of $y^{p^2-1} - 1$ modulo the monic polynomial $\Phi_l(x, y)$ in $k[x][y]$. $\square$

The idea is now to introduce $l + 1$ indeterminates B, and compute the elimination ideal

$$\langle \Phi_{l_i}(x, u_i), \Phi_{l_i}(x, v_i), \Phi_{l_i}(x, w_i), \\ \Phi_{2l_i}(u_i, v_i), \Phi_{2l_i}(u_i, w_i), \Phi_{2l_i}(v_i, w_i), \\ \begin{pmatrix} u_i^l \\ \vdots \\ 1 \end{pmatrix}^T B - 1, \begin{pmatrix} v_i^l \\ \vdots \\ 1 \end{pmatrix}^T B - 1, \begin{pmatrix} w_i^l \\ \vdots \\ 1 \end{pmatrix}^T B - 1 \rangle \cap k[x, B]$$

Now we can find polynomials $f_{i1}, ..., f_{in_i} \in k[x, B]$ that generate this ideal. Hence, we only have to find a random joint root of the univariate polynomials

$$f_{ij}(x, b_i) \quad \text{where} \quad b_i = A_i^{p^2-l-1} \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

for the matrices A_i given by Lemma 5.3.4. While we cannot explicitly write down those polynomials, we can evaluate them, evaluate their derivates and perform a series of other computations. Hence, there might be some way to find a random root of those (note that they have all $\Theta(p/12)$ supersingular j-invariants and some $o(p)$ ordinary j-invariants as roots).

Bibliography

[1] Gustavo Banegas, Valerie Gilchrist, and Benjamin Smith. Efficient supersingularity testing over $\mathbb{F}_p$ and csidh key validation. Cryptology ePrint Archive, Paper 2022/880, 2022.

[2] Jeremy Booher, Ross Bowden, Javad Doliskani, Tako Boris Fouotsa, Steven D. Galbraith, Sabrina Kunzweiler, Simon-Philipp Merz, Christophe Petit, Benjamin Smith, Katherine E. Stange, Yan Bo Ti, Christelle Vincent, José Felipe Voloch, Charlotte Weitkämper, and Lukas Zobernig. Failing to hash into supersingular isogeny graphs. Cryptology ePrint Archive, Report 2022/518, 2022. https://ia.cr/2022/518.

[3] Jan Hendrik Bruinier, Ken Ono, and Andrew V. Sutherland. Class polynomials for nonholomorphic modular functions. *Journal of Number Theory*, 161:204–229, 2016.

[4] Reinier Bröker, Kristin Lauter, and Andrew V. Sutherland. Modular polynomials via isogeny volcanoes. *Mathematics of Computation*, 81(278):1201–1231, 2011.

[5] Jeffrey Burdges and Luca De Feo. Delay encryption. Cryptology ePrint Archive, Paper 2020/638, 2020.

[6] Wouter Castryck and Thomas Decru. An efficient key recovery attack on sidh (preliminary version). Cryptology ePrint Archive, Paper 2022/975, 2022.

[7] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. Csidh: An efficient post-quantum commutative group action. Cryptology ePrint Archive, Paper 2018/383, 2018.

[8] Denis Xavier Charles, Eyal Z. Goren, and Kristin E. Lauter. Cryptographic hash functions from expander graphs. *J. Cryptology*, 22:93–113, 2009.

[9] Jeff Cheeger. A lower bound for the smallest eigenvalue of the laplacian. In *Proceedings of the Princeton conference in honor of Professor S. Bochner*, pages 195–199, 1969.

[10] Mathilde Chenu and Benjamin Smith. Higher-degree supersingular group actions. *CoRR*, abs/2107.08832, 2021.

[11] Leonardo Colò and David Kohel. Orienting supersingular isogeny graphs. Cryptology ePrint Archive, Paper 2020/985, 2020. https://eprint.iacr.org/2020/985.

[12] Jean-Marc Couveignes. Hard homogeneous spaces. Cryptology ePrint Archive, Paper 2006/291, 2006.

[13] David A Cox. *Primes of the Form X2+ny2: Fermat, Class Field Theory, and Complex Multiplication*. John Wiley & Sons, Incorporated, 2013.

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

[15] Kirsten Eisentraeger, Sean Hallgren, Kristin Lauter, Travis Morrison, and Christophe Petit. Supersingular isogeny graphs and endomorphism rings: reductions and solutions. Cryptology ePrint Archive, Paper 2018/371, 2018.

[16] Kirsten Eisenträger, Sean Hallgren, Kristin E. Lauter, Travis Morrison, and Christophe Petit. Supersingular isogeny graphs and endomorphism rings: Reductions and solutions. In *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part III*, volume 10822, pages 329–368. Springer, 2018.

[17] Luca De Feo, David Jao, and Jérôme Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. Cryptology ePrint Archive, Paper 2011/506, 2011.

[18] Luca De Feo, Simon Masson, Christophe Petit, and Antonio Sanso. Verifiable delay functions from supersingular isogenies and pairings. Cryptology ePrint Archive, Paper 2019/166, 2019.

[19] Tako Boris Fouotsa. Sidh with masked torsion point images. Cryptology ePrint Archive, Paper 2022/1054, 2022.

[20] Mireille Fouquet and François Morain. Isogeny volcanoes and the sea algorithm. In Claus Fieker and David R. Kohel, editors, *Algorithmic Number Theory*, pages 276–291. Springer Berlin Heidelberg, 2002.

[21] Shlomo Hoory and Nathan Linial. Expander graphs and their applications. *Bulletin of the American Mathematical Society*, 43:439–561, 2006.

[22] David Kohel. *Endomorphism rings of elliptic curves over finite fields*. PhD thesis, University of California at Berkeley, 1996.

[23] J. E. Littlewood. On the class-number of the corpus $\mathbb{Q}(\sqrt{-k})$. *Proceedings of the London Mathematical Society*, s2-27(1):358–372, 1928.

[24] Tomoki Moriya. Masked-degree sidh. Cryptology ePrint Archive, Paper 2022/1019, 2022.

[25] Juergen Neukirch. *Algebraische Zahlentheorie*. Springer, 1992.

[26] Arnold Pizer. Ramanujan graphs and hecke operators. *Bulletin of the American Mathematical Society*, 23:127–137, 1990.

[27] Alexander Rostovtsev and Anton Stolbunov. Public-key cryptosystem based on isogenies. Cryptology ePrint Archive, Paper 2006/145, 2006.

[28] René Schoof. Elliptic curves over finite fields and the computation of square roots $\bmod p$. *Mathematics of Computation*, 44(170):483–494, 1985.

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

[30] Anton Stolbunov. Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves. *Advances in Mathematics of Communications*, 4(2):215–235, 2010.

[31] Andrew V. Sutherland. Identifying supersingular elliptic curves. *LMS Journal of Computation and Mathematics*, 15:317–325, 2012.

[32] J. Tate. Endomorphisms of abelian varieties over finite fields. *Inventiones mathematicae*, 2:134–144, 1966.

[33] William C. Waterhouse. Abelian varieties over finite fields. *Annales scientifiques de l'École Normale Supérieure*, Ser. 4, 2(4):521–560, 1969.