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

Acknowledgements

First and foremost, I want to thank my dissertation supervisor, Cristophe Petit, who brought me in contact with this fascinating topic and provided invaluable advice throughout the research and writing process. Additionally, I want to thank my previous professor, Jens Zumbrägel, for vastly supporting me on my way into research. Without him, I would not be where I am now.

Abstract

It is currently an open problem in isogeny-based cryptography to efficiently compute supersingular Elliptic Curves without revealing their endomorphism ring or other information that might be used as trapdoor. Various ideas have been proposed in the literature, but as presented there, none of them is currently able to solve the problem. In our work, we focus on the second approach from [Boo+22], which is based on root-finding of specialized modular polynomials.

We found a special case in which we can answer an important question posed in the original work, namely to quantify the probability of the computed curve being supersingular. Our case also seems suitable for computations, and its success probability is higher than we expect it to be in the generic case. Furthermore, we present a modification of the original scheme, and argue why it might allow more efficient computations. However, both of these still suffer from the main problem of the original idea, namely that there is currently no way to efficiently work with the considered polynomial systems. Still, our analysis reveals some of the underlying structure, and we hope that further research might find a way to make this practical.

[Boo+22] Jeremy Booher et al. *Failing to hash into supersingular isogeny graphs*. Cryptology ePrint Archive, Report 2022/518. 2022. URL: https://ia.cr/2022/518

Contents

Chapter 1

Introduction

The continuing progress in the construction of quantum computers has pushed the development of post-quantum cryptographic schemes into the center of attention. One approach is isogeny-based cryptography, which relies on the theory of elliptic curves and their isogenies. Founded on ideas of Couveignes, Rostovtsev and Stolbunov [Cou06; RS06; Sto10], a variety of different schemes have been proposed since then. This includes the well-known, although recently broken [CD22], key exchange protocol SIDH [FJP11].

Although the pioneering works have been based on ordinary curves, a majority of later schemes uses supersingular curves. Hence, it is a natural question how to computationally generate supersingular curves in implementations. The good new is that methods based on complex multiplication [Brö07] together with random walks allow us to find uniformly random supersingular curves even over prime fields of exponentially large characteristic. However, this method has a drawback. Namely, whoever generates a curve using this algorithm can easily find its endomorphism ring, which can be used as a trapdoor for various cryptographically relevant problems [Eis+18].

In many cases like encryption, this is not a problem at all, since the person generating the curve has access to the secret anyway, for example because they are a legitimate party in the communication. However, even for SIDH (before it was broken), there were some subtle security problem related to the torsion-point attacks, that could be prevented by other, trapdoor-free ways of finding starting curves. Furthermore, many applications, for example in blockchain environments or for more sophisticated primitives [Feo+19; BF20], are insecure if any party has knowledge of a trapdoor for the starting curve. Hence, these scenarios currently require a trusted third party, that generates a curve using one of the known approaches, and then forgets about the additional information produced in the process. Therefore, there is natural interest in methods to eliminate this trusted third party, by finding algorithms that generate supersingular curves, for whom the endomorphism ring problem is as hard as for random curves - even when the randomness used for the generation is known. This is currently an open problem.

Some approaches have been proposed in [Boo+22] and also in [MMP22], 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 that must be overcome before it might be practical. In this work, we focus on the second idea from [Boo+22], which is proposed by Katherine Stange. Basically, it relies on the observation that Elliptic Curves with fixed-degree isogenies to their Galois conjugate are supersingular with higher probability. Further, they propose an approach based on modular polynomials and resultants that can find a random curve with two isogenies of different, fixed degree to their Galois conjugate. However, as mentioned in [Boo+22], 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 isogenies is in a certain sense independent, but 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 for the idea to work properly. According to their heuristic, it 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 case of the two-isogeny variant, in which the fraction of supersingular Elliptic Curves is provably big enough. More concretely, we present the following result.

Proposition 1 (First Result)**.** *Let l be a small prime, f be an odd integer and e an even integer such that $l^e = \Theta(p)$. Then a random Elliptic Curve over $\mathbb{F}_{p^2}$ 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.

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 2 (Second Result)**.** *Let $l_1, ..., l_r$ be a small primes with $\prod l_i \geq 2p$. Then a random Elliptic Curve over $\overline{\mathbb{F}}_p$ such that there are three l_i-isogenous 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. [Cox13]) 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 rarely treated, and then in works like [Deu41] or [Wat69], which are quite challenging. For example, the work of Deuring [Deu41] is quite old and written in German, while the work of Waterhouse [Wat69] 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 [Sil09].

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 $O = (0 : 1 : 0)$ [Sil09, Prop. III.3.1]. Furthermore, an isomorphism class of Elliptic Curves is uniquely determined by its j-invariant [Sil09, 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 [Sil09, Prop. III.2.2]. A more theoretical characterization of the group law is given by [Sil09, 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

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

A property of Elliptic Curves that can be used for some slightly exotic cryptographic primitives (like identity-based crypto, or the verifiable delay function we present in Section 4.3) is the Weil pairing. Let $m \geq 2$ be an integer coprime to p. Then there exists a map, the m-th *Weil pairing*

$$e_m : E[m] \times E[m] \to \mu_m$$

where $\mu_m \subseteq \mathbb{C}^*$ is the group of m-th roots of unity. It has the following properties (see [Sil09, Prop. III.8.1]):

- e_m is bilinear, i.e. $e_m(S + S', T) = e_m(S, T)e_m(S', T)$ and similar for the second argument.
- e_m is alternating, i.e. $e_m(T, T) = 1$.
- e_m is nondegenerate, i.e. if $e_m(S, \cdot)$ is the constant map O, then $S = O$.

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 [Sil09, 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 [Sil09, Thm III.4.10]. It is common to call isogenies of degree m also m-isogenies.

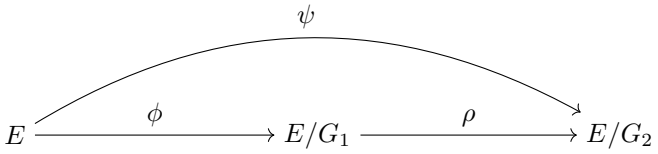
Studying again the example of the multiplication-by-m isogeny $[m] : E \to E$, one can show that this has degree m^2. Its kernel is obviously the subgroup $E[m]$, and thus, if $[m]$ is separable, we see that $E[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$. We will explain what happens in the case that $[m]$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

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

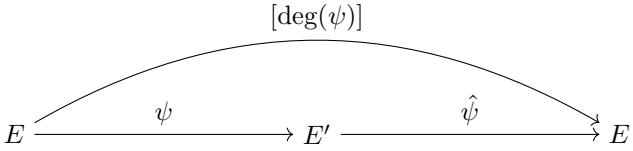
In particular, for a finite subgroup $G \leq E$ there is a unique (up to isomorphism) Elliptic Curve E' and separable isogeny $\psi : E \to E'$ with kernel G. We also denote E' by E/G, as that is the group structure on E' by the isomorphism theorem (morphisms of projective irreducible curves are always 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 $\rho : E/G_1 \to E/G_2$ such that the diagram



commutes. 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 the 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 $\overline{\mathbb{F}}_p$ 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 $\hat{\psi}$



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

Interestingly, the dual isogeny behaves like an adjoint w.r.t. the Weil pairing, i.e.

$$e_m(S, \phi(T)) = e_m(\hat{\phi}(S), T)$$

for an isogeny $\phi : E \to E'$ and the m-th Weil pairing e_m of E resp. E' (see [Sil09, Prop. III.8.2]).

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 [Sil09, 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 3. *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. [Sil09, Corollary III.9.4].

If $k \subseteq \bar{\mathbb{F}}_p$, 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
$p \nmid d(\mathrm{End}(E))$ and $p \nmid d(\mathbb{Z}[\pi_E])$	$p \mid d(\mathbb{Z}[\pi_E])$

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 [Sil09, 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 discriminant of the order $\mathrm{End}(E)$ divides the discriminant $d(\mathbb{Z}[\pi_E])$, as $\mathbb{Z}[\pi_E] \subseteq \mathrm{End}(E)$. Now it follows that $-4q < d(\mathrm{End}(E)) < 0$ in this case, because $d(\mathbb{Z}[\pi_E]) = \mathrm{Tr}(\pi_E)^2 - 4q$.

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, it is not too hard to show [Sil09, 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 isomorphic 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 with them. A fundamental algorithm based on the Velu formulas allows to compute the curve E/G 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 one 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 $l \neq p$. For this chapter, and the rest of this work, we assume $p = \mathrm{char}(k) \neq 2, 3$.

Definition 4. Denote by $\Gamma_l(k)$ the graph whose vertices are isomorphism classes of Elliptic Curves over k, and the edges are the degree l isogenies (again up to isomorphism [1]) 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. We also know that if $p \neq 2, 3$ and $l \neq p$, the graph $\Gamma_l(\bar{\mathbb{F}}_p)$ is $(l+1)$-regular except at the j-invariants 0 and 1728, 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 analyzing 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)

[1] We say two isogenies $\phi, \psi : E \to E'$ are isomorphic, if there are automorphisms $\tau \in \mathrm{Aut}(E)$ and $\rho \in \mathrm{Aut}(E')$ such that $\phi = \rho \circ \psi \circ \tau$. Note that $\mathrm{Aut}(E) = \{\pm 1\}$ unless $j(E) \in \{0, 1728\}$ (assuming $\mathrm{char}(k) \neq 2, 3$), so this case occurs only at the two vertices with j-invariants 0 and 1728.

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, and let $\mathcal{O}_K$ denote the maximal order in 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 5. *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. [Neu92, Prop. I.12.3]. From now on, write $\mathfrak{N}(\mathfrak{a})$ for the norm of an ideal $\mathfrak{a} \leq \mathcal{O}$, i.e. $\mathfrak{N}(\mathfrak{a}) := [\mathcal{O} : \mathfrak{a}]$. In the Dedekind ring $\mathcal{O}_K$ this is multiplicative, in the order $\mathcal{O}$, it is (in general) not.

Lemma 6. *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 write $\mathcal{O} = \mathbb{Z}[\phi]$ for a generator ϕ of $\mathcal{O}$. 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 for the 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 $\mathcal{O}$. □

Since multiplication of ideals can be expressed by the product of their generators, we get the following corollary.

Corollary 7. *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 8. *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 can choose a generator α of $\mathcal{O}_K$ and find $\mathcal{O}_K = \mathbb{Z}[\alpha]$ as well as $\mathcal{O} = \mathbb{Z}[f\alpha]$ where $f = [\mathcal{O}_K : \mathcal{O}]$. Thus $f \notin \mathfrak{p}$ and so $f \in \mathcal{O}_{\mathfrak{p}}^*$. Therefore $\alpha = f^{-1} f\alpha \in \mathcal{O}_{\mathfrak{p}}$ and so $(\mathcal{O}_K)_{\mathfrak{p}'} \subseteq \mathcal{O}_{\mathfrak{p}}$. □

Lemma 9. *If $\mathfrak{a} \leq \mathcal{O}$ with $\mathfrak{N}(\mathfrak{a}) \perp f := [\mathcal{O}_K : \mathcal{O}]$ then also $\mathfrak{N}(\mathfrak{a}\mathcal{O}_K) \perp f$. Conversely, if $\mathfrak{a} \leq \mathcal{O}_K$ with $\mathfrak{N}(\mathfrak{a}) \perp f$, then also $\mathfrak{N}(\mathfrak{a} \cap \mathcal{O}) \perp f$.*

Proof. For the first statement, note that if $\mathfrak{N}(\mathfrak{a}) \perp f$, then also $\mathfrak{a} \perp f\mathcal{O}$ and so there is a relation $1 = a + fb$ with $a \in \mathfrak{a}$ and $b \in \mathcal{O}$. However, then $1 \in \mathfrak{a}\mathcal{O}_K + f\mathcal{O}_K$ and so $\mathfrak{a}\mathcal{O}_K \perp f$, thus $\mathfrak{N}(\mathfrak{a}\mathcal{O}_K) \perp f$.

On the other hand, for $\mathfrak{a} \leq \mathcal{O}_K$ with $\mathfrak{N}(\mathfrak{a}) \perp f$, we have the map

$$\mathcal{O} \to \mathcal{O}_K/\mathfrak{a}, \quad x \mapsto [x]$$

It clearly has kernel $\mathfrak{a} \cap \mathcal{O}$, and so we find that $\mathcal{O}/(\mathfrak{a} \cap \mathcal{O}) \subseteq \mathcal{O}_K/\mathfrak{a}$. Thus $\mathfrak{N}(\mathfrak{a} \cap \mathcal{O}) \mid \mathfrak{N}(\mathfrak{a})$ and it follows that $\mathfrak{N}(\mathfrak{a} \cap \mathcal{O}) \perp f$. □

Instead of all ideals in $\mathcal{O}$, we often only work with the set of invertible (fractional) ideals. A fractional ideal $\mathfrak{a} \leq \mathcal{O}$ is invertible, if there is another fractional ideal $\mathfrak{b}$ with $\mathfrak{ab} = \mathcal{O}$. In contrast to the set of all ideals, this is now a group. Clearly, every ideal $\mathfrak{a}$ of the Dedekind ring $\mathcal{O}_K$ is invertible.

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

Proposition 10. *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 7, 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 $\mathfrak{a}\mathcal{O}_\mathfrak{p} = \mathfrak{b}\mathcal{O}_\mathfrak{p}$ for all primes $\mathfrak{p} \leq \mathcal{O}$. Note that if $\mathfrak{N}(\mathfrak{p}) \not\perp f$, this holds trivially, as $\mathfrak{a}\mathcal{O}_\mathfrak{p} = \mathcal{O}_\mathfrak{p} = \mathfrak{b}\mathcal{O}_\mathfrak{p}$. Otherwise, note that

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

as $\mathcal{O}_\mathfrak{p} = (\mathcal{O}_K)_\mathfrak{p}$. This shows that $\mathfrak{a}\mathcal{O}_\mathfrak{p} = \mathfrak{b}\mathcal{O}_\mathfrak{p}$ 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 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 [Neu92, Chapter I.§12].

Lemma 11. *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. This proof is taken with some modifications from [Neu92, 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 $\mathfrak{ab} = (1)$ with $\mathfrak{b} = (b_1, ..., b_m)$ and so have $1 = \sum a_i b_i c_i$ with $c_i \in \mathcal{O}$. 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 $xb_ic_i \in \mathfrak{ab} = \mathcal{O}_\mathfrak{p}$, so

$$x = a_i \underbrace{xb_ic_i}_{\in\mathcal{O}_\mathfrak{p}} \underbrace{(a_ib_ic_i)}_{\in\mathcal{O}_\mathfrak{p}^*}^{-1} \in a_i\mathcal{O}_\mathfrak{p}$$

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 [Neu92, Prop. I.12.2].

Let $(a_\mathfrak{p})_\mathfrak{p} \in \bigoplus_\mathfrak{p} K^*/\mathcal{O}_\mathfrak{p}^*$ and set $\mathfrak{a} := \bigcap_\mathfrak{p} a_\mathfrak{p}\mathcal{O}_\mathfrak{p}$. We claim that $\iota^{-1}(\mathfrak{a}) = (a_\mathfrak{p})_\mathfrak{p}$. 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 $\supseteq$.

By multiplying both $(a_\mathfrak{q})_\mathfrak{q}$ and $\mathfrak{a}$ with an appropriate constant, we can assume that all $a_\mathfrak{q} \in \mathcal{O}$. Furthermore, all but finitely many $a_\mathfrak{q} \in \mathcal{O}_\mathfrak{q}^*$, so assume wlog those are $a_\mathfrak{q} = 1$.

Let $b \in \mathcal{O} \setminus \{0\}$ with $ba_\mathfrak{q}/a_\mathfrak{p} \in \mathcal{O}$ for all finitely many $\mathfrak{q}$, $a_\mathfrak{q} \neq 1$.

Now the Chinese remainder theorem gives us $c \in \mathcal{O}$ such that

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

where $k \geq 1$ is an integer such that $\mathfrak{q}^k\mathcal{O}_\mathfrak{q} \subseteq a_\mathfrak{q}\mathcal{O}_\mathfrak{q}$. Technically, c is only unique modulo $\mathfrak{p} \cap \bigcap_{\mathfrak{q}\neq\mathfrak{p}, a_\mathfrak{q}\neq 1} \mathfrak{q}$, but we are satisfied with any representative.

Now note that $c/b \in \mathcal{O}_\mathfrak{p}^*$. Therefore, we can choose $d \in \mathcal{O} \setminus \mathfrak{p}$ with $dc/b \in \mathcal{O}$. Hence, also $\epsilon := dc/b \in \mathcal{O}_\mathfrak{p}^*$ and $\epsilon \in \mathcal{O}$. We claim that $a_\mathfrak{p}\epsilon \in \mathfrak{a}$ and the claim follows.

We have

- $a_\mathfrak{p}\epsilon \in a_\mathfrak{p}\mathcal{O}_\mathfrak{p}$ since $\epsilon \in \mathcal{O} \subseteq \mathcal{O}_\mathfrak{p}$.
- $a_\mathfrak{p}\epsilon \in a_\mathfrak{q}\mathcal{O}_\mathfrak{q}$ for $\mathfrak{q} \neq \mathfrak{p}$, $a_\mathfrak{q} \neq 1$ since $a_\mathfrak{p}c/b \equiv a_\mathfrak{q} \mod \mathfrak{q}^k$, thus $a_\mathfrak{p}c/b \in a_\mathfrak{q}\mathcal{O}_\mathfrak{q}$ and finally $a_\mathfrak{p}\epsilon = da_\mathfrak{p}c/b \in a_\mathfrak{q}\mathcal{O}_\mathfrak{q}$.
- $a_\mathfrak{p}\epsilon \in a_\mathfrak{q}\mathcal{O}_\mathfrak{q}$ for $\mathfrak{q}$ with $a_\mathfrak{q} = 1$, since $a_\mathfrak{p}, \epsilon \in \mathcal{O}$, thus $a_\mathfrak{p}\epsilon \in \mathcal{O} \subseteq \mathcal{O}_\mathfrak{q} = a_\mathfrak{q}\mathcal{O}_\mathfrak{q}$.

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

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

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 [Neu92, 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 7 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 $\iota : \bigoplus_\mathfrak{p} K^*/\mathcal{O}_\mathfrak{p}^* \to \mathfrak{I}(\mathcal{O})$ 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, $a_\mathfrak{p} = \alpha\epsilon$ 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 $\alpha \in \mathcal{O} \cap \bigcap_\mathfrak{p} R_\mathfrak{p}^* = \mathcal{O}_K^*$, 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 13. *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. 8 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

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

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 [2], and so have

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

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

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

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 14. *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 [Neu92], 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.

Most sources cite [Wat69, 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 15. 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 isogenous 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 16. *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

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

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. □

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 isogenous 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 appropriate subring of K, this shall use that embedding. It will already be used in the next statement, which describes the relationship of endomorphism rings of isogenous curves more concretely.

Proposition 17. *Let $\phi : E \to E'$ be an isogeny of prime degree p between 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

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

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

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 $\mathbb{Z} \oplus f\alpha\mathbb{Z}$, 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 $f_1 \mid pf_2$ and $f_2 \mid pf_1$, so $f_1 \mid pf_2 \mid p^2 f_1$. Since p is prime, we find $f_2 \in \{f_1/p, f_1, pf_1\}$ 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 18. *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* $[\mathrm{End}(E) \otimes \mathbb{Z}_{(l)} : \mathrm{End}(E') \otimes \mathbb{Z}_{(l)}] = l^r$ *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 19. For an ordinary Elliptic Curve E and an integral, invertible ideal [3] $\mathfrak{a} = \mathfrak{b}(p, \pi_E)^r \leq \mathrm{End}(E)$ 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.

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.

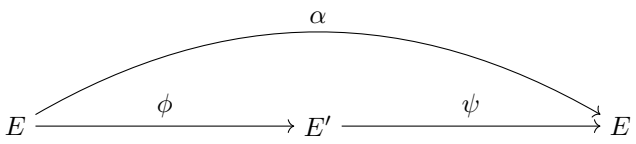
Lemma 20. *Let E be an ordinary Elliptic Curve and $\mathfrak{a} \leq \mathrm{End}(E)$ an integral, invertible ideal. Then $\mathrm{End}(E) \cong \mathrm{End}(E_{\mathfrak{a}})$. In particular, $\phi_{E,\mathfrak{a}}$ is horizontal at every prime l.*

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 $\tau(\hat{\phi}(P)) \notin E[\mathfrak{b}]$ and thus there is $\alpha \in \mathfrak{b}$ with $\tau(\hat{\phi}(P)) \notin \ker(\alpha)$. Note that α factors through ϕ as



[3] By Prop. 10, this representation of an ideal $\mathfrak{a}$ is well-defined and unique, as $\mathfrak{N}((p, \pi)) = p \nmid [\mathcal{O}_{\mathrm{End}(E) \otimes \mathbb{Q}} : \mathrm{End}(E)] \mid d(\mathrm{End}(E))$.

We assume $l \mid \deg(\phi)$, otherwise the claim is trivial. However, then we have the contradiction

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

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

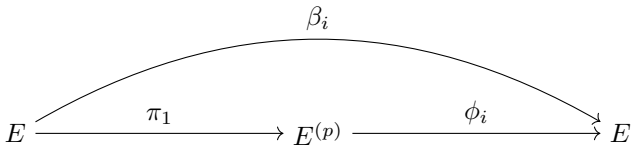
For the next statement, we need to establish the relationship between separability of endomorphisms and properties of the endomorphism ring.

Lemma 21. *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



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. 10 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 22. *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*

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

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 $\tilde{\mathfrak{a}}, \tilde{\mathfrak{b}} \perp (p, \pi)$. For q such that $\phi_{E_\mathfrak{a},\tilde{b}}$ is defined over $\mathbb{F}_q$, it is now the case that

$$\phi_{E,\mathfrak{a}\mathfrak{b}} = \pi_{r+s} \circ \phi_{E,\tilde{\mathfrak{a}}\tilde{\mathfrak{b}}}$$

and

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

where $\pi_r : E_{\tilde{\mathfrak{a}}} \to E_{\tilde{\mathfrak{a}}}^{(p^r)}$ is the p^r-th power Frobenius, and similar for π_s, π_{r+s}. Note that $\phi_{E_\mathfrak{a},\tilde{\mathfrak{b}}}$ is the separable isogeny with kernel $E_\mathfrak{a}[\tilde{\mathfrak{b}}]$ and thus $\phi^{(q/p^r)}_{E_\mathfrak{a},\tilde{\mathfrak{b}}}$ 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

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

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 21, 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 $\ker(\phi_{E_\mathfrak{a},\mathfrak{b}} \circ \phi_{E,\mathfrak{a}}) = E[\mathfrak{a}\mathfrak{b}]$. For simplicity of notation, write $\phi = \phi_{E,\mathfrak{a}}$ and $\psi = \phi_{E_\mathfrak{a},\mathfrak{b}}$. Hence, we want to show that $\ker(\psi \circ \phi) = E[\mathfrak{a}\mathfrak{b}]$.

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

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

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

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

The equality at $(*)$ holds, since

$$i'(\tau) = (\Phi \circ i)(\tau) = \frac{1}{\deg(\phi)} \phi \circ i(\tau) \circ \hat{\phi}$$ □

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

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

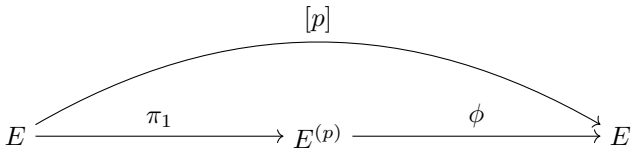
denote the set of isomorphism classes of Elliptic Curves with endomorphism ring $\mathcal{O}$.

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

Lemma 23. *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 $\mathbb{F}_{p^s}$. It follows that $(p,\pi)^s = (\pi)$ and so there is $\alpha' \in \mathcal{O}$, $\alpha' \notin (p,\pi)$ with $(\alpha)(p)^{\lceil r/s\rceil s-r} = (\pi)^{\lceil r/s\rceil}(\alpha')$. 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

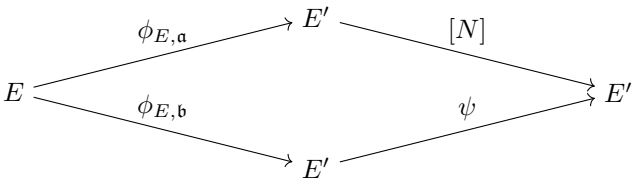


with the p-th power Frobenius π_1 and ϕ is separable with $\ker(\phi) = E[p] = \ker([p]) \cap \ker(\pi - t)$. Thus we see that $E_{(\alpha)} \cong E_{(\alpha')}$ and can assume wlog that $\alpha = \alpha' \notin (p,\pi)$.

By Lemma 21, 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 $[N]^{-1}(E[\mathfrak{a}]) \supseteq E[\mathfrak{b}]$. Note that $[N] \circ \phi_{E,\mathfrak{a}} = \phi_{E,\mathfrak{a}} \circ [N]$ and so the isogeny $[N] \circ \phi_{E,\mathfrak{a}}$ factors through $\phi_{E,\mathfrak{b}}$, i.e. we get a commutative diagram



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

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

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 theory on general abelian varieties, we will present it without proof here. For a proof, the reader is referred to the work of Tate [Tat66].

Theorem 24 (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 25. *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 Theorem 24. 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 an 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 [Wat69, 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

$$T_l E := \lim_n E[l^n]$$

Furthermore, the isogeny ϕ induces a map

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

An endomorphism α of E now acts on $T_l E$, and so $T_l E$ becomes a free $\mathcal{O}_l := (\mathcal{O} \otimes \mathbb{Z}_l)$-module of rank 1. Also $T_l E'$ becomes an $\mathcal{O}_l$-module (this is where we use the assumption that $\mathrm{End}(E) \cong \mathrm{End}(E')$). Additionally, our choice of the canonical isomorphism $\mathrm{End}(E) \cong \mathcal{O} \cong \mathrm{End}(E')$ implies that ϕ_l is 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 $M := \phi_l^{-1}(T_l E') \subseteq T_l E \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$.

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 $\text{ord}(P) = l^m$, 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 11, as only finitely many $(\alpha_l) \neq (1)$ (namely 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 [Wat69]. Notable examples are the CSIDH class group action for supersingular curves defined over $\mathbb{F}_p$ (see [Cas+18]), its generalization to so-called oriented curves (see [CK20]), 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 $\text{Ell}(\mathcal{O})$ 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

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

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

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

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 Volcanoes

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 26. For $l > 0, d \geq 0$, a graph G is called *l-volcano 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[4]
- $G[V]$ 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 "volcano" was introduced by [FM02], after Kohel had mostly determined the structure of ordinary connected components in his PhD thesis.

Theorem 27. *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-volcano. 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.*

Proof. This follows from the class group action and the description of the class group of quadratic imaginary orders (Corollary 14). For the remaining details, we refer the reader to Kohel's thesis [Koh96, Prop. 23]. □

We remark that the crater of a volcano 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.

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 it 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 28. 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

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

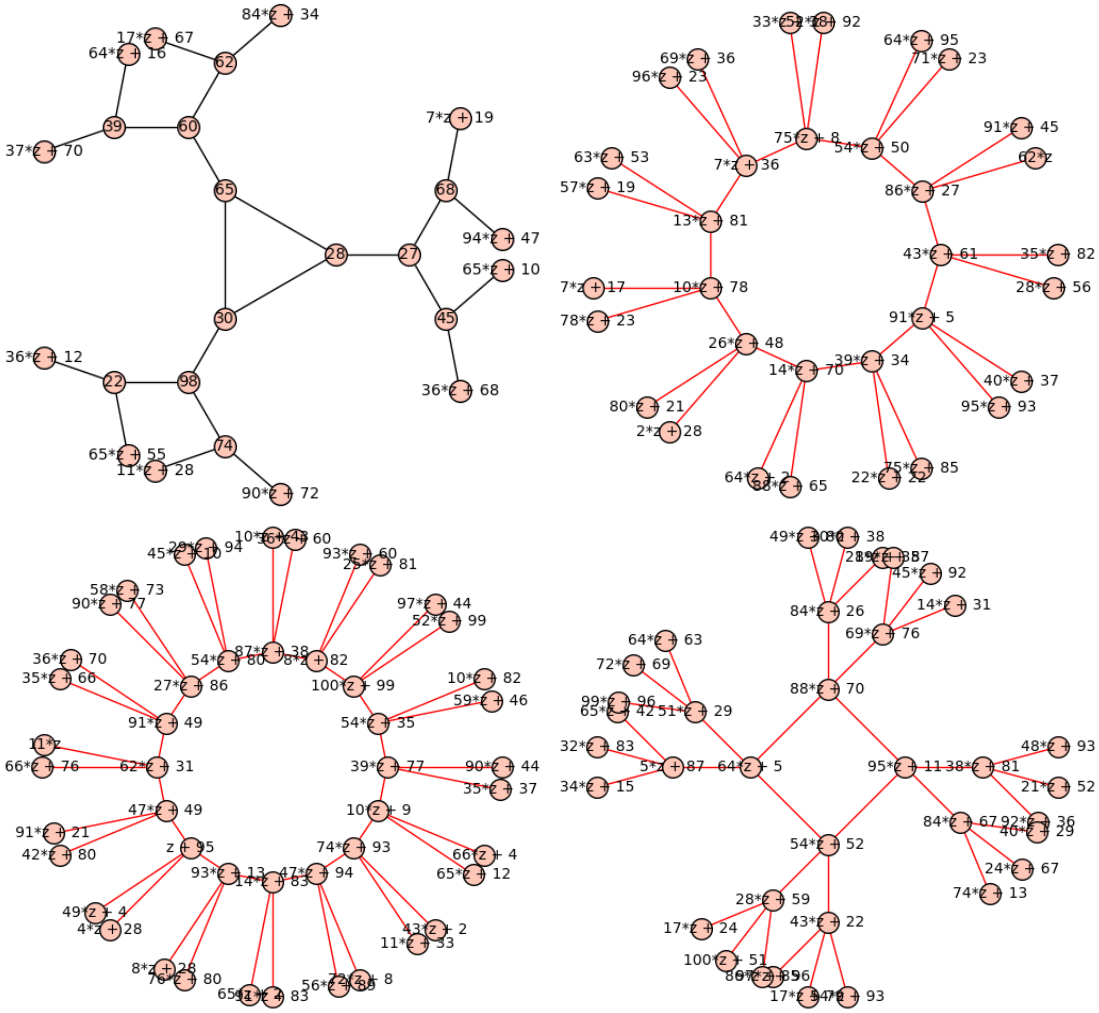


Figure 3.1: Examples of different 2-and 3-isogeny volcanoes in $\mathbb{F}_{101^2}$. The value z is the generator of $\mathbb{F}_{101^2}$ with minimal polynomial $x^2 + 97x + 2$.

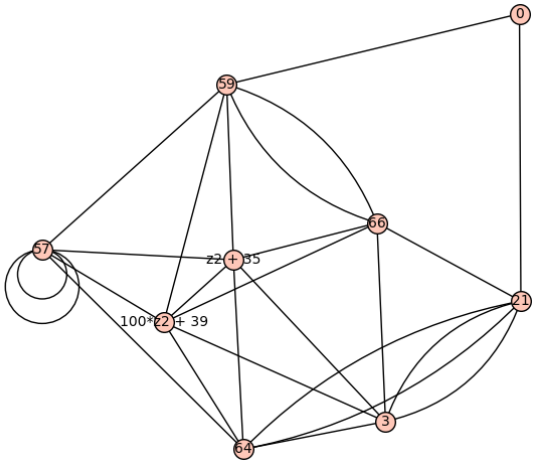


Figure 3.2: The supersingular 3-isogeny graph over $\mathbb{F}_{101^2}$. The element z is a generator of $\mathbb{F}_{101^2}$ as in Figure 3.1.

Proposition 29. *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. [Che69]. □

This inequality only correlates the so-called spectral gap $d - \lambda_2$ with $h(G)$, and does not bound $|\lambda_n|$. 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 28 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 30. 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 that random walks on them mix rapidly. That is, the final vertex of relatively short random walks is distributed almost uniformly among all vertices.

Theorem 31. *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. Theorem 3.3 in this excellent survey on expander graphs [HL06]. 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 32. 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 [5]. 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 33. *For $p \geq 5$, there are exactly*

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

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

For a proof of this statement, see e.g. [Sil09, Thm V.4.1].

In [Piz90], Pizer has now shown that

Theorem 34. *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.

Finally, we also want to shortly comment on supersingular isogeny graphs over $\mathbb{F}_p$.

Remark 35. As we defined it, the graph $\Gamma_l(\mathbb{F}_p)$ is of course a subgraph of $\Gamma_l(\mathbb{F}_{p^2})$. Even so, at least the supersingular part of $\Gamma_l(\mathbb{F}_p)$ is not particularly useful, as most of the structure does not carry over from $\Gamma_l(\mathbb{F}_{p^2})$. For example, it is not $(l+1)$-regular anymore.

Nevertheless, there are many cryptosystems (and other applications) that work with a supersingular l-isogeny graph over $\mathbb{F}_p$. However, they do not use $\Gamma_l(\mathbb{F}_p)$, but a graph G whose vertices are $\mathbb{F}_p$-isomorphism classes of supersingular curves, i.e. curves up to isomorphism defined over $\mathbb{F}_p$. Note that now the j-invariant does not characterize the isomorphism classes anymore, in particular, for every $j \in \mathbb{F}_p$ there are two $\mathbb{F}_p$-isomorphism classes corresponding to this j-invariant. Hence, G is not a subgraph of $\Gamma_l(\mathbb{F}_p)$, and it turns out that its structure is more similar to ordinary isogeny volcanoes than to a supersingular expander graph.

Since these graphs are not used in our work, we will leave it at this short remark.

[5] We will be sloppy here, and call the supersingular l-isogeny graph $(l+1)$-regular, even though it can contain up to two vertices of smaller degree (those with j-invariants 0 and 1728).

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, it 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 [Cox13, §11] for an introduction of the topic. The basic result is the following.

Theorem 36. *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 [Cox13, Thm 11.18]. A few corollaries of this theorem can easily be inferred.

Corollary 37. *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

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

□

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 [Deu41].

Lemma 38. *Let $f \in \mathcal{O}_K[X]$ be a polynomial for some number field K with a prime $\mathfrak{p}$. If $f(X) \bmod \mathfrak{p} \in \mathbb{F}_q[X]$ 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 39. *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*

$$\tilde{E_0} = E, \;\; \tilde{E_0'} = E' \quad \text{and} \quad \tilde{\phi_0} = \phi$$

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[6] $\phi = [u : Yv : w]$ 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 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 $a_j(T_0, ..., T_n)$ 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 any element in $\mathbb{F}_q$.

We know that $u^{(0)}$ is a root of a_0 modulo $\mathfrak{p}$, and so Lemma 38 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.

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

Proposition 40. *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-isogenous curves E_0 and E_0' over a number field K, and so have by Prop. 36 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 38 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. 36, 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 $\mathfrak{p}'$. □

Some properties however cannot be transferred 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 (see Section 4.1) 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 [Sch85] 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 Theorem 36, 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

$$1413599471547213586977534746910713627510046720000$$

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. [BLS11] and [BOS16]. 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

In this chapter, we give an introduction to the basic algorithms and constructions in isogeny-based cryptography. This field began in 2006 with the ideas of Couveignes [Cou06], Rostovtsev and Stolbunov [RS06; Sto10], who proposed a key exchange somewhat similar to the classical Diffie-Hellman, but secure against quantum attacks. Since then, a variety of protocols have been found, for example post-quantum key exchanges (most prominently SIDH [FJP11]), variants of collision resistant hash functions (most prominently the GCL hash function [CGL09]), digital signature schemes (e.g. [GPS16]) and others. The fundamental idea underlying all those methods is to take a random walk in an expander graph, and use that the final curve in the walk seems to be behave in an unpredictable way.

The most general problem that isogeny-based cryptography reduces to, is the *explicit isogeny problem*.

Problem 1. Given two Elliptic Curves E and E' isogenous of fixed degree d, find a d-isogeny $\phi : E \to E'$.

There are algorithms to compute such an isogeny in time polynomial in d, and so we usually are interested in exponentially large degrees d. However, this raises the question on how to even represent the isogeny ϕ. In most cases, we thus require d to be smooth, in which case we can represent an isogeny of degree d as a sequence of small-degree isogenies. This gives us the *smooth isogeny problem*.

Problem 2. Given two Elliptic Curves E and E' isogenous of fixed B-smooth degree d, find a sequence of isogenies

$$E \xrightarrow{\phi_0} E_1 \xrightarrow{\phi_1} \ ... \ \xrightarrow{\phi_{n-1}} E_n \xrightarrow{\phi_n} E'$$

of small degree $\deg(\phi_i) \leq B$.

Finally, if we further restrict the smoothness condition, and require the degree to be a power of a small prime l, we arrive at the *isogeny path problem*.

Problem 3. Given two Elliptic Curves E, E' in the same connected component of $\Gamma_l(\mathbb{F}_q)$, find a path

$$E \to E_1 \to ... \to E_n \to E'$$

in $\Gamma_l(\mathbb{F}_q)$.

This problem is conjectured to be extremely hard, even for quantum computer. Since this is in some sense the reverse problem of doing a random walk in $\Gamma_l(\mathbb{F}_q)$, we easily see that this gives us a one-way function.

Note that many cryptosystems use variants of above problem, e.g. similar to how classical Diffie-Hellman does not rely on the discrete logarithm problem itself, but on a (possibly easier) variant.

Finally, there is another very important problem, the *endomorphism ring problem.*

Problem 4. Given an Elliptic Curve E, find the endomorphism ring $\mathrm{End}(E)$.

There are two possible interpretations of this: Either we are required to compute the isomorphism type of $\mathrm{End}(E)$, i.e. a description of the ring structure of $\mathrm{End}(E)$. In the ordinary case, this could be the discriminant $d(\mathrm{End}(E))$. The stronger interpretation on the other hand would require us to compute generator isogenies of $\mathrm{End}(E)$, again represented as a sequence of small-degree isogenies. It is an interesting and nontrivial fact that in the supersingular case (which is the one we are interested in), both these problems are equivalent to the isogeny path problem [Eis+18]. In other words, if we know $\mathrm{End}(E)$ and $\mathrm{End}(E')$ for supersingular E and E', we can find an isogeny path from E to E'.

While it is technically not a cryptosystem, we first want to present Sutherland's supersingularity test. It is a clever algorithm based on isogeny graphs, and will be important again later.

4.1 Sutherland's supersingularity test

Consider the following problem: Given an Elliptic Curve E over $\mathbb{F}_{p^2}$, determine whether E is supersingular. If the j-invariant $j(E) \neq 0, 1728$, one way could be to check whether $[p] = \pm\pi$ for the p^2-th power Frobenius endomorphism of E. To do this, just sample random points P and check whether $[p](P) = \pm\pi(P)$. If this is the case for many different P, then E is supersingular with high probability [1].

However, this method is only probabilistic and cannot prove that E is supersingular. In particular, in the ordinary case, the nonconstant isogeny $[p] - \pi$ can still have separability degree $O(p)$, and thus have an exponentially large kernel.

Therefore, to prove supersingularity, different methods are needed. Sutherland [Sut12] proposed the following method based on isogeny graphs.

Note that $j(E)$ is in $\mathbb{F}_{p^2}$ if and only if there is a nontrivial element of norm p^2 in $\mathrm{End}(E)$ (either this element or its conjugate must be the p^2-th power Frobenius). Now assume we have an ordinary curve E over $\mathbb{F}_{p^2}$ on the i-th lava flow level in the 2-isogeny volcano. Then the curves on the $(i+j)$-th lava flow level have the endomorphism ring $\mathbb{Z} + 2^j\mathrm{End}(E)$ by Prop. 27. Assuming that $\pi \in \mathbb{Z} + 2^j\mathrm{End}(E)$, we then find that

$$2^{2j}|d(\mathrm{End}(E))| \;\mid\; |d(\mathbb{Z}[\pi])| = 4p^2 - \mathrm{Tr}(\pi) \leq 4p^2$$

Hence $2^{2j} \leq 4p^2$, and so if [2] $j \geq \log_2(p) + 1$, it follows that $\pi \notin \mathbb{Z} + 2^j\mathrm{End}(E)$. In other words, if we go down $\log_2(p) + 1$ levels from E, we encounter a curve not defined over $\mathbb{F}_{p^2}$. On the other hand, the whole supersingular 2-isogeny graph is defined over $\mathbb{F}_{p^2}$, so any path we take ends with a curve defined over $\mathbb{F}_{p^2}$.

[1] We also want to mention that there are more efficient probabilistic algorithms for supersingularity testing, and the above is only for illustrative purposes.

[2] As we will later see, this bound is not optimal. This was first noted by [BGS22], and we present the optimal bound in Prop. 48.

The only obstacle to making this into a supersingularity test is that there is no way how we can "go down" the lava flow, i.e. we do not know which of the 2-isogenies from E to one of its 2-isogeneous neighbors is the descending one. In other words, if we just take any (non-backtracking) path starting from E, we might end up going around the crater of the 2-isogeny volcano, and not down the lava flow. Sutherland's idea now is to simultaneously take three different (non-backtracking) random walks from E, but ensure that they have different second vertices. Hence, one of them will go down one step in the lava flow, and since the lava flow consists of trees, continue to go downwards. This yields Algorithm 1.

Algorithm 1 Sutherland's supersingularity test
Input: A j-invariant j_0
Output: True if the isomorphism class of curves represented by j is supersingular

Compute the modular polynomial Φ_2
Set $j_0^{(0)} = j_0^{(1)} = j_0^{(2)} = j_0$
Set $j_1^{(0)}, j_1^{(1)}, j_1^{(2)}$ to the three roots of $\Phi_2(X, j_0)$
for $k \in \{0, 1, 2\}$ **do**
    for $i = 1$ to $\lfloor \log_2(p) \rfloor$ **do**
        Set $j_{i+1}^{(k)}$ to any root of $\Phi_2(X, j_i^{(k)})$ other than $j_{i-1}^{(k)}$
        if $j_{i+1}^{(k)} \notin \mathbb{F}_{p^2}$ **then return** False
return True

Variants of Sutherland's supersingularity test are still the best deterministic general-purpose supersingularity check. In particular, they are faster than ideas based on point counting. Hence, this algorithm also plays an important role in isogeny-based cryptography, e.g. for key validation.

4.2 Supersingular Isogeny Diffie-Hellman

Even though the Supersingular Isogeny Diffie-Hellman (SIDH) scheme is broken, we think its ideas are important and serve well to illustrate the basic approach in isogeny-based cryptography. Hence, we want to given an overview in this section.

The structure of SIDH is, as the name suggests, somewhat similar to the classical Diffie-Hellman key exchange. The basic idea is that both Alice and Bob take a random walk start from a joint curve E in the supersingular l_A-resp. l_B-isogeny graph, ending at curves E_A and E_B. Now they exchange these curves, and then take the "same" walk on the other curve, i.e. Alice performs the same walk again, but this time starting from E_B and similar for Bob. Hence, Alice ends up at a curve E_{BA} and Bob with a curve E_{AB}. We want that $E_{AB} \cong E_{BA}$, and then $j(E_{AB}) = j(E_{BA})$ can be used as a shared secret key.

However, to achieve this, we need a suitable notion of the "same" walk, starting from a different curve. In the ordinary case, we could realize the "same" walk by a walk given by the same ideal via the class group action. In SIDH, the way to do it is to share some additional information about the isogenies $E \to E_A$ resp. $E \to E_B$.

More concretely, Alice's isogeny $\phi_A : E \to E_A$ is determined by a cyclic subgroup of $E[l_A^{e_A}]$, thus has a generator point $A \in E[l_A^{e_A}]$. Since $E[l_A^{e_A}] \cong (\mathbb{Z}/l_A^{e_A}\mathbb{Z})^2$, it has a $(\mathbb{Z}/l_A^{e_A}\mathbb{Z})$-basis, say P_A and Q_A. Now $A = m_A P_A + n_A Q_A$, and similarly, we have for Bob that $B = m_B P_B + n_B Q_B$ where P_B and Q_B are a basis of $E[l_B^{e_B}]$. After both Alice and Bob exchange their curves E_A and E_B, they also publish the additional points $\phi_A(P_B), \phi_A(Q_B), \phi_B(P_A), \phi_B(Q_A)$. This now allows Alice to take the $l_A^{e_A}$-isogeny from E_B with kernel generated by $m_A\phi_B(P_A) + n_A\phi_B(Q_A)$.

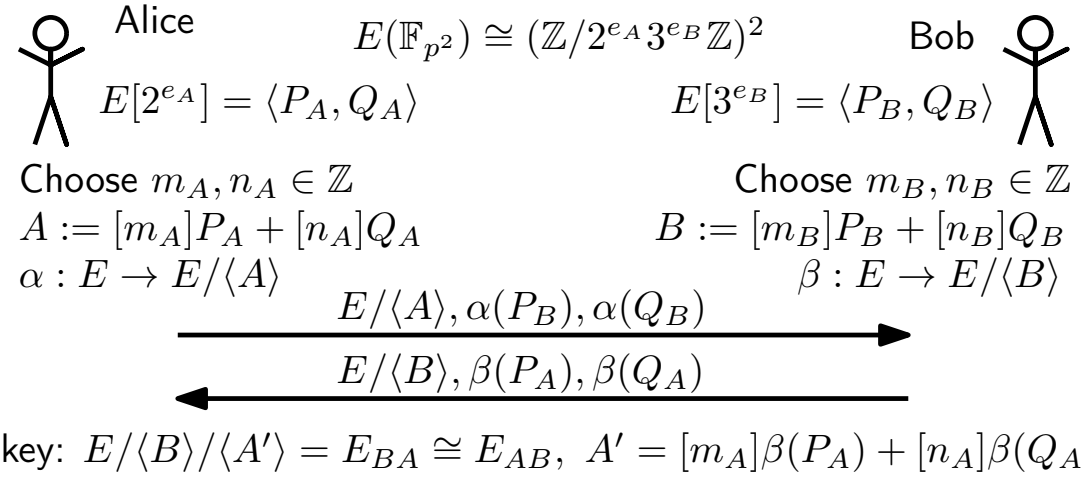


Figure 4.1: The SIDH protocol for $l_A = 2$ and $l_B = 3$.

In other words, the notion of the "same" walk refers to the corresponding isogenies having the same kernel under the isomorphism

$$E[l_A^{e_A}] \xrightarrow{\sim} E_B[l_A^{e_A}], \quad P \mapsto \phi_B(P)$$

Now it is not hard to show that this commutes in an appropriate sense, i.e. $E_{AB} \cong E_{BA}$. This method is also displayed in Figure 4.1.

Note that these additional published points $\phi_A(P_B), \phi_A(Q_B), \phi_B(P_A), \phi_B(Q_A)$ make the security assumption required for SIDH somewhat nonstandard. In particular, it is not enough to assume that the isogeny path problem is hard, and even if we relax this in an analogous way to the classical Diffie-Hellman assumption (i.e. it is impossible to find E_{AB} given E_A and E_B), it does not suffice. As it turns out, this additional information indeed decreases the security, as first mentioned by Cristophe Petit [Pet17]. However, it still was a big shock when [CD22] discovered an efficient attack using these torsion points, bringing the complete demise of SIDH. This is even more surprising, as an SIDH-based cryptosystem named SIKE [Jao+20] was already considered a promising candidate for post-quantum crypto, and made it into the fourth (and final) round of the NIST post-quantum standardization process.

Since SIDH is broken, it does not serve perfectly to motivate the usefulness of a way to generate supersingular curves without revealing a trapdoor. Still, we want to mention that choosing a starting curve with unknown endomorphism ring can prevent the torsion point attacks of [Pet17]. Next, we want to present another, slightly more exotic cryptosystem for which it is important to have a hard starting curve, i.e. a curve for which nobody knows a trapdoor (e.g. the endomorphism ring).

4.3 An isogeny-based verifiable delay function

In this section, we present the verifiable delay function by De Feo, Masson, Petit and Sanso [Feo+19]. A *verifiable delay function* (VDF) as first formalized in [Bon+18] is a cryptographic primitive consisting of three algorithms

- **KeyGen**(λ, T) takes a security parameter λ and a time parameter T and computes a pair (ek, vk) of an evaluation key ek and a verification key vk.
- **Eval**(ek, s) takes the evaluation key and an input s and computes an output a. The key feature is that it should be impossible to compute **Eval** in time less than T, no matter how much parallel computing capabilities are available.
- **Verify**(vk, s, a) takes the verification key, the input s and the output a and checks whether **Eval**$(\text{ek}, s) = a$.

Both **KeyGen** and **Verify** should run in time $O(\text{poly}(\lambda))$, while **Eval** should (of course) run in time T. The security of the VDF consists then of the three properties *Correctness*, *Soundness* and *Sequentiality*. As usual, correctness and soundness refer to the fact that **Verify** accepts correctly computed outputs (i.e. by **Eval**) and declines other outputs, both with probability $1 - 2^{-\lambda}$. The interesting property is sequentiality, which states that it is impossible to compute **Eval**(ek, s) in less than T computational steps, no matter how much parallel processing is available.

Therefore, a verifiable delay function provides a way of ensuring that an output a is only known after a certain amount of wall clock time has elapsed (starting from the point at which the input s is known). Most applications focus on the use to generate public, trusted randomness: Some public entropy source provides the input s, but we assume that an attacker has ways to influence the entropy source (a common example are stock market prices). To prevent an attacker from exploiting this, one now uses the entropy source $a =$ **Eval**(ek, s) instead, which can still be manipulated by the attacker, but not exploited anymore. More concretely, if T is larger than the natural change interval of the source s, an attacker cannot predict fast enough how a manipulation influences the output, and thus not profit from it. There are more applications, for example in blockchain technology.

The isogeny-based VDF from [Feo+19] relaxes this slightly by allowing the setup routine to take time $O(\text{poly}(\lambda, T))$. Apart from that, it satisfies above security properties under some isogeny-related security assumptions. The basic idea is as follows.

The only efficient way we know to evaluate an isogeny $\psi : E \to E'$ of exponential degree l^T is to write it as a sequence

$$E = E_0 \xrightarrow{\psi_1} E_1 \xrightarrow{\psi_2} \ \ldots \ \xrightarrow{\psi_T} E_T = E'$$

of l-isogenies, and then compute the points $P_i = \psi_i(P_{i-1})$ for an input point $P_0 \in E$. Clearly, since P_i depends on P_{i-1}, it is impossible to effectively parallelize that. Hence, it seems like a reasonable security assumption that $\psi(P)$ cannot be evaluated in less than T time steps, and thus can be used for the function **Eval**.

Verification on the other hand can now be done using the Weil pairing. If $P \in E[m]$ (with m coprime to l and p), we have that

$$e_m(\hat{\psi}(P), Q) = e_m(P, \psi(Q))$$

and (assuming that $\hat{\psi}(P)$ is known), we can compute $e_m(\hat{\psi}(P), Q)$ very efficiently. There is just one problem here. The map $e_m(P, \cdot) : E[m] \to \mu_m$ obviously cannot be injective by a cardinality argument, and indeed, given $\psi(Q)$ we can easily compute other points Q' with

$$e_m(P, \psi(Q)) = e_m(P, Q')$$

This obviously violates the soundness of system, as an attacker could compute $Q =$ **Eval**$(\text{ek}, Q) = \psi(Q)$, but then claim Q' to be the result. Verification as above will not detect this. To make it work, [Feo+19] proposes to assume that E is defined over $\mathbb{F}_p$ and use the trace map

$$\text{Tr} : E[m] \to E[m] \cap E(\mathbb{F}_p), \quad P \mapsto P + \pi_E(P)$$

This map is m-to-1, and we have that

$$e_m(P, \mathrm{Tr}(\psi(Q))) = e_m(\hat{\psi}(P), Q)^2$$

which can be used for verification. This now works, since the map $e_m(P, \cdot) : E[m] \cap E(\mathbb{F}_p) \to \mu_m$ is indeed bijective for suitable choices of P. Therefore, we get the scheme displayed in Algorithms 2, 3 and 4.

Algorithm 2 Setup
Input: A security parameter λ and a time parameter T
Output: Curves E and E', an evaluation key $\psi : E' \to E$ and a verification key $(P, \hat{\psi}(P))$

1: Find distinct primes p and m of size depending on λ
2: Find a random supersingular Elliptic Curve E over $\mathbb{F}_p$
3: Take a random walk of length T starting from E in the 2-isogeny graph, given by $\hat{\psi} : E \to E'$
4: Find a random point $P \in E[m]$
5: Compute $\hat{\psi}(P)$
6: **return** ek $= (E, E', \psi)$ and vk $= (E, E', P, \hat{\psi}(P))$

Algorithm 3 Eval
Input: The evaluation key (E, E', ψ) and an input point $Q \in E'[m]$
Output: An output point $Q' \in E[m]$

1: Compute $\psi(Q)$
2: **return** $Q' := \mathrm{Tr}(\psi(Q))$

Algorithm 4 Verify
Input: The verification key $(E, E', P, \hat{\psi}(P))$, an input $Q \in E'[m]$ and an output Q'
Output: An output point $\psi(Q)$

1: **if** $Q' \in \mathrm{im}(\mathrm{Tr}) = E[m] \cap E(\mathbb{F}_p)$ and $e_m(P, Q') = e_m(\hat{\psi}(P), Q)^2$ **then**
2: **return** Valid
3: **else**
4: **return** Invalid

In a practical implementation, we might want to exclude $P \in E[m]$ such that the map $e_m(P, \cdot) : E[m] \cap E(\mathbb{F}_p) \to \mu_m$ is not bijective. This is done in [Feo+19], but we will ignore those cases here. Furthermore, we also will not prove that this is indeed a VDL, again referring the reader to [Feo+19].

However, we do want to discuss step 2 in the setup step, Algorithm 2. In particular, we claim that the curve E has to be generated in a way that does not reveal its endomorphism ring $\mathrm{End}(E)$, or the resulting scheme will be insecure. Hence, the classical methods of using CM techniques and random walks fail here. Since there is currently no known alternative, at the moment this VDF requires a trusted party to generate the curve E, and then forget about its endomorphism ring.

Namely, note that breaking sequentiality of the VDF can be achieved by solving the *isogeny shortcut problem*.

Problem 5. Given an isogeny $\psi : E \to E'$ of exponential degree l^T and a point $Q \in E$, compute $\psi(Q)$ in time less than T.

Since the supersingular isogeny graph is an expander, there exists always a path $E \to E'$ of length $O(\log(p))$. Hence, if $T \in \omega(\log(p))$, we can solve the isogeny shortcut problem by the following three steps

- Find an isogeny $\phi : E \to E'$ of degree at most $l^{O(\log(p))}$
- Find an endomorphism $\alpha \in \mathrm{End}(E')$ such that $\alpha \circ \phi\big|_{E[m]} = \psi\big|_{E[m]}$
- Evaluate $\alpha(\phi(P))$

Using similar techniques to the reductions between the isogeny path problem and the endomorphism ring problem [Eis+18], the authors in [Feo+19] have now shown that all three of these steps are indeed possible in time polynomial in $\log(T)$ if the endomorphism ring $\mathrm{End}(E)$ is known. Hence, anyone who knows the endomorphism ring of the starting curve E from Algorithm 2 can compute **Eval** in time less than T, thus breaking the protocol.

This is one of several examples why the generation of supersingular curves without revealing a trapdoor would be an important tool for cryptography. However, as already mentioned, it is still an open problem to find an algorithm that achieves this. In the next chapter, we will now present the progress we made on this problem.

Chapter 5

Generating supersingular curves

In this chapter, we now come to the main question of this work. We have always talked about the "generation of supersingular curves without revealing a trapdoor", but in fact multiple variants of this problem are conceivable. Following [Boo+22], we thus define the following three problems.

Problem 6 (Demonstrating a hard curve)**.** Given a prime p, compute a supersingular curve E over $\mathbb{F}_{p^2}$ without revealing $\mathrm{End}(E)$.

We can formalize the requirement "without revealing $\mathrm{End}(E)$" as follows. Given E and any random bits passed to the generation algorithm, it should be impossible to compute $\mathrm{End}(E)$. This of course excludes random walk-based methods, since the random bits used for the random walk allows us to repeat the walk, and so find an isogeny $E_0 \to E$ from the starting curve E_0. Using that isogeny, we then can compute $\mathrm{End}(E)$ (assuming we know $\mathrm{End}(E_0)$). Furthermore, it excludes methods that yield curves with very small endomorphism ring, as those endomorphism rings are always efficiently computable.

Note that an algorithm solving the hard curve demonstration problem does not have to be randomized. In fact, it would already be interesting to find just a single hard curve over $\mathbb{F}_{p^2}$ for which nobody knows the endomorphism ring. This is different for the next problem.

Problem 7 (Generating a random hard curve)**.** Given a prime p, compute a random supersingular curve E uniformly selected from some exponentially sized set of supersingular curves over $\mathbb{F}_{p^2}$, without revealing $\mathrm{End}(E)$.

In particular, a solution to the problem can then be used to setup any cryptographic primitive with hard and secure starting curves.

Finally, the most difficult problem is to find a trapdoor-free hash function to the whole set of supersingular curves.

Problem 8 (Hashing into hard curves)**.** Given a prime p and an input string s, deterministically find a supersingular curve E without revealing $\mathrm{End}(E)$. Furthermore, if s is uniform on $\{0,1\}^n$ for a sufficiently large n, the resulting curve E should be uniform among all supersingular curves over $\mathbb{F}_{p^2}$.

An algorithm solving the above problem can then easily be made into a collision-free hash function by prepending it with a secure hash function. Note that for most applications, it would already be sufficient if the above problems could be solved only for certain primes p.

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.

CM methods Using the theory of complex multiplication of curves over $\mathbb{C}$ and their reduction modulo primes, Brökner [Brö07] found an algorithm that can find supersingular curves E over $\mathbb{F}_p$, even for astronomically large primes p. This method is often combined with random walks, as these naturally require a supersingular curve to start the walk from.

However, curves generated with Brökner's method have one drawback. Namely, the algorithm has time complexity polynomial in the discriminant of the endomorphism ring of the considered curves over $\mathbb{C}$, and this endomorphism ring embeds into the endomorphism ring of their reduction mod p. Hence, it is only efficient when generating curves with very small endomorphism rings. This is clearly a weakness, as small endomorphism rings can be computed efficiently, for example by an exhaustive search of all low-degree isogenies.

Polynomial with supersingular roots An idea that is more similar to what we will do next, is to use the following theorem [Sil09, Thm V.4.1].

Theorem 41. *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 [Boo+22] tries to find a random root of this polynomial, by a method similar to the Newton-Raphson iteration. Of course, this is challenging, because it is not even clear how to evaluate $H_p(\lambda)$ efficiently for a given λ.

5.2 Katherine Stange's approach

In our research, we mainly focused on analyzing and improving the second proposal in [Boo+22], which was proposed by Katherine Stange. It 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. [CS21, Thm 4.3], we can derive the following corollary.

Corollary 42. *There are $\Theta(\sqrt{mp})$ supersingular curves E over $\mathbb{F}_{p^2}$ with an m-isogeny to $E^{(p)}$.*

Since $\Phi_n(X, X^p)$ has degree np, it has in total np roots in $\bar{\mathbb{F}}_p$ (assuming it is separable), 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, [Boo+22] proposed to instead take the polynomial

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

The idea to find a root of this is to take a non-square 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. Hence, at least one of n resp. m has to be super-polynomial (or better exponential) 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

$$\exists x_1, ..., x_{e-1} : \ \Phi_l(x, x_1) = \Phi_l(x_1, x_2) = ... = \Phi_l(x_{e-1}, y) = 0$$

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 $e \in \Omega(\log_l(p))$. This follows from our results on expander graphs. More concretely, Theorem 34 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

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

has a nonzero probability of ending in any fixed vertex, by Prop. 31.

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. To begin with, 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 42. Hence, we want to find instances of l, e and m such that above system has only a small amount of ordinary roots, preferably $o(\sqrt{mp})$.

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 43. *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 [Neu92, Korollar VII.5.11].

In [Lit28, Thm 1], it was proven under GRH that $L(1,\chi) \geq \Theta(\sqrt{|d_K|}\log\log|d_K|)$, and the lower bound for $\mathcal{O}_K$ 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 14, 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 $\mathfrak{f} = f\mathcal{O}_K$. 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

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

since in the case $(-d_K/p) = 1$, 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. □

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 volcano 27, in particular

- If $l \mid d_K$, i.e. is ramified in $\mathcal{O}_K$, the crater consists of two vertices with an edge (or a single vertex with a single loop). Since the whole graph is $(l+1)$-regular, a crater vertex has l neighbors outside the crater. Thus, the class number of the first level is $h(\mathbb{Z} + l\mathcal{O}_K) = lh(\mathcal{O}_K)$.
- If $-d_K$ is a quadratic residue mod l, then l splits in $\mathcal{O}_K$ and so the crater is a cycle (or a single vertex with a double loop). 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. 10, 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 (or equivalently 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 discriminants 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, it is now easy to properly lower bound 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 $x \perp y$ of the Diophantine equation

$$x^2 + gy^2 = mp$$

where $\mathrm{End}(E) \cong \mathbb{Z}[\sqrt{g}]$, i.e. $D := d(\mathrm{End}(E)) = 4g$. Note that we want a lower bound (we have an upper bound by the degree argument), and so we can ignore the possibilities in which $\mathrm{End}(E)$ is not of this form (i.e. $\mathrm{End}(E) \cong \mathbb{Z}[(1 + \sqrt{g})/2]$).

Furthermore, at the moment we content ourselves with a very crude estimate, but note that everything can be made rigorous. We do that later with a very similar argument in Prop. 48. Neglecting log-factors, we now have

$$\begin{aligned}
\#\{j \in \bar{\mathbb{F}}_p \mid \Phi_m(j, j^p) = 0\} &\geq \sum_{\substack{x^2 - gy^2 = mp \text{ solvable} \\ \text{with } x \perp y}} h(4g) \\
&\geq \sum_{0 < x < \sqrt{mp}} h(4x^2 - 4mp) \approx \sum_{0 < x < \sqrt{mp}} 2\sqrt{mp - x^2} \\
&\approx 2 \int_0^{\sqrt{mp}} \sqrt{mp - x^2} dx = 2mp \int_0^1 \sqrt{1 - x^2} dx \in \Omega(mp)
\end{aligned}$$

None of the ways we consider to capture supersingularity by modular polynomials can completely exclude ordinary roots. This is because if an ordinary curve defined over $\mathbb{F}_p$ with endomorphisms

[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 $n \geq 2$.

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 this is not a problem, as those ordinary roots are very rare.

Proposition 44. *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. Assume that $\mathcal{O}$ is an imaginary quadratic order with $p \nmid d(\mathcal{O})$ that has a nontrivial element $\beta \in \mathcal{O} \setminus \mathbb{Z}$ of norm n. 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 nontrivial n-endomorphism is bounded by

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

This shows the claim. □

This is now as far as we can go in 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

$$\{d(\mathcal{O}) \mid \mathcal{O} \text{ has cyclic endomorphism of degree } m\} \supseteq \{4(m - x^2) \mid 0 < x < \sqrt{m}\}$$

and an appropriate converse.

While the Diophantine equation $x^2 + \frac{D}{4}y^2 = m$ has been thoroughly studied (see e.g. [Cox13]), 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. In particular, if we choose m such that there is a simple relationship between Φ_m and Φ_{l^e}, we can do something. One situation in which everything works out is presented next. In contrast to most of the other arguments we make in this section, here we argue (almost) solely with the structure of isogeny volcanoes.

Proposition 45. *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 in $\mathbb{F}_{p^2}$ [2].

[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 $(x, x_1, ..., x_{e-1})$.

Proof. We show that every ordinary root $j \in \mathbb{F}_{p^2}$ of F_{p,l^f,l^e} has an endomorphism of degree at most l^{2f} and the claim follows by Prop. 44.

For any ordinary curve E, denote now by E_R the unique vertex in the crater of the l-isogeny volcano of E that is connected to the lava flow tree of E (in particular, $E_R = E$ if E already lies on the crater). 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, by the functoriality of $\cdot^{(p)}$.

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 volcano 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 nontrivial endomorphism

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

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

If $j(E_R) \notin \mathbb{F}_p$, then $E_R \ncong E_R^{(p)}$. 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 (E_R is defined over $\mathbb{F}_{p^2}$, so $[(p, \pi)]^2 = 1$), and its generator gives a nontrivial endomorphism ϕ of $\mathrm{End}(E_R)$ of degree l^{2f-4i}. 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 nontrivial endomorphism of E with degree $l^{2f-2i} \leq l^{2f}$, so we are done.

If (l) is inert in $\mathcal{O}$, the crater only has a single vertex. Since we have $E_R \ncong E_R^{(p)}$ are both curves in a crater, we see that they must be in different l-isogeny volcanoes. 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 volcano 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. □

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 noticeable, i.e. $1/\text{poly}(\log(p))$, but even exponentially large. In particular, this proves our main result Prop. 1. Furthermore an algorithm that is able to efficiently compute a random root of F_{p,l^f,l^e} over $\mathbb{F}_{p^2}$ 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. Next, we try to demonstrate this in one example.

Example 46. Assume we choose $p = 51$, $l = 3$, $f = 3$ and $e = 4$. Then e is somewhat smaller than the bound required to have $\Phi_{l^e}(j_1, j_2) = 0$ for all supersingular j_1, j_2. Still, we expect that most roots of f_{p,l^f,l^e} are supersingular. We have that

$$\begin{aligned}\Phi_3 = &- x^3y^3 + 6x^3y^2 + 6x^2y^3 + x^4 + 8x^3y + 7x^2y^2 + 8xy^3 + y^4 + 9x^3 \\ &+ 12x^2y + 12xy^2 + 9y^3 - 26x^2 + 5xy - 26y^2 - 26x - 26y\end{aligned}$$

and hence, Φ_{l^f} and Φ_{l^e} are huge, having 1240 resp. 11162 monomials. However, we can still compute f_{p,l^f,l^e}, which is a polynomial of degree 156. It has the F_{p^2}-roots

$$39, 52\alpha + 42, \alpha + 38, 0, 46, 44\alpha + 46, 9\alpha + 10, 50$$

Of those, 0, 50, 46, $9\alpha + 10$ and $44\alpha + 46$ are supersingular, and the other three are ordinary. The corresponding 3-isogeny graphs are displayed in Figure 5.1. Note that all ordinary solutions are in a volcano with a curve that has a nontrivial 3-endomorphism.

It is a fact that this example cannot completely show that the method works, and most roots are supersingular. It would be much preferable if we could choose larger parameters, such that $\sqrt{p}$ and polynomial in $\log(p)$ look very different. However, we very soon hit the limits of computers - just remember that Φ_{34} already has 11162 monomials.

Also 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 $\log_l(p)$. Already for $l = 3$ and $e = 4$, it is very slow and takes time in the range of minutes. The original paper [Boo+22] thought it might be possible to use a "square-and-multiply" approach to compute the resultant

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

for some $\delta = \sqrt{a}$ with a non-square $a \in \mathbb{F}_p^*$. However 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.

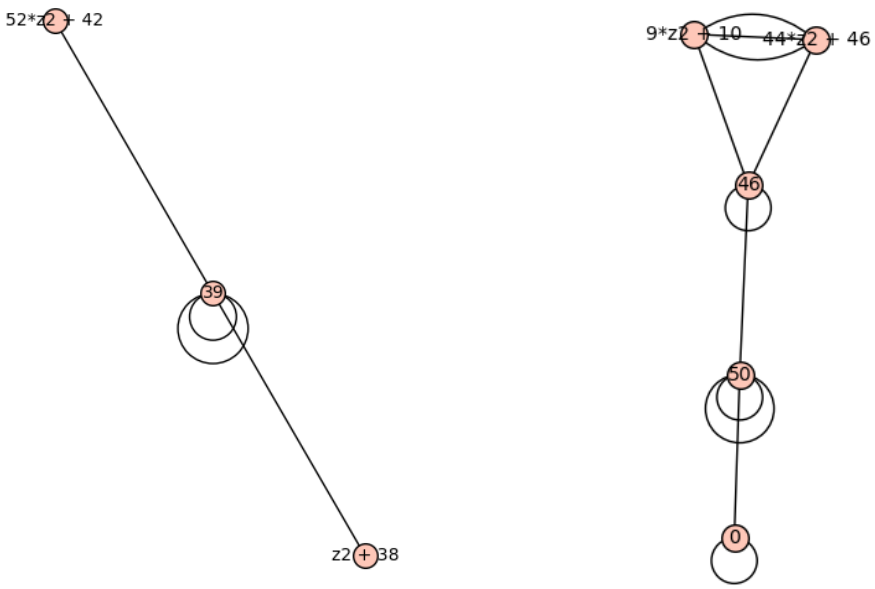


Figure 5.1: Ordinary 3-isogeny volcano (left) and supersingular 3-isogeny graph (right) over $\mathbb{F}_{51^2}$, where z2 $= \alpha$ is a generator of $\mathbb{F}_{51^2}$.

The basic idea is to use Sutherland's supersingularity test (see Section 4.1). Namely, if we take three non-backtracking walks away from an ordinary starting curve E_0 (such that the second vertices are distinct), then at least one of them will descend into a lava flow, and encounter a curve not defined over $\mathbb{F}_{p^2}$ after polynomially many steps. On the other hand, if we do the same starting from a supersingular curve, this will not happen, as the whole supersingular isogeny graph is defined over $\mathbb{F}_{p^2}$.

We have already seen that $\log_l(p)$ steps are sufficient, which is also Sutherland's original choice. However, this is not optimal, and in our case, we are also interested in how many ordinary curves we will accept if we choose n smaller than the optimal bound. In particular, our method can deal with a small number of ordinary roots (e.g. polynomially many), it should just not exponentially exceed the number of supersingular roots. All this is considered in the next two propositions, which are again phrased in the language of endomorphism rings.

Proposition 47. *Let p be an odd prime and $m \geq 2$ an integer. 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 of $\mathcal{O}$. Then*

$$\left\lfloor \frac{2p}{m^2} \right\rfloor \leq n \leq \left\lfloor \frac{2p^2}{m^2} \right\rfloor$$

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 have then for $m^2 \leq 2p$ that

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

Finally, if $m^2 \geq 4p^2$, we have $n = N = 0$.

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

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

Thus the imaginary quadratic order $\mathcal{O} := \mathbb{Z}[\sqrt{g}]$ with discriminant $D := 4g$ contains a non-trivial element of norm p^2, which must be the Frobenius π (or its conjugate). 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 $\mathcal{O}_0$, since $d(\mathcal{O}_0) = 4a(am^2 - 2p)$, and the first lower bound follows.

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 $\#\mathrm{Cl}(\mathcal{O}_0)$ curves with that endomorphism ring. Under GRH, Theorem 43 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 imaginary quadratic order $\mathcal{O}$ with $\pi \in \mathcal{O}$. Then clearly $d(\mathcal{O}) \mid d(\mathbb{Z}[\pi]) = t^2 - 4p^2$, where t is the trace of π. Thus we see that $|d(\mathcal{O})| \leq 4p^2$. If now $\mathcal{O} = \mathbb{Z} + m\mathcal{O}_0$ for some order $\mathcal{O}_0$, we know that

$$d(\mathcal{O}) = [\mathcal{O} : \mathcal{O}_0]^2 d(\mathcal{O}_0) = m^2 d(\mathcal{O}_0)$$

and so $-4p^2/m^2 \leq d(\mathcal{O}_0) < 0$. Furthermore, only half of the $d \geq -4p^2/m^2$ are congruent to $0, 1$ modulo 4, i.e. are fundamental discriminants. Therefore, there are at most $\lfloor 2p^2/m^2 \rfloor$ different endomorphism rings $\mathcal{O}_0$ with $\pi \in \mathbb{Z} + m\mathcal{O}_0$.

For a lower bound on the curves, just note that

$$\#\{j \in \mathbb{F}_{p^2} \mid \pi \in \mathbb{Z} + m\mathrm{End}(j)\} \leq \sum_{-4p^2/m^2 \leq D < 0} h(D)$$

Using the bound on the class number from Prop. 43, we can bound this by

$$\begin{aligned}&\sum_{D=1}^{\lfloor 4p^2/m^2\rfloor}\sqrt{D}\log(D)^2 \leq \Theta(\log(p)^2)\int_1^{\lfloor 4p^2/m^2\rfloor+1}\sqrt{x}dx\\ =&\Theta(\log(p)^2)\int_0^{4p^2/m^2}\sqrt{x}dx = \Theta(\log(p)^2)\frac{4p^2}{m}\int_0^1\sqrt{x}dx\\ =&\Theta\left(\frac{p^3\log(p)^2}{m^3}\right)\end{aligned}$$

This estimate is valid, since $\sqrt{x}$ is increasing and $\sqrt{\lfloor 4p^2/m^2\rfloor+1}/\sqrt{4p^2/m^2}\in O(1)$. This shows the claim. □

Note that the bound for the number of curves is not very tight. In particular, there is a factor of more that p between upper and lower bound. In the case that $m=l^e$ is a prime power (this is the case of the levels in an l-isogeny volcano), we get a much clearer picture.

Proposition 48. *Let p be an odd prime and $m=l^e$ a prime power with $l\neq 2,p$. Then we have for the numbers n resp. N from the previous proposition 47 the following improved upper bounds*

$$n\leq\left\lfloor\frac{16p^2}{m^3}\right\rfloor$$

and

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

Furthermore, if $m^2>4p$, we have that $n=N=0$.

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

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

Since m is odd, we see that m must be coprime to either $t-2p$ or $t+2p$ (it does not divide $4p$). Note that here, we use the assumption that m is a prime power.

If $m^2\mid t+2p$, then $t\in\{m^2-2p,2m^2-2p,...,km^2-2p\}$ where $k=\lfloor 4p/m^2\rfloor$.

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

In particular, there are at most $2k$ different choices for t. Additionally, it clearly implies that if $m^2>4p$, we have $k=0$ and so $n=N=0$.

Otherwise, 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

$$2k\frac{2p}{m}\leq\frac{16p^2}{m^3}$$

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

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

Note that

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

Thus we can upper bound the previous sum by

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

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 have no good description of Φ_m, we can again consider the paths explicitly. More concretely, assume that $m = l^n$. We use 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 volcanoes (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

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

The additional constraints $\Phi_{l^2}(u_i, u_{i+2})$ ensure that $u_i \neq u_{i+2}$, unless the curve of j-invariant u_i has a cyclic endomorphism of size l^2. However, this means that its endomorphism ring has polynomially large discriminant, and again there are only polynomially many such curves by Prop. 44. Hence, a root of above system is supersingular with probability $1 - 1/\text{poly}(\log(p))$.

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 do the computations, even though there are still some serious obstacles.

Proposition 49. *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. $\mathcal{O} = \mathbb{Z} \oplus \alpha\mathbb{Z}$. Then $\mathbb{Z} + l_i\mathcal{O} = \mathbb{Z} \oplus l_i\alpha\mathbb{Z}$. Furthermore, as an element of $\mathcal{O}$, the Frobenius π has a unique representation $\pi = a + b\alpha$ with integers a and b. 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

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

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 $\prod_i l_i \geq 2p$. Note that from these results, our second main result Prop. 2 follows.

5.3.2 A more explicit representation

In the hope of making computations easier, we can try to transform our system further. For this, we first need the following lemma.

Lemma 50. *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 lower-dimensional subvariety. Clearly, both of them commute in the above sense. □

We can also explicitly compute the polynomial division of $y^{p^2-1}-1$ modulo $\Phi_l(x,y)$. Note that $y^{p^2-1}-1$ is the only polynomial of exponential degree, and getting rid of it would be very nice.

Lemma 51. *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

$$b = A^{p^2-l-1}e_1 \quad \text{for the first unit vector } e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

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

$$A = \begin{pmatrix} -a_l & 1 & 0 & \dots & 0 \\ -a_{l-1} & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -a_1 & 0 & 0 & \dots & 1 \\ -a_0 & 0 & 0 & \dots & 0 \end{pmatrix} \in k[x]^{(l+1)\times(l+1)}$$

where

$$\Phi_l(x,y) = \sum_{i=0}^{l+1} a_i(x) y^i \in k[x][y]$$

as univariate polynomial over $k[x]$.

Proof. We just perform univariate polynomial division of $y^{p^2-1}-1$ by $\Phi_l(x,y)$ in $k[x][y]$.

Define a sequence of polynomials in $k[x,y]$ by

$$f_0 := y^{p^2-1} \quad \text{and} \quad f_{i+1} = f_i - \mathrm{lc}(f_i)\Phi_l(x,y)y^{p^2-l-2-i}$$

Here, $\mathrm{lc}(f_i)$ refers to the appropriate value when considering f_i as a univariate polynomial over $k[x]$, in particular $\mathrm{lc}(f_i) \in k[x]$. This clearly implies that $f_i \equiv f_j \mod \Phi_l(x,y)$. We show that

$$f_i = \begin{pmatrix} y^{p^2-1-i} \\ \vdots \\ y^{p^2-l-1-i} \end{pmatrix}^T A^i e_1$$

To see that this is true, note that f_i contains only the monomials $y^{p^2-1-i}, ..., y^{p^2-l-1-i}$ (technically, by induction hypothesis). Hence, we can write

$$f_i = y^{p^2-l-1-i} \sum_{j=0}^{l} c_j y^j$$

Since $a_{l+1} = 1$, it follows that

$$\begin{aligned} f_{i+1} =& y^{p^2-l-1-i}\Big(\sum_{j=0}^{l}(c_j - c_l a_{j+1})y^j\Big) - y^{p^2-l-2-i}c_l a_0 \\ =& y^{p^2-l-1-(i+1)} \sum_{j=0}^{l}(c_{j-1} - c_l a_j)y^j \end{aligned}$$

where we define $c_{-1} = 0$. Now we have

$$\begin{pmatrix} c_{l-1} - c_l a_l \\ \vdots \\ c_0 - c_l a_1 \\ -c_l a_0 \end{pmatrix} = A \begin{pmatrix} c_l \\ \vdots \\ c_1 \\ c_0 \end{pmatrix}$$

and the claim follows. □

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

$$\begin{aligned} &\langle \Phi_{l_i}(x,u_i), \Phi_{l_i}(x,v_i), \Phi_{l_i}(x,w_i), \\ &\Phi_{2l_i}(u_i,v_i), \Phi_{2l_i}(u_i,w_i), \Phi_{2l_i}(v_i,w_i), \\ &\begin{pmatrix} u_i^l \\ \vdots \\ 1 \end{pmatrix}^T B - 1, \begin{pmatrix} v_i^l \\ \vdots \\ 1 \end{pmatrix}^T B - 1, \begin{pmatrix} w_i^l \\ \vdots \\ 1 \end{pmatrix}^T B - 1 \rangle \cap k[x,B] \end{aligned} \tag{5.1}$$

This might now be done, since all polynomials we consider now are of polynomial degree. Next, 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

$$f_{ij}(x, b_i) \quad \text{where} \quad b_i = A_i^{p^2-l-1} e_1$$

for the matrices A_i given by Lemma 51. 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 $\Theta(p)$ supersingular j-invariants and polylogarithmically many ordinary j-invariants as roots).

Nevertheless, we should also mention that the computation of the elimination ideal from 5.1 is not trivial either. The product of the considered primes l_i must be at least $2p$, and so the largest ones are $\Theta(\log(p)/\log\log(p))$. In particular, we have to perform elimination in a polynomial ring with polynomially many unknowns. Hence, a standard Groebner basis will have exponential runtime. However, we only have to eliminate a constant number of variables, namely u_i, v_i and w_i, so there might be a way to compute a "partial" Groebner basis that still yields generators of the elimination ideal. We have not studied this in depth, as finding a joint root of the $f_{ij}(x, b_i)$ seems to be a more fundamental problem.

Chapter 6

Conclusion

In this work, we have seen some polynomial-based approaches to solving a main open problem in the field of isogeny-based cryptography: Can we efficiently generate random, hard supersingular curves without revealing the endomorphism ring, or other information that can serve as a trapdoor?

The main focus was an idea of Katherine Stange, which relied on modular polynomials. In the general case, its asymptotic success probability (i.e. the probability of finding a supersingular curve) is not so easy to study, since it is closely tied to the structure of the class group in quadratic imaginary orders. However, we were able to describe the success probability in special cases, and prove that it is sufficiently high.

Furthermore, we worked on the main problem of the method, namely that one has to work with polynomials of exponential degree. We showed how in some cases, one can instead choose to work with polynomial systems in many variables, and presented a similar idea whose system might have an easier structure. However, we have also seen that Groebner basis methods to find solutions to these polynomial systems have exponential running time, and so we still cannot compute random supersingular curves efficiently.

As already noted in [Boo+22], there are alternatives to Groebner bases, e.g. [Roj99] which can be much faster for sparse polynomial systems. It is a question for further research whether these give a significant speedup, or whether we can modify our methods to yield polynomial systems better suited for this solving algorithms.

There is also the question whether there might be some "square-and-multiply" algorithm to compute the polynomial f_{p,l^f,l^e}, as mentioned as the "dream approach" in [Boo+22]. Of course, this would require new methods to compute information about Φ_n for exponential n.

Another possible direction for future research is to see if we can use reduction theory to instead solve a polynomial system over the complex numbers $\mathbb{C}$. In this setting, we might then be able to use numeric techniques, like Newton's method. Of course, to transfer a solution over $\mathbb{C}$ back to finite fields, we require that the solution is an algebraic integer, and we need to find a representation that allows computing the reduction modulo p. However, the former is not a problem at all if the solution is given by a polynomial system. Furthermore, we might be able to address the second point by using the LLL algorithm or similar techniques, which can give us the minimal polynomial of the numerical approximation to an algebraic integer, if it has polynomial degree. This excludes CM curves, but there are many more non-CM curves with j-invariant in small-degree number fields that reduce to supersingular curves.

Finally, there are also completely different approaches. In particular, [Boo+22] mentioned one idea based on higher-genus varieties, and an idea trying to use quantum computing. For

the later, one main challenge is that the classical way of formalizing "without revealing the endomorphism ring" does not apply to the quantum setting anymore, as randomization is not given by random bits anymore, but intrinsic to the computation process.

All in all, this is a very interesting and important problem, and it is not yet clear what shape a potential solution might have.

Bibliography

[BGS22] 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. URL: https://ia.cr/2022/880.

[Bon+18] Dan Boneh et al. *Verifiable Delay Functions*. Cryptology ePrint Archive, Paper 2018/601. 2018. URL: https://eprint.iacr.org/2018/601.

[Boo+22] Jeremy Booher et al. *Failing to hash into supersingular isogeny graphs*. Cryptology ePrint Archive, Report 2022/518. 2022. URL: https://ia.cr/2022/518.

[Brö07] Reinier Bröker. "Constructing supersingular Elliptic Curves". In: 2007.

[BLS11] Reinier Bröker, Kristin Lauter, and Andrew V. Sutherland. "Modular polynomials via isogeny volcanoes". In: *Mathematics of Computation* 81.278 (2011), pp. 1201–1231.

[BOS16] Jan Hendrik Bruinier, Ken Ono, and Andrew V. Sutherland. "Class polynomials for nonholomorphic modular functions". In: *Journal of Number Theory* 161 (2016), pp. 204–229.

[BF20] Jeffrey Burdges and Luca De Feo. *Delay Encryption*. Cryptology ePrint Archive, Paper 2020/638. 2020. URL: https://eprint.iacr.org/2020/638.

[CD22] Wouter Castryck and Thomas Decru. *An efficient key recovery attack on SIDH (preliminary version)*. Cryptology ePrint Archive, Paper 2022/975. 2022. URL: https://eprint.iacr.org/2022/975.

[Cas+18] Wouter Castryck et al. *CSIDH: An Efficient Post-Quantum Commutative Group Action*. Cryptology ePrint Archive, Paper 2018/383. 2018. URL: https://eprint.iacr.org/2018/383.

[CGL09] Denis Xavier Charles, Eyal Z. Goren, and Kristin E. Lauter. "Cryptographic Hash Functions from Expander Graphs". In: *J. Cryptology* 22 (2009), pp. 93–113. DOI: 10.1007/s00145-007-9002-x.

[Che69] Jeff Cheeger. "A lower bound for the smallest eigenvalue of the Laplacian". English (US). In: *Proceedings of the Princeton conference in honor of Professor S. Bochner*. 1969, pp. 195–199.

[CS21] Mathilde Chenu and Benjamin Smith. "Higher-degree supersingular group actions". In: *CoRR* abs/2107.08832 (2021).

[CK20] Leonardo Colò and David Kohel. *Orienting supersingular isogeny graphs*. Cryptology ePrint Archive, Paper 2020/985. 2020. URL: https://eprint.iacr.org/2020/985.

[Cou06] Jean-Marc Couveignes. *Hard Homogeneous Spaces*. Cryptology ePrint Archive, Paper 2006/291. 2006. URL: https://eprint.iacr.org/2006/291.

[Cox13] David A Cox. *Primes of the Form X2+ny2: Fermat, Class Field Theory, and Complex Multiplication*. John Wiley & Sons, Incorporated, 2013.

[Deu41] Max Deuring. "Die Typen der Multiplikatorenringe elliptischer Funktionenkörper". In: *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg* 14 (1941), pp. 197–272.

[Eis+18] Kirsten Eisentraeger et al. *Supersingular isogeny graphs and endomorphism rings: reductions and solutions*. Cryptology ePrint Archive, Paper 2018/371. 2018. URL: https://eprint.iacr.org/2018/371.

[FJP11] Luca De Feo, David Jao, and Jérôme Plût. *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies*. Cryptology ePrint Archive, Paper 2011/506. 2011. URL: https://eprint.iacr.org/2011/506.

[Feo+19] Luca De Feo et al. *Verifiable Delay Functions from Supersingular Isogenies and Pairings*. Cryptology ePrint Archive, Paper 2019/166. 2019. URL: https://eprint.iacr.org/2019/166.

[FM02] Mireille Fouquet and François Morain. "Isogeny Volcanoes and the SEA Algorithm". In: *Algorithmic Number Theory*. Ed. by Claus Fieker and David R. Kohel. Springer Berlin Heidelberg, 2002, pp. 276–291.

[GPS16] Steven D. Galbraith, Christophe Petit, and Javier Silva. *Identification Protocols and Signature Schemes Based on Supersingular Isogeny Problems*. Cryptology ePrint Archive, Paper 2016/1154. 2016. URL: https://eprint.iacr.org/2016/1154.

[HL06] Shlomo Hoory and Nathan Linial. "Expander Graphs and their Applications". In: *Bulletin of the American Mathematical Society* 43 (2006), pp. 439–561.

[Jao+20] David Jao et al. *Supersingular Isogeny Key Encapsulation*. NIST PQC candidate specification. Oct. 2020. URL: https://sike.org/.

[Koh96] David Kohel. "Endomorphism rings of elliptic curves over finite fields". PhD thesis. University of California at Berkeley, 1996.

[Lit28] J. E. Littlewood. "On the Class-Number of the Corpus $\mathbb{Q}(\sqrt{-k})$". In: *Proceedings of the London Mathematical Society* s2-27.1 (1928), pp. 358–372.

[MMP22] Marzio Mula, Nadir Murru, and Federico Pintore. *On Random Sampling of Supersingular Elliptic Curves*. Cryptology ePrint Archive, Paper 2022/528. 2022. URL: https://eprint.iacr.org/2022/528.

[Neu92] Juergen Neukirch. *Algebraische Zahlentheorie*. Springer, 1992.

[Pet17] Christophe Petit. *Faster Algorithms for Isogeny Problems using Torsion Point Images*. Cryptology ePrint Archive, Paper 2017/571. 2017. URL: https://eprint.iacr.org/2017/571.

[Piz90] Arnold Pizer. "Ramanujan graphs and Hecke operators". In: *Bulletin of the American Mathematical Society* 23 (1990), pp. 127–137.

[Roj99] J.Maurice Rojas. "Solving Degenerate Sparse Polynomial Systems Faster". In: *Journal of Symbolic Computation* 28.1 (1999), pp. 155–186.

[RS06] Alexander Rostovtsev and Anton Stolbunov. *PUBLIC-KEY CRYPTOSYSTEM BASED ON ISOGENIES*. Cryptology ePrint Archive, Paper 2006/145. 2006. URL: https://eprint.iacr.org/2006/145.

[Sch85] René Schoof. "Elliptic Curves Over Finite Fields and the Computation of Square Roots mod p". In: *Mathematics of Computation* 44.170 (1985), pp. 483–494.

[Sil09] Joseph Silverman. *The Arithmetic of Elliptic Curves*. Springer, 2009.

[Sto10] Anton Stolbunov. "Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves". In: *Advances in Mathematics of Communications* 4.2 (2010), pp. 215–235.

[Sut12] Andrew V. Sutherland. "Identifying supersingular elliptic curves". In: *LMS Journal of Computation and Mathematics* 15 (2012), pp. 317–325.

[Tat66] J. Tate. "Endomorphisms of Abelian Varieties over Finite Fields." In: *Inventiones mathematicae* 2 (1966), pp. 134–144. URL: http://eudml.org/doc/141848.

[Wat69] William C. Waterhouse. "Abelian varieties over finite fields". In: *Annales scientifiques de l'École Normale Supérieure* Ser. 4, 2.4 (1969), pp. 521–560.