Mathematics of Isogeny Based Cryptography

Luca De Feo

Université de Versailles, France
Inria Saclay, Palaiseau, France
IBM Research Europe, Zürich, Switzerland
https://defeo.lu/

Marc Houben

Universiteit Leiden, Netherlands
KU Leuven, Belgium

v1 – May 2017, Thiès, Senegal
v2 – August 2019, Würzburg, Germany
v3 – October 2023, Popayan, Colombia & Rabat, Morocco

Preface

These lecture notes were first written in 2017 for a summer school on *Mathematics for post-quantum cryptography* held in Thiès, Senegal, under the patronage of the *Écoles Mathématiques Africaines* program and of CIMPA. This version is archived as [21].

The second revision [21] appeared in 2019 at the summer school *Graph Theory Meets Cryptography* in Wurzbürg, Germany. It largely reorganized contents and added material on the newly discovered CSIDH.

This third revision was written between 2022 and 2023 for three summer schools:

- crypt@b-it in Bonn, Germany;
- The CIMPA research school on "Isogenies of elliptic curves and their applications to cryptography" in Popayan, Colombia; and
- The CIMPA research school on "Mathematical aspects of post-quantum cryptography" in Rabat, Morocco.

Coming after the discovery of polynomial-time attacks on SIDH and a major reshaping of the entire field, it features several important changes and the addition of Part IV. It also welcomes a new co-author in Marc Houben, who was first a student in Bonn and then a lecturer in Popayan.

Over the course of these 6 years, isogeny based cryptography has evolved from a niche topic into a respectable subfield of public-key cryptography, going through phases of excitement and of existential doubt. Today isogeny based cryptography is too vast to be taught in a single week of lectures, hence these notes do not attempt at covering the entirety of known protocols and attacks. Instead, they are meant to give the bases to enter the field and, hopefully, start doing exciting research.

Stable version of these notes permanently hosted at https://arxiv.org/abs/1711.04062.
LaTeX source code available at https://github.com/defeo/MathematicsOfIBC/.

Acknowledgments. These notes wouldn't have existed if not for the summer schools mentioned above. For having organized such wonderful events and supported our lectures, we would like to thank CIMPA, the Écoles Mathématiques Africaines, the École Polytechnique de Thiès, and their personnel. Jörn Steuding, Katja Mönius, Pascal Stumpf, Steffen Reith, Michael Meyer, the RheinMain University of Applied Sciences and the University of Würzburg. Michael Nüsken, Sophia Grundner-Culemann, Marcel Tiepelt, Daniel Loebenberger, Jonathan Lennartz, the b-it (Bonn-Aachen International Center for Information Technology), CASA (Cyber Security in the Age of Large-Scale Adversaries), the Fachgruppe KRYPTO and the smashHit project. Marusia Rebolledo, Valerio Talamanca, Carlos Trujillo Solarte, Jhon Jairo Bravo Grijalba, Cristian Angulo and the Universidad del Cauca. Souidi El Mamoun, Damien Stehlé and the University Mohammed V of Rabbat.

Many students have contributed by pointing out mistakes and helping fixing them. We would like to thank, in particular, Simon Masson, Marcel Müller, Martin Strand, Vadym Fedyukovych and Tomáš Novotny, Sina Schaeffler, Valérien Hatey, Mehdi Kermaoui, and apologize to all those students whose name we've forgot.

Contents

Part I
Elliptic curves and isogenies

In this part, we review the basic and not-so-basic theory of elliptic curves. Our goal is to summarize the fundamental theorems necessary to understanding the foundations of isogeny based cryptography. A proper treatment of the material covered here would require more than one book, we thus skip proofs and lots of details to go straight to the useful theorems. The reader in search of a more comprehensive treatment will find more details [76, 77, 52, 62].

Throughout this part we let k be a field, and we denote by $\bar{k}$ its algebraic closure.

1 Elliptic curves

Elliptic curves are smooth projective curves of genus 1 with a distinguished point. Projective space initially appeared through the process of adding *points at infinity*, as a method to understand the geometry of projections (also known as *perspective* in classical painting). In modern terms, we define projective space as the collection of all lines in affine space passing through the origin.

Definition 1 (Projective space)**.** The *projective space of dimension n*, denoted by $\mathbb{P}^n$ or $\mathbb{P}^n(\bar{k})$, is the set of all $(n+1)$-tuples

$$(x_0, \dots, x_n) \in \bar{k}^{n+1}$$

such that $(x_0, \dots, x_n) \neq (0, \dots, 0)$, taken modulo the equivalence relation

$$(x_0, \dots, x_n) \sim (y_0, \dots, y_n)$$

if and only if there exists $\lambda \in \bar{k}$ such that $x_i = \lambda y_i$ for all i.

The equivalence class of $(x_0, \dots, x_n)$ is customarily denoted by $(x_0 : \dots : x_n)$ and called a *projective point*. The set of the *k-rational points*, denoted by $\mathbb{P}^n(k)$, is defined as

$$\mathbb{P}^n(k) = \{(x_0 : \dots : x_n) \in \mathbb{P}^n \mid x_i \in k \text{ for all } i\}.$$

By fixing arbitrarily the coordinate $x_n = 0$, we define a projective space of dimension $n-1$, which we call the *hyperplane at infinity*; its points are called *points at infinity*.

From now on we suppose that the field k has characteristic different from 2 and 3. This has the merit of greatly simplifying the representation of an elliptic curve. For a general definition, see [76, Chap. III].

Definition 2 (Weierstrass equation)**.** An *elliptic curve* defined over k is the locus in $\mathbb{P}^2(\bar{k})$ of an equation

$$Y^2Z = X^3 + aXZ^2 + bZ^3, \tag{1}$$

with $a, b \in k$ and $4a^3 + 27b^2 \neq 0$.

The point $(0 : 1 : 0)$ is the only point on the line $Z = 0$; it is called the *point at infinity* of the curve.

It is customary to write Eq. (1) in *affine form*. By defining the coordinate functions $x = X/Z$ and $y = Y/Z$, we equivalently define the elliptic curve as the locus of the equation

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

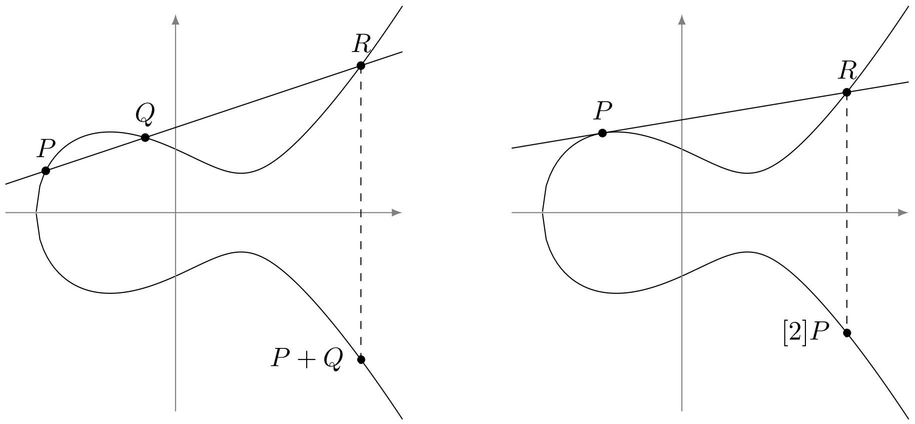


Figure 1: An elliptic curve defined over $\mathbb{R}$, and the geometric representation of its group law.

plus the point at infinity $\mathcal{O} = (0 : 1 : 0)$.

In characteristic different from 2 and 3, we can show that any smooth projective curve of genus 1 with a distinguished point $\mathcal{O}$ is isomorphic to a Weierstrass equation by sending $\mathcal{O}$ onto the point at infinity $(0 : 1 : 0)$.

Now, since any elliptic curve is defined by a cubic equation, Bézout's theorem tells us that any line in $\mathbb{P}^2$ intersects the curve in exactly three points, taken with multiplicity. We define a group law by requiring that three co-linear points sum to zero.

Definition 3. Let $E : y^2 = x^3 + ax + b$ be an elliptic curve. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be two points on E different from the point at infinity, then we define a composition law $\oplus$ on E as follows:

- $P \oplus \mathcal{O} = \mathcal{O} \oplus P = P$ for any point $P \in E$;
- If $x_1 = x_2$ and $y_1 = -y_2$, then $P_1 \oplus P_2 = \mathcal{O}$;
- Otherwise set
$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } P \neq Q, \\ \frac{3x_1^2 + a}{2y_1} & \text{if } P = Q, \end{cases}$$
then the point $(P_1 \oplus P_2) = (x_3, y_3)$ is defined by
$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2, \\ y_3 &= -\lambda x_3 - y_1 + \lambda x_1. \end{aligned}$$

It can be shown that the above law defines an Abelian group, thus we will simply write + for $\oplus$. The n-th scalar multiple of a point P will be denoted by $[n]P$. When E is defined over k, the subgroup of its *rational points over k* is customarily denoted $E(k)$. Figure 1 shows a graphical depiction of the group law on an elliptic curve defined over $\mathbb{R}$.

We now turn to the group structure of elliptic curves. The torsion part is easily characterized.

Proposition 4. *Let E be an elliptic curve defined over an algebraically closed field k, and let $m \neq 0$ be an integer. The m-torsion group of E, denoted by $E[m]$, has the following structure:*

- *$E[m] \simeq (\mathbb{Z}/m\mathbb{Z})^2$ if the characteristic of k does not divide m;*

- *If $p > 0$ is the characteristic of k, then*

$$E[p^i] \simeq \begin{cases} \mathbb{Z}/p^i\mathbb{Z} & \text{for any } i \geq 0, \text{ or} \\ \{\mathcal{O}\} & \text{for any } i \geq 0. \end{cases}$$

Proof. See [76, Coro. 6.4]. For the characteristic 0 case see also Section 3. □

When k is not algebraically closed, we write $E[m]$ for the m-torsion subgroup of $E(\bar{k})$, i.e. the torsion points in the algebraic closure. $E[m]$ may or may not be fully contained in $E(k)$, it is easy to see, however, that it will always be contained in a finite extension of k of degree less than m^2.

For curves defined over a field of positive characteristic p, the case $E[p] \simeq \mathbb{Z}/p\mathbb{Z}$ is called *ordinary*, while the case $E[p] \simeq \{\mathcal{O}\}$ is called *supersingular*. We shall see alternative characterizations of supersingularity in Sections 4 and 7.

The free part of the group is much harder to characterize. We have some partial results for elliptic curves over number fields.

Theorem 5 (Mordell-Weil)**.** *Let k be a number field, the group $E(k)$ is finitely generated.*

However the exact determination of the rank of $E(k)$ is somewhat elusive: we have algorithms to compute the rank of most elliptic curves over number fields; however, an exact formula for such rank is the object of the *Birch and Swinnerton-Dyer conjecture*, one of the *Clay Millenium Prize Problems*.

2 Maps between elliptic curves

We now focus on maps between elliptic curves. We are mostly interested in maps that preserve both facets of elliptic curves: as projective varieties, and as groups.

We first look into invertible algebraic maps, that is linear changes of coordinates that preserve the Weierstrass form of the equation. Because linear maps preserve lines, it is immediate that they also preserve the group law. It is easily verified that the only such maps take the form

$$(x, y) \mapsto (u^2x', u^3y')$$

for some $u \in \bar{k}$, thus defining an *isomorphism* between the curve $y^2 = x^3 + au^4x + bu^6$ and the curve $(y')^2 = (x')^3 + ax' + b$. Isomorphism classes are traditionally encoded by an invariant, whose origins can be traced back to complex analysis.

Proposition 6 (j-invariant)**.** *Let $E : y^2 = x^3 + ax + b$ be an elliptic curve, and define the* j-invariant *of E as*

$$j(E) = 1728\frac{4a^3}{4a^3 + 27b^2}.$$

Two curves are isomorphic over the algebraic closure $\bar{k}$ if and only if they have the same j-invariant.

Note that if two curves defined over k are isomorphic over $\bar{k}$, they are so over an extension of k of degree at most 6. An isomorphism between two elliptic curves defined over k, that is itself not defined over k is called a *twist*. Any curve defined over a non-quadratically-closed field[1] has

[1] A field is quadratically closed if every element has square root.

quadratic twists obtained by taking $u \notin k$ such that $u^2 \in k$. The two curves of j-invariant 0 and 1728 also have *cubic*, *sextic* and *quartic twists*.

More general algebraic maps, i.e. non-linear (and thus not necessarily invertible) changes of coordinates, between elliptic curves are called *isogenies*.

Definition 7. Let E, E' be two elliptic curves. An isogeny $\phi : E \to E'$ is a non-constant algebraic map of projective varieties sending the point at infinity of E onto the point at infinity of E'.

Somewhat surprisingly, being algebraic and preserving the point at infinity is sufficient to make them group morphisms.

Theorem 8. *Let E, E' be elliptic curves defined over a field k and let $\phi : E \to E'$ be an isogeny between them. Then:*

- *ϕ is a group morphism;*
- *ϕ has finite kernel;*
- *If k is algebraically closed, ϕ is surjective.*

Proof. See [76, III, Th. 4.8]. □

Two curves are called *isogenous* if there exists an isogeny between them. We shall see later that this is an equivalence relation.

Isogenies from a curve to itself are called *endomorphisms*. The prototypical endomorphism is the multiplication-by-m endomorphism defined by

$$[m] \;:\; P \mapsto [m]P.$$

Its kernel is, by definition, the m-th torsion subgroup $E[m]$.

Since they are algebraic group morphisms, we can define addition of isogenies by $(\phi+\psi)(P) = \phi(P)+\psi(P)$, and the resulting map is still an isogeny. Adding to the set of isogenies $E \to E'$ the constant map that sends every point of E to the point at infinity of E', we thus obtain a group, denoted by $\mathrm{Hom}(E, E')$. Additionally, endomorphisms $E \to E$ support composition, distributing over addition, hence the set of all endomorphisms forms a ring, denoted by $\mathrm{End}(E)$.[2]

Since each $m \in \mathbb{Z}$ defines a different multiplication-by-m endomorphism, clearly $\mathbb{Z} \hookrightarrow \mathrm{End}(E)$. But can $\mathrm{End}(E)$ be larger than $\mathbb{Z}$? The reader will have to wait until Section 7 to know the answer to this riddle.

3 Elliptic curves over $\mathbb{C}$

To better understand elliptic curves and their morphisms, we take a moment now to specialize them to the complex numbers.

Definition 9 (Complex lattice)**.** A *complex lattice* Λ is a discrete subgroup of $\mathbb{C}$ that contains an $\mathbb{R}$-basis of $\mathbb{C}$.

Explicitly, a complex lattice is generated by a *basis* (ω_1, ω_2), such that $\omega_1 \neq \lambda\omega_2$ for all $\lambda \in \mathbb{R}$, as

$$\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}.$$

Up to exchanging ω_1 and ω_2, we can assume that $\mathrm{Im}(\omega_1/\omega_2) > 0$; we then say that the basis has *positive orientation*. A positively oriented basis is obviously not unique, though.

[2] In short, isogenies are the morphisms in the Abelian category of elliptic curves.

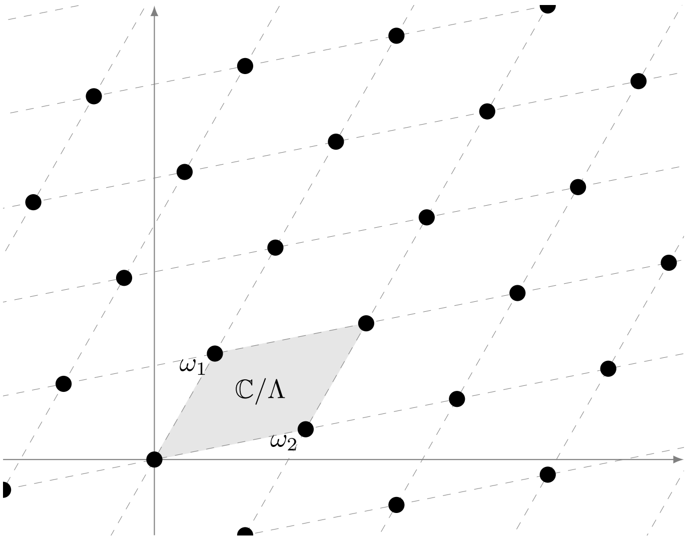


Figure 2: A complex lattice (black dots) and its associated complex torus (grayed *fundamental domain*).

Proposition 10. *Let Λ be a complex lattice, and let (ω_1, ω_2) be a positively oriented basis, then any other positively oriented basis (ω_1', ω_2') is of the form*

$$\begin{aligned} \omega_1' &= a\omega_1 + b\omega_2, \\ \omega_2' &= c\omega_1 + d\omega_2, \end{aligned}$$

for some matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$.

Proof. See [77, I, Lem. 2.4]. □

Definition 11 (Complex torus)**.** Let Λ be a complex lattice, the quotient $\mathbb{C}/\Lambda$ is called a *complex torus.*

A convex set of class representatives of $\mathbb{C}/\Lambda$ is called a *fundamental parallelogram.* Figure 2 shows a complex lattice generated by a (positively oriented) basis (ω_1, ω_2), together with a fundamental parallelogram for $\mathbb{C}/(\omega_1, \omega_2)$. The additive group structure of $\mathbb{C}$ carries over to $\mathbb{C}/\Lambda$, and can be graphically represented as operations on points inside a fundamental parallelogram. This is illustrated in Figure 3.

Definition 12 (Homothetic lattices)**.** Two complex lattices Λ and Λ' are said to be *homothetic* if there is a complex number $\alpha \in \mathbb{C}^\times$ such that $\Lambda = \alpha\Lambda'$.

Geometrically, applying a homothety to a lattice corresponds to zooms and rotations around the origin. We are only interested in complex tori up to homothety; to classify them, we introduce the *Eisenstein series of weight* $2k$, defined as

$$G_{2k}(\Lambda) = \sum_{\omega \in \Lambda \setminus \{0\}} \omega^{-2k}.$$

It is customary to set

$$g_2(\Lambda) = 60G_4(\Lambda), \quad g_3(\Lambda) = 140G_6(\Lambda);$$

when Λ is clear from the context, we simply write g_2 and g_3.

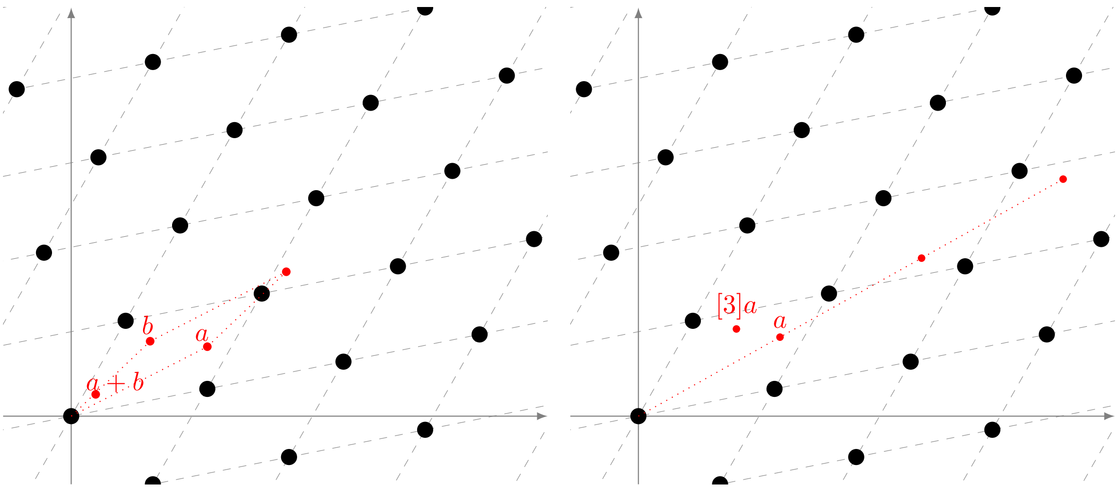


Figure 3: Addition (left) and scalar multiplication (right) of points in a complex torus $\mathbb{C}/\Lambda$.

Theorem 13 (Modular j-invariant)**.** *The* modular j-invariant *is the function on complex lattices defined by*

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

Two lattices are homothetic if and only if they have the same modular j-invariant.

Proof. See [77, I, Th. 4.1]. □

It is no chance that the invariants classifying elliptic curves and complex tori look very similar. Indeed, we can prove that the two are in one-to-one correspondence.

Definition 14 (Weierstrass $\wp$ function)**.** Let Λ be a complex lattice, the *Weierstrass $\wp$ function* associated to Λ is the series

$$\wp(z;\Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

Theorem 15. *The Weierstrass function $\wp(z;\Lambda)$ has the following properties:*

1. *It is an* elliptic function *for Λ, i.e. $\wp(z) = \wp(z+\omega)$ for all $z \in \mathbb{C}$ and $\omega \in \Lambda$.*

2. *Its Laurent series around $z = 0$ is*

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1) G_{2k+2} z^{2k}.$$

3. *It satisfies the differential equation*

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

for all $z \notin \Lambda$.

4. The curve

$$E \;:\; y^2 = 4x^3 - g_2x - g_3$$

is an elliptic curve over $\mathbb{C}$. The map

$$\begin{aligned}\mathbb{C}/\Lambda &\to E(\mathbb{C}),\\ 0 &\mapsto (0:1:0),\\ z &\mapsto (\wp(z) : \wp'(z) : 1)\end{aligned}$$

is an isomorphism of Riemann surfaces and a group morphism.

Proof. See [76, VI, Th. 3.1, Th. 3.5, Prop. 3.6]. □

By comparing the two definitions for the j-invariants, we see that $j(\Lambda) = j(E)$. So, for any homothety class of complex tori, we have a corresponding isomorphism class of elliptic curves. The converse is also true.

Theorem 16 (Uniformization theorem)**.** *Let $a, b \in \mathbb{C}$ be such that $4a^3 + 27b^2 \neq 0$, then there is a unique complex lattice Λ such that $g_2(\Lambda) = -4a$ and $g_3(\Lambda) = -4b$.*

Proof. See [77, I, Coro. 4.3]. □

Using the correspondence between elliptic curves and complex tori, we now have a new perspective on their group structure. Looking at complex tori, it becomes immediately evident why the torsion part has rank 2, i.e. why $E[m] \simeq (\mathbb{Z}/m\mathbb{Z})^2$. This is illustrated in Figure 4a; in the picture we see two lattices Λ and Λ', generated respectively by the black and the red dots. We already defined the multiplication-by-m map of Λ as $[m] : z \mapsto mz \bmod \Lambda$. This map is the same as reducing

$$\begin{aligned}\mathbb{C}/\Lambda &\to \mathbb{C}/\Lambda',\\ z &\mapsto z \bmod \Lambda'\end{aligned}$$

first, and then composing with the homothety $\Lambda = m\Lambda'$.

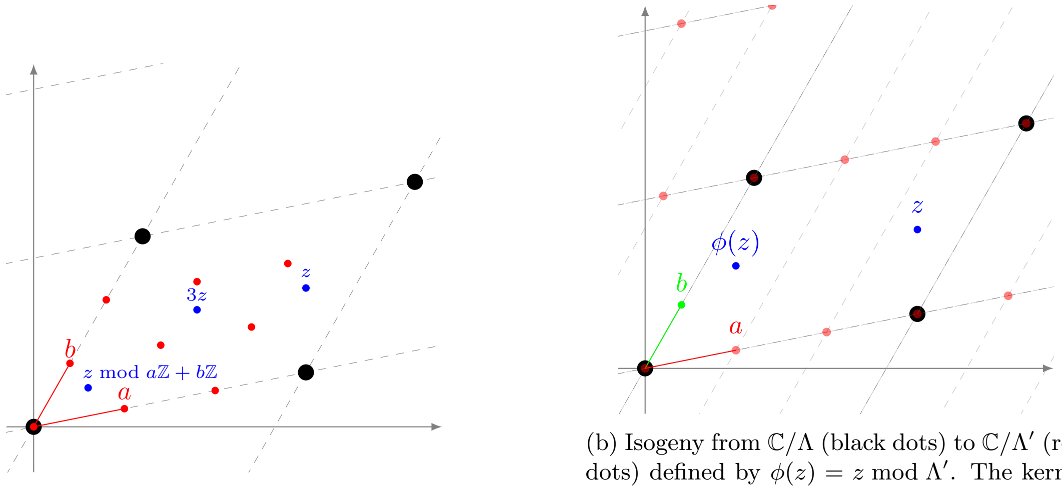
Within this new perspective, isogenies are a mild generalization of scalar multiplications. Whenever two lattices Λ, Λ' verify $\alpha\Lambda \subset \Lambda'$, there is a well defined map

$$\begin{aligned}\phi_\alpha : \mathbb{C}/\Lambda &\to \mathbb{C}/\Lambda',\\ z &\mapsto \alpha z \bmod \Lambda'\end{aligned}$$

that is holomorphic and also a group morphism. One example of such maps is given in Figure 4b: there, $\alpha = 1$ and the red lattice strictly contains the black one; the map is simply defined as reduction modulo Λ'. It turns out that these maps are exactly the isogenies of the corresponding elliptic curves.

Theorem 17. *Let E, E' be elliptic curves over $\mathbb{C}$, with corresponding lattices Λ, Λ'. There is a bijection between the set of isogenies from E to E' and the set of maps ϕ_α for all α such that $\alpha\Lambda \subset \Lambda'$.*

Proof. See [76, VI, Th. 4.1]. □



(a) 3-torsion group on a complex torus (red points), with two generators a and b, and action of the multiplication-by-3 map (blue dots).

(b) Isogeny from $\mathbb{C}/\Lambda$ (black dots) to $\mathbb{C}/\Lambda'$ (red dots) defined by $\phi(z) = z \bmod \Lambda'$. The kernel of ϕ is contained in $(\mathbb{C}/\Lambda)[3]$ and is generated by a. The kernel of the dual isogeny $\hat{\phi}$ is generated by the vector b in Λ'.

Figure 4: Maps between complex tori.

Looking again at Figure 4b, we see that there is a second isogeny $\hat{\phi}$ from Λ' to $\Lambda/3$, whose kernel is generated by $b \in \Lambda'$. The composition $\hat{\phi} \circ \phi$ is an endomorphism of $\mathbb{C}/\Lambda$, up to the homothety sending $\Lambda/3$ to Λ, and we verify that it corresponds to the multiplication-by-3 map. In this example, the kernels of both ϕ and $\hat{\phi}$ contain 3 elements, and we say that ϕ and $\hat{\phi}$ have *degree* 3. Although not immediately evident from the picture, this same construction can be applied to any isogeny. The isogeny $\hat{\phi}$ is called the *dual* of ϕ. Dual isogenies exist not only in characteristic 0, but also for any base field, as we shall see in Section 5.

Under which conditions does an isogeny become an endomorphism? By virtue of the last theorem, there is a one-to-one correspondence between the endomorphisms $E \to E$ and the complex numbers α such that $\alpha\Lambda \subset \Lambda$. In general, the only possible choices are given by α an integer, corresponding to scalar multiplications. For some lattices, however, something “special” happens; we shall study this case in Sections 7 and 11.

4 Elliptic curves over finite fields

In this section we shift our attention to elliptic curves defined over a finite field, which are the main objects manipulated in cryptography. From now on we will use q to denote a power of a prime p, and $\mathbb{F}_q$ do denote a finite field with q elements.

Obviously, the group of rational points of a curve defined over a finite field is finite. Because every element of $\bar{\mathbb{F}}_q$ is defined over a finite extension of $\mathbb{F}_q$, the algebraic group $E(\bar{\mathbb{F}}_q)$ only contains torsion elements, and we have already characterized precisely the structure of the torsion part of E.

For curves over finite fields, the Frobenius endomorphism plays a very special role, and governs much of their structure.

Definition 18 (Frobenius endomorphism)**.** Let E be an elliptic curve defined over a field with

q elements, its *Frobenius endomorphism*, denoted by π, is the map that sends

$$(X : Y : Z) \mapsto (X^q : Y^q : Z^q).$$

Proposition 19. *Let π be the Frobenius endomorphism of E. Then:*

- $\ker \pi = \{\mathcal{O}\}$*;*
- $\ker(\pi - 1) = E(k)$*.*

Theorem 20 (Hasse)**.** *Let E be an elliptic curve defined over a finite field with q elements. Its Frobenius endomorphism π satisfies a quadratic equation*

$$\pi^2 - t\pi + q = 0, \tag{2}$$

for some $|t| \leq 2\sqrt{q}$.

Proof. See [76, V, Th. 2.3.1]. □

The coefficient t in the equation is called the *trace* of π. It gives an alternative characterization of supersingularity.

Proposition 21. *An elliptic curve E defined over a finite field of characteristic p is supersingular if and only if p divides the trace of its Frobenius endomorphism.*

By replacing $\pi = 1$ in eq. (2), we immediately obtain the cardinality of E as $\#E(k) = \#\ker(\pi - 1) = q + 1 - t$.

Corollary 22. *Let E be an elliptic curve defined over a finite field k with q elements, then*

$$|\#E(k) - q - 1| \leq 2\sqrt{q}.$$

It turns out that the cardinality of E over its *base field* k determines its cardinality over any finite extension of it. This is a special case of Weil's famous conjectures, proven by Weil himself in 1949 for Abelian varieties, and more generally by Deligne in 1973.

Definition 23. Let V be a projective variety defined over a finite field $\mathbb{F}_q$, its *zeta function* is the power series

$$Z(V/\mathbb{F}_q; T) = \exp\left(\sum_{n=1}^{\infty} \#V(\mathbb{F}_{q^n}) \frac{T^n}{n}\right).$$

Theorem 24. *Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$, and let $\#E(\mathbb{F}_q) = q+1-a$. Then*

$$Z(E/\mathbb{F}_q; T) = \frac{1 - aT + qT^2}{(1-T)(1-qT)}.$$

Proof. See [76, V, Th. 2.4]. □

5 Isogenies

We now look more in detail at isogenies of elliptic curves. We start with some basic definitions.

Definition 25 (Degree, separability)**.** Let $\phi : E \to E'$ be an isogeny defined over a field k, and let $k(E), k(E')$ be the function fields of E, E'. By composing ϕ with the functions of $k(E')$, we obtain a subfield of $k(E)$ that we denote by $\phi^*(k(E'))$.

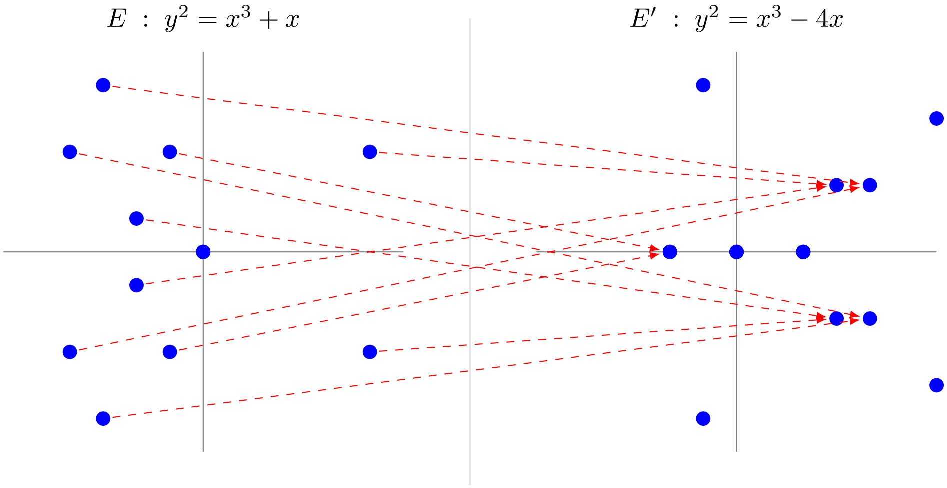


Figure 5: The isogeny $(x, y) \mapsto \big((x^2+1)/x,\ y(x^2-1)/x^2\big)$, as a map between curves defined over $\mathbb{F}_{11}$.

1. The *degree* of ϕ is defined as $\deg\phi = [k(E) : \phi^*(k(E'))]$; it is always finite.
2. ϕ is said to be *separable*, *inseparable*, or *purely inseparable* if the extension of function fields is.
3. If ϕ is separable, then $\deg\phi = \#\ker\phi$.
4. If ϕ is purely inseparable, then $\deg\phi$ is a power of the characteristic of k.
5. Any isogeny can be decomposed as a product of a separable and a purely inseparable isogeny.

Proof. See [76, II, Th. 2.4]. □

In practice, most of the time we will be considering separable isogenies, and we can take $\deg\phi := \#\ker\phi$ as the definition of the degree. Notice that in this case $\deg\phi$ is the size of any fiber of ϕ (over the algebraic closure). When the kernel of a separable isogeny is cyclic, we will call it a *cyclic* isogeny.

Example 26. The map ϕ from the elliptic curve $y^2 = x^3 + x$ to $y^2 = x^3 - 4x$ defined by

$$\begin{aligned} \phi(x, y) &= \left(\frac{x^2+1}{x}, y\frac{x^2-1}{x^2}\right), \\ \phi(0,0) &= \phi(\mathcal{O}) = \mathcal{O} \end{aligned} \tag{3}$$

is a separable isogeny between curves defined over $\mathbb{Q}$. It has degree 2, and its kernel is generated by the point $(0, 0)$.

Plotting the isogeny (3) over $\mathbb{R}$ would be cumbersome, however, since the curves are defined by integer coefficients, we may reduce the equations modulo a prime p, then the isogeny descends to an isogeny of curves over $\mathbb{F}_p$. Figure 5 plots the action of the isogeny after reduction modulo 11. A red arrow indicates that a point of the left curve is sent onto a point on the right curve; the action on the point in $(0, 0)$, going to the point at infinity, is not shown. We observe a symmetry with respect to the x-axis, a consequence of the fact that ϕ is a group morphism; and, by looking closer, we may also notice that collinear points are sent to collinear points, also a necessity for a group morphism.

It is evident that the isogeny is 2-to-1, however, over $\mathbb{F}_p$, we are unable to see all fibers, because the isogeny is only surjective over the algebraic closure. This is not dissimilar from the way power-by-n maps act on the multiplicative group $k^\times$ of a field k: the map $x \mapsto x^2$, for example, is a 2-to-1 (algebraic) group morphism on $\mathbb{F}_{11}^\times$, and those elements that have no preimage, the non-squares, will have exactly two square roots in $\mathbb{F}_{11^2}$, and so on.

The defining property of separable isogenies is that they are entirely determined by their kernel.

Proposition 27. *Let E be an elliptic curve defined over an algebraically closed field, and let G be a finite subgroup of E. There is a curve E', and a separable isogeny ϕ, such that* $\ker\phi = G$ *and $\phi : E \to E'$. Furthermore, E' and ϕ are unique up to composition with an isomorphism $E' \simeq E''$.*

Proof. See [76, Prop. III.4.12] □

Said otherwise, for any finite subgroup $G \subset E$, we have an exact sequence of algebraic groups

$$0 \longrightarrow G \longrightarrow E \xrightarrow{\phi} E' \longrightarrow 0.$$

Uniqueness up to isomorphisms justifies the notation E/G for the isomorphism class of the image curve E'. Conversely, since any non-constant morphism of elliptic curves necessarily has finite kernel, we have a bijection between the finite subgroups of a curve E and the isogenies with domain E up to isomorphisms. This correspondence is rich in consequences: it is an easy exercise to prove the following useful facts.

Corollary 28.

1. *Let H and G be finite subgroups $H \subset G \subset E$, and $\phi : E \to E/G$. Then ϕ factors as $\psi \circ \chi$, with $\chi : E \to E/H$ and $\psi : E/H \to (E/H)/\chi(G)$, up to post-composition by an isomorphism.*
2. *Any isogeny of elliptic curves can be decomposed as a product of prime degree isogenies.*
3. *Let E be defined over an algebraically closed field k, let ℓ be a prime different from the characteristic of k, then there are exactly $\ell + 1$ isogenies of degree ℓ having E for domain, up to post-composition with an isomorphism.*

Slightly more work is required to prove the following, fundamental, theorem (the difficulty comes essentially from the inseparable part, see [76, III.6.1] for a detailed proof).

Theorem 29 (Dual isogeny theorem)**.** *Let $\phi : E \to E'$ be an isogeny of degree m. There is a unique isogeny $\hat{\phi} : E' \to E$ such that*

$$\hat{\phi} \circ \phi = [m]_E, \quad \phi \circ \hat{\phi} = [m]_{E'}.$$

$\hat{\phi}$ is called the dual isogeny of *ϕ; it has the following properties:*

1. *$\hat{\phi}$ has degree m;*
2. *$\hat{\phi}$ is defined over k if and only if ϕ is;*

3. $\widehat{\psi \circ \phi} = \hat{\phi} \circ \hat{\psi}$ *for any isogeny* $\psi : E' \to E''$*;*

4. $\widehat{\psi + \phi} = \hat{\psi} + \hat{\phi}$ *for any isogeny* $\psi : E \to E'$*;*

5. $\deg \phi = \deg \hat{\phi}$*;*

6. $\hat{\hat{\phi}} = \phi$*.*

Computing isogenies. The computational counterpart to the kernel-isogeny correspondence is given by Vélu's celebrated formulas.

Proposition 30 (Vélu [85])**.** *Let* $E : y^2 = x^3 + ax + b$ *be an elliptic curve defined over a field* k*, and let* $G \subset E(\bar{k})$ *be a finite subgroup. A rational expression for the separable isogeny* $\phi : E \to E/G$ *of kernel* G *is given by*

$$\phi(P) = \left(x(P) + \sum_{Q \in G \setminus \{\mathcal{O}\}} x(P+Q) - x(Q), \quad y(P) + \sum_{Q \in G \setminus \{\mathcal{O}\}} y(P+Q) - y(Q) \right)$$

for any point $P \notin G$*, taking the curve of equation* $y^2 = x^3 + a'x + b'$ *with*

$$\begin{aligned} a' &= a - 5 \sum_{Q \in G \setminus \{\mathcal{O}\}} (3x(Q)^2 + a), \\ b' &= b - 7 \sum_{Q \in G \setminus \{\mathcal{O}\}} (5x(Q)^3 + 3ax(Q) + 2b), \end{aligned}$$

as a representative for E/G*.*

Using Vélu's formulas, or one of their variants [60, 17, 70], we can represent isogenies and evaluate them at arbitrary points using a number of field operations polynomial in their degree. In some favorable cases, an isogeny of degree d can even be represented in constant space and be evaluated at arbitrary points using only $\sqrt{d}\,\mathrm{polylog}(d)$ operations [3].

We extend this representation to chains of isogenies: we represent each isogeny in the chain by its kernel, and evaluate it using Vélu's formulas. Thanks to Corollary 28, any isogeny of composite degree N can thus be evaluated in time polynomial in $\log(N)$ and the largest prime factor of N.

We would like to abstract the way an isogeny is actually stored and evaluated and only focus on the cost of its evaluation. This motivates the following definition, where we restrict to isogenies over finite fields to keep things concrete.

Definition 31 (Isogeny representation)**.** Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$. An *(efficient) isogeny representation* of an isogeny $\phi : E \to E'$ is a deterministic algorithm which on input an arbitrary point $P \in E(\mathbb{F}_{q^k})$ outputs $\phi(P)$ using $\mathrm{poly}(k \log(q))$ operations.

There is a little ambiguity on what is meant by "algorithm" in the definition. Any model of computation will be acceptable, as long as it is polynomial-time equivalent to another. In this text we will informally describe algorithms, sometimes using pseudo-code, without focusing too much on a detailed complexity analysis.

Remark 32. An isogeny representation of $\phi : E \to E'$ is enough to compute an equation for the image curve E'. It is indeed sufficient to evaluate ϕ at all points of order 2 to get the roots of $f(x)$ in the Weierstrass equation $y^2 = f(x)$ of E'.

6 The Weil pairing

The definition below is given for free modules over a ring. If the reader feels uncomfortable with rings and modules, they may think of vector spaces over a field instead.

Definition 33. Let M_1, M_2 be free modules over a commutative ring R. A bilinear form is a mapping $e : M_1 \times M_2 \to R$ such that:

- $e(aP, Q) = e(P, aQ) = a \cdot e(P, Q)$,
- $e(P + P', Q) = e(P, Q) + e(P', Q)$,
- $e(P, Q + Q') = e(P, Q) + e(P, Q')$,

for all $a \in R$, all $P, P' \in M_1$ and all $Q, Q' \in M_2$.

A bilinear form is said to be *non-degenerate* if:

- $e(P, Q) = 0$ for all P implies $Q = 0$, and
- $e(P, Q) = 0$ for all Q implies $Q = 0$.

A bilinear form is said to be *alternating* if $M_1 = M_2$ and $e(P, P) = 0$ for all P.

If instead of taking values in R, we define a map $M_1 \times M_2 \to M_3$, with the same properties as above, but taking values in an R-module M_3, we talk of a bilinear map, or *pairing.*

Proposition 34. *Let E/k be an elliptic curve defined over a field k, and let m be a positive integer prime to the characteristic of k. Write $\mu_m \subset \bar{k}$ for the subgroup of m-th roots of unity of the algebraic closure of k.*

There exist a non-degenerate alternating pairing of $\mathbb{Z}/m\mathbb{Z}$-modules

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

called the Weil pairing.

The exact definition of the Weil pairing requires more geometric tools than we are willing to introduce here (see, e.g., [76, 33] for details). For the sake of these notes, it suffices to recall that the torsion subgroup $E[m]$ is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^2$, i.e. is a free module of rank two. On the other hand, the image group μ_m only has rank one, thus the Weil pairing is just a bilinear form in disguise. . . and not just any bilinear form! Indeed, under the constraint of being non-degenerate and alternating, the Weil pairing is, essentially, the 2×2 determinant form, as the following proposition shows.

Proposition 35. *Let M be a $\mathbb{Z}/m\mathbb{Z}$ module of rank 2, and let (P, Q) be a pair of generators. Let e be an alternating pairing on $M \times M$ taking values in a multiplicative group G of order m, and let $\zeta = e(P, Q)$. Then*

$$e([a]P + [b]Q, [c]P + [d]Q) = \zeta^{\det\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)}.$$

In particular e is non-degenerate if and only if ζ generates G.

It is remarkable that the Weil pairings of isogenous curves are "compatible" in a precise sense. Indeed, it turns out that the dual isogeny is the "transpose" in the sense of bilinear forms.

Theorem 36. *Let E, E' be elliptic curves, let $\phi : E \to E'$ be an isogeny, $\hat{\phi} : E' \to E$ its dual, let m be a positive integer. For any $P \in E[m]$ and $Q \in E'[m]$*

$$e'_m\bigl(\phi(P), Q\bigr) = e_m\bigl(P, \hat{\phi}(Q)\bigr). \tag{4}$$

where e_m and e'_m denote the Weil pairing of E and E' respectively.

Proof. See [76, III.8.2]. □

Corollary 37. *Let $\phi : E \to E'$ be an isogeny of degree d. For any m, P, Q*

$$e'_m\bigl(\phi(P), \phi(Q)\bigr) = e_m(P, Q)^d.$$

There exist algorithms to compute the Weil pairing taking a number of operations over the field of definition of $E[m]$ polynomial (and even quasi-linear) in $\log(m)$. There exist other pairings defined for elliptic curves over finite fields, which are sometimes faster to compute than the Weil pairing. However they are all related, and will not make a difference for our purposes, thus we will ignore them. For a review of known elliptic pairings, addressed to non-specialists, see [36].

7 The endomorphism ring

We come back to the question of determining the structure of $\mathrm{End}(E)$. To put the right words on it, we need to recall some background from algebraic number theory; for an in-depth treatment, see [53, 86].

A quadratic number field is a quadratic extension K of the rationals; it is called *real* if there exists an embedding $K \subset \mathbb{R}$, *imaginary* otherwise. All such fields can be expressed as $\mathbb{Q}(\sqrt{d})$ for some integer d, the *Gaussian integers* $\mathbb{Q}(i)$ being a typical example of an imaginary one.

Definition 38 (Discriminant)**.** Let d be a square free integer, the *discriminant* of the quadratic number field $\mathbb{Q}(\sqrt{d})$ is d if $d = 1 \bmod 4$, and $4d$ otherwise.

An integer Δ that is the discriminant of a quadratic number field is called a *fundamental discriminant.*

Definition 39. Let $\alpha = a + b\sqrt{d}$ be an element of a quadratic number field.

- Its *conjugate* is $\bar{\alpha} = a - b\sqrt{d}$;
- Its *norm* is $N(\alpha) = \alpha\bar{\alpha} = a^2 - db^2$;
- Its *trace* is $\mathrm{Tr}(\alpha) = \alpha + \bar{\alpha} = 2a$.

Proposition 40. *Let α be an element of a quadratic imaginary field, then it is a root of the quadratic polynomial with rational coefficients*

$$x^2 - \mathrm{Tr}(\alpha)x + N(\alpha).$$

The elements with integer trace and norm can be seen as a generalization of the ring $\mathbb{Z}$ of integers inside $\mathbb{Q}$.

Definition 41 (Ring of integers)**.** Let K be a quadratic number field, an *algebraic integer* of K is an element $\alpha \in K$ that is a root of an irreducible monic polynomial with integer coefficients. The algebraic integers of K form a ring, called the *ring of integers* of K.

For example, $\mathbb{Z}[i]$ is the ring of integers of $\mathbb{Q}(i)$; more generally, if Δ is a fundamental discriminant, the ring of integers of $\mathbb{Q}(\sqrt{\Delta})$ is $\mathbb{Z}[\delta]$, where $\delta = (\Delta + \sqrt{\Delta})/2$.

Definition 42 (Fractional ideals, orders)**.** Let K be a quadratic number field. A *fractional ideal* $I \subset K$ is a $\mathbb{Z}$-lattice of rank 2. An *order* $\mathcal{O} \subset K$ is a fractional ideal that is also a ring.

Let $I \subset K$ be a fractional ideal, its order is the ring

$$\mathcal{O}_I = \{\alpha \in K \mid I\alpha \subset I\}.$$

When $I \subset \mathcal{O}_I$ we say that I is *integral.* when $I = \alpha\mathcal{O}_I$ for some $\alpha \in K$, we say that I is *principal.* If there exists another fractional ideal I^{-1} such that $II^{-1} = \mathcal{O}_I$ we say that I is *invertible.*

It is clear that I is an $\mathcal{O}_I$-module, and when it is integral we recover the usual definition of an ideal of $\mathcal{O}_I$. In this case, we will omit “fractional” and simply call I an *ideal* of $\mathcal{O}_I$. Clearly I is also an $\mathcal{O}$-module for any $\mathcal{O} \subset \mathcal{O}_I$, and we thus say it is a (fractional) $\mathcal{O}$-ideal.

We now generalize the concept of norm to an ideal. We need a technical definition first.

Definition 43 (gcd of rational numbers)**.** For two rational numbers $a = m/n, b = r/s$, written such that $\gcd(m, n) = 1 = \gcd(r, s)$, we define their greatest common divisor as $\gcd(a, b) := \gcd(m, r)/\operatorname{lcm}(n, s)$. By extension, we can also define the gcd of an arbitrary subset of $\mathbb{Q}$, as long as the least common multiple of the denominators of its elements is finite.

Proposition 44 (Ideal norm)**.** *Let I be a fractional ideal. Its* norm $N(I)$ *is the gcd of the norms of its elements. An ideal is integral if and only if its norm is an integer.*

By these definitions, the ring of integers $\mathcal{O}_K$ is an order of K: indeed it has $(1, \delta)$ as a *basis*, i.e., as a set of $\mathbb{Z}$-module generators. It is, in fact, the *maximal order* of K, i.e. it contains any other order of K. A more precise statement is the following.

Proposition 45. *Let K be a quadratic number field, let $\mathcal{O}_K$ be its ring of integers, and let $\mathcal{O} \subset \mathcal{O}_K$ be an arbitrary order. The index $f = [\mathcal{O}_K : \mathcal{O}]$ as abelian groups is called the* conductor *of $\mathcal{O}$. Then, $\mathcal{O}$ can be written as $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$.*

We generalize the notion of discriminant to any order.

Definition 46 (Discriminant)**.** Let $\mathcal{O}$ be an order with basis $(1, \delta)$. Its *discriminant* is $(\delta - \bar{\delta})^2$, where $\bar{\delta}$ denotes the complex conjugate of δ. It is independent of the choice of a basis.

Proposition 47. *Let $\mathcal{O}$ be an order, let Δ be its discriminant and let f be its conductor. Let Δ_K the discriminant of the maximal order, then $\Delta = f^2\Delta_K$. If $\mathcal{O}, \mathcal{O}'$ are two orders of discriminants Δ, Δ', then $\mathcal{O} \subset \mathcal{O}'$ if and only if $\Delta' | \Delta$.*

Because $\mathcal{O}_K$ is the “most obvious” order of K, (fractional) $\mathcal{O}_K$-ideals are often simply called (fractional) ideals of K.

Proposition 48. *Any fractional $\mathcal{O}_K$-ideal is invertible.*

Quaternion algebras are a 4-dimensional generalization of quadratic number fields: like in number fields, any element satisfies a quadratic equation; unlike them, they are not fields. The theory on quaternion algebras is very rich, and possesses deep connections with many objects in number theory, such as quadratic forms, modular forms, and elliptic curves [51, 86].

Definition 49 (Quaternion algebra)**.** A *quaternion algebra over* $\mathbb{Q}$ is an algebra of the form

$$K = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + k\mathbb{Q},$$

where the generators satisfy the relations

$$0 \neq i^2 \in \mathbb{Q}, \quad 0 \neq j^2 \in \mathbb{Q}, \quad k = ij = -ji.$$

If $i^2 = a$ and $j^2 = b$, we denote such an algebra by $\left(\frac{a,b}{\mathbb{Q}}\right)$.

An arbitrary element of a quaternion algebra can be written as $\alpha = t + xi + yj + zk$, where $t, x, y, z \in \mathbb{Q}$. The *real part* of such an element is $\mathrm{Re}(\alpha) = t$, the *imaginary part* is $\mathrm{Im}(\alpha) = xi + yj + zk$. The *conjugate* $\overline{\alpha}$ is obtained by flipping the sign of the imaginary part; $\overline{\alpha} = t - xi - yj - zk$. The (reduced) *norm* and *trace* are defined as

$$N(\alpha) := \alpha\overline{\alpha} = t^2 - ax^2 - by^2 + abz^2, \qquad \mathrm{Tr}(\alpha) := \alpha + \overline{\alpha} = 2t$$

respectively.[3] This motivates the following definition.

Definition 50. The *norm form* associated to the quaternion algebra $\left(\frac{a,b}{\mathbb{Q}}\right)$ is the polynomial $t^2 - ax^2 - by^2 + abz^2 \in \mathbb{Q}[t, x, y, z]$.

Let p be a prime number and let K be a quaternion algebra over $\mathbb{Q}$. We say that K is *split* at p if $K \otimes \mathbb{Q}_p \cong M_2(\mathbb{Q}_p)$. This is equivalent to the norm form having a non-trivial zero over $\mathbb{Q}_p$. Otherwise, we say that the quaternion algebra is *ramified* at p.

We say K is *ramified at* ∞ if the norm form has no non-trivial zero over $\mathbb{R}$. This is equivalent to a, b being both negative.

The *reduced discriminant* of a quaternion algebra is the product of the primes at which it ramifies. For every prime number p, there is, up to isomorphism, a unique quaternion algebra with discriminant p, which we denote $B_{p,\infty}$. It ramifies exactly at p and ∞.

Proposition 51. *Let p be a prime number, then we can choose the following representations for the quaternion algebra $B_{p,\infty}$.*

1. $B_{p,\infty} \cong \left(\frac{-1,-1}{\mathbb{Q}}\right)$ *if* $p = 2$*;*

2. $B_{p,\infty} \cong \left(\frac{-1,-p}{\mathbb{Q}}\right)$ *if* $p \equiv 3 \pmod 4$*;*

3. $B_{p,\infty} \cong \left(\frac{-2,-p}{\mathbb{Q}}\right)$ *if* $p \equiv 5 \pmod 8$*;*

4. $B_{p,\infty} \cong \left(\frac{-r,-p}{\mathbb{Q}}\right)$ *if* $p \equiv 1 \pmod 8$*, where* $r \equiv 3 \pmod 4$ *is a prime number that is not a square modulo* p*.*

Proof. See [66]. □

From now onward, our main quaternion algebra of concern will be $B_{p,\infty}$; it turns out to be the most interesting one in the context of elliptic curves, because it contains all endomorphism rings of supersingular elliptic curves over fields of characteristic p. However, many of the definitions and results that follow are equally valid for arbitrary quaternion algebras.

[3] Although the adjective *reduced* is technically necessary from a purely mathematical point of view, the terms *reduced norm* and *norm*, and similarly for the trace, are often used interchangably in the context of quaternions.

Fractional ideals in $B_{p,\infty}$ are $\mathbb{Z}$-lattices $I \subset B_{p,\infty}$ of rank 4. The (reduced) *norm* of an ideal is defined as the gcd of the (reduced) norms of its elements; $N(I) = \operatorname{nrd}(I) := \gcd\{N(\alpha) \mid \alpha \in I\}$. If $I \subset J$ are two fractional ideals, then the index $[J : I]$ as an abelian group equals $(N(I)/N(J))^2$. If $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ is a $\mathbb{Z}$-basis for I, then we define the *reduced discriminant* of I as $\operatorname{discrd}(I) := |\det(\operatorname{Tr}(\alpha_i\overline{\alpha_j}))_{1\le i,j\le 4}|^{1/2}$; it is independent of the chosen basis.

Orders in $B_{p,\infty}$ are fractional ideals that are also subrings. We say an order $\mathcal{O} \subset B_{p,\infty}$ is *maximal* if it is not strictly contained in any other order. An order is maximal if and only if its reduced discriminant is p. Given a fractional ideal $I \subset B_{p,\infty}$, we denote by $\mathcal{O}_L(I) := \{\alpha \in B_{p,\infty} \mid \alpha I \subset I\}$ its *left order*, and by $\mathcal{O}_R(I) := \{\alpha \in B_{p,\infty} \mid I\alpha \subset I\}$ its *right order*. We say that I is a fractional left (respectively right) $\mathcal{O}$-ideal if $\mathcal{O} \subset \mathcal{O}_L(I)$ (respectively $\mathcal{O} \subset \mathcal{O}_R(I)$). A (left or right) $\mathcal{O}$-ideal I is called *integral* if $I \subset \mathcal{O}$.

Proposition 52. *Let $B_{p,\infty}$ be represented like in Proposition 51. Then*

$$\mathcal{O} = \begin{cases} \left\langle \frac{1+i+j+ij}{2}, i, j, ij \right\rangle & \text{if } p = 2, \\ \left\langle 1, i, \frac{1+j}{2}, \frac{i+ij}{2} \right\rangle & \text{if } p \equiv 3 \pmod 4, \\ \left\langle 1, i, \frac{-1+i+j}{2}, \frac{2-i+ij}{4} \right\rangle & \text{if } p \equiv 5 \pmod 8, \\ \left\langle \frac{1+i}{2}, \frac{j+ij}{2}, \frac{i+cij}{r}, ij \right\rangle & \text{if } p \equiv 1 \pmod 8, \text{ where } c^2p = -1 \pmod r, \end{cases}$$

is a maximal order of $B_{p,\infty}$.

Proof. See [48, Lemmas 2–4] or [89, Lemmas 2.2–3]. □

The endomorphism ring. We finally have all the necessary language to classify endomorphism rings of elliptic curves: they all turn out to be lattices of rank 1, 2 or 4. A more precise statement is the following.

Theorem 53 (Deuring). *Let E be an elliptic curve defined over a field k of characteristic p. The ring* $\operatorname{End}(E)$ *is isomorphic to one of the following:*

- *$\mathbb{Z}$;*
- *An order $\mathcal{O}$ in a quadratic imaginary field; in this case we say that E has* complex multiplication *by $\mathcal{O}$;*
- *Only if $p > 0$, a maximal order $\mathcal{O}$ in $B_{p,\infty}$; in this case we say that E has* quaternionic multiplication *by $\mathcal{O}$. This happens if and only if E is supersingular.*

Proof. See [76, III, Coro. 9.4] and [47]. □

The smallest $\mathbb{Q}$-algebra containing $\operatorname{End}(E)$, i.e. $\operatorname{End}(E)\otimes\mathbb{Q}$, is called the *endomorphism algebra* of E. For curves over finite fields, this is entirely determined by the Frobenius endomorphism, which we recall satisfies a quadratic equation $\pi^2 - t\pi + q = 0$. Indeed we already saw that a curve is supersingular if and only if the characteristic divides the trace t. Otherwise the curve is ordinary and $\operatorname{End}(E)$ must contain an algebraic integer with the same minimal equation, which has discriminant $\Delta_\pi = t^2 - 4q < 0$, and thus $\operatorname{End}(E) \subset \mathbb{Q}(\sqrt{\Delta_\pi})$.

The minimal polynomial of Frobenius can be computed in polynomial time using Schoof's algorithm [72] (see Appendix B), and thus the endomorphism algebra can be determined with the same complexity. Determining the exact order isomorphic to $\operatorname{End}(E)$ is (in general) much more complicated and we shall come back to it in Sections 10 and 22.

Example 54. The elliptic curve $y^2 = x^3 + x$ has supersingular reduction at all primes $p = 3 \bmod 4$. Its ring of $\mathbb{F}_p$-rational endomorphisms is generated by $\pi = \sqrt{-p}$, and it is not maximal in $\mathbb{Q}(\sqrt{-p})$.

The automorphism $\iota : (x, y) \mapsto (-x, iy)$ is only defined over $\mathbb{F}_{p^2}$, and anti-commutes with π. The full endomorphism ring is isomorphic to the maximal order inside $B_{p,\infty}$ containing both π and ι.

Exercises

Exercise I.1. Prove Proposition 6.

Exercise I.2. Determine all the possible automorphisms of elliptic curves.

Exercise I.3. Prove Proposition 19.

Exercise I.4. Using Proposition 24, devise an algorithm to effectively compute $\#E(\mathbb{F}_{q^n})$ given $\#E(\mathbb{F}_q)$.

Exercise I.5. Prove Corollary 28.

Exercise I.6. Prove Proposition 35.

Exercise I.7. Prove Corollary 37.

Exercise I.8. Let K be a complex imaginary number field, $\Lambda \subset K$ a complex lattice, and $\mathcal{O}_\Lambda$ its order as defined in Eq. (5). Prove that $\mathcal{O}_\Lambda$ is an order of K.

Part II

Isogeny graphs

We now look at isogeny graphs: graphs with isomorphisms classes of elliptic curves for vertices, and isogenies for edges. Depending on the constraints we put on the isogenies, we will get graphs with different properties. In this part we will study *isogeny volcanoes* and *CM graphs*, whereas Part IV will be devoted to *supersingular graphs*.

The classification of isogeny graphs was initiated by Mestre [58], Pizer [67, 68] and Kohel [47]; further algorithmic treatment of graphs of ordinary curves, and the now famous name of *isogeny volcanoes*, was subsequently given by Fouquet and Morain [32].

8 Isogeny classes

We have previously learned that being isogenous is an equivalence relation,[4] it thus makes sense to speak of the *isogeny class* of an elliptic curve. Here, we are interested in characterizing these isogeny classes and their connectivity structure. We will mostly focus on isogeny classes over finite fields, however we will occasionally mention the complex case.

We start by linking isogeny classes to endomorphism rings.

Theorem 55 (Serre-Tate)**.** *Two elliptic curves E, E' with complex multiplication are isogenous (over the algebraic closure) if and only if their* endomorphism algebras $\mathrm{End}(E)\otimes\mathbb{Q}$ *and* $\mathrm{End}(E')\otimes\mathbb{Q}$ *are isomorphic.*

In layman terms, this theorem is telling us that two curves with complex multiplication by $\mathcal{O}$ and $\mathcal{O}'$ respectively are isogenous if and only if $\mathcal{O}\subset\mathcal{O}'$ or $\mathcal{O}'\subset\mathcal{O}$; or equivalently if and only if $\mathcal{O}$ and $\mathcal{O}'$ have the same field of fractions.

For supersingular curves, we learned that there exists a unique possibility for $\mathrm{End}(E)\otimes\mathbb{Q}$, namely the unique quaternion algebra ramified at p and ∞. Then, a similar statement to the complex multiplication case holds.

Theorem 56. *Any two supersingular curves over a field of characteristic p are isogenous (over the algebraic closure).*

In the case of finite fields, we saw that $\mathrm{End}(E)\otimes\mathbb{Q}$ is entirely determined by the Frobenius endomorphism. We can strengthen the previous theorems as follows.

Proposition 57. *Two elliptic curves E, E' defined over a finite field k are isogenous over k if and only if $\#E(k) = \#E'(k)$.*

At this stage, we are only interested in elliptic curves up to isomorphism, i.e., j-invariants. Accordingly, we say that two j-invariants are *isogenous* whenever their corresponding curves are.[5]

[4] Reflexivity and transitivity are obvious, symmetry is guaranteed by the dual isogeny theorem.

[5] In some cases we will be interested in elliptic curves up to k-rational isomorphisms, and we will then need finer invariants to classify them. Likewise, we will say the invariants are isogenous when the corresponding curves are.

9 Graphs

We recall some basic concepts about graphs and their spectra. For a comprehensive treatment, see [84, 82, 39].

Definition 58 (Multigraph)**.** A *directed multigraph* (or *multidigraph* or *quiver*) G is a pair (V, E) where V is a set of *vertices* and $E \in \mathbb{N}^{V \times V}$ is a multiset of ordered pairs called *edges*.

When E is a simple set, i.e. $E \in \{0,1\}^{V \times V}$, we recover the usual definition of a directed graph.

The *neighbors* of a vertex v are the vertices of V connected to it by an edge. A *path* from a vertex v to another vertex v' is a sequence of vertices $v \to v_1 \to \cdots \to v'$ such that any two consecutive vertices are neighbors. The *distance* from v to v' is the length of the shortest path between them; if there is no such path, v' is said to be at infinite distance from v. The *degree* of a vertex is the number of edges departing from it; a multigraph where every edge has degree k is called *k-regular*. The *adjacency matrix* of a finite multigraph $G = (V, E)$ is the $|V| \times |V|$ matrix with columns and rows indexed by the vertices, where the (i, j)-th entry is the multiplicity of the edge (v, v').

Definition 59 (Undirected multigraph)**.** A multigraph (V, E) is *undirected* if $E(v, v') = E(v', v)$ for any $v, v' \in V$, i.e. if there are as many edges from v to v' as there are from v' to v.

A weakly undirected multigraph is called *connected* if any two vertices have a path connecting them; it is called *disconnected* otherwise. A *connected component* of an undirected multigraph is a maximal subgraph (i.e. a subset $V' \subset V$ together with the restriction of E to V') that is connected. The *diameter* of a connected multigraph is the largest of all distances between its vertices.

Definition 60 (Spectrum)**.** The *spectrum* of a finite multigraph is the multiset of the eigenvalues of its adjacency matrix.

When the multigraph is undirected, the adjacency matrix is symmetric, thus its spectrum is real. Let (V, E) be k-regular and undirected, and let $V' \subset V$ be the set of vertices of a connected component. It is easy to see that the vector having 1's for the entries corresponding to V' and 0's elsewhere is an eigenvector with eigenvalue k. We can in fact prove a stronger statement.

Theorem 61. *Let G be a k-regular undirected multigraph and let $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$ be its spectrum. Then $|\lambda_i| \leq k$, and the multiplicity of the eigenvalue k equals the number of connected components of G.*

Proof. See [84, Chap. 3]. □

Expansion is a way to express how "well connected" the nodes of a graph are. There are several related definitions of it. We start with the spectral definition, which is simpler to state and often easier to prove, but whose implications are less obvious. From now on, whenever we have a multigraph, we denote by $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$ its spectrum.

Definition 62 (Expander graph)**.** Let $\varepsilon > 0$ and $k \geq 1$. A k-regular undirected multigraph is called a (one-sided) *ε-expander* if

$$\lambda_2 \leq (1 - \varepsilon)k;$$

and a *two-sided ε-expander* if it also satisfies

$$\lambda_n \geq -(1 - \varepsilon)k.$$

A sequence $G_i = (V_i, E_i)$ of multigraphs with $\#V_i \to \infty$ is said to be a one-sided (resp. two-sided) *expander family* if there is an $\varepsilon > 0$ such that G_i is a one-sided (resp. two-sided) ε-expander for all sufficiently large i.

Ramanujan proved a bound on how large ε can be in an expander family.

Theorem 63 (Ramanujan graph)**.** *Let $k \geq 1$, and let G_i be a sequence of k-regular undirected multigraphs on n vertices. Then*

$$\max(|\lambda_2|, |\lambda_n|) \geq 2\sqrt{k-1} - o(1),$$

as $n \to \infty$. A multigraph such that $|\lambda_j| \leq 2\sqrt{k-1}$ for any λ_j except λ_1 is called a Ramanujan multigraph.

Another way to characterize expansion is *edge expansion*, which quantifies how well subsets of vertices are connected to the whole graph, or, said otherwise, how far the graph is from being disconnected.

Definition 64 (Edge expansion)**.** Let $F \subset V$ be a subset of the vertices of G. The *boundary of F*, denoted by $\partial F \subset E$, is the subset of the edges of G that go from F to $V \setminus F$. The *edge expansion ratio* of G, denoted by $h(G)$ is the quantity

$$h(G) = \min_{\substack{F \subset V, \\ \#F \leq \#V/2}} \frac{\#\partial F}{\#F}.$$

Note that $h(G) = 0$ if and only if G is disconnected. Edge expansion is strongly tied to spectral expansion, as the following theorem shows.

Theorem 65 (Discrete Cheeger inequality)**.** *Let G be a k-regular one-sided ε-expander, then*

$$\frac{\varepsilon}{2}k \leq h(G) \leq \sqrt{2\varepsilon}k.$$

Expander families of multigraphs have many applications in theoretical computer science, thanks to their *pseudo-randomness* properties: they are useful to construct *pseudo-random number generators*, *error-correcting codes*, *probabilistic checkable proofs*, and, as we shall see, *cryptographic protocols*. Among their properties, they have *short diameter* and *rapidly mixing walks.*

Proposition 66. *Let G be a k-regular one sided ε-expander. For any vertex v and any radius $r > 0$, let $B(v, r)$ be the* ball *of vertices at distance at most r from v. Then, there is a constant $c > 0$, depending only on k and ε, such that*

$$\#B(v, r) \geq \min((1 + c)^r, \#V).$$

In particular, this shows that the diameter of an expander is bounded by $O(\log n)$, where the constant depends only on k and ε.

A *random walk* of length m is a path $v_1 \to \cdots \to v_m$, defined by the random process that selects v_i uniformly at random among the neighbors of v_{i-1}. If we start from some probability distribution $\mathbf{p}$ on V and walk randomly for m steps, the final vertex of the walk will be distributed like $(A/k)^m\mathbf{p}$, where A is the adjacency matrix of the graph. The following theorem tells us that, for two-sided expanders, this distribution converges exponentially fast in m to the uniform distribution.

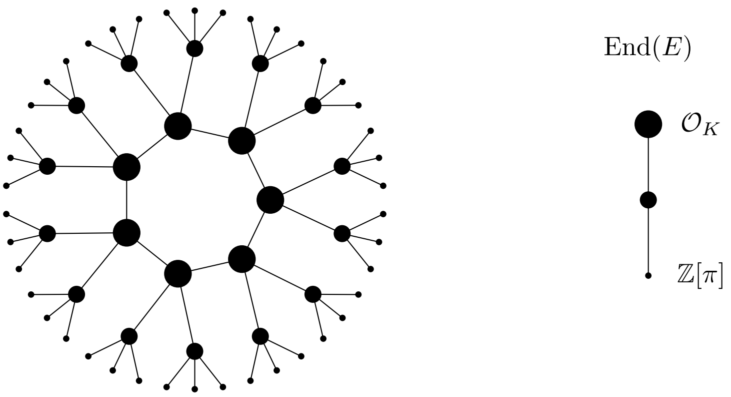


Figure 6: A volcano of 3-isogenies (ordinary elliptic curves, Elkies case), and the corresponding tower of orders inside the endomorphism algebra.

Proposition 67 (Mixing theorem)**.** *Let $G = (V, E)$ be an undirected k-regular multigraph, let A be its adjacency matrix, and let $\sigma_2 = \max(|\lambda_2|, |\lambda_n|)$. Then for every distribution* $\mathbf{p}$ *on V and every $m > 0$, we have*

$$\|\mathbf{u} - (A/k)^m\mathbf{p}\|_1 \leq \sqrt{n}\left(\frac{\sigma_2}{k}\right)^m,$$

where $\mathbf{u}$ *denotes the uniform distribution on V.*

Proof. See [84, Chap. 21]. □

Random regular graphs typically make good expanders, but only a handful of deterministic constructions is known, most of them based on Cayley graphs [57, 13, 39, 84]. In this part we will encounter a construction based on isogenies which is essentially a Cayley graph. In Part IV we will introduce a different construction which achieves Ramanujan's bound.

Definition 68 (Isogeny graph)**.** An *isogeny graph* is a multigraph whose vertices are isomorphism classes of isogenous curves, and whose edges are isogenies between them.

Whenever we include an isogeny in an isogeny graph we will always include its dual too, thus we will usually draw the (multi)graphs as undirected. Figure 6 shows a typical example of isogeny graph over a finite field, where we restrict to isogenies of degree 3.

Note, however that there is an asymmetry in this definition: because we take isogenies up to composition with isomorphisms on the right, several distinct isogenies may have the same dual.[6] This means that isogeny graphs are not undirected in the sense previously defined, however they will behave as such for most practical purposes.

10 Isogeny volcanoes

When we restrict to isogenies of a prescribed degree ℓ, we say that two curves are ℓ-isogenous; by the dual isogeny theorem, this is a symmetric relation. Remark that being ℓ-isogenous is also well defined up to isomorphism.

Let us start from the local structure: given an elliptic curve E and a prime ℓ, how many isogenies of degree ℓ have E as domain? Thanks to Proposition 27, we know this is equivalent to

[6] This can only happen when the automorphism groups of two connected vertices have different sizes, and can thus only happen at a finite number of vertices.

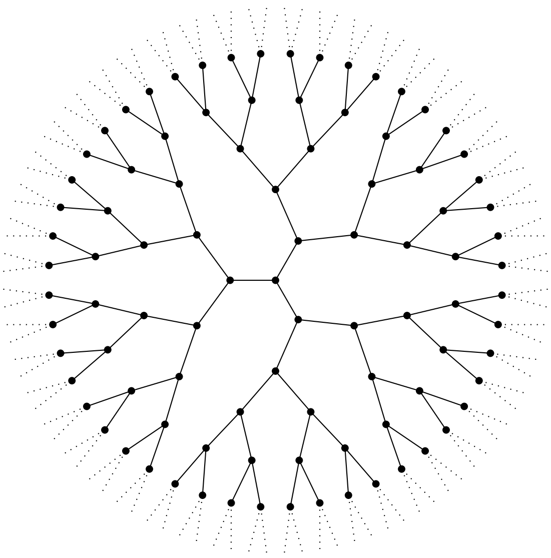


Figure 7: Infinite 2-isogeny graph of elliptic curves over $\mathbb{C}$ without complex multiplication.

asking how many subgroups of order ℓ the curve has; but then we immediately know there are exactly $\ell+1$ isogenies whenever $\ell \neq p$.

For our first example, let us consider a curve $E/\mathbb{C}$ *without* complex multiplication, i.e., such that $\mathrm{End}(E) = \mathbb{Z}$. Its ℓ-isogeny graph, i.e., the connected component of the graph of ℓ-isogenies containing E, is $(\ell+1)$-regular, and cannot have loops, otherwise that would provide a non-trivial cyclic endomorphism of E of degree a power of ℓ. Hence, the ℓ-isogeny graph of E is an infinite $(\ell+1)$-tree, as pictured in Figure 7.

When we think about curves over finite fields, however, some of the isogenies may only be defined in the algebraic closure, thus we would like to restrict our graphs to those isogenies that are defined over $\mathbb{F}_q$. Fortunately, we have a Swiss-army-knife to address this question: the *Frobenius endomorphism* π. Formally, an isogeny ϕ is $\mathbb{F}_q$-rational if and only if $\pi(\ker\phi) = \ker\phi$, which suggests looking at the restriction of π to $E[\ell]$. Assume $\ell \neq p$, then $E[\ell]$ is a group of rank 2 and π acts on it like an element of $\mathrm{GL}_2(\mathbb{F}_\ell)$, up to conjugation. Clearly, the order of π in $\mathrm{GL}_2(\mathbb{F}_\ell)$ is the degree of the smallest extension of $\mathbb{F}_q$ where all ℓ-isogenies of E are defined. But we can tell even more by diagonalizing the matrix: π must have between 0 and 2 eigenvalues, and the corresponding eigenvectors define kernels of rational isogenies. We thus are in one of the following four cases[7]:

(0) π is not triangularizable over $\mathbb{F}_\ell$, then it has no eigenvalues and E has no ℓ-isogenies.

(1.1) π has one eigenvalue of (geometric) multiplicity one, i.e., it is conjugate to a non-diagonal matrix $\left(\begin{smallmatrix}\lambda & * \\ 0 & \lambda\end{smallmatrix}\right)$; then E has one ℓ-isogeny.

(1.2) π has one eigenvalue of multiplicity two, i.e., it acts like a scalar matrix $\left(\begin{smallmatrix}\lambda & 0 \\ 0 & \lambda\end{smallmatrix}\right)$; then E has $\ell+1$ isogenies of degree ℓ.

(2) π has two distinct eigenvalues, i.e., it is conjugate to a diagonal matrix $\left(\begin{smallmatrix}\lambda & 0 \\ 0 & \mu\end{smallmatrix}\right)$ with $\lambda \neq \mu$; then E has two ℓ-isogenies.

[7] In the point counting literature, Case (0) is known as the *Atkin case*, and Case (2) as the *Elkies case*. See Appendix B.

Naturally, the number of eigenvalues of π depends on the factorization of its characteristic polynomial $x^2 - tx + q$ over $\mathbb{F}_\ell$, or equivalently on whether $\Delta_\pi = t^2 - 4q$ is a square modulo ℓ.

But what about the global structure? Any curve $E/\mathbb{F}_q$ can be seen as the reduction modulo p of some curve $E/\bar{\mathbb{Q}}$; thus it must inherit the connectivity structure of the isogeny graph of $E/\bar{\mathbb{Q}}$. However, there is only a finite number of curves defined over $\mathbb{F}_q$, and not all isogenies will be $\mathbb{F}_q$-rational. Thus, the infinite tree of Figure 7 must somehow "fold" or "be pruned" to fit inside $\mathbb{F}_q$.

For example, if $E/\mathbb{F}_q$ is a supersingular curve, we shall see later that its isogeny graph "folds" to a finite $(\ell+1)$-regular graph containing all supersingular curves, up to $\bar{\mathbb{F}}_q$-isomorphisms.

For the case of ordinary curves, Kohel [47] introduced a notion of "depth" in the graph. Let $E/\mathbb{F}_q$ have complex multiplication by an order $\mathcal{O}$ in a number field $K = \mathbb{Q}(\pi)$. Write $\mathcal{O}_K$ for the maximal order of K, then we know that $\mathbb{Z}[\pi] \subset \mathcal{O} \subset \mathcal{O}_K$. We have already seen that two elliptic curves are isogenous if and only if they have the same endomorphism algebra K; Kohel refined this statement as follows.

Proposition 69 (Kohel [47, Prop. 21])**.** *Let E, E' be elliptic curves defined over a finite field, and let $\mathcal{O}, \mathcal{O}'$ be their respective endomorphism rings. Suppose that there exists an isogeny $\phi : E \to E'$ of prime degree ℓ, then $\mathcal{O}$ contains $\mathcal{O}'$ or $\mathcal{O}'$ contains $\mathcal{O}$, and the index of one in the other divides ℓ.*

For a fixed prime ℓ, Kohel defines a curve E to be *at the surface* if $v_\ell([\mathcal{O}_K : \mathrm{End}(E)]) = 0$, where v_ℓ is the ℓ-adic valuation. E is said to be *at depth d* if $v_\ell([\mathcal{O}_K : \mathrm{End}(E)]) = d$; the maximal depth being $d_{\max} = v_\ell([\mathcal{O}_K : \mathbb{Z}[\pi]])$, curves at depth $d_{\max}$ are said to be *at the floor (of rationality)*, and $d_{\max}$ is called the *height* of the graph of E. Kohel calls then an ℓ-isogeny *horizontal* if it goes to a curve at the same depth, *descending* if it goes to a curve at greater depth, *ascending* if it goes to a curve at lesser depth.

But how many horizontal and vertical ℓ-isogenies does a given curve have? The following theorem gives a complete classification, also summarized in Table 1.

Theorem 70 (Kohel [47])**.** *Let $E/\mathbb{F}_q$ be an ordinary elliptic curve, π its Frobenius endomorphism, and Δ_K the fundamental discriminant of $\mathbb{Q}(\pi)$.*

1. *If E is not at the floor, there are $\ell+1$ isogenies of degree ℓ from E, in total.*

2. *If E is at the floor, there are no descending ℓ-isogenies from E.*

3. *If E is at the surface, then there are $\left(\frac{\Delta_K}{\ell}\right) + 1$ horizontal ℓ-isogenies from E (and no ascending ℓ-isogenies).*

4. *If E is not at the surface, there are no horizontal ℓ-isogenies from E, and one ascending ℓ-isogeny.*

Proof. See [47, Prop. 21], or [80, Lecture 23]. □

This theorem shows that, away from the surface, isogeny graphs just look like ℓ-regular complete trees of bounded height, with ℓ descending isogenies at every level except the floor. However, the surface has a more varied structure:

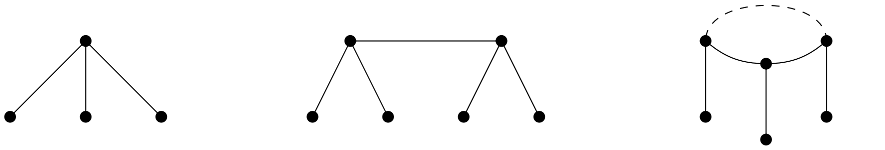
(0) If $\left(\frac{\Delta_K}{\ell}\right) = -1$, there are no horizontal isogenies: the isogeny graph is just a complete tree of degree $\ell+1$ (in the graph theoretic sense) at each level but the last. We call this the *Atkin case*, as it is an extension of the Atkin case in the SEA point counting algorithm.

			Isogeny types		
			$\rightarrow$	$\uparrow$	$\downarrow$
$v_\ell(\Delta_\pi/\Delta_K)=0$	$\ell\nmid[\mathcal{O}_K:\mathcal{O}]$	$\ell\nmid[\mathcal{O}:\mathbb{Z}[\pi]]$	$1+\left(\frac{\Delta_K}{\ell}\right)$		
$v_\ell(\Delta_\pi/\Delta_K)\geq 1$	$\ell\nmid[\mathcal{O}_K:\mathcal{O}]$	$\ell\mid[\mathcal{O}:\mathbb{Z}[\pi]]$	$1+\left(\frac{\Delta_K}{\ell}\right)$		$\ell-\left(\frac{\Delta_K}{\ell}\right)$
	$\ell\mid[\mathcal{O}_K:\mathcal{O}]$	$\ell\mid[\mathcal{O}:\mathbb{Z}[\pi]]$		1	ℓ
	$\ell\mid[\mathcal{O}_K:\mathcal{O}]$	$\ell\nmid[\mathcal{O}:\mathbb{Z}[\pi]]$		1	

Table 1: Number and types of ℓ-isogenies, according to splitting type of the characteristic polynomial of π.

(1) If $\left(\frac{\Delta_K}{\ell}\right)=0$, there is exactly one horizontal isogeny $\phi : E\rightarrow E'$ at the surface. Since E' also has one horizontal isogeny, it necessarily is $\hat{\phi}$, so the surface only contains two elliptic curves, each the root of a complete tree. We call this the *ramified case*.

(2) The case $\left(\frac{\Delta_K}{\ell}\right)=1$ is arguably the most interesting one. Each curve at the surface has exactly two horizontal isogenies, thus the subgraph made by curves on the surface is two-regular and finite, i.e., a cycle. Below each curve of the surface there are $\ell-1$ curves, each the root of a complete tree. We call this the *Elkies case*, again by extension of point counting.



Atkin: $\left(\frac{\Delta_K}{\ell}\right)=-1$ ramified: $\left(\frac{\Delta_K}{\ell}\right)=0$ Elkies: $\left(\frac{\Delta_K}{\ell}\right)=+1$

Figure 8: The three shapes of volcanoes of 2-isogenies of height 1.

The three cases are summarized in Figure 8. Their looks have justified the name of *isogeny volcanoes* for them [32]; in the Elkies case, we call *crater* the cycle at the surface.

We are left with one last question: how large are these graphs? To address this question, we shall need the theory of complex multiplication.

11 Complex multiplication

We now introduce a powerful tool for the study of isogeny graphs. Our goal is to characterize elliptic curves with complex multiplication; to do so, we start from elliptic curves defined over the complex numbers.

Let K be a quadratic imaginary field and let Λ be a complex lattice such that $\Lambda\subset K$. Recall that the order $\mathcal{O}_\Lambda$ of Λ is the ring

$$\mathcal{O}_\Lambda=\{\alpha\in K \mid \alpha\Lambda\subset\Lambda\}, \tag{5}$$

i.e. Λ is a fractional $\mathcal{O}_\Lambda$-ideal. Using Theorem 15 we associate to Λ a complex elliptic curve E_Λ; but then, by definition, $\mathcal{O}_\Lambda\simeq\mathrm{End}(E_\Lambda)$. Said otherwise, E_Λ has *complex multiplication* by $\mathcal{O}_\Lambda$.

We have thus found a way to construct elliptic curves over the complex numbers with complex multiplication by a specified order. Conversely, every curve with complex multiplication arises this way. To show this, we look at the set of all isomorphism classes of elliptic curves with complex multiplication by a specified order $\mathcal{O}$, which we will denote by $\mathrm{Ell}(\mathcal{O})$. Because homothetic lattices give rise to isomorphic curves, fractional ideals $\mathfrak{a}$ and $c\mathfrak{a}$ will be associated to isomorphic curves $E_{\mathfrak{a}}$ and $E_{c\mathfrak{a}}$ as long as $c \neq 0$. This justifies looking at fractional ideals modulo principal ideals.

Definition 71 (Ideal class group)**.** Let $\mathcal{O}$ be an order of a number field K. Let $\mathcal{I}(\mathcal{O})$ be the group of invertible fractional $\mathcal{O}$-ideals, and let $\mathcal{P}(\mathcal{O})$ be the group of principal ideals.

The *ideal class group* of $\mathcal{O}$ is the quotient group

$$\mathrm{Cl}(\mathcal{O}) = \mathcal{I}(\mathcal{O})/\mathcal{P}(\mathcal{O}).$$

It is a finite Abelian group; its order is called the *class number* of $\mathcal{O}$, and denoted by $h(\mathcal{O})$.

When $\mathcal{O}$ is the maximal order, $\mathrm{Cl}(\mathcal{O})$ is also called the class group of K. The class group is a fundamental object in *class field theory*: when $\mathcal{O}$ is the maximal order of an imaginary quadratic number field K, it is isomorphic to the Galois group of the maximal unramified Abelian extension of K, also called the *Hilbert class field* of K; more generally, non-maximal orders are connected to ramified Abelian extensions of K. The next theorem highlights a fundamental connection between the class group and the modular j-invariant, and thus to elliptic curves with complex multiplication by $\mathcal{O}$.

Theorem 72. *Let $\mathcal{O}$ be an order of an imaginary quadratic number field K, and let $\mathfrak{a}_1, \dots, \mathfrak{a}_{h(\mathcal{O})}$ be representatives of* $\mathrm{Cl}(\mathcal{O})$*. Then:*

- *$K(j(\mathfrak{a}_i))$ is an Abelian extension of K;*
- *The $j(\mathfrak{a}_i)$ are all conjugate over K;*
- *The Galois group of $K(j(\mathfrak{a}_i))$ is isomorphic to* $\mathrm{Cl}(\mathcal{O})$*;*
- *$[\mathbb{Q}(j(\mathfrak{a}_i)) : \mathbb{Q}] = [K(j(\mathfrak{a}_i)) : K] = h(\mathcal{O})$;*
- *The $j(\mathfrak{a}_i)$ are integral, their minimal polynomial is called the* Hilbert class polynomial *of $\mathcal{O}$;*
- $\mathrm{Cl}(\mathcal{O})$ *acts freely and transitively on* $\mathrm{Ell}(\mathcal{O})$*, in particular* $\#\,\mathrm{Ell}(\mathcal{O}) = h(\mathcal{O})$*.*

Proof. See [77, Ch. II] and [52, Ch. 10]. □

Hence, we have completely characterized all elliptic curves with complex multiplication by an order $\mathcal{O}$, up to isomorphism; in particular, we now know that j-invariants with complex multiplication (sometimes called *singular j-invariants*) are algebraic integers. In the next section, we shall say more on how $\mathrm{Cl}(\mathcal{O})$ acts on the set $\mathrm{Ell}(\mathcal{O})$.

Example 73. Let $\mathcal{O} = \mathbb{Z}[i]$, so that $\mathcal{O}$ is the ring of integers of $\mathbb{Q}(i)$. It was already proven by Gauss that $\mathbb{Z}[i]$ is a principal ideal domain, and thus that its class group is trivial. Up to homothety, there is a unique lattice with order $\mathbb{Z}[i]$, and one such representative is $\mathbb{Z}[i]$ itself.

Recall the definition of the Eisenstein series

$$G_{2k}(\Lambda) = \sum_{\omega \in \Lambda \setminus \{0\}} \omega^{-2k}.$$

But in our case $\Lambda = \mathbb{Z}[i]$, thus $i\Lambda = \Lambda$, hence

$$G_{2k}(\Lambda) = G_{2k}(i\Lambda) = i^{-2k}G_{2k}(\Lambda) = (-1)^k G_{2k}(\Lambda).$$

In particular $G_6(\Lambda) = -G_6(\Lambda) = 0$, hence, by the definition of the modular j-invariant (Theorem 13), $j(\mathbb{Z}[i]) = 1728$.

This shows that that the Hilbert class polynomial of $\mathbb{Z}[i]$ is $X - 1728$, and that the curve $E : y^2 = x^3 + x$ is the only curve over $\mathbb{C}$, up to isomorphism, with complex multiplication by $\mathbb{Z}[i]$. In particular, $\mathbb{Z}[i]$ contains a subgroup of units $\{\pm 1, \pm i\}$, which correspond to the four automorphisms generated by the map

$$\begin{aligned} \iota : E &\longrightarrow E, \\ (x, y) &\longmapsto (-x, iy). \end{aligned}$$

11.1 Complex multiplication for finite fields

At this point, we have a complete characterization of complex multiplication elliptic curves in characteristic 0. What happens, then, in positive characteristic p?

There are at least two ways in which we could construct elliptic curves over a finite field with endomorphism ring larger than $\mathbb{Z}$. One is to start from a complex multiplication elliptic curve E defined over a number field L, and then reduce at a place[8] $\mathfrak{p}$ over p. We write $\bar{E} = E(\mathfrak{p})$ for the reduction of E at the place $\mathfrak{p}$; if we do this carefully (for example, we must avoid singular reductions), non-trivial endomorphisms of E will descend to non-trivial endomorphisms of $\bar{E}$.

Theorem 74 (Deuring)**.** *Let E be an elliptic curve over a number field L, with complex multiplication by an order $\mathcal{O} \subset K$. Let $\mathfrak{p}$ be a place of L over p, and assume that E has non-singular reduction $\bar{E}$ modulo $\mathfrak{p}$. The curve $\bar{E}$ is supersingular if and only if p has only one prime of K above it (p fully ramifies or remains prime in k).*

Suppose that p splits completely in K. Let f be the conductor of $\mathcal{O}$, and write $f = p^r f_0$, where $p \nmid f_0$. Then:

- *$\bar{E}$ has complex multiplication by the order in K with conductor f_0.*
- *If $p \nmid f$, then the map $\omega \mapsto \omega(\mathfrak{p})$ defines an isomorphism of* $\mathrm{End}(E)$ *and* $\mathrm{End}(\bar{E})$*.*

Proof. See [52, Ch. 13]. □

Note that $p > 2$ splits in K if and only if the fundamental discriminant Δ_K of K is a square modulo p, i.e. if the Legendre symbol $\left(\frac{\Delta_K}{p}\right)$ is equal to 1. To cover the case $p = 2$ with the same notation, we may use Kronecker's extension of Legendre's symbol, which is equal to 1 if and only if p splits.

Example 75. We have seen that the elliptic curve $E/\mathbb{Q}$ defined by $y^2 = x^3 + x$ has complex multiplication by $\mathbb{Z}[i]$. Assume $p > 2$; by virtue of the theorem above, $E(p)$ is supersingular if and only if $(-4/p) = -1$, i.e., if and only if $p \equiv 3 \bmod 4$.

In particular, this implies that -1 is not a square modulo p, and thus that the automorphism $(x, y) \mapsto (-x, iy)$ does not descend to an $\mathbb{F}_p$-automorphism of $E(p)$. It does, however, descend to an $\mathbb{F}_{p^2}$-automorphism, showing that $\mathrm{End}(E(p))$ contains is not commutative, but contains a subring isomorphic to $\mathbb{Z}[i]$.

[8] A *place* is just a fancy name for a prime ideal of L.

Another approach is to directly construct a curve $E/\mathbb{F}_q$ so that its Frobenius endomorphism is in the desired order. Recall that the Frobenius endomorphism π satisfies a quadratic equation

$$\pi^2 - t\pi + q = 0,$$

with discriminant $\Delta_\pi = t^2 - 4q \leq 0$. Setting the case $\Delta_\pi = 0$ aside, $\operatorname{End}(E)$ necessarily contains a subring $\mathbb{Z}[\pi]$, isomorphic to an order of $\mathbb{Q}(\sqrt{\Delta_\pi})$. It turns out that these approach is essentially equivalent to the previous one, as a famous theorem shows.

Theorem 76 (Deuring's lifting theorem)**.** *Let E_0 be an elliptic curve in characteristic p, with an endomorphism ω_o which is not trivial. Then there exists an elliptic curve E defined over a number field L, an endomorphism ω of E, and a non-singular reduction of E at a place $\mathfrak{p}$ of L lying above p, such that E_0 is isomorphic to $E(\mathfrak{p})$, and ω_0 corresponds to $\omega(\mathfrak{p})$ under the isomorphism.*

Proof. See [52, Ch. 13]. □

12 Isogenies and the CM action

From now on we abbreviate "complex multiplication" by CM. We saw in Theorem 72 that the class group $\operatorname{Cl}(\mathcal{O})$ acts on the set $\operatorname{Ell}(\mathcal{O})$ of CM elliptic curves over $\mathbb{C}$ with complex multiplication by $\mathcal{O}$. After having identified $\operatorname{Cl}(\mathcal{O})$ with the Galois group of the Hilbert class field, this action is just the Galois action, however we are still missing an explicit identification.

Additionally, when working with CM curves over a finite field, it becomes clumsy (and even computationally infeasible) to go back to $\mathbb{C}$ in order to identify the curves with the generators of the Hilbert class field and then act on them by Galois. Instead, we will now give the action of $\operatorname{Cl}(\mathcal{O})$ on $\operatorname{Ell}(\mathcal{O})$ explicitly, without any mention of class field theory.

From now on we let $\mathcal{O}$ be an order in a number field K, we denote by $\operatorname{Ell}_q(\mathcal{O})$ the set of elliptic curves over $\mathbb{F}_q$ with CM by $\mathcal{O}$, and we assume that it is non-empty. Because curves in $\operatorname{Ell}_q(\mathcal{O})$ are connected exclusively by horizontal isogenies, we will also call it a *horizontal isogeny class*.

Let $E \in \operatorname{Ell}_q(\mathcal{O})$, let $\mathfrak{a}$ be an invertible ideal in $\mathcal{O}$, of norm coprime to q, and define the $\mathfrak{a}$-*torsion* subgroup of E as

$$E[\mathfrak{a}] = \{P \in E(\bar{\mathbb{F}}_q) \mid \sigma(P) = 0 \text{ for all } \sigma \in \mathfrak{a}\}.$$

This subgroup is the kernel of a separable isogeny $\phi_\mathfrak{a} : E \to E/E[\mathfrak{a}]$; it can be proven that $\phi_\mathfrak{a}$ is horizontal, and that its degree is the *norm* of $\mathfrak{a}$. By composing with an appropriate purely inseparable isogeny, the definition of $\phi_\mathfrak{a}$ is easily extended to invertible ideals of any norm.[9]

Writing $\mathfrak{a}\cdot E$ for the isomorphism class of the image of $\phi_\mathfrak{a}$, we get an action $\cdot : \mathcal{I}(\mathcal{O})\times\operatorname{Ell}_q(\mathcal{O}) \to \operatorname{Ell}_q(\mathcal{O})$ of the group of invertible ideals of $\mathcal{O}$ on $\operatorname{Ell}_q(\mathcal{O})$. It is then apparent that endomorphisms of E correspond to principal ideals in $\mathcal{O}$, and act trivially on $\operatorname{Ell}_q(\mathcal{O})$. Since the action factors through principal ideals, it natural to consider the induced action of $\operatorname{Cl}(\mathcal{O})$ on $\operatorname{Ell}_q(\mathcal{O})$. The main theorem of complex multiplication states that this action is *simply transitive*.

Theorem 77 (Complex multiplication)**.** *Let $\mathbb{F}_q$ be a finite field, $\mathcal{O} \subset \mathbb{Q}(\sqrt{-D})$ an order in a quadratic imaginary field, and $\operatorname{Ell}_q(\mathcal{O})$ the set of $\bar{\mathbb{F}}_q$-isomorphism classes of curves with complex multiplication by $\mathcal{O}$.*

[9] A more formal treatment encompassing inseparable isogenies will be given in Section 20.

Number fields	**Elliptic curves**
Order	Endomorphism ring
Integral invertible ideal	Horizontal isogeny
Integral principal ideal	Endomorphism
Conjugate ideal	Dual isogeny
Ideal norm	Isogeny degree
Ideal class	$\mathrm{Hom}(E, E')$

Table 2: Correspondences of complex multiplication.

Assume $\mathrm{Ell}_q(\mathcal{O})$ *is non-empty, then it is a* principal homogeneous space *for the class group* $\mathrm{Cl}(\mathcal{O})$*, under the action*

$$\begin{aligned} \mathrm{Cl}(\mathcal{O}) \times \mathrm{Ell}_q(\mathcal{O}) &\longrightarrow \mathrm{Ell}_q(\mathcal{O}), \\ (\mathfrak{a}, E) &\longmapsto \mathfrak{a} \cdot E \end{aligned}$$

defined above.

Being a principal homogeneous space (also called a *torsor*) means that, for any fixed base point $E \in \mathrm{Ell}_q(\mathcal{O})$, there is a bijection

$$\begin{aligned} \mathrm{Cl}(\mathcal{O}) &\longrightarrow \mathrm{Ell}_q(\mathcal{O}) \\ \text{Ideal class of } \mathfrak{a} &\longmapsto \text{Isomorphism class of } \mathfrak{a} \cdot E. \end{aligned}$$

This confirms what we already knew, that $\#\mathrm{Ell}_q(\mathcal{O}) = h(\mathcal{O})$. We summarize in Table 2 the correspondence between ideals and isogenies given by complex multiplication. We now have all the necessary element to answer our original question on the size of ℓ-isogeny volcanoes.

Corollary 78. *Let* $\mathcal{O}$ *be a quadratic imaginary order, and assume that* $\mathrm{Ell}_q(\mathcal{O})$ *is non-empty. Let* ℓ *be a prime such that* $\mathcal{O}$ *is* ℓ*-maximal, i.e., such that* ℓ *does not divide the conductor of* $\mathcal{O}$*. All* ℓ*-isogeny volcanoes of curves in* $\mathrm{Ell}_q(\mathcal{O})$ *are isomorphic. Furthermore, one of the following is true.*

(0) If the ideal (ℓ) *is prime in* $\mathcal{O}$*, then there are* $h(\mathcal{O})$ *distinct* ℓ*-isogeny volcanoes of Atkin type, with surface in* $\mathrm{Ell}_q(\mathcal{O})$*.*

(1) If (ℓ) *is ramified in* $\mathcal{O}$*, i.e., if it decomposes as a square* $\mathfrak{l}^2$*, then there are* $h(\mathcal{O})/2$ *distinct* ℓ*-isogeny volcanoes of ramified type, with surface in* $\mathrm{Ell}_q(\mathcal{O})$*.*

(2) If (ℓ) *splits as a product* $\mathfrak{l} \cdot \hat{\mathfrak{l}}$ *of two distinct prime ideals, then there are* $h(\mathcal{O})/n$ *distinct* ℓ*-isogeny volcanoes of Elkies type, with craters in* $\mathrm{Ell}_q(\mathcal{O})$ *of size* n*, where* n *is the order of* $\mathfrak{l}$ *in* $\mathrm{Cl}(\mathcal{O})$*.*

But we can extract even more information from the group action. Assume that the Frobenius endomorphism splits modulo ℓ, i.e., that

$$\pi^2 - t\pi + q = (\pi - \lambda)(\pi - \mu) \mod \ell$$

for two distinct eigenvalues λ, μ of the action of π on $E[\ell]$. Associate to λ and μ the prime ideals $\mathfrak{a} = (\pi - \lambda, \ell)$ and $\hat{\mathfrak{a}} = (\pi - \mu, \ell)$, both of norm ℓ; then $E[\mathfrak{a}] \subset E[\ell]$ is the eigenspace of λ, and $E[\hat{\mathfrak{a}}] \subset E[\ell]$ that of μ. Because $\mathfrak{a}\hat{\mathfrak{a}} = \hat{\mathfrak{a}}\mathfrak{a} = (\ell)$, the ideal classes $\mathfrak{a}$ and $\hat{\mathfrak{a}}$ are the inverse of one

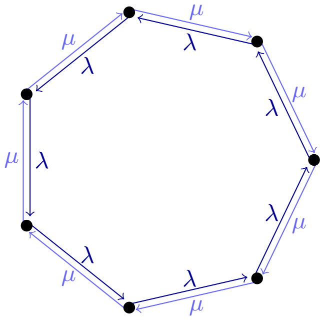


Figure 9: An isogeny cycle for an Elkies prime ℓ, with edge directions associated with the Frobenius eigenvalues λ and μ.

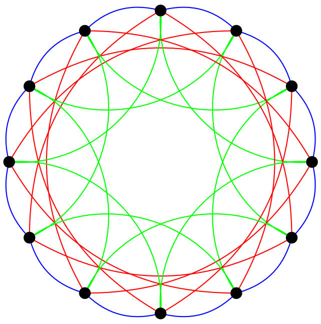


Figure 10: Graph of horizontal isogenies on 12 curves, with isogenies of three different degrees (represented in different colors).

another in $\mathrm{Cl}(\mathcal{O})$, therefore the isogenies $\phi_{\mathfrak{a}} : E \to \mathfrak{a} \cdot E$ and $\phi_{\hat{\mathfrak{a}}} : \mathfrak{a} \cdot E \to E$ are dual to one another (up to isomorphism).

Hence, we see that the eigenvalues λ and μ define two opposite directions on the ℓ-isogeny crater, independent of the starting curve, as shown in Figure 9. The size of the crater is the order of $(\pi - \lambda, \ell)$ in $\mathrm{Cl}(\mathcal{O})$, and the set $\mathrm{Ell}_q(\mathcal{O})$ is partitioned into craters of equal size. What we have here is a very basic example of *Cayley graph*.

Definition 79 (Cayley graph)**.** Let G be a group and $S \subset G$ be a symmetric subset (i.e., $s \in S$ implies $s^{-1} \in S$). The *Cayley graph* of (G, S) is the undirected graph whose vertices are the elements of G, and such that there is an edge between g and sg if and only if $s \in S$.

The graph in Figure 9 is isomorphic to a Cayley graph of $\mathrm{Cl}(\mathcal{O})$ for an edge set $S = \{\mathfrak{a}, \hat{\mathfrak{a}}\}$, but, unlike the Cayley graph itself, its vertex set is $\mathrm{Ell}_q(\mathcal{O})$, which is in bijection with $\mathrm{Cl}(\mathcal{O})$ only up to automorphism.[10] This graph is sometimes called the *Schreier graph* of $(\mathrm{Cl}(\mathcal{O}), S, \mathrm{Ell}_q(\mathcal{O}))$, to distinguish it from the proper Cayley graph.

Is this graph, a cycle when seen as an undirected 2-regular graph, an expander? By properly arranging vertices, its adjacency matrix is circulant with two non-zero entries per row, hence its eigenvalues are $\lambda_t = e^{2i\pi t/n} + e^{-2i\pi t/n}$ for $t = 0, \dots, n-1$ where $n = h(\mathcal{O})$. In particular $\lambda_0 = 2$, and $\lambda_1 \to 2$ as $n \to \infty$, proving that cycles are not expanders; and indeed, it is obvious that this graph has large diameter relative to the number of vertices, contradicting Proposition 66.

It turns out that we can obtain expanders in this way by "gluing many isogeny craters together", as represented in Figure 10, by taking just a slightly larger set $S \subset \mathrm{Cl}(\mathcal{O})$. The following theorem is an instance of a classic technique to construct expanders from Cayley graphs (see [84, Chap. 16]).

Theorem 80 (Jao, Miller, Venkatesan [41])**.** *Let $\mathcal{O}$ be a quadratic imaginary order, and assume that $\mathrm{Ell}_q(\mathcal{O})$ is non-empty. Let $\delta > 0$, and define the graph G on $\mathrm{Ell}_q(\mathcal{O})$ where two vertices are connected whenever there is a horizontal isogeny between them of prime degree bounded by $O((\log q)^{2+\delta})$.*

Then G is a regular graph and, under the generalized Riemann hypothesis for the characters of $\mathrm{Cl}(\mathcal{O})$, there exists an ε independent of $\mathcal{O}$ and q such that G is a two-sided ε-expander.

[10] Said otherwise, any vertex could be mapped to the identity of $\mathrm{Cl}(\mathcal{O})$, and "we forgot which one it was".

Exercises

Exercise II.1. Prove that Proposition 57 implies the finite field case of Theorems 55 and 56. Then, prove the converse.

Exercise II.2. Prove that the dual of a horizontal isogeny is horizontal, and that the dual of a descending isogeny is ascending.

Exercise II.3. Prove that the height of a volcano of ℓ-isogenies is $v_\ell(f_\pi)$, the ℓ-adic valuation of the Frobenius endomorphism.

Exercise II.4. Let $X^2 - tX - q$ be the minimal polynomial of π, and suppose that it splits as $(X - \lambda)(X - \mu)$ in $\mathbb{Z}_\ell$ (the ring of ℓ-adic integers). Prove that the volcano of ℓ-isogenies has height $v_\ell(\lambda - \mu)$.

Exercise II.5. Prove that $E[\ell] \subset E(\mathbb{F}_q)$ implies $\ell | (q - 1)$.

Exercise II.6. Let $\omega \in \mathbb{C}$ be a cube root of unity, the ring $\mathbb{Z}[\omega]$ is also known as the *Eisenstein integers*. Determine all elliptic curves with complex multiplication by $\mathbb{Z}[\omega]$.

Exercise II.7. Prove that -163 is not a square modulo all odd primes < 41. (Hint: $\mathbb{Q}(\sqrt{-163})$ has class number 1).

Exercise II.8. Find a prime power q and an elliptic curve $E/\mathbb{F}_q$ such that the 3-isogeny volcano of E is the same as the one in Figure 6.

Part III

Cryptographic group actions

In this part we introduce our first isogeny based cryptographic protocols. We start with the classic elliptic curve Diffie–Hellman key exchange (ECDH), then we introduce a generalization of Diffie–Hellman based on the theory of complex multiplication and we present a particularly efficient instantiation named CSIDH. Finally we discuss security and rapidly survey other schemes based on complex multiplication.

13 Diffie–Hellman key exhange

Elliptic curves are largely present in modern technology thanks to their applications in cryptography. The simplest of these applications is the *Diffie–Hellman key exchange*, a cryptographic protocol by which two parties communicating over a public channel can agree on a common secret string unknown to any other party listening on the same channel.

The original protocol was invented in the 1970s by Whitfield Diffie and Martin Hellman [28], and constitutes the first practical example of *public key cryptography*. The two communicating parties are customarily called *Alice* and *Bob*, and the snooping third party is represented by the character *Eve* (for *eavesdropper*). To set up the protocol, Alice and Bob agree on a set of public parameters:

- A *large enough* prime number p, such that $p-1$ has a *large enough* prime factor;
- A multiplicative generator $g \in \mathbb{Z}/p\mathbb{Z}$.

Then, Alice and Bob perform the following steps:

1. Each chooses a *secret* integer in the interval $]0, p-1[$; call *a Alice's secret* and *b Bob's secret.*
2. They respectively compute $A = g^a$ and $B = g^b$.
3. They exchange A and B over the public channel.
4. They respectively compute the *shared secret* $B^a = A^b = g^{ab}$.

The protocol can be easily generalized by replacing the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ with any other cyclic group $G = \langle g \rangle$. From Eve's point of view, she is given the knowledge of the group G, the generator g, and Alice's and Bob's public data $A, B \in G$; her goal is to recover the shared secret g^{ab}. This is known as the *Computational Diffie–Hellman* (CDH) problem. An even simpler problem is the following.

Definition 81 (Discrete logarithm)**.** Let G be a cyclic group generated by an element g. For any element $A \in G$, we define the *discrete logarithm of A in base g*, denoted $\log_g(A)$, as the unique integer in the interval $[0, \#G[$ such that

$$g^{\log_g(A)} = A.$$

It is clear that if Eve can compute discrete logarithms in G efficiently, then she can solve CDH. The converse is not true in general, but it is generally assumed to be. At any rate, the best attacks against CDH use a discrete logarithm solver, this is why we usually say that the

Public parameters	Finite field $\mathbb{F}_p$, with $\log_2 p \approx 256$, Elliptic curve $E/\mathbb{F}_p$, such that $\#E(\mathbb{F}_p)$ is prime, A generator P of $E(\mathbb{F}_p)$.	
	Alice	**Bob**
Pick random secret	$0 < a < \#E(\mathbb{F}_p)$	$0 < b < \#E(\mathbb{F}_p)$
Compute public data	$A = [a]P$	$B = [b]P$
Exchange data	$A \longrightarrow$	$\longleftarrow B$
Compute shared secret	$S = [a]B$	$S = [b]A$

Figure 11: The Diffie–Hellman protocol over elliptic curves

Diffie–Hellman protocol is based on the hardness of the discrete logarithm problem in the group G.

We know algorithms to compute discrete logarithms in a *generic* group G that require $O(\sqrt{q})$ computational steps (see [43]), where q is the largest prime divisor of $\#G$; we also know that these algorithms are *optimal for abstract cyclic groups* [75]. For this reason, G is usually chosen so that the largest prime divisor q has size at least $\log_2 q \approx 256$. However, the proof of optimality does not exclude the existence of better algorithms for *specific* groups G. And indeed, algorithms of complexity better than $O(\sqrt{\#G})$ are known for the case $G = (\mathbb{Z}/p\mathbb{Z})^\times$ [43], thus requiring parameters of considerably larger size to guarantee cryptographic strength.

On the contrary, no algorithms better than the generic ones are known when G is a subgroup of $E(k)$, where E is an elliptic curve defined over a finite field k. This led Miller [59] and Koblitz [45, 46] to suggest, in the 1980s, to replace $(\mathbb{Z}/p\mathbb{Z})^\times$ in the Diffie–Helman protocol by the group of rational points of an elliptic curve of (almost) prime order over a finite field. The resulting protocol is summarized in Figure 11.

The Elliptic Curve Diffie–Hellman protocol (ECDH) is today a widely adopted standard, used for example to establish secure TLS connection, the encrypted layer of Internet. Other protocols built on top of the difficulty of solving the elliptic curve discrete logarithm problem, such as the ECDSA signing algorithm, are also widely in use today.

In recent years, however, there has been a push to amend cryptographic standards in view of the threat posed by general purpose *quantum computers*. It is well known, indeed, that Shor's algorithm [74] would solve the factorization and the discrete logarithm problems in polynomial time on a quantum computer, thus sealing the fate of RSA, ECDH, and any other protocol based on them.

In the next sections we shall present *cryptographic group actions*, a generalization of discrete logarithm groups that is believed to be, in general, resistant to attacks by quantum computers. The only examples of quantum-resistant cryptographic commutative group actions currently known are based on the theory of complex multiplication.

14 Cryptographic group actions

In his seminal unpublished work [18], Couveignes defined a generalization of discrete logarithm groups called *hard homogeneous spaces*, a fancy name for a group action with some associated hard computational problem. Group actions had previously been considered by Brassard and Yung [9], although their focus differs slightly from Couveignes'. We shall follow here the more modern treatment of [1], where these are called *cryptographic group actions*.

Below we write $(G, X, \cdot)$ for the action of a group G on a set X, denoted by $x' = g \cdot x$.

Definition 82 (Effective Group Action)**.** A group action $(G, X, \cdot)$ is *effective* if the following properties are satisfied:

1. The group G is finite and there exist efficient algorithms for:

   (a) *Membership testing*, i.e., to decide if a given bit string represents a valid group element in G.

   (b) *Equality testing*, i.e., to decide if two bit strings represent the same group element in G.

   (c) *Sampling*, i.e., to sample an element g from a distribution on G statistically close to uniform.

   (d) *Operation*, i.e., to compute gh for any $g, h \in G$.

   (e) *Inversion*, i.e., to compute g^{-1} for any $g \in G$.

2. The set X is finite and there exist efficient algorithms for:

   (a) *Membership testing*, i.e., to decide if a bit string represents a valid set element.

   (b) *Unique representation*, i.e., given any arbitrary set element $x \in X$, compute a string $\hat{x}$ that canonically represents x.

3. There exists a distinguished element $x_0 \in X$, called the *origin*, such that its bit-string representation is known.[11]

4. There exists an efficient algorithm that given (some bit-string representations of) any $g \in G$ and any $x \in X$, outputs $g \cdot x$.

In practice, we will mostly deal with regular group actions, i.e. such that for any $x, x' \in X$ there is a unique $g \in G$ such that $g \cdot x = x'$. Then, $\#G = \#X$. Additionally, we will only consider Abelian group actions.

Definition 83. Let $(G, X, \cdot)$ be an effective group action. Define the functions

$$\begin{aligned} f_x : G &\to X, & \pi_g : X &\to X, \\ g &\mapsto g \cdot x, & x &\mapsto g \cdot x. \end{aligned}$$

The group action is said to be:

1. *One-way* if the family of functions f_x is one-way.

2. *Weakly unpredictable* if the family of permutations π_g is weakly unpredictable, i.e., if given a list of random pairs $(x, \pi_g(x))$ it is hard to guess $\pi_g(x^*)$ for a random x^* not in the list.

3. *Weakly pseudorandom* if the family of permutations π_g is weakly pseudorandom, i.e., if it is hard to distinguish between a list of random pairs $(x, \pi_g(x))$ and one of random pairs $(x, \pi(x))$, where π is a uniformly drawn permutation of X.

Discrete logarithm groups are special cases of cryptographic group actions. Indeed, if H is a group of order n, we let $X \subset H$ be the subset of elements of order n, and we let $G = (\mathbb{Z}/n\mathbb{Z})^\times$. Then G acts regularly on X, and it is easy to check that one-wayness, weak unpredictability and

[11] Like a group generator, the origin does not necessarily have a distinguishing mathematical property, and can be taken arbitrarily.

weak pseudorandomness correspond to the difficulty of, respectively, discrete logarithm, CDH and DDH[12].

Likewise, we can generalize the Diffie–Hellman key exchange to cryptographic (Abelian) group actions. The system parameters are the effective group action $(G, X, \cdot)$ with its origin $x_0 \in X$. A secret key is a random element $g \in G$, and the associated public key is $g \cdot x_0$. If Alice and Bob have keypairs (g_A, x_A) and (g_B, x_B), respectively, the shared secret is derived as

$$g_A \cdot x_B = g_A g_B \cdot x_0 = g_B g_A \cdot x_0 = g_B \cdot x_A.$$

Of course, we want to instantiate this protocol with group actions that are not just a discrete logarithm group in disguise. For example, for the group action of complex multiplication, the three hardness properties correspond to the following three problems.

Problem 1 (Group action inverse problem, Vectorization)**.** Given two elliptic curves E, E' with complex multiplication by an order $\mathcal{O}$, find an ideal (class) $\mathfrak{a} \subset \mathcal{O}$ such that $E' = \mathfrak{a} \cdot E$.

Problem 2 (Parallelization, Group action CDH)**.** Let E, E' be elliptic curves with complex multiplication by $\mathcal{O}$. Let $\mathfrak{a} \in \mathrm{Cl}(\mathcal{O})$. Given $(E, \mathfrak{a} \cdot E, E')$, compute $\mathfrak{a} \cdot E'$.

Problem 3 (Group action DDH)**.** Let E, E' be elliptic curves with complex multiplication by $\mathcal{O}$. Let $\mathfrak{a} \in \mathrm{Cl}(\mathcal{O})$. Given a tuple $(E, \mathfrak{a} \cdot E, E', E'')$, decide whether $E'' = \mathfrak{a} \cdot E'$.

Each of these problems appears to be legitimately hard, when the isogeny class is large enough. We haven't shown yet that the complex multiplication group action is an effective one, though. We are going to see there is a catch.

15 Evaluating the CM group action

At the same time as he introduced the formalism of cryptographic group actions, Couveignes also indicated the complex multiplication group action as a candidate. His ideas were independently rediscovered by Rostovtsev and Stolbunov [71, 78], who were the first to point out that the schemes thus obtained are plausibly post-quantum.

However, in order to fulfill the definition of an effective group action, we need to be able to take an arbitrary element $\mathfrak{a} \in \mathrm{Cl}(\mathcal{O})$, an arbitrary curve $E \in \mathrm{Ell}_q(\mathcal{O})$, and to evaluate $\mathfrak{a} \cdot E$. But, if we do not choose carefully an ideal representative for $\mathfrak{a}$, the norm $N(\mathfrak{a}) = \deg \phi_{\mathfrak{a}}$ may contain arbitrarily large prime factors, and we do not necessarily have an efficient representation for it. The best algorithm known for an arbitrary ideal representative has subexponential complexity in $\log(q)$ [42], which overshoots our definition of "efficient". Instead, following Rostovtsev and Stolbunov [71], we may define a variant of the key exchange based on walks in a Cayley graph of $\mathrm{Cl}(\mathcal{O})$, which always picks "efficient" ideal representatives.

As an example, let us consider again the action of exponentiation on a discrete logarithm group. Let $H = \langle g \rangle$ be a cyclic group of order p, let $D = \{s_1, \ldots, s_n\} \subset (\mathbb{Z}/p\mathbb{Z})^\times$ be a generating set such that $\sigma \in D$ implies $\sigma^{-1} \notin D$, and let $S = D \cup D^{-1}$ so that S is symmetric as in Definition 79. Then, $(\mathbb{Z}/p\mathbb{Z})^\times$ acts on H minus the identity by

$$e \cdot g_0 = g_0^e \qquad \text{for } e \in (\mathbb{Z}/p\mathbb{Z})^\times \text{ and } g_0 \in H \setminus \{1\}.$$

We may thus define the Schreier graph of $((\mathbb{Z}/p\mathbb{Z})^\times, S, H \setminus \{1\})$, which is isomorphic to the Cayley graph $((\mathbb{Z}/p\mathbb{Z})^\times, S)$; an example for $p = 13$ is given in Figure 12.

[12] DDH is the *decisional* variant of CDH: distinguish (g, h, g^a, h^a) from a random tuple (g, h, g^a, h^b) of group elements

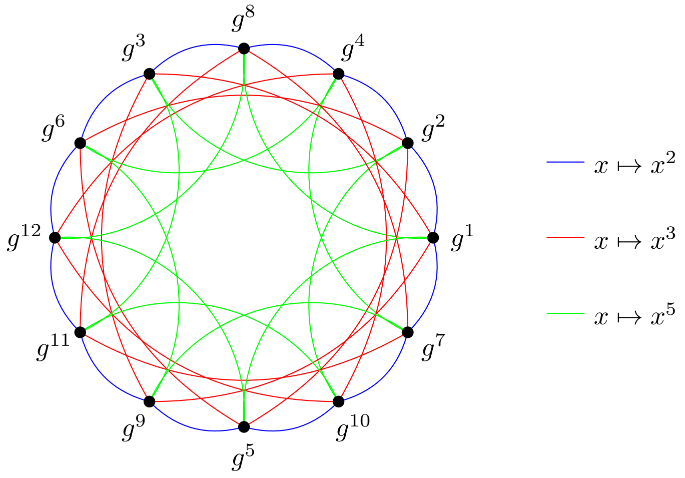


Figure 12: Schreier graph of the generators of a group of order 13 under the action of $S = \{2, 3, 5, 2^{-1}, 3^{-1}, 5^{-1}\} \subset (\mathbb{Z}/13\mathbb{Z})^\times$.

Public parameters	A group G of prime order p, A generating set $D \subset (\mathbb{Z}/p\mathbb{Z})^\times$ such that $\sigma \in D \Rightarrow \sigma^{-1} \notin D$, A generator g of G.	
	Alice	**Bob**
Pick random secret	$a = \prod_{s \in D} s^{a_i}$	$b = \prod_{s \in D} s^{b_i}$
Compute public data	$g_a = a \cdot g$	$g_b = b \cdot g$
Exchange data	$g_a \longrightarrow$	$\longleftarrow g_b$
Compute shared secret	$g_{ab} = a \cdot (g_b)$	$g_{ab} = b \cdot (g_a)$

Figure 13: Key exchange protocol based on random walks in a Schreier graph.

As already seen, a random walk in this graph is a sequence of random edges starting from some vertex g_0 and ending in some vertex g_1. However we see that, because the group action of $(\mathbb{Z}/p\mathbb{Z})^\times$ is Abelian, the order in which the edges are taken from the set S does not matter for determining g_1: only matters the multiplicity of each $s \in S$. We thus define a *non-backtracking random walk* as a tuple of multiplicities $(e_1, \dots, e_n) \in \mathbb{Z}^n$, associated to the element

$$e = \prod_{i=1}^{n} s_i^{e_i} \in (\mathbb{Z}/p\mathbb{Z})^\times,$$

defining the walk $g_0 \to e \cdot g_0$.

We can now define a key exchange protocol where the secrets are non-backtracking random walks, and the public data are vertices of the Schreier graph. The protocol is summarized in Figure 13.

Because $g_a = a \cdot g = g^a$, it is evident that this protocol is closely related to the Diffie–Hellman protocol on the group G, the only difference being that the secret exponents a, b are drawn from an unusual distribution. While this example instance is of no practical interest, its instantiation using a Schreier graph of the complex multiplication group action yields a usable variant of Couveignes' key exchange. We fix a set S of small norm representatives of ideal classes of $\mathrm{Cl}(\mathcal{O})$, corresponding to small degree isogenies between curves in $\mathrm{Ell}_q(\mathcal{O})$. Instead

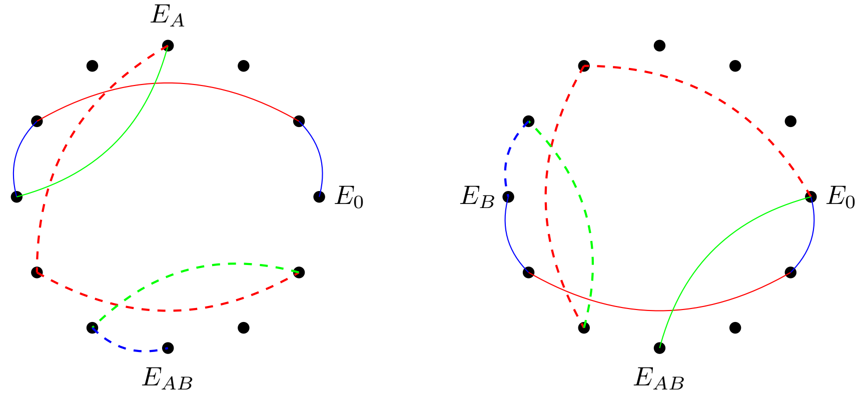


Figure 14: Example of key exchange on the isogeny graph of Figure 10. Alice's path is represented by continuous lines, Bob's path by dashed lines. On the left, Bob computes the shared secret starting from Alice's public data. On the right, Alice does the analogous computation.

of uniformly sampling secrets from $\mathrm{Cl}(\mathcal{O})$, we sample non-backtracking random walks in the Schreier graph of $(\mathrm{Cl}(\mathcal{O}), S, \mathrm{Ell}_q(\mathcal{O}))$, and exchange j-invariants as public data. The walks can be computed efficiently as a composition of small degree isogenies, as discussed in Section 12. Using Theorem 80, we know that the graph is an expander as soon as $\#S \sim (\log q)^2$, thus we can approach the uniform distribution on $\mathrm{Ell}_q(\mathcal{O})$ by taking sufficiently long walks. Hence we have proved that this mode of sampling secrets can be as good as sampling uniformly from $\mathrm{Cl}(\mathcal{O})$, from a security standpoint. The protocol is illustrated in Figure 14.

16 CSIDH and oriented supersingular curves

Even with the adjustments of the previous section, the protocol is far from practical: in 2012 Stolbunov managed to run a 108 bit secure implementation in around 5 minutes [79]. To understand why, let's recap how the CM group action is computed. We have a list of primes splitting in $\mathcal{O}$, which are the norms of the ideals in S. For one such prime ℓ, the Frobenius endomorphism splits as

$$\pi^2 - t\pi + q = (\pi - \lambda)(\pi - \mu) \mod \ell,$$

where we call λ and μ the *eigenvalues of Frobenius* modulo ℓ. Thus the ideals in S are $(\pi - \lambda, \ell)$ and $(\pi - \mu, \ell)$, corresponding to the two directions on the crater of the ℓ-isogeny volcano (see Section 12).

A secret key is a product of ideals in S

$$\mathfrak{s} = \prod_{\mathfrak{a}_i \in S} \mathfrak{a}_i^{e_i}. \tag{6}$$

For simplicity, we may assume that the exponents e_i are taken in a box $[-B, B]$,[13] then the size of the key space is at most $(2B+1)^{\#S}$.

On the other hand, the action of $\mathfrak{s}$ is evaluated by computing e_i isogenies of degree $N(\mathfrak{a}_i)$, for each $\mathfrak{a}_i \in S$, thus at most $\#S \cdot B$ isogenies. We see that, for a fixed set S, increasing B only increases the key space polynomially, while it also increases the running time linearly. On

[13] Negative values represent the dual direction to $(\pi - \lambda, \ell)$, associated to the ideal $(\pi - \mu, \ell)$.

```
**Input:** A curve $E$, its order $N = \#E(\mathbb{F}_q)$,
    a prime $\ell$ such that $(\pi - 1)(\pi - q) = 0 \mod \ell$ with $q \neq 1 \mod \ell$.
**Output:** The curve $(\pi - 1, \ell) \cdot E$.
repeat
    Pick a random point $P$ on $E$;
    Set $K = [N/\ell]P$;
until $K$ is not the point at infinity;
Compute the isogeny $\phi : E \to E/\langle K \rangle$ using Velu's formulas;
return $E/\langle K \rangle$.
```

Figure 15: Evaluation of the CM group action using a special prime.

the other hand, for a fixed B, increasing $\#S$ exponentially increases the key space, while it only increases the running time linearly. Thus, to strike a balance between security and running time, we need to use a fairly large set S: values in the hundreds are typical for $\#S$, and all ideals in S must have different (prime) norms to avoid duplicates. Hence, evaluating the action of $\mathfrak{s}$ implies computing up to $\#S \cdot B$ isogenies of degrees as large as a few thousands!

What algorithms do we have at our disposal to compute these isogenies? We have a curve $E/\mathbb{F}_q$, a prime ℓ and a *direction* $\pi - \lambda$. Without further assumptions, we need to find a field extension $\mathbb{F}_{q^n}$ such that $E[\ell] \subset E(\mathbb{F}_{q^n})$, then find the null subspace of $\pi - \lambda$, and finally apply Vélu's formulas. With the extension degree n generally growing as $O(\ell)$, it is no surprise that evaluating one $\mathrm{Cl}(\mathcal{O})$-action takes several minutes. Better algorithms exist, but they still require $O(\ell^3)$ operations to find the isogeny.

Is it possible to do better? By choosing parameters carefully, we may hope to limit the degrees of the extensions where the $E[\ell]$ live, as first proposed in [25]. Suppose, for example, that $\pi|E[\ell]$ acts like $\left(\begin{smallmatrix}1 & 0\\ 0 & q\end{smallmatrix}\right)$, with $q \neq 1 \mod \ell$. In this case, there is an easily recognizable direction associated to the eigenvalue 1: the corresponding eigenspace is the unique cyclic group of $\mathbb{F}_q$-rational ℓ-torsion points. A point in this eigenspace can be computed by taking a random point in $E(\mathbb{F}_q)$, and multiplying it by $\#E/\ell$: there is a $(\ell - 1)/\ell$ chance that the result is not zero, and can thus be used to compute the ℓ-isogeny of direction $\pi - 1$ using Vélu's formulas. This algorithm is illustrated in Figure 15.

We can do even better. Suppose that $\pi|E[\ell]$ acts like $\left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)$, then both directions are recognizable: $\pi - 1$ is obtained like before, while $\pi + 1$ corresponds to those points such that $\pi(x, y) = (x, -y)$, i.e. the points whose x-coordinate is in $\mathbb{F}_q$ and whose y-coordinate is in $\mathbb{F}_{q^2}$. A simple modification to the algorithm in Figure 15 lets us handle both cases at once.[14] This constraint on π forces two conditions:

1. $N(\pi) = q = -1 \mod \ell$,
2. $\mathrm{Tr}(\pi) = t = 0 \mod \ell$,

and this for each of the norms ℓ in the set S.

The first condition is easy to fulfill: choose a prime $q = f \cdot \prod_i \ell_i - 1$ for some cofactor f. The second one is much harder, because it essentially requires to find a curve $E/\mathbb{F}_q$ with a specific trace t. For E an ordinary curve, the best technique at our disposal consists, essentially, in taking random curves $E/\mathbb{F}_q$ and computing $\#E$, until a suitable one is found [25].

[14] Alternatively, we may note that $E[(\pi + 1, \ell)]$ is the image of $\tilde{E}[(\pi - 1, \ell)]$, where $\tilde{E}$ is a quadratic twist of E. Then, acting by $(\pi - 1, \ell)$ on $\tilde{E}$ and then computing a twist has the same effect as acting by $(\pi + 1, \ell)$ on E.

Public parameters	A set of primes $\{\ell_1, \dots, \ell_m\}$, a prime $q = 4 \prod \ell_i - 1$, A supersingular elliptic curve E_0 defined over $\mathbb{F}_q$, For each ℓ_i the prime ideal $\mathfrak{l}_i = (\ell_i, \pi - 1)$,	
	Alice	**Bob**
Pick random secret	$(a_1, \dots, a_m) \in [-B, B]^m$	$(b_1, \dots, b_m) \in [-B, B]^m$
Compute public data	$E_A = (\prod \mathfrak{l}_i^{a_i}) \cdot E_0$	$E_B = \left(\prod \mathfrak{l}_i^{b_i}\right) \cdot E_0$
Exchange data	$E_A \longrightarrow$	$\longleftarrow E_B$
Compute shared secret	$E_{AB} = (\prod \mathfrak{l}_i^{e_i}) \cdot E_B$	$E_{AB} = \left(\prod \mathfrak{l}_i^{b_i}\right) \cdot E_A$

Figure 16: CSIDH protocol, based on non-backtracking random walks in a supersingular CM-like graph.

CSIDH. On the other hand, if we enforce the constraints above for enough primes ℓ (it is enough that $\prod \ell > 2\sqrt{q}$), then we effectively force t to be 0, and thus E to be supersingular. We saw that supersingular curves do not have complex multiplication, but it turns out there still is a way to define an action of $\mathbb{Z}[\pi]$ on a set of supersingular elliptic curves.

Take a prime field $\mathbb{F}_q$, then any supersingular curve $E/\mathbb{F}_q$ has trace 0, i.e. its Frobenius satisfies the equation

$$\pi^2 = -q.$$

Hence $\mathbb{Z}[\pi]$ is a quadratic imaginary order and a subring of $\mathrm{End}(E)$; it is, in fact, (almost) the subring of $\mathbb{F}_q$-rational endomorphism of E.[15] Then, $\mathrm{Cl}(\mathbb{Z}[\pi])$ acts on the set of $\mathbb{F}_q$-isomorphism classes of supersingular curves, like in the CM case. This fact was first observed in [27] and then leveraged in [10] to define the key exchange protocol CSIDH[16], the *Commutative Supersingular Isogeny Diffie–Hellman* protocol.

CSIDH uses a prime q of the form $4 \cdot \prod_i \ell_i - 1$, and the supersingular curve $y^2 = x^3 - x$ as starting point, so that $\pi|E[\ell_i] = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ for all ℓ_i. By cleverly optimizing computations, CSIDH achieves a key-exchange at the 128 (classical) bits security level in fractions of a second. The scheme is summarized in Figure 16.

Supersingular curves over a prime field and the CSIDH group action are a special case of a more general setting called *orientations of supersingular curves.* Oriented curves are pairs $(E, \mathcal{O} \hookrightarrow \mathrm{End}(E))$, where E is a supersingular curve and $\mathcal{O} \hookrightarrow \mathrm{End}(E)$ is an embedding of a quadratic imaginary order inside $\mathrm{End}(E)$. As Kohel and Coló showed [15], $\mathrm{Cl}(\mathcal{O})$ acts on these curves like in the CM case, and this was leveraged in [23] to define an analogue of CSIDH, named SCALLOP, based on orientations by arbitrary orders.

17 Security and quantum computers

We now do a quick review of the security of protocols based on complex multiplication. The cornerstone of isogeny based cryptography is the isogeny path problem: given isogenous curves E, E', find an isogeny of smooth degree between them. CM based protocols are no exception: find an isogeny walk between E and E', and the group action inverse problem is solved. Naturally, the first parameter to look at is the size of the isogeny class of E, E': too small, and we can find the isogeny by brute force.

[15] There are, in fact, two possibilities for $\mathrm{End}_{\mathbb{F}_p}(E)$, namely $\mathbb{Z}[\pi]$ or $\mathbb{Z}[(\pi+1)/2]$.

[16] Pronounced *sea-side.*

For simplicity we assume that E and E' have complex multiplication by a maximal order. Indeed, if this is not the case, we may use the theory of isogeny volcanoes to find ascending paths from E and E' to two curves $\hat{E}, \hat{E}'$ with complex multiplication by the maximal order.[17] Then, we are left with the problem of finding a horizontal isogeny between $\hat{E}$ and $\hat{E}'$. Since the horizontal isogeny class of $\mathcal{O}_K$ is the smallest among all horizontal isogeny classes of curves with complex multiplication by some $\mathcal{O} \subset \mathcal{O}_K$, this is an easier problem to solve, as first noted by Galbraith, Hess and Smart [34, 38].

Problem 4 (Horizontal isogeny path problem)**.** Let $\mathbb{F}_q$ be a finite field, and let $\mathcal{O}_K$ be the ring of integers of a quadratic imaginary field $K = \mathbb{Q}(\sqrt{-D})$. Given two elliptic curves E, E' defined over $\mathbb{F}_q$ with complex multiplication by $\mathcal{O}_K$, find an isogeny $E \to E'$ of smooth degree.

The size of the horizontal isogeny class is $h(\mathcal{O}_K)$; it is known by the class number formula that this is in $O(\sqrt{\Delta_K}\log\Delta_K)$, and, for the typical isogeny class[18], $\Delta_K = O(q)$. The best generic attack against the Horizontal isogeny path problem is a Pollard-rho style algorithm, performing random walks from E and E' until a collision is found [35]. Its average complexity is $O(\sqrt{h(\mathcal{O}_K)})$, thus $O(q^{1/4})$ for a typical isogeny class. This justifies choosing a prime q of $4n$ bits, for a security level of 2^n, and this is indeed and what CSIDH does [10].

However, we must also ensure that the key space covers the whole $\mathrm{Ell}_q(\mathcal{O}_K)$, possibly approaching the uniform distribution. This means that isogeny walks, as in Eq. (6), must be sampled from a relatively large subset $S \subset \mathrm{Cl}(\mathcal{O}_K)$, implying that $\#S \gg \log q$. For efficiency reasons, practical instantiations take S just large enough: $\#S \sim (\log q)/2$;[19] however it will not go unnoticed that this choice is insufficient to apply Theorem 80. We may as well live with it, changing our security assumptions to take into account the biased distributions given by random walks in graphs that are not provably expander families, but behave in practice as such.

Quantum security. The discussion on security would not be complete without surveying quantum attacks. Indeed, the main selling point of isogeny-based key exchange protocols is their (conjectured) resistance to quantum algorithms.

Couveignes' Hard Homogeneous Spaces setting is scarily similar to the Diffie–Hellman key exchange, which is indeed a special case of it. Shor's algorithm [74] solves the discrete logarithm problem in polynomial time on a quantum computer, and thus breaks the Diffie–Hellman protocol. But is there a variant of Shor's algorithm that also breaks group actions?

Definition 84 (Hidden Subgroup Problem (HSP))**.** Let $f : G \to X$ be a function from a group G to a set X. Assume that there is a subgroup $H \subset G$ such that $f(g) = f(g')$ if and only if $g' \in gH$. The function f is said to *hide* the subgroup H, and the *hidden subgroup problem* consists in finding generators for H, given access to f.

It is well known that Kitaev's generalization of Shor's algorithm [44] solves the hidden subgroup problem in quantum polynomial time, when G is a finitely generated abelian group.

Definition 85 (Hidden Shift Problem (HShP))**.** Let $f_0, f_1 : G \to X$ be two injective functions from a group G to a set X. Assume that there is an element $s \in G$ such that $f_0(g) = f_1(gs)$ for any $g \in G$. The element s is called a *hidden shift* for f_0, f_1, and the *hidden shift problem* is to find s, given access to f_0 and f_1.

[17] Ascending an ℓ-volcano can be done efficiently as long as ℓ is polynomially sized. However SCALLOP [23] uses supersingular curves oriented by a non-maximal quadratic order of large prime conductor, a case where it is not currently known how to efficiently walk to the maximal order.

[18] Including the isogeny class of trace zero supersingular curves used in CSIDH.

[19] Additional constraints in CSIDH force $\#S$ to grow as $(\log q)/(\mathrm{loglog}\, q)$.

For any group G, the hidden shift problem reduces to the hidden subgroup problem for the (generalized) dihedral group $G \rtimes C_2$.[20] No generalization of Kitaev's algorithm is known for non-abelian groups, but a different family of algorithms, due to Kuperberg [49, 50] and Regev [69], solves the HShP in subexponential quantum time $\exp(\sqrt{\log \#G})$.

As first noted in [12] and then improved in [7, 40, 8, 63], Kuperberg's algorithm can be used to solve the Horizontal isogeny path problem as follows: let E, E' be the two curves with complex multiplication by $\mathcal{O}_K$, define two functions $f_0, f_1 : \mathrm{Cl}(\mathcal{O}_K) \to \mathrm{Ell}_q(\mathcal{O}_K)$ as $f_0(\mathfrak{a}) = \mathfrak{a} \cdot E$ and $f_1(\mathfrak{a}) = \mathfrak{a} \cdot E'$, then the hidden shift defines a horizontal isogeny between E and E'.

Kuperberg's algorithm is a game changer for protocols based on complex multiplication: indeed, to ensure 2^n quantum security we need to take $\log q = O(n^2)$. The actual constant depends on the variant of Kuperberg's algorithm, and various parameters such as available quantum memory; its exact value is still debated [4, 63, 14].

18 Beyond key exchange

The isogeny group action framework can be used to construct many other interesting cryptographic protocols than key exchange. Signature schemes were first sketched by Couveignes [18] and Stolbunov [79], and then refined in [24, 6].

TODO: this section will be finished at a later time. In the meantime, you can find a survey on isogeny based signature schemes here [5]

[20] To reduce HShP to HSP, simply define the function f by $f(g, 1) = f_0(g)$ and $f(g, -1) = f_1(g)$, so that the hidden subgroup is generated by $(s, -1)$.

Part IV
The full supersingular isogeny graph

All isogeny graphs we have seen so far were governed by the theory of complex multiplication, and these are essentially the only interesting graphs of ordinary curves. We saw two ways of constructing them: as isogeny graphs of CM curves in characteristic 0, or as graphs of ordinary curves over finite fields. Deuring's theorems (Theorems 74 and 76) showed that these two points of view are essentially the same, while the correspondence between ideals and isogenies presented in Section 12 gave us an algebraic way to realize the action independently of the base field.

Although we encounter again the same theory in the context of supersingular curves, for example in the CSIDH group action (Section 16), the general theory of these curves is more complicated. As we stated in Theorem 53, endomorphism rings of supersingular curves are 4-dimensional objects, the maximal orders of a quaternion algebra. We have no hope of lifting these to endomorphism rings of curves in characteristic 0, but Deuring's lifting theorem gives us a partial result: for every endomorphism $\omega \in \mathrm{End}(E)$, we can find a curve $\bar{E}/\mathbb{C}$ and an endomorphism $\bar{\omega} \in \mathrm{End}(\bar{E})$ above it. Hence the CM theory of $\mathbb{Z}[\omega]$ still applies to the isogeny class of E, but only describes a small part it.

Said otherwise, while isogeny graphs of ordinary curves are completely understood as the reduction modulo p of isogeny graphs of CM curves, supersingular isogeny graphs arise from the simultaneous reduction and "collision" of several CM graphs of unrelated quadratic orders. This part is devoted to these graphs, and to the theory of *quaternionic multiplication* that governs them.

19 Expander graphs from isogenies

The main object in the study of supersingular isogeny graphs is the following.

Definition 86 (Supersingular ℓ-isogeny graph)**.** Fix a prime $\ell \neq p$, the *(full) supersingular ℓ-isogeny graph* is the graph of $\bar{\mathbb{F}}_p$-isomorphism classes of supersingular curves with ℓ-isogenies between them.

In Section 10 we saw how the action of the Frobenius endomorphism on $E[\ell]$ controls the number of $\mathbb{F}_q$-rational isogenies, and thus the structure of the volcano. By Hasse's theorem, supersingular curves over a prime field $\mathbb{F}_p$ necessarily have trace $t = 0$ and thus Frobenius acts like a square root of $-p$, giving an embedding $\mathbb{Z}[\sqrt{-p}] \hookrightarrow \mathrm{End}(E)$ an the CM action used in CSIDH.

But for supersingular curves over $\mathbb{F}_{p^2}$ the most common[21] cases are $t = \pm 2p$, and thus Frobenius acts like $\pm p$, fixing any cyclic subgroup of $E[\ell]$. Said otherwise, all isogenies of a supersingular curve are $\mathbb{F}_{p^2}$-rational.

Proposition 87. *Let E be a supersingular curve defined over a field of characteristic p. Then*

- *$j(E) \in \mathbb{F}_{p^2}$;*
- *There exists an isomorphism (not necessarily $\mathbb{F}_{p^2}$-rational) from E to a curve $E'/\mathbb{F}_{p^2}$ with trace of Frobenius equal to $-2p$;*
- *$E'(\mathbb{F}_{p^2}) \simeq (\mathbb{Z}/(p+1)\mathbb{Z})^2$;*

[21] The only ones, in fact, except if $j = 0, 1728$.

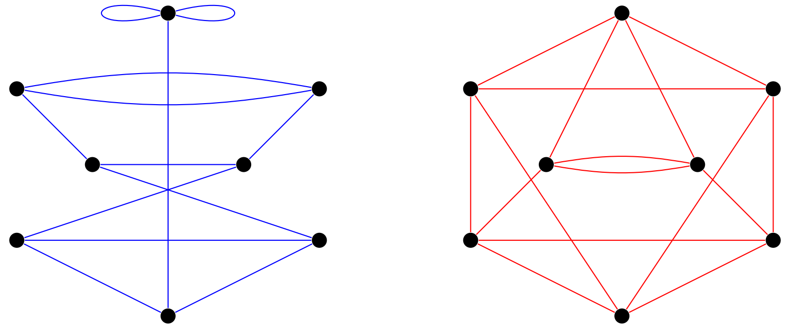


Figure 17: Supersingular isogeny graphs of degree 2 (left, blue) and 3 (right, red) on $\mathbb{F}_{97^2}$.

- *All isogenies and endomorphisms of E' are $\mathbb{F}_{p^2}$-rational.*

Proof. See [80, Lectures 13–14] and [87, § 4]. □

By the proposition above, the supersingular ℓ-isogeny graph is isomorphic to the graph of $\mathbb{F}_{p^2}$-isomorphism classes of curves with trace $-2p$, and every vertex has out-degree $\ell+1$. Mapping every isomorphism class to its quadratic twist, we see that it is also isomorphic to the graph of curves with trace $2p$. Two examples of such graphs are shown in Figure 17.

Although the graph contains all isogenies with their duals, it is not necessarily undirected. Indeed the vertices $j = 0$ and $j = 1728$ have larger automorphism groups (respectively of order 4 and 6, assuming $p > 3$) than any other curve, and thus have more outgoing than incoming edges. Taking $p = 1 \mod 12$ (like in Figure 17) ensures neither curve is supersingular and sidesteps the problem. But even when $p \neq 1 \mod 12$, we can prove that the adjacency matrix of the graph has real eigenvalues and apply all the definitions of Section 9, obtaining a very powerful result.

Theorem 88 (Mestre [58], Pizer [67, 68], Kohel [47])**.** *The supersingular ℓ-isogeny graph is connected, has real spectrum, its largest eigenvalue is $\ell+1$ and every other eigenvalue is smaller than $2\sqrt{\ell}$ in absolute value, i.e. it is a Ramanujan graph.*

The standard proof of this result involves Hecke operators acting on modular forms and is beyond the scope of these lecture notes. As explained in [16], these graphs are distant cousins of Lubotzky–Phillips–Sarnak (LPS) graphs [57, 56], however, unlike those, do not enjoy the structure of a Cayley graph.

The CGL cryptographic hash function. The mixing properties of expander graphs have long been used in computer science to produce pseudo-random behavior. In [11], Charles, Goren and Lauter (CGL) used expander graphs to define cryptographic hash functions.

Their construction assumes a k-regular expander graph is given, with vertices and edges described by arbitrary unique labels. As a first attempt, the graph could be seen as a state machine: for each vertex j, label its outgoing edges from 1 to k (e.g., by ordering them alphabetically). Then, to hash a k-ary string, start from an arbitrary vertex j_0. Read the symbols in the string one-by-one, advancing from the current vertex j to the next vertex j' reached by the edge corresponding to the read symbol. This process defines a pseudo-random walk in the expander graph. The hash is the label of the final vertex of the walk.

The only difference between this description and the actual CGL proposal is that they forbid *backtracking walks*. I.e., they use a $(k+1)$-regular graph instead, and only label from 1 to k the outgoing edges of the current vertex, excluding the edge the walk came from (for the first

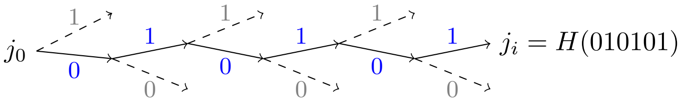


Figure 18: Hashing the string 010101 using an expander graph

step, an arbitrary forbidden edge can be chosen). This has the advantage of mixing considerably faster than backtracking walks. An example with $k = 2$ is pictured in Figure 18.

For the process to be a good pseudo-random function, the walks need to be substantially longer than the diameter of the graph. However this is not enough to guarantee a *cryptographically strong* hash function. Indeed the two main properties of cryptographic hash functions, translate in this setting as the following computational problems.

Problem 5 (Preimage resistance)**.** Given a vertex j in the graph, find a path from the start vertex j_0 to j.

Problem 6 (Collision resistance)**.** Find a non-trivial loop (i.e., one that does not track backwards) from j_0 to itself.

Charles, Goren and Lauter suggested two possible instantiations for the expander graph in the construction above. The first was based on LPS Cayley graphs, and was broken shortly after it was introduced [83, 64, 65].

The second was the supersingular 2-isogeny graph of a large prime. Although collision resistance of this proposal has been broken in many instances [29], the general problem of computing paths and cycles in a supersingular isogeny graph remains hard and is the basis of most of isogeny based cryptography. We shall come back to it in Section 23.

20 Quaternionic multiplication aka the Deuring correspondence

In Part II we could fully explain the structure of isogeny volcanoes using the theory of complex multiplication. Quaternionic multiplication, also known as the *Deuring correspondence*, will help us understand the structure of supersingular graphs.

For supersingular elliptic curves E, the full endomorphism ring is isomorphic to a maximal order $\mathcal{O}$ in $B_{p,\infty}$ (the quaternion algebra over $\mathbb{Q}$ ramified exactly at p and ∞). We find a correspondence similar to the imaginary quadratic case, in the sense that (left) ideals of $\mathcal{O}$ correspond to isogenies with domain E, and fractional (left) ideal classes of $\mathcal{O}$ correspond to isomorphism classes of elliptic curves isogenous to E. A major difference is that this no longer provides a group action on the set of all curves, since the set of fractional ideal classes no longer admits a group structure. Also, unlike in the CM case, it is very rare for supersingular curves to have isomorphic endomorphism rings.

Throughout the text, we have seen several characterizations of supersingularity, so let us recall:

Theorem 89. *Let E be a elliptic curve over a field of positive characteristic p. Then the following are equivalent:*

1. *E is supersingular.*
2. *$E[p] = \{0\}$.*

3. *The map* $[p] : E \to E$ *is purely inseparable.*

4. *The trace* t *of* π_q*, the* q*-Frobenius map, is divisible by* p*.*

5. $\mathrm{End}(E)$ *is isomorphic to a maximal order in* $B_{p,\infty}$*.*

For the rest of the section, we denote by E a supersingular curve defined over $\mathbb{F}_{p^2}$, and by $\mathrm{End}(E) = \mathcal{O} \subset B_{p,\infty}$ its endomorphism ring.

Before we dive into the exact relationship between ideals and isogenies that the Deuring correspondence provides, we need a slightly more precise relationship between isogenies and subgroups. Recall from Proposition 27 that separable isogenies with domain E correspond to finite subgroups of E (namely their kernels). The same description can be used to treat general isogenies, not only separable ones, as long as we keep track of the inseparable degree.

Definition 90 (Separable and inseparable degree)**.** The *separable degree* of an isogeny $\varphi : E \to E'$ is defined as $\deg_s(\varphi) := \#\ker(\varphi)$. The *inseparable degree* $\deg_i(\varphi)$ is defined by the equation $\deg(\varphi) = \deg_s(\varphi) \cdot \deg_i(\varphi)$.

The (in)separable degree of an isogeny equals that of the corresponding extension of function fields (see Definition 25). In particular, the inseparable degree is always a power of p. The inseparable degree of a separable isogeny is 1, and the inseparable degree of a purely inseparable isogeny is equal to its degree. The main example of a purely inseparable isogeny is the Frobenius map $E \to E^{(p)}$, $(x, y) \mapsto (x^p, y^p)$, where $E^{(p)}$ denotes the Weierstrass curve whose coefficients are all raised to the power p. In essence, any other purely inseparable isogeny is a power of the Frobenius. More precisely, we have the following lemma.

Lemma 91. *Let* $\psi : E_1 \to E_2$ *be an isogeny of elliptic curves such that* $\deg_i(\psi) = q$*. Then there exists a separable isogeny* $\lambda : E_1^{(q)} \to E_2$ *such that* $\psi = \lambda \circ \pi_q$*, where* $q : E_1 \to E_1^{(q)}$ *denotes the* q*-Frobenius.*

Proof. [76, II, Coro. 2.12] □

Where *separable* isogenies correspond to finite subgroups, arbitrary isogenies correspond to *finite subgroup schemes*. Essentially, a subgroup scheme is a generalization of a subgroup that keeps track of information about inseparability. A precise definition is outside of the scope of these notes, so for now we will use the following terminology.

Definition 92 (subgroup scheme)**.** A *subgroup scheme* is a pair (H, p^r) where $H \subset E$ is a subgroup and $r \in \mathbb{Z}_{\geq 0}$. The *rank* is defined as $\mathrm{rk}(H, p^r) := \#H \cdot p^r$. Given two such subgroup schemes, the *scheme-theoretic intersection* $(H_1, p^r) \cap (H_2, p^s)$ is defined as $(H_1 \cap H_2, p^{\min(r,s)})$. We write $(H_1, p^r) \leq (H_2, p^s)$ if $H_1 \subset H_2$ and $r \leq s$.

The *scheme-theoretic kernel* of an isogeny $\varphi : E \to E'$, denoted $E[\varphi]$, is $(\ker \varphi, \deg_i \varphi)$.

Conversely, to every finite subgroup scheme $H \leq E$ one can associate an isogeny whose scheme-theoretic kernel is H; similar to Proposition 27, the codomain E/H of this isogeny is unique up to isomorphism. The degree of this isogeny equals $\mathrm{rk}\, H$.

In terms of subgroup schemes, we have the following "factorization theorem" for isogenies.

Proposition 93. *Let* $\varphi : E_1 \to E_2$ *and* $\psi : E_1 \to E_3$ *be isogenies. If* $E[\varphi] \leq E[\psi]$ *then there exists an isogeny* $\lambda : E_2 \to E_3$ *such that* $\psi = \lambda \circ \varphi$*.*

Now we are ready to formulate the Deuring correspondence (compare to Section 12).

Definition 94. For an integral left $\mathcal{O}$-ideal I, we define

$$E[I] := \bigcap_{\alpha \in I} E[\alpha].$$

Conversely, to a subgroup scheme $H \leq E$, we associate the integral left $\mathcal{O}$-ideal

$$I(H) := \{\alpha \in \mathcal{O} \mid H \leq E[\alpha]\}.$$

To an integral left $\mathcal{O}$-ideal I, we associate the isogeny φ_I with kernel $E[I]$ (which is unique up to post-composition by an isomorphism).

Proposition 95. *We have* $\mathrm{rk}(E[I]) = N(I)$*. In other words, the isogeny* φ_I *has degree* $N(I)$*.*

Theorem 96 (Deuring Correspondence I)**.** *The maps defined above induce a bijection*

$$\begin{tikzcd} \left\{\begin{matrix}\text{subgroup schemes} \\ H \leq E\end{matrix}\right\} \arrow[r, shift left, "I(\cdot)"] & \left\{\begin{matrix}\text{integral left} \\ \mathcal{O}\text{-ideals } I \subset \mathcal{O}\end{matrix}\right\} \arrow[l, shift left, "E[\cdot]"] \end{tikzcd}$$

We say that two fractional left $\mathcal{O}$-ideals I, J are *equivalent* if there exists a $\beta \in B_{p,\infty}$ such that $I\beta = J$. In that case we also say that I, J are in the same *left ideal class.* This happens if and only if I and J are isomorphic as left $\mathcal{O}$-modules. Every fractional left $\mathcal{O}$-ideal is equivalent to an integral one.

Proposition 97. *Two integral left* $\mathrm{End}(E)$*-ideals* I, J *are equivalent if and only if* $E/E[I] \cong E/E[J]$*.*

This proposition is reminiscent of the main theorem of complex multiplication. As a consequence, we have the following "coarser" version of Theorem 96, which is what most people refer to as the Deuring correspondence.

Theorem 98 (Deuring correspondence II)**.** *The bijection in Theorem 96 induces a one-to-one correspondence*

$$\begin{tikzcd} \left\{\begin{matrix}\text{supersingular elliptic curves over } \mathbb{F}_{p^2} \\ \text{up to isomorphism}\end{matrix}\right\} \arrow[r, shift left] & \left\{\begin{matrix}\text{fractional left} \\ \mathcal{O}\text{-ideal classes}\end{matrix}\right\} \arrow[l, shift left] \end{tikzcd}$$

In summary, the same correspondences between ideals and isogenies given in Table 2 for complex multiplication also hold for the Deuring correspondence. Unlike in the CM case, left $\mathcal{O}$-ideal classes do not form a group, though at least we obtain the exact size of the left ideal class set, and thus of the supersingular isogeny class, thanks to Eichler's mass formula.

Corollary 99. *The number of isomorphism classes of supersingular elliptic curves is equal to*

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

There also exists a more precise, functorial statement of the Deuring correspondence, which we give here for completeness. The reader unfamiliar with categories can safely ignore this version.

Lemma 100. *Given an isogeny $\varphi : E_1 \to E_2$, the pullback map* $\mathrm{Hom}(E_2, E_1) \to \mathrm{End}(E_1)$, $\psi \mapsto \psi \circ \varphi$ *is an injective morphism of left* $\mathrm{End}(E_1)$*-modules. In particular, it is an isomorphism onto the image* $I(E_1[\varphi])$.

Theorem 101 (Deuring correspondence III)**.** *The contravariant functor* $\mathrm{Hom}(-, E)$ *defines an equivalence of categories*

$$\begin{tikzcd} \left\{\begin{matrix}\text{supersingular elliptic curves over } \mathbb{F}_{p^2},\\ \text{with isogenies}\end{matrix}\right\} \arrow[r, shift left] & \left\{\begin{matrix}\text{invertible left } \mathrm{End}(E)\text{-modules,}\\ \text{with nonzero homomorphisms}\end{matrix}\right\} \arrow[l, shift left] \end{tikzcd}$$

Endomorphism rings. Using the Deuring correspondence, we were able to count the number of isomorphism classes of supersingular elliptic curves. Each such supersingular elliptic curve has an endomorphism ring isomorphic to some maximal order in $B_{p,\infty}$. We saw that quadratic number fields have a unique maximal order, so it is natural to ask whether something similar happens in quaternion algebras. In other words, what is the number of isomorphism classes of *endomorphism rings* of supersingular elliptic curves?

We say two maximal orders $\mathcal{O}, \mathcal{O}' \subset B_{p,\infty}$ are *conjugate* if there exists a $\beta \in B_{p,\infty}$ such that $\mathcal{O}' = \beta\mathcal{O}\beta^{-1}$. This is equivalent to $\mathcal{O}$ and $\mathcal{O}'$ being isomorphic as rings. If I is an integral left $\mathcal{O}$-ideal, then by the Deuring correspondence we obtain an isogeny $\varphi_I : E \to E'$ with kernel $E[I]$. One can then show that $\mathcal{O}_L(I) = \mathcal{O} \cong \mathrm{End}(E)$ and $\mathcal{O}_R(I) = \mathcal{O}' \cong \mathrm{End}(E')$. Such an ideal I is called a *connecting ideal* for the orders $\mathcal{O}$ and $\mathcal{O}'$. Note that, since $\mathcal{O}_R(I\beta) = \beta^{-1}\mathcal{O}'\beta$ for every $\beta \in B_{p,\infty}$, ideals equivalent to I indeed have conjugate (hence isomorphic) right orders.

Now suppose that $\mathcal{O}$ and $\mathcal{O}'$ are isomorphic. By taking a different representative for the same fractional ideal class, we then may assume that I is such that $\mathcal{O} = \mathcal{O}'$. In other words, I is a *two-sided* $\mathcal{O}$-ideal. Just like in the imaginary quadratic case, the two-sided fractional ideals form a group, and by considering them up to equivalence, we obtain the *(two-sided) ideal class group* $\mathrm{Pic}(\mathcal{O})$ of $\mathcal{O}$. We have the following result about its structure.

Theorem 102. *There is a unique two-sided fractional $\mathcal{O}$-ideal of norm p. It generates the two-sided ideal class group* $\mathrm{Pic}(\mathcal{O})$ *of $\mathcal{O}$. As an element of this group it has order at most* 2.

Under the Deuring correspondence, this special two-sided fractional $\mathcal{O}$-ideal of norm p corresponds to the Frobenius $E \to E^{(p)}$. In particular, the group $\mathrm{Pic}(\mathcal{O})$ is trivial if and only if E is defined over $\mathbb{F}_p$, and it is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ if and only if E is not defined over $\mathbb{F}_p$ (recall that E, being supersingular, is automatically defined over $\mathbb{F}_{p^2}$). We can summarize as follows:

Theorem 103. *There is a one-to-one correspondence:*

$$\begin{tikzcd} \left\{\begin{matrix}\text{supersingular } j\text{-invariants,}\\ \text{up to the action of Frobenius}\end{matrix}\right\} \arrow[r, shift left] & \left\{\begin{matrix}\text{maximal orders } \mathcal{O} \subset B_{p,\infty},\\ \text{up to conjugacy}\end{matrix}\right\} \arrow[l, shift left] \end{tikzcd}$$

21 The effective Deuring correspondence

The correspondence between ideal classes of quadratic orders and isogenies let us efficiently evaluate the CM action and construct isogeny-based cryptographic schemes, as described in Part III. We would like to have an analogous collection of algorithms for the Deuring correspondence.

The first step is to establish an *efficient representation* of an endomorphism ring. Concretely, for a given curve E_0, we seek a basis of $\mathrm{End}(E_0)$ made of four efficiently represented endomorphisms, together with an explicit injection $\mathrm{End}(E_0) \hookrightarrow B_{p,\infty}$.

This is easier said than done: ordinary curves have an obvious endomorphism generating the endomorphism algebra, the Frobenius endomorphism, and finding a corresponding algebraic integer amounts to computing its minimal polynomial, or equivalently to counting the number of points of the curve (see Appendix B). For supersingular curves, on the other hand, it is in general difficult to find even a single endomorphism. Luckily, some curves have a natural quaternion representation.

Proposition 104. *Let $B_{p,\infty}$ be represented as in Proposition 51 and let $\mathcal{O}_0$ be the maximal order of Proposition 52. Assuming the generalized Riemann hypothesis (GRH), there exists a supersingular curve E_0 such that $\operatorname{End}(E_0) \simeq \mathcal{O}_0$ and a basis of $\operatorname{End}(E_0)$ made of efficiently represented endomorphisms.*

Proof. If $p = 2$, then E_0 is the curve $y^2 + y = x^3$ with j-invariant 0, $(1 + i + j + ij)/2$ is one of its automorphisms of order 6, i, j and k are automorphisms of order 4.

For all other cases, we follow [29, Proposition 3]. If $p \equiv 3 \bmod 4$, then E_0 is again $y^2 = x^3 + x$, with the automorphism $\iota : (x, y) \mapsto (-x, \sqrt{-1}y)$ for i and Frobenius for j (see Example 54).

For $p \equiv 5 \bmod 8$, we choose $E_0 : y^2 = x^3 + x^2 - 3x + 1$ of j-invariant 8000. This curve has a single point of order 2 defined over $\mathbb{Q}$, generating the kernel of an endomorphism of degree 2, take its reduction for i. The Frobenius endomorphism corresponds to j.

Finally, for $p \equiv 1 \bmod 8$, consider the maximal order $\mathcal{O}$ of $\mathbb{Q}(\sqrt{-r})$: because $q = 3 \mod 4$, its class number must be odd (see [61]). By hypothesis $\left(\frac{r}{p}\right) = \left(\frac{-r}{p}\right) = -1$, thus by Theorem 74 all curves over $\mathbb{C}$ with CM by $\mathcal{O}$ have supersingular reduction modulo p. Because they are odd in number at least one of these reductions must be defined over $\mathbb{F}_p$, let it be E_0. Finally, let ι be one of its endomorphisms such that $\iota^2 = -r$, then the quaternion i corresponds to ι and j corresponds to the $\mathbb{F}_p$-Frobenius endomorphism.

Assuming GRH, the smallest r satisfying the conditions of Proposition 51 is in $O(\log(p)^2)$. Then all the computations above can be done in time polylog(p), which fits within the budget of Defintion 31. □

From now on we shall call *special* a supersingular curve produced by the proposition. In practice, virtually all supersingular isogeny based cryptography uses $p = 3 \mod 4$ and sets $E_0 : y^2 = x^3 + x$. We shall thus only focus on this case in the rest of the manuscript.

Having an efficient representation of $\operatorname{End}(E_0)$ is sufficient, in principle, to efficiently represent the endomorphism ring of any other curve in the isogeny class. Indeed, from the Deuring correspondence we have the following description of $\operatorname{End}(E)$ for any curve isogenous to E_0.

Proposition 105. *Let $\phi : E_0 \to E$ be an isogeny of supersingular curves and let $\iota_0 : \operatorname{End}(E_0) \hookrightarrow \mathcal{O}_0 \subset B_{p,\infty}$ be a representation of $\operatorname{End}(E_0)$. The map*

$$\begin{aligned} \iota_\phi : \operatorname{End}(E) &\hookrightarrow B_{p,\infty} \\ \omega &\mapsto \frac{\iota_0(\hat{\phi} \circ \omega \circ \phi)}{\deg \phi} \end{aligned}$$

is injective and $\iota_\phi(\operatorname{End}(E)) = \mathcal{O}_R(I(E_0[\phi]))$.

Proof. See [86, Lemma 42.2.10]. □

Said otherwise, we have an explicit representation of $\operatorname{End}(E)$ as a subring of $B_{p,\infty}$ as soon as we have an isogeny $\phi : E_0 \to E$, but is it an efficient representation? Suppose we have a quaternion $\alpha \in B_{p,\infty}$ representing an endomorphism of E, and let $d = \deg \phi$. Applying the isomorphism backwards we know there exists $\omega_0 \in \operatorname{End}(E_0)$ such that $\iota_0(\omega_0) = d\beta$; then,

$$\iota_0^{-1}(d\beta) = \omega_0 = \hat{\phi} \circ \omega \circ \phi$$

and

$$d^2\omega = \phi \circ \omega_0 \circ \hat{\phi},$$

and every $\omega \in \mathrm{End}(E)$ can be written this way. Suppose we want to evaluate ω at a point $P \in E$, we can compute Q such that $[d^2]Q = P$, then

$$\phi\omega_0\hat{\phi}(Q) = d^2\omega(Q) = \omega(P).$$

Thus we have an efficient representation of ω as long as:

1. ϕ is efficiently represented,
2. we can efficiently "divide by d^2".

Let us start from the case where d is "small", then Vélu's formulas provide an efficient representation of ϕ. Moreover, if $P \in E(\mathbb{F}_q)$, a point Q such that $[d^2]Q = P$ is defined in an extension of $\mathbb{F}_q$ of degree less than d^4 (see Appendix B and in particular Definition 107). Hence, we have an efficient representation of ω whenever $d \in \mathrm{polylog}(p)$.

We easily extend this to the case where d is *powersmooth*, i.e. where $d = \prod_{i=1}^{n} \ell_i^{e_i}$ with the ℓ_i coprime and $n, \ell_i^{e_i} \in \mathrm{polylog}(p)$. Indeed, by Corollary 28, ϕ can be efficiently represented as a composition of isogenies of degree ℓ_i. Dividing by d^2 is trickier: for each i we can efficiently compute Q_i such that $[\ell_i^{2e_i}]Q_i = P$, implying that $Q = \sum_i Q_i$ satisfies $[d^2]Q = P$. Then we evaluate $\phi\omega_0\hat{\phi}(Q)$ as

$$\phi\omega_0\hat{\phi}(Q) = \phi\omega_0\hat{\phi}\left(\sum_i Q_i\right) = \sum_i \phi\omega_0\hat{\phi}(Q_i),$$

involving only computations in extensions of $\mathbb{F}_q$ of degree less than $\ell_i^{4e_i}$ and a final chain of point additions over $\mathbb{F}_q$.

In summary, whenever we know an isogeny $\phi : E_0 \to E$ of powersmooth degree, we have an efficient representation of $\mathrm{End}(E)$. Knowledge of endomorphism rings is contagious! We can prove that such an isogeny always exists.

Proposition 106. *Let E_0 be a special curve as defined by Proposition 104, let E be an arbitrary curve in the same isogeny class, then, assuming GRH, there exists an isogeny $\phi : E_0 \to E$ of degree* $\mathrm{polylog}(p)$*-powersmooth.*

Proof. Thanks to the Deuring correspondence, after fixing an appropriate smoothness bound $B \in \mathrm{polylog}(p)$, it suffices to prove that any ideal class of $\mathcal{O}_0$ contains an ideal of B-powersmooth norm. See [89] for details. □

Even though $\phi : E_0 \to E$ always exists, it is not necessarily easy to compute. We will come back to the problem of computing isogenies of supersingular curves and its relationship to computing their endomorphsim rings in Section 23.

22 Signatures based on the Deuring correspondence

TODO: this section will cover the signature schemes GPS [37] and SQISign [26] (see also https://sqisign.org/).

23 Security of supersingular isogeny problems

TODO: this section will cover the security reductions between hard problems in supersingular isogeny cryptography [88] and in particular the equivalence between the isogeny path problem and the endormorphism ring problem [89].

References

[1] Navid Alamati, Luca De Feo, Hart Montgomery, and Sikhar Patranabis. Cryptographic group actions and applications. In Shiho Moriai and Huaxiong Wang, editors, *ASIACRYPT 2020, Part II*, volume 12492 of *LNCS*, pages 411–439. Springer, Heidelberg, December 2020. doi:10.1007/978-3-030-64834-3_14.

[2] Arthur O. L. Atkin. The number of points on an elliptic curve modulo a prime. Manuscript, Chicago IL, 1991. URL: http://www.lix.polytechnique.fr/Labo/Francois.Morain/AtkinEmails/19910614.txt.

[3] Daniel J Bernstein, Luca De Feo, Antonin Leroux, and Benjamin Smith. Faster computation of isogenies of large prime degree. *Open Book Series*, 4(1):39–55, 2020. doi:10.2140/obs.2020.4.39.

[4] Daniel J. Bernstein, Tanja Lange, Chloe Martindale, and Lorenz Panny. Quantum circuits for the CSIDH: Optimizing quantum evaluation of isogenies. In Yuval Ishai and Vincent Rijmen, editors, *EUROCRYPT 2019, Part II*, volume 11477 of *LNCS*, pages 409–441. Springer, Heidelberg, May 2019. doi:10.1007/978-3-030-17656-3_15.

[5] Ward Beullens, Luca De Feo, Steven D. Galbraith, and Christophe Petit. Proving knowledge of isogenies: a survey. *Designs, Codes and Cryptography*, 91(11):3425–3456, Jun 2023. doi:10.1007/s10623-023-01243-3.

[6] Ward Beullens, Thorsten Kleinjung, and Frederik Vercauteren. CSI-FiSh: Efficient isogeny based signatures through class group computations. In Steven D. Galbraith and Shiho Moriai, editors, *ASIACRYPT 2019, Part I*, volume 11921 of *LNCS*, pages 227–247. Springer, Heidelberg, December 2019. doi:10.1007/978-3-030-34578-5_9.

[7] Jean-François Biasse, Annamaria Iezzi, and Michael J. Jr. Jacobson. A note on the security of CSIDH. In Debrup Chakraborty and Tetsu Iwata, editors, *Progress in Cryptology – INDOCRYPT 2018*, pages 153–168, Cham, 2018. Springer International Publishing. doi:10.1007/978-3-030-05378-9_9.

[8] Xavier Bonnetain and André Schrottenloher. Quantum security analysis of CSIDH. In Anne Canteaut and Yuval Ishai, editors, *EUROCRYPT 2020, Part II*, volume 12106 of *LNCS*, pages 493–522. Springer, Heidelberg, May 2020. doi:10.1007/978-3-030-45724-2_17.

[9] Gilles Brassard and Moti Yung. One-way group actions. In Alfred J. Menezes and Scott A. Vanstone, editors, *CRYPTO'90*, volume 537 of *LNCS*, pages 94–107. Springer, Heidelberg, August 1991. doi:10.1007/3-540-38424-3_7.

[10] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: An efficient post-quantum commutative group action. In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part III*, volume 11274 of *LNCS*, pages 395–427. Springer, Heidelberg, December 2018. doi:10.1007/978-3-030-03332-3_15.

[11] Denis Xavier Charles, Kristin E. Lauter, and Eyal Z. Goren. Cryptographic hash functions from expander graphs. *Journal of Cryptology*, 22(1):93–113, January 2009. doi:10.1007/s00145-007-9002-x.

[12] Andrew Childs, David Jao, and Vladimir Soukharev. Constructing elliptic curve isogenies in quantum subexponential time. *Journal of Mathematical Cryptology*, 8(1):1–29, 2014. doi:10.1515/jmc-2012-0016.

[13] Fan R.K. Chung. Diameters and eigenvalues. *Journal of the American Mathematical Society*, 2(2):187–196, 1989.

[14] Jorge Chávez-Saab, Jesús-Javier Chi-Domínguez, Samuel Jaques, and Francisco Rodríguez-Henríquez. The SQALE of CSIDH: square-root Vélu quantum-resistant isogeny action with low exponents. Cryptology ePrint Archive, Report 2020/1520, 2020. URL: https://eprint.iacr.org/2020/1520.

[15] Leonardo Colò and David Kohel. Orienting supersingular isogeny graphs. *Journal of Mathematical Cryptology*, 14(1):414–437, 2020. doi:10.1515/jmc-2019-0034.

[16] Anamaria Costache, Brooke Feigon, Kristin Lauter, Maike Massierer, and Anna Puskas. Ramanujan graphs in cryptography. Cryptology ePrint Archive, Report 2018/593, 2018. https://eprint.iacr.org/2018/593.

[17] Craig Costello and Hüseyin Hisil. A simple and compact algorithm for SIDH with arbitrary degree isogenies. In Tsuyoshi Takagi and Thomas Peyrin, editors, *ASIACRYPT 2017, Part II*, volume 10625 of *LNCS*, pages 303–329. Springer, Heidelberg, December 2017. doi:10.1007/978-3-319-70697-9_11.

[18] Jean-Marc Couveignes. Hard homogeneous spaces. Cryptology ePrint Archive, Report 2006/291, 2006. https://eprint.iacr.org/2006/291.

[19] Jean-Marc Couveignes and Reynald Lercier. Fast construction of irreducible polynomials over finite fields. *Israel Journal of Mathematics*, 194(1):77–105, 2013.

[20] Luca De Feo. *Algorithmes Rapides pour les Tours de Corps Finis et les Isogénies*. PhD thesis, Ecole Polytechnique X, December 2010. URL: http://tel.archives-ouvertes.fr/tel-00547034/en/.

[21] Luca De Feo. Mathematics of isogeny based cryptography, 2017. URL: http://arxiv.org/abs/1711.04062, arXiv:1711.04062.

[22] Luca De Feo, Javad Doliskani, and Éric Schost. Fast algorithms for ℓ-adic towers over finite fields. In *Proceedings of the 38th International Symposium on Symbolic and Algebraic Computation*, ISSAC '13, pages 165–172, New York, NY, USA, 2013. ACM. doi:10.1145/2465506.2465956.

[23] Luca De Feo, Tako Boris Fouotsa, Péter Kutas, Antonin Leroux, Simon-Philipp Merz, Lorenz Panny, and Benjamin Wesolowski. SCALLOP: Scaling the CSI-FiSh. In Alexandra Boldyreva and Vladimir Kolesnikov, editors, *PKC 2023, Part I*, volume 13940 of *LNCS*, pages 345–375. Springer, Heidelberg, May 2023. doi:10.1007/978-3-031-31368-4_13.

[24] Luca De Feo and Steven D. Galbraith. SeaSign: Compact isogeny signatures from class group actions. In Yuval Ishai and Vincent Rijmen, editors, *EUROCRYPT 2019, Part III*, volume 11478 of *LNCS*, pages 759–789. Springer, Heidelberg, May 2019. doi:10.1007/978-3-030-17659-4_26.

[25] Luca De Feo, Jean Kieffer, and Benjamin Smith. Towards practical key exchange from ordinary isogeny graphs. In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part III*, volume 11274 of *LNCS*, pages 365–394. Springer, Heidelberg, December 2018. doi:10.1007/978-3-030-03332-3_14.

[26] Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski. SQISign: Compact post-quantum signatures from quaternions and isogenies. In Shiho Moriai and Huaxiong Wang, editors, *ASIACRYPT 2020, Part I*, volume 12491 of *LNCS*, pages 64–93. Springer, Heidelberg, December 2020. doi:10.1007/978-3-030-64837-4_3.

[27] Christina Delfs and Steven D. Galbraith. Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$. *Designs, Codes and Cryptography*, 78(2):425–440, February 2016. doi:10.1007/s10623-014-0010-1.

[28] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976. doi:10.1109/TIT.1976.1055638.

[29] Kirsten Eisenträger, Sean Hallgren, Kristin E. Lauter, Travis Morrison, and Christophe Petit. Supersingular isogeny graphs and endomorphism rings: Reductions and solutions. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part III*, volume 10822 of *LNCS*, pages 329–368. Springer, Heidelberg, April / May 2018. doi:10.1007/978-3-319-78372-7_11.

[30] Noam D. Elkies. Explicit isogenies. 1992.

[31] Noam D. Elkies. Elliptic and modular curves over finite fields and related computational issues. In *Computational perspectives on number theory (Chicago, IL, 1995)*, volume 7 of *Studies in Advanced Mathematics*, pages 21–76, Providence, RI, 1998. AMS International Press. URL: http://www.ams.org/mathscinet-getitem?mr=1486831.

[32] Mireille Fouquet and François Morain. Isogeny volcanoes and the SEA algorithm. In Claus Fieker and David R. Kohel, editors, *Algorithmic Number Theory Symposium*, volume 2369 of *Lecture Notes in Computer Science*, pages 47–62, Berlin, Heidelberg, 2002. Springer Berlin / Heidelberg. doi:10.1007/3-540-45455-1_23.

[33] Steven D. Galbraith. *Mathematics of public key cryptography*. Cambridge University Press, 2012. https://www.math.auckland.ac.nz/~sgal018/crypto-book/crypto-book.html.

[34] Steven D. Galbraith, Florian Hess, and Nigel P. Smart. Extending the GHS Weil descent attack. In Lars R. Knudsen, editor, *EUROCRYPT 2002*, volume 2332 of *LNCS*, pages 29–44. Springer, Heidelberg, April / May 2002. doi:10.1007/3-540-46035-7_3.

[35] Steven D. Galbraith, Florian Hess, and Nigel P. Smart. Extending the GHS Weil descent attack. In *Advances in cryptology–EUROCRYPT 2002 (Amsterdam)*, volume 2332 of *Lecture Notes in Computer Science*, pages 29–44. Springer, Berlin, 2002.

[36] Steven D. Galbraith, Kenneth G. Paterson, and Nigel P. Smart. Pairings for cryptographers. *Discrete Applied Mathematics*, 156(16):3113–3121, sep 2008. doi:10.1016/j.dam.2007.12.010.

[37] Steven D. Galbraith, Christophe Petit, and Javier Silva. Identification protocols and signature schemes based on supersingular isogeny problems. *Journal of Cryptology*, 33(1):130–175, January 2020. doi:10.1007/s00145-019-09316-0.

[38] Steven D. Galbraith and Anton Stolbunov. Improved algorithm for the isogeny problem for ordinary elliptic curves. *Applicable Algebra in Engineering, Communication and Computing*, 24(2):107–131, June 2013. doi:10.1007/s00200-013-0185-0.

[39] Oded Goldreich. *Basic Facts about Expander Graphs*, pages 451–464. Springer Berlin Heidelberg, Berlin, Heidelberg, 2011. doi:10.1007/978-3-642-22670-0_30.

[40] David Jao, Jason LeGrow, Christopher Leonardi, and Luis Ruiz-Lopez. A subexponential-time, polynomial quantum space algorithm for inverting the CM group action. *Journal of Mathematical Cryptology*, 14(1):129–138, 2020. doi:10.1515/jmc-2015-0057.

[41] David Jao, Stephen D. Miller, and Ramarathnam Venkatesan. Expander graphs based on GRH with an application to elliptic curve cryptography. *Journal of Number Theory*, 129(6):1491–1504, June 2009. doi:10.1016/j.jnt.2008.11.006.

[42] David Jao and Vladimir Soukharev. A subexponential algorithm for evaluating large degree isogenies. In *ANTS IX: Proceedings of the Algorithmic Number Theory 9th International Symposium*, volume 6197 of *Lecture Notes in Computer Science*, pages 219–233, Berlin, Heidelberg, 2010. Springer. doi:10.1007/978-3-642-14518-6_19.

[43] Antoine Joux. *Algorithmic cryptanalysis*. CRC Press, 2009.

[44] Alexey Yuri Kitaev. Quantum measurements and the abelian stabilizer problem. *arXiv preprint quant-ph/9511026*, 1995. URL: https://arxiv.org/abs/quant-ph/9511026.

[45] Neal Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, 48(177):203–209, 1987. URL: http://www.jstor.org/stable/2007884.

[46] Neal Koblitz. Hyperelliptic cryptosystems. *Journal of Cryptology*, 1(3):139–150, October 1989. doi:10.1007/BF02252872.

[47] David Kohel. *Endomorphism rings of elliptic curves over finite fields*. PhD thesis, University of California at Berkley, 1996. URL: http://iml.univ-mrs.fr/~kohel/pub/thesis.pdf.

[48] David R. Kohel, Kristin Lauter, Christophe Petit, and Jean-Pierre Tignol. On the quaternion-isogeny path problem. *LMS Journal of Computation and Mathematics*, 17(A):418–432, 2014.

[49] Greg Kuperberg. A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. *SIAM Journal of Computing*, 35(1):170–188, 2005. doi:10.1137/S0097539703436345.

[50] Greg Kuperberg. Another Subexponential-time Quantum Algorithm for the Dihedral Hidden Subgroup Problem. In Simone Severini and Fernando Brandao, editors, *8th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2013)*, volume 22 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 20–34, Dagstuhl, Germany, 2013. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. doi:10.4230/LIPIcs.TQC.2013.20.

[51] T. Y. Lam. *Introduction to quadratic forms over fields*, volume 67 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2005.

[52] Serge Lang. *Elliptic Functions*, volume 112 of *Graduate texts in mathematics*. Springer, 1987.

[53] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, 1994. doi:10.1007/978-1-4612-0853-2.

[54] Hendrik W. Lenstra. Factoring integers with elliptic curves. *Annals of Mathematics*, 126:649–673, 1987.

[55] Reynald Lercier. *Algorithmique des courbes elliptiques dans les corps finis.* PhD thesis, LIX - CNRS, June 1997.

[56] Alexander Lubotzky. *Discrete groups, expanding graphs and invariant measures*, volume 125 of *Progress in Mathematics*. Birkhäuser Verlag, Basel, 1994. doi:10.1007/978-3-0346-0332-4.

[57] Alexander Lubotzky, Ralph Phillips, and Peter Sarnak. Ramanujan graphs. *Combinatorica*, 8(3), 1988. doi:10.1007/BF02126799.

[58] Jean-François Mestre. La méthode des graphes. Exemples et applications. In *Proceedings of the international conference on class numbers and fundamental units of algebraic number fields (Katata, 1986)*, Nagoya, 1986. Nagoya University. URL: https://wstein.org/msri06/refs/mestre-method-of-graphs/mestre-fr.pdf.

[59] Victor S. Miller. Use of elliptic curves in cryptography. In Hugh C. Williams, editor, *CRYPTO'85*, volume 218 of *LNCS*, pages 417–426. Springer, Heidelberg, August 1986. doi:10.1007/3-540-39799-X_31.

[60] Dustin Moody and Daniel Shumow. Analogues of Vélu's formulas for isogenies on alternate models of elliptic curves. *Mathematics of Computation*, 85(300):1929–1951, 2016. doi:10.1090/mcom/3036.

[61] Louis J. Mordell. Mathematical notes: The congruence $(p-1/2)! \equiv \pm 1 \mod p$. *The American Mathematical Monthly*, 68(2):131–149, Feb 1961. doi:10.1080/00029890.1961.11989636.

[62] Jürgen Neukirch. *Algebraic number theory*, volume 322. Springer Verlag, 1999. doi:10.1007/978-3-662-03983-0.

[63] Chris Peikert. He gives C-sieves on the CSIDH. In Anne Canteaut and Yuval Ishai, editors, *EUROCRYPT 2020, Part II*, volume 12106 of *LNCS*, pages 463–492. Springer, Heidelberg, May 2020. doi:10.1007/978-3-030-45724-2_16.

[64] Christophe Petit, Kristin Lauter, and Jean-Jacques Quisquater. Full cryptanalysis of LPS and Morgenstern hash functions. In Rafail Ostrovsky, Roberto De Prisco, and Ivan Visconti, editors, *SCN 08*, volume 5229 of *LNCS*, pages 263–277. Springer, Heidelberg, September 2008. doi:10.1007/978-3-540-85855-3_18.

[65] Christophe Petit and Jean-Jacques Quisquater. Preimages for the Tillich-Zémor hash function. In Alex Biryukov, Guang Gong, and Douglas R. Stinson, editors, *SAC 2010*, volume 6544 of *LNCS*, pages 282–301. Springer, Heidelberg, August 2011. doi:10.1007/978-3-642-19574-7_20.

[66] Arnold Pizer. An algorithm for computing modular forms on $\gamma_0(n)$. *Journal of Algebra*, 64(2):340–390, Jun 1980. doi:10.1016/0021-8693(80)90151-9.

[67] Arnold K. Pizer. Ramanujan graphs and Hecke operators. *Bulletin of the American Mathematical Society (N.S.)*, 23(1), 1990. doi:10.1090/S0273-0979-1990-15918-X.

[68] Arnold K. Pizer. Ramanujan graphs. In *Computational perspectives on number theory (Chicago, IL, 1995)*, volume 7 of *AMS/IP Stud. Adv. Math.* Amer. Math. Soc., Providence, RI, 1998.

[69] Oded Regev. A subexponential time algorithm for the dihedral hidden subgroup problem with polynomial space. arXiv:quant-ph/0406151, June 2004. URL: http://arxiv.org/abs/quant-ph/0406151.

[70] Joost Renes. Computing isogenies between Montgomery curves using the action of (0, 0). In Tanja Lange and Rainer Steinwandt, editors, *Post-Quantum Cryptography - 9th International Conference, PQCrypto 2018*, pages 229–247. Springer, Heidelberg, 2018. doi:10.1007/978-3-319-79063-3_11.

[71] Alexander Rostovtsev and Anton Stolbunov. Public-Key Cryptosystem Based On Isogenies. Cryptology ePrint Archive, Report 2006/145, 2006. https://eprint.iacr.org/2006/145.

[72] René Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Mathematics of Computation*, 44(170):483–494, 1985. doi:10.2307/2007968.

[73] René Schoof. Counting points on elliptic curves over finite fields. *Journal de Théorie des Nombres de Bordeaux*, 7(1):219–254, 1995. URL: http://www.ams.org/mathscinet-getitem?mr=1413578.

[74] Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *35th FOCS*, pages 124–134. IEEE Computer Society Press, November 1994. doi:10.1109/SFCS.1994.365700.

[75] Victor Shoup. Lower bounds for discrete logarithms and related problems. In Walter Fumy, editor, *EUROCRYPT'97*, volume 1233 of *LNCS*, pages 256–266. Springer, Heidelberg, May 1997. doi:10.1007/3-540-69053-0_18.

[76] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992.

[77] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, volume 151 of *Graduate Texts in Mathematics*. Springer, January 1994. URL: http://www.amazon.com/exec/obidos/redirect?tag=citeulike07-20&path=ASIN/0387943285.

[78] Anton Stolbunov. Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves. *Advances in Mathematics of Communications*, 4(2):215–235, 2010. doi:10.3934/amc.2010.4.215.

[79] Anton Stolbunov. Cryptographic schemes based on isogenies, 2012.

[80] Andrew Sutherland. Lecture notes on elliptic curves, 2017. URL: https://math.mit.edu/classes/18.783/2017/lectures.html.

[81] Andrew V. Sutherland. Genus 1 point counting over prime fields. Last accessed July 16, 2010. http://www-math.mit.edu/~drew/SEArecords.html, 2010. URL: #.

[82] Terence Tao. Expansion in groups of Lie type – basic theory of expander graphs, 2011. URL: https://terrytao.wordpress.com/2011/12/02/245b-notes-1-basic-theory-of-expander-graphs/.

[83] Jean-Pierre Tillich and Gilles Zémor. Collisions for the LPS expander graph hash function. In Nigel P. Smart, editor, *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 254–269. Springer, Heidelberg, April 2008. doi:10.1007/978-3-540-78967-3_15.

[84] Luca Trevisan. Lecture notes on graph partitioning, expanders and spectral methods, 2017. URL: https://lucatrevisan.github.io/books/expanders-2016.pdf.

[85] Jacques Vélu. Isogénies entre courbes elliptiques. *Comptes Rendus de l'Académie des Sciences de Paris*, 273:238–241, July 1971. URL: https://gallica.bnf.fr/ark:/12148/bpt6k56191248/f52.item.

[86] John Voight. Quaternion algebras, 2018. URL: https://math.dartmouth.edu/~jvoight/quat-book.pdf.

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

[88] Benjamin Wesolowski. Orientations and the supersingular endomorphism ring problem. In Orr Dunkelman and Stefan Dziembowski, editors, *EUROCRYPT 2022, Part III*, volume 13277 of *LNCS*, pages 345–371. Springer, Heidelberg, May / June 2022. doi:10.1007/978-3-031-07082-2_13.

[89] Benjamin Wesolowski. The supersingular isogeny path and endomorphism ring problems are equivalent. In *62nd FOCS*, pages 1100–1111. IEEE Computer Society Press, February 2022. doi:10.1109/FOCS52979.2021.00109.

Part V
Other applications

This material used to be part of the first version of these lecture notes, but we decided to discard it from the main body to focus on the more central topics.

We keep it in this appendix for historical reference, however we do not guarantee its coherence with the main material.

A Application: Elliptic curve factoring method

A second popular use of elliptic curves in technology is for factoring large integers, a problem that also occurs frequently in cryptography.

The earliest method for factoring integers was already known to the ancient Greeks: the *sieve of Eratosthenes* finds all primes up to a given bound by crossing composite numbers out in a table. Applying the Eratosthenes' sieve up to $\sqrt{N}$ finds all prime factors of a composite number N. Examples of modern algorithms used for factoring are Pollard's *Rho algorithm* and Coppersmith's *Number Field Sieve (NFS)*.

In the 1980s H. Lenstra [54] introduced an algorithm for factoring that has become known as the *Elliptic Curve Method (ECM)*. Its complexity is between Pollard's and Coppersmith's algorithms in terms of number of operations; at the same time it only requires a constant amount of memory, and is very easy to parallelize. For these reasons, ECM is typically used to factor integers having medium sized prime factors.

From now on we suppose that $N = pq$ is an integer which factorization we wish to compute, where p and q are distinct primes. Without loss of generality, we can suppose that $p < q$.

Lenstra's idea has its roots in an earlier method for factoring special integers, also due to Pollard. Pollard's $(p - 1)$ *factoring method* is especially suited for integers $N = pq$ such that $p - 1$ only has *small* prime factors. It is based on the isomorphism

$$\begin{aligned} \rho : \mathbb{Z}/N\mathbb{Z} &\to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}, \\ x &\mapsto (x \bmod p, x \bmod q) \end{aligned}$$

given by the Chinese remainder theorem. The algorithm is detailed in Figure 19a. It works by guessing a multiple e of $p-1$, then taking a random element $x \in (\mathbb{Z}/N\mathbb{Z})^\times$, to deduce a random element y in $\langle 1 \rangle \oplus (\mathbb{Z}/q\mathbb{Z})^\times$. If the guessed exponent e was correct, and if $y \neq 1$, the gcd of $y - 1$ with N yields a non-trivial factor.

The $p - 1$ method is very effective when the bound B is small, but its complexity grows exponentially with B. For this reason it is only usable when $p - 1$ has small prime factors, a constraint that is very unlikely to be satisfied by random primes.

Lenstra's ECM algorithm is a straightforward generalization of the $p - 1$ method, where the multiplicative groups $(\mathbb{Z}/p\mathbb{Z})^\times$ and $(\mathbb{Z}/q\mathbb{Z})^\times$ are replaced by the groups of points $E(\mathbb{F}_p)$ and $E(\mathbb{F}_q)$ of an elliptic curve defined over $\mathbb{Q}$. Now, the requirement is that $\#E(\mathbb{F}_p)$ only has small prime factors. This condition is also extremely rare, but now we have the freedom to try the method many times by changing the elliptic curve.

The algorithm is summarized in Figure 19b. It features two remarkable subtleties. First, it would feel natural to pick a random elliptic curve $E : y^2 = x^3 + ax + b$ by picking random a and b, however taking a point on such curve would then require computing a square root modulo N, a problem that is known to be has hard as factoring N. For this reason, the algorithm starts by taking a random point, and then deduces the equation of E from it. Secondly, all computations

```
Input: An integer $N = pq$,
    a bound $B$ on the largest prime factor of $p - 1$;
Output: $(p, q)$ or FAIL.
Set $e = \prod_{r \text{ prime } < B} r^{\lfloor \log_r \sqrt{N} \rfloor}$;
Pick a random $1 < x < N$;
Compute $y = x^e \mod N$;
Compute $q' = \gcd(y - 1, N)$;
if $q' \neq 1, N$ then
    return $N/q', q'$;
else
    return FAIL.
end if
```

(a) Pollard's $(p - 1)$ algorithm

```
Input: An integer $N = pq$, a bound $B$;
Output: $(p, q)$ or FAIL.
Pick random integers $a, X, Y$ in $[0, N[$;
Compute $b = Y^2 - X^3 - aX \mod N$;
Define the elliptic curve $E : y^2 = x^3 - ax - b$.
Define the point $P = (X : Y : 1) \in E(\mathbb{Z}/N\mathbb{Z})$.
Set $e = \prod_{r \text{ prime } < B} r^{\lfloor \log_r \sqrt{N} \rfloor}$;
Compute $Q = [e]P = (X' : Y' : Z')$;
Compute $q' = \gcd(Z', N)$;
if $q' \neq 1, N$ then
    return $N/q', q'$;
else
    return FAIL.
end if
```

(b) Lenstra's ECM algorithm

Figure 19: The $(p - 1)$ and ECM factorization algorithms

on coordinates happen in the projective plane over $\mathbb{Z}/N\mathbb{Z}$; however, properly speaking, projective space cannot be defined over non-integral rings. Implicitly, $E(\mathbb{Z}/N\mathbb{Z})$ is defined as the product group $E(\mathbb{F}_p) \oplus E(F_q)$, and any attempt at inverting a non-invertible in $\mathbb{Z}/N\mathbb{Z}$ will result in a factorization of N.

B Application: point counting

Before going more in depth into the study of the endomorphism ring, let us pause for a while on a simpler problem. Hasse's theorem relates the cardinality of a curve defined over a finite field with the trace of its Frobenius endomorphism. However, it does not give us an algorithm to compute either.

The first efficient algorithm to compute the trace of π was proposed by Schoof in the 1980s [72]. The idea is very simple: compute the value of $t_\pi \bmod \ell$ for many small primes ℓ, and then reconstruct the trace using the Chinese remainder theorem. To compute $t_\pi \bmod \ell$, Schoof's algorithm formally constructs the group $E[\ell]$, takes a generic point $P \in E[\ell]$, and then runs a search for the integer t such that

$$\pi([t]P) = [q]P + \pi^2(P).$$

The formal computation must be carried out by computing modulo a polynomial that vanishes on the whole $E[\ell]$; the smallest such polynomial is provided by the *division polynomial* ψ_ℓ.

Definition 107 (Division polynomial)**.** Let $E : y^2 = x^3 + ax + b$ be an elliptic curve, the *division polynomials* ψ_m are defined by the initial values

$$\begin{aligned}
\psi_1 &= 1,\\
\psi_2 &= 2y,\\
\psi_3 &= 3x^4 + 6ax^2 + 12bx - a^2,\\
\psi_4 &= (2x^6 + 10ax^4 + 40bx^3 - 10a^2x^2 - 8abx - 2a^3 - 16b^2)2y,
\end{aligned}$$

and by the recurrence

$$\begin{aligned}
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 && \text{for } m \geq 2,\\
\psi_2\psi_{2m} &= (\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)\psi_m && \text{for } m \geq 3.
\end{aligned}$$

The m-th division polynomial ψ_m vanishes on $E[m]$; the multiplication-by-m map can be written as

$$[m]P = \left(\frac{\phi_m(P)}{\psi_m(P)^2}, \frac{\omega_m(P)}{\psi_m(P)^3}\right)$$

for any point $P \neq \mathcal{O}$, where ϕ_m and ω_m are defined as

$$\begin{aligned}
\phi_m &= x\psi_m^2 - \psi_{m+1}\psi_{m-1},\\
\omega_m &= \psi_{m-1}^2\psi_{m+2} + \psi_{m-2}\psi_{m+1}^2.
\end{aligned}$$

Schoof's algorithm runs in time polynomial in $\log \#E(k)$, however it is quite slow in practice. Among the major advances that have enabled the use of elliptic curves in cryptography are the optimizations of Schoof's algorithm due to Atkin and Elkies [2, 30, 73, 31]. Both improvements use a better understanding of the action of π on $E[\ell]$. Assume that ℓ is different from the characteristic, we have already seen that $E[\ell]$ is a group of rank two. Hence, π acts on $E[\ell]$ like a matrix M in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, and its characteristic polynomial is exactly

$$\chi(X) = X^2 - t_\pi X + q \mod \ell.$$

Now we have three possibilities:

- χ splits modulo ℓ, as $\chi(X) = (X-\lambda)(X-\mu)$, with $\lambda \neq \mu$; we call this the *Elkies case*.
- χ does not split modulo ℓ; we call this the *Atkin case*;
- χ is a square modulo ℓ.

The SEA algorithm, treats each of these cases in a slightly different way; for simplicity, we will only sketch the Elkies case. In this case, there exists a basis $\langle P, Q\rangle$ for $E[\ell]$ onto which π acts as a matrix $M = \left(\begin{smallmatrix}\lambda & 0\\ 0 & \mu\end{smallmatrix}\right)$. Each of the two eigenspaces of M is the kernel of an isogeny of degree ℓ from E to another curve E'. If we can determine the curve corresponding to, e.g., $\langle P\rangle$, then we can compute the isogeny $\phi : E \to E/\langle P\rangle$, and use it to formally represent the point P. Then, λ is recovered by solving the equation

$$[\lambda]P = \pi(P),$$

and from it we recover $t_\pi = \lambda + q/\lambda \mod \ell$.

Elkies' method is very similar to Schoof's original way of computing t_π, however it is considerably more efficient thanks to the degree of the extension rings involved. Indeed, in Schoof's algorithm a generic point of $E[\ell]$ is represented modulo the division polynomial ψ_ℓ, which has degree $(\ell^2-1)/2$. In Elkies' algorithm, instead, the formal representation of $\langle P\rangle$ only requires working modulo a polynomial of degree $\approx \ell$.

The other cases have similar complexity gains. For a more detailed overview, we address the reader to [73, 55, 31, 81].

C Application: computing irreducible polynomials

In the applications seen in the first part, we have followed an old *mantra*: whenever an algorithm relies solely on the properties of the multiplicative group $\mathbb{F}_q^*$, it can be generalized by replacing $\mathbb{F}_q^*$ with the group of points of an elliptic curve over $\mathbb{F}_q$ (or, eventually, a higher dimensional Abelian variety). Typically, the generalization adds some complexity to the computation, but comes with the advantage of having more freedom in the choice of the group size and structure. We now present another instance of the same *mantra*, that is particularly remarkable in our opinion: to the best of our knowledge, it is the first algorithm where replacing $\mathbb{F}_q^*$ with $E(\mathbb{F}_q)$ required some non-trivial work with isogenies.

Constructing irreducible polynomials of arbitrary degree over a finite field $\mathbb{F}_q$ is a classical problem. A classical solution consists in picking polynomials at random, and applying an irreducibility test, until an irreducible one is found. This solution is not satisfactory for at least two reasons: it is not deterministic, and has average complexity quadratic both in the degree of the polynomial and in $\log q$.

For a few special cases, we have well known irreducible polynomials. For example, when d divides $q-1$, there exist $\alpha \in \mathbb{F}_q$ such that $X^d - \alpha$ is irreducible. Such an α can be computed using Hilbert's theorem 90, or –more pragmatically, and assuming that the factorization of $q-1$ is known– by taking a random element and testing that it has no d-th root in $\mathbb{F}_q$. It is evident that this algorithm relies on the fact that the multiplicative group $\mathbb{F}_q^*$ is cyclic of order $q-1$.

At this point our *mantra* suggests that we replace α with a point $P \in E(\mathbb{F}_q)$ that has no ℓ-divisor in $E(\mathbb{F}_q)$, for some well chosen curve E. The obvious advantage is that we now require $\ell | \#E(\mathbb{F}_q)$, thus we are no longer limited to $\ell | (q-1)$; however, what irreducible polynomial shall we take? Intuition would suggest that we take the polynomial defining the ℓ-divisors of P; however we know that the map $[\ell]$ has degree ℓ^2, thus the resulting polynomial would have degree too large, and it would not even be irreducible.

This idea was first developed by Couveignes and Lercier [19] and then slightly generalized in [22]. Their answer to the question is to decompose the map $[\ell]$ as a composition of isogenies $\hat{\phi} \circ \phi$, and then take the (irreducible) polynomial vanishing on the fiber $\phi^{-1}(P)$.

More precisely, let $\mathbb{F}_q$ be a finite field, and let $\ell \nmid (q-1)$ be odd and such that $\ell \ll q+1+2\sqrt{q}$. Then there exists a curve E which cardinality $\#E(\mathbb{F}_q)$ is divisible by ℓ. The hypothesis $\ell \nmid (q-1)$ guarantees that $G = E[\ell] \cap E(\mathbb{F}_q)$ is cyclic (see Exercise II.5). Let ϕ be the degree ℓ isogeny of kernel G, and let E' be its image curve. Let P be a point in $E'(\mathbb{F}_q) \setminus [\ell]E'(\mathbb{F}_q)$, Couveignes and Lercier show that $\phi^{-1}(P)$ is an *irreducible fiber*, i.e., that the polynomial

$$f(X) = \prod_{Q \in \phi^{-1}(P)} (X - x(Q))$$

is irreducible over $\mathbb{F}_q$.

To effectively compute the polynomial f, we need one last technical ingredient: a way to compute a representation of the isogeny ϕ as a rational function. This is given to us by the famous Vélu's formulas [85].

Proposition 108 (Vélu's formulas)**.** *Let $E : y^2 = x^3 + ax + b$ be an elliptic curve defined over a field k, and let $G \subset E(\bar{k})$ be a finite subgroup. The separable isogeny $\phi : E \to E/G$, of kernel G, can be written as*

$$\phi(P) = \left(x(P) + \sum_{Q \in G \setminus \{\mathcal{O}\}} x(P+Q) - x(Q), y(P) + \sum_{Q \in G \setminus \{\mathcal{O}\}} y(P+Q) - y(Q) \right);$$

```
Input: A finite field $\mathbb{F}_q$,
    a prime power $\ell^e$ such that $\ell \nmid (q-1)$ and $\ell \ll q$;
Output: An irreducible polynomial of degree $\ell^e$.
Take random curves $E_0$, until one with $\ell | \#E_0$ is found;
Factor $\#E_0$;
for $1 \leq i \leq e$ do
    Use Vélu's formulas to compute a degree $\ell$ isogeny $\phi_i : E_{i-1} \to E_i$;
end for
Take random points $P \in E_i(\mathbb{F}_q)$ until one not in $[\ell]E_i(\mathbb{F}_q)$ is found;
return The polynomial vanishing on the abscissas of $\phi_i^{-1} \circ \cdots \circ \phi_1^{-1}(P)$.
```

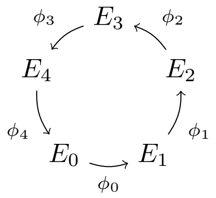


Figure 20: Couveignes-Lercier algorithm to compute irreducible polynomials, and structure of the computed isogeny cycle.

and the curve E/G has equation $y^2 = x^3 + a'x + b'$, where

$$a' = a - 5 \sum_{Q \in G \setminus \{\mathcal{O}\}} (3x(Q)^2 + a),$$

$$b' = b - 7 \sum_{Q \in G \setminus \{\mathcal{O}\}} (5x(Q)^3 + 3ax(Q) + 2b).$$

Proof. See [20, §8.2]. □

Corollary 109. *Let E and G be as above. Let*

$$h(X) = \prod_{Q \in G \setminus \{\mathcal{O}\}} (X - x(Q)).$$

Then the isogeny ϕ can be expressed as

$$\phi(X, Y) = \left(\frac{g(X)}{h(X)}, y \left(\frac{g(x)}{h(x)} \right)' \right),$$

where $g(X)$ is defined by

$$\frac{g(X)}{h(X)} = dX - p_1 - (3X^2 + a)\frac{h'(X)}{h(X)} - 2(X^3 + aX + b) \left(\frac{h'(X)}{h(X)} \right)',$$

with p_1 the trace of $h(X)$ and d its degree.

Proof. See [20, §8.2]. □

The Couveignes-Lercier algorithm is summarized in Figure 20. What is most interesting, is the fact that it can be immediately generalized to computing irreducible polynomials of degree ℓ^e, by iterating the construction. Looking at the specific parameters, it is apparent that ℓ is an *Elkies prime* for E (i.e., $\left(\frac{D}{\ell}\right) = 1$), and that each isogeny ϕ_i is horizontal, thus their composition eventually forms a cycle, the *crater* of a volcano.

D SIDH/SIKE, a defunct key exchange scheme

TODO