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, Wurzbürg, Germany
v3 – July 2023, Popayan, Colombia

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 [5].

The second revision [5] 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 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 **??**. 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.

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 and the Universidad del Cauca. Souidi El Mamoun, Damien Stehlé and the University 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, 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 [27, 28, 16, 22].

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 a projective point $(x_0, \dots, x_n)$ is customarily denoted by $(x_0 : \dots : x_n)$. 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 [27, Chap. III].

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

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

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

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

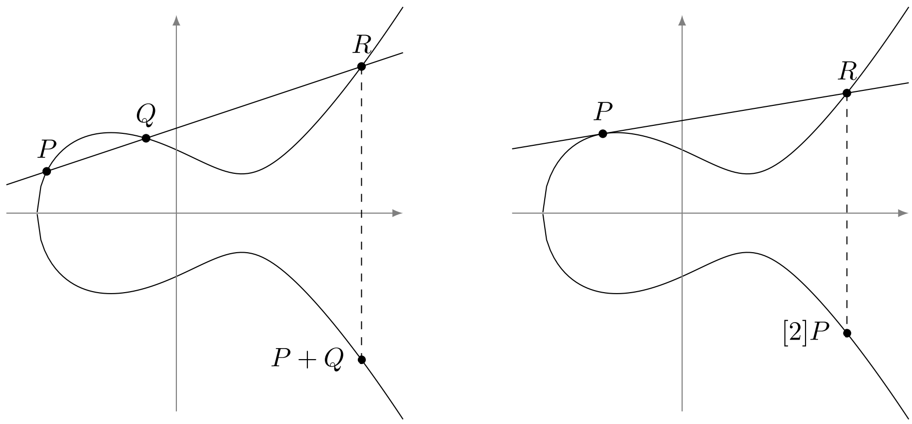


Figure 1: An elliptic curve defined over $\mathbb{R}$, and the geometric representation of its group law.

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*

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

Proof. See [27, 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.

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

Finally, we 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 dividing 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 *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*.

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

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 [27, 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.

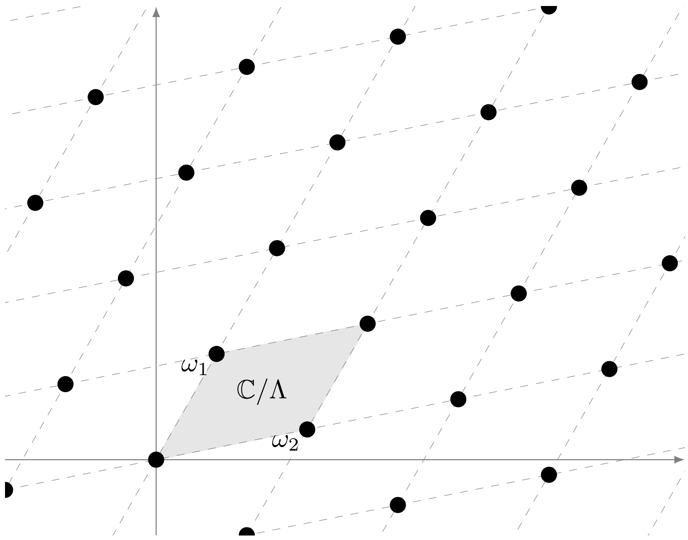


Figure 2: A complex lattice (black dots) and its associated complex torus (grayed *fundamental domain*).

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 [28, 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

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

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

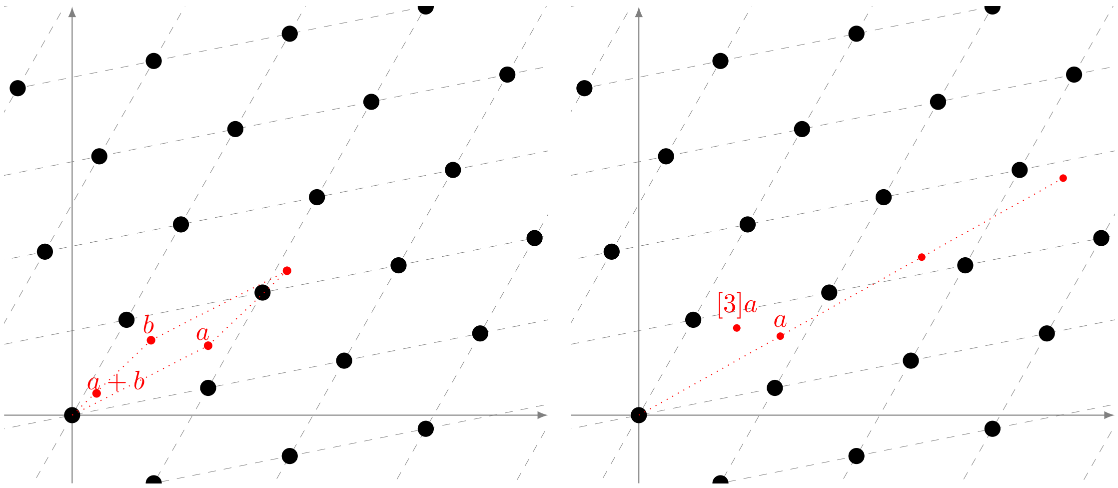


Figure 3: Addition (left) and scalar multiplication (right) of points in a complex torus $\mathbb{C}/\Lambda$.

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 [28, 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 [27, 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 [28, 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 $\Lambda = m\Lambda'$.

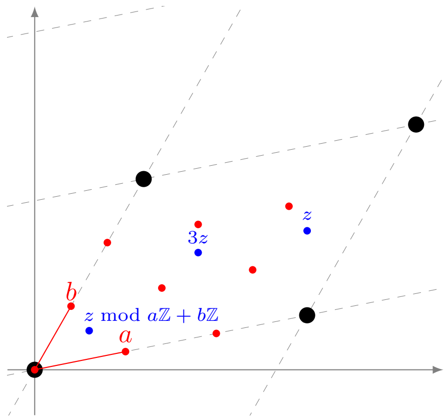
Within this new perspective, isogenies are a mild generalization of scalar multiplications. Whenever two lattices Λ, Λ' verify $\alpha\Lambda \subset \Lambda'$, there is a well defined map

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

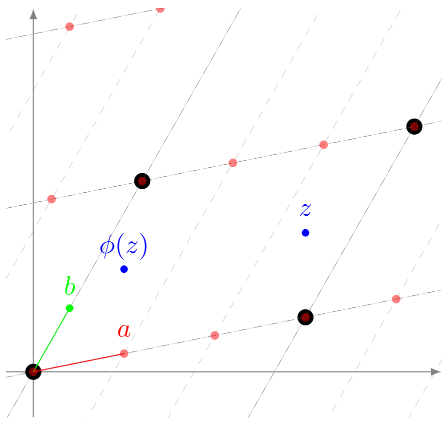
that is holomorphic and also a group morphism. One example of such maps is given in Figure 4b: there, $\alpha = 1$ and the red lattice strictly contains the black one; the map is simply defined as reduction modulo Λ'. It turns out that these maps are exactly the isogenies of the corresponding elliptic 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 [27, 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 k with q elements, which are the main objects manipulated in cryptography. Obviously, the group of k-rational points is finite, thus the algebraic group $E(\bar{k})$ 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 [27, 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 [27, 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 $\phi^*(k(E'))$.

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.

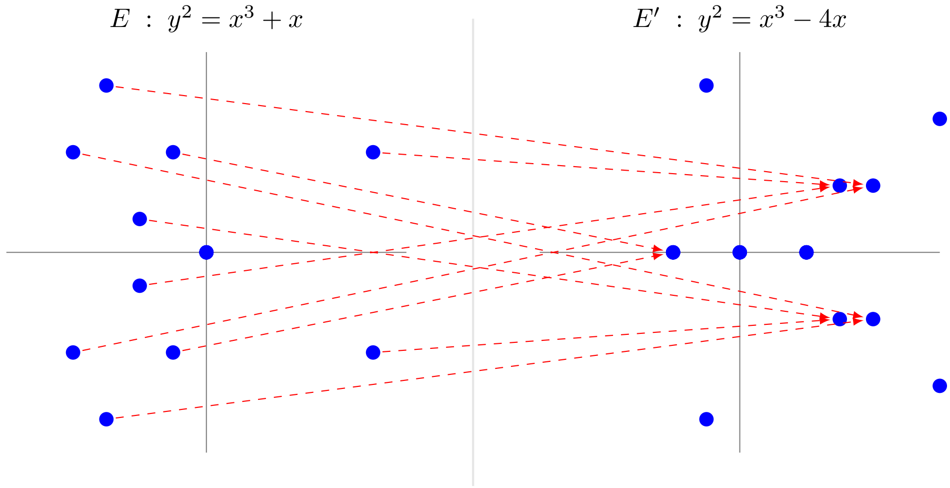


Figure 5: The isogeny $(x, y) \mapsto \big((x^2+1)/x,\ y(x^2-1)/x^2\big)$, as a map between curves defined over $\mathbb{F}_{11}$.

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 [27, 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 $E' \simeq E''$.*

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. *Any isogeny of elliptic curves can be decomposed as a product of prime degree isogenies.*
2. *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 [27, 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. *$\hat{\hat\phi} = \phi$.*

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

Proposition 30 (Vélu [33])**.** *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.

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 31. 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 32. *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., [27, 10] 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 33. *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 34. *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 $Q \in E'[m]$*

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

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

Proof. See [27, III.8.2]. $\square$

Corollary 35. *Let $\phi : E \to E'$ be an isogeny of degree d. For any m, P, Q*

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

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 [11].

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 [17, 34].

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 36 (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 37. 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 38. *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 39 (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 40 (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 41 (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 42 (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, is the *maximal order* of K, i.e. it contains any other order of K. A more precise statement is the following.

Proposition 43. *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 $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$.*

If Δ_K is the discriminant of $\mathcal{O}_K$, the discriminant *of $\mathcal{O}$ is $f^2\Delta_K$. 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 44. *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 [15, 34].

Definition 45 (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 46. 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 47. *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. $B_{p,\infty} \cong \left(\frac{-1,-p}{\mathbb{Q}}\right)$ *if* $p \equiv 5 \pmod 8$*;*

[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.

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*.*

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.

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; $N(I) = \mathrm{nrd}(I) := \gcd\{N(\alpha) \mid \alpha \in I\}$. 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 $\mathrm{discrd}(I) := |\det(\mathrm{Tr}(\alpha_i\overline{\alpha_j}))_{1\le i,j\le 4}|^{1/2}$; 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 $I \subset \mathcal{O}$.

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

- $\mathbb{Z}$*; this can happen only if* $p = 0$*;*
- *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 [27, III, Coro. 9.4] and [14]. □

The smallest $\mathbb{Q}$-algebra containing $\mathrm{End}(E)$, i.e. $\mathrm{End}(E)\otimes\mathbb{Q}$, 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 $\mathrm{End}(E)$ must contain an algebraic integer with the same minimal equation, which has discriminant $\Delta_\pi = t^2 - 4q < 0$, and thus $\mathrm{End}(E) \subset \mathbb{Q}(\sqrt{\Delta_\pi})$.

The minimal polynomial of Frobenius can be computed in polynomial time using Schoof's algorithm [25] (see Appendix B), and thus the endomorphism algebra can be determined with the same complexity. Determining the exact order isomorphic to $\mathrm{End}(E)$ is (in general) much more complicated and we shall come back to it in Sections 10 and **??**.

Example 49. 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 33.

Exercise I.7. Prove Corollary 35.

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 [21], Pizer [23, 24] and Kohel [14]; further algorithmic treatment of graphs of ordinary curves, and the now famous name of *isogeny volcanoes*, was subsequently given by Fouquet and Morain [9].

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 50 (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 51. *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 52. *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 [32, 31, 12].

Definition 53 (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 54 (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 55 (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 56. *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 [32, 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 57 (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 58 (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 59 (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 60 (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 61. *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.

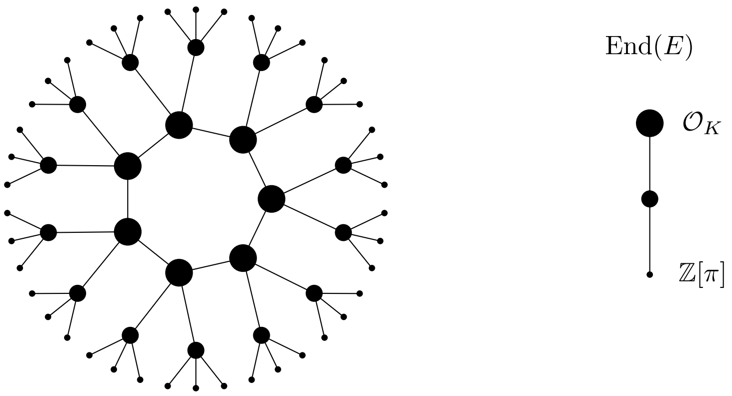


Figure 6: A volcano of 3-isogenies (ordinary elliptic curves, Elkies case), and the corresponding tower of orders inside the endomorphism algebra.

Proposition 62 (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 [32, 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 [20, 2, 12, 32]. 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 63 (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.

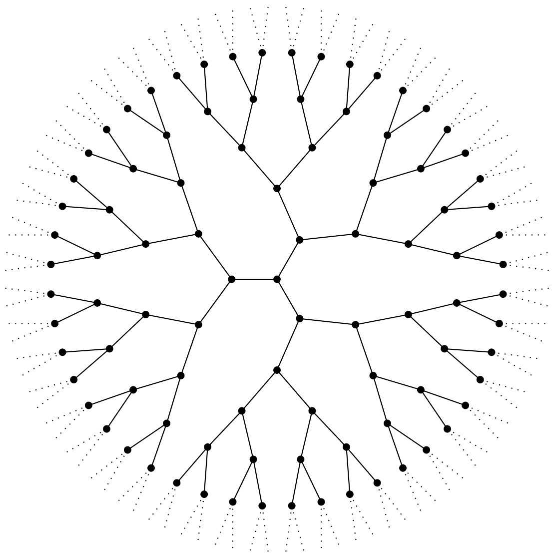


Figure 7: Infinite 2-isogeny graph of elliptic curves over $\mathbb{C}$ without complex multiplication.

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 diagonalizable in $\mathbb{F}_\ell$, then 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 [14] 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 64 (Kohel [14, 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 65 (Kohel [14])**.** *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 [14, Prop. 21], or [29, 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:

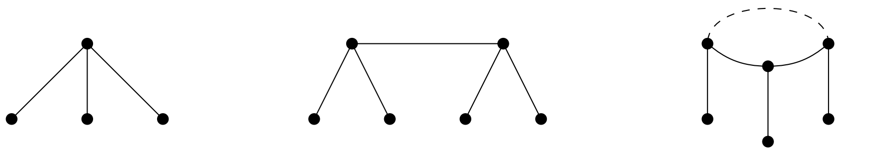
(0) If $\left(\frac{\Delta_K}{\ell}\right) = -1$, there are no horizontal isogenies: the isogeny graph is just a complete tree of degree $\ell + 1$ (in the graph theoretic sense) at each level but the last. We call this the *Atkin case*, as it is an extension of the Atkin case in the SEA point counting 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 $\phi : E \to E'$ 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 [9]; 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 66 (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, 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 67. *Let $\mathcal{O}$ be an order of a number field K, and let $\mathfrak{a}_1, \ldots, \mathfrak{a}_{h(\mathcal{O})}$ 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 [28, Ch. II] and [16, 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 68. 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 69 (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 [16, 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 70. 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 $\mathbb{Z}[i]$.

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

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

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

with discriminant $\Delta_\pi = t^2 - 4q \leq 0$. Setting the case $\Delta_\pi = 0$ aside, $\mathrm{End}(E)$ 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 71 (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 [16, Ch. 13]. □

12 Isogenies and the CM action

From now on we abbreviate "complex multiplication" by CM. We saw in Theorem 67 that the class group $\mathrm{Cl}(\mathcal{O})$ acts on the set $\mathrm{Ell}(\mathcal{O})$ of CM elliptic curves over $\mathbb{C}$ with complex multiplication by $\mathcal{O}$. After having identified $\mathrm{Cl}(\mathcal{O})$ 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 $\mathrm{Cl}(\mathcal{O})$ on $\mathrm{Ell}(\mathcal{O})$ 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 $\mathrm{Ell}_q(\mathcal{O})$ 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 $\mathrm{Ell}_q(\mathcal{O})$ are connected exclusively by horizontal isogenies, we will also call it a *horizontal isogeny class.*

Let $E \in \mathrm{Ell}_q(\mathcal{O})$, 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.

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

Theorem 72 (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 $\mathrm{Ell}_q(\mathcal{O})$ the set of $\bar{\mathbb{F}}_q$-isomorphism classes of curves with complex multiplication by $\mathcal{O}$.*

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 $\#\,\mathrm{Ell}_q(\mathcal{O}) = h(\mathcal{O})$, but also answers our question on the size of ℓ-isogeny volcanoes.

Corollary 73. *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 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 74 (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.[9] 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 $t = 0, \ldots, n-1$ where $n = h(\mathcal{O})$. In particular $\lambda_0 = 2$,

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

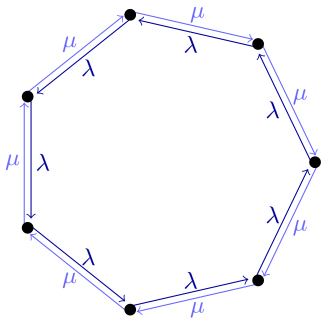


Figure 9: An isogeny cycle for an Elkies prime ℓ, with edge directions associated with the Frobenius eigenvalues λ and μ.

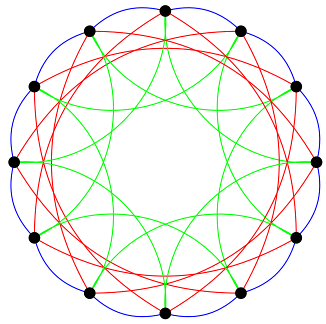


Figure 10: Graph of horizontal isogenies on 12 curves, with isogenies of three different degrees (represented in different colors).

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 61.

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 [32, Chap. 16]).

Theorem 75 (Jao, Miller, Venkatesan [13])**.** *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.

Exercises

Exercise II.1. Prove that Proposition 52 implies the finite field case of Theorems 50 and 51. 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

Part IV
The full supersingular isogeny graph

References

[1] 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.

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

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

[4] 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/.

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

[6] 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.

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

[8] 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.

[9] 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.

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

[11] 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.

[12] 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.

[13] 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.

[14] 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.

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

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

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

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

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

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

[21] 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.

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

[23] 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.

[24] 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.

[25] 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.

[26] 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.

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

[28] 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.

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

[30] 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: #.

[31] 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/.

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

[33] 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.

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

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 [18] 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 11a. 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 11b. 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.

1. Set $e = \prod_{r \text{ prime } < B} r^{\lfloor \log_r \sqrt{N} \rfloor}$;
2. Pick a random $1 < x < N$;
3. Compute $y = x^e \mod N$;
4. Compute $q' = \gcd(y-1, N)$;
5. **if** $q' \neq 1, N$ **then**
6. **return** $N/q', q'$;
7. **else**
8. **return** FAIL.
9. **end if**

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

Input: An integer $N = pq$, a bound B;
Output: (p, q) or FAIL.

1. Pick random integers a, X, Y in $[0, N[$;
2. Compute $b = Y^2 - X^3 - aX \mod N$;
3. Define the elliptic curve $E : y^2 = x^3 - ax - b$.
4. Define the point $P = (X : Y : 1) \in E(\mathbb{Z}/N\mathbb{Z})$.
5. Set $e = \prod_{r \text{ prime } < B} r^{\lfloor \log_r \sqrt{N} \rfloor}$;
6. Compute $Q = [e]P = (X' : Y' : Z')$;
7. Compute $q' = \gcd(Z', N)$;
8. **if** $q' \neq 1, N$ **then**
9. **return** $N/q', q'$;
10. **else**
11. **return** FAIL.
12. **end if**

(b) Lenstra's ECM algorithm

Figure 11: 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 [25]. 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 76 (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 [1, 7, 26, 8]. 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 [26, 19, 8, 30].

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 [3] and then slightly generalized in [6]. 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 [33].

Proposition 77 (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 ℓ^e such that $\ell \nmid (q-1)$ and $\ell \ll q$;
Output: An irreducible polynomial of degree ℓ^e.
Take random curves E_0, until one with $\ell | \# E_0$ is found;
Factor $\# E_0$;
for $1 \le i \le e$ **do**
  Use Vélu's formulas to compute a degree ℓ 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 $\phi_i^{-1} \circ \cdots \circ \phi_1^{-1}(P)$.

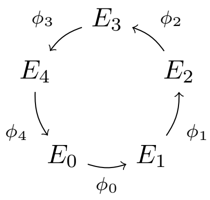


Figure 12: Couveignes-Lercier algorithm to compute irreducible polynomials, and structure of the computed isogeny cycle.

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 [4, §8.2]. □

Corollary 78. *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 [4, §8.2]. □

The Couveignes-Lercier algorithm is summarized in Figure 12. 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.