Isogeny Graphs in Cryptography

Luca De Feo
Université Paris Saclay – UVSQ
https://defeo.lu/

Graph Theory Meets Cryptography
July 29 – August 2, 2019, Wurzbürg, Germany

Introduction

These lectures notes were written for the summer school *Graph Theory Meets Cryptography* in Wurzbürg, Germany.

The presentation is divided in four parts, roughly corresponding to the four lectures given.

Contents

LaTeX source code available at https://github.com/defeo/wurzburg/.

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 [15, 16, 7, 12].

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

1 Elliptic curves

Elliptic curves are 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 $x_i = \lambda_i y_i$ 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 [15, 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 coordinates $x = X/Z$ and $y = Y/Z$, we equivalently define the elliptic curve as the locus of the equation

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

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

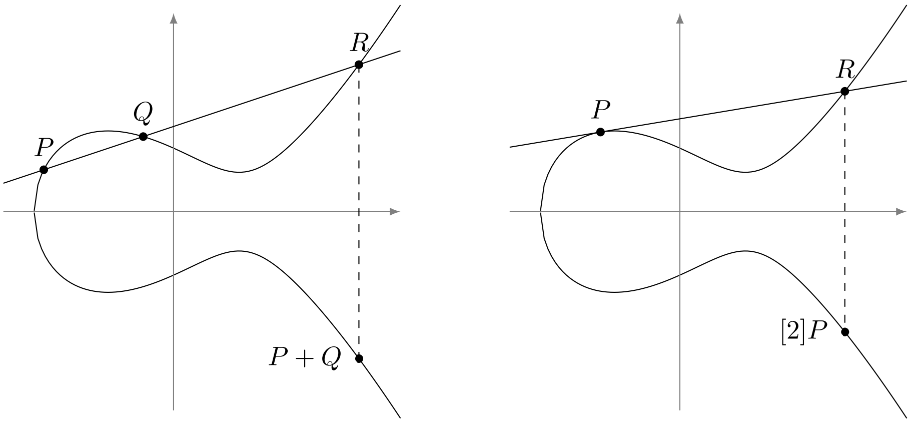


Figure 1: An elliptic curve defined over $\mathbb{R}$, and the geometric representation of its group law.

In characteristic different from 2 and 3, we can show that any 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, Bezout'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
$$x_3 = \lambda^2 - x_1 - x_2,$$
$$y_3 = -\lambda x_3 - y_1 + \lambda x_1.$$

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

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

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

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

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

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

Proof. See [15, Coro. 6.4]. For the characteristic 0 case see also Section 3. □

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 an alternative characterization of supersingularity in the next section.

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 has a *quadratic twist*, unique up to isomorphism, 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*.

A surjective group morphism, not necessarily invertible, between two elliptic curves is called an *isogeny*. It turns out that isogenies are algebraic maps as well.

Theorem 7. *Let E, E' be two elliptic curves, and let $\phi : E \to E$ be a map between them. The following conditions are equivalent:*

1. *ϕ is a surjective group morphism,*

2. *ϕ is a group morphism with finite kernel,*

3. *ϕ is a non-constant algebraic map of projective varieties sending the point at infinity of E onto the point at infinity of E'.*

Proof. See [15, 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 exactly 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. Thus, by including the constant map that sends every point to the point at infinity, the set of isogenies $E \to E'$ forms a group. Additionally, endomorphisms $E \to E$ support composition, distributing over addition, hence the set of all endomorphisms forms a ring, denoted by $\mathrm{End}(E)$.[1]

Since each $m \in \mathbb{Z}$ defines a different multiplication-by-m endomorphism, clearly $\mathbb{Z} \subset \mathrm{End}(E)$. But can $\mathrm{End}(E)$ be larger? We shall now give a complete characterization of the endomorphism ring for any elliptic curve.

Definition 8 (Order)**.** Let K be a finitely generated $\mathbb{Q}$-algebra. An *order* $\mathcal{O} \subset K$ is a subring of K that is a finitely generated $\mathbb{Z}$-module, and that contains a $\mathbb{Q}$-basis for K.

The prototypical example of order is the ring of integers $\mathcal{O}_K$ of a number field K. It turns out that $\mathcal{O}_K$ is the *maximal order* of K, i.e., it contains any other order of K. We shall discuss this case in depth in Section 6.

Definition 9 (Quaternion algebra)**.** A *quaternion algebra* is an algebra of the form

$$K = \mathbb{Q} + \alpha\mathbb{Q} + \beta\mathbb{Q} + \alpha\beta\mathbb{Q},$$

where the generators satisfy the relations

$$\alpha^2, \beta^2 \in \mathbb{Q}, \quad \alpha^2 < 0, \quad \beta^2 < 0, \quad \beta\alpha = -\alpha\beta.$$

Theorem 10 (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:*

- *$\mathbb{Z}$, only if $p = 0$;*

- *An order $\mathcal{O}$ in a quadratic imaginary field (a number field of the form $\mathbb{Q}(\sqrt{-D})$ for some $D > 0$); in this case we say that E has* complex multiplication *by $\mathcal{O}$;*

- *Only if $p > 0$, a maximal order in a quaternion algebra ramified at p and ∞; in this case we say that E is* supersingular.

Proof. See [15, III, Coro. 9.4] and [6]. □

In positive characteristic, a curve that is not supersingular is called *ordinary*; we shall see that it necessarily has complex multiplication.

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

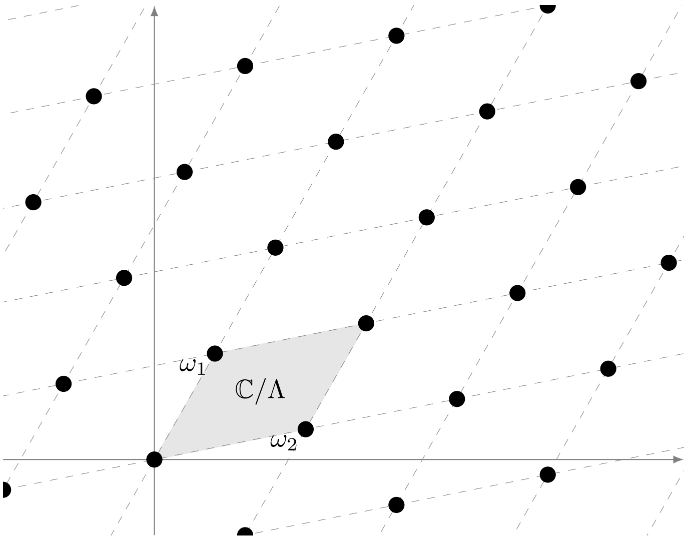


Figure 2: A complex lattice (black dots) and its associated complex torus (grayed *fundamental domain*).

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 11 (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 any $\lambda \in \mathbb{R}$, 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.

Proposition 12. *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*

$$\omega_1' = a\omega_1 + b\omega_2,$$
$$\omega_1' = c\omega_1 + d\omega_2,$$

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

Proof. See [16, I, Lem. 2.4]. □

Definition 13 (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.

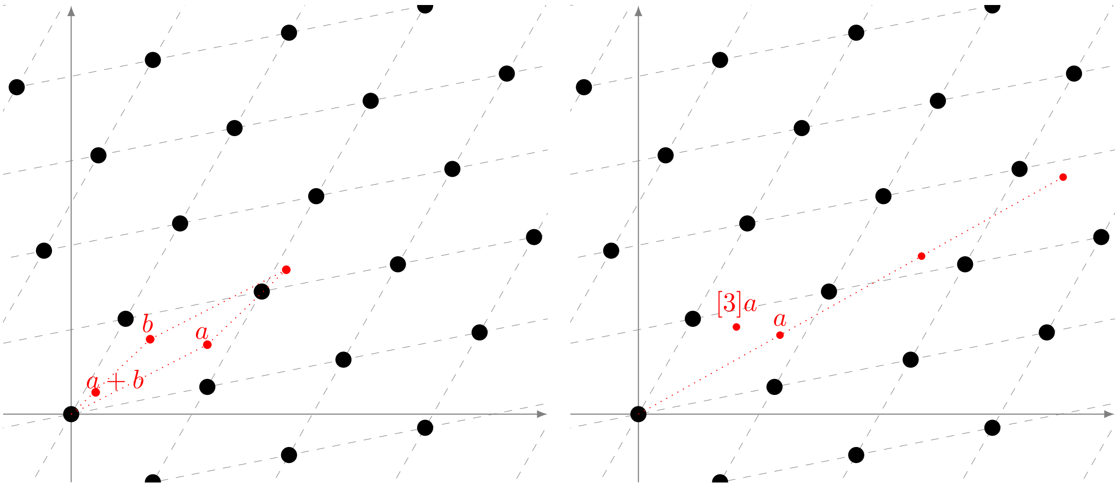


Figure 3: Addition (left) and scalar multiplication (right) of points in a complex torus $\mathbb{C}/\Lambda$.

Definition 14 (Homothetic lattices)**.** Two complex lattices Λ and Λ' are said to be *homothetic* if there is a complex number $\alpha \in \mathbb{C}^\times$ such that $\Lambda = \alpha\Lambda'$.

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

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

It is customary to set

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

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

Theorem 15 (Modular j-invariant)**.** *The* modular j-invariant *is the function on complex lattices defined by*

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

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

Proof. See [16, 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 16 (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 17. *The Weierestrass 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 [15, 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 18 (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 [16, 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. The multiplication-by-m map corresponds then to

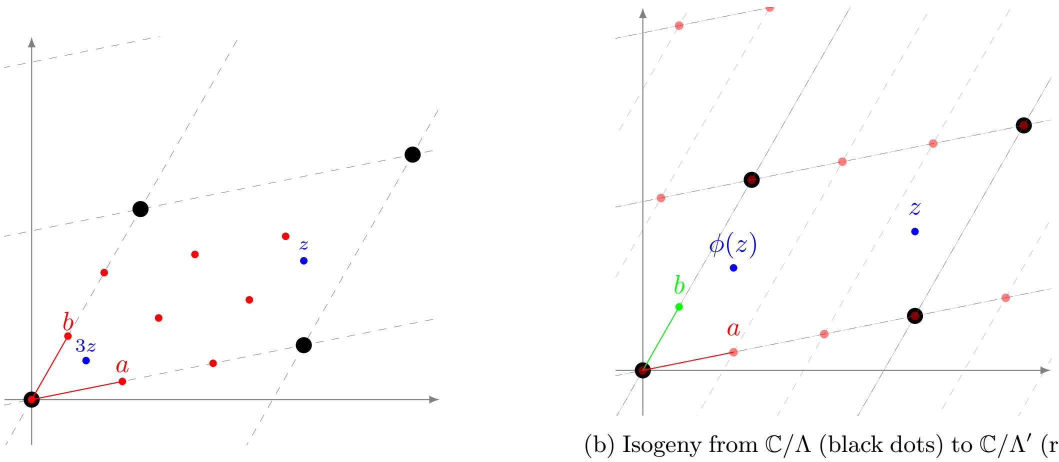
$$\begin{aligned}[m] : \mathbb{C}/\Lambda &\to \mathbb{C}/\Lambda',\\ z &\mapsto z \bmod \Lambda';\end{aligned}$$

or equivalently $[m] : z \mapsto mz \bmod \Lambda$, after applying the homothety $m\Lambda' = \Lambda$, as expected.

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 4a: 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.



(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.

Theorem 19. *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 [15, VI, Th. 4.1]. □

Looking again at Figure 4a, 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 Section 6.

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 20 (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 21. *Let π be the Frobenius endomorphism of E. Then:*

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

Theorem 22 (Hasse)**.** *Let E be an elliptic curve defined over a finite field with q elements. Its Frobenius endomorphism π satisfies a quadratic equation*

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

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

Proof. See [15, V, Th. 2.3.1]. □

The coefficient t in the equation is called the *trace* of π. By replacing $\pi = 1$ in the equation, we immediately obtain the cardinality of E as $\#E(k) = \#\ker(\pi - 1) = q + 1 - t$.

Corollary 23. *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 24. 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 25. *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 [15, V, Th. 2.4]. □

5 Isogenies

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

Definition 26 (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.

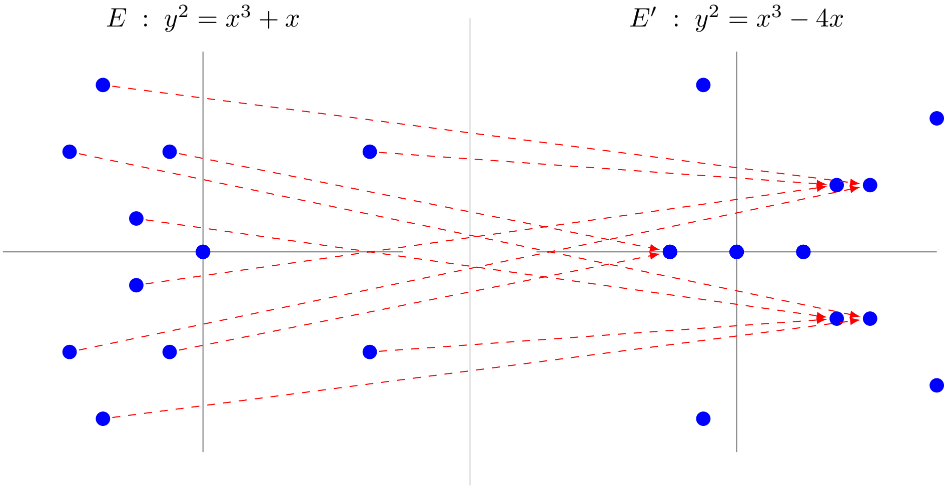


Figure 5: The isogeny $(x, y) \mapsto \big((x^2+1)/x,\ y(x^2-1)/x^2\big)$, as a map between curves defined over $\mathbb{F}_{11}$.

2. ϕ is said to be *separable*, *inseparable*, or *purely inseparable* if the extension of function fields is.
3. If ϕ is separable, then $\deg\phi = \#\ker\phi$.
4. If ϕ is purely inseparable, then $\deg\phi$ is a power of the characteristic of k.
5. Any isogeny can be decomposed as a product of a separable and a purely inseparable isogeny.

Proof. See [15, II, Th. 2.4]. □

In practice, most of the time we will be considering separable isogenies, and we can take $\deg\phi \equiv \#\ker\phi$ as the definition of the degree. Notice that in this case $\deg\phi$ is the size of any fiber of ϕ.

Example 27. The map ϕ from the elliptic curve $y^2 = x^3 + x$ to $y^2 = x^3 - 4x$ defined by

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

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 (2) 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 we are unable to see all fibers over $\mathbb{F}_p$, 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 most unique property of separable isogenies is that they are entirely determined by their kernel.

Proposition 28. *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 29.

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 with domain E, up to isomorphism.*

Slightly more work is required to prove the following, fundamental, theorem (the difficulty comes essentially from the inseparable part, see [15, III.6.1] for a detailed proof).

Theorem 30 (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 31 (Vélu [18]). *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*

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

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

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

6 Complex multiplication

We conclude with one of the most power tools for the study of isogeny graphs: the theory of *complex multiplication*. Our goal is to characterize elliptic curves with endomorphism rings larger than $\mathbb{Z}$; to do so, we start from elliptic curves defined over the complex numbers. But first, we need to recall some basic definitions from algebraic number theory; for a more detailed treatment, see [8].

An *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 32 (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 33 (Ring of integers). Let K be a number field, an *algebraic integer* of K is an element $\alpha \in K$ that is 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 $\delta = (\Delta + \sqrt{\Delta})/2$. By Definition 8, an order of a quadratic field K is a subring of K that is a $\mathbb{Z}$-module of rank 2. The ring of integers $\mathcal{O}_K$ of K fits the bill: it always has $(1, \delta)$ as *integral basis*, i.e., as a set of $\mathbb{Z}$-module generators. Furthermore, it is easy to prove that any other order is contained in $\mathcal{O}_K$; for this reason we will some times call it the *maximal order* of K. More precisely, we can prove the following.

Proposition 34. *Let K be a quadratic number field, and let $\mathcal{O}_K$ be its ring of integers. Any order $\mathcal{O} \subset K$ can be written as $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ for an integer f, called the* conductor *of $\mathcal{O}$. If Δ_K is the discriminant of 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 $\Delta' | \Delta$.

When K is imaginary quadratic, any order $\mathcal{O} \subset K \subset \mathbb{C}$ is a complex lattice by definition. We now define a broader class of algebraic lattices, that are not necessarily rings.

Definition 35 (Fractional ideal)**.** Let $\mathcal{O}$ be an order of a number field K. A *(fractional) $\mathcal{O}$-ideal* $\mathfrak{a}$ is a finitely generated non-zero $\mathcal{O}$-submodule of K.

If $\mathfrak{a}$ is generated by a single element, then it is called *principal.* If $\mathfrak{a} \subset \mathcal{O}$, then it is called an *integral* ideal.

An $\mathcal{O}$-ideal $\mathfrak{a}$ is *invertible* if there exists another ideal $\mathfrak{a}^{-1}$ such that $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{a}^{-1}\mathfrak{a} = \mathcal{O}$. If $\mathcal{O}$ is the maximal order of K, then any $\mathcal{O}$-ideal is invertible.

When $\mathcal{O}$ is the maximal order, we often omit specifying the order, and simply speak of (fractional) ideals of K.

Now, let K be a quadratic imaginary field. Let Λ be a complex lattice such that $\Lambda \subset K$, and define its order $\mathcal{O}_\Lambda$ to be

$$\mathcal{O}_\Lambda = \{\alpha \in K \mid \alpha\Lambda \subset \Lambda\}. \tag{3}$$

It is clear that $\mathcal{O}_\Lambda$ is a ring, and it is easy to show that it is an order of K, and thus that Λ is a fractional $\mathcal{O}_\Lambda$-ideal. Using Theorem 17 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 *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 36 (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 37. *Let $\mathcal{O}$ be an order of a number field K, and let $\mathfrak{a}_1, \dots, \mathfrak{a}_{h(\mathcal{O})}$ be representatives of* $\mathrm{Cl}(\mathcal{O})$*. Then:*

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

Proof. See [16, Ch. II] and [7, 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 part, we shall say more on how $\mathrm{Cl}(\mathcal{O})$ acts on the set $\mathrm{Ell}(\mathcal{O})$.

Example 38. 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, $j(\mathbb{Z}[i]) = 1728$.

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

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

6.1 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[2] $\mathfrak{p}$ 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 39 (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 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 [7, Ch. 13]. □

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

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

Example 40. 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 $\mathrm{End}(E(p))$ is not commutative.

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

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

with discriminant $\Delta_\pi = t^2 - 4q \leq 0$. Setting the case $\Delta_\pi = 0$ aside, $\mathrm{End}(E)$ 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 41 (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 [7, Ch. 13]. □

Exercises

Exercise I.1. Prove Proposition 6.

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

Exercise I.3. Prove Proposition 21.

Exercise I.4. Using Proposition 25, devise an algorithm to effectively compute $\#E(\mathbb{F}_{q^n})$ given $\#E(\mathbb{F}_q)$.

Exercise I.5. Prove Corollary 29

Exercise I.6. Let K be a complex imaginary number field, $\Lambda \subset K$ a complex lattice, and $\mathcal{O}_\Lambda$ its order as defined in Eq. (3). Prove that $\mathcal{O}_\Lambda$ is an order of K.

Exercise I.7. 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 I.8. Prove that -163 is not a square modulo all odd primes < 41. (Hint: $\mathbb{Q}(\sqrt{-163})$ has class number 1).

Part II
Isogeny graphs

We now look at isogeny graphs: graphs with isomorphisms classes of ellitpic curves for vertices, and isogenies for edges. Depending on the constraints we put on the isogenies, we will get graphs with different properties; the most important ones will be *isogeny volcanoes*, *Cayley graphs*, and *supersingular graphs*.

The classification of isogeny graphs was initiated by Mestre [11], Pizer [13, 14] and Kohel [6]; further algorithmic treatment of graphs of ordinary curves, and the now famous name of *isogeny volcanoes* was subsequently given by Fouquet and Morain [3]. We now review the different kinds of graphs.

7 Isogeny classes

We have learned previously that being isogenous is an equivalence relation,[3] it thus makes sens 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 with a theorem that links isogeny classes with the complex multiplication theory we previously learned about.

Theorem 42 (Serre-Tate)**.** *Two elliptic curves E, E' with complex or quaternionic multiplication are isogenous 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 multiplications 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.
- Any two supersingular curves over a field of characteristic p are isogenous.

An easy consequence for the finite field is case is the following.

Corollary 43. *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. Like we have already done before, we shall use the notation $\mathrm{Ell}_q(\mathcal{O})$ for the subclass of elliptic j-invariants over $\bar{\mathbb{F}}_q$ with complex multiplication by an order $\mathcal{O}$.

8 Graphs

We recall some basic concepts of graph theory; for simplicity, we will restrict to undirected graphs. An undirected graph G is a pair (V, E) where V is a finite set of *vertices* and $E \subset V \times V$ is a set of unordered pairs called *edges*. Two vertices v, v' are said to be *connected by an edge*

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

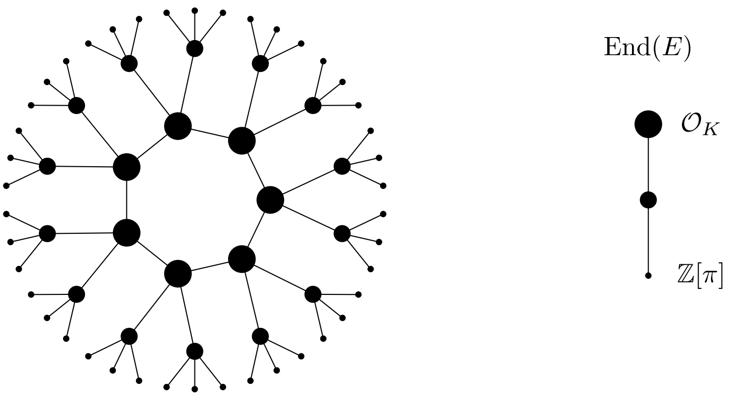


Figure 6: A volcano of 3-isogenies (ordinary elliptic curves, Elkies case), and the corresponding tower of orders inside the endomorphism algebra.

if $\{v, v'\} \in E$. The *neighbors* of a vertex v are the vertices of V connected to it by an edge. A *path* between two vertices v, v' is a sequence of vertices $v \to v_1 \to \cdots \to v'$ such that each vertex is connected to the next by an edge. The *distance* between two vertices is the length of the shortest path between them; if there is no such path, the vertices are said to be at infinite distance. A graph is called *connected* if any two vertices have a path connecting them; it is called *disconnected* otherwise. The *diameter* of a connected graph is the largest of all distances between its vertices. The *degree* of a vertex is the number of edges pointing to (or from) it; a graph where every edge has degree k is called *k-regular*. The *adjacency matrix* of a graph G with vertex set $V = \{v_1, \dots, v_n\}$ and edge set E, is the $n \times n$ matrix where the (i, j)-th entry is 1 if there is an edge between v_i and v_j, and 0 otherwise. Because our graphs are undirected, the adjacency matrix is symmetric, thus it has n real eigenvalues

$$\lambda_1 \geq \cdots \geq \lambda_n.$$

Definition 44 (Isogeny graph)**.** An *isogeny graph* is a (multi)-graph whose vertices are the j-invariants of isogenous curves, and whose edges are isogenies between them.

The dual isogeny theorem guarantees that for every isogeny $E \to E'$ there is a corresponding isogeny $E' \to E$ of the same degree. For this reason, isogeny graphs are usually drawn undirected. Figure 6 shows a typical example of isogeny graph over a finite field, where we restrict to isogenies of degree 3.

9 ℓ-isogeny graphs

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 28, we know this is equivalent to 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

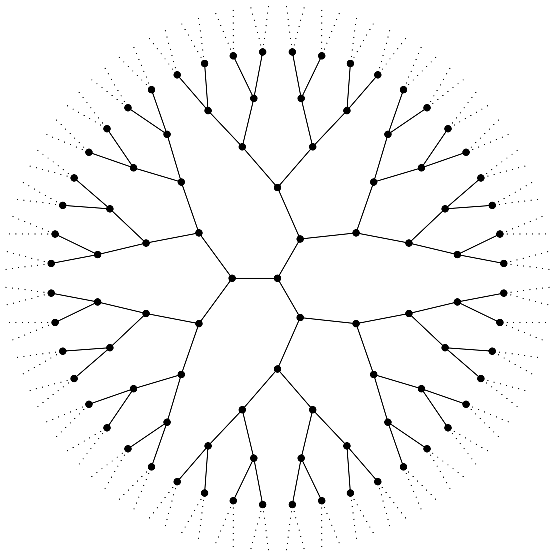


Figure 7: Infinite 2-isogeny graph of elliptic curves without complex multiplication.

containing E, is $(\ell+1)$-regular, and cannot have loops, otherwise that would provide a non-trivial 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 $\phi : E \to E/G$ is $\mathbb{F}_q$-rational if and only if $\pi(G) = G$, 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[4]:

(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.

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

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

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

$E/\bar{\mathbb{Q}}$. 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 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 [6] 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 as follows.

Proposition 45 (Kohel [6, 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 46 (Kohel [6])**.** *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 [6, Prop. 21], or [?]. □

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.

(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.

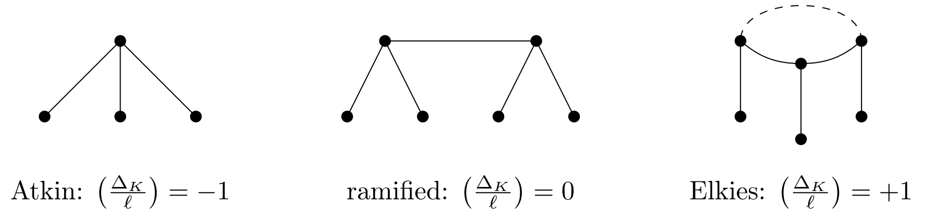

Atkin: $\left(\frac{\Delta_K}{\ell}\right) = -1$
ramified: $\left(\frac{\Delta_K}{\ell}\right) = 0$
Elkies: $\left(\frac{\Delta_K}{\ell}\right) = +1$

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 if *isogeny volcanoes* for them [3]; in the Elkies case, we call *crater* the cycle at the surface.

We are left with one last question: how large are these graphs? Theorem 37 tells us that for any order $\mathcal{O}$ there are exactly $h(\mathcal{O})$ curves in $\mathrm{Ell}(\mathcal{O})$, thus we know exactly how many curves there are in each level of the volcano; for example we know that there will be exactly $h(\mathcal{O}_K)$ distinct trees in the Atkin case. What we do not know yet, is the number of connected components in the Elkies case. To address this question, we shall go back to complex multiplication.

10 Complex multiplication

We have already seen how the theory of complex multiplication gives a correspondence between the class group $\mathrm{Cl}(\mathcal{O})$ and the set of CM elliptic curves $\mathrm{Ell}(\mathcal{O})$. However, the (omitted) proof of Theorem 37 provides much more than a simple bijection of sets: it constructs an *action* of the group $\mathrm{Cl}(\mathcal{O})$ on the set $\mathrm{Ell}(\mathcal{O})$. We now complete our study of complex multiplication by defining the group action, and then constructing *Cayley graphs* associated to it.

We let $\mathcal{O}$ be an order in a number field K, and we assume that $\mathrm{Ell}_q(\mathcal{O})$ is non-empty. Because curves in $\mathrm{Ell}_q(\mathcal{O})$ are connected exclusively by horizontal (cyclic) isogenies, we will 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 47 (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 48. *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. 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 $E[\mathfrak{a}]$ is the eigenspace of λ, and $E[\hat{\mathfrak{a}}]$ 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).

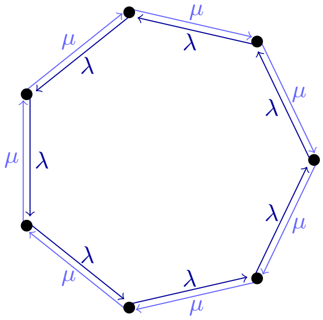


Figure 9: An isogeny cycle for an Elkies prime ℓ, with edge directions associated with the Frobenius eigenvalues λ and μ.

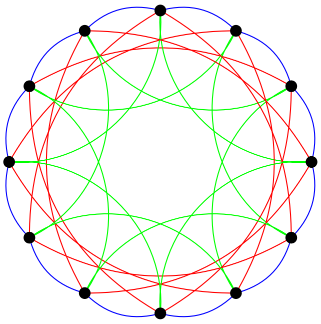


Figure 10: Graph of horizontal isogenies on 12 curves, with isogenies of three different degrees (represented in different colors).

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 49 (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 vertices are in bijection with $\mathrm{Cl}(\mathcal{O})$ only up to automorphism.[5] These kind of graphs obtained from group actions are sometimes called *Schreier graphs* to distinguish them from the more specific case.

In the sequel, we shall work with a larger edge set S, which will amount to "glue many isogeny craters together", as shown in Figure 10.

11 Quaternionic multiplication

Supersingular curves are generally not covered by the theory of complex multiplication. For most of them, indeed, the Frobenius endomorphism acts like an element of $\mathbb{Z}$, instead of acting like a "complex multiplier".

Supersingular curves are defined by the fact that multiplication by p is purely inseparable, i.e., $E[p]$ is trivial. This implies that the curve $E^{(p^2)}$ is isomorphic to E, and thus that both are isomorphic to a curve defined over $\mathbb{F}_{p^2}$.

When E is defined over $\mathbb{F}_p$, we can still use what we know about complex multiplication. Indeed, these curves have trace 0, and thus the Frobenius endomorphism has two distinct eigenvalue $\pm\sqrt{-p}$, implying that $\mathrm{End}_{\mathbb{F}_p}(E)$, the ring of $\mathbb{F}_p$-rational endomorphisms, is isomorphic to an order in $\mathbb{Q}(\sqrt{-p})$.

When E is defined over $\mathbb{F}_{p^2}$, however,[6] its Frobenius endomorphism must satisfy $\pi^2 - t\pi + p^2 = 0$, with t a multiple of p; hence, by Hasse's theorem, $t \in \{0, \pm p, \pm 2p\}$. The cases $t \in \{0, \pm p\}$ only happen for a very limited number of curves with j-invariant 0 or 1728; we are thus mostly

[5] Said otherwise, any vertex could correspond to 1, and we do not know which.

[6] This also applies to curves defined over $\mathbb{F}_p$, when we extend scalars.

interested in the case $t = \pm 2p$, i.e., $\pi = \pm p$. Then, the *full* endomorphism ring $\mathrm{End}(E)$ (i.e., not restricted to $\mathbb{F}_p$-rational endomorphisms) is isomorphic to a maximal order the quaternion algebra $B_{p,\infty}$ ramified at p and at infinity.

Example 50. 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 does not commute with π. The full endomorphism ring is isomorphic to the order generated by π and ι inside the quaternion algebra $B_{p,\infty}$.

Like the CM case, isogenies are in correspondence with (left) ideals of $\mathcal{O}$. Unlike the CM case, $B_{p,\infty}$ has more than one maximal order, and there is no concept of *depth*, thus no ascending, descending or horizontal isogenies.

More precisely, let $\mathfrak{a} \subset B_{p,\infty}$ a lattice, the *left order* of $\mathfrak{a}$ is the ring $\mathcal{O}(\mathfrak{a}) = \{x \in B_{p,\infty} \mid x\mathfrak{a} \subset \mathfrak{a}\}$. Two lattices $\mathfrak{a}, \mathfrak{b}$ are said to be *right isomorphic* if $\mathfrak{a} = \mathfrak{b}x$ for some $x \in B_{p,\infty}$. If $\mathcal{O} \subset B_{p,\infty}$ is an order, $\mathfrak{a}$ is called a *left ideal* of $\mathcal{O}$ if $\mathcal{O} \subset \mathcal{O}(\mathfrak{a})$; the *left class set* $\mathrm{Cl}(\mathcal{O})$ is the set of right ideal classes of left ideals of $\mathcal{O}$. The order $\#\,\mathrm{Cl}(\mathcal{O})$ only depends on the quaternion algebra, and is called the *class number* of $B_{p,\infty}$. Analogous definitions can be given by swapping left and right; we refer to [19, Chapter 42] for more properties and definitions.

Like in the CM case, the set $\mathrm{Cl}(\mathcal{O})$ is in bijection with the vertex set of a supersingular graph.

Theorem 51. *Let $B_{p,\infty}$ be the quaternion algebra ramified at p and infinity, and let $\mathcal{O} \subset B_{p,\infty}$ be a maximal order. Let E_0/F_{p^2} be a supersingular elliptic curve with $\mathrm{End}(E_0) \simeq \mathcal{O}$.*

1. *The number of isomorphism classes of supersingular elliptic curves is equal to the class number of $B_{p,\infty}$.*

2. *There is a one-to-one correspondence $\mathfrak{a} \mapsto \mathfrak{a} \cdot E_0$ between $\mathrm{Cl}(\mathcal{O})$ and the set of isomorphism classes of supersingular elliptic curves, such that $\mathrm{End}(\mathfrak{a} \cdot E_0)$ is isomorphic to the right order of $\mathfrak{a}$.*

This theorem can be turned into an equivalence of categories, see [6, Theorem 45]. Thanks to the Eichler mass formula, we obtain the exact size of the isogeny class.

Corollary 52. *The number of isomorphism classes of supersingular elliptic curves is equal to*

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

We thus have a bound on the size of a supersingular isogeny graph over $\mathbb{F}_{p^2}$. Since the Frobenius acts like a scalar, all isogenies are defined over $\mathbb{F}_{p^2}$, hence supersingular ℓ-isogeny graphs are necessarily $(\ell + 1)$-regular. In the next section we will learn that the supersingular ℓ-isogeny graph has a unique connected component.

12 Expander graphs from isogenies

We are finally introducing two families of isogeny graphs suitable for cryptographic use. We will want them to somehow "behave like large random graphs", while at the same time having a strong algebraic structure: the first is needed for security, the second to produce complex protocols such as key exchange.

The random-like properties of isogeny graphs are typically expressed in terms of *expansion*. An undirected graph on n vertices has n real eigenvalues $\lambda_1 \geq \cdots \geq \lambda_n$, and, if the graph is k-regular, it can be proven that $k = \lambda_1 \geq \lambda_n \geq -k$. Because of this equality, λ_1 is called the *trivial eigenvalue*. An *expander graph* is a k-regular graph such that its non-trivial eigenvalues are bounded away, in absolute value, from k. We recall here some basic facts about expanders; for an in depth review, see [4, 17].

Definition 53 (Expander graph)**.** Let $\varepsilon > 0$ and $k \geq 1$. A k-regular graph 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 k-regular graphs 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.

Theorem 54 (Ramanujan graph)**.** *Let $k \geq 1$, and let G_i be a sequence of k-regular graphs. Then*

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

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

Two related properties of expander graphs are relevant to us. First, they have *short diameter*: as $n \to \infty$ the diameter of an expander is bounded by $O(\log n)$, with the constant depending only on k and ε. Second, expanders have *rapidly mixing walks*: loosely speaking, the next proposition says that random walks of length close to the diameter terminate on any vertex with probability close to uniform.

Proposition 55 (Mixing theorem ([5]))**.** *Let $G = (V, E)$ be a k-regular two-sided ε-expander. Let $F \subset V$ be any subset of the vertices of G, and let v be any vertex in V. Then a random walk of length at least*

$$\frac{\log(\#F^{1/2}/(2\#V))}{\log(1-\varepsilon)}$$

starting from v will land in F with probability at least $\#F/(2\#V)$.

The walk length in the mixing theorem is also called the *mixing length* of the expander graph.

Random regular graphs typically make good expanders, but only a handful of deterministic constructions is known, most of them based on Cayley graphs [10, 1, 4]. We just introduced Cayley graphs constructed from isogeny craters in Section 10, and, unsurprisingly, they turn out to be expanders, provided we add enough edges to them.

Theorem 56 (Jao, Miller, Venkatesan [5])**.** *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.

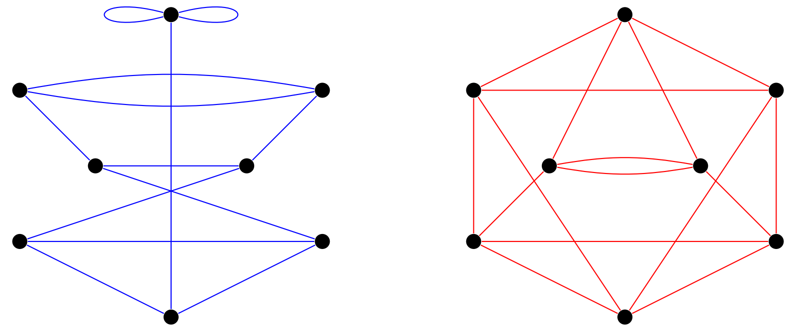


Figure 11: Supersingular isogeny graphs of degree 2 (left, blue) and 3 (right, red) on $\mathbb{F}_{97^2}$.

The theorem is readily generalized to supersingular curves and isogenies defined over $\mathbb{F}_p$.

A radically different construction of expander graphs is given by graphs of supersingular curves *defined over* $\mathbb{F}_{p^2}$ with ℓ-isogenies, for a *single* prime $\ell \neq p$. Two examples of such graphs are shown in Figure 11. This construction is related to LPS graphs [10, 9, 2], but is not isomorphic to a Cayley graph.

Theorem 57 (Mestre [11], Pizer [13, 14])**.** *Let $\ell \neq p$ be two primes. The ℓ-isogeny graph of supersingular curves in $\bar{\mathbb{F}}_p$, is connected, $(\ell+1)$-regular, and has the Ramanujan property.*

Both of these isogeny graphs will be used in the next part to build key exchange protocols. For reasons that will be apparent soon, there will only be a mild connection between the expansions properties of the graphs and the security of the protocols: the expansion theorems will mostly serve as a blueprint for devising good cryptosystems, but will have no provable impact.

Exercises

Exercise II.1. Prove Corollary 43.

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. 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

Key exchange

Part IV
Signatures, other protocols, open problems

References

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

[2] Anamaria Costache, Brooke Feigon, Kristin Lauter, Maike Massierer, and Anna Puskas. Ramanujan graphs in cryptography. Cryptology ePrint Archive, Report 2018/593, 2018.

[3] 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.

[4] Oded Goldreich. *Basic Facts about Expander Graphs*, pages 451–464. Springer Berlin Heidelberg, Berlin, Heidelberg, 2011.

[5] 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.

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

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

[8] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics.* Springer-Verlag, 1994.

[9] Alexander Lubotzky. *Discrete groups, expanding graphs and invariant measures*, volume 125 of *Progress in Mathematics.* Birkhäuser Verlag, Basel, 1994.

[10] Alexander Lubotzky, Ralph Phillips, and Peter Sarnak. Ramanujan graphs. *Combinatorica*, 8(3), 1988.

[11] 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.

[12] Jürgen Neukirch. *Algebraic number theory*, volume 322. Springer Verlag, 1999.

[13] Arnold K. Pizer. Ramanujan graphs and Hecke operators. *Bulletin of the American Mathematical Society (N.S.)*, 23(1), 1990.

[14] 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.

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

[16] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, volume 151 of *Graduate Texts in Mathematics.* Springer, January 1994.

[17] Terence Tao. Expansion in groups of Lie type – basic theory of expander graphs, 2011.

[18] Jacques Vélu. Isogénies entre courbes elliptiques. *Comptes Rendus de l'Académie des Sciences de Paris*, 273:238–241, 1971.

[19] John Voight. Quaternion algebras, 2018.