Mathematics of Isogeny Based Cryptography

Luca De Feo
Université de Versailles & Inria Saclay
http://defeo.lu/

École mathématique africaine
May 10 – 23, 2017, Thiès, Senegal

Introduction

These lectures notes were written for a summer school on *Mathematics for Post-quantum cryptography* in Thiès, Senegal. They try to provide a guide for Masters' students to get through the vast literature on elliptic curves, without getting lost on their way to learning isogeny-based cryptography. They are by no means a reference text on the theory of elliptic curves, nor on cryptography; students are encouraged to complement these notes with some of the books recommended in the bibliography.

The presentation is divided in three parts, roughly corresponding to the three lectures given. In an effort to keep the reader interested, each sections alternates between the fundamental theory of elliptic curves, and applications in cryptography. We often prefer to have the main ideas flow smoothly, rather than having a rigorous presentation as one would have in a more classical book. The reader will excuse us for the inaccuracies and the omissions.

Isogeny Based Cryptography is a very young field, that has only begun in the 2000s. It has its roots in *Elliptic Curve Cryptography* (ECC), a somewhat older branch of public-key cryptography that was started in the 1980s, when Miller and Koblitz first suggested to use elliptic curves inside the Diffie-Hellman key exchange protocol (see Section 4).

ECC only started to gain traction in the 1990s, after Schoof's algorithm made it possible to easily find elliptic curves of large prime order. It is nowadays a staple in public-key cryptography. The 2000s have seen two major innovations in ECC: the rise of *Pairing Based Cryptography* (PBC), epitomized by Joux' one-round tripartite Diffie-Hellman key exchange, and the advent of Isogeny-based cryptography, initiated by the works of Teske and Rostovtsev & Stolbunov. While PBC has attracted most of the attention during the first decade, thanks to its revolutionary applications, isogeny based cryptography has stayed mostly discrete during this time. It is only in the second half of the 2010 that the attention has partly shifted to isogenies. The main reason for this is the sudden realization by the cryptographic community of the very possibly near arrival of a *general purpose quantum computer*. While the capabilities of such futuristic machine would render all ECC and PBC suddenly worthless, isogeny based cryptography seems to resist much better to the cryptanalytic powers of the quantum computer.

In these notes, after a review of the general theory of elliptic curves and isogenies, we will present the most important isogeny-based systems, and their cryptographic properties.

Contents

Part I
Elliptic curves and cryptography

Throughout this section we let k be a field, and we denote by $\bar{k}$ its algebraic closure. We review the basic theory of elliptic curves, and two classic applications in cryptography. The interested reader will find more details on elliptic curves in [24], and on their use in cryptography in [12, 9].

1 Elliptic curves

Elliptic curves are projective curves of genus 1 having a specified base 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 *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 *space 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 [24, Chap. III].

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

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

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

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

It is customary to write Eq. (1) in *affine form.* By defining the 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 $\mathcal{O} = (0 : 1 : 0)$.

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 $(0 : 1 : 0)$.

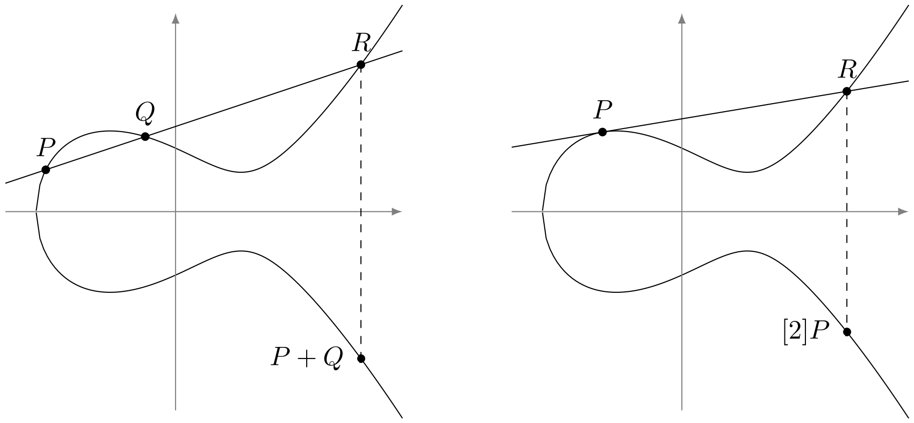


Figure 1: An elliptic curve defined over $\mathbb{R}$, and the geometric representation of its group law.

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
$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2, \\ y_3 &= -\lambda x_3 - y_1 + \lambda x_1. \end{aligned}$$

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

Proof. See [24, Coro. 6.4]. For the characteristic 0 case see also next section. □

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*.

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 tracked 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[24, III, Th. 4.8]. □

Two curves are called *isogenous* if there exists an isogeny between them. We shall see in the next section 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 $E[m]$. For most elliptic curves, this is the end of the story: the only endomorphisms are the scalar multiplications. We shall however see some non-trivial endomorphisms soon.

3 Elliptic curves over finite fields

From now on we let E be an elliptic curve defined over a finite field k with q elements. 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.

Curves over finite fields always have a non-trivial endomorphism.

Definition 8 (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 9. *Let π be the Frobenius endomorphism of E. Then:*

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

Corollary 10 (Hasse's theorem)**.** *Let E be an elliptic curve defined over a finite field k with q elements, then*

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

Proof. See[24, V, Th. 1.1]. □

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 a special case of the famous *Weil's conjectures*, proven by Weil himself in 1949 for Abelian varieties, and more generally by Deligne in 1973.

Definition 11. 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 12. *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 [24, V, Th. 2.4]. □

We conclude with a theorem that links the isogenies between two elliptic curves with their Frobenius endomorphisms.

Theorem 13 (Sato-Tate)**.** *Two elliptic curves E, E' defined over a finite field k are isogenous over k if and only if $\#E(k) = \#E'(k)$.*

4 Application: Diffie-Hellman key exhange

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

The original protocol was invented in the 1970s by Whitfield Diffie and Martin Hellman [6], and constitutes the first practical example of *public key cryptography.* The two communicating parties are customarily called *Alice* and *Bob*, and the listening third party is represented by the character *Eve* (for *eavesdropper*). To set up the protocol, Alice and Bob agree on a set of public parameters:

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

Then, Alice and Bob perform the following steps:

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

The protocol can be easily generalized by replacing the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ with any other cyclic group $G = \langle g \rangle$. From Eve's point of view, she is given the knowledge of the group G, the generator g, and Alice's and Bob's public data $A, B \in G$; her goal is to recover the shared secret g^{ab}. This is mathematically possible, but not necessarily *easy* from a computational point of view.

Definition 14 (Discrete logarithm)**.** Let G be a cyclic group generated by an element g. For any element $A \in G$, we define the *discrete logarithm of A in base g*, denoted $\log_g(A)$, as the unique integer in the interval $[0, \#G[$ such that

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

It is evident that if Eve can compute discrete logarithms in G, then she can compute the shared secret; the converse is not true in general, but it is widely believed to be. Thus, the strength of the Diffie-Hellman protocol is entirely dependent on the *hardness* of the *discrete logarithm problem* in the group G.

We know algorithms to compute discrete logarithms in a *generic* group G that require $O(\sqrt{q})$ computational steps (see [12]), where q is the largest prime divisor of $\#G$; we also know that these algorithms are *optimal for abstract cyclic groups.* For this reason, G is usually chosen so that the largest prime divisor q has size at least $\log_2 q \approx 256$. However, the proof of optimally does not exclude the existence of better algorithms for *specific* groups G. And indeed, algorithms of complexity better than $O(\sqrt{\#G})$ are known for the case $G = (\mathbb{Z}/p\mathbb{Z})^\times$ [12], thus requiring parameter of considerably larger size to guarantee cryptographic strength.

On the contrary, no algorithms better than the generic ones are known when G is a subgroup of $E(k)$, where E is an elliptic curve defined over a finite field k. This has led Miller [17] and Koblitz [13] to suggest, in the 1980s, to replace $(\mathbb{Z}/p\mathbb{Z})^\times$ in the Diffie-Helman protocol by the group of rational points of an elliptic curve of (almost) prime order over a finite field. The resulting protocol is summarized in Figure 2.

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

Figure 2: The Diffie-Hellman protocol over elliptic curves

5 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 [15] 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 whose 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 3a. 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 3b. 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,

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

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

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

(b) Lenstra's ECM algorithm

Figure 3: The $(p - 1)$ and ECM factorization algorithms

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 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.

Exercices

Exercice I.1. Prove Proposition 6.

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

Exercice I.3. Prove Proposition 9.

Exercice I.4. Using Proposition 12, devise an algorithm to effectively compute $\#E(\mathbb{F}_{q^n})$ given $\#E(\mathbb{F}_q)$.

Exercice I.5. Implement the ECDH key exchange in the language of your choice.

Exercice I.6 (Polig-Hellman algorithm)**.** Let G be a cyclic group of order $N = pq$, generated by an element g. Show how to solve discrete logarithms in G by computing two separate discrete logarithms in the subgroups $\langle g^p \rangle$ and $\langle g^q \rangle$.

Exercice I.7. Implement the ECM factorization method in the language of your choice.

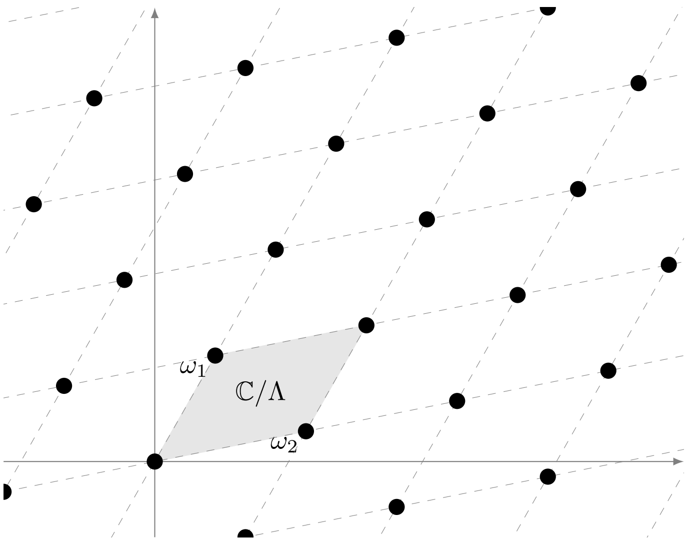


Figure 4: A complex lattice (black dots) and its associated complex torus (grayed *fundamental domain*).

Part II
Isogenies and applications

6 Elliptic curves over $\mathbb{C}$

Definition 15 (Complex lattice)**.** A complex lattice Λ is a discrete subgroup of $\mathbb{C}$ that contains an $\mathbb{R}$-basis.

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 16. *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 [25, I, Lem. 2.4]. □

Definition 17 (Complex tours)**.** Let Λ be a complex lattice, the quotient $\mathbb{C}/\Lambda$ is called a *complex torus.*

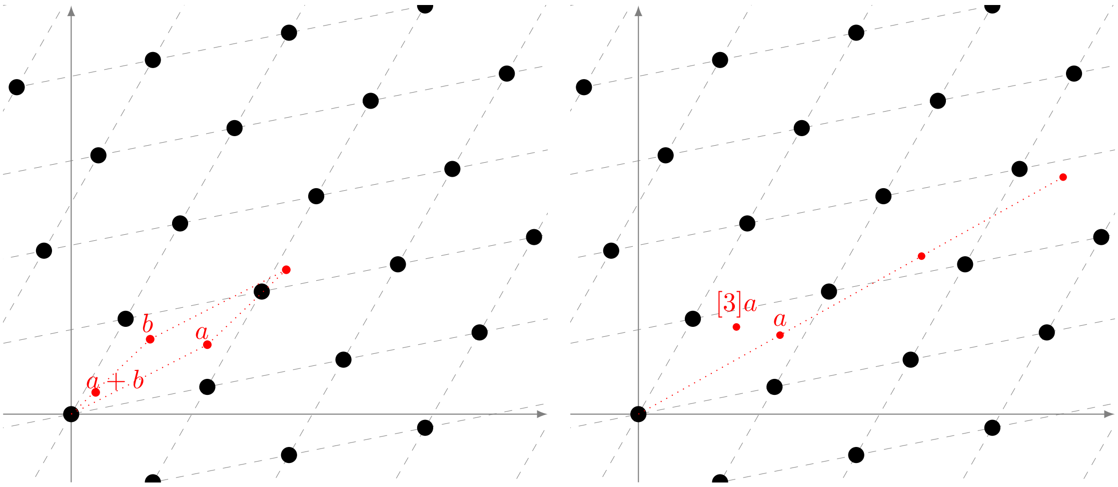


Figure 5: Addition (left) and scalar multiplication (right) of points in a complex torus $\mathbb{C}/\Lambda$.

A convex set of class representatives of $\mathbb{C}/\Lambda$ is called a *fundamental parallelogram.* Figure 4 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 5.

Definition 18 (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 19 (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 [25, 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 20 (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 21. *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 [24, 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 homotety class of complex tori, we have a corresponding isomorphism class of elliptic curves. The converse is also true.

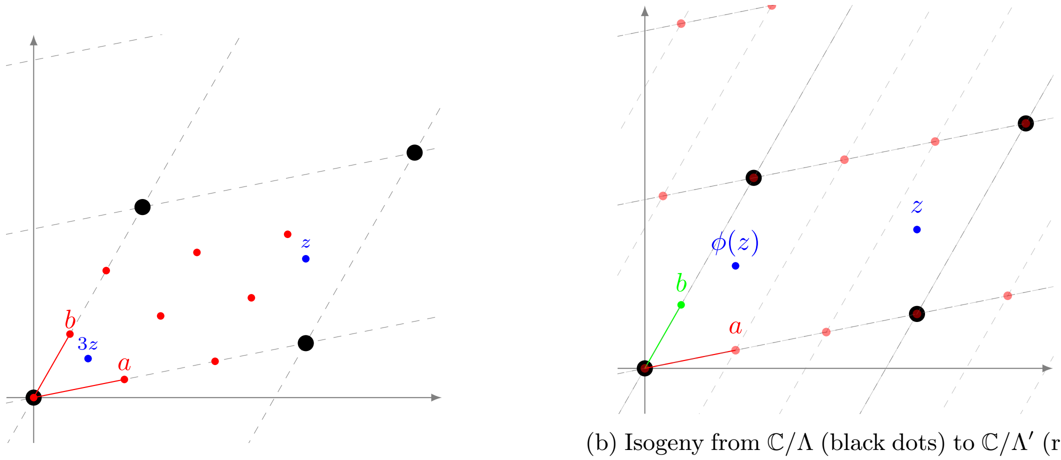
Theorem 22 (Uniformization theorem)**.** *Let $a, b \in \mathbb{C}$ be such that $4a^3 + 27b^2 \neq 0$, then there is a unique complex lattice Λ such that $g_2(\Lambda) = -4a$ and $g_3(\Lambda) = -4b$.*

Proof. See [25, 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 6a; in the picture wee see two lattices Λ and Λ', generated respectively by the black and the red dots. The multiplication-by-m map corresponds then to

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

and we verify that it is and endomorphism because Λ and Λ' are homothetic.



(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 6: Maps between complex tori.

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 6a: 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 23. *Let E, E' be elliptic curves over $\mathbb{C}$, with corresponding lattices Λ, Λ'. There is a bijection between the group of isogenies from E to E' and the group of maps ϕ_α for all α such that $\Lambda \subset \alpha\Lambda'$.*

Proof. See [24, VI, Th. 4.1]. □

Looking again at Figure 6a, 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 for any base field.

We finish this section by summarizing the most important algebraic properties of isogenies; we start with a technical definition.

Definition 24 (Degree)**.** 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.
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 [24, 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.

Theorem 25 (Dual isogeny)**.** *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. *$\hat{\phi}$ is defined over k if and only if ϕ is;*
2. *$\widehat{\psi \circ \phi} = \hat{\phi} \circ \hat{\psi}$ for any isogeny $\psi : E' \to E''$;*
3. *$\widehat{\psi + \phi} = \hat{\psi} + \hat{\phi}$ for any isogeny $\psi : E \to E'$;*
4. *$\deg \phi = \deg \hat{\phi}$;*
5. *$\hat{\hat{\phi}} = \phi$.*

7 The endomorphism ring

We have already defined an endomorphism as an isogeny from a curve to itself. If we add the multiplication-by-0, the set of all endomorphisms of E form a ring under the operations of addition and composition, denoted by $\mathrm{End}(E)$.

We have already seen that the multiplication-by-m is a different endomorphism for any integer m, thus $\mathbb{Z} \subset \mathrm{End}(E)$. For the case of finite fields, we have also learned about the Frobenius endomorphism π; so certainly $\mathbb{Z}[\pi] \subset \mathrm{End}(E)$ in this case. We shall now give a complete characterization of the endomorphism ring for any field.

Definition 26 (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 of maximal dimension.

The prototypical example of order is the ring of integers $\mathcal{O}_K$ of a number field K, i.e., the ring of all elements of K such that their monic minimal polynomial has coefficients in $\mathbb{Z}$. It turns out that $\mathcal{O}_K$ is the *maximal order* of K, i.e., it contains any other order of K.

Definition 27 (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 28 (Deuring)**.** *Let E be an elliptic curve defined over a field k of characteristic p. The ring* End(E) *is isomorphic to one of the following:*

- $\mathbb{Z}$*, only if* $p = 0$*;*
- *An order 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*;*
- *Only if* $p > 0$*, a maximal order in the quaternion algebra ramified at* p *and* ∞*; in this case we say that* E *is* supersingular*.*

Proof. See [24, III, Coro. 9.4] and [1]. □

In positive characteristic, a curve that is not supersingular is called *ordinary*; it necessarily has complex multiplication. We focus again on the finite field case; we have already seen that $Z[\pi] \subset \mathrm{End}(E)$. Now, Hasse's theorem can be made more precise as follows.

Theorem 29. *Let E be an elliptic curve defined over a finite field. Its Frobenius endomorphism π satisfies a quadratic equation*

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

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

Proof. See [24, 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 $\#E = q + 1 - t$. Now, if we let $D_\pi = t^2 - 4q < 0$, we verify that $\pi \in \mathbb{Q}[\sqrt{D_\pi}]$; so, at least in the ordinary case, we can affirm that

$$\mathbb{Z}[\pi] \subset \mathrm{End}(E) \subset \mathcal{O}_K,$$

where $K = \mathbb{Q}[\sqrt{D_\pi}]$ is called the *endomorphism algebra* of E. The structure of the orders of K is very simple in this case.

Proposition 30. *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 d_K is the* discriminant *of K, the discriminant of $\mathcal{O}$ is $f^2 d_K$.*

If $\mathcal{O}, \mathcal{O}'$ are two orders of discriminants f, f', then $\mathcal{O} \subset \mathcal{O}'$ if and only if $f'|f$.

In our case, we can write $D_\pi = f^2 d_K$, with d_K squarefree. Then, any order $\mathbb{Z}[\pi] \subset \mathcal{O} \subset \mathcal{O}_K$ has conductor dividing f.

8 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 [22]. 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 31 (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

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

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 [23]. 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 E' corresponding to, e.g., $\langle P\rangle$, then we can compute the isogeny $\phi : E \to E'$, 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 $\langle P\rangle$ we 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 [23, 16, 7, 26].

9 Isogeny graphs

We now look at the graph structure that isogenies create on the set of j-invariants defined over a finite field. We start with an easy generalization of the Sato-Tate theorem 13.

Theorem 32 (Sato-Tate)**.** *Two elliptic curves E, E' are isogenous if and only if their endomorphisms algebras $\mathrm{End}(E) \otimes \mathbb{Q}$ and $\mathrm{End}(E') \otimes \mathbb{Q}$ are isomorphic.*

An equivalence class of isogenous elliptic curves is called an *isogeny class*. In particular, we see that it is impossible for an isogeny class to contain both ordinary and supersingular curves. When we restrict to isogenies of a prescribed degree ℓ, we say that two curves are ℓ-isogenous; by the dual isogeny theorem, this too is an equivalence relation. Remark that if E is ℓ-isogenous to E', and if E'' is isomorphic to E', then by composition E and E'' are also ℓ-isogenous.

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.

Definition 33 (Isogeny graph)**.** An *isogeny graph* is a (multi)-graph whose nodes 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 7 shows a typical example of isogeny graph, where we restrict to isogenies of degree 3.

The classification of isogeny graphs was initiated by Pizer [20, 21] 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 [8]. We start with some generalities.

Proposition 34. *Let $E : y^2 = x^3 + ax + b$ be an elliptic curve defined over a finite field k of characteristic p, and let $\ell \neq p$ be a prime.*

1. *There are $\ell + 1$ distinct isogenies of degree ℓ with domain E defined over the algebraic closure $\bar{k}$.*

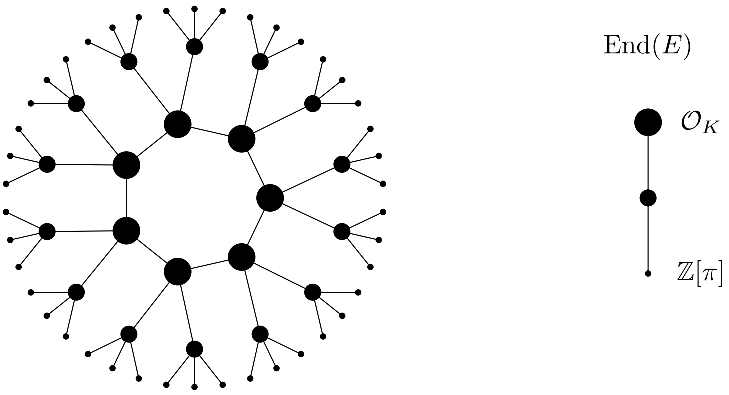


Figure 7: A volcano of 3-isogenies (ordinary elliptic curves, Elkies case), and the correspond tower of orders inside the endomorphism algebra.

2. *There are* $0, 1, 2$ *or* $\ell + 1$ *isogenies of degree* ℓ *with domain* E *defined over* k*.*
3. *If* E *is ordinary, there is a unique separable isogeny of degree* p *with domain* E*; there are none if* E *is supersingular.*
4. *The map* $(x, y) \mapsto (x^p, y^p)$ *is a purely inseparable isogeny of degree* p *from* E *to* $E^{(p)} : y^2 = x^3 + a^p x + b^p$*.*

There are many differences between the structure of isogeny graphs of ordinary curves and those of supersingular ones. We focus here on the ordinary case, and we leave the supersingular one for the last section.

Proposition 35 (Horizontal and vertical isogenies)**.** *Let* $\phi : E \to E'$ *be an isogeny of prime degree* ℓ*, and let* $\mathcal{O}, \mathcal{O}'$ *be the orders corresponding to* E, E'*. Then, either* $\mathcal{O} \subset \mathcal{O}'$ *or* $\mathcal{O}' \subset \mathcal{O}$*, and one of the following is true:*

- $\mathcal{O} = \mathcal{O}'$*, in this case* ϕ *is said to* horizontal*;*
- $[\mathcal{O}' : \mathcal{O}] = \ell$*, in this case* ϕ *is said to be* ascending*;*
- $[\mathcal{O} : \mathcal{O}'] = \ell$*, in this case* ϕ *is said to be* descending.

Proof. See [14, Prop. 21]. □

Observe that vertical isogenies can only exist for primes that divide the conductor of $\mathbb{Z}[\pi]$, so the horizontal case is the generic one. Like we did for the SEA algorithm we can further distinguish three cases, depending on the value of the Legendre symbol $\left(\frac{D}{\ell}\right)$, i.e., depending on whether π splits (Elkies case), is inert (Atkin case), or ramifies modulo ℓ. All possible cases are encoded in the following proposition.

Proposition 36. *Let* E *be an elliptic curve over a finite field* k*. Let* $\mathcal{O}$ *its endomorphism ring,* f *its conductor,* D *its discriminant,* π *the Frobenius endormphism,* f_π *the conductor of* $\mathbb{Z}[\pi]$*. Let* ℓ *be a prime different from the characteristic of* k*, then the types of degree* ℓ *isogenies with domain* E *are as follows:*

- *If* $\ell | f$ *and* $\ell \nmid (f_\pi / f)$*, there is one ascending isogeny;*

- *If $\ell | f$ and $\ell | (f_\pi / f)$, there is one ascending isogeny and ℓ descending ones;*
- *If $\ell \nmid f$ and $\ell \nmid (f_\pi / f)$, there are $1 + \left(\frac{D}{\ell}\right)$ horizontal isogenies, where $\left(\frac{D}{\ell}\right)$ represents the Legendre symbol;*
- *If $\ell \nmid f$ there are $1 + \left(\frac{D}{\ell}\right)$ horizontal isogenies, plus $\ell - \left(\frac{D}{\ell}\right)$ descending isogenies only if $\ell | (f_\pi / f)$.*

Proof. See [14, Prop. 21]. □

Putting the pieces together, we see that graphs of ordinary curves have a very rigid structure: a cycle of horizontal isogenies (Elkies case), possibly reduced to one point (Atkin case), or to two points (ramified case); and a tree of descending isogenies of height $v_\ell(f_\pi)$ (the ℓ-adic valuation of the conductor of π). Such graphs are called *isogeny volcanoes* for obvious reasons (have a look at Figure 7).

The action of π on $E[\ell]$, or more generally on $E[\ell^k]$ for k large enough, can be used to determine even more precisely which isogenies are ascending, descending or horizontal. We will not give details here, but see [19, 18, 10, 11, 5].

10 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 [2] and then slightly generalized in [4]. 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 whose 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 Exercice II.8). 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 [27].

Proposition 37 (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 $\phi : E \to E'$ 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' has equation $y^2 = x^3 + a'x + b'$, where

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

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

Proof. See [3, §8.2]. □

Corollary 38. *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 [3, §8.2]. □

The Couveignes-Lercier algorithm is summarized in Figure 8. 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.

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

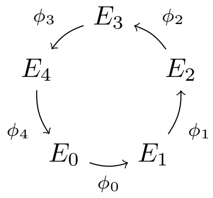


Figure 8: Couveignes-Lercier algorithm to compute irreducible polynomials, and structure of the computed isogeny cycle.

Exercices

Exercice II.1. Prove Lemma 16.

Exercice II.2. Prove that y divides the m-th division polynomial ψ_m if and only if m is even, and that no division polynomial is divisible by y^2.

Exercice II.3. Using the Sato-Tate theorem 32, prove that two curves are isogenous if and only if they have the same number of points.

Exercice II.4. Prove Propostion 34.

Exercice II.5. Prove that the dual of a horizontal isogeny is horizontal, and that the dual of a descending isogeny is ascending.

Exercice II.6. Prove that the height of a volcano of ℓ-isogenies is $v_\ell(f_\pi)$, the ℓ-adic valuation of the Frobenius endomorphism.

Exercice II.7. 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 $v_\ell(\lambda - \mu)$.

Exercice II.8. Prove that $E[\ell] \subset E(\mathbb{F}_q)$ implies $\ell | (q-1)$.

Part III
Isogeny based cryptography

References

[1] Juliana V. Belding. *Number Theoretic Algorithms for Elliptic Curves.* PhD thesis, University of Maryland, 2008.

[2] Jean-Marc Couveignes and Reynald Lercier. Fast construction of irreducible polynomials over finite fields. *To appear in the Israel Journal of Mathematics*, July 2011.

[3] Luca De Feo. *Algorithmes Rapides pour les Tours de Corps Finis et les Isogénies.* PhD thesis, Ecole Polytechnique X, December 2010.

[4] Luca De Feo, Javad Doliskani, and Éric Schost. Fast algorithms for ℓ-adic towers over finite fields. In *ISSAC'13*, pages 165–172. ACM, 2013.

[5] Luca De Feo, Cyril Hugounenq, Jérôme Plût, and Éric Schost. Explicit isogenies in quadratic time in any characteristic. *LMS Journal of Computation and Mathematics*, 19(A):267–282, 2016.

[6] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644–654, 1976.

[7] 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.

[8] 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.

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

[10] Sorina Ionica and Antoine Joux. Pairing the volcano. In *ANTS*, pages 201–218, 2010.

[11] Sorina Ionica and Antoine Joux. Pairing the volcano. *Mathematics of Computation*, 82(281):581–603, 2013.

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

[13] Neal Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, 48(177):203–209, 1987.

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

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

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

[17] Victor S. Miller. Use of elliptic curves in cryptography. In *Lecture notes in computer sciences; 218 on Advances in cryptology–CRYPTO 85*, pages 417–426, New York, NY, USA, 1986. Springer-Verlag New York, Inc.

[18] Josep M. Miret, R. Moreno, Daniel Sadornil, Juan Tena, and Magda Valls. An algorithm to compute volcanoes of 2-isogenies of elliptic curves over finite fields. *Applied Mathematics and Computation*, 176(2):739–750, 2006.

[19] Josep M. Miret, Ramiro Moreno, Ana Rio, and Magda Valls. Determining the 2-sylow subgroup of an elliptic curve over a finite field. *Mathematics of Computation*, 74(249):411–427, 2005.

[20] Arnold K. Pizer. Ramanujan graphs and Hecke operators. *Bull. Amer. Math. Soc. (N.S.)*, 23(1), 1990.

[21] 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.

[22] René Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Math. Comp.*, 44(170):483–494, 1985.

[23] René Schoof. Counting points on elliptic curves over finite fields. *Journal de Théorie des Nombres de Bordeaux*, 7(1):219–254, 1995.

[24] Joseph H. Silverman. *The Arithmetic of Elliptic Curves.* Number 106 in Graduate Texts in Mathematics. Springer, 1986.

[25] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves (Graduate Texts in Mathematics).* Springer, January 1994.

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

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