

Isogeny graphs in cryptography

Luca De Feo

Université Paris Saclay, UVSQ

March 18, 2019

Mathematical foundations of asymmetric cryptography
Aussois, Savoie

Slides online at <https://defeo.lu/docet/>

Overview

1 Isogeny graphs

- Elliptic Curves
- Isogenies
- Isogeny graphs
- Endomorphism rings
- Ordinary graphs
- Supersingular graphs

2 Cryptography

- Isogeny walks and Hash functions
- Pairing verification and Verifiable Delay Functions
- Key exchange
- Proofs of knowledge and Signatures
- Open Problems

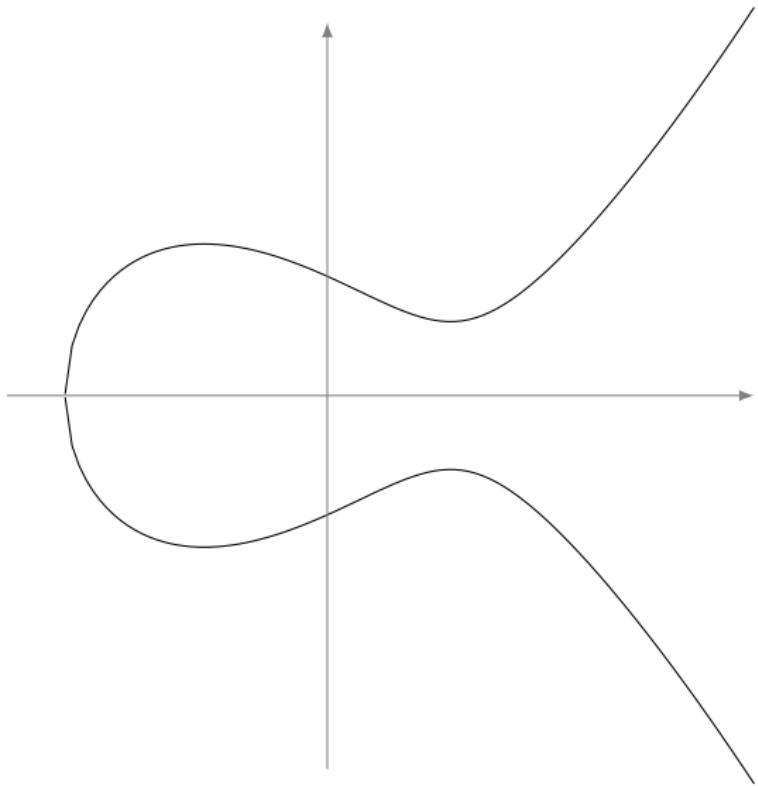
Elliptic curves

Let k be a field of characteristic $\neq 2, 3$.

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

$$Y^2Z = X^3 + aXZ^2 + bZ^3,$$

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



Elliptic curves

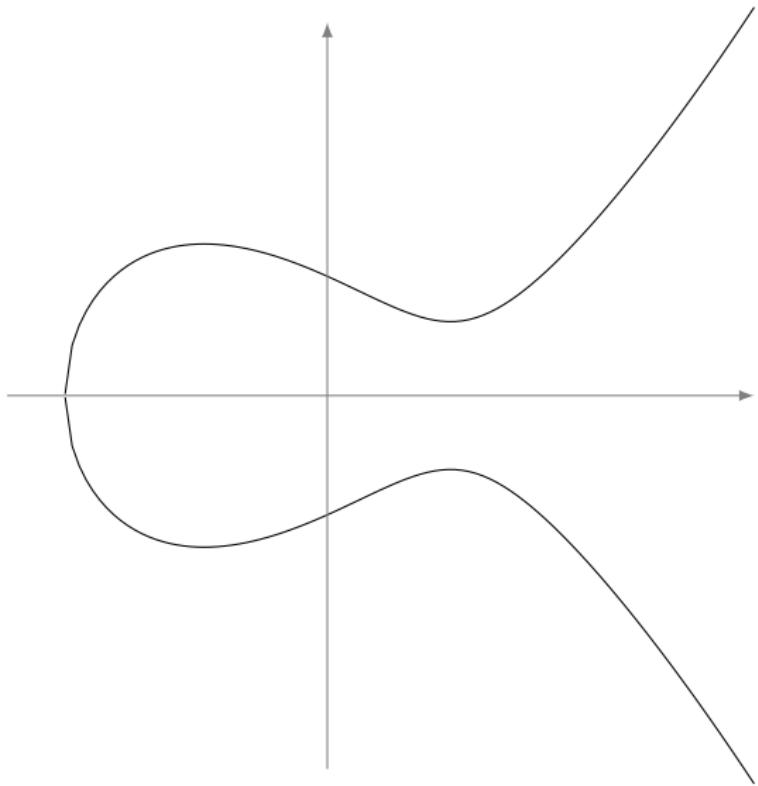
Let k be a field of characteristic $\neq 2, 3$.

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

$$Y^2Z = X^3 + aXZ^2 + bZ^3,$$

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

- $\mathcal{O} = (0 : 1 : 0)$ is the point at infinity;



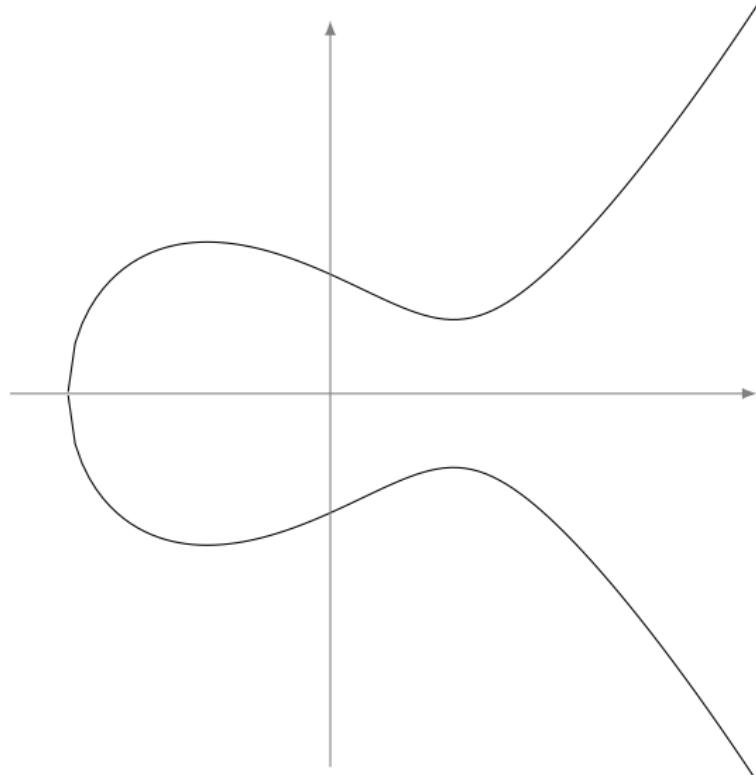
Elliptic curves

Let k be a field of characteristic $\neq 2, 3$.

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

$$Y^2Z = X^3 + aXZ^2 + bZ^3,$$

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



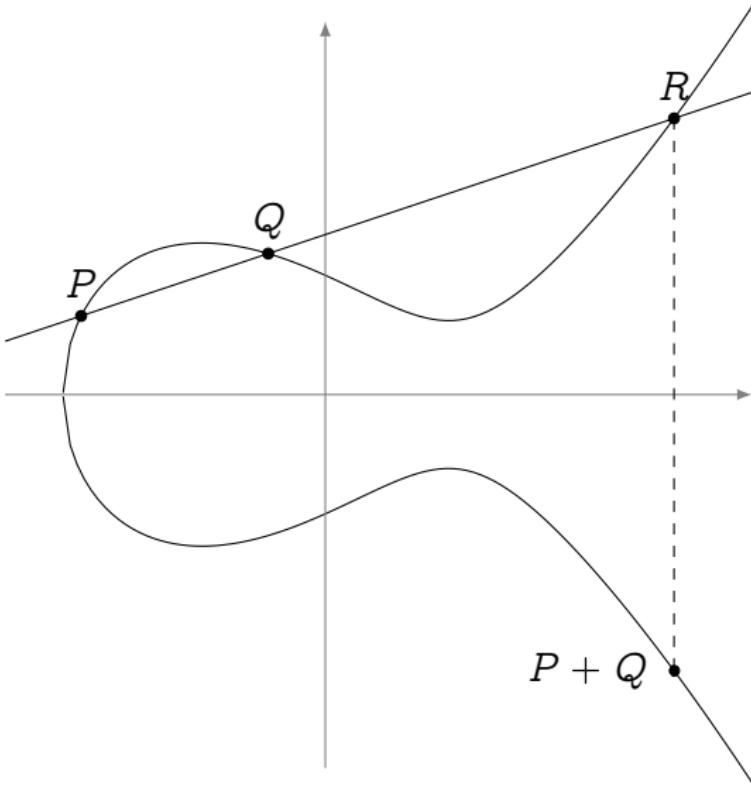
- $\mathcal{O} = (0 : 1 : 0)$ is the point at infinity;
- $y^2 = x^3 + ax + b$ is the affine Weierstrass equation.

The group law

Bezout's theorem

Every line cuts E in exactly three points (counted with multiplicity).

Define a [group law](#) such that any three colinear points add up to zero.



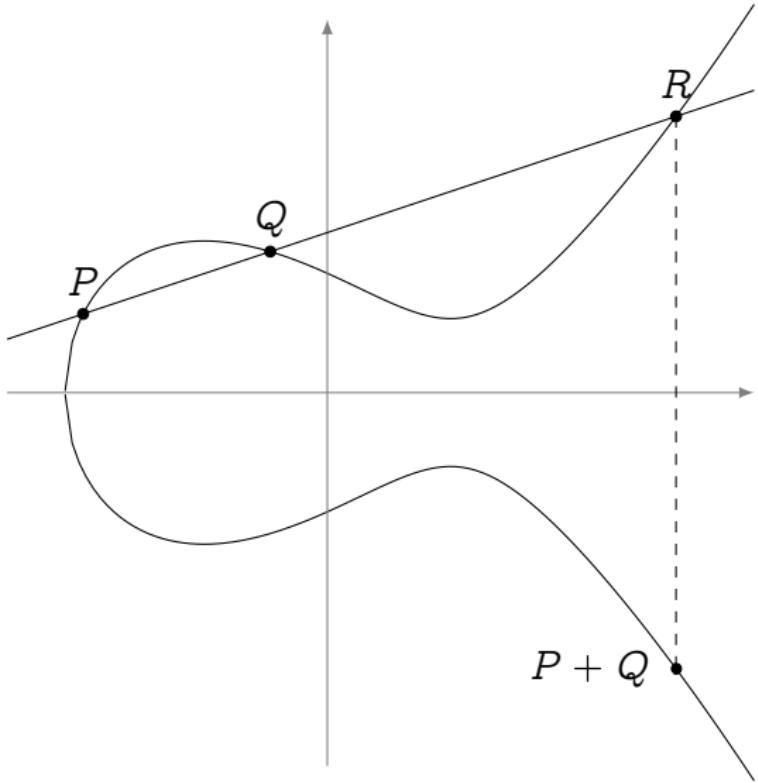
The group law

Bezout's theorem

Every line cuts E in exactly three points (counted with multiplicity).

Define a **group law** such that any three colinear points add up to zero.

- The law is **algebraic** (it has *formulas*);



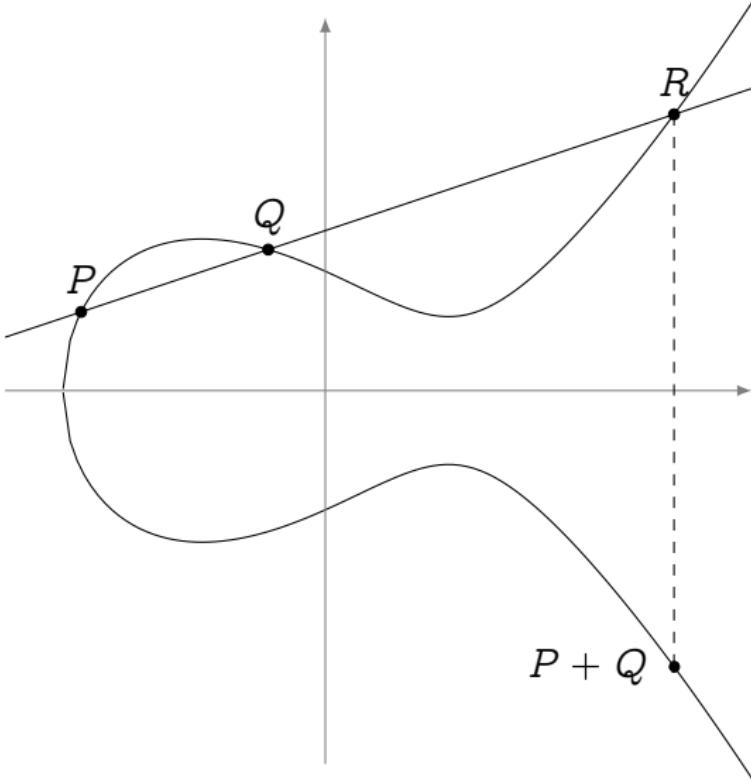
The group law

Bezout's theorem

Every line cuts E in exactly three points (counted with multiplicity).

Define a **group law** such that any three colinear points add up to zero.

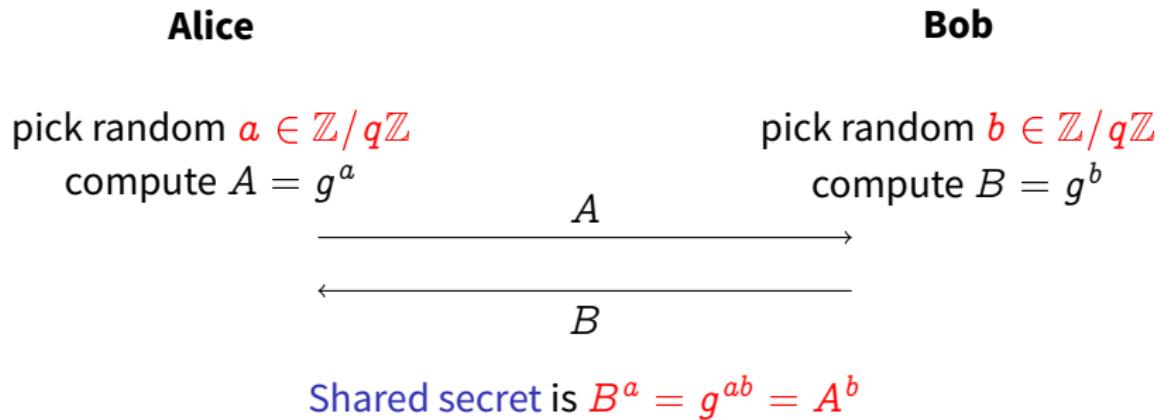
- The law is **algebraic** (it has *formulas*);
- The law is **commutative**;
- \mathcal{O} is the **group identity**;
- **Opposite points** have the same x -value.



Why should I care? (Diffie–Hellman key exchange)

Goal: Alice and Bob have never met before. They are chatting over a public channel, and want to agree on a **shared secret** to start a private conversation.

Setup: They agree on a (large) cyclic group $G = \langle g \rangle$ of (prime) order q .



Brief history of DH key exchange

- 1976 Diffie & Hellman publish [New directions in cryptography](#), suggest using $G = \mathbb{F}_p^*$.
- 1978 Pollard publishes his [discrete logarithm](#) algorithm ($O(\sqrt{\#G})$ complexity).
- 1980 Miller and Koblitz independently suggest using [elliptic curves](#) $G = E(\mathbb{F}_p)$.
- 1994 Shor publishes his quantum polynomial time [discrete logarithm / factoring](#) algorithm.
- 2005 NSA standardizes elliptic curve key agreement (ECDH) and signatures ECDSA.
- 2017 ~ 70% of web traffic is secured by ECDH and/or ECDSA.
- 2017 NIST launches [post-quantum competition](#), says “not to bother moving to elliptic curves, if you haven’t yet”.

Why should I care? (cont'd)

But, also:

- Elliptic Curve Factoring Method (Lenstra '85);
- Elliptic Curve Primality Proving (Atkin, Morain '86-'93);
- Efficient normal bases for finite fields (Couveignes, Lercier '10);
- ...

What are elliptic curves?

For mathematicians

- The smooth projective curves of genus 1;
- The simplest abelian varieties (dimension 1);
- Finitely generated abelian groups of mysterious free rank (aka BSD conjecture);
- What you use to make examples.

What are elliptic curves?

For mathematicians

- The smooth projective curves of genus 1;
- The simplest abelian varieties (dimension 1);
- Finitely generated abelian groups of mysterious free rank (aka BSD conjecture);
- What you use to make examples.

For cryptographers

- Finite abelian groups (often cyclic);
- Easy to compute the order;
- “2-dimensional” generalizations of μ_k (the roots of unity of k)...
- ...with bilinear maps (aka pairings)!

Isomorphisms

Isomorphisms

The only invertible algebraic maps between elliptic curves are of the form

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

for some $u \in \bar{k}$.

They are group isomorphisms.

j -Invariant

Let $E : y^2 = x^3 + ax + b$, its j -invariant is

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

Two elliptic curves E, E' are isomorphic if and only if $j(E) = j(E')$.

Group structure

Torsion structure

Let E be defined over an algebraically closed field \bar{k} of characteristic p .

$$E[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \quad \text{if } p \nmid m,$$

$$E[p^e] \simeq \begin{cases} \mathbb{Z}/p^e\mathbb{Z} & \text{ordinary case,} \\ \{\mathcal{O}\} & \text{supersingular case.} \end{cases}$$

Finite fields (Hasse's theorem)

Let E be defined over a finite field \mathbb{F}_q , then

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

In particular, there exist integers n_1 and $n_2 | (q - 1)$ such that

$$E(\mathbb{F}_q) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}.$$

What is scalar multiplication?

$$[n] : P \mapsto \underbrace{P + P + \cdots + P}_{n \text{ times}}$$

- A map $E \rightarrow E$,
- a group morphism,
- with finite kernel
(the torsion group $E[n] \simeq (\mathbb{Z}/n\mathbb{Z})^2$),
- surjective (in the algebraic closure),
- given by rational maps of degree n^2 .

What is scalar multiplication by an isogeny?

$$[n] : P \mapsto \underbrace{P + P + \cdots + P}_{n \text{ times}}$$

- A map $E \rightarrow E$,
- a group morphism,
- with finite kernel
(the torsion group $E[n] \simeq (\mathbb{Z}/n\mathbb{Z})^2$),
- surjective (in the algebraic closure),
- given by rational maps of degree n^2 .

What is ~~scalar multiplication~~ an isogeny?

$$\phi : P \mapsto \phi(P)$$

- A map $E \rightarrow E$,
- a group morphism,
- with finite kernel
(the torsion group $E[n] \simeq (\mathbb{Z}/n\mathbb{Z})^2$),
- surjective (in the algebraic closure),
- given by rational maps of degree n^2 .

What is ~~scalar multiplication~~ an isogeny?

$$\phi : P \mapsto \phi(P)$$

- A map $E \rightarrow E'$,
- a group morphism,
- with finite kernel
(the torsion group $E[n] \simeq (\mathbb{Z}/n\mathbb{Z})^2$),
- surjective (in the algebraic closure),
- given by rational maps of degree n^2 .

What is ~~scalar multiplication~~ an isogeny?

$$\phi : P \mapsto \phi(P)$$

- A map $E \rightarrow E'$,
- a group morphism,
- with finite kernel
(the torsion subgroup $E[m]/(E[m]/mE[m])^2$ any finite subgroup $H \subset E$),
- surjective (in the algebraic closure),
- given by rational maps of degree n^2 .

What is ~~scalar multiplication~~ an isogeny?

$$\phi : P \mapsto \phi(P)$$

- A map $E \rightarrow E'$,
- a group morphism,
- with finite kernel
(the torsion subgroup $E[m]/\#(E[m])^2$ any finite subgroup $H \subset E$),
- surjective (in the algebraic closure),
- given by rational maps of degree $\#H$.

What is scalar multiplication by an isogeny?

$$\phi : P \mapsto \phi(P)$$

- A map $E \rightarrow E'$,
- a group morphism,
- with finite kernel
(the torsion subgroup $E[m]/\{0\}/(E[m])^2$ for any finite subgroup $H \subset E$),
- surjective (in the algebraic closure),
- given by rational maps of degree $\#H$.

(Separable) isogenies \Leftrightarrow finite subgroups:

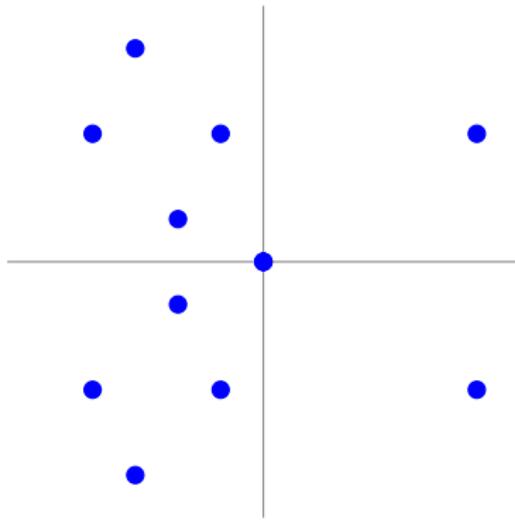
$$0 \longrightarrow H \longrightarrow E \xrightarrow{\phi} E' \rightarrow 0$$

The kernel H determines the image curve E' up to isomorphism

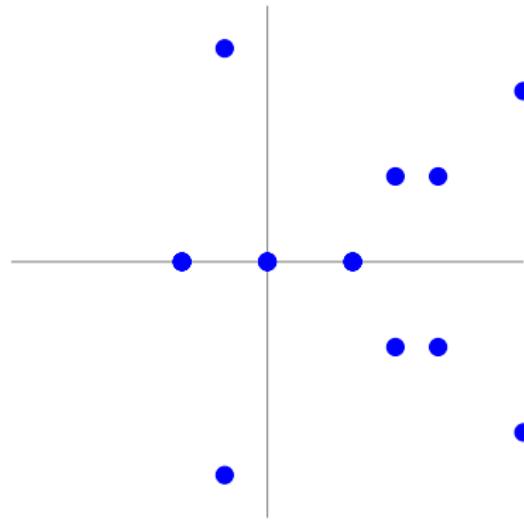
$$E/H \stackrel{\text{def}}{=} E'.$$

Isogenies: an example over \mathbb{F}_{11}

$$E : y^2 = x^3 + x$$



$$E' : y^2 = x^3 - 4x$$

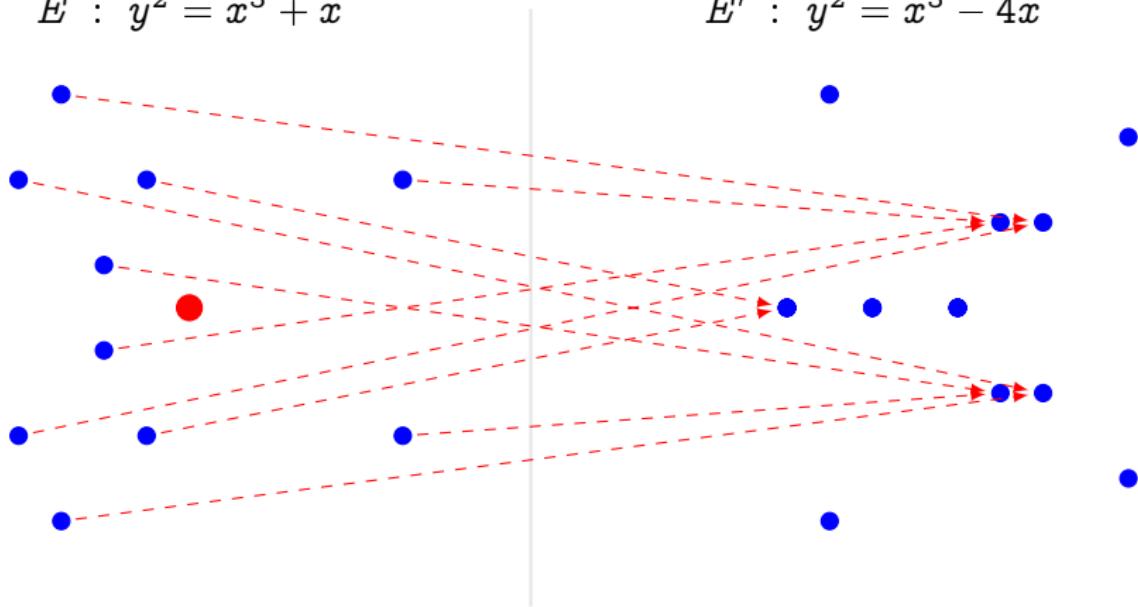


$$\phi(x, y) = \left(\frac{x^2 + 1}{x}, \quad y \frac{x^2 - 1}{x^2} \right)$$

Isogenies: an example over \mathbb{F}_{11}

$$E : y^2 = x^3 + x$$

$$E' : y^2 = x^3 - 4x$$



$$\phi(x, y) = \left(\frac{x^2 + 1}{x}, \quad y \frac{x^2 - 1}{x^2} \right)$$

- Kernel generator in red.
- This is a degree 2 map.
- Analogous to $x \mapsto x^2$ in \mathbb{F}_q^* .

Isogeny properties

Let $\phi : E \rightarrow E'$ be an isogeny defined over a field k of characteristic p .

- $k(E)$ is the **field of all rational functions** from E to k ;
- $\phi^* k(E')$ is the subfield of $k(E)$ defined as

$$\phi^* k(E') = \{f \circ \phi \mid f \in k(E')\}.$$

Degree, separability

- ① The **degree** of ϕ is $\deg \phi = [k(E) : \phi^* k(E')]$. 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 $\ker \phi = \{\mathcal{O}\}$ and $\deg \phi$ is a power of p .
- ⑤ Any isogeny can be decomposed as a product of a separable and a purely inseparable isogeny.

Isogeny properties

Let $\phi : E \rightarrow E'$ be an isogeny defined over a field k of characteristic p .

- $k(E)$ is the **field of all rational functions** from E to k ;
- $\phi^* k(E')$ is the subfield of $k(E)$ defined as

$$\phi^* k(E') = \{f \circ \phi \mid f \in k(E')\}.$$

Degree, separability

- ① The **degree** of ϕ is $\deg \phi = [k(E) : \phi^* k(E')]$. 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 $\ker \phi = \{\mathcal{O}\}$ and $\deg \phi$ is a power of p .
- ⑤ Any isogeny can be decomposed as a product of a separable and a purely inseparable isogeny.

The dual isogeny

Let $\phi : E \rightarrow E'$ be an isogeny of degree m . There is a unique isogeny $\hat{\phi} : E' \rightarrow E$ 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:

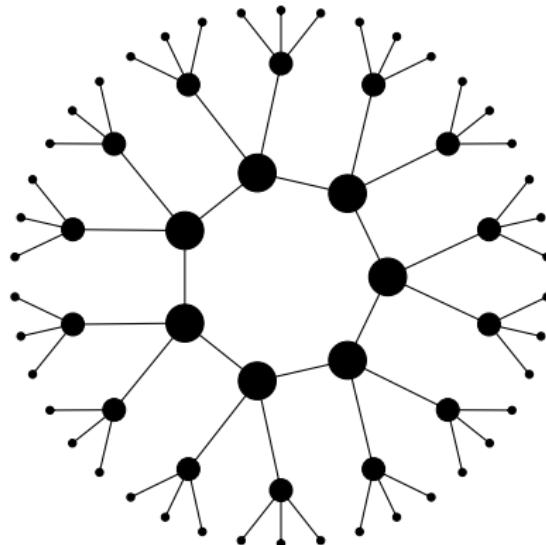
- ① $\hat{\phi}$ is defined over k if and only if ϕ is;
- ② $\widehat{\psi \circ \phi} = \hat{\phi} \circ \hat{\psi}$ for any isogeny $\psi : E' \rightarrow E''$;
- ③ $\widehat{\psi + \phi} = \hat{\psi} + \hat{\phi}$ for any isogeny $\psi : E \rightarrow E'$;
- ④ $\deg \phi = \deg \hat{\phi}$;
- ⑤ $\widehat{\hat{\phi}} = \phi$.

Isogeny graphs

We look at the graph of elliptic curves with isogenies up to isomorphism. We say two isogenies ϕ, ϕ' are isomorphic if:

$$\begin{array}{ccc} E & \xrightarrow{\phi} & E' \\ & \searrow \phi' & \uparrow \wr \\ & & E' \end{array}$$

Example: Finite field, ordinary case, graph of isogenies of degree 3.



What do isogeny graphs look like?

Torsion subgroups (ℓ prime)

In an algebraically closed field:

$$E[\ell] = \langle P, Q \rangle \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$$

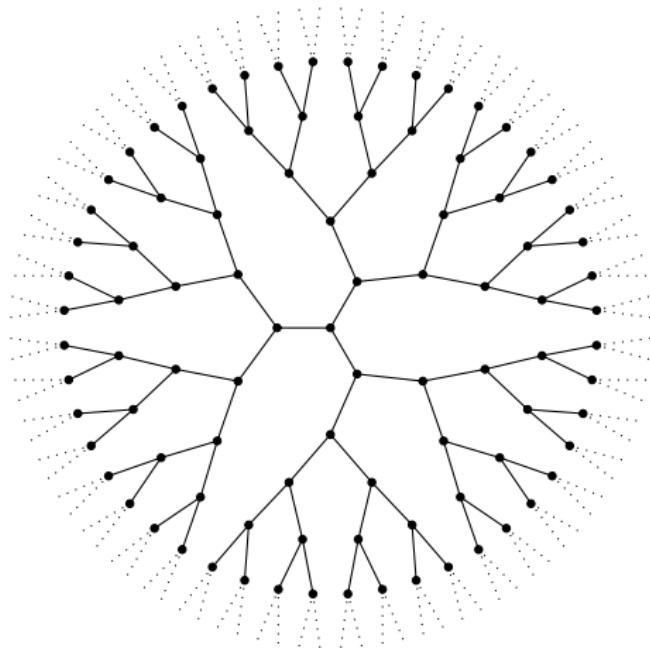


There are exactly $\ell + 1$ cyclic subgroups $H \subset E$ of order ℓ :

$$\langle P + Q \rangle, \langle P + 2Q \rangle, \dots, \langle P \rangle, \langle Q \rangle$$



There are exactly $\ell + 1$ distinct isogenies of degree ℓ .



(non-CM) 2-isogeny graph over \mathbb{C}

What happens over a finite field \mathbb{F}_p ?

Rational isogenies ($\ell \neq p$)

In the algebraic closure $\bar{\mathbb{F}}_p$

$$E[\ell] = \langle P, Q \rangle \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$$

However, an isogeny is defined over \mathbb{F}_p only if its kernel is Galois invariant.

Enter the Frobenius map

$$\pi : E \longrightarrow E$$

$$(x, y) \longmapsto (x^p, y^p)$$

E is seen here as a curve over $\bar{\mathbb{F}}_p$.

The Frobenius action on $E[\ell]$

$$\pi(P) = aP + bQ$$

$$\pi(Q) = cP + dQ$$

What happens over a finite field \mathbb{F}_p ?

Rational isogenies ($\ell \neq p$)

In the algebraic closure $\bar{\mathbb{F}}_p$

$$E[\ell] = \langle P, Q \rangle \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$$

However, an isogeny is defined over \mathbb{F}_p only if its kernel is Galois invariant.

Enter the Frobenius map

$$\pi : E \longrightarrow E$$

$$(x, y) \longmapsto (x^p, y^p)$$

E is seen here as a curve over $\bar{\mathbb{F}}_p$.

The Frobenius action on $E[\ell]$

$$aP + bQ$$

$$cP + dQ$$

What happens over a finite field \mathbb{F}_p ?

Rational isogenies ($\ell \neq p$)

In the algebraic closure $\bar{\mathbb{F}}_p$

$$E[\ell] = \langle P, Q \rangle \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$$

However, an isogeny is defined over \mathbb{F}_p only if its kernel is Galois invariant.

Enter the Frobenius map

$$\begin{aligned}\pi : E &\longrightarrow E \\ (x, y) &\longmapsto (x^p, y^p)\end{aligned}$$

E is seen here as a curve over $\bar{\mathbb{F}}_p$.

The Frobenius action on $E[\ell]$

$$\begin{pmatrix} aP + bQ \\ cP + dQ \end{pmatrix}$$

What happens over a finite field \mathbb{F}_p ?

Rational isogenies ($\ell \neq p$)

In the algebraic closure $\bar{\mathbb{F}}_p$

$$E[\ell] = \langle P, Q \rangle \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$$

However, an isogeny is defined over \mathbb{F}_p only if its kernel is Galois invariant.

Enter the Frobenius map

$$\begin{aligned}\pi : E &\longrightarrow E \\ (x, y) &\longmapsto (x^p, y^p)\end{aligned}$$

E is seen here as a curve over $\bar{\mathbb{F}}_p$.

The Frobenius action on $E[\ell]$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

What happens over a finite field \mathbb{F}_p ?

Rational isogenies ($\ell \neq p$)

In the algebraic closure $\bar{\mathbb{F}}_p$

$$E[\ell] = \langle P, Q \rangle \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$$

However, an isogeny is defined over \mathbb{F}_p only if its kernel is Galois invariant.

Enter the Frobenius map

$$\begin{aligned}\pi : E &\longrightarrow E \\ (x, y) &\longmapsto (x^p, y^p)\end{aligned}$$

E is seen here as a curve over $\bar{\mathbb{F}}_p$.

The Frobenius action on $E[\ell]$

$$\pi : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ mod } \ell$$

What happens over a finite field \mathbb{F}_p ?

Rational isogenies ($\ell \neq p$)

In the algebraic closure $\bar{\mathbb{F}}_p$

$$E[\ell] = \langle P, Q \rangle \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$$

However, an isogeny is defined over \mathbb{F}_p only if its kernel is Galois invariant.

Enter the Frobenius map

$$\begin{aligned}\pi : E &\longrightarrow E \\ (x, y) &\longmapsto (x^p, y^p)\end{aligned}$$

E is seen here as a curve over $\bar{\mathbb{F}}_p$.

The Frobenius action on $E[\ell]$

$$\pi : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ mod } \ell$$

We identify $\pi|_{E[\ell]}$ to a conjugacy class in $\text{GL}(\mathbb{Z}/\ell\mathbb{Z})$.

What happens over a finite field \mathbb{F}_p ?

Galois invariant subgroups of $E[\ell]$

=

eigenspaces of $\pi \in \mathrm{GL}(\mathbb{Z}/\ell\mathbb{Z})$

=

rational isogenies of degree ℓ

What happens over a finite field \mathbb{F}_p ?

Galois invariant subgroups of $E[\ell]$
=
eigenspaces of $\pi \in \mathrm{GL}(\mathbb{Z}/\ell\mathbb{Z})$
=
rational isogenies of degree ℓ

How many Galois invariant subgroups?

- $\pi|E[\ell] \sim \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$ $\rightarrow \ell + 1$ isogenies
- $\pi|E[\ell] \sim \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$ with $\lambda \neq \mu$ \rightarrow two isogenies
- $\pi|E[\ell] \sim \begin{pmatrix} \lambda & * \\ 0 & \lambda \end{pmatrix}$ \rightarrow one isogeny
- $\pi|E[\ell]$ is not diagonalizable \rightarrow no isogeny

Weil pairing

Let $(N, p) = 1$, fix any basis $E[N] = \langle R, S \rangle$. For any points $P, Q \in E[N]$

$$P = aR + bS$$

$$Q = cR + dS$$

the form $\det_N(P, Q) = \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc \in \mathbb{Z}/N\mathbb{Z}$
is bilinear, non-degenerate, and independent from the choice of basis.

Theorem

Let E/\mathbb{F}_q be a curve, there exists a Galois invariant bilinear map

$$e_N : E[N] \times E[N] \longrightarrow \mu_N \subset \bar{\mathbb{F}}_q,$$

called the Weil pairing of order N , and a primitive N -th root of unity $\zeta \in \bar{\mathbb{F}}_q$
such that

$$e_N(P, Q) = \zeta^{\det_N(P, Q)}.$$

The degree k of the smallest extension such that $\zeta \in \mathbb{F}_{q^k}$ is called the
embedding degree of the pairing.

Weil pairing and isogenies

Note

The Weil pairing is Galois invariant $\Leftrightarrow \det(\pi|E[N]) = q$.

Theorem

Let $\phi : E \rightarrow E'$ be an isogeny and $\hat{\phi} : E' \rightarrow E$ its dual.

Let e_N be the Weil pairing of E and e'_N that of E' . Then, for

$$e_N(P, \hat{\phi}(Q)) = e_N(\phi(P), Q),$$

for any $P \in E[N]$ and $Q \in E'[N]$.

Corollary

$$e'_N(\phi(P), \phi(Q)) = e_N(P, Q)^{\deg \phi}.$$

From local to global

Theorem (Hasse)

Let E be defined over a finite field \mathbb{F}_q . Its Frobenius map π satisfies a quadratic equation

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

for some $|t| \leq 2\sqrt{q}$, called the **trace** of π . The trace t is coprime to q if and only if E is ordinary.

Endomorphisms

An isogeny $E \rightarrow E$ is also called an **endomorphism**. Examples:

- scalar multiplication $[n]$,
- Frobenius map π .

With **addition** and **composition**, the endomorphisms form a ring $\text{End}(E)$.

The endomorphism ring

Theorem (Deuring)

Let E be an **ordinary** elliptic curve defined over a finite field \mathbb{F}_q .

Let π be its Frobenius endomorphism, and $D_\pi = t^2 - 4q < 0$ the **discriminant** of its minimal polynomial.

Then $\text{End}(E)$ is isomorphic to an **order** \mathcal{O} of the **quadratic imaginary field** $\mathbb{Q}(\sqrt{D_\pi})$.^a

^aAn order is a subring that is a \mathbb{Z} -module of rank 2 (equiv., a 2-dimensional \mathbb{R} -lattice).

In this case, we say that E has **complex multiplication** (CM) by \mathcal{O} .

Theorem (Serre-Tate)

CM elliptic curves E, E' are isogenous iff $\text{End}(E) \otimes \mathbb{Q} \simeq \text{End}(E') \otimes \mathbb{Q}$.

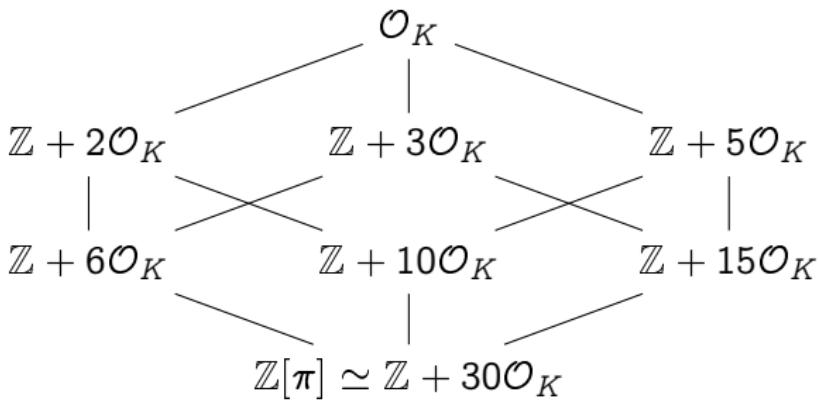
Corollary: E/\mathbb{F}_p and E'/\mathbb{F}_p are isogenous iff $\#E(\mathbb{F}_p) = \#E'(\mathbb{F}_p)$.

Endomorphism rings of ordinary curves

Classifying quadratic orders

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} , denoted by $[\mathcal{O}_K : \mathcal{O}]$.
- 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 with discriminants D, D' , then $\mathcal{O} \subset \mathcal{O}'$ iff $D' | D$.

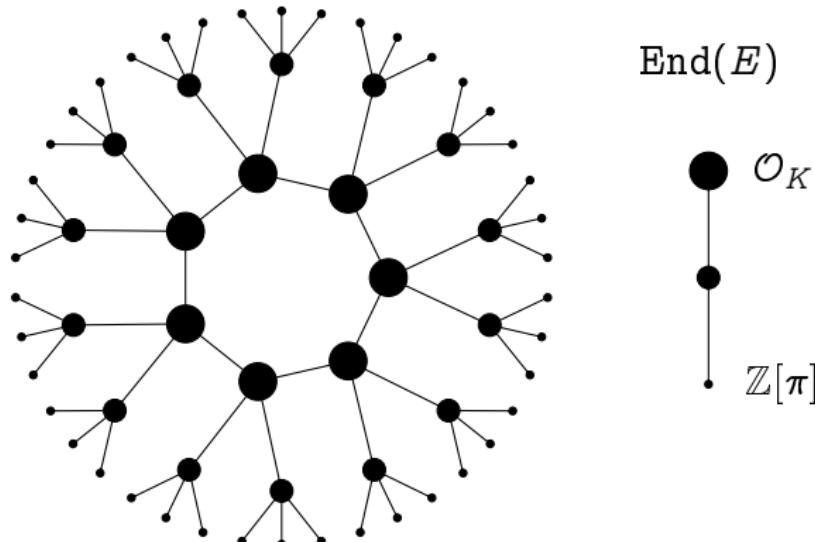


Volcanology (Kohel 1996)

Let E, E' be curves with respective endomorphism rings $\mathcal{O}, \mathcal{O}' \subset K$.

Let $\phi : E \rightarrow E'$ be an isogeny of prime degree ℓ , then:

if $\mathcal{O} = \mathcal{O}'$, ϕ is horizontal;
if $[\mathcal{O}' : \mathcal{O}] = \ell$, ϕ is ascending;
if $[\mathcal{O} : \mathcal{O}'] = \ell$, ϕ is descending.

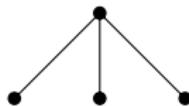


Ordinary isogeny volcano of degree $\ell = 3$.

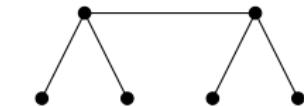
Volcanology (Kohel 1996)

Let E be ordinary,
 $\text{End}(E) \subset K$.

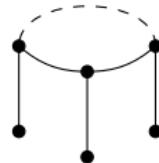
\mathcal{O}_K : maximal order of K ,
 D_K : discriminant of K .



$$\left(\frac{D_K}{\ell}\right) = -1$$



$$\left(\frac{D_K}{\ell}\right) = 0$$



$$\left(\frac{D_K}{\ell}\right) = +1$$

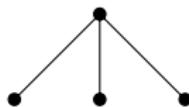
		Horizontal	Ascending	Descending
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$	$1 + \left(\frac{D_K}{\ell}\right)$		
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$	$1 + \left(\frac{D_K}{\ell}\right)$		$\ell - \left(\frac{D_K}{\ell}\right)$
$\ell \mid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$		1	ℓ
$\ell \mid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$		1	

Volcanology (Kohel 1996)

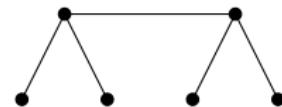
Let E be ordinary,
 $\text{End}(E) \subset K$.

\mathcal{O}_K : maximal order of K ,
 D_K : discriminant of K .

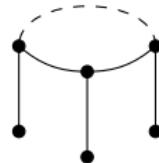
Height = $v_\ell([\mathcal{O}_K : \mathbb{Z}[\pi]])$.



$$\left(\frac{D_K}{\ell}\right) = -1$$



$$\left(\frac{D_K}{\ell}\right) = 0$$

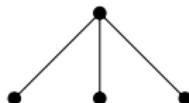


$$\left(\frac{D_K}{\ell}\right) = +1$$

		Horizontal	Ascending	Descending
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$	$1 + \left(\frac{D_K}{\ell}\right)$		
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$	$1 + \left(\frac{D_K}{\ell}\right)$		$\ell - \left(\frac{D_K}{\ell}\right)$
$\ell \mid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$		1	ℓ
$\ell \mid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$		1	

Volcanology (Kohel 1996)

Let E be ordinary,
 $\text{End}(E) \subset K$.

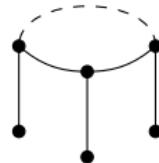


\mathcal{O}_K : maximal order of K ,
 D_K : discriminant of K .

$$\left(\frac{D_K}{\ell}\right) = -1$$

$$\left(\frac{D_K}{\ell}\right) = 0$$

Height = $v_\ell([\mathcal{O}_K : \mathbb{Z}[\pi]])$.



How large is the crater?

$$\left(\frac{D_K}{\ell}\right) = +1$$

		Horizontal	Ascending	Descending
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$	$1 + \left(\frac{D_K}{\ell}\right)$		
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$	$1 + \left(\frac{D_K}{\ell}\right)$		$\ell - \left(\frac{D_K}{\ell}\right)$
$\ell \mid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$		1	ℓ
$\ell \mid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$		1	

How large is the crater of a volcano?

Let $\text{End}(E) = \mathcal{O} \subset \mathbb{Q}(\sqrt{-D})$. Define

- $\mathcal{I}(\mathcal{O})$, the group of invertible fractional ideals,
- $\mathcal{P}(\mathcal{O})$, the group of principal ideals,

The class group

The class group of \mathcal{O} is

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

- It is a finite abelian group.
- Its order $h(\mathcal{O})$ is called the class number of \mathcal{O} .
- It arises as the Galois group of an abelian extension of $\mathbb{Q}(\sqrt{-D})$.

Complex multiplication

The \mathfrak{a} -torsion

- Let $\mathfrak{a} \subset \mathcal{O}$ be an (integral invertible) ideal of \mathcal{O} ;
- Let $E[\mathfrak{a}]$ be the subgroup of E annihilated by \mathfrak{a} :

$$E[\mathfrak{a}] = \{P \in E \mid \alpha(P) = 0 \text{ for all } \alpha \in \mathfrak{a}\};$$

- Let $\phi : E \rightarrow E_{\mathfrak{a}}$, where $E_{\mathfrak{a}} = E/E[\mathfrak{a}]$.

Then $\text{End}(E_{\mathfrak{a}}) = \mathcal{O}$ (i.e., ϕ is horizontal).

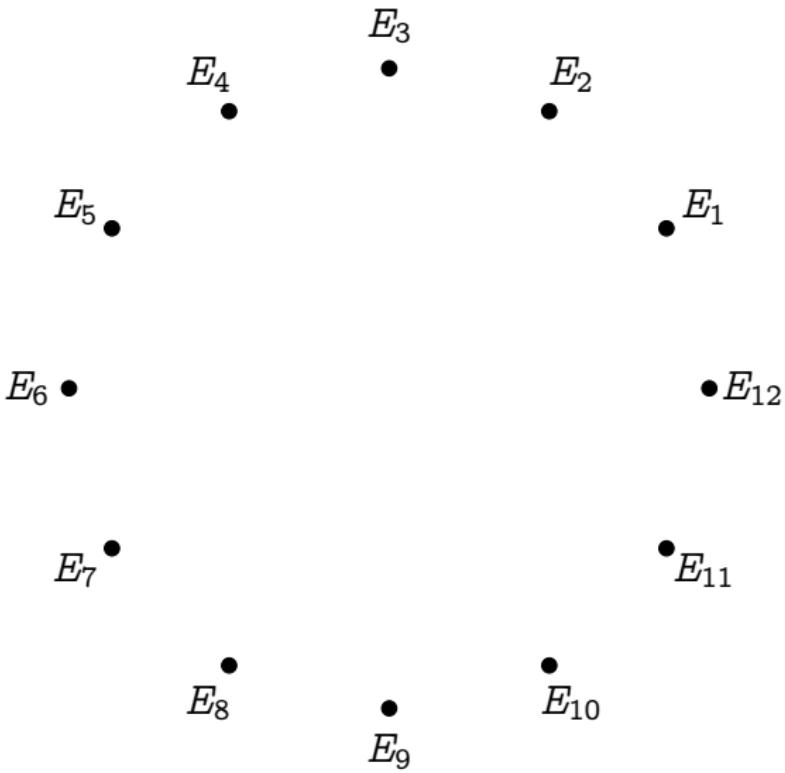
Theorem (Complex multiplication)

The action on the set of elliptic curves with complex multiplication by \mathcal{O} defined by $\mathfrak{a} * j(E) = j(E_{\mathfrak{a}})$ factors through $\text{Cl}(\mathcal{O})$, is faithful and transitive.

Corollary

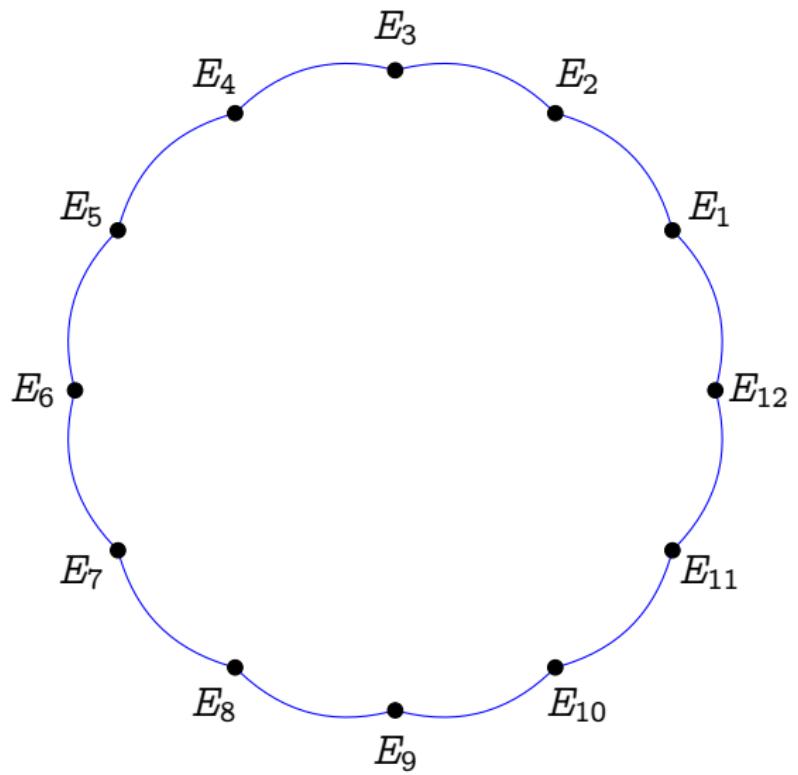
Let $\text{End}(E)$ have discriminant D . Assume that $\left(\frac{D}{\ell}\right) = 1$, then E is on a crater of an ℓ -volcano, and the crater contains $h(\text{End}(E))$ curves.

Complex multiplication graphs



Vertices are elliptic curves with complex multiplication by \mathcal{O}_K (i.e., $\text{End}(E) \simeq \mathcal{O}_K \subset \mathbb{Q}(\sqrt{-D})$).

Complex multiplication graphs

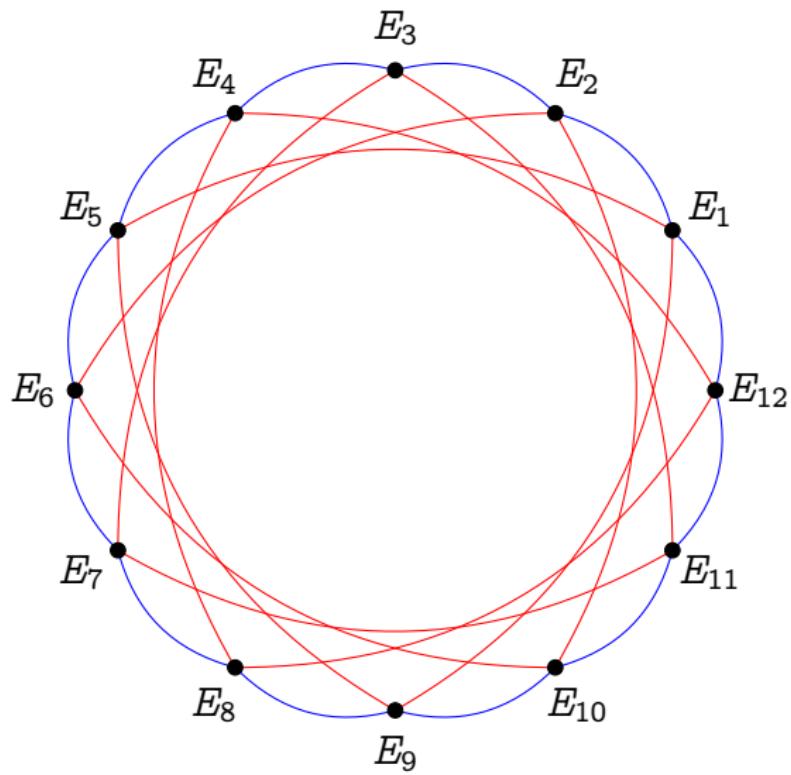


Vertices are elliptic curves with complex multiplication by \mathcal{O}_K (i.e., $\text{End}(E) \simeq \mathcal{O}_K \subset \mathbb{Q}(\sqrt{-D})$).

Edges are horizontal isogenies of bounded prime degree.

— degree 2

Complex multiplication graphs



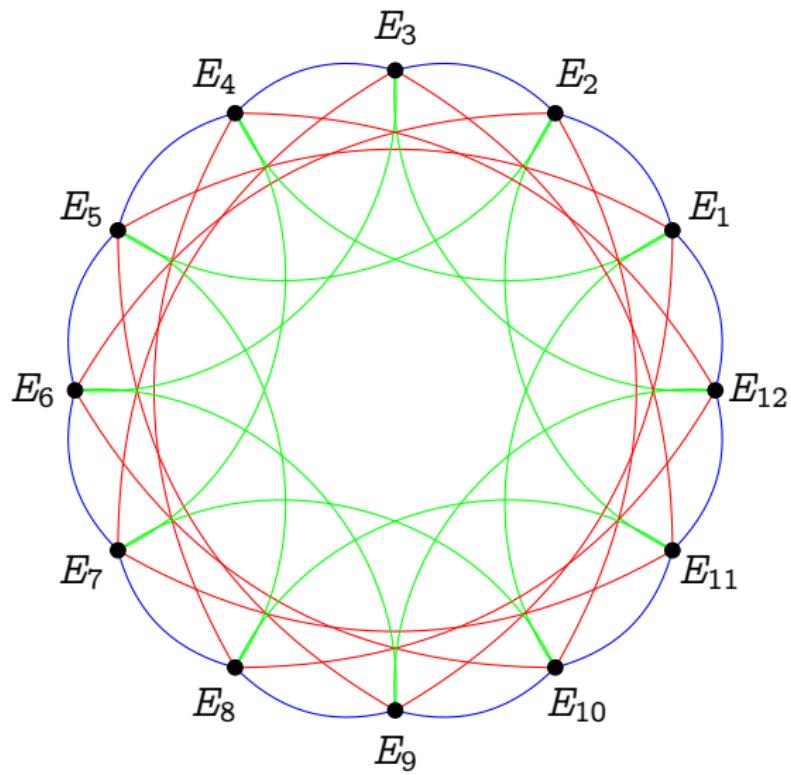
Vertices are elliptic curves with complex multiplication by \mathcal{O}_K (i.e., $\text{End}(E) \simeq \mathcal{O}_K \subset \mathbb{Q}(\sqrt{-D})$).

Edges are horizontal isogenies of bounded prime degree.

— degree 2

— degree 3

Complex multiplication graphs



Vertices are elliptic curves with complex multiplication by \mathcal{O}_K (i.e., $\text{End}(E) \simeq \mathcal{O}_K \subset \mathbb{Q}(\sqrt{-D})$).

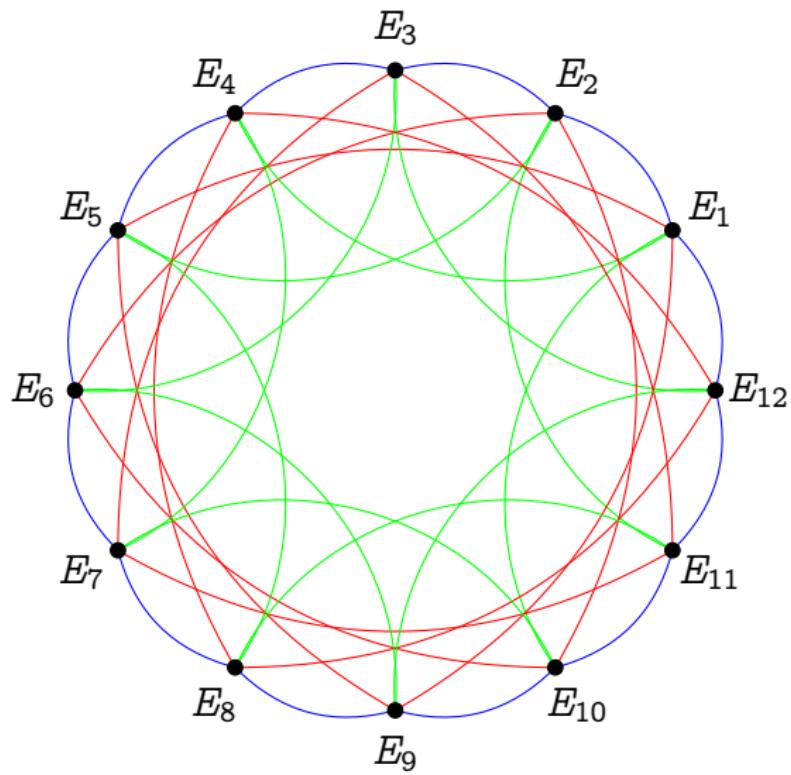
Edges are horizontal isogenies of bounded prime degree.

degree 2

degree 3

degree 5

Complex multiplication graphs



Vertices are elliptic curves with complex multiplication by \mathcal{O}_K (i.e., $\text{End}(E) \simeq \mathcal{O}_K \subset \mathbb{Q}(\sqrt{-D})$).

Edges are horizontal isogenies of bounded prime degree.

degree 2

degree 3

degree 5

Isomorphic to a Cayley graph of $\text{Cl}(\mathcal{O}_K)$.

Supersingular endomorphisms

Recall, a curve E over a field \mathbb{F}_q of characteristic p is **supersingular** iff

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

with $t \equiv 0 \pmod{p}$.

Case: $t = 0 \Rightarrow D_\pi = -4q$

- Only possibility for E/\mathbb{F}_p ,
- E/F_p has CM by an order of $\mathbb{Q}(\sqrt{-p})$, similar to the ordinary case.

Case: $t = \pm 2\sqrt{q} \Rightarrow D_\pi = 0$

- General case for E/\mathbb{F}_{p^2} ,
- $\pi = \pm q$, hence no complex multiplication.

We will ignore marginal cases: $t = \pm\sqrt{q}, \pm\sqrt{2q}, \pm\sqrt{3q}$.

Supersingular complex multiplication

Let E/\mathbb{F}_p be a supersingular curve, then $\pi^2 = -p$, and

$$\pi = \begin{pmatrix} \sqrt{-p} & 0 \\ 0 & -\sqrt{-p} \end{pmatrix} \mod \ell$$

for any ℓ s.t. $\left(\frac{-p}{\ell}\right) = 1$.

Theorem (Delfs and Galbraith 2016)

Let $\text{End}_{\mathbb{F}_p}(E)$ denote the ring of \mathbb{F}_p -rational endomorphisms of E . Then

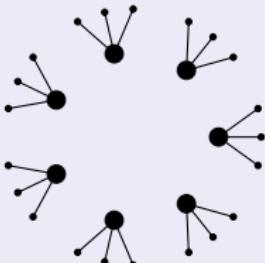
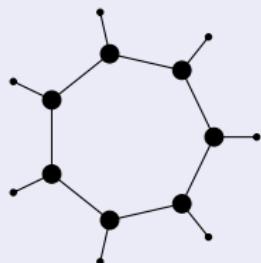
$$\mathbb{Z}[\pi] \subset \text{End}_{\mathbb{F}_p}(E) \subset \mathbb{Q}(\sqrt{-p}).$$

Orders of $\mathbb{Q}(\sqrt{-p})$

- If $p \equiv 1 \pmod{4}$, then $\mathbb{Z}[\pi]$ is the maximal order.
- If $p \equiv -1 \pmod{4}$, then $\mathbb{Z}[\frac{\pi+1}{2}]$ is the maximal order, and $[\mathbb{Z}[\frac{\pi+1}{2}] : \mathbb{Z}[\pi]] = 2$.

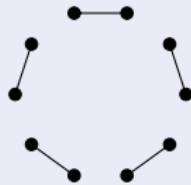
Supersingular CM graphs

2-volcanoes, $p = -1 \bmod 4$



$$\begin{array}{c} \bullet \\ \text{---} \\ \bullet \end{array} \quad \mathbb{Z}\left[\frac{\pi+1}{2}\right]$$
$$\bullet \\ \text{---} \\ \bullet \end{array} \quad \mathbb{Z}[\pi]$$

2-graphs, $p = 1 \bmod 4$



$$\bullet \\ \text{---} \\ \bullet \end{array} \quad \mathbb{Z}[\pi]$$

All other ℓ -graphs are cycles of horizontal isogenies iff $\left(\frac{-p}{\ell}\right) = 1$.

The full endomorphism ring

Theorem (Deuring)

Let E be a supersingular elliptic curve, then

- E is isomorphic to a curve defined over \mathbb{F}_{p^2} ;
- Every isogeny of E is defined over \mathbb{F}_{p^2} ;
- Every endomorphism of E is defined over \mathbb{F}_{p^2} ;
- $\text{End}(E)$ is isomorphic to a maximal order in a quaternion algebra ramified at p and ∞ .

In particular:

- If E is defined over \mathbb{F}_p , then $\text{End}_{\mathbb{F}_p}(E)$ is strictly contained in $\text{End}(E)$.
- Some endomorphisms do not commute!

An example

The curve of j -invariant 1728

$$E : y^2 = x^3 + x$$

is supersingular over \mathbb{F}_p iff $p \equiv -1 \pmod{4}$.

Endomorphisms

$\text{End}(E) = \mathbb{Z}\langle \iota, \pi \rangle$, with:

- π the Frobenius endomorphism, s.t. $\pi^2 = -p$;
- ι the map

$$\iota(x, y) = (-x, iy),$$

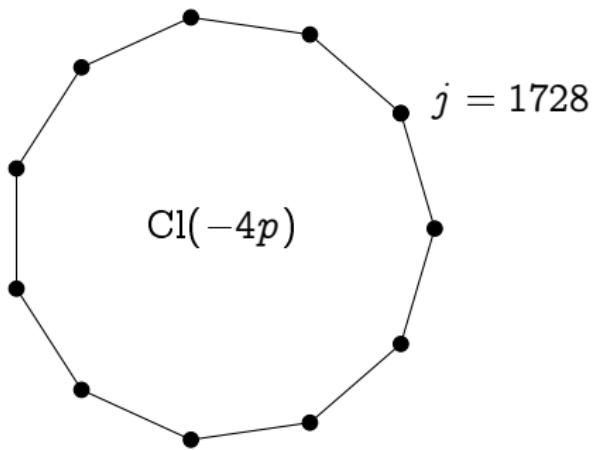
where $i \in \mathbb{F}_{p^2}$ is a 4-th root of unity. Clearly, $\iota^2 = -1$.

And $\iota\pi = -\pi\iota$.

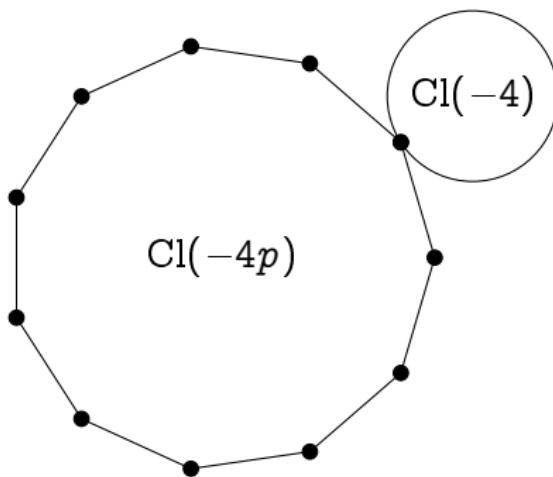
Class group action party

- $j = 1728$

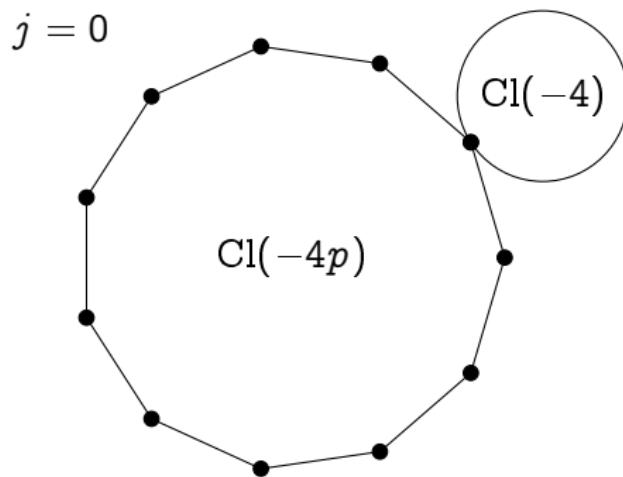
Class group action party



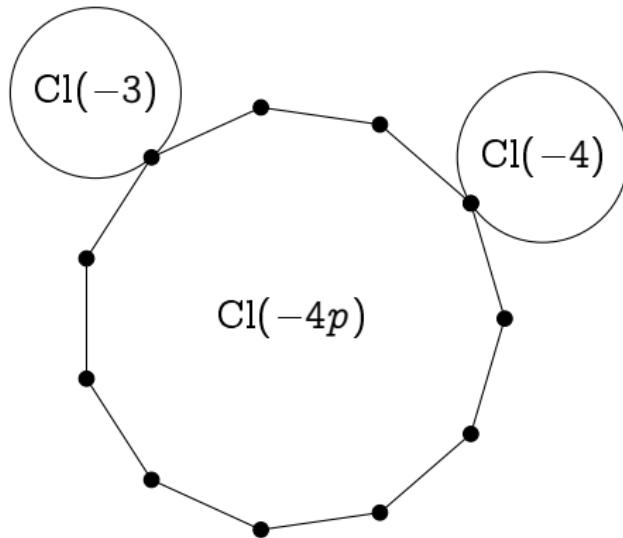
Class group action party



Class group action party



Class group action party



Quaternion algebra?! WTF?²

The quaternion algebra $B_{p,\infty}$ is:

- A 4-dimensional \mathbb{Q} -vector space with basis $(1, i, j, k)$;
- A non-commutative division algebra¹ $B_{p,\infty} = \mathbb{Q}\langle i, j \rangle$ with the relations:

$$i^2 = a, \quad j^2 = -p, \quad ij = -ji = k,$$

for some $a < 0$ (depending on p).

- All elements of $B_{p,\infty}$ are quadratic algebraic numbers;
- $B_{p,\infty} \otimes \mathbb{Q}_\ell \simeq M_{2 \times 2}(\mathbb{Q}_\ell)$ for all $\ell \neq p$.
I.e., endomorphisms restricted to $E[\ell^e]$ are just 2×2 matrices mod ℓ^e .
- $B_{p,\infty} \otimes \mathbb{R} \simeq M_{2 \times 2}(\mathbb{R})$.

¹All elements have inverses.

²What The Field?

Supersingular graphs

- Quaternion algebras have many maximal orders.
- For every maximal order type of $B_{p,\infty}$ there are 1 or 2 curves over \mathbb{F}_{p^2} having endomorphism ring isomorphic to it.
- There is a unique isogeny class of supersingular curves over $\bar{\mathbb{F}}_p$ of size $\approx p/12$.
- Left ideals act on the set of maximal orders like isogenies.
- The graph of ℓ -isogenies is $(\ell + 1)$ -regular.

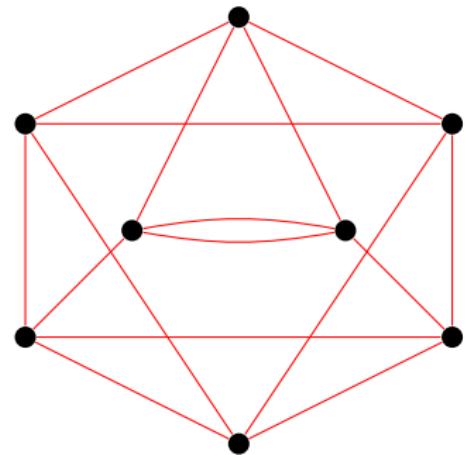


Figure: 3-isogeny graph on \mathbb{F}_{97^2} .

Graphs lexicon

Degree: Number of (outgoing/ingoing) edges.

k -regular: All vertices have degree k .

Connected: There is a path between any two vertices.

Distance: The length of the shortest path between two vertices.

Diameter: The longest distance between two vertices.

$\lambda_1 \geq \dots \geq \lambda_n$: The (ordered) eigenvalues of the adjacency matrix.

Expander graphs

Proposition

If G is a k -regular graph, its largest and smallest eigenvalues satisfy

$$k = \lambda_1 \geq \lambda_n \geq -k.$$

Expander families

An infinite family of connected k -regular graphs on n vertices is an **expander family** if there exists an $\epsilon > 0$ such that all **non-trivial** eigenvalues satisfy $|\lambda| \leq (1 - \epsilon)k$ for n large enough.

- Expander graphs have **short diameter** ($O(\log n)$);
- Random walks **mix rapidly** (after $O(\log n)$ steps, the induced distribution on the vertices is close to uniform).

Expander graphs from isogenies

Theorem (Pizer 1990, 1998)

Let ℓ be fixed. The family of graphs of supersingular curves over \mathbb{F}_{p^2} with ℓ -isogenies, as $p \rightarrow \infty$, is an expander family^a.

^aEven better, it has the Ramanujan property.

Theorem (Jao, Miller, and Venkatesan 2009)

Let $\mathcal{O} \subset \mathbb{Q}(\sqrt{-D})$ be an order in a quadratic imaginary field. The graphs of all curves over \mathbb{F}_q with complex multiplication by \mathcal{O} , with isogenies of prime degree bounded^a by $(\log q)^{2+\delta}$, are expanders.

^aMay contain traces of GRH.



Thank you

<https://defeo.lu/>

 @luca_defeo