Distortion Maps for Elliptic Curves over Finite Fields

Dimitrios Noulas

National and Kapodistrian University of Athens

Greek Algebra and Number Theory
April 2026

Initially a CIMPA school project

CIMPA stands for: Centre International de Mathématiques Pures et Appliquées.

The entire project is a work of the FP-team: Nikita Andrusov, Sevag Büyüksimkeşyan, D. N., Fabien Pazuki, Mustafa Umut Kazancıoğlu, Jordi Vilà-Casadevall

Distorting a Point

Elliptic Curves over Finite Fields

Let $\mathbb{F}_q$ be a finite field, where q is a power of a prime number p. An Elliptic Curve E over $\mathbb{F}_q$ is a non-singular projective curve of genus 1 with a specified $\mathbb{F}_q$-rational point $\mathcal{O}$. If $p \neq 2, 3$, it is given by an equation:

$$E/\mathbb{F}_q : \; y^2 = x^3 + Ax + B, \quad 4A^3 + 27B^2 \neq 0, \quad A, B \in \mathbb{F}_q$$

Distorting a Point

Elliptic Curves over Finite Fields

Let $\mathbb{F}_q$ be a finite field, where q is a power of a prime number p. An Elliptic Curve E over $\mathbb{F}_q$ is a non-singular projective curve of genus 1 with a specified $\mathbb{F}_q$-rational point $\mathcal{O}$. If $p \neq 2, 3$, it is given by an equation:

$$E/\mathbb{F}_q : \; y^2 = x^3 + Ax + B, \quad 4A^3 + 27B^2 \neq 0, \quad A, B \in \mathbb{F}_q$$

$E(\mathbb{F}_q)$ denotes the set of $\mathbb{F}_q$-rational points of E. It is a finite abelian group with identity element $\mathcal{O}$.

Distorting a Point

Elliptic Curves over Finite Fields

Let $\mathbb{F}_q$ be a finite field, where q is a power of a prime number p. An Elliptic Curve E over $\mathbb{F}_q$ is a non-singular projective curve of genus 1 with a specified $\mathbb{F}_q$-rational point $\mathcal{O}$. If $p \neq 2, 3$, it is given by an equation:

$$E/\mathbb{F}_q : \; y^2 = x^3 + Ax + B, \quad 4A^3 + 27B^2 \neq 0, \quad A, B \in \mathbb{F}_q$$

$E(\mathbb{F}_q)$ denotes the set of $\mathbb{F}_q$-rational points of E. It is a finite abelian group with identity element $\mathcal{O}$.

Endomorphisms

By $\mathrm{End}(E)$ we denote the ring of (geometric) endomorphisms of E given by rational functions with coefficients in an algebraic closure $\overline{\mathbb{F}}_q$, which respect the group structure of $E(\overline{\mathbb{F}}_q)$.

Distorting a Point

Elliptic Curves over Finite Fields

Let $\mathbb{F}_q$ be a finite field, where q is a power of a prime number p. An Elliptic Curve E over $\mathbb{F}_q$ is a non-singular projective curve of genus 1 with a specified $\mathbb{F}_q$-rational point $\mathcal{O}$. If $p \neq 2, 3$, it is given by an equation:

$$E/\mathbb{F}_q : \; y^2 = x^3 + Ax + B, \quad 4A^3 + 27B^2 \neq 0, \quad A, B \in \mathbb{F}_q$$

$E(\mathbb{F}_q)$ denotes the set of $\mathbb{F}_q$-rational points of E. It is a finite abelian group with identity element $\mathcal{O}$.

Endomorphisms

By $\mathrm{End}(E)$ we denote the ring of (geometric) endomorphisms of E given by rational functions with coefficients in an algebraic closure $\overline{\mathbb{F}}_q$, which respect the group structure of $E(\overline{\mathbb{F}}_q)$.

E.g. $E/\mathbb{F}_5 : \; y^2 = x^3 + 1$ with the map $(x, y) \mapsto (\zeta \cdot x, y)$, where ζ is a primitive cube root of unity (defined over $\mathbb{F}_{5^2}$!).

Distorting a Point

Definition: Distortion map

Let P in $E(\mathbb{F}_q)$. A *distortion map* ϕ with respect to P is an element in $\mathrm{End}(E)$ such that $\phi(P) \notin \langle P \rangle$, i.e. it maps the point P outside the cyclic group P generates.

Distorting a Point

Definition: Distortion map

Let P in $E(\mathbb{F}_q)$. A *distortion map* ϕ with respect to P is an element in $\mathrm{End}(E)$ such that $\phi(P) \notin \langle P \rangle$, i.e. it maps the point P outside the cyclic group P generates.

Distorting m-torsion points

Denote by $E[m] = \{P \in E(\overline{\mathbb{F}}_q) : \ m \cdot P = \mathcal{O}\}$ the m-torsion points of $E(\overline{\mathbb{F}}_q)$. We say ϕ is a distortion map for $E[m]$ if it is a distortion map for every P in $E[m]$.

Distorting a Point

Definition: Distortion map

Let P in $E(\mathbb{F}_q)$. A *distortion map* ϕ with respect to P is an element in $\mathrm{End}(E)$ such that $\phi(P) \notin \langle P \rangle$, i.e. it maps the point P outside the cyclic group P generates.

Distorting m-torsion points

Denote by $E[m] = \{P \in E(\overline{\mathbb{F}}_q) : \ m \cdot P = \mathcal{O}\}$ the m-torsion points of $E(\overline{\mathbb{F}}_q)$. We say ϕ is a distortion map for $E[m]$ if it is a distortion map for every P in $E[m]$.

The Weil Pairing

The group $E[m]$ comes equipped with a bilinear, non-degenerate pairing called the Weil pairing: $e_m : E[m] \times E[m] \longrightarrow \mu_m$, where $e_m(P, Q)$ is an m-th root of unity. In particular, $e_m(P, P) = 1$ for every m-torsion point P.

A modification

Modified Weil pairing

Given a distortion map ϕ with respect to $E[m]$, we define the modified Weil pairing

$$e_{m,\phi} : E[m] \times E[m] \to \mu_m$$

$$e_{m,\phi}(P, Q) = e_m(P, \phi(Q)).$$

In particular, $e_{m,\phi}(P, P)$ is an m-th root of unity $\neq 1$.

Some applications

Discrete Logarithm Problem: Knowing P and $a \cdot P$, find a.

A toy-example: Tripartite secret key

Suppose three parties Alice, Bob and Chris want to agree on a shared secret based on the public parameters $(E, \mathbb{F}_q, P)$ where P is an m-torsion point and $E[m]$ admits a known distortion map ϕ. Each of them has private keys a, b, c and public keys $a \cdot P$, $b \cdot P$, $c \cdot P$ respectively.

Some applications

Discrete Logarithm Problem: Knowing P and $a \cdot P$, find a.

A toy-example: Tripartite secret key

Suppose three parties Alice, Bob and Chris want to agree on a shared secret based on the public parameters $(E, \mathbb{F}_q, P)$ where P is an m-torsion point and $E[m]$ admits a known distortion map ϕ. Each of them has private keys a, b, c and public keys $a \cdot P$, $b \cdot P$, $c \cdot P$ respectively.

Each one of them has enough information to compute:

$$e_{m,\phi}(P,P)^{abc} = e_{m,\phi}(b \cdot P, c \cdot P)^a = e_{m,\phi}(a \cdot P, c \cdot P)^b = e_{m,\phi}(a \cdot P, b \cdot P)^c,$$

and use it as a key!

Attack vs. Defense

Breaking Decision Diffie-Hellman (DDH)

Because $e_{m,\phi}(P,P) \neq 1$, we can easily distinguish triples (aP, bP, cP) from $(aP, bP, (ab)P)$ by checking if they pair correctly:

$$e_{m,\phi}(a \cdot P, b \cdot P) \stackrel{?}{=} e_{m,\phi}(P, c \cdot P)$$

Attack vs. Defense

Breaking Decision Diffie-Hellman (DDH)

Because $e_{m,\phi}(P,P) \neq 1$, we can easily distinguish triples (aP, bP, cP) from $(aP, bP, (ab)P)$ by checking if they pair correctly:

$$e_{m,\phi}(a \cdot P, b \cdot P) \stackrel{?}{=} e_{m,\phi}(P, c \cdot P)$$

The MOV Attack & Verheul's Theorem

- **MOV Attack:** The map $P \longmapsto e_m(P,Q)$ embeds the curve into $\mathbb{F}^*_{q^k}$. This reduces the hard Discrete Logarithm Problem on the curve to an easier problem in the finite field!
- **Verheul's Theorem:** If this MOV embedding has a computable inverse, we can easily compute $(ab) \cdot P$ from $a \cdot P$ and $b \cdot P$. Recall, the Elliptic Curve Diffie-Helmann key exchange provides the key $(ab) \cdot P = a \cdot (b \cdot P) = b \cdot (a \cdot P)$.

A quote (or not)

As Hilbert famously said (not really)

We must know about the existence of distortion maps for elliptic curves over finite fields.

We will know!

Back to Endomorphisms

One should understand Elliptic curves over $\mathbb{C}$!

Back to Endomorphisms

One should understand Elliptic curves over $\mathbb{C}$!

In this case an elliptic curve is a torus $\mathbb{C}/\Lambda$ for a $\mathbb{Z}$-lattice $\Lambda = \langle \omega_1, \omega_2 \rangle$.

$$\mathrm{End}(E) = \mathbb{Z} \text{ (usually)}$$

$$n \in \mathbb{Z}: \quad [n] : E \longrightarrow E, \quad P \mapsto n \cdot P, \quad E[n] = \frac{\frac{1}{n}\Lambda}{\Lambda} \cong (\mathbb{Z}/n\mathbb{Z})^2$$

Back to Endomorphisms

One should understand Elliptic curves over $\mathbb{C}$!

In this case an elliptic curve is a torus $\mathbb{C}/\Lambda$ for a $\mathbb{Z}$-lattice $\Lambda = \langle \omega_1, \omega_2 \rangle$.

$$\mathrm{End}(E) = \mathbb{Z} \text{ (usually)}$$

$$n \in \mathbb{Z}: \quad [n] : E \longrightarrow E, \quad P \mapsto n \cdot P, \quad E[n] = \frac{\frac{1}{n}\Lambda}{\Lambda} \cong (\mathbb{Z}/n\mathbb{Z})^2$$

Unless the lattice Λ has extra symmetries, i.e. it is preserved by multiplication by a complex number.

Back to Endomorphisms

One should understand Elliptic curves over $\mathbb{C}$!

In this case an elliptic curve is a torus $\mathbb{C}/\Lambda$ for a $\mathbb{Z}$-lattice $\Lambda = \langle \omega_1, \omega_2 \rangle$.

$$\mathrm{End}(E) = \mathbb{Z} \text{ (usually)}$$

$$n \in \mathbb{Z}: \quad [n] : E \longrightarrow E, \quad P \mapsto n \cdot P, \quad E[n] = \frac{\frac{1}{n}\Lambda}{\Lambda} \cong (\mathbb{Z}/n\mathbb{Z})^2$$

Unless the lattice Λ has extra symmetries, i.e. it is preserved by multiplication by a complex number.

Example: $E/\mathbb{C} : y^2 = x^3 - x$, $(\Lambda = \mathbb{Z} \oplus i\mathbb{Z})$ has the automorphism $(X, Y) \mapsto (-X, i \cdot Y)$, usually denoted as $[i]$ and $[i]^2 = [-1]$.

Back to Endomorphisms

One should understand Elliptic curves over $\mathbb{C}$!

In this case an elliptic curve is a torus $\mathbb{C}/\Lambda$ for a $\mathbb{Z}$-lattice $\Lambda = \langle \omega_1, \omega_2 \rangle$.

$$\mathrm{End}(E) = \mathbb{Z} \text{ (usually)}$$

$$n \in \mathbb{Z}: \quad [n] : E \longrightarrow E, \quad P \mapsto n \cdot P, \quad E[n] = \frac{\frac{1}{n}\Lambda}{\Lambda} \cong (\mathbb{Z}/n\mathbb{Z})^2$$

Unless the lattice Λ has extra symmetries, i.e. it is preserved by multiplication by a complex number.

Example: $E/\mathbb{C} : y^2 = x^3 - x$, $(\Lambda = \mathbb{Z} \oplus i\mathbb{Z})$ has the automorphism $(X, Y) \mapsto (-X, i \cdot Y)$, usually denoted as $[i]$ and $[i]^2 = [-1]$.

No hope to distort a point (over $\mathbb{C}$) if $\mathrm{End}(E) = \mathbb{Z}$. We have to look specifically for the extra endomorphisms/automorphisms in the reduction to $\mathbb{F}_q$.

Endomorphisms over $\overline{\mathbb{F}}_q$

The Frobenius

For $E/\mathbb{F}_q$, we have $\pi_q : E \to E$ with $\pi_q(X, Y) = (X^q, Y^q)$.

Endomorphisms over $\overline{\mathbb{F}}_q$

The Frobenius

For $E/\mathbb{F}_q$, we have $\pi_q : E \to E$ with $\pi_q(X, Y) = (X^q, Y^q)$.
By Hasse's theorem, it is a root of the polynomial $\phi^2 - t\phi + q$, of negative discriminant where t is the "Trace of Frobenius".

Endomorphisms over $\overline{\mathbb{F}}_q$

The Frobenius

For $E/\mathbb{F}_q$, we have $\pi_q : E \to E$ with $\pi_q(X, Y) = (X^q, Y^q)$.
By Hasse's theorem, it is a root of the polynomial $\phi^2 - t\phi + q$, of negative discriminant where t is the "Trace of Frobenius".

Ordinary and Supersingular

$\mathrm{End}(E)$ (over $\overline{\mathbb{F}}_q$) can only be one of the following two:

$$\mathrm{End}(E) = \begin{cases} \text{An order in } \mathbb{Q}(\sqrt{-d}),\ d \in \mathbb{Z}_{>0} \text{ squarefree}, \\ \text{An order in a Quaternion algebra over } \mathbb{Q}, \end{cases}$$

That is a $\mathbb{Q}$-vector space with basis $\{1, i, j, k\}$ such that $ij = k, ji = -k, i^2, j^2 \in \mathbb{Q}$. We say E is *ordinary* in the first case and *supersingular* in the second.

Frobenius as distortion map

Can we use the Frobenius? Yes, but...

Frobenius as distortion map

Can we use the Frobenius? Yes, but... For $E/\mathbb{F}_q$ the Frobenius fixes pointwise the points $E(\mathbb{F}_q)$. One has to pick a point that is not in the field of definition $\mathbb{F}_q$.

Frobenius as distortion map

Can we use the Frobenius? Yes, but... For $E/\mathbb{F}_q$ the Frobenius fixes pointwise the points $E(\mathbb{F}_q)$. One has to pick a point that is not in the field of definition $\mathbb{F}_q$.

If $P \in E(\mathbb{F}_q) \cap E[\ell]$ for a prime ℓ, then we evaluate $\phi^2 - t\phi + q \equiv (\phi - 1)(\phi - q) \mod \ell$.

Frobenius as distortion map

Can we use the Frobenius? Yes, but... For $E/\mathbb{F}_q$ the Frobenius fixes pointwise the points $E(\mathbb{F}_q)$. One has to pick a point that is not in the field of definition $\mathbb{F}_q$.

If $P \in E(\mathbb{F}_q) \cap E[\ell]$ for a prime ℓ, then we evaluate $\phi^2 - t\phi + q \equiv (\phi - 1)(\phi - q) \mod \ell$.

The Frobenius will distort any point in $E[\ell]$ that is not in an eigenspace!

A Criterion for a distortion map on $E[\ell]$

Let $B = \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ be the endomorphism algebra of $E/\mathbb{F}_q$. Pick an isogeny $\phi \in \mathrm{End}(E) \setminus \mathbb{Z}$, then $K_\phi := \mathbb{Z}[\phi] \otimes_{\mathbb{Z}} \mathbb{Q}$ is an imaginary quadratic subfield of B. We have that $\mathbb{Z}[\phi]$ is an order in K_ϕ with discriminant D_ϕ.

A Criterion for a distortion map on $E[\ell]$

Let $B = \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ be the endomorphism algebra of $E/\mathbb{F}_q$. Pick an isogeny $\phi \in \mathrm{End}(E) \setminus \mathbb{Z}$, then $K_\phi := \mathbb{Z}[\phi] \otimes_{\mathbb{Z}} \mathbb{Q}$ is an imaginary quadratic subfield of B. We have that $\mathbb{Z}[\phi]$ is an order in K_ϕ with discriminant D_ϕ.

Proposition (D.Charles, FP-team)

If $\ell \mid [\mathrm{End}(E) \cap K_\phi : \mathbb{Z}[\phi]]$, then ϕ is not a distortion map for any $P \in E[\ell] \setminus \{O\}$. Otherwise,

1. $\left(\frac{D_\phi}{\ell}\right) = 1$ if and only if ϕ is a distortion map for all but two cyclic subgroups of $E[\ell]$.
2. $\left(\frac{D_\phi}{\ell}\right) = -1$ if and only if ϕ is a distortion map for $E[\ell]$.
3. $\left(\frac{D_\phi}{\ell}\right) = 0$ if and only if ϕ is a distortion map for all but one cyclic subgroup of $E[\ell]$.

Proof (Sketch)

If $\mathrm{End}(E) \cap K_\phi = \mathbb{Z}[\beta]$ for some endomorphism β, then $\phi = \alpha + f\beta$, for $f = [\mathrm{End}(E) \cap K_\phi : \mathbb{Z}[\phi]]$ and $\alpha \in \mathbb{Z}$. Thus, if $\ell \mid f$

$$\phi|_{E[\ell]} = \alpha|_{E[\ell]} \quad \text{not a distortion map.}$$

Proof (Sketch)

If $\mathrm{End}(E) \cap K_\phi = \mathbb{Z}[\beta]$ for some endomorphism β, then $\phi = \alpha + f\beta$, for $f = [\mathrm{End}(E) \cap K_\phi : \mathbb{Z}[\phi]]$ and $\alpha \in \mathbb{Z}$. Thus, if $\ell \mid f$

$$\phi|_{E[\ell]} = \alpha|_{E[\ell]} \quad \text{not a distortion map.}$$

Now if χ_ϕ is the characteristic polynomial of ϕ with discriminant D_ϕ, and $\overline{\chi}_\phi$ is the reduction mod ℓ, we have to consider the cases:

$$\overline{\chi}_\phi \text{ irreducible}, \quad \overline{\chi}_\phi(x) = (x-\alpha)(x-\beta), \quad \overline{\chi}_\phi(x) = (x-\alpha)^2 \pmod{\ell}$$

Proof (Sketch)

If $\mathrm{End}(E) \cap K_\phi = \mathbb{Z}[\beta]$ for some endomorphism β, then $\phi = \alpha + f\beta$, for $f = [\mathrm{End}(E) \cap K_\phi : \mathbb{Z}[\phi]]$ and $\alpha \in \mathbb{Z}$. Thus, if $\ell \mid f$

$$\phi|_{E[\ell]} = \alpha|_{E[\ell]} \quad \text{not a distortion map.}$$

Now if χ_ϕ is the characteristic polynomial of ϕ with discriminant D_ϕ, and $\overline{\chi}_\phi$ is the reduction mod ℓ, we have to consider the cases:

$$\overline{\chi}_\phi \text{ irreducible}, \quad \overline{\chi}_\phi(x) = (x-\alpha)(x-\beta), \quad \overline{\chi}_\phi(x) = (x-\alpha)^2 \pmod{\ell}$$

which are related to the splitting behaviour of ℓ according to:

$$\left(\frac{D_\phi}{\ell}\right) = -1, 1, 0,$$

Proof (Sketch)

If $\mathrm{End}(E) \cap K_\phi = \mathbb{Z}[\beta]$ for some endomorphism β, then $\phi = \alpha + f\beta$, for $f = [\mathrm{End}(E) \cap K_\phi : \mathbb{Z}[\phi]]$ and $\alpha \in \mathbb{Z}$. Thus, if $\ell \mid f$

$$\phi|_{E[\ell]} = \alpha|_{E[\ell]} \quad \text{not a distortion map.}$$

Now if χ_ϕ is the characteristic polynomial of ϕ with discriminant D_ϕ, and $\overline{\chi}_\phi$ is the reduction mod ℓ, we have to consider the cases:

$$\overline{\chi}_\phi \text{ irreducible}, \quad \overline{\chi}_\phi(x) = (x-\alpha)(x-\beta), \quad \overline{\chi}_\phi(x) = (x-\alpha)^2 \pmod{\ell}$$

which are related to the splitting behaviour of ℓ according to:

$$\left(\frac{D_\phi}{\ell}\right) = -1, 1, 0,$$

with some extra details to be filled in the third case that we have a 1-dimensional subspace. An interesting subcase of this is $\overline{\chi}_\phi(x) = x^2$ when $\ell \mid [\mathcal{O}_{K_\phi} : \mathrm{End}(E) \cap K_\phi]$.

Consequences

Corollary

Let $m > 1$ an integer coprime to $\mathrm{char}\mathbb{F}_q = p$ and $\phi \in \mathrm{End}(E) \setminus \mathbb{Z}$ with $D_\phi = \mathrm{disc}(\mathbb{Z}[\phi])$.

$$\phi \text{ distorts } E[m] \iff$$

$$\phi \text{ distorts } E[\ell], \text{ for all } \ell \mid m \iff$$

$$\left(\frac{D_\phi}{\ell}\right) = -1 \text{ for all } \ell \mid m$$

Consequences

Corollary

Let $m > 1$ an integer coprime to $\mathrm{char}\mathbb{F}_q = p$ and $\phi \in \mathrm{End}(E) \setminus \mathbb{Z}$ with $D_\phi = \mathrm{disc}(\mathbb{Z}[\phi])$.

$$\phi \text{ distorts } E[m] \iff$$

$$\phi \text{ distorts } E[\ell], \text{ for all } \ell \mid m \iff$$

$$\left(\frac{D_\phi}{\ell}\right) = -1 \text{ for all } \ell \mid m$$

Two notable things: 1) Density of primes 2) $m = \ell^k$

Consequences

Corollary

Let $m > 1$ an integer coprime to $\mathrm{char}\mathbb{F}_q = p$ and $\phi \in \mathrm{End}(E) \setminus \mathbb{Z}$ with $D_\phi = \mathrm{disc}(\mathbb{Z}[\phi])$.

$$\phi \text{ distorts } E[m] \iff$$
$$\phi \text{ distorts } E[\ell], \text{ for all } \ell \mid m \iff$$
$$\left(\frac{D_\phi}{\ell}\right) = -1 \text{ for all } \ell \mid m$$

Two notable things: 1) Density of primes 2) $m = \ell^k$

Transfer via isogenies (FP-team)

Consider $E_1, E_2/\mathbb{F}_q$ and an isogeny $\psi : E_1 \to E_2$, with $d := \deg \psi$ and its dual $\hat{\psi} : E_2 \to E_1$, i.e. $\psi\hat{\psi} = [d]$. Then,

Consequences

Corollary

Let $m > 1$ an integer coprime to $\mathrm{char}\mathbb{F}_q = p$ and $\phi \in \mathrm{End}(E) \setminus \mathbb{Z}$ with $D_\phi = \mathrm{disc}(\mathbb{Z}[\phi])$.

$$\phi \text{ distorts } E[m] \iff$$
$$\phi \text{ distorts } E[\ell], \text{ for all } \ell \mid m \iff$$
$$\left(\frac{D_\phi}{\ell}\right) = -1 \text{ for all } \ell \mid m$$

Two notable things: 1) Density of primes 2) $m = \ell^k$

Transfer via isogenies (FP-team)

Consider $E_1, E_2/\mathbb{F}_q$ and an isogeny $\psi : E_1 \to E_2$, with $d := \deg \psi$ and its dual $\hat{\psi} : E_2 \to E_1$, i.e. $\psi\hat{\psi} = [d]$. Then, if P is in $E_1[m]$, with $(m, pd) = 1$ and ϕ is a distortion map for P, then $\psi \circ \phi \circ \widehat{\psi}$ is a distortion map for $\psi(P)$.

The Ordinary case

Theorem (Verheul)

Let $P \in E(\mathbb{F}_q)$ be a point of order ℓ. If $E[\ell]$ is not defined over $\mathbb{F}_q$, then P does not admit a distortion map.

The Ordinary case

Theorem (Verheul)

Let $P \in E(\mathbb{F}_q)$ be a point of order ℓ. If $E[\ell]$ is not defined over $\mathbb{F}_q$, then P does not admit a distortion map.

$$E[\ell] \cap E(\mathbb{F}_q) = \langle P \rangle, \quad \pi_q(\phi(P)) = \phi(\pi_q(P)) = \phi(P)$$

$$\Longrightarrow \ \phi(P) \in \langle P \rangle$$

The Ordinary case

Theorem (Verheul)

Let $P \in E(\mathbb{F}_q)$ be a point of order ℓ. If $E[\ell]$ is not defined over $\mathbb{F}_q$, then P does not admit a distortion map.

$$E[\ell] \cap E(\mathbb{F}_q) = \langle P \rangle, \quad \pi_q(\phi(P)) = \phi(\pi_q(P)) = \phi(P)$$

$$\Longrightarrow \ \phi(P) \in \langle P \rangle$$

Charles' Theorem

Assume $E[\ell] \subseteq E(\mathbb{F}_q)$ (possibly by extending the initial $\mathbb{F}_q$), set $D = \mathrm{disc}(\mathrm{End}(E))$. Then $(D/\ell) = -1, 1, 0$ classifies the existence of distortion maps on the points of $E[\ell]$.

On the shoulders of giants

$\mathbb{Z}_\ell$ denotes the ℓ-adic integers $\mathbb{Z}_\ell = \varprojlim \mathbb{Z}/\ell^n\mathbb{Z}$.

A Theorem of Tate

Let K be a finite field and E/K be an elliptic curve. Fix a prime $\ell \neq \mathrm{char}(K)$ and let $\mathrm{End}_K(T_\ell(E))$ denote the ring of $\mathrm{Gal}(\overline{K}/K)$-equivariant $\mathbb{Z}_\ell$-linear endomorphisms of $T_\ell(E) := \varprojlim E[\ell^n]$. The canonical map

$$\mathrm{End}_K(E) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \quad \longrightarrow \quad \mathrm{End}_K(T_\ell(E))$$

is an isomorphism of rings.

The supersingular case

Theorem (Verheul, Schoof)

For a supersingular elliptic curve $E/\mathbb{F}_q$ and a point $P \in E[\ell]$, $\ell \neq p$, there exists a distortion map for P.

The supersingular case

Theorem (Verheul, Schoof)

For a supersingular elliptic curve $E/\mathbb{F}_q$ and a point $P \in E[\ell]$, $\ell \neq p$, there exists a distortion map for P.

Theorem (FP-team)

Let E be a supersingular elliptic curve over a finite field $\mathbb{F}_q$ and let $m > 1$ be an integer coprime to q. Then $E[m]$ admits a distortion map.

Proof (Sketch)

Step 1: Center of $\mathrm{End}(E)$ is $\mathbb{Z}$ for a supersingular elliptic curve. $B = \mathrm{End}(E) \otimes \mathbb{Q}$ is a quaternion algebra over $\mathbb{Q}$ which is a central $\mathbb{Q}$-algebra.

Proof (Sketch)

Step 1: Center of $\mathrm{End}(E)$ is $\mathbb{Z}$ for a supersingular elliptic curve. $B = \mathrm{End}(E) \otimes \mathbb{Q}$ is a quaternion algebra over $\mathbb{Q}$ which is a central $\mathbb{Q}$-algebra.

Step 2: Work over $K = \mathbb{F}_{q^k}$ the minimal field of definition of $\mathrm{End}(E)$. Use Step 1 to show that π_{q^k} is in $\mathbb{Z}$. From the Theorem of Tate deduce that $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \cong \mathrm{End}(T_\ell(E))$ as $(x \mapsto x^{q^k})$ profinitely generates $\mathrm{Gal}(\overline{K}/K)$ and commutes with every element of $\mathrm{End}(E)$.

Proof (Sketch)

Step 1: Center of $\mathrm{End}(E)$ is $\mathbb{Z}$ for a supersingular elliptic curve. $B = \mathrm{End}(E) \otimes \mathbb{Q}$ is a quaternion algebra over $\mathbb{Q}$ which is a central $\mathbb{Q}$-algebra.

Step 2: Work over $K = \mathbb{F}_{q^k}$ the minimal field of definition of $\mathrm{End}(E)$. Use Step 1 to show that π_{q^k} is in $\mathbb{Z}$. From the Theorem of Tate deduce that $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \cong \mathrm{End}(T_\ell(E))$ as $(x \mapsto x^{q^k})$ profinitely generates $\mathrm{Gal}(\overline{K}/K)$ and commutes with every element of $\mathrm{End}(E)$.

Step 3: Use the canonical surjection $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \longrightarrow \mathrm{End}_{\mathbb{Z}/\ell^n\mathbb{Z}}(E[\ell^n])$

Proof (Sketch)

Step 1: Center of $\mathrm{End}(E)$ is $\mathbb{Z}$ for a supersingular elliptic curve. $B = \mathrm{End}(E) \otimes \mathbb{Q}$ is a quaternion algebra over $\mathbb{Q}$ which is a central $\mathbb{Q}$-algebra.

Step 2: Work over $K = \mathbb{F}_{q^k}$ the minimal field of definition of $\mathrm{End}(E)$. Use Step 1 to show that π_{q^k} is in $\mathbb{Z}$. From the Theorem of Tate deduce that $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \cong \mathrm{End}(T_\ell(E))$ as $(x \mapsto x^{q^k})$ profinitely generates $\mathrm{Gal}(\overline{K}/K)$ and commutes with every element of $\mathrm{End}(E)$.

Step 3: Use the canonical surjection $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \longrightarrow \mathrm{End}_{\mathbb{Z}/\ell^n\mathbb{Z}}(E[\ell^n])$

Step 4: Use density of $\mathbb{Z} \hookrightarrow \mathbb{Z}_\ell$ to drop "$\otimes\mathbb{Z}_\ell$" and CRT for $m = \prod \ell_i^{n_i}$.

Proof (Sketch)

Step 1: Center of $\mathrm{End}(E)$ is $\mathbb{Z}$ for a supersingular elliptic curve. $B = \mathrm{End}(E) \otimes \mathbb{Q}$ is a quaternion algebra over $\mathbb{Q}$ which is a central $\mathbb{Q}$-algebra.

Step 2: Work over $K = \mathbb{F}_{q^k}$ the minimal field of definition of $\mathrm{End}(E)$. Use Step 1 to show that π_{q^k} is in $\mathbb{Z}$. From the Theorem of Tate deduce that $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \cong \mathrm{End}(T_\ell(E))$ as $(x \mapsto x^{q^k})$ profinitely generates $\mathrm{Gal}(\overline{K}/K)$ and commutes with every element of $\mathrm{End}(E)$.

Step 3: Use the canonical surjection $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \longrightarrow \mathrm{End}_{\mathbb{Z}/\ell^n\mathbb{Z}}(E[\ell^n])$

Step 4: Use density of $\mathbb{Z} \hookrightarrow \mathbb{Z}_\ell$ to drop "$\otimes\mathbb{Z}_\ell$" and CRT for $m = \prod \ell_i^{n_i}$.

Step 5: Find matrix in $M_2(\mathbb{Z}/m\mathbb{Z})$ with no eigenvectors. This is done by picking for each $E[\ell^n]$ the matrix $A = (0\ \overline{\alpha}, 1\ 0)$ for $\overline{\alpha}$ the image of a quadratic non-redisude α modulo ℓ.

Example 1

Let $E/\mathbb{C}$ with equation $y^2 = x^3 + 1$ and complex multiplication by $[\zeta] : (x, y) \mapsto (\zeta x, y)$ for ζ a primitive third root of unity. Based on the arithmetic of $\mathbb{Q}(\zeta)$, and the Deuring reduction theorem, reducting to $p = 2 \mod 3$ yields a supersingular curve, and $p = 1 \mod 3$ an ordinary.

Example 1

Let $E/\mathbb{C}$ with equation $y^2 = x^3 + 1$ and complex multiplication by $[\zeta] : (x, y) \mapsto (\zeta x, y)$ for ζ a primitive third root of unity. Based on the arithmetic of $\mathbb{Q}(\zeta)$, and the Deuring reduction theorem, reducting to $p = 2 \mod 3$ yields a supersingular curve, and $p = 1 \mod 3$ an ordinary.

$E/\mathbb{F}_{13}$ is ordinary and ζ can be $3 \mod 13$, thus the distortion map is simply $(x, y) \mapsto (3x, y)$. By computation $\#E(\mathbb{F}_{13}) = 12$, so we check the primes $\ell = 2, 3$. $E[3]$ is not defined in $\mathbb{F}_{13}$ so no distortion map on $E[3]$. Also $E[2] = \{\mathcal{O}, (4, 0), (10, 0), (12, 0)\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. It is easy to see all four points are distorted. Observe that $D_{[\zeta]} = -3$ and $(-3/2) = -1$. (In general $(D/2) = -1$ if $D = \pm 3 \mod 8$).

Example 1

Let $E/\mathbb{C}$ with equation $y^2 = x^3 + 1$ and complex multiplication by $[\zeta] : (x, y) \mapsto (\zeta x, y)$ for ζ a primitive third root of unity. Based on the arithmetic of $\mathbb{Q}(\zeta)$, and the Deuring reduction theorem, reducting to $p = 2 \mod 3$ yields a supersingular curve, and $p = 1 \mod 3$ an ordinary.

$E/\mathbb{F}_{13}$ is ordinary and ζ can be $3 \mod 13$, thus the distortion map is simply $(x, y) \mapsto (3x, y)$. By computation $\#E(\mathbb{F}_{13}) = 12$, so we check the primes $\ell = 2, 3$. $E[3]$ is not defined in $\mathbb{F}_{13}$ so no distortion map on $E[3]$. Also $E[2] = \{\mathcal{O}, (4, 0), (10, 0), (12, 0)\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. It is easy to see all four points are distorted. Observe that $D_{[\zeta]} = -3$ and $(-3/2) = -1$. (In general $(D/2) = -1$ if $D = \pm 3 \mod 8$).

For the supersingular $E/\mathbb{F}_{11}$, we have to extend to $\mathbb{F}_{11^2}$ to define $[\zeta]$. Nonetheless, again it holds that as $D_{[\zeta]} = -3$ and $\#E(\mathbb{F}_{11}) = 12$. As $(-3/2) = -1$, the map $[\zeta]$ distorts the entire $E[2]$.

Example 2

Let $E/\mathbb{F}_{13}$ be given by $y^2 = x^3 + 11x + 4$. E is ordinary and $E[2]$ is defined over $\mathbb{F}_{13}$. Its conductor $[\mathcal{O}_K : \mathrm{End}(E)]$ is 2 for $K = \mathbb{Q}(\sqrt{-3})$ (by Deuring reduction from $y^2 = x^3 - 3375/121x + 675/121$ over $\mathbb{C}$). So we expect a nilpotent action, recall $\overline{\chi}_\phi(x) = x^2$.

Example 2

Let $E/\mathbb{F}_{13}$ be given by $y^2 = x^3 + 11x + 4$. E is ordinary and $E[2]$ is defined over $\mathbb{F}_{13}$. Its conductor $[\mathcal{O}_K : \mathrm{End}(E)]$ is 2 for $K = \mathbb{Q}(\sqrt{-3})$ (by Deuring reduction from $y^2 = x^3 - 3375/121x + 675/121$ over $\mathbb{C}$). So we expect a nilpotent action, recall $\overline{\chi}_\phi(x) = x^2$.

Extend the field to $\mathbb{F}_{13^2} = \mathbb{F}_{13}[X]/(X^6 + 10X^3 + 11X^2 + 11^X + 2)$, generated by z. Then $P = (4, 3z^5 + 9z^4 + 7z^3 + 12z + 5)$ is in $E[4]$. The group $\langle P \rangle$ can be the kernel of some isogeny $\psi : E \to E'$. A method by Vélu recovers $E' : y^2 = x^3 + 8x + 9$ and the coordinates of the isogeny ψ given $\langle P \rangle$, and is implemented in SageMath. For this example it holds that $j(E') = j(E)$. Thus there is an isomorphism $\gamma : E' \to E$, $(x, y) \mapsto (4x, -5y)$.

Example 2

Let $E/\mathbb{F}_{13}$ be given by $y^2 = x^3 + 11x + 4$. E is ordinary and $E[2]$ is defined over $\mathbb{F}_{13}$. Its conductor $[\mathcal{O}_K : \mathrm{End}(E)]$ is 2 for $K = \mathbb{Q}(\sqrt{-3})$ (by Deuring reduction from $y^2 = x^3 - 3375/121x + 675/121$ over $\mathbb{C}$). So we expect a nilpotent action, recall $\overline{\chi}_\phi(x) = x^2$.

Extend the field to $\mathbb{F}_{13^2} = \mathbb{F}_{13}[X]/(X^6 + 10X^3 + 11X^2 + 11^X + 2)$, generated by z. Then $P = (4, 3z^5 + 9z^4 + 7z^3 + 12z + 5)$ is in $E[4]$. The group $\langle P \rangle$ can be the kernel of some isogeny $\psi : E \to E'$. A method by Vélu recovers $E' : y^2 = x^3 + 8x + 9$ and the coordinates of the isogeny ψ given $\langle P \rangle$, and is implemented in SageMath. For this example it holds that $j(E') = j(E)$. Thus there is an isomorphism $\gamma : E' \to E$, $(x, y) \mapsto (4x, -5y)$. Set $\phi = \gamma \circ \psi$. On $E[2]$ we have:

$$\phi(11, 0) = \mathcal{O},\ \phi(6, 0) = (11, 0),\ \phi(9, 0) = (11, 0).$$

Algorithmic Aspects

Assume that for an elliptic curve over $\mathbb{F}_p$, we do not know which curve $/\mathbb{C}$ was used to construct it.

Algorithmic Aspects

Assume that for an elliptic curve over $\mathbb{F}_p$, we do not know which curve $/\mathbb{C}$ was used to construct it.

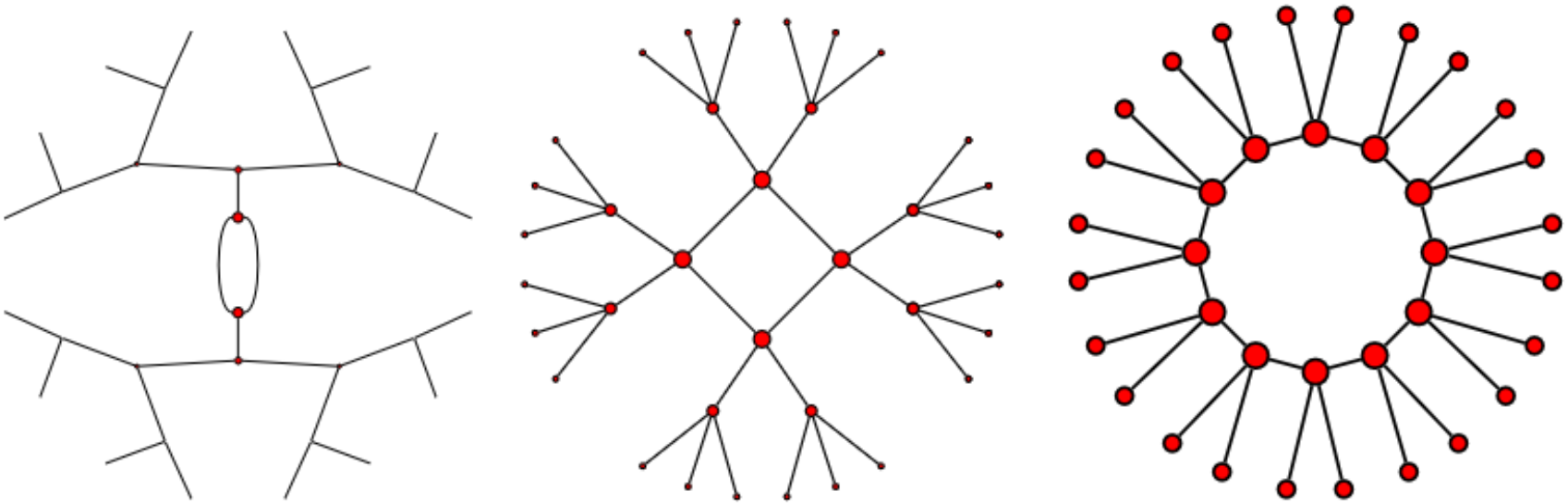
Over $\mathbb{F}_p$ all supersingular curves are isogenous and form a complete isogeny graph. Based on this, Galbraith and Rotger gave an alternative proof of Verheul and Schoof's Theorem by considering isogeny paths on the graphs. Once we reach the same j-invariant as the one we started, we twist with an isomorphism to get a distortion map.

$$E = E_0 \xrightarrow{\psi_1} E_1 \xrightarrow{\psi_2} \cdots \xrightarrow{\psi_{c-1}} E_{c-1} \xrightarrow{\psi_c} E_c = E' \overset{\gamma}{\simeq} E.$$

Their algorithm is *constructive*.

Algorithmic Aspects

Over $\mathbb{F}_p$ the isogeny graphs form volcanoes:



The same idea is used in the "Distorting the Volcano" paper by M. Fouquet, J. Miret and J. Valera, but there does not exist a deterministic algorithm *yet*.

(Figure from "Ordinary isogeny graphs over $\mathbb{F}_p$: the inverse volcano problem" by H.Bambury, F. Campagna, F. Pazuki)

References

- Distortion Maps for Elliptic Curves over Finite Fields, N. Andrusov, S. Büyüksimkeşyan, D. N., F. Pazuki, M. U. Kazancıoğlu, J. Vilà-Casadevall. To appear in: The Polynesian Journal of Mathematics, Special Volume "AJAX": Arithmetic, Jacobians, Algorithms & Exposition — Celebrating the mathematics of René Schoof, 2026.
- J. H. Silverman. The Arithmetic of Elliptic Curves. 2nd. Vol. 106. Graduate Texts in Mathematics. Springer, 2009.
- E. R. Verheul. "Evidence that XTR Is More Secure than Supersingular Elliptic Curve Cryptosystems". In: J. Cryptology 17 (2004), pp. 277–296.
- D. Charles. On the existence of distortion maps on ordinary elliptic curves. 2006. arXiv:math/0603724 [math.NT].

Thank you for your attention!