Orienteering on Supersingular Isogeny Volcanoes Using One Endomorphism

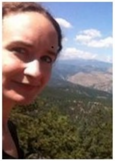
Renate Scheidler

UNIVERSITY OF CALGARY

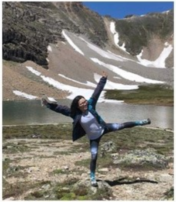
Joint work with **Sarah Arpin**, **Mingjie Chen**, **Kristin E. Lauter**, **Katherine E. Stange** and **Ha T. N Tran** (thanks to *Women in Numbers* 5)

Number Theory and Combinatorics Seminar
University of Lethbridge
March 13, 2023

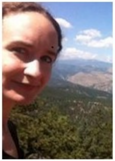
Let the Adventure Begin . . .



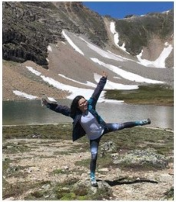


Let the Adventure Begin . . .



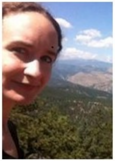


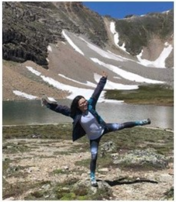
Orienteering

Finding one's way across to checkpoints across varied terrain using only map and compass.

Let the Adventure Begin . . .





Orienteering

Finding one's way across to checkpoints across varied terrain using only map and compass.

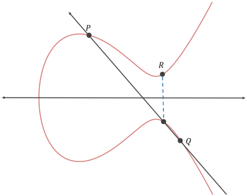
- Our terrain: oriented supersingular ℓ-isogeny volcano
- Our wayfinding tool: one endomorphism
- Our task: get to a given elliptic curve (which we may or may not reach)

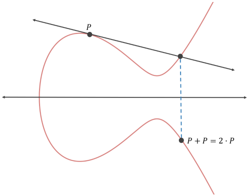
Isogenies

Let $E/\mathbb{F}_q$ be an elliptic curve ($q = p^n$ with p prime).

Let $E/\mathbb{F}_q$ be an elliptic curve ($q = p^n$ with p prime).

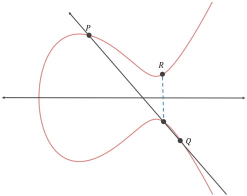
The points on E (over any extension of $\mathbb{F}_q$) form a finite abelian group under "cord & tangent" addition:

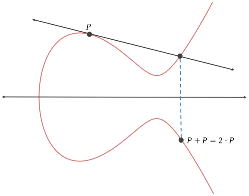




Let $E/\mathbb{F}_q$ be an elliptic curve ($q = p^n$ with p prime).

The points on E (over any extension of $\mathbb{F}_q$) form a finite abelian group under "cord & tangent" addition:



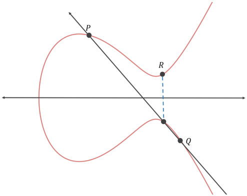


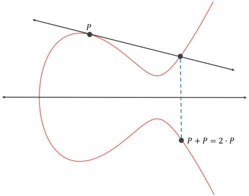
Isogeny: non-trivial group homomorphism between elliptic curves;

Isogenies

Let $E/\mathbb{F}_q$ be an elliptic curve ($q = p^n$ with p prime).

The points on E (over any extension of $\mathbb{F}_q$) form a finite abelian group under "cord & tangent" addition:



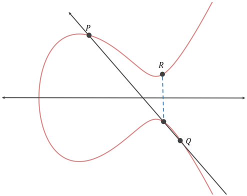


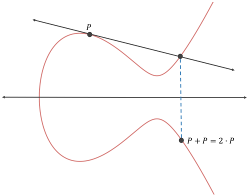
Isogeny: non-trivial group homomorphism between elliptic curves;

Degree of an isogeny φ: degree as an algebraic map

Let $E/\mathbb{F}_q$ be an elliptic curve ($q = p^n$ with p prime).

The points on E (over any extension of $\mathbb{F}_q$) form a finite abelian group under "cord & tangent" addition:





Isogeny: non-trivial group homomorphism between elliptic curves;

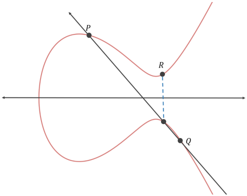
Degree of an isogeny φ: degree as an algebraic map

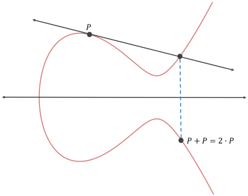
- If $p \nmid \deg(\varphi)$, then $\deg(\varphi) = \#\ker(\varphi)$

Isogenies

Let $E/\mathbb{F}_q$ be an elliptic curve ($q = p^n$ with p prime).

The points on E (over any extension of $\mathbb{F}_q$) form a finite abelian group under "cord & tangent" addition:





Isogeny: non-trivial group homomorphism between elliptic curves;

Degree of an isogeny φ: degree as an algebraic map

- If $p \nmid \deg(\varphi)$, then $\deg(\varphi) = \# \ker(\varphi)$
- Every subgroup $G \subset E(\overline{\mathbb{F}}_q)$ is the kernel of such an isogeny, computable via Vélu's formulas (Vélu 1971)

Isogeny Path Finding

Isogeny Path Finding Problem

Given a set $\mathcal{L}$ of primes (small, distinct from p) and two elliptic curves E, E' over $\mathbb{F}_q$, find an $\mathcal{L}$-**isogeny path** from E to E',

Isogeny Path Finding

Isogeny Path Finding Problem

Given a set $\mathcal{L}$ of primes (small, distinct from p) and two elliptic curves E, E' over $\mathbb{F}_q$, find an $\mathcal{L}$-**isogeny path** from E to E', i.e. a sequence

$$\rho : E = E_0 \xrightarrow{\varphi_1} E_1 \xrightarrow{\varphi_2} E_2 \xrightarrow{\varphi_3} \cdots \xrightarrow{\varphi_m} E_m = E'$$

of isogenies with $\deg(\varphi_i) \in \mathcal{L}$ for $1 \leq i \leq m$.

Isogeny Path Finding

Isogeny Path Finding Problem

Given a set $\mathcal{L}$ of primes (small, distinct from p) and two elliptic curves E, E' over $\mathbb{F}_q$, find an $\mathcal{L}$-**isogeny path** from E to E', i.e. a sequence

$$\rho : E = E_0 \xrightarrow{\varphi_1} E_1 \xrightarrow{\varphi_2} E_2 \xrightarrow{\varphi_3} \cdots \xrightarrow{\varphi_m} E_m = E'$$

of isogenies with $\deg(\varphi_i) \in \mathcal{L}$ for $1 \leq i \leq m$.

Questions

- How hard is this problem computationally?
- How do we solve it?

Path Finding Applications

UNIVERSITY OF CALGARY

Cryptography

- Hash Functions (Charles-Goren-Lauter 2006/2009)
- Cryptographic key agreement
  (Couveignes 1996/2006, Rostovtsev-Stolbunov 2006, De Feo-Jao-Plût 2011 (broken), Castryck-Lange-Martindale-Panny-Renes 2018, Colò-Kohel 2020)
- Constructing elliptic curves with a hard discrete log problem
  (Belding-Bröker-Enge-Lauter 2008)

Path Finding Applications

Cryptography

- Hash Functions (Charles-Goren-Lauter 2006/2009)
- Cryptographic key agreement
  (Couveignes 1996/2006, Rostovtsev-Stolbunov 2006, De Feo-Jao-Plût 2011 (broken), Castryck-Lange-Martindale-Panny-Renes 2018, Colò-Kohel 2020)
- Constructing elliptic curves with a hard discrete log problem
  (Belding-Bröker-Enge-Lauter 2008)

Computing endomorphism rings (Kohel 1996, Bisson-Sutherland 2011)

Path Finding Applications

UNIVERSITY OF CALGARY

Cryptography

- Hash Functions (Charles-Goren-Lauter 2006/2009)
- Cryptographic key agreement
  (Couveignes 1996/2006, Rostovtsev-Stolbunov 2006, De Feo-Jao-Plût 2011 (broken), Castryck-Lange-Martindale-Panny-Renes 2018, Colò-Kohel 2020)
- Constructing elliptic curves with a hard discrete log problem
  (Belding-Bröker-Enge-Lauter 2008)

Computing endomorphism rings (Kohel 1996, Bisson-Sutherland 2011)

Point counting (Elkies 1997, Fouquet-Morain 2002)

Path Finding Applications

UNIVERSITY OF CALGARY

Cryptography

- Hash Functions (Charles-Goren-Lauter 2006/2009)
- Cryptographic key agreement
  (Couveignes 1996/2006, Rostovtsev-Stolbunov 2006, De Feo-Jao-Plût 2011 (broken), Castryck-Lange-Martindale-Panny-Renes 2018, Colò-Kohel 2020)
- Constructing elliptic curves with a hard discrete log problem
  (Belding-Bröker-Enge-Lauter 2008)

Computing endomorphism rings (Kohel 1996, Bisson-Sutherland 2011)

Point counting (Elkies 1997, Fouquet-Morain 2002)

Computing modular polynomials (Bröker-Lauter-Sutherland 2012, Sutherland 2014)

Path Finding Applications

UNIVERSITY OF CALGARY

Cryptography

- Hash Functions (Charles-Goren-Lauter 2006/2009)
- Cryptographic key agreement
  (Couveignes 1996/2006, Rostovtsev-Stolbunov 2006, De Feo-Jao-Plût 2011 (broken), Castryck-Lange-Martindale-Panny-Renes 2018, Colò-Kohel 2020)
- Constructing elliptic curves with a hard discrete log problem
  (Belding-Bröker-Enge-Lauter 2008)

Computing endomorphism rings (Kohel 1996, Bisson-Sutherland 2011)

Point counting (Elkies 1997, Fouquet-Morain 2002)

Computing modular polynomials (Bröker-Lauter-Sutherland 2012, Sutherland 2014)

Generating irreducible polynomials (Couveignes-Lercier 2013)

Path Finding Algorithms

E, E' ordinary (p-torsion $\mathbb{Z}/p\mathbb{Z}$):

- Classical: $\tilde{O}(q^{1/4})$ (Galbraith-Heß-Smart 2002)
- Quantum: $\exp\left(\frac{\sqrt{3}}{2}\sqrt{\log q \log\log q}\right)$ (Childs-Jao-Shoukarev 2014)

Path Finding Algorithms

UNIVERSITY OF CALGARY

E, E' ordinary (p-torsion $\mathbb{Z}/p\mathbb{Z}$):

- Classical: $\tilde{O}(q^{1/4})$ (Galbraith-Heß-Smart 2002)
- Quantum: $\exp\left(\frac{\sqrt{3}}{2}\sqrt{\log q \log\log q}\right)$ (Childs-Jao-Shoukarev 2014)

E, E' supersingular (p-torsion trivial) and defined over $\mathbb{F}_p$:

- Classical : $\tilde{O}(p^{1/4})$ (Delfts-Galbraith 2014)
- Quantum : $\exp\left(\frac{\sqrt{3}}{2}\sqrt{\log p \log\log p}\right)$ (Biasse-Jao-Sankar 2014)

Path Finding Algorithms

UNIVERSITY OF CALGARY

E, E' ordinary (p-torsion $\mathbb{Z}/p\mathbb{Z}$):

- Classical: $\tilde{O}(q^{1/4})$ (Galbraith-Heß-Smart 2002)
- Quantum: $\exp\left(\frac{\sqrt{3}}{2}\sqrt{\log q \log\log q}\right)$ (Childs-Jao-Shoukarev 2014)

E, E' supersingular (p-torsion trivial) and defined over $\mathbb{F}_p$:

- Classical : $\tilde{O}(p^{1/4})$ (Delfts-Galbraith 2014)
- Quantum : $\exp\left(\frac{\sqrt{3}}{2}\sqrt{\log p \log\log p}\right)$ (Biasse-Jao-Sankar 2014)

E, E' supersingular, in general (i.e. defined over $\mathbb{F}_{p^2}$):

- Classical: $\tilde{O}(p^{1/2})$ (Delfts-Galbraith 2014)
- Quantum: $\tilde{O}(p^{1/4})$ (Biasse-Jao-Sankar 2014)

Path Finding Algorithms

E, E' ordinary (p-torsion $\mathbb{Z}/p\mathbb{Z}$):

- Classical: $\tilde{O}(q^{1/4})$ (Galbraith-Heß-Smart 2002)
- Quantum: $\exp\left(\frac{\sqrt{3}}{2}\sqrt{\log q \log\log q}\right)$ (Childs-Jao-Shoukarev 2014)

E, E' supersingular (p-torsion trivial) and defined over $\mathbb{F}_p$:

- Classical : $\tilde{O}(p^{1/4})$ (Delfts-Galbraith 2014)
- Quantum : $\exp\left(\frac{\sqrt{3}}{2}\sqrt{\log p \log\log p}\right)$ (Biasse-Jao-Sankar 2014)

E, E' supersingular, in general (i.e. defined over $\mathbb{F}_{p^2}$):

- Classical: $\tilde{O}(p^{1/2})$ (Delfts-Galbraith 2014)
- Quantum: $\tilde{O}(p^{1/4})$ (Biasse-Jao-Sankar 2014)

This work: New subexponential algorithms

Path Finding Algorithms

UNIVERSITY OF CALGARY

E, E' ordinary (p-torsion $\mathbb{Z}/p\mathbb{Z}$):

- Classical: $\tilde{O}(q^{1/4})$ (Galbraith-Heß-Smart 2002)
- Quantum: $\exp\left(\frac{\sqrt{3}}{2}\sqrt{\log q \log\log q}\right)$ (Childs-Jao-Shoukarev 2014)

E, E' supersingular (p-torsion trivial) and defined over $\mathbb{F}_p$:

- Classical : $\tilde{O}(p^{1/4})$ (Delfts-Galbraith 2014)
- Quantum : $\exp\left(\frac{\sqrt{3}}{2}\sqrt{\log p \log\log p}\right)$ (Biasse-Jao-Sankar 2014)

E, E' supersingular, in general (i.e. defined over $\mathbb{F}_{p^2}$):

- Classical: $\tilde{O}(p^{1/2})$ (Delfts-Galbraith 2014)
- Quantum: $\tilde{O}(p^{1/4})$ (Biasse-Jao-Sankar 2014)

This work: New subexponential algorithms

Different subexponential algorithms due to Wesolowski 2021 (concurrently)

Endomorphism Ring

Endomorphism of E: group homomorphism $E \to E$

Endomorphism Ring

Endomorphism of E: group homomorphism $E \to E$

The endomorphisms of E form a ring under addition and composition called the **endomorphism ring** of E and denoted $\mathrm{End}(E)$.

Endomorphism Ring

UNIVERSITY OF CALGARY

Endomorphism of E: group homomorphism $E \to E$

The endomorphisms of E form a ring under addition and composition called the **endomorphism ring** of E and denoted $\text{End}(E)$.

By the theory of *complex multiplication*, $\text{End}(E)$ is isomorphic to

- an imaginary quadratic order $\mathcal{O}$ when E is **ordinary** (non-trivial p-torsion)
- a maximal order $\mathcal{O}$ in the quaternion algebra ramified at p and ∞ when E is **supersingular** (trivial p-torsion)

Endomorphism Ring

Endomorphism of E: group homomorphism $E \to E$

The endomorphisms of E form a ring under addition and composition called the **endomorphism ring** of E and denoted $\mathrm{End}(E)$.

By the theory of *complex multiplication*, $\mathrm{End}(E)$ is isomorphic to

- an imaginary quadratic order $\mathcal{O}$ when E is **ordinary** (non-trivial p-torsion)
- a maximal order $\mathcal{O}$ in the quaternion algebra ramified at p and ∞ when E is **supersingular** (trivial p-torsion)

E has **complex multiplication** (CM) **by** $\mathcal{O}$: $\mathrm{End}(E) \cong \mathcal{O}$.

How Hard is Path Finding?

Path finding for supersingular elliptic curves is equivalent to computing endomorphism rings (Eisenträger-Hallgren-Lauter-Morrison-Petit 2018, Wesolowski 2022).

How Hard is Path Finding?

Path finding for supersingular elliptic curves is equivalent to computing endomorphism rings (Eisenträger-Hallgren-Lauter-Morrison-Petit 2018, Wesolowski 2022).

Easy **if**

- The endomorphism rings are known (Kohel-Lauter-Petit-Tignol 2014)
- One small non-integer endomorphism is known (Love-Boneh 2020)

How Hard is Path Finding?

Path finding for supersingular elliptic curves is equivalent to computing endomorphism rings (Eisenträger-Hallgren-Lauter-Morrison-Petit 2018, Wesolowski 2022).

Easy **if**

- The endomorphism rings are known (Kohel-Lauter-Petit-Tignol 2014)
- One small non-integer endomorphism is known (Love-Boneh 2020)

Problem:

- Finding endomorphism rings is hard
- Small non-integer endomorphisms are rare and hard to find

How Hard is Path Finding?

Path finding for supersingular elliptic curves is equivalent to computing endomorphism rings (Eisenträger-Hallgren-Lauter-Morrison-Petit 2018, Wesolowski 2022).

Easy **if**

- The endomorphism rings are known (Kohel-Lauter-Petit-Tignol 2014)
- One small non-integer endomorphism is known (Love-Boneh 2020)

Problem:

- Finding endomorphism rings is hard
- Small non-integer endomorphisms are rare and hard to find

Question: Can paths be found with one (possibly large) endomorphism?

j-Invariant

j-**invariant** of $E : y^2 = x^3 + ax + b \quad (a, b \in \mathbb{F}_q,\ p \geq 5)$:

$$j(E) = 1728 \, \frac{4a^3}{4a^3 + 27b^2} \in \mathbb{F}_q$$

j-Invariant

j-**invariant** of $E : y^2 = x^3 + ax + b \quad (a, b \in \mathbb{F}_q,\ p \geq 5)$:

$$j(E) = 1728 \, \frac{4a^3}{4a^3 + 27b^2} \in \mathbb{F}_q$$

Properties:

- Every $j \in \mathbb{F}_q$ is the j-invariant of some elliptic curve over $\mathbb{F}_q$

j-Invariant

j-**invariant** of $E : y^2 = x^3 + ax + b \quad (a, b \in \mathbb{F}_q,\ p \geq 5)$:

$$j(E) = 1728 \, \frac{4a^3}{4a^3 + 27b^2} \in \mathbb{F}_q$$

Properties:

- Every $j \in \mathbb{F}_q$ is the j-invariant of some elliptic curve over $\mathbb{F}_q$
- E supersingular $\Rightarrow j(E) \in \mathbb{F}_{p^2}$

j-Invariant

j-**invariant** of $E : y^2 = x^3 + ax + b \quad (a, b \in \mathbb{F}_q,\ p \geq 5)$:

$$j(E) = 1728 \, \frac{4a^3}{4a^3 + 27b^2} \in \mathbb{F}_q$$

Properties:

- Every $j \in \mathbb{F}_q$ is the j-invariant of some elliptic curve over $\mathbb{F}_q$
- E supersingular $\Rightarrow j(E) \in \mathbb{F}_{p^2}$
- The j-invariant is invariant under isomorphism (isomorphism = bijective isogeny)

Class Group Action

Let $E/\mathbb{F}_q$ be ordinary with an isomorphism $\iota : \mathcal{O} \xrightarrow{\sim} \mathrm{End}(E)$

1

2

Class Group Action

Let $E/\mathbb{F}_q$ be ordinary with an isomorphism $\iota : \mathcal{O} \xrightarrow{\sim} \mathrm{End}(E)$

For any invertible $\mathcal{O}$-ideal $\mathfrak{a}$ with $p \nmid \mathrm{Norm}(\mathfrak{a}) = [\mathcal{O} : \mathfrak{a}]$, the subgroup

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

defines an isogeny $\varphi_{\mathfrak{a}} : E \to E'$ with kernel $E[\mathfrak{a}]$ and $E' \cong E/E[\mathfrak{a}]$.

1

2

Class Group Action

Let $E/\mathbb{F}_q$ be ordinary with an isomorphism $\iota : \mathcal{O} \xrightarrow{\sim} \mathrm{End}(E)$

For any invertible $\mathcal{O}$-ideal $\mathfrak{a}$ with $p \nmid \mathrm{Norm}(\mathfrak{a}) = [\mathcal{O} : \mathfrak{a}]$, the subgroup

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

defines an isogeny $\varphi_{\mathfrak{a}} : E \to E'$ with kernel $E[\mathfrak{a}]$ and $E' \cong E/E[\mathfrak{a}]$.

This induces a faithful[1] and transitive[2] action of $\mathrm{Cl}(\mathcal{O})$ on the **CM torsor**

$$\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q) = \{j(E) \mid E \text{ an elliptic curve over } \mathbb{F}_q \text{ with } \mathrm{End}(E) \cong \mathcal{O}\}$$

[1] Only the principal ideal class acts trivially

[2] Any two j-invariants in $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$ are related by some ideal class

Class Group Action

Let $E/\mathbb{F}_q$ be ordinary with an isomorphism $\iota : \mathcal{O} \xrightarrow{\sim} \mathrm{End}(E)$

For any invertible $\mathcal{O}$-ideal $\mathfrak{a}$ with $p \nmid \mathrm{Norm}(\mathfrak{a}) = [\mathcal{O} : \mathfrak{a}]$, the subgroup

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

defines an isogeny $\varphi_{\mathfrak{a}} : E \to E'$ with kernel $E[\mathfrak{a}]$ and $E' \cong E/E[\mathfrak{a}]$.

This induces a faithful[1] and transitive[2] action of $\mathrm{Cl}(\mathcal{O})$ on the **CM torsor**

$$\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q) = \{j(E) \mid E \text{ an elliptic curve over } \mathbb{F}_q \text{ with } \mathrm{End}(E) \cong \mathcal{O}\}$$

via

$$[\mathfrak{a}] \star j(E) \;\mapsto\; j(E/E[\mathfrak{a}])$$

[1] Only the principal ideal class acts trivially

[2] Any two j-invariants in $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$ are related by some ideal class

Isogeny Graph

ℓ-**isogeny graph** $\mathcal{G}_\ell(\mathbb{F}_q)$ ($\ell \neq p$ prime):

- *Vertices*: $\mathbb{F}_q$, viewed as the set of isomorphism classes (j-invariants) of elliptic curves over $\mathbb{F}_q$ (independent of ℓ)
- *Directed Edges*: isogenies of degree ℓ

Isogeny Graph

ℓ-**isogeny graph** $\mathcal{G}_\ell(\mathbb{F}_q)$ ($\ell \neq p$ prime):

- *Vertices*: $\mathbb{F}_q$, viewed as the set of isomorphism classes (j-invariants) of elliptic curves over $\mathbb{F}_q$ (independent of ℓ)
- *Directed Edges*: isogenies of degree ℓ

By identifying an isogeny with its *dual*, $\mathcal{G}_\ell(\mathbb{F}_q)$ becomes an undirected graph.

Isogeny Graph

ℓ-**isogeny graph** $\mathcal{G}_\ell(\mathbb{F}_q)$ ($\ell \neq p$ prime):

- *Vertices*: $\mathbb{F}_q$, viewed as the set of isomorphism classes (j-invariants) of elliptic curves over $\mathbb{F}_q$ (independent of ℓ)
- *Directed Edges*: isogenies of degree ℓ

By identifying an isogeny with its *dual*, $\mathcal{G}_\ell(\mathbb{F}_q)$ becomes an undirected graph.

The **dual** of an isogeny $\varphi : E \to E'$ of degree n is the unique isogeny $\hat{\varphi} : E' \to E$ (same degree) such that

$$\hat{\varphi}\varphi = [n] \text{ on } E, \quad \varphi\hat{\varphi} = [n] \text{ on } E'$$

Isogeny Graph

ℓ-**isogeny graph** $\mathcal{G}_\ell(\mathbb{F}_q)$ ($\ell \neq p$ prime):

- *Vertices*: $\mathbb{F}_q$, viewed as the set of isomorphism classes (j-invariants) of elliptic curves over $\mathbb{F}_q$ (independent of ℓ)
- *Directed Edges*: isogenies of degree ℓ

By identifying an isogeny with its *dual*, $\mathcal{G}_\ell(\mathbb{F}_q)$ becomes an undirected graph.

The **dual** of an isogeny $\varphi : E \to E'$ of degree n is the unique isogeny $\hat{\varphi} : E' \to E$ (same degree) such that

$$\hat{\varphi}\varphi = [n] \text{ on } E, \quad \varphi\hat{\varphi} = [n] \text{ on } E'$$

where $[n]P = \underbrace{P + P + \cdots + P}_{n \text{ times}}$.

Structure of $\mathcal{G}_\ell(\mathbb{F}_q)$ (Kohel 1996)

$\mathcal{G}_\ell(\mathbb{F}_q)$ is a disconnected graph that is almost $(\ell + 1)$-regular.

Structure of $\mathcal{G}_\ell(\mathbb{F}_q)$ (Kohel 1996)

$\mathcal{G}_\ell(\mathbb{F}_q)$ is a disconnected graph that is almost $(\ell+1)$-regular.

- Almost every vertex is incident with $\ell + 1$ edges:
  - Every ℓ-isogeny on E has a kernel that is an order ℓ subgroup of $E[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$
  - There are $\ell + 1$ such subgroups

Structure of $\mathcal{G}_\ell(\mathbb{F}_q)$ (Kohel 1996)

UNIVERSITY OF CALGARY

$\mathcal{G}_\ell(\mathbb{F}_q)$ is a disconnected graph that is almost $(\ell+1)$-regular.

- Almost every vertex is incident with $\ell+1$ edges:
  - Every ℓ-isogeny on E has a kernel that is an order ℓ subgroup of $E[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$
  - There are $\ell+1$ such subgroups

Exceptions: $j=0$ and $j=1728$ and their neighbours:

- $j=0$ has CM by $\mathcal{O} \cong \mathbb{Z}[\sqrt{-1}]$
  $j=1728$ has CM by $\mathcal{O} \cong \mathbb{Z}[\sqrt{-3}]$
- These curves have extra automorphisms because of the extra units in $\mathcal{O}$

Structure of $\mathcal{G}_\ell(\mathbb{F}_q)$ (Kohel 1996)

$\mathcal{G}_\ell(\mathbb{F}_q)$ is a disconnected graph that is almost $(\ell+1)$-regular.

- Almost every vertex is incident with $\ell+1$ edges:
  - Every ℓ-isogeny on E has a kernel that is an order ℓ subgroup of $E[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$
  - There are $\ell+1$ such subgroups

  Exceptions: $j = 0$ and $j = 1728$ and their neighbours:
  - $j = 0$ has CM by $\mathcal{O} \cong \mathbb{Z}[\sqrt{-1}]$
    $j = 1728$ has CM by $\mathcal{O} \cong \mathbb{Z}[\sqrt{-3}]$
  - These curves have extra automorphisms because of the extra units in $\mathcal{O}$

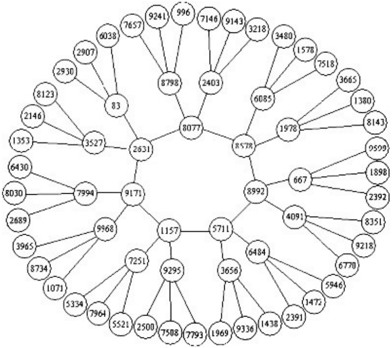
- All supersingular curves (there are about $p/12$ of them) lie in one connected component which is a **Ramanujan graph** (an optimal expander graph) when $p \equiv 1 \pmod{12}$ (Pizer 1990)

Structure of $\mathcal{G}_\ell(\mathbb{F}_q)$ (Kohel 1996)

$\mathcal{G}_\ell(\mathbb{F}_q)$ is a disconnected graph that is almost $(\ell + 1)$-regular.

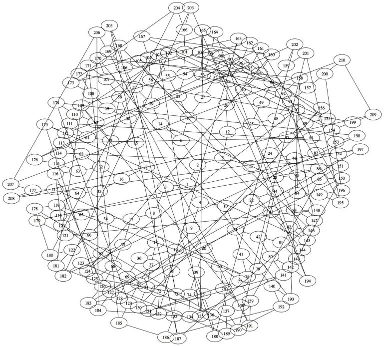
- Almost every vertex is incident with $\ell + 1$ edges:
  - Every ℓ-isogeny on E has a kernel that is an order ℓ subgroup of $E[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$
  - There are $\ell + 1$ such subgroups

  Exceptions: $j = 0$ and $j = 1728$ and their neighbours:
  - $j = 0$ has CM by $\mathcal{O} \cong \mathbb{Z}[\sqrt{-1}]$
    $j = 1728$ has CM by $\mathcal{O} \cong \mathbb{Z}[\sqrt{-3}]$
  - These curves have extra automorphisms because of the extra units in $\mathcal{O}$
- All supersingular curves (there are about $p/12$ of them) lie in one connected component which is a **Ramanujan graph** (an optimal expander graph) when $p \equiv 1 \pmod{12}$ (Pizer 1990)
- Ordinary components are **volcanoes** (Fouquet 2001, Fouquet-Morain 2002)



Ordinary component
($\ell = 3$)

Image: Dustin Moody



Supersingular component
($\ell = 2$)

Image: Dennis Charles

Volcanology

The ordinary components of $G_\ell(\mathbb{F}_q)$ are **volcanoes**:

3

Volcanology

The ordinary components of $G_\ell(\mathbb{F}_q)$ are **volcanoes**:

- Unique cycle (possibly degenerate) called the **rim**

3

UNIVERSITY OF CALGARY

The ordinary components of $G_\ell(\mathbb{F}_q)$ are **volcanoes**:

- Unique cycle (possibly degenerate) called the **rim**
- Each rim vertex is the root of a full[3] tree of height $h = v_\ell(f_\pi)$

[3] All leaf notes at the same level

Volcanology

The ordinary components of $G_\ell(\mathbb{F}_q)$ are **volcanoes**:

- Unique cycle (possibly degenerate) called the **rim**
- Each rim vertex is the root of a full[3] tree of height $h = v_\ell(f_\pi)$ where f_π is the conductor of the *Frobenius order* $\mathbb{Z}[\pi]$ with $\pi(x, y) = (x^q, y^q)$

[3] All leaf notes at the same level

Volcanology

The ordinary components of $G_\ell(\mathbb{F}_q)$ are **volcanoes**:

- Unique cycle (possibly degenerate) called the **rim**
- Each rim vertex is the root of a full[3] tree of height $h = v_\ell(f_\pi)$ where f_π is the conductor of the *Frobenius order* $\mathbb{Z}[\pi]$ with $\pi(x, y) = (x^q, y^q)$
- The nodes at level k $(0 \leq k \leq h)$ have CM by the order $\mathcal{O}_k$ whose conductor has ℓ-adic valuation k

[3] All leaf notes at the same level

Volcanology

The ordinary components of $G_\ell(\mathbb{F}_q)$ are **volcanoes**:

- Unique cycle (possibly degenerate) called the **rim**
- Each rim vertex is the root of a full[3] tree of height $h = v_\ell(f_\pi)$ where f_π is the conductor of the *Frobenius order* $\mathbb{Z}[\pi]$ with $\pi(x, y) = (x^q, y^q)$
- The nodes at level k $(0 \leq k \leq h)$ have CM by the order $\mathcal{O}_k$ whose conductor has ℓ-adic valuation k
- If $\mathfrak{l}$ is a prime ideal in $\mathcal{O}_0$ (the rim order) above ℓ, then the ideal class $[\mathfrak{l}] \in \mathrm{Cl}(\mathcal{O}_0)$ acts on the rim vertices; In particular, the rim has size $\mathrm{ord}([\mathfrak{l}])$

[3] All leaf notes at the same level

Volcanology

The ordinary components of $G_\ell(\mathbb{F}_q)$ are **volcanoes**:

- Unique cycle (possibly degenerate) called the **rim**
- Each rim vertex is the root of a full[3] tree of height $h = v_\ell(f_\pi)$ where f_π is the conductor of the *Frobenius order* $\mathbb{Z}[\pi]$ with $\pi(x, y) = (x^q, y^q)$
- The nodes at level k $(0 \le k \le h)$ have CM by the order $\mathcal{O}_k$ whose conductor has ℓ-adic valuation k
- If $\mathfrak{l}$ is a prime ideal in $\mathcal{O}_0$ (the rim order) above ℓ, then the ideal class $[\mathfrak{l}] \in \mathrm{Cl}(\mathcal{O}_0)$ acts on the rim vertices; In particular, the rim has size $\mathrm{ord}([\mathfrak{l}])$

The class group action significantly facilitates rim navigation!

[3] All leaf notes at the same level

Uses of Volcano Navigation

Walking down to the floor is used to

- Determine wether a curve is ordinary or supersingular (in the latter case, the floor is never reached)

Uses of Volcano Navigation

Walking down to the floor is used to

- Determine wether a curve is ordinary or supersingular (in the latter case, the floor is never reached)
- Computing ordinary endomorphism rings in subexponential time: for each ℓ dividing f_π, locate the ordinary curve in the ℓ-volcano and determine the level k via a path to the floor (assumes knowledge of the factorization of f_π)

Uses of Volcano Navigation

Walking down to the floor is used to

- Determine wether a curve is ordinary or supersingular (in the latter case, the floor is never reached)
- Computing ordinary endomorphism rings in subexponential time: for each ℓ dividing f_π, locate the ordinary curve in the ℓ-volcano and determine the level k via a path to the floor (assumes knowledge of the factorization of f_π)
- Point counting

Uses of Volcano Navigation

Walking down to the floor is used to

- Determine wether a curve is ordinary or supersingular (in the latter case, the floor is never reached)
- Computing ordinary endomorphism rings in subexponential time: for each ℓ dividing f_π, locate the ordinary curve in the ℓ-volcano and determine the level k via a path to the floor (assumes knowledge of the factorization of f_π)
- Point counting

Walking the rim is used to compute

- Hilbert class polynomials (needed in the CM method for constructing cryptographically suitable elliptic curves over a given field $\mathbb{F}_p$ with a given number of $\mathbb{F}_p$-points)

Uses of Volcano Navigation

Walking down to the floor is used to

- Determine wether a curve is ordinary or supersingular (in the latter case, the floor is never reached)
- Computing ordinary endomorphism rings in subexponential time: for each ℓ dividing f_π, locate the ordinary curve in the ℓ-volcano and determine the level k via a path to the floor (assumes knowledge of the factorization of f_π)
- Point counting

Walking the rim is used to compute

- Hilbert class polynomials (needed in the CM method for constructing cryptographically suitable elliptic curves over a given field $\mathbb{F}_p$ with a given number of $\mathbb{F}_p$-points)
- Modular polynomials $\Phi_\ell(X, Y)$: j, j' ℓ-isogenous iff $\Phi_\ell(j, j') = 0$

The Supersingular Component

The supersingular component of $\mathcal{G}_\ell(\mathbb{F}_q)$ is an expander graph – messy!

The Supersingular Component

The supersingular component of $\mathcal{G}_\ell(\mathbb{F}_q)$ is an expander graph – messy!

All the ordinary elliptic curves in $\mathcal{G}_\ell(\mathbb{F}_q)$ have CM by an order in the quadratic field $\mathbb{Q}(\pi) = \mathbb{Q}(\sqrt{-p})$ (*one* quadratic field).

The Supersingular Component

The supersingular component of $\mathcal{G}_\ell(\mathbb{F}_q)$ is an expander graph – messy!

All the ordinary elliptic curves in $\mathcal{G}_\ell(\mathbb{F}_q)$ have CM by an order in the quadratic field $\mathbb{Q}(\pi) = \mathbb{Q}(\sqrt{-p})$ (*one* quadratic field).

The supersingular curves generally have CM by a maximal order in a quaternion algebra (a non-commutative 4-dimensional object).

The Supersingular Component

The supersingular component of $\mathcal{G}_\ell(\mathbb{F}_q)$ is an expander graph – messy!

All the ordinary elliptic curves in $\mathcal{G}_\ell(\mathbb{F}_q)$ have CM by an order in the quadratic field $\mathbb{Q}(\pi) = \mathbb{Q}(\sqrt{-p})$ (*one* quadratic field).

The supersingular curves generally have CM by a maximal order in a quaternion algebra (a non-commutative 4-dimensional object).

- Many quadratic orders generally embed into $\mathrm{End}(E)$
- We can no longer navigate this component as for ordinary curves
- Path finding is much harder – good for cryptography!

The Supersingular Component

The supersingular component of $\mathcal{G}_\ell(\mathbb{F}_q)$ is an expander graph – messy!

All the ordinary elliptic curves in $\mathcal{G}_\ell(\mathbb{F}_q)$ have CM by an order in the quadratic field $\mathbb{Q}(\pi) = \mathbb{Q}(\sqrt{-p})$ (*one* quadratic field).

The supersingular curves generally have CM by a maximal order in a quaternion algebra (a non-commutative 4-dimensional object).

- Many quadratic orders generally embed into End(E)
- We can no longer navigate this component as for ordinary curves
- Path finding is much harder – good for cryptography!

Orientations to the rescue!

The Supersingular Component

The supersingular component of $\mathcal{G}_\ell(\mathbb{F}_q)$ is an expander graph – messy!

All the ordinary elliptic curves in $\mathcal{G}_\ell(\mathbb{F}_q)$ have CM by an order in the quadratic field $\mathbb{Q}(\pi) = \mathbb{Q}(\sqrt{-p})$ (*one* quadratic field).

The supersingular curves generally have CM by a maximal order in a quaternion algebra (a non-commutative 4-dimensional object).

- Many quadratic orders generally embed into $\mathrm{End}(E)$
- We can no longer navigate this component as for ordinary curves
- Path finding is much harder – good for cryptography!

Orientations to the rescue!

Our work: path finding with *one* endomorphism (orientation).

Oriented Elliptic Curves

Let

- E be an elliptic curve

[4] aka *optimal embedding* of E

Oriented Elliptic Curves

Let

- E be an elliptic curve
- K be an imaginary quadratic field in which p does not split

[4] aka *optimal embedding* of E

Oriented Elliptic Curves

UNIVERSITY OF CALGARY

Let

- E be an elliptic curve
- K be an imaginary quadratic field in which p does not split
  - Then K embeds into the quaternion algebra ramified at p and ∞ (in many ways)

[4] aka *optimal embedding* of E

Oriented Elliptic Curves

Let

- E be an elliptic curve
- K be an imaginary quadratic field in which p does not split
  - Then K embeds into the quaternion algebra ramified at p and ∞ (in many ways)

K-**Orientation of** E**:** $\iota : K \hookrightarrow \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$

[4] aka *optimal embedding* of E

Oriented Elliptic Curves

UNIVERSITY OF CALGARY

Let

- E be an elliptic curve
- K be an imaginary quadratic field in which p does not split
  - Then K embeds into the quaternion algebra ramified at p and ∞ (in many ways)

K-**Orientation of** E**:** $\iota : K \hookrightarrow \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$

- **Example:** ordinary $E/\mathbb{F}_q$ have $\mathbb{Q}(\sqrt{-p})$-orientations (isomorphisms)

[4] aka *optimal embedding* of E

Let

- E be an elliptic curve
- K be an imaginary quadratic field in which p does not split
  - Then K embeds into the quaternion algebra ramified at p and ∞ (in many ways)

K-**Orientation of** E**:** $\iota : K \hookrightarrow \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$

- **Example:** ordinary $E/\mathbb{F}_q$ have $\mathbb{Q}(\sqrt{-p})$-orientations (isomorphisms)

$\mathcal{O}$-**Orientation of** E ($\mathcal{O}$ an order of K): $\iota(\mathcal{O}) \subseteq \mathrm{End}(E)$

[4] aka *optimal embedding* of E

Oriented Elliptic Curves

Let

- E be an elliptic curve
- K be an imaginary quadratic field in which p does not split
  - Then K embeds into the quaternion algebra ramified at p and ∞ (in many ways)

K-**Orientation of** E**:** $\iota : K \hookrightarrow \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$

- **Example:** ordinary $E/\mathbb{F}_q$ have $\mathbb{Q}(\sqrt{-p})$-orientations (isomorphisms)

$\mathcal{O}$-**Orientation of** E ($\mathcal{O}$ an order of K): $\iota(\mathcal{O}) \subseteq \mathrm{End}(E)$

Primitive[4] $\mathcal{O}$-**Orientation on** E: $\iota(\mathcal{O}) = \mathrm{End}(E) \cap \iota(K)$

[4] aka *optimal embedding* of E

Oriented Elliptic Curves

Let

- E be an elliptic curve
- K be an imaginary quadratic field in which p does not split
  - Then K embeds into the quaternion algebra ramified at p and ∞ (in many ways)

K-**Orientation of** E**:** $\iota : K \hookrightarrow \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$

- **Example:** ordinary $E/\mathbb{F}_q$ have $\mathbb{Q}(\sqrt{-p})$-orientations (isomorphisms)

$\mathcal{O}$-**Orientation of** E ($\mathcal{O}$ an order of K): $\iota(\mathcal{O}) \subseteq \mathrm{End}(E)$

Primitive[4] $\mathcal{O}$-**Orientation on** E: $\iota(\mathcal{O}) = \mathrm{End}(E) \cap \iota(K)$

- **Example:** for ordinary curves, $\mathrm{End}(E) \cong \mathcal{O}$ iff E is primitively $\mathcal{O}$-embedded.

[4] aka *optimal embedding* of E

Let

- $\varphi : E \to E'$ be an isogeny of elliptic curves
- $\iota : K \hookrightarrow \mathrm{End}(E) \oplus_{\mathbb{Z}} \mathbb{Q}$ a K-orientation on E

Oriented Isogenies

UNIVERSITY OF CALGARY

Let

- $\varphi : E \to E'$ be an isogeny of elliptic curves
- $\iota : K \hookrightarrow \mathrm{End}(E) \oplus_{\mathbb{Z}} \mathbb{Q}$ a K-orientation on E

K-**Orientation on** E' **induced by** φ**:** $\quad \iota' = \varphi_*(\iota) \quad$ via

$$\iota'(\alpha) = \frac{1}{\deg(\varphi)} \, \varphi \, \iota(\alpha) \, \hat{\varphi} \in \mathrm{End}(E')$$

for all $\alpha \in K$.

Oriented Isogenies

Let

- $\varphi : E \to E'$ be an isogeny of elliptic curves
- $\iota : K \hookrightarrow \mathrm{End}(E) \oplus_{\mathbb{Z}} \mathbb{Q}$ a K-orientation on E

K-Orientation on E' induced by φ: $\iota' = \varphi_*(\iota)$ via

$$\iota'(\alpha) = \frac{1}{\deg(\varphi)} \, \varphi \, \iota(\alpha) \, \hat{\varphi} \in \mathrm{End}(E')$$

for all $\alpha \in K$.

$$\begin{array}{ccc} E & \xrightarrow{\varphi} & E' \\ {\scriptstyle \iota(\alpha)}\downarrow & & \downarrow{\scriptstyle \iota'(\alpha)} \\ E & \xrightarrow{\varphi} & E' \end{array}$$

Oriented Isogenies

Let

- $\varphi : E \to E'$ be an isogeny of elliptic curves
- $\iota : K \hookrightarrow \mathrm{End}(E) \oplus_{\mathbb{Z}} \mathbb{Q}$ a K-orientation on E

K-**Orientation on** E' **induced by** φ**:** $\iota' = \varphi_*(\iota)$ via

$$\iota'(\alpha) = \frac{1}{\deg(\varphi)} \varphi \, \iota(\alpha) \, \hat{\varphi} \in \mathrm{End}(E')$$

for all $\alpha \in K$.

$$\begin{array}{ccc} E & \xrightarrow{\varphi} & E' \\ \iota(\alpha)\downarrow & & \downarrow\iota'(\alpha) \\ E & \xrightarrow{\varphi} & E' \end{array}$$

Write $\varphi \cdot (E, \iota) = (\varphi(E), \varphi_*(\iota)) = (E', \iota')$.

Oriented Isogeny Graph

Fix an imaginary quadratic field K.

Oriented Isogeny Graph

Fix an imaginary quadratic field K.

K-**oriented supersingular** ℓ-**isogeny graph** (Colò-Kohel 2020):

- *Vertices*: Ordered pairs (j, ι) with $j \in \mathbb{F}_{p^2}$ and ι a K-orientation on the supersingular isomorphism class with j-invariant j
- *Edges*: oriented ℓ-isogenies $(E, \iota) \xrightarrow{\varphi} (\varphi(E), \varphi_*(\iota))$

Oriented Isogeny Graph

Fix an imaginary quadratic field K.

K-**oriented supersingular** ℓ-**isogeny graph** (Colò-Kohel 2020):

- *Vertices*: Ordered pairs (j, ι) with $j \in \mathbb{F}_{p^2}$ and ι a K-orientation on the supersingular isomorphism class with j-invariant j
- *Edges*: oriented ℓ-isogenies $(E, \iota) \xrightarrow{\varphi} (\varphi(E), \varphi_*(\iota))$

Structure: The components are ...

Oriented Isogeny Graph

Fix an imaginary quadratic field K.

K-**oriented supersingular ℓ-isogeny graph** (Colò-Kohel 2020):

- *Vertices*: Ordered pairs (j, ι) with $j \in \mathbb{F}_{p^2}$ and ι a K-orientation on the supersingular isomorphism class with j-invariant j
- *Edges*: oriented ℓ-isogenies $(E, \iota) \xrightarrow{\varphi} (\varphi(E), \varphi_*(\iota))$

Structure: The components are . . . infinite volcanoes! (No floor)

Oriented Isogeny Graph

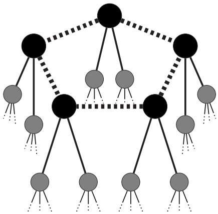
Fix an imaginary quadratic field K.

K-**oriented supersingular** ℓ-**isogeny graph** (Colò-Kohel 2020):

- *Vertices*: Ordered pairs (j, ι) with $j \in \mathbb{F}_{p^2}$ and ι a K-orientation on the supersingular isomorphism class with j-invariant j
- *Edges*: oriented ℓ-isogenies $(E, \iota) \xrightarrow{\varphi} (\varphi(E), \varphi_*(\iota))$

Structure: The components are . . . infinite volcanoes! (No floor)

- Every j-invariant appears on every volcano infinitely often, each time paired with a different orientation
- $(\ell + 1)$-regular except near $j = 0, 1728$
- Vertices at level k are primitively oriented by an order $\mathcal{O}_k$ whose conductor has ℓ-adic valuation k



An oriented 3-isogeny volcano

Orientations from Endomorphisms

For a primitive orientation $\iota : \mathcal{O} = \mathbb{Z}[\omega] \xrightarrow{\sim} \mathrm{End}(E)$, the generator image $\iota(\omega)$ defines an endomorphism of E.

Orientations from Endomorphisms

For a primitive orientation $\iota : \mathcal{O} = \mathbb{Z}[\omega] \xrightarrow{\sim} \text{End}(E)$, the generator image $\iota(\omega)$ defines an endomorphism of E.

Conversely, let

- $\theta \in \text{End}(E)$
- $\omega, \overline{\omega}$ be the roots of the minimal polynomial of θ

Orientations from Endomorphisms

UNIVERSITY OF CALGARY

For a primitive orientation $\iota : \mathcal{O} = \mathbb{Z}[\omega] \xrightarrow{\sim} \mathrm{End}(E)$, the generator image $\iota(\omega)$ defines an endomorphism of E.

Conversely, let

- $\theta \in \mathrm{End}(E)$
- $\omega, \overline{\omega}$ be the roots of the minimal polynomial of θ

Then there are two primitive $\mathbb{Z}[\omega]$-orientations of E via

$$\iota_\theta(\omega) = \theta$$

$$\widehat{\iota_\theta}(\omega) = \hat{\theta}\,, \qquad \text{equivalently,} \quad \widehat{\iota_\theta}(\overline{\omega}) = \theta$$

Orientations from Endomorphisms

For a primitive orientation $\iota : \mathcal{O} = \mathbb{Z}[\omega] \xrightarrow{\sim} \text{End}(E)$, the generator image $\iota(\omega)$ defines an endomorphism of E.

Conversely, let

- $\theta \in \text{End}(E)$
- $\omega, \overline{\omega}$ be the roots of the minimal polynomial of θ

Then there are two primitive $\mathbb{Z}[\omega]$-orientations of E via

$$\iota_\theta(\omega) = \theta$$

$$\widehat{\iota_\theta}(\omega) = \hat{\theta}\,, \qquad \text{equivalently,} \quad \widehat{\iota_\theta}(\overline{\omega}) = \theta$$

Note: $(E, \iota_\theta) \neq (E, \widehat{\iota_\theta})$.

Orientations from Endomorphisms

UNIVERSITY OF CALGARY

For a primitive orientation $\iota : \mathcal{O} = \mathbb{Z}[\omega] \xrightarrow{\sim} \mathrm{End}(E)$, the generator image $\iota(\omega)$ defines an endomorphism of E.

Conversely, let

- $\theta \in \mathrm{End}(E)$
- $\omega, \overline{\omega}$ be the roots of the minimal polynomial of θ

Then there are two primitive $\mathbb{Z}[\omega]$-orientations of E via

$$\iota_\theta(\omega) = \theta$$

$$\widehat{\iota_\theta}(\omega) = \hat{\theta}\,, \qquad \text{equivalently,} \quad \widehat{\iota_\theta}(\overline{\omega}) = \theta$$

Note: $(E, \iota_\theta) \neq (E, \widehat{\iota_\theta})$.

Fortunately, in terms of navigating oriented ℓ-volcanoes, the two vertices "look and behave the same locally" (same j-invariant, same level, same neighbours due to identifying dual edges etc.)

Orientations from Endomorphisms

For a primitive orientation $\iota : \mathcal{O} = \mathbb{Z}[\omega] \xrightarrow{\sim} \mathrm{End}(E)$, the generator image $\iota(\omega)$ defines an endomorphism of E.

Conversely, let

- $\theta \in \mathrm{End}(E)$
- $\omega, \overline{\omega}$ be the roots of the minimal polynomial of θ

Then there are two primitive $\mathbb{Z}[\omega]$-orientations of E via

$$\iota_\theta(\omega) = \theta$$

$$\widehat{\iota_\theta}(\omega) = \hat{\theta}\,, \qquad \text{equivalently,} \quad \widehat{\iota_\theta}(\overline{\omega}) = \theta$$

Note: $(E, \iota_\theta) \neq (E, \widehat{\iota_\theta})$.

Fortunately, in terms of navigating oriented ℓ-volcanoes, the two vertices "look and behave the same locally" (same j-invariant, same level, same neighbours due to identifying dual edges etc.)

We work with endomorphisms instead of orientations because they are much more concrete and computationally amenable!

Direction Finding and Navigation

Let

- $\varphi : E \to E'$ be an ℓ-isogeny
- $\theta \in \mathrm{End}(E)$ represent the orientation on E

Direction Finding and Navigation

Let

- $\varphi : E \to E'$ be an ℓ-isogeny
- $\theta \in \mathrm{End}(E)$ represent the orientation on E

Assume that θ has a certain *normal form* (achieved via translation by a suitable integer).

Direction Finding and Navigation

Let

- $\varphi : E \to E'$ be an ℓ-isogeny
- $\theta \in \mathrm{End}(E)$ represent the orientation on E

Assume that θ has a certain *normal form* (achieved via translation by a suitable integer).

The induced endomorphism on E' is θ'/ℓ where $\theta' = \varphi\theta\hat{\varphi}$.

Direction Finding and Navigation

Let

- $\varphi : E \to E'$ be an ℓ-isogeny
- $\theta \in \mathrm{End}(E)$ represent the orientation on E

Assume that θ has a certain *normal form* (achieved via translation by a suitable integer).

The induced endomorphism on E' is θ'/ℓ where $\theta' = \varphi\theta\hat{\varphi}$.

Proposition

If $\ell \nmid \theta$, then φ has the following direction:

- $\uparrow$ if $\ell^2 \mid \theta'$
- $\rightarrow$ or $\leftarrow$ (i.e. in the rim) if $\ell \mid \theta'$ and $\ell^2 \nmid \theta'$
- $\downarrow$ if $\ell \nmid \theta'$

Direction Finding and Navigation

Let

- $\varphi : E \to E'$ be an ℓ-isogeny
- $\theta \in \mathrm{End}(E)$ represent the orientation on E

Assume that θ has a certain *normal form* (achieved via translation by a suitable integer).

The induced endomorphism on E' is θ'/ℓ where $\theta' = \varphi\theta\hat{\varphi}$.

Proposition

If $\ell \nmid \theta$, then φ has the following direction:

- $\uparrow$ if $\ell^2 \mid \theta'$
- $\rightarrow$ or $\leftarrow$ (i.e. in the rim) if $\ell \mid \theta'$ and $\ell^2 \nmid \theta'$
- $\downarrow$ if $\ell \nmid \theta'$

Can also use the eigenvalues of θ acting on $E[\ell]$ for direction finding (but for traversing edges, division by ℓ incurs ℓ-adic precision losses!)

Oriented Class Group Action

Let (E, ι) be supersingular and primitively oriented by $\mathcal{O}$.

5

Let (E, ι) be supersingular and primitively oriented by $\mathcal{O}$.

For any invertible $\mathcal{O}$-ideal $\mathfrak{a}$ with $p \nmid \text{Norm}(\mathfrak{a}) = [\mathcal{O} : \mathfrak{a}]$, define

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

5

Oriented Class Group Action

Let (E, ι) be supersingular and primitively oriented by $\mathcal{O}$.

For any invertible $\mathcal{O}$-ideal $\mathfrak{a}$ with $p \nmid \mathrm{Norm}(\mathfrak{a}) = [\mathcal{O} : \mathfrak{a}]$, define

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

$\mathrm{Cl}(\mathcal{O})$ acts freely[5], with one or two orbits related via Frobenius π, on

$$\mathrm{SS}_{\mathcal{O}}^{\mathrm{pr}}(p) = \{(j(E), \iota) \mid \iota \text{ is an } \mathcal{O}\text{-primitive orientation on } E\}$$

via $[\mathfrak{a}] \star j(E) \;\mapsto\; j(E/E[\mathfrak{a}])$ (Onuki 2021, ACLSST 2022).

[5] No fixed points

Oriented Class Group Action

Let (E, ι) be supersingular and primitively oriented by $\mathcal{O}$.

For any invertible $\mathcal{O}$-ideal $\mathfrak{a}$ with $p \nmid \mathrm{Norm}(\mathfrak{a}) = [\mathcal{O} : \mathfrak{a}]$, define

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

$\mathrm{Cl}(\mathcal{O})$ acts freely[5], with one or two orbits related via Frobenius π, on

$$\mathrm{SS}_{\mathcal{O}}^{\mathrm{pr}}(p) = \{(j(E), \iota) \mid \iota \text{ is an } \mathcal{O}\text{-primitive orientation on } E\}$$

via $[\mathfrak{a}] \star j(E) \;\mapsto\; j(E/E[\mathfrak{a}])$ (Onuki 2021, ACLSST 2022).

This action can again be used to walk rims of oriented ℓ-isogeny volcanoes.

[5] No fixed points

Supersingular Path Finding (ACLSST 2022)

To find an ℓ-isogeny path starting at a curve E to a curve E' *with known endomorphism ring*[6], given **one** endomorphism $\theta \in \mathrm{End}(E)$:

[6] e.g. $j = 0$ or $j = 1728$

Supersingular Path Finding (ACLSST 2022)

To find an ℓ-isogeny path starting at a curve E to a curve E' *with known endomorphism ring*[6], given **one** endomorphism $\theta \in \mathrm{End}(E)$:

1. Pick a K such that ι_θ is a K-orientation of E ($\mathrm{disc}(\theta) = f^2\,\mathrm{disc}(K)$ with $f \in \mathbb{Z}$, ideally $\mathrm{disc}(K)$ small)

[6] e.g. $j = 0$ or $j = 1728$

Supersingular Path Finding (ACLSST 2022)

To find an ℓ-isogeny path starting at a curve E to a curve E' *with known endomorphism ring*[6], given **one** endomorphism $\theta \in \mathrm{End}(E)$:

1. Pick a K such that ι_θ is a K-orientation of E ($\mathrm{disc}(\theta) = f^2\,\mathrm{disc}(K)$ with $f \in \mathbb{Z}$, ideally $\mathrm{disc}(K)$ small)
2. Walk a K-oriented ℓ-isogeny path from E to the rim of its volcano

[6] e.g. $j = 0$ or $j = 1728$

Supersingular Path Finding (ACLSST 2022)

To find an ℓ-isogeny path starting at a curve E to a curve E' *with known endomorphism ring*[6], given **one** endomorphism $\theta \in \mathrm{End}(E)$:

1. Pick a K such that ι_θ is a K-orientation of E ($\mathrm{disc}(\theta) = f^2\,\mathrm{disc}(K)$ with $f \in \mathbb{Z}$, ideally $\mathrm{disc}(K)$ small)
2. Walk a K-oriented ℓ-isogeny path from E to the rim of its volcano
3. Orient E' by K (feasible because $\mathrm{End}(E')$ is known)

[6] e.g. $j = 0$ or $j = 1728$

Supersingular Path Finding (ACLSST 2022)

UNIVERSITY OF CALGARY

To find an ℓ-isogeny path starting at a curve E to a curve E' *with known endomorphism ring*[6], given **one** endomorphism $\theta \in \mathrm{End}(E)$:

1. Pick a K such that ι_θ is a K-orientation of E ($\mathrm{disc}(\theta) = f^2\,\mathrm{disc}(K)$ with $f \in \mathbb{Z}$, ideally $\mathrm{disc}(K)$ small)
2. Walk a K-oriented ℓ-isogeny path from E to the rim of its volcano
3. Orient E' by K (feasible because $\mathrm{End}(E')$ is known)
4. Walk a K-oriented ℓ-isogeny path from E' to the rim of its volcano

[6] e.g. $j = 0$ or $j = 1728$

Supersingular Path Finding (ACLSST 2022)

To find an ℓ-isogeny path starting at a curve E to a curve E' *with known endomorphism ring*[6], given **one** endomorphism $\theta \in \mathrm{End}(E)$:

1. Pick a K such that ι_θ is a K-orientation of E ($\mathrm{disc}(\theta) = f^2\,\mathrm{disc}(K)$ with $f \in \mathbb{Z}$, ideally $\mathrm{disc}(K)$ small)
2. Walk a K-oriented ℓ-isogeny path from E to the rim of its volcano
3. Orient E' by K (feasible because $\mathrm{End}(E')$ is known)
4. Walk a K-oriented ℓ-isogeny path from E' to the rim of its volcano
5. Hoping you hit the same oriented rim, walk it via the class group action to connect the two paths; if not, try again with a different K

[6] e.g. $j = 0$ or $j = 1728$

Supersingular Path Finding (ACLSST 2022)

UNIVERSITY OF CALGARY

To find an ℓ-isogeny path starting at a curve E to a curve E' *with known endomorphism ring*[6], given **one** endomorphism $\theta \in \mathrm{End}(E)$:

1. Pick a K such that ι_θ is a K-orientation of E ($\mathrm{disc}(\theta) = f^2\,\mathrm{disc}(K)$ with $f \in \mathbb{Z}$, ideally $\mathrm{disc}(K)$ small)
2. Walk a K-oriented ℓ-isogeny path from E to the rim of its volcano
3. Orient E' by K (feasible because $\mathrm{End}(E')$ is known)
4. Walk a K-oriented ℓ-isogeny path from E' to the rim of its volcano
5. Hoping you hit the same oriented rim, walk it via the class group action to connect the two paths; if not, try again with a different K
6. Put the segments together to form the path and forget all the orientations

[6] e.g. $j = 0$ or $j = 1728$

Example

$p = 179, \quad \mathbb{F}_{179^2} = \mathbb{F}_{179}(i)$ with $i^2 = -1, \quad \ell = 2.$

Example

$p = 179, \quad \mathbb{F}_{179^2} = \mathbb{F}_{179}(i)$ with $i^2 = -1, \quad \ell = 2.$

Find a 2-isogeny path from E to E' over $\mathbb{F}_{179^2}$ where

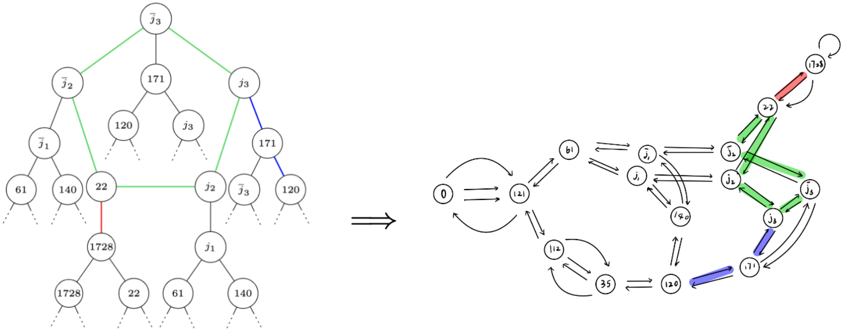
- $E = E_{120} : y^2 = x^3 + (7i + 86)x + (45i + 174)$
- $E' = E_{1728} : y^2 = x^3 - x$

Example

$p = 179, \quad \mathbb{F}_{179^2} = \mathbb{F}_{179}(i)$ with $i^2 = -1, \quad \ell = 2.$

Find a 2-isogeny path from E to E' over $\mathbb{F}_{179^2}$ where

- $E = E_{120} : y^2 = x^3 + (7i + 86)x + (45i + 174)$
- $E' = E_{1728} : y^2 = x^3 - x$



$(j_1 = 64i + 55, \quad j_2 = 99i + 107, \quad j_3 = 5i + 109)$

Step 1: Choose K

An endomorphism on E_{120} is given by $\theta_{120} \in \mathrm{End}(E)$ as follows:

$$\theta_{120}(x,y) = \left(\frac{(122i+167)x^{288} + (17i+68)x^{287} + \cdots + 174i + 157}{x^{287} + (78i+156)x^{286} + \cdots + (16i+54)}, \frac{(69i+109)x^{431} + (60i+178)x^{430} + \cdots + 98i + 124}{x^{431} + (146i+53)x^{430} + \cdots + (44i+89)}\, y \right).$$

Step 1: Choose K

An endomorphism on E_{120} is given by $\theta_{120} \in \mathrm{End}(E)$ as follows:

$$\theta_{120}(x,y) = \left(\frac{(122i+167)x^{288} + (17i+68)x^{287} + \cdots + 174i + 157}{x^{287} + (78i+156)x^{286} + \cdots + (16i+54)}, \frac{(69i+109)x^{431} + (60i+178)x^{430} + \cdots + 98i + 124}{x^{431} + (146i+53)x^{430} + \cdots + (44i+89)} y \right).$$

Replacing θ_{120} by $\theta_{120} + [-10]$ yields

$$\theta_{120}(x,y) = \left(\frac{159x^{188} + (29i+65)x^{187} + \cdots + 74i + 78}{x^{187} + (97i+131)x^{186} + \cdots + (161i+162)}, \frac{126ix^{281} + (163i+30)x^{280} + \cdots + 99i + 154}{x^{281} + (85i+105)x^{280} + \cdots + (36i+106)} y \right).$$

Step 1: Choose K

An endomorphism on E_{120} is given by $\theta_{120} \in \mathrm{End}(E)$ as follows:

$$\theta_{120}(x,y) = \left(\frac{(122i+167)x^{288} + (17i+68)x^{287} + \cdots + 174i + 157}{x^{287} + (78i+156)x^{286} + \cdots + (16i+54)}, \frac{(69i+109)x^{431} + (60i+178)x^{430} + \cdots + 98i + 124}{x^{431} + (146i+53)x^{430} + \cdots + (44i+89)} y \right).$$

Replacing θ_{120} by $\theta_{120} + [-10]$ yields

$$\theta_{120}(x,y) = \left(\frac{159x^{188} + (29i+65)x^{187} + \cdots + 74i + 78}{x^{187} + (97i+131)x^{186} + \cdots + (161i+162)}, \frac{126ix^{281} + (163i+30)x^{280} + \cdots + 99i + 154}{x^{281} + (85i+105)x^{280} + \cdots + (36i+106)} y \right).$$

This has the desired normal form and is not divisible by 2, with

$$\mathrm{disc}(\theta_{120}) = 4^2(-47) \ .$$

So we orient E by $K = \mathbb{Q}(\sqrt{-47})$.

Step 1: Choose K

An endomorphism on E_{120} is given by $\theta_{120} \in \mathrm{End}(E)$ as follows:

$$\theta_{120}(x,y) = \left(\frac{(122i+167)x^{288} + (17i+68)x^{287} + \cdots + 174i + 157}{x^{287} + (78i+156)x^{286} + \cdots + (16i+54)}, \frac{(69i+109)x^{431} + (60i+178)x^{430} + \cdots + 98i + 124}{x^{431} + (146i+53)x^{430} + \cdots + (44i+89)} y \right).$$

Replacing θ_{120} by $\theta_{120} + [-10]$ yields

$$\theta_{120}(x,y) = \left(\frac{159x^{188} + (29i+65)x^{187} + \cdots + 74i + 78}{x^{187} + (97i+131)x^{186} + \cdots + (161i+162)}, \frac{126ix^{281} + (163i+30)x^{280} + \cdots + 99i + 154}{x^{281} + (85i+105)x^{280} + \cdots + (36i+106)} y \right).$$

This has the desired normal form and is not divisible by 2, with

$$\mathrm{disc}(\theta_{120}) = 4^2(-47) .$$

So we orient E by $K = \mathbb{Q}(\sqrt{-47})$.

We find that θ_{120} is divisible by 2 (in fact by 2^2), so up we go!

Step 2: Walk from E_{120} to the Rim

We compute the blue path from 120 to the rim:

$$(E_{120}, \theta_{120}) \xrightarrow{\varphi_{120}} (E_{171}, \theta_{171}) \xrightarrow{\varphi_{171}} (E_{5i+109}, \theta_{5i+109})$$

Step 2: Walk from E_{120} to the Rim

We compute the blue path from 120 to the rim:

$$(E_{120}, \theta_{120}) \xrightarrow{\varphi_{120}} (E_{171}, \theta_{171}) \xrightarrow{\varphi_{171}} (E_{5i+109}, \theta_{5i+109})$$

where

$$\varphi_{120}(x, y) = \left(\frac{45x^2 + (-75i - 1)x + (-33i - 73)}{x + (58i - 4)}, \frac{67x^2 + (75i + 1)x + (-48i + 24)}{x^2 + (-63i - 8)x + (73i + 53)} y \right).$$

Step 2: Walk from E_{120} to the Rim

We compute the blue path from 120 to the rim:

$$(E_{120}, \theta_{120}) \xrightarrow{\varphi_{120}} (E_{171}, \theta_{171}) \xrightarrow{\varphi_{171}} (E_{5i+109}, \theta_{5i+109})$$

where

$$\varphi_{120}(x,y) = \left(\frac{45x^2 + (-75i-1)x + (-33i-73)}{x + (58i-4)}, \frac{67x^2 + (75i+1)x + (-48i+24)}{x^2 + (-63i-8)x + (73i+53)} y \right).$$

$$E_{171} : y^2 = x^3 + (120i+119)x + (66i+112)$$

Step 2: Walk from E_{120} to the Rim

We compute the blue path from 120 to the rim:

$$(E_{120}, \theta_{120}) \xrightarrow{\varphi_{120}} (E_{171}, \theta_{171}) \xrightarrow{\varphi_{171}} (E_{5i+109}, \theta_{5i+109})$$

where

$$\varphi_{120}(x, y) = \left(\frac{45x^2 + (-75i - 1)x + (-33i - 73)}{x + (58i - 4)}, \frac{67x^2 + (75i + 1)x + (-48i + 24)}{x^2 + (-63i - 8)x + (73i + 53)} y \right).$$

$E_{171} : y^2 = x^3 + (120i + 119)x + (66i + 112)$

$\theta_{171} = \frac{1}{2} \varphi_{120} \theta_{120} \widehat{\varphi_{120}}$ with $\varphi_{120} \theta_{120} \widehat{\varphi_{120}}$ divisible by 2^2.

Step 2: Walk from E_{120} to the Rim

We compute the blue path from 120 to the rim:

$$(E_{120}, \theta_{120}) \xrightarrow{\varphi_{120}} (E_{171}, \theta_{171}) \xrightarrow{\varphi_{171}} (E_{5i+109}, \theta_{5i+109})$$

where

$$\varphi_{120}(x,y) = \left(\frac{45x^2 + (-75i-1)x + (-33i-73)}{x + (58i-4)}, \frac{67x^2 + (75i+1)x + (-48i+24)}{x^2 + (-63i-8)x + (73i+53)} y \right).$$

$$E_{171} : y^2 = x^3 + (120i+119)x + (66i+112)$$

$\theta_{171} = \frac{1}{2}\,\varphi_{120}\theta_{120}\widehat{\varphi_{120}}$ with $\varphi_{120}\theta_{120}\widehat{\varphi_{120}}$ divisible by 2^2.

$$\varphi_{171}(x,y) = \left(\frac{45x^2 + (-75i+12)x + (89i+85)}{x + (58i+48)}, \frac{67x^2 + (75i-12)x + (-25i-4)}{x^2 + (-63i-83)x + (19i+14))} y \right).$$

Step 2: Walk from E_{120} to the Rim

We compute the blue path from 120 to the rim:

$$(E_{120}, \theta_{120}) \xrightarrow{\varphi_{120}} (E_{171}, \theta_{171}) \xrightarrow{\varphi_{171}} (E_{5i+109}, \theta_{5i+109})$$

where

$$\varphi_{120}(x,y) = \left(\frac{45x^2 + (-75i-1)x + (-33i-73)}{x+(58i-4)}, \frac{67x^2 + (75i+1)x + (-48i+24)}{x^2 + (-63i-8)x + (73i+53)} y \right).$$

$$E_{171} : y^2 = x^3 + (120i+119)x + (66i+112)$$

$\theta_{171} = \frac{1}{2} \varphi_{120}\theta_{120}\widehat{\varphi_{120}}$ with $\varphi_{120}\theta_{120}\widehat{\varphi_{120}}$ divisible by 2^2.

$$\varphi_{171}(x,y) = \left(\frac{45x^2 + (-75i+12)x + (89i+85)}{x+(58i+48)}, \frac{67x^2 + (75i-12)x + (-25i-4)}{x^2 + (-63i-83)x + (19i+14))} y \right).$$

$$E_{5i+109} : y^2 = x^3 + (120i+69)x + (5i+43)$$

Step 2: Walk from E_{120} to the Rim

We compute the blue path from 120 to the rim:

$$(E_{120}, \theta_{120}) \xrightarrow{\varphi_{120}} (E_{171}, \theta_{171}) \xrightarrow{\varphi_{171}} (E_{5i+109}, \theta_{5i+109})$$

where

$$\varphi_{120}(x,y) = \left(\frac{45x^2 + (-75i-1)x + (-33i-73)}{x + (58i-4)}, \frac{67x^2 + (75i+1)x + (-48i+24)}{x^2 + (-63i-8)x + (73i+53)} y \right).$$

$$E_{171} : y^2 = x^3 + (120i+119)x + (66i+112)$$

$\theta_{171} = \frac{1}{2}\varphi_{120}\theta_{120}\widehat{\varphi_{120}}$ with $\varphi_{120}\theta_{120}\widehat{\varphi_{120}}$ divisible by 2^2.

$$\varphi_{171}(x,y) = \left(\frac{45x^2 + (-75i+12)x + (89i+85)}{x + (58i+48)}, \frac{67x^2 + (75i-12)x + (-25i-4)}{x^2 + (-63i-83)x + (19i+14))} y \right).$$

$$E_{5i+109} : y^2 = x^3 + (120i+69)x + (5i+43)$$

$\theta_{5i+109} = \frac{1}{2}\varphi_{171}\theta_{171}\widehat{\varphi_{171}}$ with $\varphi_{171}\theta_{171}\widehat{\varphi_{171}}$ divisible by 2 but not by 2^2.

Step 2: Walk from E_{120} to the Rim

We compute the blue path from 120 to the rim:

$$(E_{120}, \theta_{120}) \xrightarrow{\varphi_{120}} (E_{171}, \theta_{171}) \xrightarrow{\varphi_{171}} (E_{5i+109}, \theta_{5i+109})$$

where

$$\varphi_{120}(x,y) = \left(\frac{45x^2 + (-75i-1)x + (-33i-73)}{x + (58i-4)}, \frac{67x^2 + (75i+1)x + (-48i+24)}{x^2 + (-63i-8)x + (73i+53)} y \right).$$

$$E_{171} : y^2 = x^3 + (120i+119)x + (66i+112)$$

$\theta_{171} = \frac{1}{2}\,\varphi_{120}\theta_{120}\widehat{\varphi_{120}}$ with $\varphi_{120}\theta_{120}\widehat{\varphi_{120}}$ divisible by 2^2.

$$\varphi_{171}(x,y) = \left(\frac{45x^2 + (-75i+12)x + (89i+85)}{x + (58i+48)}, \frac{67x^2 + (75i-12)x + (-25i-4)}{x^2 + (-63i-83)x + (19i+14))} y \right).$$

$$E_{5i+109} : y^2 = x^3 + (120i+69)x + (5i+43)$$

$\theta_{5i+109} = \frac{1}{2}\,\varphi_{171}\theta_{171}\widehat{\varphi_{171}}$ with $\varphi_{171}\theta_{171}\widehat{\varphi_{171}}$ divisible by 2 but not by 2^2.

So $(E_{5i+109}, \theta_{5i+109})$ is at the rim.

Step 3: Orient E_{1728} by K

$$\mathrm{End}(E_{1728}) = \mathbb{Z} + \mathbb{Z}[i] + \mathbb{Z}\,\frac{1+\pi}{2} + \mathbb{Z}\,\frac{[i](1+\pi)}{2},$$

where $[i](x,y) = (x, iy)$ and $\pi(x,y) = (x^{179}, y^{179})$

(Algebraically, $[i]^2 = [-1],\ \pi^2 = [-179]$)

Step 3: Orient E_{1728} by K

$$\mathrm{End}(E_{1728}) = \mathbb{Z} + \mathbb{Z}[i] + \mathbb{Z}\,\frac{1+\pi}{2} + \mathbb{Z}\,\frac{[i](1+\pi)}{2},$$

where $[i](x,y) = (x, iy)$ and $\pi(x,y) = (x^{179}, y^{179})$

(Algebraically, $[i]^2 = [-1],\ \pi^2 = [-179]$)

We orient E_{1728} by $K = \mathbb{Q}(\sqrt{-47})$, finding

$$\theta_{1728} = \frac{[i](1+\pi)}{2}$$

given by

$$\theta_{1728}(x,y) = \left(\frac{99x^{47} + 22x^{46} + \cdots + 77}{x^{46} + 40x^{45} + \cdots + 77}, \frac{113ix^{69} + 157ix^{68} + \cdots + 63i}{x^{69} + 60x^{68} \cdots + 158} y \right).$$

Step 3: Orient E_{1728} by K

$$\mathrm{End}(E_{1728}) = \mathbb{Z} + \mathbb{Z}[i] + \mathbb{Z}\,\frac{1+\pi}{2} + \mathbb{Z}\,\frac{[i](1+\pi)}{2},$$

where $[i](x,y) = (x, iy)$ and $\pi(x,y) = (x^{179}, y^{179})$

(Algebraically, $[i]^2 = [-1],\ \pi^2 = [-179]$)

We orient E_{1728} by $K = \mathbb{Q}(\sqrt{-47})$, finding

$$\theta_{1728} = \frac{[i](1+\pi)}{2}$$

given by

$$\theta_{1728}(x,y) = \left(\frac{99x^{47} + 22x^{46} + \cdots + 77}{x^{46} + 40x^{45} + \cdots + 77}, \frac{113ix^{69} + 157ix^{68} + \cdots + 63i}{x^{69} + 60x^{68} \cdots + 158} y \right).$$

Replacing θ_{1728} by $\theta_{1728} + [1]$ yields the normal form.

Step 3: Orient E_{1728} by K (cont'd)

An alternative approach is to find an endomorphism $\theta'_{1728} \in \mathrm{End}(E_{1728})$ as a product of $\{2,3\}$-power-smooth isogenies:

Step 3: Orient E_{1728} by K (cont'd)

An alternative approach is to find an endomorphism $\theta'_{1728} \in \mathrm{End}(E_{1728})$ as a product of $\{2,3\}$-power-smooth isogenies:

$\theta'_{1728} = \psi_{171}\psi_{1728}$, of degree $3 \cdot 2^4$,

Step 3: Orient E_{1728} by K (cont'd)

An alternative approach is to find an endomorphism $\theta'_{1728} \in \mathrm{End}(E_{1728})$ as a product of $\{2,3\}$-power-smooth isogenies:

$\theta'_{1728} = \psi_{171}\psi_{1728}$, of degree $3 \cdot 2^4$,

with $\psi_{171} : E_{171} \to E_{1728}$ of degree 3 given by

$$\psi_{171}(x,y) = \left(\frac{x^3 + (102i+30)x^2 + (31i+74)x + 10i + 158}{x^2 + (102i+30)x + (98i+130)}, \frac{x^3 + (153i+45)x^2 + (3i+88)x + 102i + 108}{x^3 + (153i+45)x^2 + (115i+32)x + (45i+174)} y \right).$$

Step 3: Orient E_{1728} by K (cont'd)

An alternative approach is to find an endomorphism $\theta'_{1728} \in \text{End}(E_{1728})$ as a product of $\{2,3\}$-power-smooth isogenies:

$\theta'_{1728} = \psi_{171}\psi_{1728}$, of degree $3 \cdot 2^4$,

with $\psi_{171} : E_{171} \to E_{1728}$ of degree 3 given by

$$\psi_{171}(x,y) = \left(\frac{x^3 + (102i+30)x^2 + (31i+74)x + 10i + 158}{x^2 + (102i+30)x + (98i+130)}, \frac{x^3 + (153i+45)x^2 + (3i+88)x + 102i + 108}{x^3 + (153i+45)x^2 + (115i+32)x + (45i+174)} y \right).$$

and $\psi_{1728} : E_{1728} \to E_{171}$ of degree 16 given by

$$\psi_{1728}(x,y) = \left(\frac{x^{16} + (156i+63)x^{15} + \cdots + 56i + 36}{x^{15} + (156i+63)x^{14} + \cdots + (10i+71)}, \frac{x^{23} + (55i+95)x^{22} + \cdots + 105i + 82}{x^{23} + (55i+95)x^{22} + \cdots + (26i+87)} y \right)$$

Step 3: Orient E_{1728} by K (cont'd)

UNIVERSITY OF CALGARY

An alternative approach is to find an endomorphism $\theta'_{1728} \in \mathrm{End}(E_{1728})$ as a product of $\{2,3\}$-power-smooth isogenies:

$\theta'_{1728} = \psi_{171}\psi_{1728}$, of degree $3 \cdot 2^4$,

with $\psi_{171} : E_{171} \to E_{1728}$ of degree 3 given by

$$\psi_{171}(x,y) = \left(\frac{x^3 + (102i+30)x^2 + (31i+74)x + 10i + 158}{x^2 + (102i+30)x + (98i+130)}, \frac{x^3 + (153i+45)x^2 + (3i+88)x + 102i + 108}{x^3 + (153i+45)x^2 + (115i+32)x + (45i+174)}y\right).$$

and $\psi_{1728} : E_{1728} \to E_{171}$ of degree 16 given by

$$\psi_{1728}(x,y) = \left(\frac{x^{16} + (156i+63)x^{15} + \cdots + 56i + 36}{x^{15} + (156i+63)x^{14} + \cdots + (10i+71)}, \frac{x^{23} + (55i+95)x^{22} + \cdots + 105i + 82}{x^{23} + (55i+95)x^{22} + \cdots + (26i+87)}y\right)$$

We find that ψ_{1728}, and hence θ'_{1728} is divisible by 2, so up we go!

Step 4: Walk from E_{1728} to the Rim

We compute the red path from 1728 to the rim:

$$(E_{1728}, \theta'_{1728}) \xrightarrow{\varphi_{1728}} (E_{22}, \theta_{22})$$

Step 4: Walk from E_{1728} to the Rim

We compute the red path from 1728 to the rim:

$$(E_{1728}, \theta'_{1728}) \xrightarrow{\varphi_{1728}} (E_{22}, \theta_{22})$$

where

$E_{22} : y^2 = x^3 + 168x + 14$

Step 4: Walk from E_{1728} to the Rim

We compute the red path from 1728 to the rim:

$$(E_{1728}, \theta'_{1728}) \xrightarrow{\varphi_{1728}} (E_{22}, \theta_{22})$$

where

$E_{22} : y^2 = x^3 + 168x + 14$

and, again in factored and already final form,

$\theta_{22} = \psi_{174i+109}\psi_{22}$ of degree 12,

Step 4: Walk from E_{1728} to the Rim

We compute the red path from 1728 to the rim:

$$(E_{1728}, \theta'_{1728}) \xrightarrow{\varphi_{1728}} (E_{22}, \theta_{22})$$

where

$E_{22} : y^2 = x^3 + 168x + 14$

and, again in factored and already final form,

$\theta_{22} = \psi_{174i+109}\psi_{22}$ of degree 12, with isogenies

$\psi_{174i+109} : E_{174i+109} \to E_{22}$ of degree 3,

Step 4: Walk from E_{1728} to the Rim

We compute the red path from 1728 to the rim:

$$(E_{1728}, \theta'_{1728}) \xrightarrow{\varphi_{1728}} (E_{22}, \theta_{22})$$

where

$E_{22} : y^2 = x^3 + 168x + 14$

and, again in factored and already final form,

$\theta_{22} = \psi_{174i+109}\psi_{22}$ of degree 12, with isogenies

$\psi_{174i+109} : E_{174i+109} \to E_{22}$ of degree 3,

$\psi_{22} = \frac{1}{4}\,\sigma_{171}\psi_{1728}\widehat{\varphi_{1728}}$ of degree 4,

Step 4: Walk from E_{1728} to the Rim

We compute the red path from 1728 to the rim:

$$(E_{1728}, \theta'_{1728}) \xrightarrow{\varphi_{1728}} (E_{22}, \theta_{22})$$

where

$E_{22} : y^2 = x^3 + 168x + 14$

and, again in factored and already final form,

$\theta_{22} = \psi_{174i+109}\psi_{22}$ of degree 12, with isogenies

$\psi_{174i+109} : E_{174i+109} \to E_{22}$ of degree 3,

$\psi_{22} = \frac{1}{4}\,\sigma_{171}\psi_{1728}\widehat{\varphi_{1728}}$ of degree 4,

where $\sigma_{171} : E_{171} \to E_{174i+109}$ has degree 2.

Step 4: Walk from E_{1728} to the Rim

We compute the red path from 1728 to the rim:

$$(E_{1728}, \theta'_{1728}) \xrightarrow{\varphi_{1728}} (E_{22}, \theta_{22})$$

where

$E_{22} : y^2 = x^3 + 168x + 14$

and, again in factored and already final form,

$\theta_{22} = \psi_{174i+109}\psi_{22}$ of degree 12, with isogenies

$\psi_{174i+109} : E_{174i+109} \to E_{22}$ of degree 3,

$\psi_{22} = \frac{1}{4}\,\sigma_{171}\psi_{1728}\widehat{\varphi_{1728}}$ of degree 4,

where $\sigma_{171} : E_{171} \to E_{174i+109}$ has degree 2.

θ_{22} is not divisible by 2, so (E_{22}, θ_{22}) is at the rim.

Step 5: Walk the Rim to Meet Up

Start walking the rim from (E_{22}, θ_{22}) via the oriented class group action.

Step 5: Walk the Rim to Meet Up

Start walking the rim from (E_{22}, θ_{22}) via the oriented class group action.

First step: compute, via Vélu's formulas, the isogeny φ_{22} with kernel $E_{22}[\mathfrak{l}]$, where $\mathfrak{l}$ is a prime ideal above ℓ in the rim order.

Step 5: Walk the Rim to Meet Up

Start walking the rim from (E_{22}, θ_{22}) via the oriented class group action.

First step: compute, via Vélu's formulas, the isogeny φ_{22} with kernel $E_{22}[\mathfrak{l}]$, where $\mathfrak{l}$ is a prime ideal above ℓ in the rim order.

1. The rim order is $\mathcal{O}_K = \mathbb{Z}[\omega]$ with $\omega = (1 + \sqrt{-47})/2$

Step 5: Walk the Rim to Meet Up

Start walking the rim from (E_{22}, θ_{22}) via the oriented class group action.

First step: compute, via Vélu's formulas, the isogeny φ_{22} with kernel $E_{22}[\mathfrak{l}]$, where $\mathfrak{l}$ is a prime ideal above ℓ in the rim order.

1. The rim order is $\mathcal{O}_K = \mathbb{Z}[\omega]$ with $\omega = (1 + \sqrt{-47})/2$
2. Find $\rho \in \mathrm{End}(E_{22})$ with $\iota_{\theta_{22}}(\omega) = \rho$

Step 5: Walk the Rim to Meet Up

Start walking the rim from (E_{22}, θ_{22}) via the oriented class group action.

First step: compute, via Vélu's formulas, the isogeny φ_{22} with kernel $E_{22}[\mathfrak{l}]$, where $\mathfrak{l}$ is a prime ideal above ℓ in the rim order.

1. The rim order is $\mathcal{O}_K = \mathbb{Z}[\omega]$ with $\omega = (1 + \sqrt{-47})/2$
2. Find $\rho \in \mathrm{End}(E_{22})$ with $\iota_{\theta_{22}}(\omega) = \rho$
3. A prime ideal above 2 is $\mathfrak{l} = 2\mathcal{O}_K + \omega\mathcal{O}_K$

Step 5: Walk the Rim to Meet Up

Start walking the rim from (E_{22}, θ_{22}) via the oriented class group action.

First step: compute, via Vélu's formulas, the isogeny φ_{22} with kernel $E_{22}[\mathfrak{l}]$, where $\mathfrak{l}$ is a prime ideal above ℓ in the rim order.

1. The rim order is $\mathcal{O}_K = \mathbb{Z}[\omega]$ with $\omega = (1 + \sqrt{-47})/2$
2. Find $\rho \in \mathrm{End}(E_{22})$ with $\iota_{\theta_{22}}(\omega) = \rho$
3. A prime ideal above 2 is $\mathfrak{l} = 2\mathcal{O}_K + \omega\mathcal{O}_K$
4. $E_{22}[\mathfrak{l}] = \ker([2]) \cap \ker(\rho)$

Step 5: Walk the Rim to Meet Up

Start walking the rim from (E_{22}, θ_{22}) via the oriented class group action.

First step: compute, via Vélu's formulas, the isogeny φ_{22} with kernel $E_{22}[\mathfrak{l}]$, where $\mathfrak{l}$ is a prime ideal above ℓ in the rim order.

1. The rim order is $\mathcal{O}_K = \mathbb{Z}[\omega]$ with $\omega = (1 + \sqrt{-47})/2$
2. Find $\rho \in \mathrm{End}(E_{22})$ with $\iota_{\theta_{22}}(\omega) = \rho$
3. A prime ideal above 2 is $\mathfrak{l} = 2\mathcal{O}_K + \omega\mathcal{O}_K$
4. $E_{22}[\mathfrak{l}] = \ker([2]) \cap \ker(\rho) = E_{22}[2] \cap \ker(\rho)$

Step 5: Walk the Rim to Meet Up

Start walking the rim from (E_{22}, θ_{22}) via the oriented class group action.

First step: compute, via Vélu's formulas, the isogeny φ_{22} with kernel $E_{22}[\mathfrak{l}]$, where $\mathfrak{l}$ is a prime ideal above ℓ in the rim order.

1. The rim order is $\mathcal{O}_K = \mathbb{Z}[\omega]$ with $\omega = (1 + \sqrt{-47})/2$
2. Find $\rho \in \mathrm{End}(E_{22})$ with $\iota_{\theta_{22}}(\omega) = \rho$
3. A prime ideal above 2 is $\mathfrak{l} = 2\mathcal{O}_K + \omega\mathcal{O}_K$
4. $E_{22}[\mathfrak{l}] = \ker([2]) \cap \ker(\rho) = E_{22}[2] \cap \ker(\rho) = \ker(\rho|_{E_{22}[2]})$

Step 5: Walk the Rim to Meet Up

Start walking the rim from (E_{22}, θ_{22}) via the oriented class group action.

First step: compute, via Vélu's formulas, the isogeny φ_{22} with kernel $E_{22}[\mathfrak{l}]$, where $\mathfrak{l}$ is a prime ideal above ℓ in the rim order.

1. The rim order is $\mathcal{O}_K = \mathbb{Z}[\omega]$ with $\omega = (1 + \sqrt{-47})/2$
2. Find $\rho \in \mathrm{End}(E_{22})$ with $\iota_{\theta_{22}}(\omega) = \rho$
3. A prime ideal above 2 is $\mathfrak{l} = 2\mathcal{O}_K + \omega\mathcal{O}_K$
4. $E_{22}[\mathfrak{l}] = \ker([2]) \cap \ker(\rho) = E_{22}[2] \cap \ker(\rho) = \ker(\rho|_{E_{22}[2]})$

$$E_{22}[2] = \{\infty, (2, 0), (156i + 178, 0), (23i + 178, 0)\}$$

Step 5: Walk the Rim to Meet Up

UNIVERSITY OF CALGARY

Start walking the rim from (E_{22}, θ_{22}) via the oriented class group action.

First step: compute, via Vélu's formulas, the isogeny φ_{22} with kernel $E_{22}[\mathfrak{l}]$, where $\mathfrak{l}$ is a prime ideal above ℓ in the rim order.

1. The rim order is $\mathcal{O}_K = \mathbb{Z}[\omega]$ with $\omega = (1 + \sqrt{-47})/2$
2. Find $\rho \in \mathrm{End}(E_{22})$ with $\iota_{\theta_{22}}(\omega) = \rho$
3. A prime ideal above 2 is $\mathfrak{l} = 2\mathcal{O}_K + \omega\mathcal{O}_K$
4. $E_{22}[\mathfrak{l}] = \ker([2]) \cap \ker(\rho) = E_{22}[2] \cap \ker(\rho) = \ker(\rho|_{E_{22}[2]})$

$$E_{22}[2] = \{\infty, (2,0), (156i + 178, 0), (23i + 178, 0)\}$$

$$E_{22}[\mathfrak{l}] = \{\infty, (156i + 178, 0)\}$$

Step 5: Walk the Rim to Meet Up

Start walking the rim from (E_{22}, θ_{22}) via the oriented class group action.

First step: compute, via Vélu's formulas, the isogeny φ_{22} with kernel $E_{22}[\mathfrak{l}]$, where $\mathfrak{l}$ is a prime ideal above ℓ in the rim order.

1. The rim order is $\mathcal{O}_K = \mathbb{Z}[\omega]$ with $\omega = (1 + \sqrt{-47})/2$
2. Find $\rho \in \mathrm{End}(E_{22})$ with $\iota_{\theta_{22}}(\omega) = \rho$
3. A prime ideal above 2 is $\mathfrak{l} = 2\mathcal{O}_K + \omega\mathcal{O}_K$
4. $E_{22}[\mathfrak{l}] = \ker([2]) \cap \ker(\rho) = E_{22}[2] \cap \ker(\rho) = \ker(\rho|_{E_{22}[2]})$

$$E_{22}[2] = \{\infty, (2, 0), (156i + 178, 0), (23i + 178, 0)\}$$

$$E_{22}[\mathfrak{l}] = \{\infty, (156i + 178, 0)\}$$

5. The isogeny on E_{22} with kernel $E_{22}[\mathfrak{l}]$ is

$$\varphi_{22} : E_{22} \to E_{99i+107} : y^2 = x^3 + (26i + 88)x + (141i + 104)$$

Step 5: Walk the Rim to Meet Up

Start walking the rim from (E_{22}, θ_{22}) via the oriented class group action.

First step: compute, via Vélu's formulas, the isogeny φ_{22} with kernel $E_{22}[\mathfrak{l}]$, where $\mathfrak{l}$ is a prime ideal above ℓ in the rim order.

1. The rim order is $\mathcal{O}_K = \mathbb{Z}[\omega]$ with $\omega = (1 + \sqrt{-47})/2$
2. Find $\rho \in \mathrm{End}(E_{22})$ with $\iota_{\theta_{22}}(\omega) = \rho$
3. A prime ideal above 2 is $\mathfrak{l} = 2\mathcal{O}_K + \omega\mathcal{O}_K$
4. $E_{22}[\mathfrak{l}] = \ker([2]) \cap \ker(\rho) = E_{22}[2] \cap \ker(\rho) = \ker(\rho|_{E_{22}[2]})$
$$E_{22}[2] = \{\infty, (2,0), (156i + 178, 0), (23i + 178, 0)\}$$
$$E_{22}[\mathfrak{l}] = \{\infty, (156i + 178, 0)\}$$
5. The isogeny on E_{22} with kernel $E_{22}[\mathfrak{l}]$ is
$$\varphi_{22} : E_{22} \to E_{99i+107} : y^2 = x^3 + (26i + 88)x + (141i + 104)$$
6. The induced endomorphism on $E_{99i+107}$ is $\theta_{99i+107} = \frac{1}{2}\,\varphi_{22}\theta_{22}\widehat{\varphi_{22}}$

Step 6: Form the Path

With this technique, we can in fact compute the *entire* rim:

$$E_{22} \xrightarrow{\varphi_{22}} E_{99i+107} \xrightarrow{\varphi_{99i+107}} E_{5i+109} \xrightarrow{\varphi_{5i+109}} E_{174i+109}$$
$$\xrightarrow{\varphi_{174i+109}} E_{80i+107} \xrightarrow{\varphi_{80i+107}} E'_{22} \cong E_{22}$$

of length 5, where each curve E_j has an attached endomorphism θ_j (not written here).

Step 6: Form the Path

UNIVERSITY OF CALGARY

With this technique, we can in fact compute the *entire* rim:

$$E_{22} \xrightarrow{\varphi_{22}} E_{99i+107} \xrightarrow{\varphi_{99i+107}} E_{5i+109} \xrightarrow{\varphi_{5i+109}} E_{174i+109}$$
$$\xrightarrow{\varphi_{174i+109}} E_{80i+107} \xrightarrow{\varphi_{80i+107}} E'_{22} \cong E_{22}$$

of length 5, where each curve E_j has an attached endomorphism θ_j (not written here).

Note: $K = \mathbb{Q}(\sqrt{-47})$ has class number 5, and the ideal class of $\mathfrak{l}$
generates $\mathrm{Cl}(K)$.

Step 6: Form the Path

With this technique, we can in fact compute the *entire* rim:

$$E_{22} \xrightarrow{\varphi_{22}} E_{99i+107} \xrightarrow{\varphi_{99i+107}} E_{5i+109} \xrightarrow{\varphi_{5i+109}} E_{174i+109} \xrightarrow{\varphi_{174i+109}} E_{80i+107} \xrightarrow{\varphi_{80i+107}} E'_{22} \cong E_{22}$$

of length 5, where each curve E_j has an attached endomorphism θ_j (not written here).

Note: $K = \mathbb{Q}(\sqrt{-47})$ has class number 5, and the ideal class of $\mathfrak{l}$ generates $\mathrm{Cl}(K)$.

Happily, $(E_{5i+109}, \theta_{5i+109})$ and (E_{22}, θ_{22}) lie on the same rim!

Step 6: Form the Path

With this technique, we can in fact compute the *entire* rim:

$$E_{22} \xrightarrow{\varphi_{22}} E_{99i+107} \xrightarrow{\varphi_{99i+107}} E_{5i+109} \xrightarrow{\varphi_{5i+109}} E_{174i+109}$$
$$\xrightarrow{\varphi_{174i+109}} E_{80i+107} \xrightarrow{\varphi_{80i+107}} E'_{22} \cong E_{22}$$

of length 5, where each curve E_j has an attached endomorphism θ_j (not written here).

Note: $K = \mathbb{Q}(\sqrt{-47})$ has class number 5, and the ideal class of $\mathfrak{l}$ generates $\mathrm{Cl}(K)$.

Happily, $(E_{5i+109}, \theta_{5i+109})$ and (E_{22}, θ_{22}) lie on the same rim!

A path from 120 to 1728 in $\mathcal{G}_2(179^2)$ is thus given by

$$E_{120} \xrightarrow{\varphi_{120}} E_{171} \xrightarrow{\varphi_{171}} E_{5i+109} \xrightarrow{\widehat{\varphi_{99i+107}}} 99i+107 \xrightarrow{\widehat{\varphi_{22}}} E_{22} \xrightarrow{\widehat{\varphi_{1728}}} E_{1728}$$

Algorithmic Ingredients

1. Standard elliptic curve stuff: point arithmetic, computing isogenies via Vélu, endomorphism translates $\theta + [n]$, torsion subgroups, isogeny kernels, dual isogenies, evaluating isogenies on ℓ-torsion points, composing isogenies

Algorithmic Ingredients

UNIVERSITY OF CALGARY

1. Standard elliptic curve stuff: point arithmetic, computing isogenies via Vélu, endomorphism translates $\theta + [n]$, torsion subgroups, isogeny kernels, dual isogenies, evaluating isogenies on ℓ-torsion points, composing isogenies
2. Dividing an endomorphism by ℓ to go up one level
   (McMurdy 2014 for $\ell = 2$, ACLSST 2022 for $\ell > 2$)

Algorithmic Ingredients

UNIVERSITY OF CALGARY

1. Standard elliptic curve stuff: point arithmetic, computing isogenies via Vélu, endomorphism translates $\theta + [n]$, torsion subgroups, isogeny kernels, dual isogenies, evaluating isogenies on ℓ-torsion points, composing isogenies
2. Dividing an endomorphism by ℓ to go up one level
   (McMurdy 2014 for $\ell = 2$, ACLSST 2022 for $\ell > 2$)
3. Carrying along orientations (i.e. computing induced orientations)

Algorithmic Ingredients

1. Standard elliptic curve stuff: point arithmetic, computing isogenies via Vélu, endomorphism translates $\theta + [n]$, torsion subgroups, isogeny kernels, dual isogenies, evaluating isogenies on ℓ-torsion points, composing isogenies
2. Dividing an endomorphism by ℓ to go up one level
   (McMurdy 2014 for $\ell = 2$, ACLSST 2022 for $\ell > 2$)
3. Carrying along orientations (i.e. computing induced orientations)
4. Class group action (for walking rims)

Algorithmic Ingredients

UNIVERSITY OF CALGARY

1. Standard elliptic curve stuff: point arithmetic, computing isogenies via Vélu, endomorphism translates $\theta + [n]$, torsion subgroups, isogeny kernels, dual isogenies, evaluating isogenies on ℓ-torsion points, composing isogenies
2. Dividing an endomorphism by ℓ to go up one level
   (McMurdy 2014 for $\ell = 2$, ACLSST 2022 for $\ell > 2$)
3. Carrying along orientations (i.e. computing induced orientations)
4. Class group action (for walking rims)
5. Computing an $\mathcal{O}$-orientation/endomorphism on a curve with known endomorphism ring (uses Cornacchia's algorithm)

Algorithmic Ingredients

1. Standard elliptic curve stuff: point arithmetic, computing isogenies via Vélu, endomorphism translates $\theta + [n]$, torsion subgroups, isogeny kernels, dual isogenies, evaluating isogenies on ℓ-torsion points, composing isogenies
2. Dividing an endomorphism by ℓ to go up one level
   (McMurdy 2014 for $\ell = 2$, ACLSST 2022 for $\ell > 2$)
3. Carrying along orientations (i.e. computing induced orientations)
4. Class group action (for walking rims)
5. Computing an $\mathcal{O}$-orientation/endomorphism on a curve with known endomorphism ring (uses Cornacchia's algorithm)
6. Computing a primitive orientation from an orientation
   (not considered in Wesolowski 2022)

Algorithmic Ingredients

1. Standard elliptic curve stuff: point arithmetic, computing isogenies via Vélu, endomorphism translates $\theta + [n]$, torsion subgroups, isogeny kernels, dual isogenies, evaluating isogenies on ℓ-torsion points, composing isogenies
2. Dividing an endomorphism by ℓ to go up one level
   (McMurdy 2014 for $\ell = 2$, ACLSST 2022 for $\ell > 2$)
3. Carrying along orientations (i.e. computing induced orientations)
4. Class group action (for walking rims)
5. Computing an $\mathcal{O}$-orientation/endomorphism on a curve with known endomorphism ring (uses Cornacchia's algorithm)
6. Computing a primitive orientation from an orientation
   (not considered in Wesolowski 2022)
7. Factoring power-smooth isogenies

Algorithmic Ingredients

1. Standard elliptic curve stuff: point arithmetic, computing isogenies via Vélu, endomorphism translates $\theta + [n]$, torsion subgroups, isogeny kernels, dual isogenies, evaluating isogenies on ℓ-torsion points, composing isogenies
2. Dividing an endomorphism by ℓ to go up one level
   (McMurdy 2014 for $\ell = 2$, ACLSST 2022 for $\ell > 2$)
3. Carrying along orientations (i.e. computing induced orientations)
4. Class group action (for walking rims)
5. Computing an $\mathcal{O}$-orientation/endomorphism on a curve with known endomorphism ring (uses Cornacchia's algorithm)
6. Computing a primitive orientation from an orientation
   (not considered in Wesolowski 2022)
7. Factoring power-smooth isogenies
8. Finding power-smooth suitable translates via sieving

Algorithmic Ingredients

UNIVERSITY OF CALGARY

1. Standard elliptic curve stuff: point arithmetic, computing isogenies via Vélu, endomorphism translates $\theta + [n]$, torsion subgroups, isogeny kernels, dual isogenies, evaluating isogenies on ℓ-torsion points, composing isogenies
2. Dividing an endomorphism by ℓ to go up one level
   (McMurdy 2014 for $\ell = 2$, ACLSST 2022 for $\ell > 2$)
3. Carrying along orientations (i.e. computing induced orientations)
4. Class group action (for walking rims)
5. Computing an $\mathcal{O}$-orientation/endomorphism on a curve with known endomorphism ring (uses Cornacchia's algorithm)
6. Computing a primitive orientation from an orientation
   (not considered in Wesolowski 2022)
7. Factoring power-smooth isogenies
8. Finding power-smooth suitable translates via sieving

SageMath code at `https://github.com/SarahArpin/WIN5`

Classical Path Finding

UNIVERSITY OF CALGARY

Theorem 1 (ACLSST 2022, La Matematica)

Let $\theta \in \text{End}(E)$ have degree $d = \deg(\theta)$ and discriminant $\Delta = \text{disc}(\theta)$.

Classical Path Finding

Theorem 1 (ACLSST 2022, La Matematica)

Let $\theta \in \mathrm{End}(E)$ have degree $d = \deg(\theta)$ and discriminant $\Delta = \mathrm{disc}(\theta)$. Suppose d is sufficiently large

Classical Path Finding

Theorem 1 (ACLSST 2022, La Matematica)

Let $\theta \in \mathrm{End}(E)$ have degree $d = \deg(\theta)$ and discriminant $\Delta = \mathrm{disc}(\theta)$. Suppose d is sufficiently large and θ can be evaluated efficiently on points on E.

Classical Path Finding

UNIVERSITY OF CALGARY

Theorem 1 (ACLSST 2022, La Matematica)

Let $\theta \in \mathrm{End}(E)$ have degree $d = \deg(\theta)$ and discriminant $\Delta = \mathrm{disc}(\theta)$. Suppose d is sufficiently large and θ can be evaluated efficiently on points on E. Let Δ' be the ℓ-fundamental factor of Δ,

Classical Path Finding

UNIVERSITY OF CALGARY

Theorem 1 (ACLSST 2022, La Matematica)

Let $\theta \in \mathrm{End}(E)$ have degree $d = \deg(\theta)$ and discriminant $\Delta = \mathrm{disc}(\theta)$. Suppose d is sufficiently large and θ can be evaluated efficiently on points on E. Let Δ' be the ℓ-fundamental factor of Δ,

- $\Delta = \ell^{2r}\Delta'$ where $v_\ell(\Delta') = 0$ or $v_\ell(\Delta') \in \{3, 2\}$ if $\ell = 2 \mid \Delta$

Classical Path Finding

Theorem 1 (ACLSST 2022, La Matematica)

Let $\theta \in \mathrm{End}(E)$ have degree $d = \deg(\theta)$ and discriminant $\Delta = \mathrm{disc}(\theta)$. Suppose d is sufficiently large and θ can be evaluated efficiently on points on E. Let Δ' be the ℓ-fundamental factor of Δ, and assume that $|\Delta'| \leq p^{2+\varepsilon}$.

- $\Delta = \ell^{2r}\Delta'$ where $v_\ell(\Delta') = 0$ or $v_\ell(\Delta') \in \{3, 2\}$ if $\ell = 2 \mid \Delta$

Classical Path Finding

UNIVERSITY OF CALGARY

Theorem 1 (ACLSST 2022, La Matematica)

Let $\theta \in \mathrm{End}(E)$ have degree $d = \deg(\theta)$ and discriminant $\Delta = \mathrm{disc}(\theta)$. Suppose d is sufficiently large and θ can be evaluated efficiently on points on E. Let Δ' be the ℓ-fundamental factor of Δ, and assume that $|\Delta'| \leq p^{2+\varepsilon}$. Then there is a heuristic classical algorithm that finds an ℓ-isogeny path of length $O(\log p + h_{\Delta'})$ from E to a curve of known endomorphism ring.

- $\Delta = \ell^{2r}\Delta'$ where $v_\ell(\Delta') = 0$ or $v_\ell(\Delta') \in \{3, 2\}$ if $\ell = 2 \mid \Delta$

Classical Path Finding

UNIVERSITY OF CALGARY

Theorem 1 (ACLSST 2022, La Matematica)

Let $\theta \in \mathrm{End}(E)$ have degree $d = \deg(\theta)$ and discriminant $\Delta = \mathrm{disc}(\theta)$. Suppose d is sufficiently large and θ can be evaluated efficiently on points on E. Let Δ' be the ℓ-fundamental factor of Δ, and assume that $|\Delta'| \leq p^{2+\varepsilon}$. Then there is a heuristic classical algorithm that finds an ℓ-isogeny path of length $O(\log p + h_{\Delta'})$ from E to a curve of known endomorphism ring.

- $\Delta = \ell^{2r}\Delta'$ where $v_\ell(\Delta') = 0$ or $v_\ell(\Delta') \in \{3, 2\}$ if $\ell = 2 \mid \Delta$
- $h_{\Delta'}$ is the class number of the quadratic order of discriminant Δ'; $h_{\Delta'} < \sqrt{|\Delta'|} \log |\Delta'|/3$

Classical Path Finding

UNIVERSITY OF CALGARY

Theorem 1 (ACLSST 2022, La Matematica)

Let $\theta \in \mathrm{End}(E)$ have degree $d = \deg(\theta)$ and discriminant $\Delta = \mathrm{disc}(\theta)$. Suppose d is sufficiently large and θ can be evaluated efficiently on points on E. Let Δ' be the ℓ-fundamental factor of Δ, and assume that $|\Delta'| \leq p^{2+\varepsilon}$. Then there is a heuristic classical algorithm that finds an ℓ-isogeny path of length $O(\log p + h_{\Delta'})$ from E to a curve of known endomorphism ring.

Run time: $h_{\Delta'} \exp\left(C\sqrt{\log d \log\log d}\right) \mathrm{poly}(\log p)$.

- $\Delta = \ell^{2r}\Delta'$ where $v_\ell(\Delta') = 0$ or $v_\ell(\Delta') \in \{3, 2\}$ if $\ell = 2 \mid \Delta$
- $h_{\Delta'}$ is the class number of the quadratic order of discriminant Δ'; $h_{\Delta'} < \sqrt{|\Delta'|}\log|\Delta'|/3$

Classical Path Finding

UNIVERSITY OF CALGARY

Theorem 1 (ACLSST 2022, La Matematica)

Let $\theta \in \mathrm{End}(E)$ have degree $d = \deg(\theta)$ and discriminant $\Delta = \mathrm{disc}(\theta)$. Suppose d is sufficiently large and θ can be evaluated efficiently on points on E. Let Δ' be the ℓ-fundamental factor of Δ, and assume that $|\Delta'| \leq p^{2+\varepsilon}$. Then there is a heuristic classical algorithm that finds an ℓ-isogeny path of length $O(\log p + h_{\Delta'})$ from E to a curve of known endomorphism ring.

Run time: $h_{\Delta'} \exp\left(C\sqrt{\log d \log\log d}\right) \mathrm{poly}(\log p)$.

- $\Delta = \ell^{2r}\Delta'$ where $v_\ell(\Delta') = 0$ or $v_\ell(\Delta') \in \{3, 2\}$ if $\ell = 2 \mid \Delta$
- $h_{\Delta'}$ is the class number of the quadratic order of discriminant Δ'; $h_{\Delta'} < \sqrt{|\Delta'|}\log|\Delta'|/3$

Runtime improves to $h_{\Delta'}\mathrm{poly}(B)\log p$ if θ is given as a B-powersmooth product.

Quantum Isogeny Finding

Theorem 2 (ACLSST 2022, La Matematica)

Let $\theta \in \mathrm{End}(E)$ have degree $d = \deg(\theta)$ and discriminant $\Delta = \mathrm{disc}(\theta)$.

Quantum Isogeny Finding

Theorem 2 (ACLSST 2022, La Matematica)

Let $\theta \in \mathrm{End}(E)$ have degree $d = \deg(\theta)$ and discriminant $\Delta = \mathrm{disc}(\theta)$.
Suppose $d \ll |\Delta| \leq p^{2+\varepsilon}$

Quantum Isogeny Finding

UNIVERSITY OF CALGARY

Theorem 2 (ACLSST 2022, La Matematica)

Let $\theta \in \mathrm{End}(E)$ have degree $d = \deg(\theta)$ and discriminant $\Delta = \mathrm{disc}(\theta)$. Suppose $d \ll |\Delta| \leq p^{2+\varepsilon}$ and θ can be evaluated efficiently on points on E.

Quantum Isogeny Finding

Theorem 2 (ACLSST 2022, La Matematica)

Let $\theta \in \mathrm{End}(E)$ have degree $d = \deg(\theta)$ and discriminant $\Delta = \mathrm{disc}(\theta)$. Suppose $d \ll |\Delta| \leq p^{2+\varepsilon}$ and θ can be evaluated efficiently on points on E. Then there is a heuristic quantum algorithm that finds a smooth isogeny of norm $O(\sqrt{|\Delta|})$ (and hence a path) from E to a curve of known endomorphism ring.

Quantum Isogeny Finding

UNIVERSITY OF CALGARY

Theorem 2 (ACLSST 2022, La Matematica)

Let $\theta \in \mathrm{End}(E)$ have degree $d = \deg(\theta)$ and discriminant $\Delta = \mathrm{disc}(\theta)$. Suppose $d \ll |\Delta| \leq p^{2+\varepsilon}$ and θ can be evaluated efficiently on points on E. Then there is a heuristic quantum algorithm that finds a smooth isogeny of norm $O(\sqrt{|\Delta|})$ (and hence a path) from E to a curve of known endomorphism ring.

Smoothness bound: $\exp(C\sqrt{\log|\Delta| \log\log|\Delta|})$.

Quantum Isogeny Finding

Theorem 2 (ACLSST 2022, La Matematica)

Let $\theta \in \mathrm{End}(E)$ have degree $d = \deg(\theta)$ and discriminant $\Delta = \mathrm{disc}(\theta)$. Suppose $d \ll |\Delta| \leq p^{2+\varepsilon}$ and θ can be evaluated efficiently on points on E. Then there is a heuristic quantum algorithm that finds a smooth isogeny of norm $O(\sqrt{|\Delta|})$ (and hence a path) from E to a curve of known endomorphism ring.

Smoothness bound: $\exp(C\sqrt{\log|\Delta| \log\log|\Delta|})$.

Run time: $\exp(C'\sqrt{\log|\Delta| \log\log|\Delta|})\,\mathrm{poly}(\log p)$.

Quantum Isogeny Finding

UNIVERSITY OF CALGARY

Theorem 2 (ACLSST 2022, La Matematica)

Let $\theta \in \mathrm{End}(E)$ have degree $d = \deg(\theta)$ and discriminant $\Delta = \mathrm{disc}(\theta)$. Suppose $d \ll |\Delta| \leq p^{2+\varepsilon}$ and θ can be evaluated efficiently on points on E. Then there is a heuristic quantum algorithm that finds a smooth isogeny of norm $O(\sqrt{|\Delta|})$ (and hence a path) from E to a curve of known endomorphism ring.

Smoothness bound: $\exp(C\sqrt{\log|\Delta| \log\log|\Delta|})$.

Run time: $\exp(C'\sqrt{\log|\Delta| \log\log|\Delta|})\,\mathrm{poly}(\log p)$.

The algorithm uses *vectorization* (Couveignes 2006) to solve the following new problem (not considered in Wesolowski 2022):

Primitive Orientation Problem

Given a supersingular elliptic curve E and an endomorphism θ on E, find the imaginary quadratic order $\mathcal{O}$ so that the orientation ι_θ is $\mathcal{O}$-primitive.

Rims and Cycles

UNIVERSITY OF CALGARY

Theorem 3 (ACLSST 2022, WIN5 Proceedings)

For any $r \geq 3$, there is a bijection between the following two sets:

- Primitive non-backtracking closed walks of length r in $\mathcal{G}_\ell(\mathbb{F}_{p^2})$;
- Directed rims of length r, identified with conjugates, in $\bigcup_K \mathcal{G}_{\ell,K}(\mathbb{F}_{p^2})$.

Theorem 3 (ACLSST 2022, WIN5 Proceedings)

For any $r \geq 3$, there is a bijection between the following two sets:

- Primitive non-backtracking closed walks of length r in $\mathcal{G}_\ell(\mathbb{F}_{p^2})$;
- Directed rims of length r, identified with conjugates, in $\bigcup_K \mathcal{G}_{\ell,K}(\mathbb{F}_{p^2})$.

Corollary 1

1. The cardinality c_r of the sets of Theorem 3 is a weighted average of class numbers of certain imaginary quadratic orders.

Rims and Cycles

UNIVERSITY OF CALGARY

Theorem 3 (ACLSST 2022, WIN5 Proceedings)

For any $r \geq 3$, there is a bijection between the following two sets:

- Primitive non-backtracking closed walks of length r in $\mathcal{G}_\ell(\mathbb{F}_{p^2})$;
- Directed rims of length r, identified with conjugates, in $\bigcup_K \mathcal{G}_{\ell,K}(\mathbb{F}_{p^2})$.

Corollary 1

1. The cardinality c_r of the sets of Theorem 3 is a weighted average of class numbers of certain imaginary quadratic orders.
2. If $p \equiv 1 \pmod{12}$, then $c_r \sim \ell^r/2r$ as $r \to \infty$ (expected count for Ramanujan graphs).

Rims and Cycles

UNIVERSITY OF CALGARY

Theorem 3 (ACLSST 2022, WIN5 Proceedings)

For any $r \geq 3$, there is a bijection between the following two sets:

- Primitive non-backtracking closed walks of length r in $\mathcal{G}_\ell(\mathbb{F}_{p^2})$;
- Directed rims of length r, identified with conjugates, in $\bigcup_K \mathcal{G}_{\ell,K}(\mathbb{F}_{p^2})$.

Corollary 1

1. The cardinality c_r of the sets of Theorem 3 is a weighted average of class numbers of certain imaginary quadratic orders.
2. If $p \equiv 1 \pmod{12}$, then $c_r \sim \ell^r/2r$ as $r \to \infty$ (expected count for Ramanujan graphs).
3. $c_r \leq \dfrac{2\pi e^\gamma \log(4\ell)}{3}\left(\log\log(2\sqrt{\ell}) + \dfrac{7}{3} + \log r\right)\ell^r + O(\ell^{3r/4}\log r)$, as $r \to \infty$, where the O-constant is explicit.

Conclusion

One endomorphism is enough for supersingular isogeny path finding:

- Classically, run time is subexponential in the degree and linear in a certain class number
- Significant improvement if the endomorphism is power-smooth
- Quantumly, the run time is subexponential in the discriminant of the endomorphism

Conclusion

One endomorphism is enough for supersingular isogeny path finding:

- Classically, run time is subexponential in the degree and linear in a certain class number
- Significant improvement if the endomorphism is power-smooth
- Quantumly, the run time is subexponential in the discriminant of the endomorphism

The algorithm finds a path to a curve E_0 with *known* endomorphism ring. For paths between arbitrary elliptic curves E, E':

1. Construct a K-oriented path P from E to E_0
2. Construct a K'-oriented path P from E' to E_0
3. Forget the orientations and construct the path $P\widehat{P'}$ from E to E', where $\widehat{P'}$ is P backwards with the dual isogenies as edges

Conclusion

One endomorphism is enough for supersingular isogeny path finding:

- Classically, run time is subexponential in the degree and linear in a certain class number
- Significant improvement if the endomorphism is power-smooth
- Quantumly, the run time is subexponential in the discriminant of the endomorphism

The algorithm finds a path to a curve E_0 with *known* endomorphism ring. For paths between arbitrary elliptic curves E, E':

1. Construct a K-oriented path P from E to E_0
2. Construct a K'-oriented path P from E' to E_0
3. Forget the orientations and construct the path $P\widehat{P'}$ from E to E', where $\widehat{P'}$ is P backwards with the dual isogenies as edges

Oriented rims of any length r are in bijection with un-oriented primitive closed walks of length r.

References

- Sarah Arpin, Mingjie Chen, Kristin E. Lauter, Renate Scheidler, Katherine E. Stange and Ha T. N. Tran

  Orienteering with one endomorphism

  arXiv:2201.11079v3 [math.NT]

  To appear in *La Mathematica*

- Sarah Arpin, Mingjie Chen, Kristin E. Lauter, Renate Scheidler, Katherine E. Stange and Ha T. N. Tran

  Orientations and cycles in supersingular isogeny graphs

  arXiv:2205.03976 [math.NT]

  To appear in *Research Directions in Number Theory — Proceedings of Women in Numbers 5*

That's All, Folks!

Thank You — Questions (or Answers)?