Orienteering on Supersingular Isogeny Volcanoes Using One Endomorphism

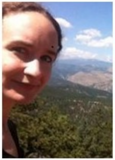
Renate Scheidler

UNIVERSITY OF CALGARY

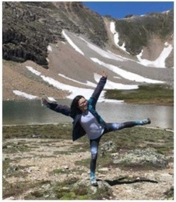
Joint work with **Sarah Arpin**, **Mingjie Chen**, **Kristin E. Lauter**, **Katherine E. Stange** and **Ha T. N Tran** (thanks to *Women in Numbers* 5)

LMFDB, Computation, and Number Theory (LuCaNT)
ICERM, Providence, Rhode Island
July 14, 2023

Let the Adventure Begin . . .





Orienteering

Finding one's way 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 always reach)

Meheti'a,
French Polynesia

Isogeny Path Finding

Throughout, let $\mathbb{F}_q$ be a finite field ($q = p^n$ with p prime).

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

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

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?

We only consider $\mathcal{L} = \{\ell\}$ (one prime).

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)

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)

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 With Help

UNIVERSITY OF CALGARY

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

Easy **if**

- The endomorphism ring is explicitly 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

Questions: Can paths be found with one (possibly large) endomorphism? If so, how?

Answers: Yes, and we have algorithms!

(Work concurrent with Wesolowski 2022)

Isogeny Graphs

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

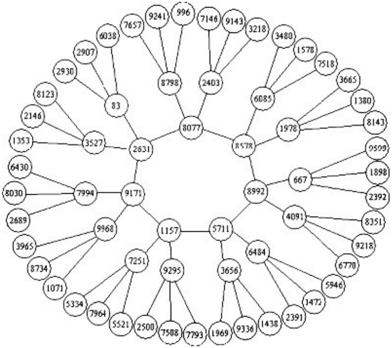
- *Vertices*: $\mathbb{F}_q$ (set of j-invariants of elliptic curves over $\mathbb{F}_q$)
- *Edges*: ℓ-isogenies, paired with their duals[1]

Properties:

- Almost $(\ell + 1)$-regular (except near 0 and 1728)
- Many ordinary components which are **volcanoes**
  - Unique cycle called the **rim** (or **crater**)
  - Vertices at level k from the rim all have CM by the same order whose conductor has ℓ-adic valuation k (Kohel 1996, Fouquet 2001, Fouquet-Morain 2002)
  - Floor has CM by Frobenius order
- One supersingular component with $\approx p/12$ vertices which is an expander graph (Ramanujan when $p \equiv 1 \pmod{12}$) (Pizer 1990)

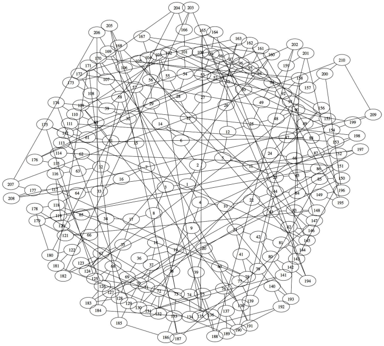
[1] Not quite right near $j = 0$ and $j = 1728$

Two Isogeny Graph Components



Ordinary component
$(\ell = 3)$

Image: Dustin Moody



Supersingular component
$(\ell = 2)$

Image: Dennis Charles

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

All elliptic curves in the same ordinary component of $\mathcal{G}_\ell(\mathbb{F}_q)$ have CM by some order in a fixed imaginary quadratic field (a commutative 2D object).

Supersingular curves have CM by a maximal order in the quaternion algebra ramified at p and ∞ (a non-commutative 4D object).

- Many quadratic fields generally embed into this quaternion algebra
- We can no longer navigate this component as for ordinary curves
- Path finding is much messier!

Orientations to the rescue!

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

Oriented Elliptic Curves

Let

- $E/\mathbb{F}_q$ be an elliptic curve ($q = p^n$)
- 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 $\mathbb{Q}\left(\sqrt{\mathrm{tr}(\pi)^2 - 4q}\right)$-orientations

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

Primitive[2] $\mathcal{O}$-**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 $\mathcal{O}$-oriented.

[2] aka *optimal embedding* of E

Oriented Isogenies

Let

- $\varphi : E \to E'$ be an isogeny of elliptic curves
- $\iota : K \hookrightarrow \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ 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 $\alpha \in K$ (Waterhouse 1969).

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

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

Oriented Isogeny Graph

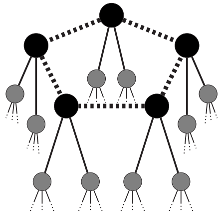
Fix an imaginary quadratic field K.

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 and Endomorphisms

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

Conversely, let

- $\theta \in \mathrm{End}(E) \cap \iota(K)$
- $\omega, \overline{\omega}$ 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

Let

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

Assume that θ satisfies a certain normal form called *ℓ-suitable* (needed for dividing by $[\ell]$, achieved via translation by a suitable integer).

The induced endomorphism on E' is $\theta'/[\ell]$ 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 $[\ell] \nmid \theta'$

Note: 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!)

Recap: Ordinary 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[3] and transitive[4] 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

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

Note: $\#\,\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q) = \#\,\mathrm{Cl}(\mathcal{O})$, the class number of $\mathcal{O}$.

---

[3] Only the principal ideal class acts trivially

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

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).

Note: $\# \mathrm{SS}_{\mathcal{O}}^{\mathrm{pr}}(p) = \# \mathrm{Cl}(\mathcal{O})$ or $2\# Cl(\mathcal{O})$.

[5]No fixed points

Volcano Navigation

Navigation in both ordinary and oriented supersingular volcanos:

$\uparrow$ and $\downarrow$: Vélu's formulas

Rim ($\rightarrow$ or $\leftarrow$): (oriented) class group action by $\mathfrak{l} \mid \ell$

$\mathfrak{l} = \langle \ell, \omega \rangle$ ($\mathcal{O}_K$-module of rank 2)

$$E[\mathfrak{l}] = \ker([\ell]) \cap \ker(\iota(\omega)) = \ker(\iota(\omega)|_{E[\ell]})$$

More efficient than Vélu.

In the oriented setting, we also need to carry along the orientation via the Waterhouse transfer.

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 $\theta \in \mathrm{End}(E)$:

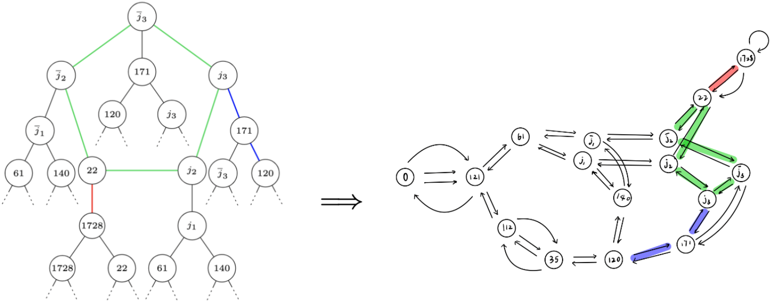
1. Pick K such that ι_θ is a K-orientation of E ($\mathrm{disc}(\theta) = f^2\,\mathrm{disc}(K)$ with $f \in \mathbb{Z}$, ideally $\mathrm{disc}(K)$ small)
2. Walk a K-oriented ℓ-isogeny path from E to the rim of its volcano
3. Generate that entire rim via class group action
4. Orient E' by K (feasible because $\mathrm{End}(E')$ is known)
5. Walk a K-oriented ℓ-isogeny path from E' to the rim of its volcano
6. If that path hits the rim of E's volcano, connect the two paths with the appropriate rim segment; else, go back to step 1 and try a different K
7. Forget all the orientations and output the unoriented path.

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

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

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

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



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

(Order of algorithms steps in the example changed to 1, 2, 4, 5, 3, 6)

Step 1: Choose K

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

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

Translating $\tilde{\theta}_{120}$ by $[-10]$ 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 is 2-suitable, with

$$\mathrm{disc}(\theta_{120}) = 2^2 \Delta_0 \text{ with } \Delta_0 = -4 \cdot 47 = -188 \text{ fundamental.}$$

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 using Vélu's algorithm:

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

where

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

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

$\theta_{171} = \frac{1}{2}\,\varphi_{120}\theta_{120}\widehat{\varphi_{120}} + [1]$ divisible by exactly [2].

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

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

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

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

Step 4: Orient E_{1728} by K

$$\mathrm{End}(E_{1728}) = \mathbb{Z} + \mathbb{Z}\mathbf{i} + \mathbb{Z}\,\frac{\mathbf{i}+\mathbf{ij}}{2} + \mathbb{Z}\,\frac{(1+\mathbf{j})}{2},$$

where $\mathbf{i}(x,y) = (x, iy)$ and $\mathbf{j}(x,y) = (x^{179}, y^{179})$

(Algebraically, $\mathbf{i}^2 = [-1]$, $\mathbf{j}^2 = [-179]$)

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

$$\tilde{\theta}_{1728} = \mathbf{i} + \frac{\mathbf{i}+\mathbf{ij}}{2}$$

given by

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

$\theta_{1728} := \tilde{\theta}_{1728} + [1]$ is 2-suitable.

Step 4: Orient E_{1728} by K (cont'd)

An alternative approach to walking up is to give our endomorphisms in power-smooth factored form; in this case, as a product of $\{2, 3\}$-power degree isogenies, and refactor in each step:

$\theta_{1728} = \psi_{171}\psi_{1728}$, 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} is divisible by [2], and hence so is θ_{1728}. So up we go!

Step 5: 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 already $\{2,3\}$-power-smooth factored and 2-suitable 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,

$\psi_{22} = [4]^{-1}\sigma_{171}\psi_{1728}\widehat{\varphi_{1728}}$ 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 3: Generate the Rim

The rim order is the maximal order $\mathcal{O}_K$.

Using the $\mathrm{Cl}(\mathcal{O}_K)$-action of $\mathfrak{l} = \langle 2, (1+\sqrt{-47})/2 \rangle$ generates the 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 E_{120} to E_{1728} in $\mathcal{G}_2(179^2)$ is thus given by

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

Algorithmic Ingredients

1. Standard elliptic curve stuff: point arithmetic, Vélu, endomorphism translates $\theta + [n]$, torsion subgroups, isogeny kernels, dual isogenies, evaluating isogenies on ℓ-torsion points, composing isogenies
2. Dividing an ℓ-suitable endomorphism by $[\ell]$ (to go up)
   (McMurdy 2014 for $\ell = 2$, ACLSST 2022 for $\ell > 2$)
3. Waterhouse transfer (i.e. computing induced orientations)
4. Oriented class group action (for traversing 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 $\theta \in \mathrm{End}(E)$ 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 Smooth 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 $O(\sqrt{|\Delta|})$ from E to a curve of known endomorphism ring.

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

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

Uses *oriented vectorization* to solve the following new problem:

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.

Classically, exponential in the size of the largest prime power factor of Δ.

Rims and Cycles

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.

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]

  La Mathematica (2023), 60pp,

  `https://doi.org/10.1007/s44007-023-00053-2`

- 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*

Thank You — Questions (or Answers)?