

# Orienteering with one endomorphism

Sarah Arpin  
Universiteit Leiden

Joint with Mingjie Chen, Kristin E. Lauter, Renate Scheidler, Katherine E. Stange, &  
Ha T. N. Tran

**Arithmetic, Algebra, and Algorithms ICMS**

13 April 2023



# The supersingular endomorphism ring problem is hard

## Definition

Let  $E$  be an elliptic curve defined over a field  $K$  of characteristic  $p \neq \infty$ .  $E$  is **supersingular** iff one of the following equivalent conditions hold:

- $[p] : E \rightarrow E$  is purely inseparable and  $j(E) \in \mathbb{F}_{p^2}$ ,
- $\text{End}(E)$  is a maximal order in a quaternion algebra.
- $E[p^k] = \{\mathcal{O}_E\}$  for any  $k \geq 1$ .

Fixing  $K = \overline{\mathbb{F}}_p$ , there are finitely many isomorphism classes of supersingular elliptic curves over  $K$ .

For  $E$  supersingular,  $\text{End}(E)$  is difficult to compute.

...but we know certain endomorphism rings

$$p \equiv 3 \pmod{4}$$

$$E_{1728} : y^2 = x^3 + x/\overline{\mathbb{F}_p}$$

$$j = 1728$$

$$[\pm 1](x, y) = (x, \pm y)$$

$$\pi_p(x, y) = (x^p, y^p)$$

$$[i](x, y) = (-x, \sqrt{-1}y)$$

$$\text{End}(E_{1728}) =$$

$$\mathbb{Z}\langle 1, [i], \frac{1+\pi_p}{2}, \frac{[i]+[i]\circ\pi_p}{2} \rangle$$

$$p \equiv 2 \pmod{3}$$

$$E_0 : y^2 = x^3 + 1/\overline{\mathbb{F}_p}$$

$$j = 0$$

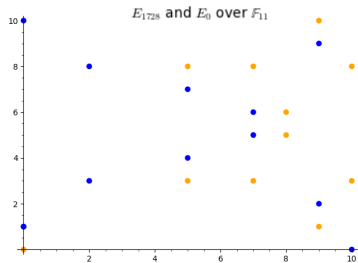
$$[\pm 1](x, y) = (x, \pm y)$$

$$\pi_p(x, y) = (x^p, y^p)$$

$$\frac{(1-[i])}{2}(x, y) = (\sqrt[6]{1}^2 x, y)$$

$$\text{End}(E_0) =$$

$$\mathbb{Z}\langle 1, \frac{1-[i]}{2}, \frac{\pi_p+[i]\circ\pi_p}{2}, \frac{[i]+[i]\circ\pi_p}{3} \rangle$$



## Maps to $j = 0, 1728$ give endomorphisms

$$p = 179, E_{22} : y^2 = x^3 + 5x + 101$$

A few obvious endomorphisms:

$$[\pm 1] : (x, y) \mapsto (x, \pm y)$$

$$\pi_p : (x, y) \mapsto (x^p, y^p)$$

How to find others? Use an  $\ell$ -isogeny graph!

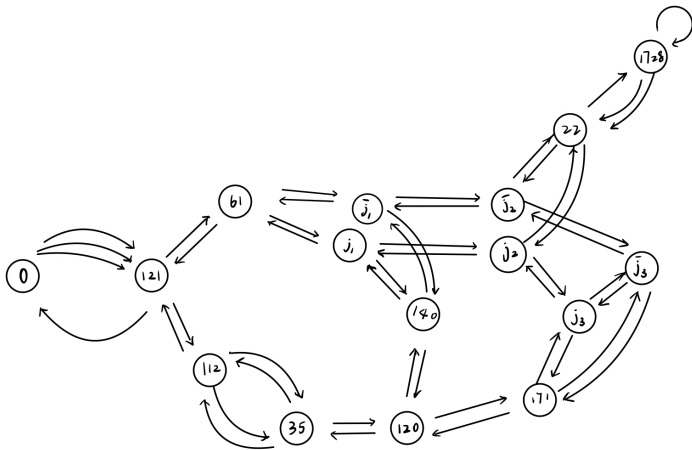
We have a degree-2 isogeny  $\phi : E_{22} \rightarrow E_{1728}$ , so we can take endomorphisms from  $E_{1728}$ :

$$\phi \circ \text{End}(E) \circ \hat{\phi} \subseteq \text{End}(E_{22})$$

This information reveals the endomorphism ring:

$$\text{End}(E_{22}) \cong \mathbb{Z} \left\langle 1, 2i, \frac{1}{2} + \frac{3}{4}i + \frac{1}{4}ij, \frac{1}{2} + i - \frac{1}{2}j \right\rangle$$

# Supersingular elliptic curve $\ell$ -isogeny graph



$p = 179, \ell = 2$

Finding maps to  $E_{1728}$ ,  $E_0$  is hard. But what if we had a *little* bit of endomorphism ring information to start with?

# Orientations add structure and allow us to path-find

## Definition ((Primitive) Orientation\*)

A  **$K$ -orientation** on  $E$  is an embedding

$$\iota : K \hookrightarrow \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q} \cong B_{p,\infty}.$$

A  $K$ -orientation is an  **$\mathcal{O}$ -orientation** if  $\iota(\mathcal{O}) \subseteq \mathrm{End}(E)$ , and it is a **primitive  $\mathcal{O}$ -orientation** if  $\iota(\mathcal{O}) = \mathrm{End}(E) \cap \iota(K)$ .

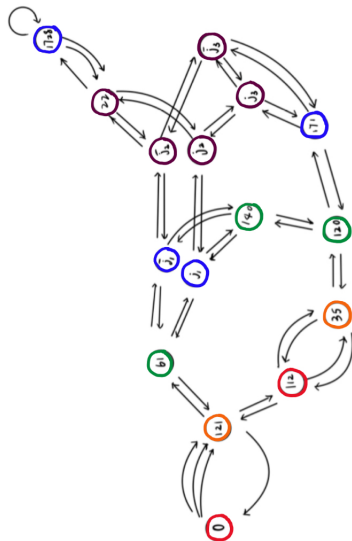
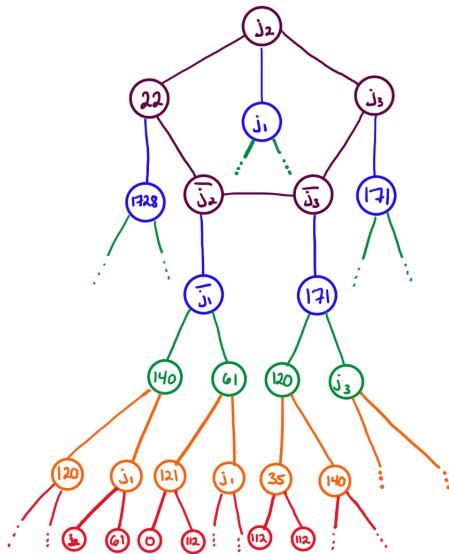
An isogeny  $\varphi : E \rightarrow E'$  induces an isogeny  $\varphi : (E, \iota) \rightarrow (E', \varphi_*\iota)$ :

$$\begin{aligned} (\varphi_*\iota) : K &\rightarrow \mathrm{End}(E') \otimes_{\mathbb{Z}} \mathbb{Q} \\ (\varphi_*\iota)(\alpha) &:= \frac{1}{[\deg \varphi]} \varphi \circ \iota(\alpha) \circ \hat{\varphi}. \end{aligned}$$

If  $(E, \iota)$  is a primitively  $\mathcal{O}$ -oriented supersingular elliptic curve, then  $(E', \varphi_*\iota)$  is primitively  $\mathcal{O}'$ -oriented and one of the following is true:  
 $\mathcal{O}' =$  or  $\subsetneq$  or  $\supsetneq \mathcal{O}$  ( $\varphi$  is **horizontal**/descending/**ascending**).

\*This terminology was popularized for isogenists by Colo-Kohel '20, Onuki '20. In quaternion literature, primitive embeddings are called optimal embeddings.

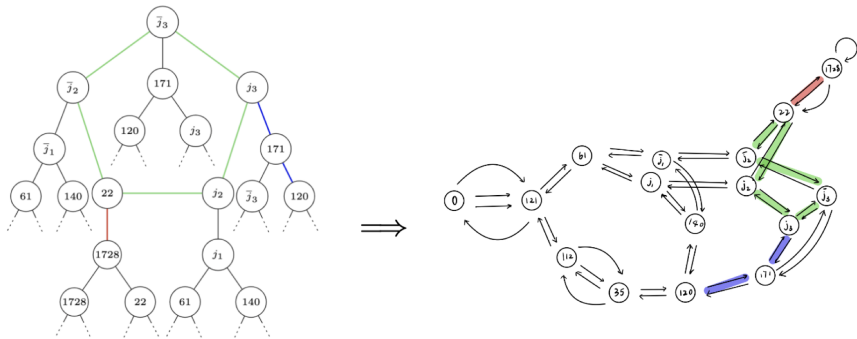
Each oriented isogeny volcano covers the  $\ell$ -isogeny graph:



# Finding paths to $E_{1728}, E_0$

Using the oriented isogeny volcano structure within the  $\ell$ -isogeny graphs, we can find paths to  $E_0, E_{1728}$ .

$$p = 179, \ell = 2, \mathcal{O} = \mathbb{Z}[\sqrt{-47}]$$



Combining blue, green, and red paths in the oriented volcano, we find a path from  $E_{120}$  to  $E_{1728}$  in the supersingular 2-isogeny graph.

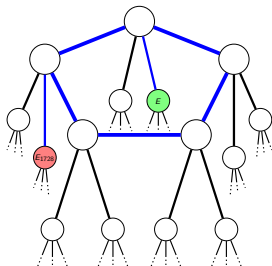
Given  $(E, \iota)$  by specifying an endomorphism, find the order  $\mathcal{O}$  such that  $\iota$  is  $\mathcal{O}$ -primitive

Given  $(E, \iota)$  a primitive  $\mathcal{O}$ -orientation, walk to the rim of the oriented  $\ell$ -isogeny volcano.

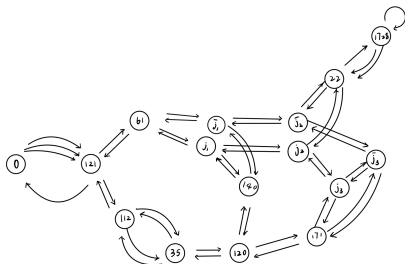
Given an imaginary quadratic field, find a  $K$ -orientation  $(E_{1728}, \iota_{1728})$  and walk to the rim.

Walk the rim of an oriented  $\ell$ -isogeny volcano.

We provide classical and quantum algorithms. Runtime is usually subexponential, but polynomial time in some cases.



# Cycles in $\ell$ -isogeny graph come from class groups



isogeny cycle	length	endomorphism	$\mathcal{O}$	$h(\mathcal{O})$
$(j_3, \bar{j}_3, 171)$	3	$\frac{\pm 1 \pm \sqrt{-31}}{2}$	$\mathbb{Z} \left[ \frac{1 + \sqrt{-31}}{2} \right]$	3
$(61, j_1, 140, \bar{j}_1)$	4	$\frac{\pm 5 \pm \sqrt{-39}}{2}$	$\mathbb{Z} \left[ \frac{1 + \sqrt{-39}}{2} \right]$	4
$(22, \bar{j}_2, \bar{j}_3, j_3, j_2)$	5	$\frac{\pm 9 \pm \sqrt{-47}}{2}$	$\mathbb{Z} \left[ \frac{1 + \sqrt{-47}}{2} \right]$	5

**Table:** Cycles of lengths 3, 4, and 5 in  $\mathcal{G}_2$  with  $p = 179$ , with the associated endomorphisms to which the cycles compose.

# Cohen-Lenstra heuristics provide framework for understanding class groups

## “Heuristics on class groups of number fields”

by H. Cohen & H. W. Lenstra, Jr.,  
Number theory, Noordwijkerhout 1983, 33–62, Lecture Notes in Math.,  
1068, Springer, Berlin, 1984.

*The odd part of the class group of an imaginary quadratic field seems to be quite rarely non cyclic.*

If we have a primitively  $\mathcal{O}$ -oriented isogeny volcano,  $[1] \in \text{Cl}(\mathcal{O})$  allows us to walk the rim of the volcano. Most likely  $[1]$  generates  $\text{Cl}(\mathcal{O})$ , so we know what size rim to expect.

# Thank you.

