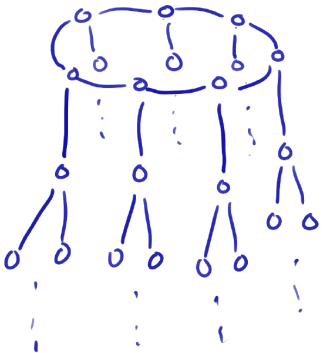
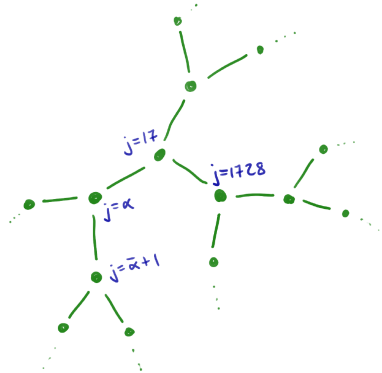
Supersingular graphs and orientations

Katherine E. Stange



AMMCS, August 16th, 2023

ℓ-isogeny graphs



- vertices: elliptic curves /$\overline{\mathbb{F}}_p$ up to isomorphism (given as j-invariants)
- edges: isogenies of degree ℓ up to equivalence (given as kernels)

identifying φ with dual $\widehat{\varphi}$: an undirected $\ell+1$ regular graph

(away from $j = 0, 1728$)

endomorphism rings

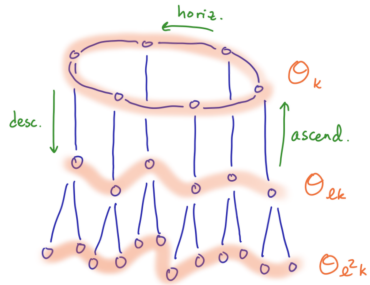
An elliptic curve $/\overline{\mathbb{F}}_p$ is either:

- ordinary: $\mathrm{End}(E) \cong \mathcal{O}$, order in an imaginary quadratic field
- supersingular: $\mathrm{End}(E) \cong \mathfrak{O}$ order in a quaternion algebra $B_{p,\infty}$ ramified at p and ∞

ordinary graph structure

End(E) an order in an imaginary quadratic field K

Each component is a volcano:



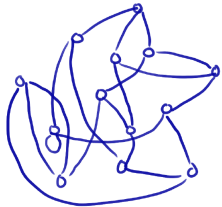
- Fixed K so that all End(E) $\subseteq K$.
- Rim: curves with End(E) $\cong \mathcal{O}_k$ an order of K
- level n: curves with End(E) $\cong \mathcal{O}_{\ell^n k}$ of index ℓ^n in $\mathcal{O}_k$.

volcano: edges are *ascending*, *descending* or *horizontal*

supersingular graph structure

End(E) an order in $B_{p,\infty}$

One random-looking component:



- around $p/12$ curves, all defined over $\mathbb{F}_{p^2}$
- $\ell + 1$-regular

we typically assume $j = 1728$ is in the graph (or another curve with known End(E))

supersingular isogeny graphs are Ramanujan

$\frac{1}{\ell+1}A$ = normalized adjacency matrix, operator for flow of mass between vertices

supersingular isogeny graphs are Ramanujan

$\frac{1}{\ell+1}A$ = normalized adjacency matrix, operator for flow of mass between vertices

eigenvalues: $1 = \lambda_0 \geq \lambda_1 \geq \cdots \geq -1$.

uniform distribution is eigenvector with eigenvalue $\lambda_0 = 1$

supersingular isogeny graphs are Ramanujan

$\frac{1}{\ell+1}A$ = normalized adjacency matrix, operator for flow of mass between vertices

eigenvalues: $1 = \lambda_0 \geq \lambda_1 \geq \cdots \geq -1$.

uniform distribution is eigenvector with eigenvalue $\lambda_0 = 1$

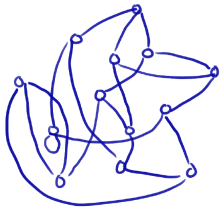
spectral gap: $\max_{i>1} |\lambda_i| \leq \frac{2\sqrt{\ell}}{\ell+1} < 1$

called a *Ramanujan graph*.

$\Rightarrow$ *well-mixing*: a random path of length $O(\log(p))$ will reach all vertices uniformly

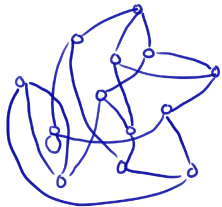
Hard problems and cryptographic use

Hard problems for supersingular ℓ-isogeny graphs



p is cryptographic size (size of graph), ℓ is fixed and small (degree)

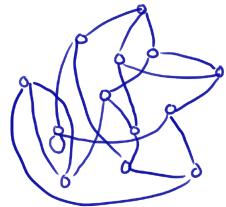
Hard problems for supersingular ℓ-isogeny graphs



p is cryptographic size (size of graph), ℓ is fixed and small (degree)

- Given j_1, j_2, find a path in graph between them

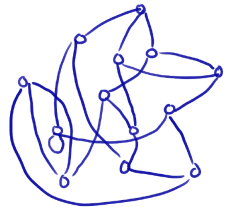
Hard problems for supersingular ℓ-isogeny graphs



p is cryptographic size (size of graph), ℓ is fixed and small (degree)

- Given j_1, j_2, find a path in graph between them
- Given j, find a path in graph to 1728

Hard problems for supersingular ℓ-isogeny graphs

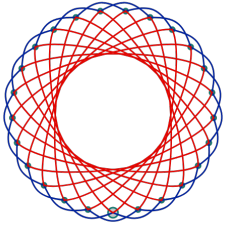


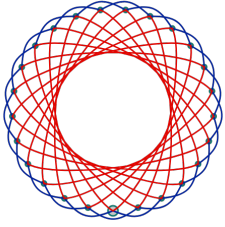
p is cryptographic size (size of graph), ℓ is fixed and small (degree)

- Given j_1, j_2, find a path in graph between them
- Given j, find a path in graph to 1728
- Given j, find $\mathrm{End}(E_j)$, either by generating endomorphisms, or abstract isomorphism type

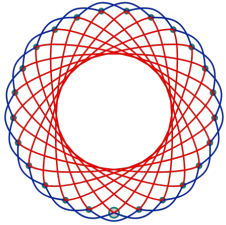
supersingular isogeny-based cryptography: CSIDH

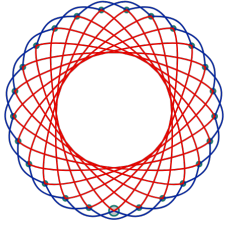
Alice





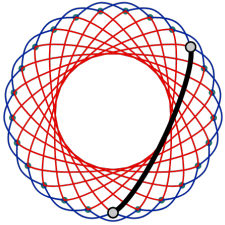
Bob

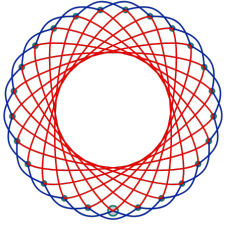




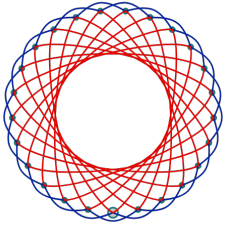
isogeny-based cryptography: CSIDH

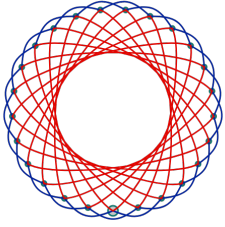
Alice





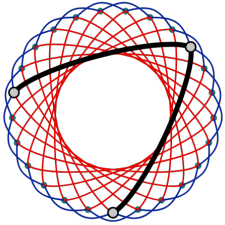
Bob

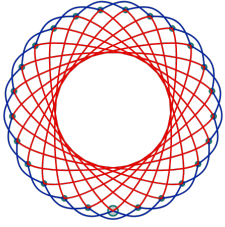




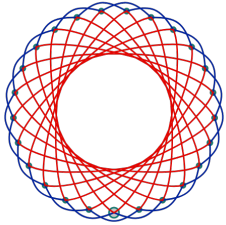
isogeny-based cryptography: CSIDH

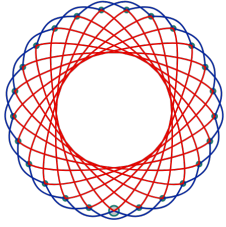
Alice





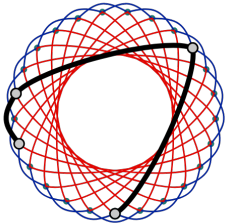
Bob

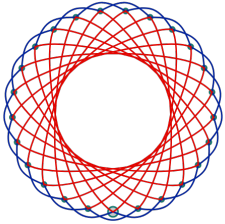




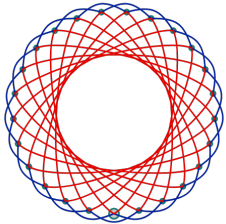
isogeny-based cryptography: CSIDH

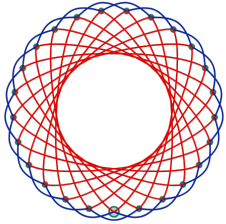
Alice





Bob

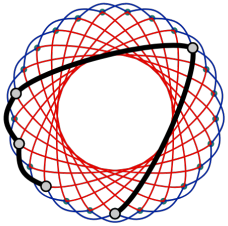


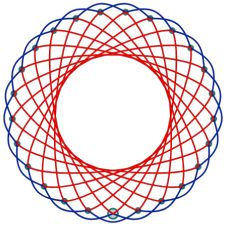


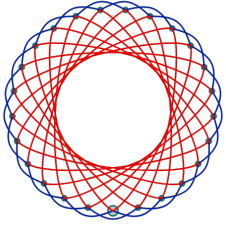
isogeny-based cryptography: CSIDH

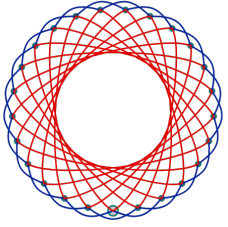
Alice

Bob



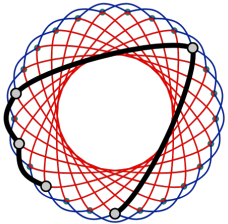


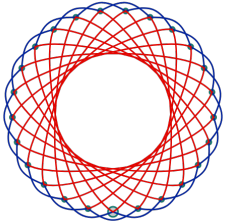




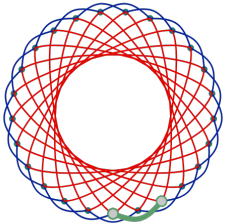
isogeny-based cryptography: CSIDH

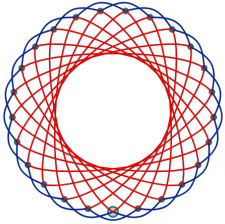
Alice





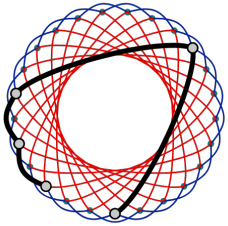
Bob

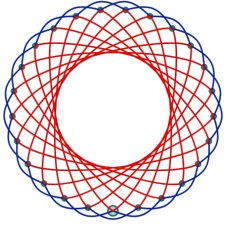




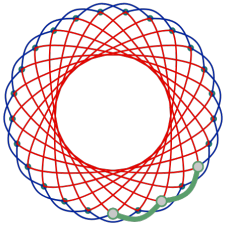
isogeny-based cryptography: CSIDH

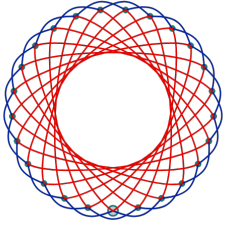
Alice





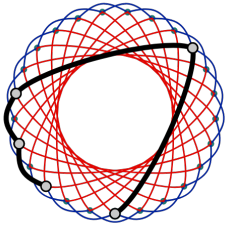
Bob

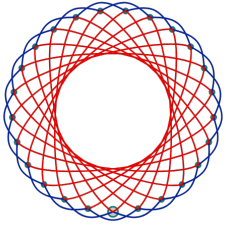




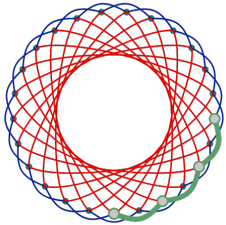
isogeny-based cryptography: CSIDH

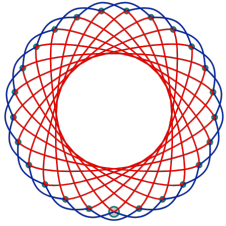
Alice





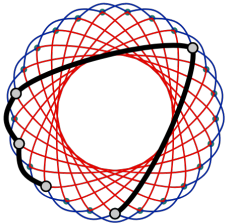
Bob

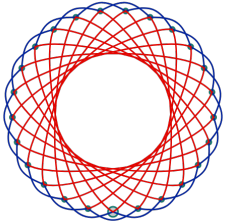




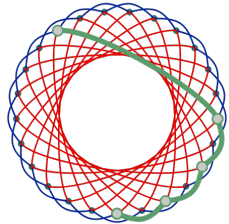
isogeny-based cryptography: CSIDH

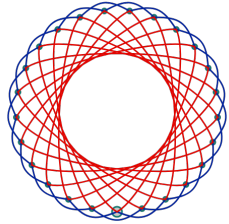
Alice



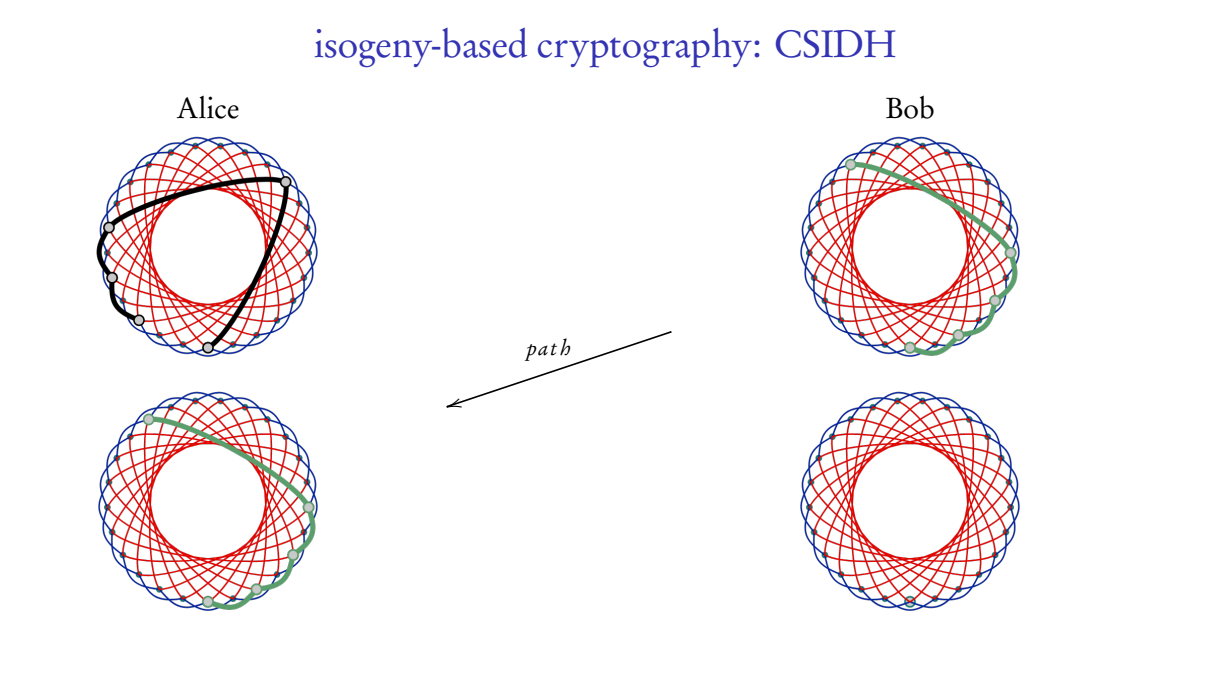


Bob





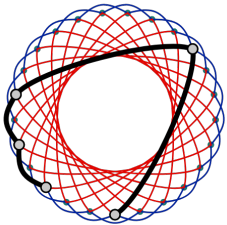
isogeny-based cryptography: CSIDH

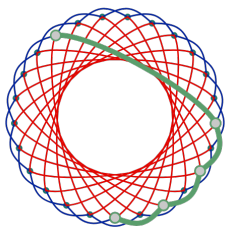


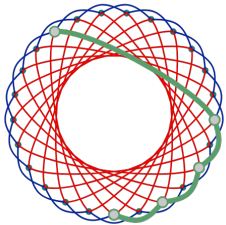
isogeny-based cryptography: CSIDH

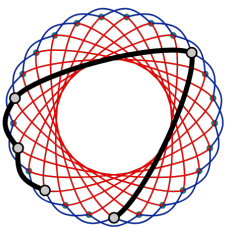
Alice

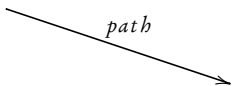
Bob





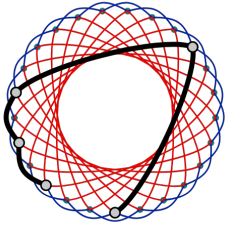




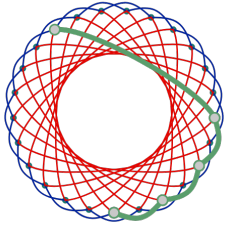


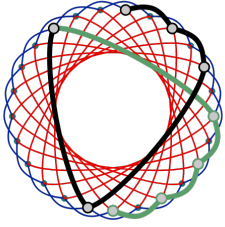
isogeny-based cryptography: CSIDH

Alice

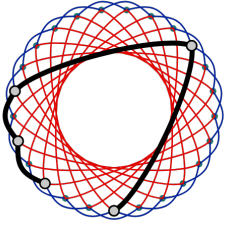


Bob



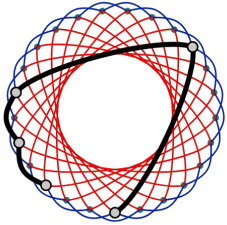


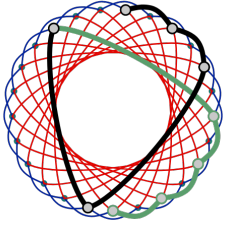
compose paths



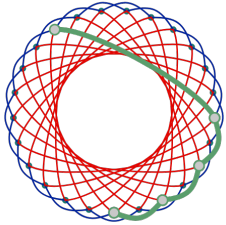
isogeny-based cryptography: CSIDH

Alice

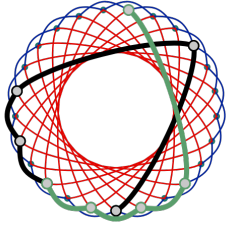




Bob



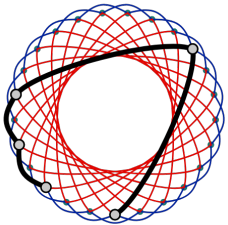
compose paths

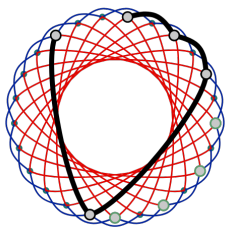


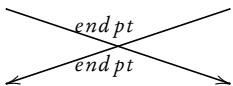
isogeny-based cryptography: CSIDH

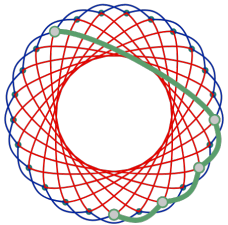
Alice

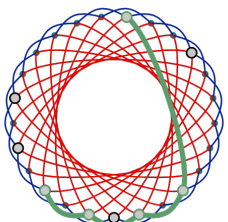
Bob



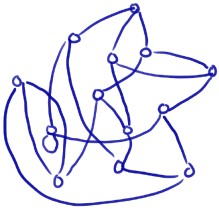




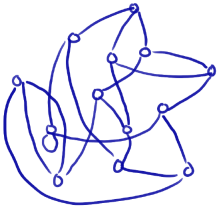




j-invariants vs. endomorphism rings

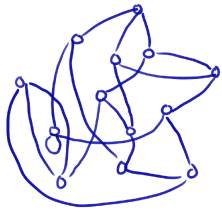


labelled with j-invariants
????



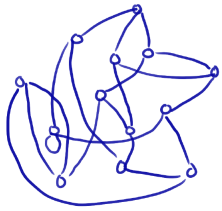
labelled with endomorphism rings
can compare & navigate

j-invariants vs. endomorphism rings



labelled with j-invariants

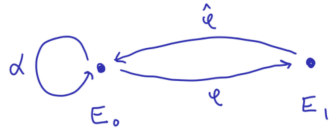
????



labelled with endomorphism rings

can compare & navigate

- Hard problem: computing the endomorphism ring
- With endomorphism rings, Kohel-Lauter-Petit-Tignol algorithm finds path (uses ideals of orders)



Orientations

Orientations

An elliptic curve $/\overline{\mathbb{F}}_p$ is either:

- ordinary: $\mathrm{End}(E) \cong \mathcal{O}$, an order in an imaginary quadratic field
- supersingular: $\mathrm{End}(E) \cong \mathfrak{O}$ an order in a quaternion algebra $B_{p,\infty}$ ramified at p and ∞

Orientations

An elliptic curve $/\overline{\mathbb{F}}_p$ is either:

- ordinary: $\mathrm{End}(E) \cong \mathcal{O}$, an order in an imaginary quadratic field
- supersingular: $\mathrm{End}(E) \cong \mathfrak{O}$ an order in a quaternion algebra $B_{p,\infty}$ ramified at p and ∞

Supersingular case: Every element of $B_{p,\infty} \setminus \mathbb{Q}$ is quadratic of negative discriminant
$\Rightarrow$ many imaginary quadratic fields $\iota : K \hookrightarrow B_{p,\infty}$ (many ways!)
$\Rightarrow \mathfrak{O} \cap \iota(K)$ is an order in an imaginary quadratic field

A pair (E, ι) where $\iota : K \to \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(E) \cong B_{p,\infty}$ is a *K-oriented elliptic curve*.

Orientations

An elliptic curve $/\overline{\mathbb{F}}_p$ is either:

- ordinary: $\mathrm{End}(E) \cong \mathcal{O}$, an order in an imaginary quadratic field
- supersingular: $\mathrm{End}(E) \cong \mathfrak{O}$ an order in a quaternion algebra $B_{p,\infty}$ ramified at p and ∞

Supersingular case: Every element of $B_{p,\infty} \setminus \mathbb{Q}$ is quadratic of negative discriminant
$\Rightarrow$ many imaginary quadratic fields $\iota : K \hookrightarrow B_{p,\infty}$ (many ways!)
$\Rightarrow \mathfrak{O} \cap \iota(K)$ is an order in an imaginary quadratic field

A pair (E, ι) where $\iota : K \to \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(E) \cong B_{p,\infty}$ is a *K-oriented elliptic curve*.

One explicit endomorphism is equivalent to an orientation

Path finding in the supersingular isogeny graph

Knowledge of endomorphism ring enables path finding

Path finding in the supersingular isogeny graph

Knowledge of endomorphism ring enables path finding

What about knowledge of a single endomorphism?

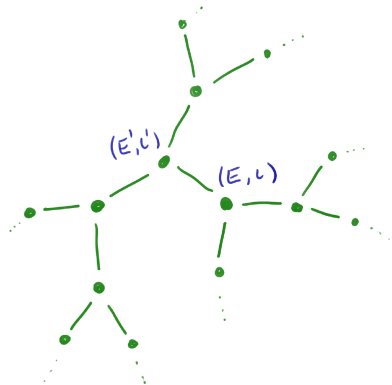
Path finding in the supersingular isogeny graph

Knowledge of endomorphism ring enables path finding

What about knowledge of a single endomorphism?

Our tool: orientations

K-oriented supersingular ℓ-isogeny graphs



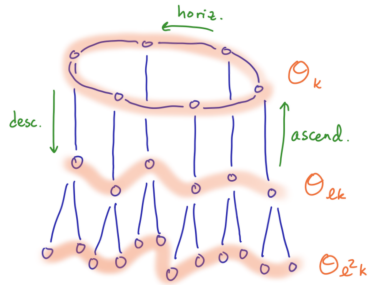
- vertices: K-oriented elliptic curves (E, ι) over $\overline{\mathbb{F}}_p$ up to isomorphism
- edges: isogenies of degree ℓ up to equivalence, respecting the orientations

identifying φ with dual $\widehat{\varphi}$: an undirected $\ell + 1$ regular graph

ordinary graph structure

End(E) an order in an imaginary quadratic field K

Each component is a volcano:



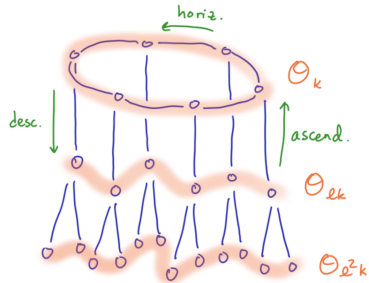
- Fixed K so that all End(E) $\subseteq K$.
- Rim: curves with End(E) $\cong \mathcal{O}_k$ an order of K
- level n: curves with End(E) $\cong \mathcal{O}_{\ell^n k}$ of index ℓ^n in $\mathcal{O}_k$.

volcano: edges are *ascending*, *descending* or *horizontal*

K-oriented graph structure

$\mathrm{End}(E) \cap \iota(K)$ an order in an imaginary quadratic field K

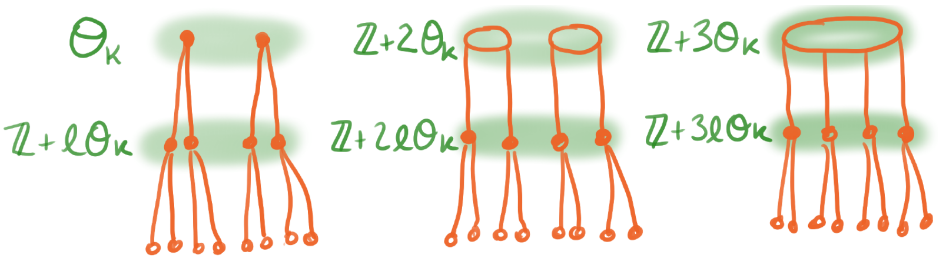
Each component is a volcano:



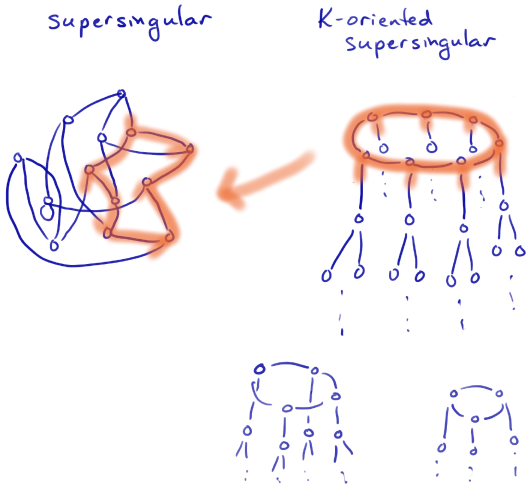
- Fixed K so that all $\mathrm{End}(E) \subseteq K$.
- Rim: curves with $\mathrm{End}(E) \cap \iota(K) \cong \mathcal{O}_k$ an order of K
- level n: curves with $\mathrm{End}(E) \cap \iota(K) \cong \mathcal{O}_{\ell^n k}$ of index ℓ^n in $\mathcal{O}_k$.

volcano: edges are *ascending*, *descending* or *horizontal*

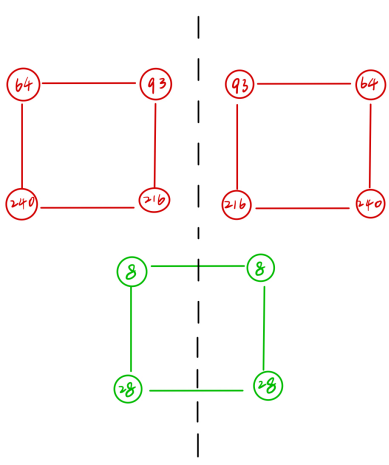
Big picture

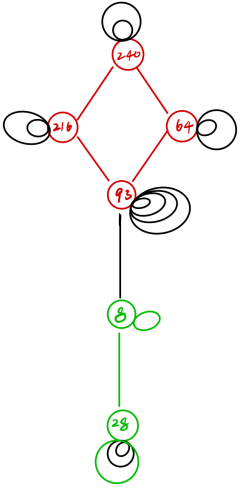

Θ_K
$\mathbb{Z}+\ell\Theta_K$
$\mathbb{Z}+2\Theta_K$
$\mathbb{Z}+2\ell\Theta_K$
$\mathbb{Z}+3\Theta_K$
$\mathbb{Z}+3\ell\Theta_K$

Forgetting orientation

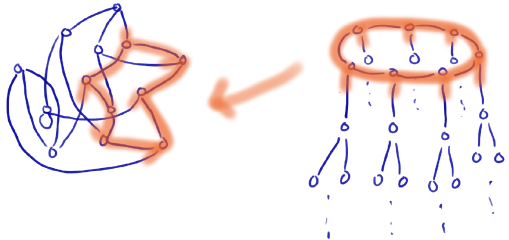


Forgetting orientation





Forgetting orientation



A **rim** goes to an **isogeny cycle**:

- a closed walk of the same length (may repeat vertices/edges)
- no backtracking
- not a repeat of a smaller closed walk 

Rims and isogeny cycles

Theorem (Arpin, Chen, Lauter, Scheidler, S., Tran)

Let $\ell < p$ be primes. Let $r > 2$ be an integer.
Let $\mathcal{G}_\ell$ be the supersingular ℓ-isogeny graph over $\overline{\mathbb{F}}_p$.
Then there is a bijection:

$$\left\{\begin{array}{c}\text{isogeny cycles of length} \\ r \text{ in } \mathcal{G}_\ell\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{rims of size } r \text{ in the union} \\ \text{of all oriented} \\ \text{ss } \ell\text{-isogeny volcanoes} \\ \text{up to conjugation}\end{array}\right\}$$

$$\xleftarrow{\text{forget orientation}}$$

$$\xrightarrow[\text{to get endomorphism hence orientation}]{\text{compose around cycle}}$$

Rims and isogeny cycles

Theorem (Arpin, Chen, Lauter, Scheidler, S., Tran)

Let $\ell < p$ be primes. Let $r > 2$ be an integer.
Let $\mathcal{G}_\ell$ be the supersingular ℓ-isogeny graph over $\overline{\mathbb{F}}_p$.
Then there is a bijection:

$$\left\{\begin{array}{c}\text{isogeny cycles of length} \\ r \text{ in } \mathcal{G}_\ell\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{rims of size } r \text{ in the union} \\ \text{of all oriented} \\ \text{ss } \ell\text{-isogeny volcanoes} \\ \text{up to conjugation}\end{array}\right\}$$

- not canonical (because of extra automorphisms)
- self-conjugate rims occur when p is ramified

The class group action

Class group action for imaginary quadratic order $\mathcal{O}$

- A set:

$$SS_{\mathcal{O}}^{pr}(p) := \{(E,\iota) : \iota \text{ is primitive } \}$$

where *primitive* means $\iota(K) \cap \mathrm{End}(E) = \iota(\mathcal{O})$.

Class group action for imaginary quadratic order $\mathcal{O}$

- A set:

$$SS_{\mathcal{O}}^{pr}(p) := \{(E, \iota) : \iota \text{ is primitive } \}$$

  where *primitive* means $\iota(K) \cap \mathrm{End}(E) = \iota(\mathcal{O})$.
- A group: the class group $\mathrm{Cl}(\mathcal{O})$.

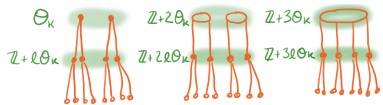
Class group action for imaginary quadratic order $\mathcal{O}$

- A set:
$$SS_{\mathcal{O}}^{pr}(p) := \{(E,\iota) : \iota \text{ is primitive } \}$$
where *primitive* means $\iota(K) \cap \mathrm{End}(E) = \iota(\mathcal{O})$.
- A group: the class group $\mathrm{Cl}(\mathcal{O})$.
- An action:
$$[\mathfrak{a}] \cdot E = E/E[\mathfrak{a}], \quad E[\mathfrak{a}] = \cap_{\alpha \in \mathfrak{a}} \ker(\alpha).$$

Class group action for imaginary quadratic order $\mathcal{O}$

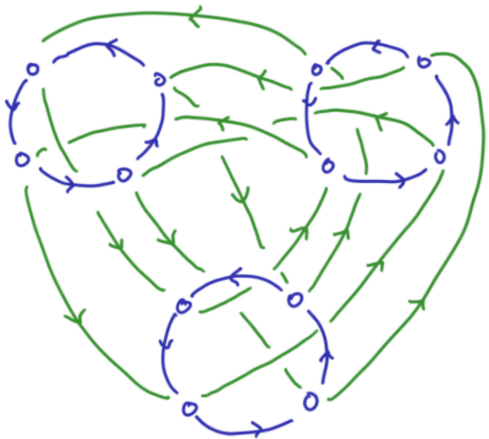
- A set:
$$SS_{\mathcal{O}}^{pr}(p) := \{(E,\iota) : \iota \text{ is primitive } \}$$
where *primitive* means $\iota(K) \cap \mathrm{End}(E) = \iota(\mathcal{O})$.
- A group: the class group $\mathrm{Cl}(\mathcal{O})$.
- An action:
$$[\mathfrak{a}] \cdot E = E/E[\mathfrak{a}], \quad E[\mathfrak{a}] = \cap_{\alpha \in \mathfrak{a}} \ker(\alpha).$$

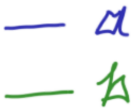
Action is free, with 1 or 2 orbits, and *horizontal*.



Descends from the action on curves over $\mathbb{C}$.

Class group action





If $\mathfrak{a}$ has norm ℓ, then the blue cycles *are* the oriented ℓ-isogeny volcano rims.

Counting isogeny cycles

We expect (Ramanujan graphs) as $r \to \infty$:

$$\#\text{ of isogeny cycles of length } r \sim \frac{\ell^r}{2r}$$

Counting isogeny cycles

We expect (Ramanujan graphs) as $r \to \infty$:

$$\#\text{ of isogeny cycles of length } r \sim \frac{\ell^r}{2r}$$

Theorem (Arpin, Chen, Lauter, Scheidler, S., Tran)

$$\#\textit{ of isogeny cycles of length } r = \frac{1}{r} \sum_{\mathcal{O} \in \mathscr{I}_r} \epsilon_{\mathcal{O}} h_{\mathcal{O}},$$

where $\epsilon_{\mathcal{O}} \in \{1, 2\}$ *and* $h_{\mathcal{O}}$ *is the class number, and*

$$\mathscr{I}_r = \left\{ \textit{imaginary quadratic orders } \mathcal{O} : \begin{array}{c} p \textit{ does not split in the field containing } \mathcal{O} \\ p \textit{ does not divide the conductor of } \mathcal{O} \\ \mathcal{O} \textit{ is an } \ell\textit{-fundamental order,} \\ (\ell) = \mathfrak{l}\bar{\mathfrak{l}} \textit{ splits in } \mathcal{O}, \\ \textit{and } [\mathfrak{l}] \textit{ has order } r \textit{ in } \mathrm{Cl}(\mathcal{O}). \end{array} \right\}.$$

Algorithm to count isogeny cycles

To find all possible α of norm ℓ^r in orders of $\mathscr{I}_r$:

Algorithm to count isogeny cycles

To find all possible α of norm ℓ^r in orders of $\mathscr{I}_r$:

- Splitting of ℓ bounds discriminant

Algorithm to count isogeny cycles

To find all possible α of norm ℓ^r in orders of $\mathscr{I}_r$:

- Splitting of ℓ bounds discriminant
- Find all representations $N(\alpha) = \ell^r$

Algorithm to count isogeny cycles

To find all possible α of norm ℓ^r in orders of $\mathscr{I}_r$:

- Splitting of ℓ bounds discriminant
- Find all representations $N(\alpha) = \ell^r$
- Check splitting of ℓ, p in $\mathbb{Q}(\alpha)$

Algorithm to count isogeny cycles

To find all possible α of norm ℓ^r in orders of $\mathscr{I}_r$:

- Splitting of ℓ bounds discriminant
- Find all representations $N(\alpha) = \ell^r$
- Check splitting of ℓ, p in $\mathbb{Q}(\alpha)$
- Find all orders $\mathbb{Z}[\alpha] \subseteq \mathcal{O} \subseteq \mathbb{Q}(\alpha)$

Algorithm to count isogeny cycles

To find all possible α of norm ℓ^r in orders of $\mathscr{I}_r$:

- Splitting of ℓ bounds discriminant
- Find all representations $N(\alpha) = \ell^r$
- Check splitting of ℓ, p in $\mathbb{Q}(\alpha)$
- Find all orders $\mathbb{Z}[\alpha] \subseteq \mathcal{O} \subseteq \mathbb{Q}(\alpha)$
- Check if $\mathfrak{l} \mid (\ell)$ has order r in $\mathrm{Cl}(\mathcal{O})$

Algorithm to count isogeny cycles

To find all possible α of norm ℓ^r in orders of $\mathscr{I}_r$:

- Splitting of ℓ bounds discriminant
- Find all representations $N(\alpha) = \ell^r$
- Check splitting of ℓ, p in $\mathbb{Q}(\alpha)$
- Find all orders $\mathbb{Z}[\alpha] \subseteq \mathcal{O} \subseteq \mathbb{Q}(\alpha)$
- Check if $\mathfrak{l} \mid (\ell)$ has order r in $\mathrm{Cl}(\mathcal{O})$

Then:

Algorithm to count isogeny cycles

To find all possible α of norm ℓ^r in orders of $\mathscr{I}_r$:

- Splitting of ℓ bounds discriminant
- Find all representations $N(\alpha) = \ell^r$
- Check splitting of ℓ, p in $\mathbb{Q}(\alpha)$
- Find all orders $\mathbb{Z}[\alpha] \subseteq \mathcal{O} \subseteq \mathbb{Q}(\alpha)$
- Check if $\mathfrak{l} \mid (\ell)$ has order r in $\mathrm{Cl}(\mathcal{O})$

Then:

- For each α, its orbit under the action of $\mathfrak{l}$ is a oriented volcano rim

Algorithm to count isogeny cycles

To find all possible α of norm ℓ^r in orders of $\mathscr{I}_r$:

- Splitting of ℓ bounds discriminant
- Find all representations $N(\alpha) = \ell^r$
- Check splitting of ℓ, p in $\mathbb{Q}(\alpha)$
- Find all orders $\mathbb{Z}[\alpha] \subseteq \mathcal{O} \subseteq \mathbb{Q}(\alpha)$
- Check if $\mathfrak{l} \mid (\ell)$ has order r in $\mathrm{Cl}(\mathcal{O})$

Then:

- For each α, its orbit under the action of $\mathfrak{l}$ is a oriented volcano rim
- This gives an isogeny cycle.

Algorithm to count isogeny cycles

To find all possible α of norm ℓ^r in orders of $\mathscr{I}_r$:

- Splitting of ℓ bounds discriminant
- Find all representations $N(\alpha) = \ell^r$
- Check splitting of ℓ, p in $\mathbb{Q}(\alpha)$
- Find all orders $\mathbb{Z}[\alpha] \subseteq \mathcal{O} \subseteq \mathbb{Q}(\alpha)$
- Check if $\mathfrak{l} \mid (\ell)$ has order r in $\mathrm{Cl}(\mathcal{O})$

Then:

- For each α, its orbit under the action of $\mathfrak{l}$ is a oriented volcano rim
- This gives an isogeny cycle.
- Watch for conjugation.

Counting isogeny cycles: upper bound

Corollary (Arpin, Chen, Lauter, Scheidler, S., Tran)

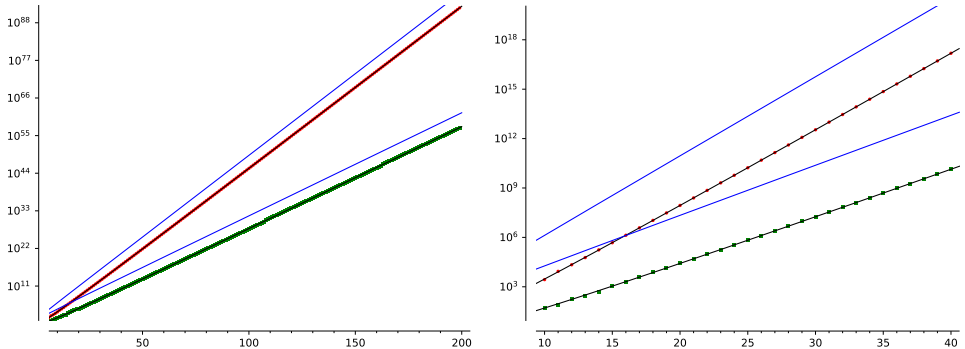
$$\#\text{ of isogeny cycles of length } r < \frac{2\pi e^{\gamma}\log(4\ell)}{3}\,\ell^{r}(\log r+\log\log(2\sqrt{\ell})+7/3)+O(\ell^{3r/4}\log r)$$

as $r \to \infty$, *where* $\gamma = 0.577\ldots$ *is the Euler-Mascheroni constant.*

Tools: Möbius inversion and known class group estimates.

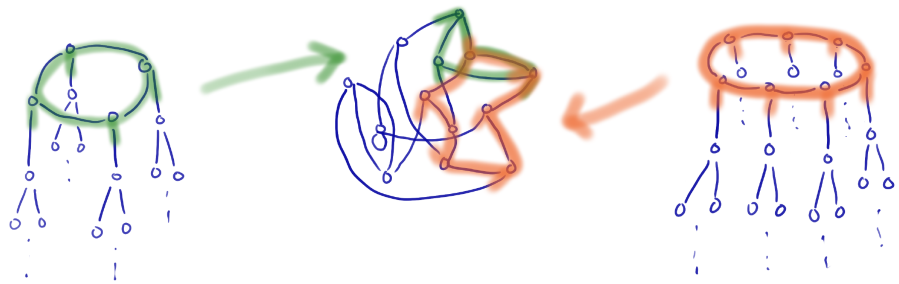
Counting isogeny cycles: upper bound

Semilog plot, $p = 3361, \ell = 2$ (green), $p = 3229, \ell = 3$ (red) compared to dominant term



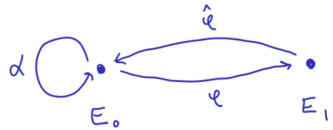
$$\#\text{ of isogeny cycles of length } r < \frac{2\pi e^{\gamma}\log(4\ell)}{3}\,\ell^{r}(\log r + \log\log(2\sqrt{\ell}) + 7/3) + O(\ell^{3r/4}\log r)$$

Relationship between class groups



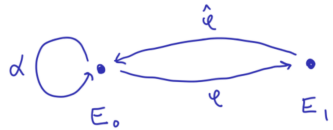
Navigating the graph with one endomorphism

The view from one vertex



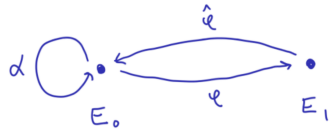
- Have an orientation ι
- Taking a step along isogeny φ, have a derived orientation $\varphi \circ \iota \circ \varphi^{-1}$

The view from one vertex



- Have an orientation ι
- Taking a step along isogeny φ, have a derived orientation $\varphi \circ \iota \circ \varphi^{-1}$
- Can detect if it is horizontal, ascending or descending
  - either by checking if you can divide by ℓ;
  - or using a method of eigenvalues

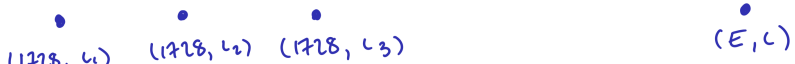
The view from one vertex



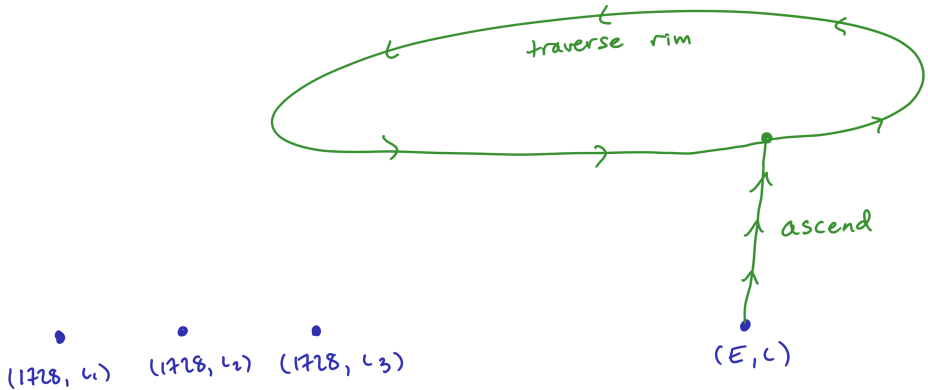
- Have an orientation ι
- Taking a step along isogeny φ, have a derived orientation $\varphi \circ \iota \circ \varphi^{-1}$
- Can detect if it is horizontal, ascending or descending
  - either by checking if you can divide by ℓ;
  - or using a method of eigenvalues

Upshot: can tell which way is up on the oriented volcano

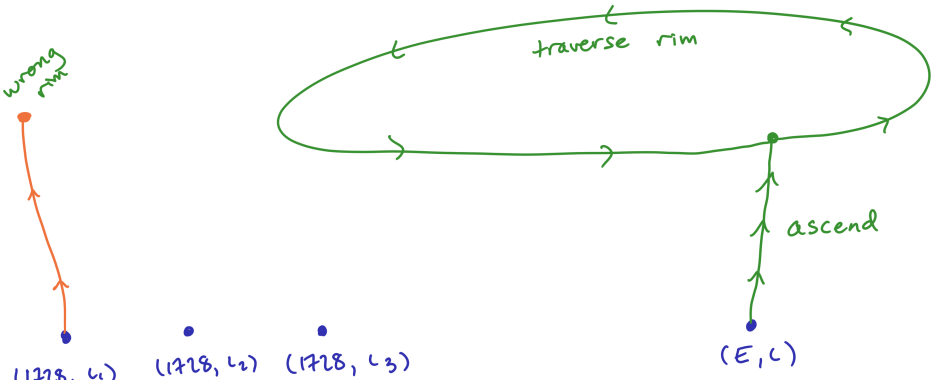
Path-finding idea



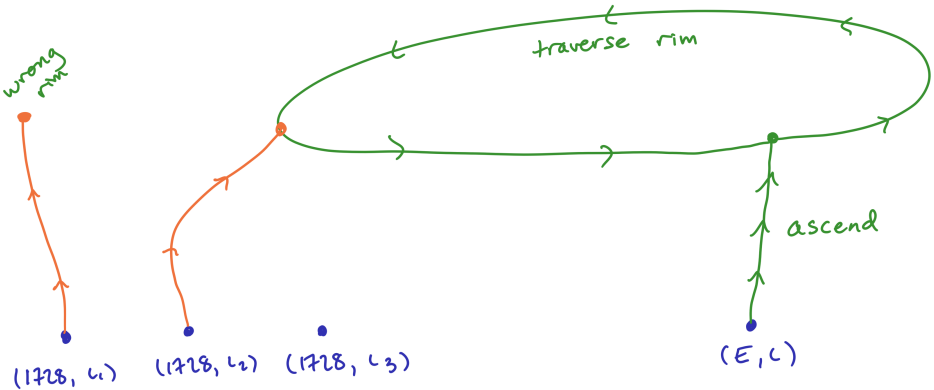
Path-finding idea



Path-finding idea



Path-finding idea



Path-finding idea

See Mingjie Chen's talk at 16:40 in *Computational Number Theory*.