The Topography of Isogeny Graphs

Jonathan Love

Mathematical Institute, Leiden University
https://jonathanlove.info/

Includes joint work with Dan Boneh and with Eyal Goren

April 8, 2025

Preview

Take primes p, ℓ with

- p large (main example in this talk: $p = 100003$),
- ℓ small (main example in this talk: $\ell = 2$).

Preview

Take primes p, ℓ with

- p large (main example in this talk: $p = 100003$),
- ℓ small (main example in this talk: $\ell = 2$).

The supersingular isogeny graph $\mathcal{G}(p, \ell)$ has

- Vertices: isomorphism classes of supersingular elliptic curves over $\mathbb{F}_{p^2}$ ($\approx \frac{p}{12}$ vertices).
- Edges: degree ℓ isogenies, up to post-composition with an isomorphism ($\ell + 1$ edges from each vertex).

Preview

Take primes p, ℓ with

- p large (main example in this talk: $p = 100003$),
- ℓ small (main example in this talk: $\ell = 2$).

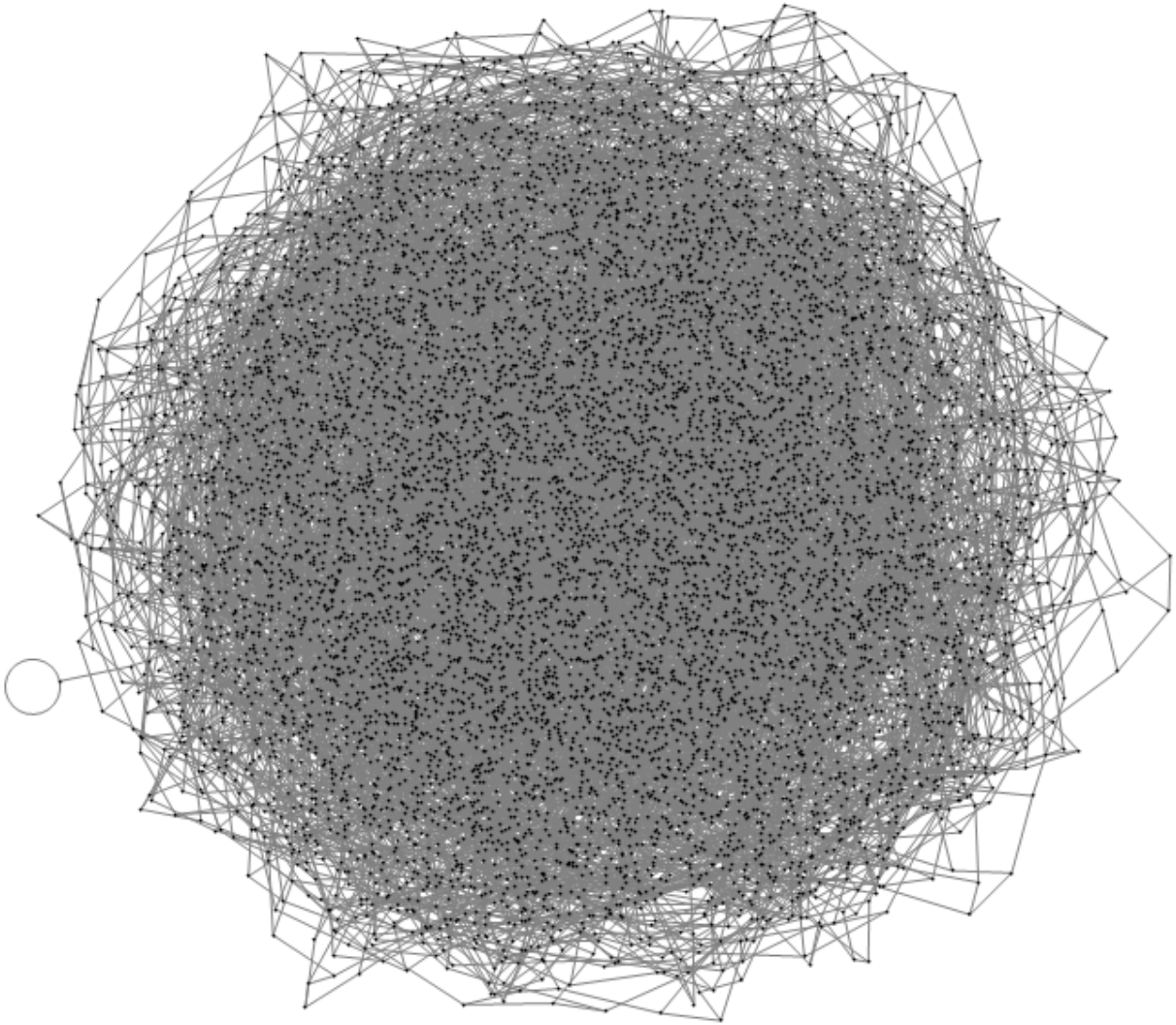
The supersingular isogeny graph $\mathcal{G}(p, \ell)$ has

- Vertices: isomorphism classes of supersingular elliptic curves over $\mathbb{F}_{p^2}$ ($\approx \frac{p}{12}$ vertices).
- Edges: degree ℓ isogenies, up to post-composition with an isomorphism ($\ell + 1$ edges from each vertex).

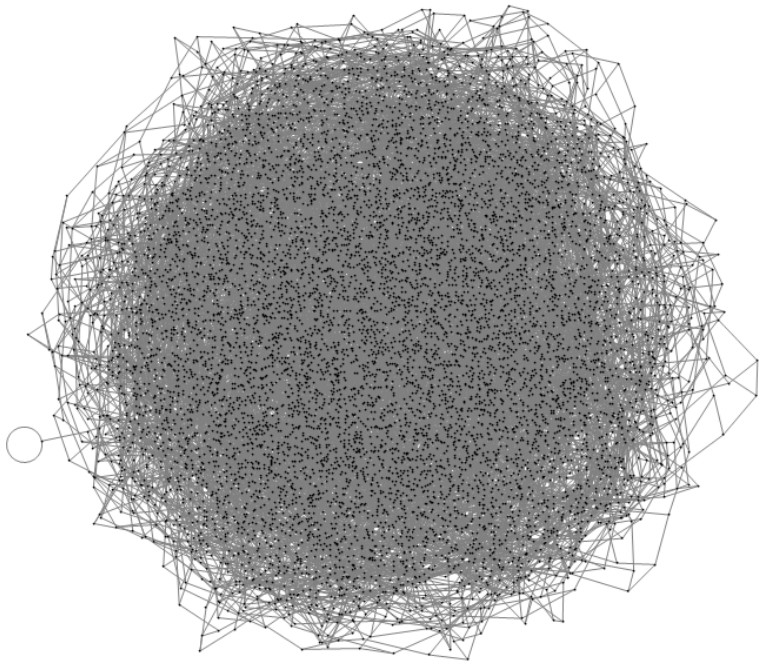
$\mathcal{G}(p, \ell)$ is directed, but we can associate each isogeny $E \to E'$ with its dual $E' \to E$ to get an undirected graph (small issues at curves with extra automorphisms).

Preview

$\mathcal{G}(100003, 2)$:



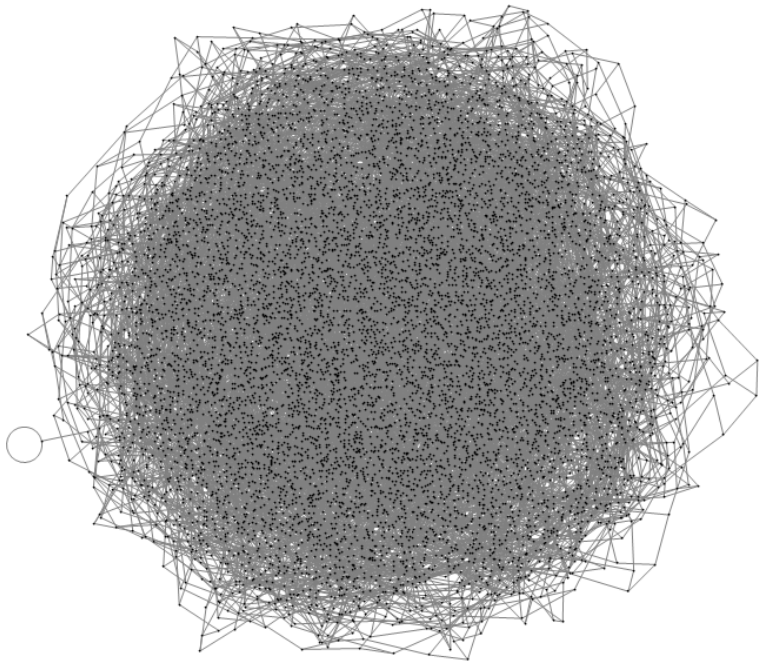
Preview



Supersingular isogeny graphs are known for being “messy”

- Expander graphs (Ramanujan property)
- No known efficient path-finding algorithm

Preview



Supersingular isogeny graphs are known for being "messy"

- Expander graphs (Ramanujan property)
- No known efficient path-finding algorithm

Goal: identify structures within these graphs.

Key idea:

The shape of the endomorphism ring of E
determines the structure of $\mathcal{G}(p, \ell)$ near E.

A quaternion primer

$B_{p,\infty}$: the quaternion algebra over $\mathbb{Q}$ ramified at p and ∞.

A quaternion primer

$B_{p,\infty}$: the quaternion algebra over $\mathbb{Q}$ ramified at p and ∞.

If $p \equiv 3 \bmod 4$ (e.g. $p = 100003$),

$$B_{p,\infty} := \{a + bi + cj + dk : a, b, c, d \in \mathbb{Q}\}$$

is a $\mathbb{Q}$-algebra with multiplication determined by

$$i^2 = -1, \quad j^2 = k^2 = -p, \quad ij = -ji = k.$$

A quaternion primer

$B_{p,\infty}$: the quaternion algebra over $\mathbb{Q}$ ramified at p and ∞.

If $p \equiv 3 \bmod 4$ (e.g. $p = 100003$),

$$B_{p,\infty} := \{a + bi + cj + dk : a, b, c, d \in \mathbb{Q}\}$$

is a $\mathbb{Q}$-algebra with multiplication determined by

$$i^2 = -1, \quad j^2 = k^2 = -p, \quad ij = -ji = k.$$

For $\alpha = a + bi + cj + dk \in B_{p,\infty}$,

- Conjugate: $\overline{\alpha} := a - bi - cj - dk$,
- Trace: $\mathrm{Tr}(\alpha) := \alpha + \overline{\alpha} = 2a$,
- Norm: $N(\alpha) := \alpha\overline{\alpha} = a^2 + b^2 + pc^2 + pd^2$.

A quaternion primer

For $\alpha = a + bi + cj + dk \in B_{p,\infty}$,

- Conjugate: $\overline{\alpha} := a - bi - cj - dk$,
- Trace: $\mathrm{Tr}(\alpha) := \alpha + \overline{\alpha} = 2a$,
- Norm: $N(\alpha) := \alpha\overline{\alpha} = a^2 + b^2 + pc^2 + pd^2$.

A quaternion primer

For $\alpha = a + bi + cj + dk \in B_{p,\infty}$,

- Conjugate: $\overline{\alpha} := a - bi - cj - dk$,
- Trace: $\mathrm{Tr}(\alpha) := \alpha + \overline{\alpha} = 2a$,
- Norm: $N(\alpha) := \alpha\overline{\alpha} = a^2 + b^2 + pc^2 + pd^2$.

The norm N is a *positive-definite quadratic form* on $B_{p,\infty} \simeq \mathbb{Q}^4$.
Inner product:

$$\begin{aligned}\langle x, y\rangle &= \frac{1}{2}(N(x+y) - N(x) - N(y)) \\ &= \frac{1}{2}((x+y)(\overline{x}+\overline{y}) - x\overline{x} - y\overline{y}) \\ &= \frac{1}{2}(x\overline{y} + y\overline{x}) \\ &= \frac{1}{2}\,\mathrm{Tr}(x\overline{y})\end{aligned}$$

A quaternion primer

An order in $B_{p,\infty}$ is a discrete subring, isomorphic (as an additive group) to $\mathbb{Z}^4$. An order is maximal if it is not strictly contained in another order.

A quaternion primer

An order in $B_{p,\infty}$ is a discrete subring, isomorphic (as an additive group) to $\mathbb{Z}^4$. An order is maximal if it is not strictly contained in another order.

Two orders $\mathcal{O}, \mathcal{O}'$ are equivalent if $\mathcal{O}' = x\mathcal{O}x^{-1}$ for some $x \in B_{p,\infty}$.

A quaternion primer

An order in $B_{p,\infty}$ is a discrete subring, isomorphic (as an additive group) to $\mathbb{Z}^4$. An order is maximal if it is not strictly contained in another order.

Two orders $\mathcal{O}, \mathcal{O}'$ are equivalent if $\mathcal{O}' = x\mathcal{O}x^{-1}$ for some $x \in B_{p,\infty}$.

Equivalently, $\mathcal{O}, \mathcal{O}'$ equivalent if $\mathcal{O}' \simeq \mathcal{O}$ as rings:

- Ring structure "knows" isometry structure (via the norm)
- Every isometry of $B_{p,\infty}$ fixing $\mathbb{Q}$ is conjugation

A quaternion primer

An order in $B_{p,\infty}$ is a discrete subring, isomorphic (as an additive group) to $\mathbb{Z}^4$. An order is maximal if it is not strictly contained in another order.

Two orders $\mathcal{O}, \mathcal{O}'$ are equivalent if $\mathcal{O}' = x\mathcal{O}x^{-1}$ for some $x \in B_{p,\infty}$.

Equivalently, $\mathcal{O}, \mathcal{O}'$ equivalent if $\mathcal{O}' \simeq \mathcal{O}$ as rings:

- Ring structure "knows" isometry structure (via the norm)
- Every isometry of $B_{p,\infty}$ fixing $\mathbb{Q}$ is conjugation

The number of equivalence classes of maximal orders in $B_{p,\infty}$ is finite, but large ($> \frac{p}{24}$).

A quaternion primer

For supersingular $E/\mathbb{F}_{p^2}$, the endomorphism ring $\mathrm{End}(E)$ is the set of all isogenies from E to itself (and the zero map), with operations

$$(f+g)(P) = f(P) + g(P) \qquad \text{and} \qquad (f \cdot g)(P) = f(g(P)).$$

A quaternion primer

For supersingular $E/\mathbb{F}_{p^2}$, the endomorphism ring $\mathrm{End}(E)$ is the set of all isogenies from E to itself (and the zero map), with operations

$$(f+g)(P) = f(P) + g(P) \qquad \text{and} \qquad (f \cdot g)(P) = f(g(P)).$$

Proposition (follows from Deuring correspondence)

1. $\mathrm{End}(E)$ is isomorphic to a maximal order in $B_{p,\infty}$.

A quaternion primer

For supersingular $E/\mathbb{F}_{p^2}$, the endomorphism ring $\mathrm{End}(E)$ is the set of all isogenies from E to itself (and the zero map), with operations

$$(f+g)(P) = f(P) + g(P) \qquad \text{and} \qquad (f \cdot g)(P) = f(g(P)).$$

Proposition (follows from Deuring correspondence)

1. $\mathrm{End}(E)$ is isomorphic to a maximal order in $B_{p,\infty}$.
2. Each maximal order in $\mathcal{O}$ is isomorphic to $\mathrm{End}(E)$ for some E, uniquely determined up to $E \mapsto E^{(p)}$.

A quaternion primer

For supersingular $E/\mathbb{F}_{p^2}$, the endomorphism ring $\mathrm{End}(E)$ is the set of all isogenies from E to itself (and the zero map), with operations

$$(f+g)(P) = f(P) + g(P) \qquad \text{and} \qquad (f \cdot g)(P) = f(g(P)).$$

Proposition (follows from Deuring correspondence)

1. $\mathrm{End}(E)$ is isomorphic to a maximal order in $B_{p,\infty}$.
2. Each maximal order in $\mathcal{O}$ is isomorphic to $\mathrm{End}(E)$ for some E, uniquely determined up to $E \mapsto E^{(p)}$.
3. If $\phi : E \to E'$ is an isogeny, there exist orders $\mathcal{O} \simeq \mathrm{End}(E)$ and $\mathcal{O}' \simeq \mathrm{End}(E')$ such that

$$|\mathcal{O} : \mathcal{O} \cap \mathcal{O}'| = |\mathcal{O}' : \mathcal{O} \cap \mathcal{O}'| = \deg \phi.$$

Successive Minima of Gross Lattice

Successive Minima of Gross Lattice

$\mathcal{O} := \mathrm{End}(E)$ is 4-dimensional,
but one of these dimensions is just a copy of $\mathbb{Z}$.

Successive Minima of Gross Lattice

$\mathcal{O} := \mathrm{End}(E)$ is 4-dimensional,
but one of these dimensions is just a copy of $\mathbb{Z}$.

Definition

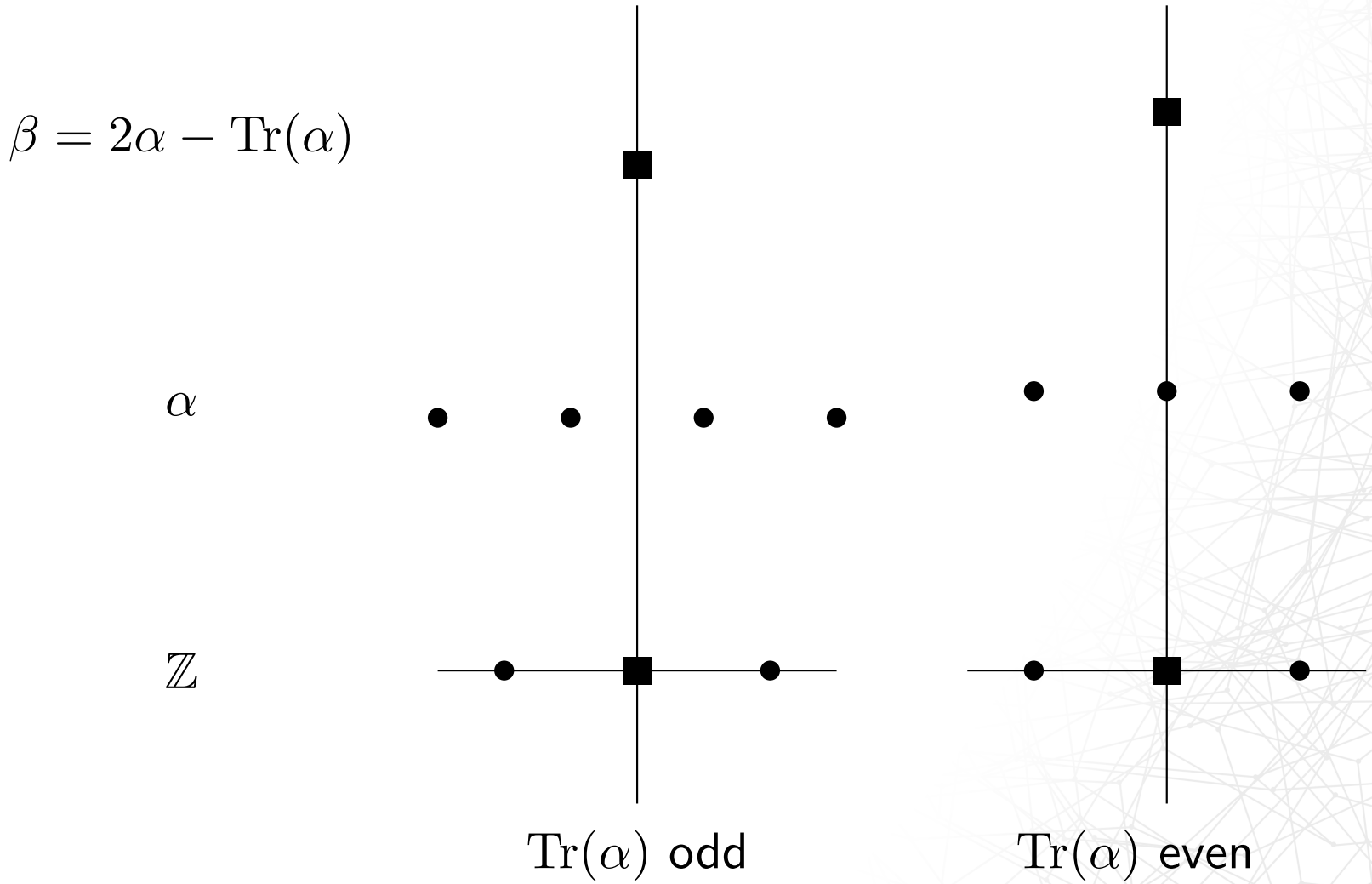
The Gross lattice of $\mathcal{O}$ is

$$\begin{aligned}\mathcal{O}^T &:= \{2\alpha - \mathrm{Tr}(\alpha) : \alpha \in \mathcal{O}\} \\ &= 2 \cdot (\text{orthogonal projection of } \mathcal{O} \text{ onto } B^0_{p,\infty})\end{aligned}$$

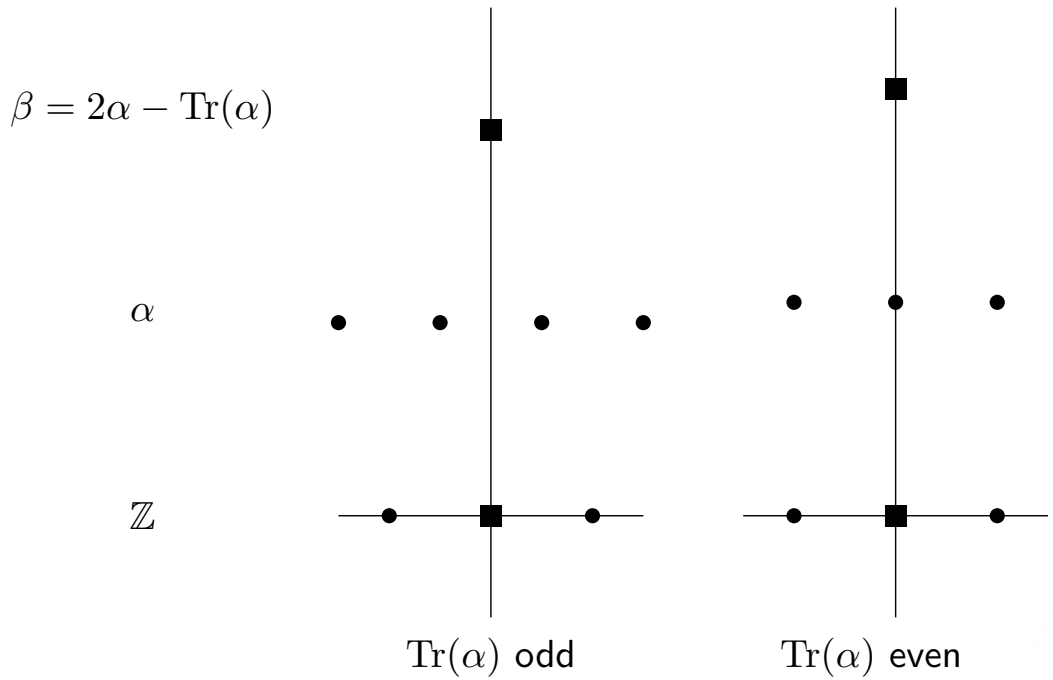
where $B^0_{p,\infty}$ is the trace-zero subspace of $B_{p,\infty}$.

Successive Minima of Gross Lattice

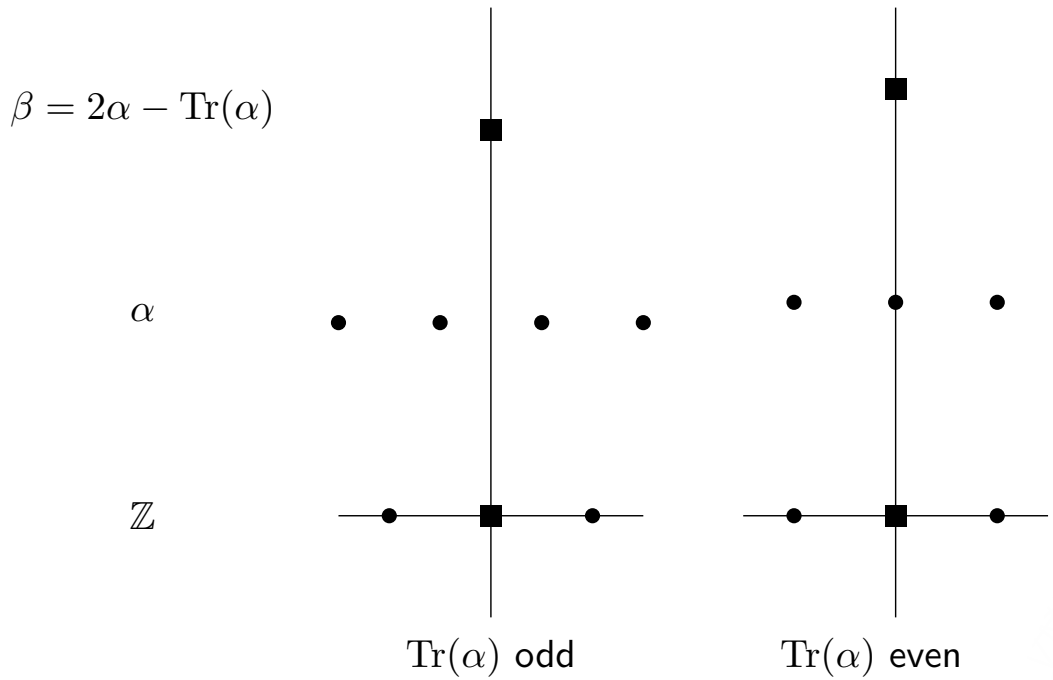
2-d slices of $\mathcal{O}$: intersect $\mathcal{O}$ with the subspace of $B_{p,\infty}$ spanned by 1 and $\alpha \in \mathcal{O} \setminus \mathbb{Z}$.



Successive Minima of Gross Lattice



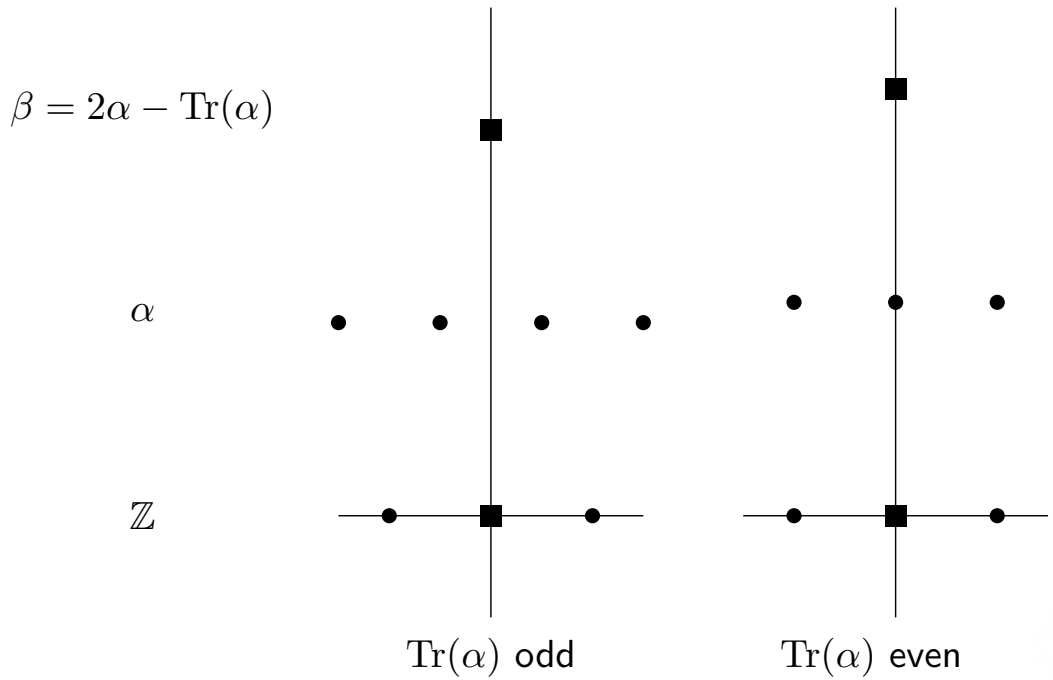
Successive Minima of Gross Lattice



Nice Fact: If $\mathbb{Z}[\alpha]$ is a quadratic order of discriminant $-D$, then

$$N(\beta) = N(2\alpha - \mathrm{Tr}(\alpha)) = 4N(\alpha) - \mathrm{Tr}(\alpha)^2 = D.$$

Successive Minima of Gross Lattice



Nice Fact: If $\mathbb{Z}[\alpha]$ is a quadratic order of discriminant $-D$, then

$$N(\beta) = N(2\alpha - \mathrm{Tr}(\alpha)) = 4N(\alpha) - \mathrm{Tr}(\alpha)^2 = D.$$

Gross lattice **parametrizes embeddings of quadratic orders in $\mathcal{O}$.**

Successive Minima of Gross Lattice

We will consider a "short basis" for $\mathcal{O}^T$.

Successive Minima of Gross Lattice

We will consider a "short basis" for $\mathcal{O}^T$.

Definition

For $i = 1, 2, 3$, let $\beta_1, \beta_2, \beta_3$ be a basis of $\mathcal{O}^T$, and $D_i := N(\beta_i)$ for each i. If

$$\text{span}\{x \in \mathcal{O}^T : N(x) < D_i\}$$

has dimension smaller than i for $i = 1, 2, 3$, then D_1, D_2, D_3 are called the successive minima of $\mathcal{O}^T$, and $\beta_1, \beta_2, \beta_3$ attain the successive minima.

Successive Minima of Gross Lattice

We will consider a "short basis" for $\mathcal{O}^T$.

Definition

For $i = 1, 2, 3$, let $\beta_1, \beta_2, \beta_3$ be a basis of $\mathcal{O}^T$, and $D_i := N(\beta_i)$ for each i. If

$$\text{span}\{x \in \mathcal{O}^T : N(x) < D_i\}$$

has dimension smaller than i for $i = 1, 2, 3$, then D_1, D_2, D_3 are called the successive minima of $\mathcal{O}^T$, and $\beta_1, \beta_2, \beta_3$ attain the successive minima.

WARNING: Very non-standard definition!

- In most sources, the successive minima of a lattice are *lengths* λ_i, not values of a quadratic form. Here you can think of $D_i = \lambda_i^2$.
- For lattices of dimension ≥ 5, a basis satisfying the above property may not exist! Successive minima are typically defined in terms of *independent sets* rather than bases.

Successive Minima of Gross Lattice

The isometry type of the Gross lattice $\mathcal{O}^T$ determines $\mathcal{O}$ up to equivalence (even Clifford algebra of dual lattice).

Successive Minima of Gross Lattice

The isometry type of the Gross lattice $\mathcal{O}^T$ determines $\mathcal{O}$ up to equivalence (even Clifford algebra of dual lattice).

Theorem (Chevyrev–Galbraith '14, Goren–L '24)

A maximal order $\mathcal{O}$ in $B_{p,\infty}$ is uniquely determined up to isomorphism by the successive minima of its Gross lattice.

Successive Minima of Gross Lattice

The isometry type of the Gross lattice $\mathcal{O}^T$ determines $\mathcal{O}$ up to equivalence (even Clifford algebra of dual lattice).

Theorem (Chevyrev–Galbraith '14, Goren–L '24)

A maximal order $\mathcal{O}$ in $B_{p,\infty}$ is uniquely determined up to isomorphism by the successive minima of its Gross lattice.

We can use the successive minima (D_1, D_2, D_3) of $\mathrm{End}(E)^T$ as a label for E: only $E^{(p)}$ will have the same label.

Successive Minima of Gross Lattice

Example: $p = 100003$. Recall $B_{p,\infty}$ spanned by $1, i, j, k$ with

$$i^2 = -1, \quad j^2 = k^2 = -p, \quad ij = -ji = k.$$

Successive Minima of Gross Lattice

Example: $p = 100003$. Recall $B_{p,\infty}$ spanned by $1, i, j, k$ with

$$i^2 = -1, \quad j^2 = k^2 = -p, \quad ij = -ji = k.$$

Let $E/\mathbb{F}_p$ have j-invariant 1728. We have

$$\mathrm{End}(E) \simeq \left\{ a + bi + c\left(\frac{1+j}{2}\right) + d\left(\frac{i+k}{2}\right) : a, b, c, d \in \mathbb{Z} \right\}.$$

(Observations: $i \in \mathrm{End}(E)$ because E has extra automorphisms, and Frobenius $j \in \mathrm{End}(E)$ because $E/\mathbb{F}_p$.)

Successive Minima of Gross Lattice

Example: $p = 100003$. Recall $B_{p,\infty}$ spanned by $1, i, j, k$ with

$$i^2 = -1, \quad j^2 = k^2 = -p, \quad ij = -ji = k.$$

Let $E/\mathbb{F}_p$ have j-invariant 1728. We have

$$\mathrm{End}(E) \simeq \left\{ a + bi + c\left(\frac{1+j}{2}\right) + d\left(\frac{i+k}{2}\right) : a, b, c, d \in \mathbb{Z} \right\}.$$

(Observations: $i \in \mathrm{End}(E)$ because E has extra automorphisms, and Frobenius $j \in \mathrm{End}(E)$ because $E/\mathbb{F}_p$.) Applying $\alpha \mapsto 2\alpha - \mathrm{Tr}(\alpha)$,

$$\mathrm{End}(E)^T \simeq \{ b(2i) + cj + d(i+k) : b, c, d \in \mathbb{Z} \}.$$

Successive Minima of Gross Lattice

Example: $p = 100003$. Recall $B_{p,\infty}$ spanned by $1, i, j, k$ with

$$i^2 = -1, \quad j^2 = k^2 = -p, \quad ij = -ji = k.$$

Let $E/\mathbb{F}_p$ have j-invariant 1728. We have

$$\mathrm{End}(E) \simeq \left\{ a + bi + c\left(\frac{1+j}{2}\right) + d\left(\frac{i+k}{2}\right) : a, b, c, d \in \mathbb{Z} \right\}.$$

(Observations: $i \in \mathrm{End}(E)$ because E has extra automorphisms, and Frobenius $j \in \mathrm{End}(E)$ because $E/\mathbb{F}_p$.) Applying $\alpha \mapsto 2\alpha - \mathrm{Tr}(\alpha)$,

$$\mathrm{End}(E)^T \simeq \{ b(2i) + cj + d(i+k) : b, c, d \in \mathbb{Z} \}.$$

$$D_1 = N(2i) = 4, \quad D_2 = N(j) = p, \quad D_3 = N(i+k) = 1 + p,$$

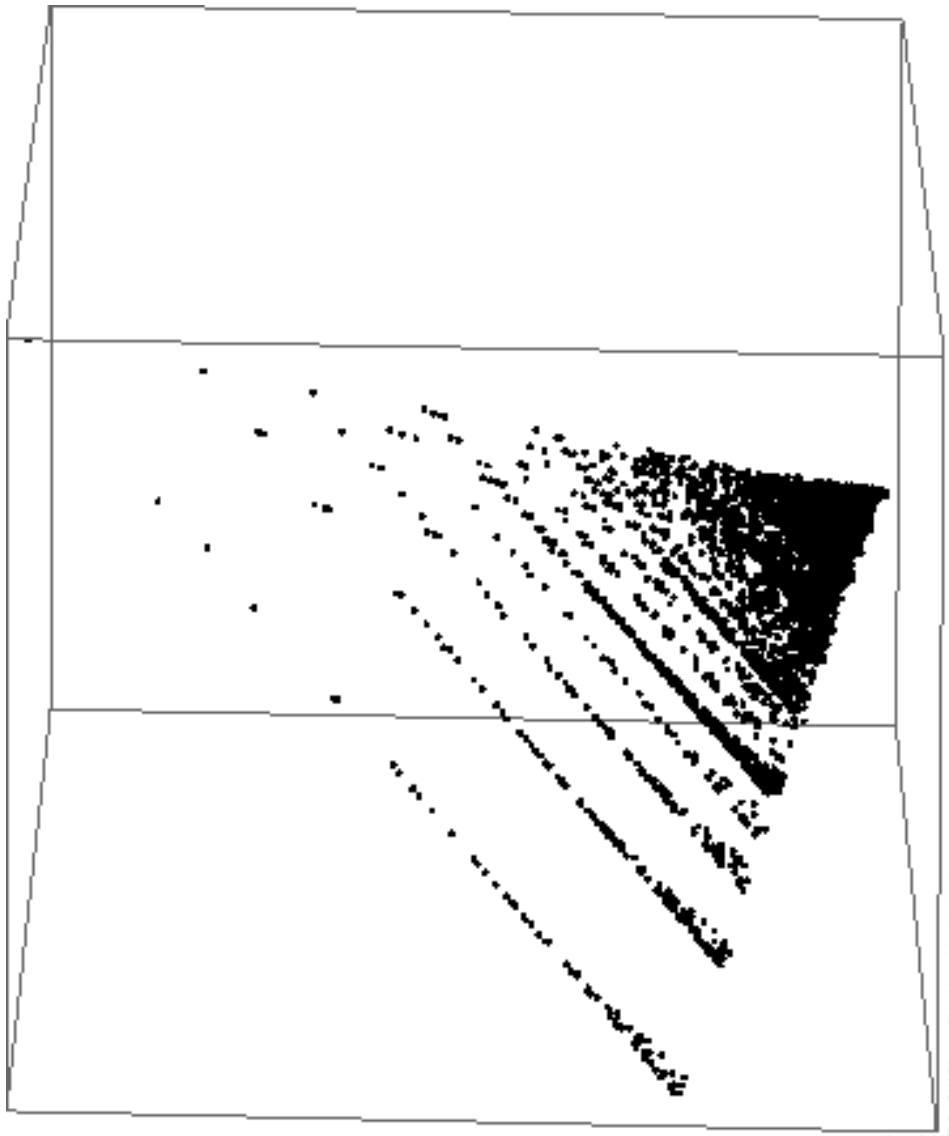
so E has label $(4, 100003, 100004)$.

Let's plot (D_1, D_2, D_3) for all supersingular $E/\mathbb{F}_{100003^2}$.

Let's plot (D_1, D_2, D_3) for all supersingular $E/\mathbb{F}_{1000003^2}$.

Since the successive minima can get quite large, we'll plot in *log scale* (i.e. actually plot $(\log D_1, \log D_2, \log D_3)$).

Plotting (D_1, D_2, D_3) in log-scale for all supersingular $E/\mathbb{F}_{100003^2}$



- Why does (D_1, D_2, D_3) appear to lie in a plane?
- What are the bounds on the region these points lie in?
- Which points are in the sparse zone?
- Which points are connected by 2-isogenies?
- Why are there stripes?

Why does (D_1, D_2, D_3) appear to lie in a plane?

Why does (D_1, D_2, D_3) appear to lie in a plane?

Given a lattice Λ with inner product, let $b_1, \ldots, b_n$ be a basis for Λ. We define the determinant

$$\det \Lambda := \det \left(\langle b_i, b_j \rangle \right)_{i,j} .$$

Why does (D_1, D_2, D_3) appear to lie in a plane?

Given a lattice Λ with inner product, let $b_1, \ldots, b_n$ be a basis for Λ. We define the determinant

$$\det \Lambda := \det \left(\langle b_i, b_j \rangle \right)_{i,j}.$$

If $\Lambda \subseteq \mathbb{R}^n$ with standard inner product, and B is the matrix with columns $b_1, \ldots, b_n$, then

$$\det \Lambda = \det(B^T B) = (\det B)^2.$$

$\det \Lambda$ is the *squared* covolume.

Why does (D_1, D_2, D_3) appear to lie in a plane?

Fact: For a maximal order $\mathcal{O}$,

$$\det \mathcal{O} = \frac{1}{16} p^2.$$

Why does (D_1, D_2, D_3) appear to lie in a plane?

Fact: For a maximal order $\mathcal{O}$,

$$\det \mathcal{O} = \frac{1}{16} p^2.$$

$\mathbb{Z} \oplus \mathcal{O}^T$ is an index 8 sublattice of $\mathcal{O}$, so

$$\begin{aligned} \det \mathcal{O}^T &= \det(\mathbb{Z} \oplus \mathcal{O}^T) \\ &= 8^2 \det \mathcal{O} \\ &= 4p^2. \end{aligned}$$

Why does (D_1, D_2, D_3) appear to lie in a plane?

Fact: For a maximal order $\mathcal{O}$,

$$\det \mathcal{O} = \frac{1}{16} p^2.$$

$\mathbb{Z} \oplus \mathcal{O}^T$ is an index 8 sublattice of $\mathcal{O}$, so

$$\begin{aligned} \det \mathcal{O}^T &= \det(\mathbb{Z} \oplus \mathcal{O}^T) \\ &= 8^2 \det \mathcal{O} \\ &= 4p^2. \end{aligned}$$

Gross lattices of maximal orders have equal determinants.

Why does (D_1, D_2, D_3) appear to lie in a plane?

Vectors attaining successive minima are "almost" an orthogonal basis, and so $D_1 D_2 D_3 \approx \det \mathcal{O}^T = 4p^2$.

Why does (D_1, D_2, D_3) appear to lie in a plane?

Vectors attaining successive minima are "almost" an orthogonal basis, and so $D_1 D_2 D_3 \approx \det \mathcal{O}^T = 4p^2$. More precisely,

$$4p^2 \leq D_1 D_2 D_3 \leq 8p^2,$$

Why does (D_1, D_2, D_3) appear to lie in a plane?

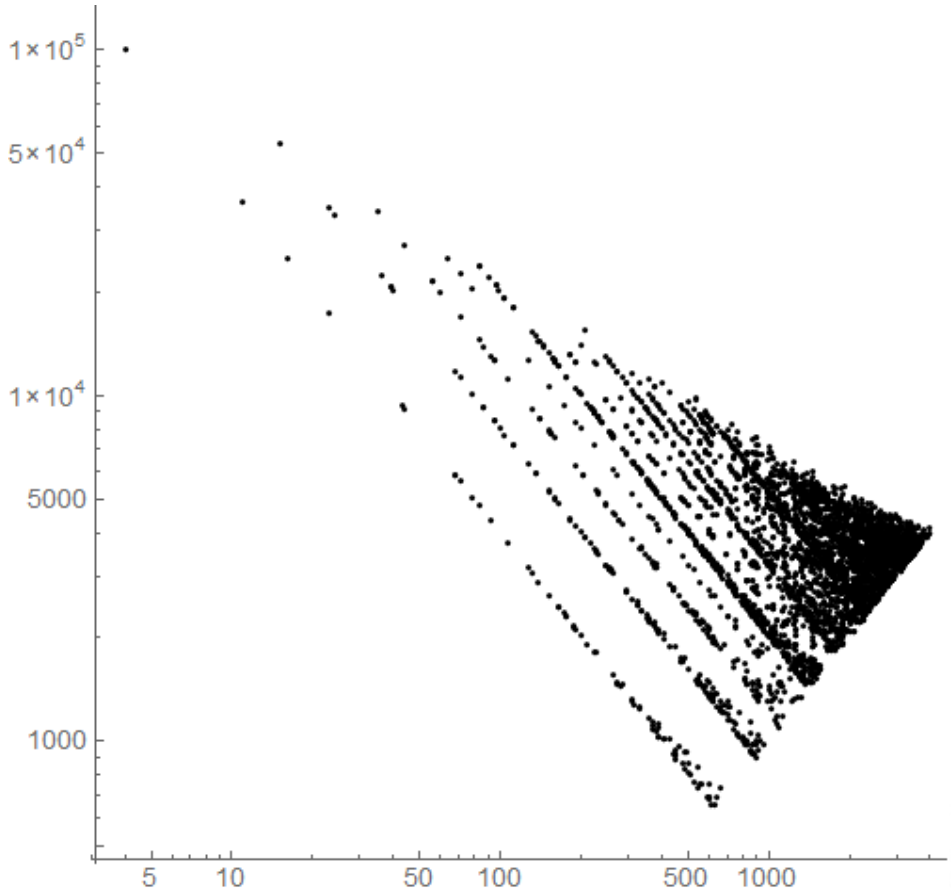
Vectors attaining successive minima are "almost" an orthogonal basis, and so $D_1 D_2 D_3 \approx \det \mathcal{O}^T = 4p^2$. More precisely,

$$4p^2 \leq D_1 D_2 D_3 \leq 8p^2,$$

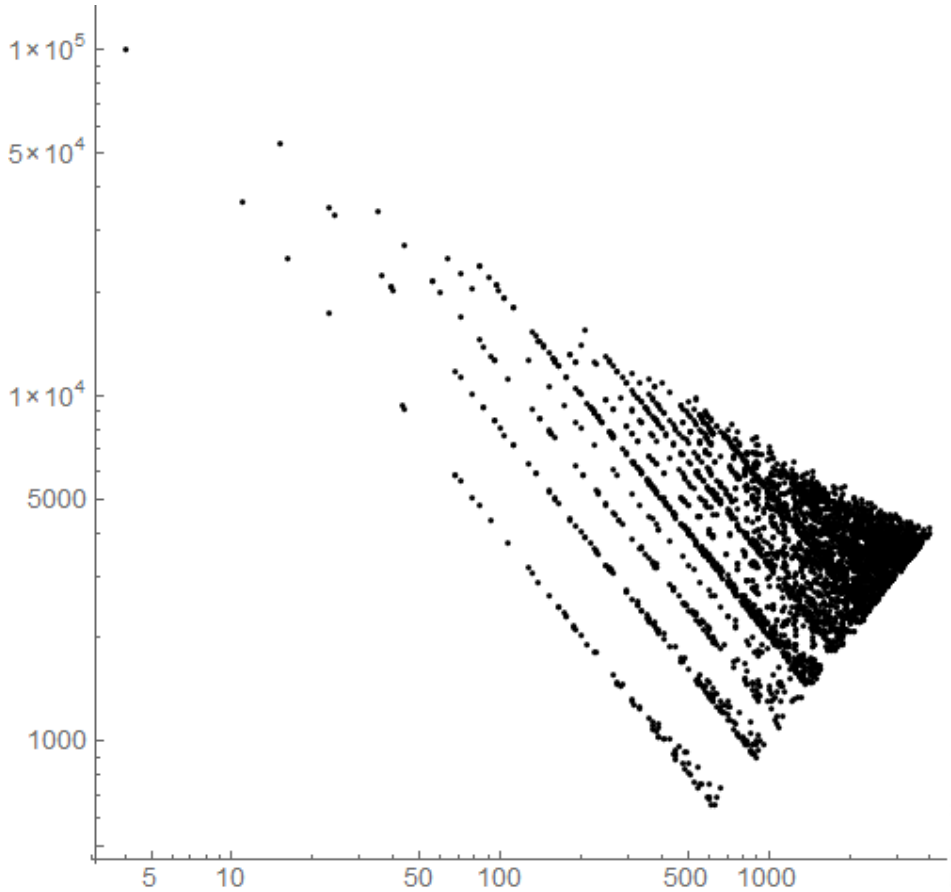
so

$$|(\log D_1 + \log D_2 + \log D_3) - (\log 4p^2)| \leq \log 2.$$

Plotting (D_1, D_2) for all supersingular $E/\mathbb{F}_{1000003^2}$

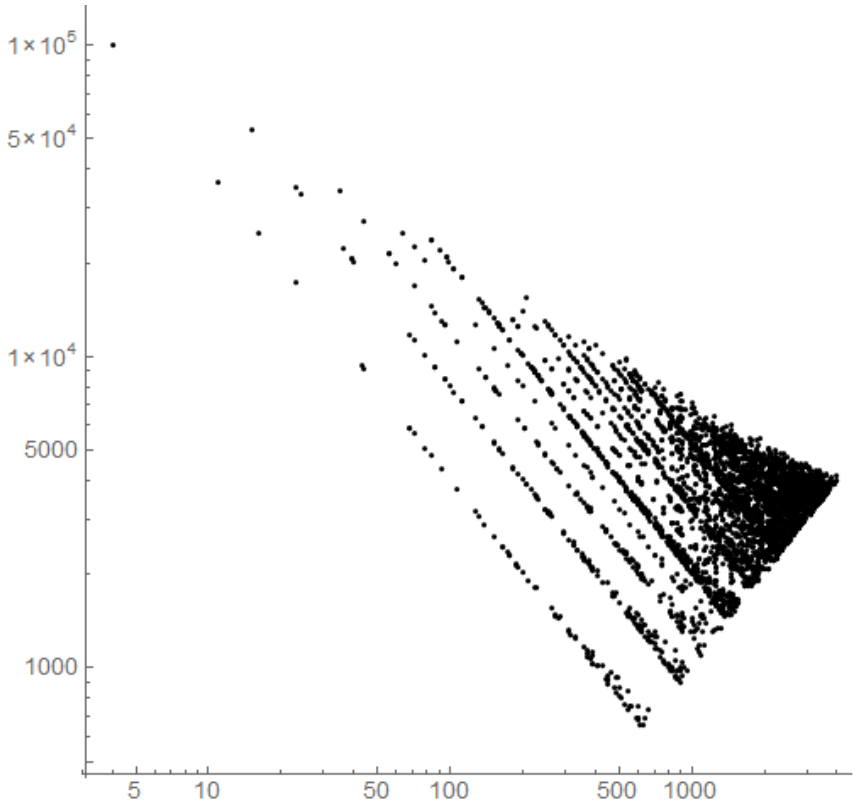


Plotting (D_1, D_2) for all supersingular $E/\mathbb{F}_{1000003^2}$

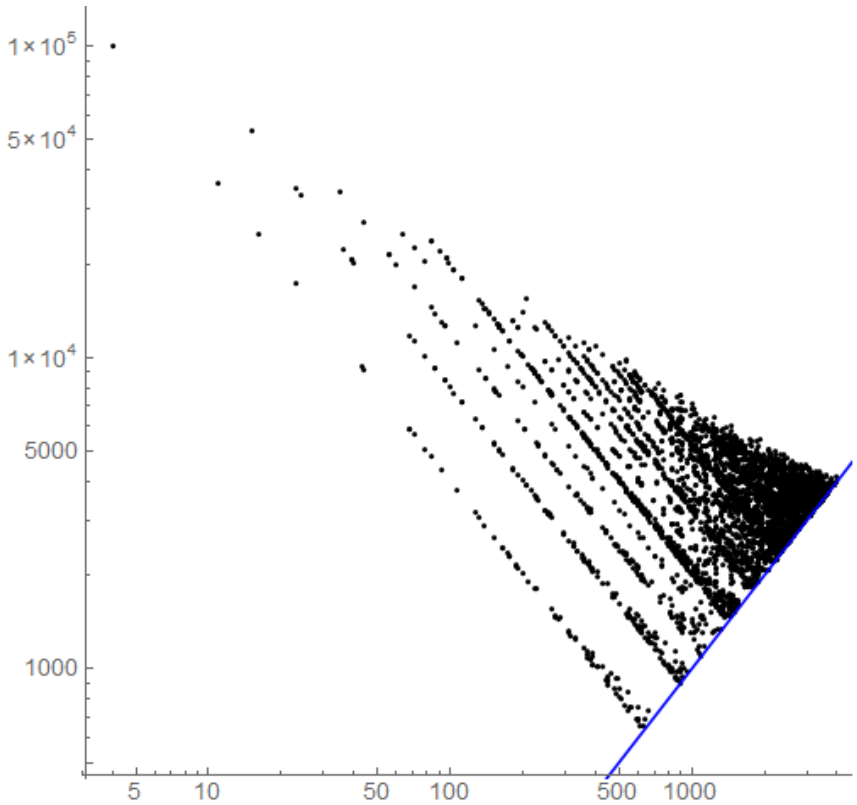


WARNING: (D_1, D_2) does not determine the maximal order. Out of 4206 maximal orders, there are 738 pairs with equal (D_1, D_2): e.g.
$(D_1, D_2, D_3) = (183, 13151, 17504)$ and $(183, 13151, 17487)$ occur.

What are the bounds on this region?



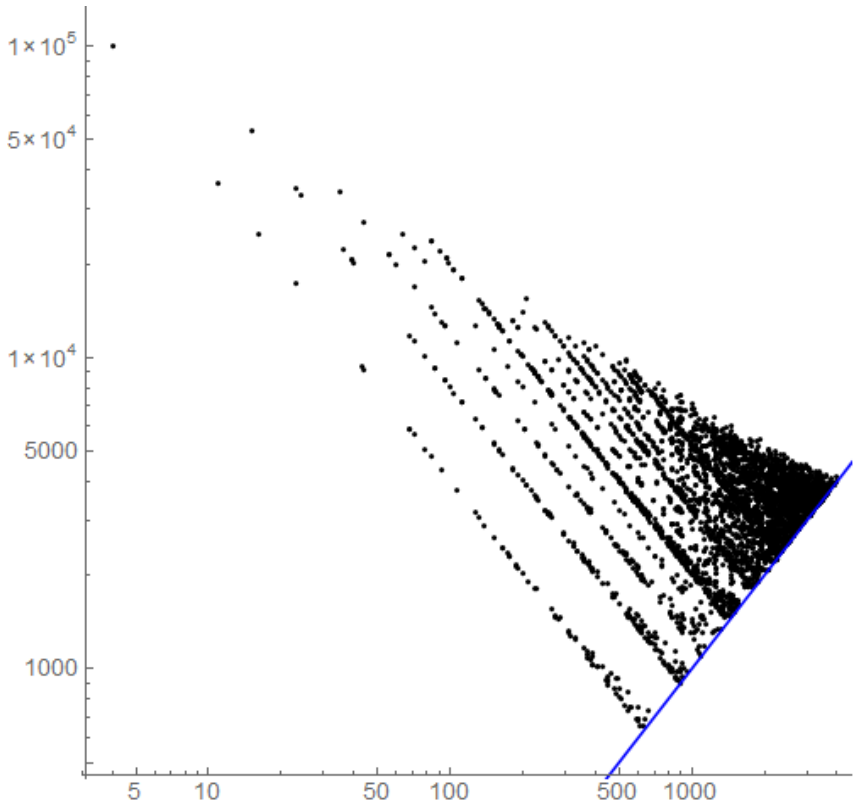
What are the bounds on this region?



Definition of successive minima:

- $D_1 \leq D_2$.

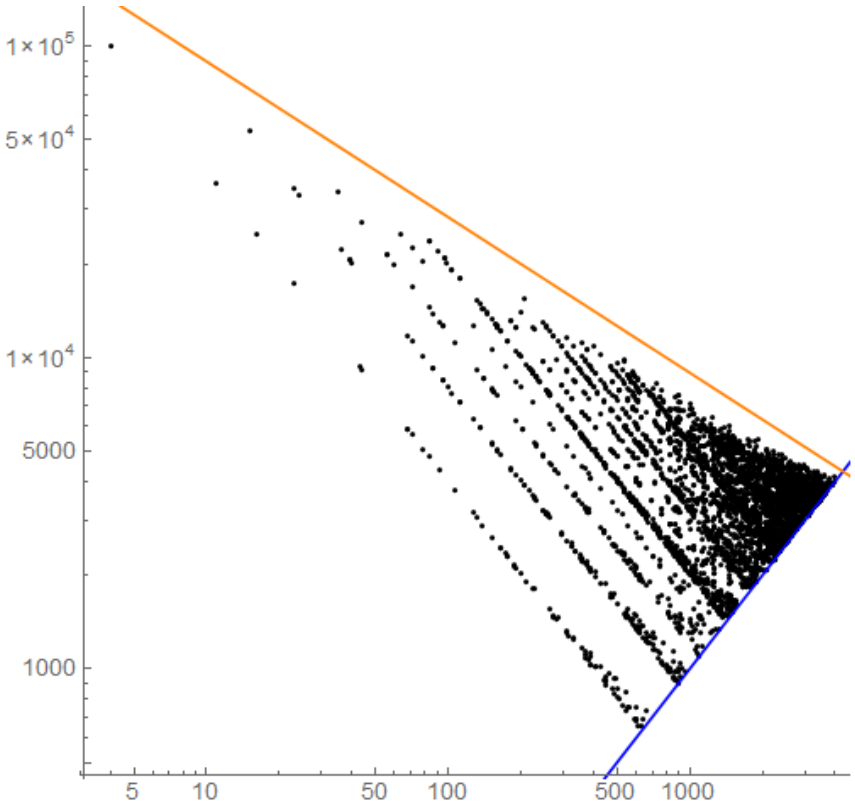
What are the bounds on this region?



Definition of successive minima:

- $D_1 \leq D_2$.
- $D_2 \leq D_3$

What are the bounds on this region?

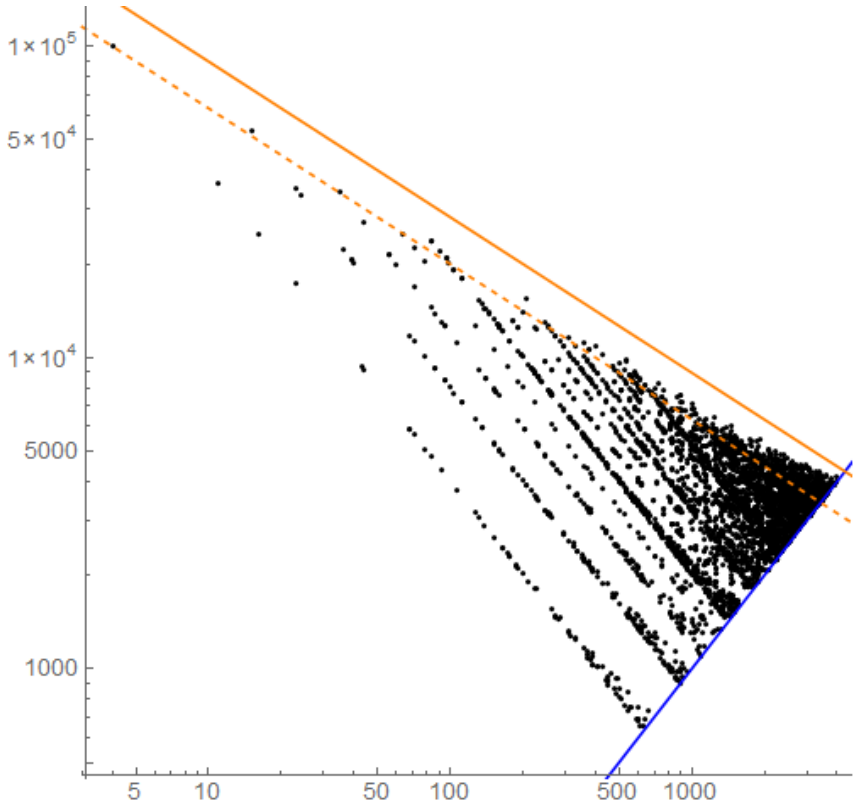


Definition of successive minima:

- $D_1 \leq D_2$.
- $D_2 \leq D_3 \leq \frac{8p^2}{D_1 D_2}$, so $D_2 \leq \frac{2p\sqrt{2}}{\sqrt{D_1}}$.

(Recall $4p^2 \leq D_1 D_2 D_3 \leq 8p^2$)

What are the bounds on this region?



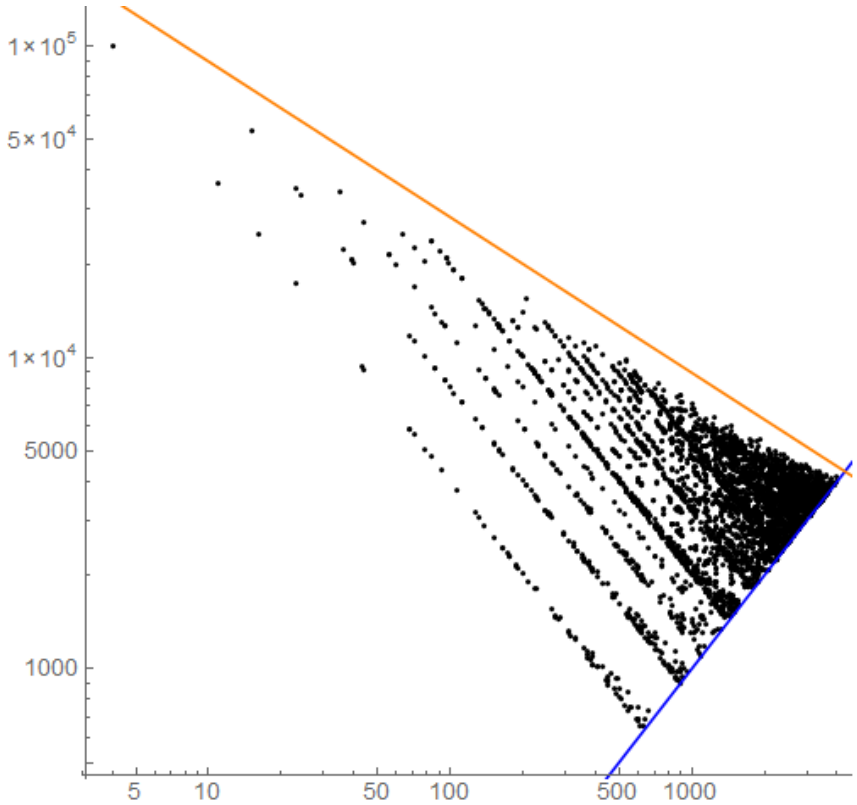
Definition of successive minima:

- $D_1 \leq D_2$.
- $D_2 \leq D_3 \leq \frac{8p^2}{D_1 D_2}$, so $D_2 \leq \frac{2p\sqrt{2}}{\sqrt{D_1}}$.

  If $\mathcal{O}^T$ has an orthogonal basis, then $D_1 D_2 D_3 = 4p^2$ and so $D_2 \leq \frac{2p}{\sqrt{D_1}}$.

(Recall $4p^2 \leq D_1 D_2 D_3 \leq 8p^2$)

What are the bounds on this region?

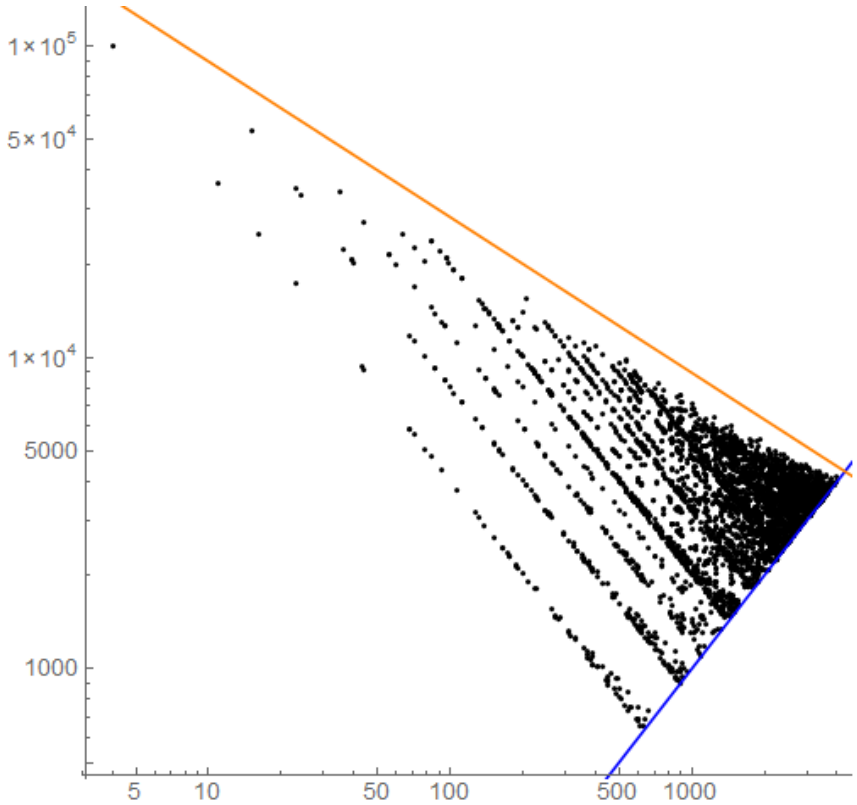


Definition of successive minima:

- $D_1 \leq D_2$.
- $D_2 \leq D_3 \leq \frac{8p^2}{D_1 D_2}$, so $D_2 \leq \frac{2p\sqrt{2}}{\sqrt{D_1}}$.

(Recall $4p^2 \leq D_1 D_2 D_3 \leq 8p^2$)

What are the bounds on this region?



Definition of successive minima:

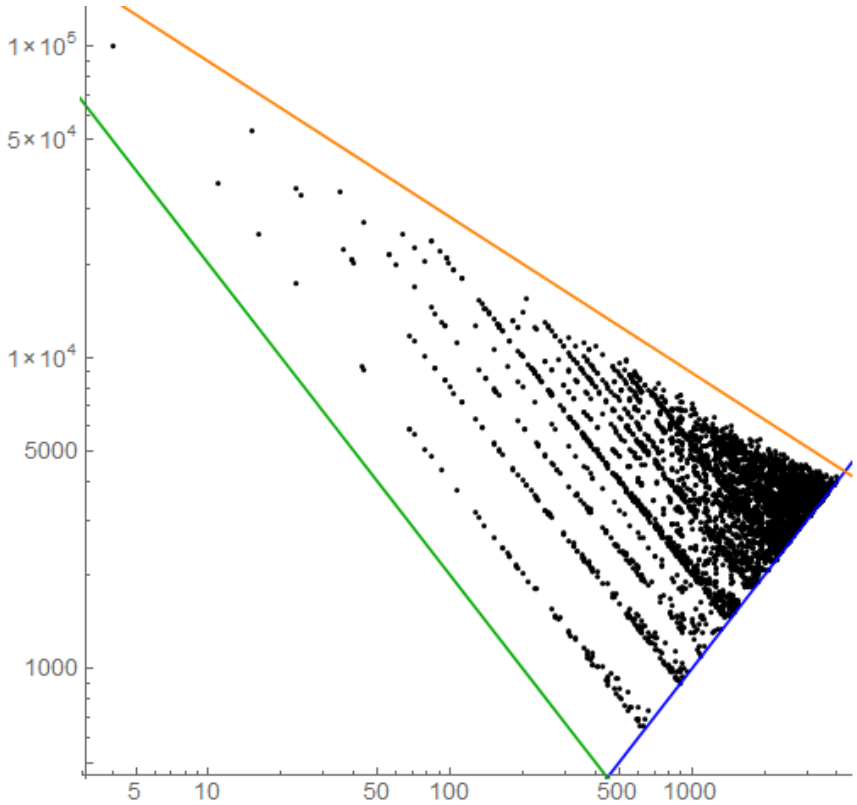
- $D_1 \leq D_2$.
- $D_2 \leq D_3 \leq \frac{8p^2}{D_1 D_2}$, so $D_2 \leq \frac{2p\sqrt{2}}{\sqrt{D_1}}$.

$\mathcal{O}$ closed under multiplication:

- $D_1 D_2 \geq D_3$

(Recall $4p^2 \leq D_1 D_2 D_3 \leq 8p^2$)

What are the bounds on this region?



Definition of successive minima:

- $D_1 \leq D_2$.
- $D_2 \leq D_3 \leq \frac{8p^2}{D_1 D_2}$, so $D_2 \leq \frac{2p\sqrt{2}}{\sqrt{D_1}}$.

$\mathcal{O}$ closed under multiplication:

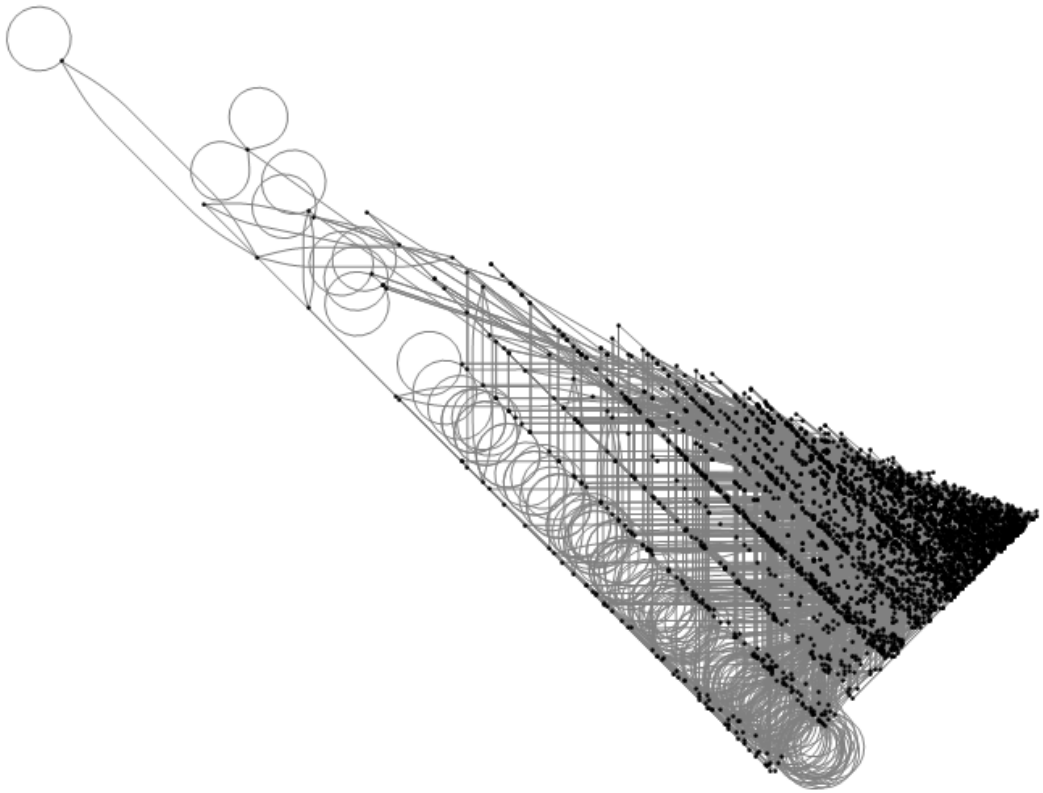
- $D_1 D_2 \geq D_3 \geq \frac{4p^2}{D_1 D_2}$, so $D_2 \geq \frac{2p}{D_1}$.

(Recall $4p^2 \leq D_1 D_2 D_3 \leq 8p^2$)

Which points are connected by isogenies?

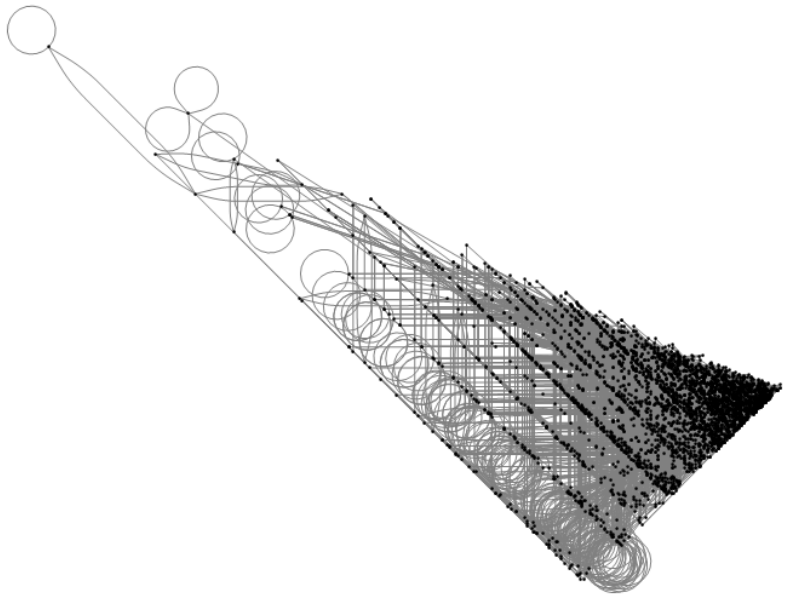
Which points are connected by isogenies?

Image of $\mathcal{G}(p, 2)$:



Which points are connected by isogenies?

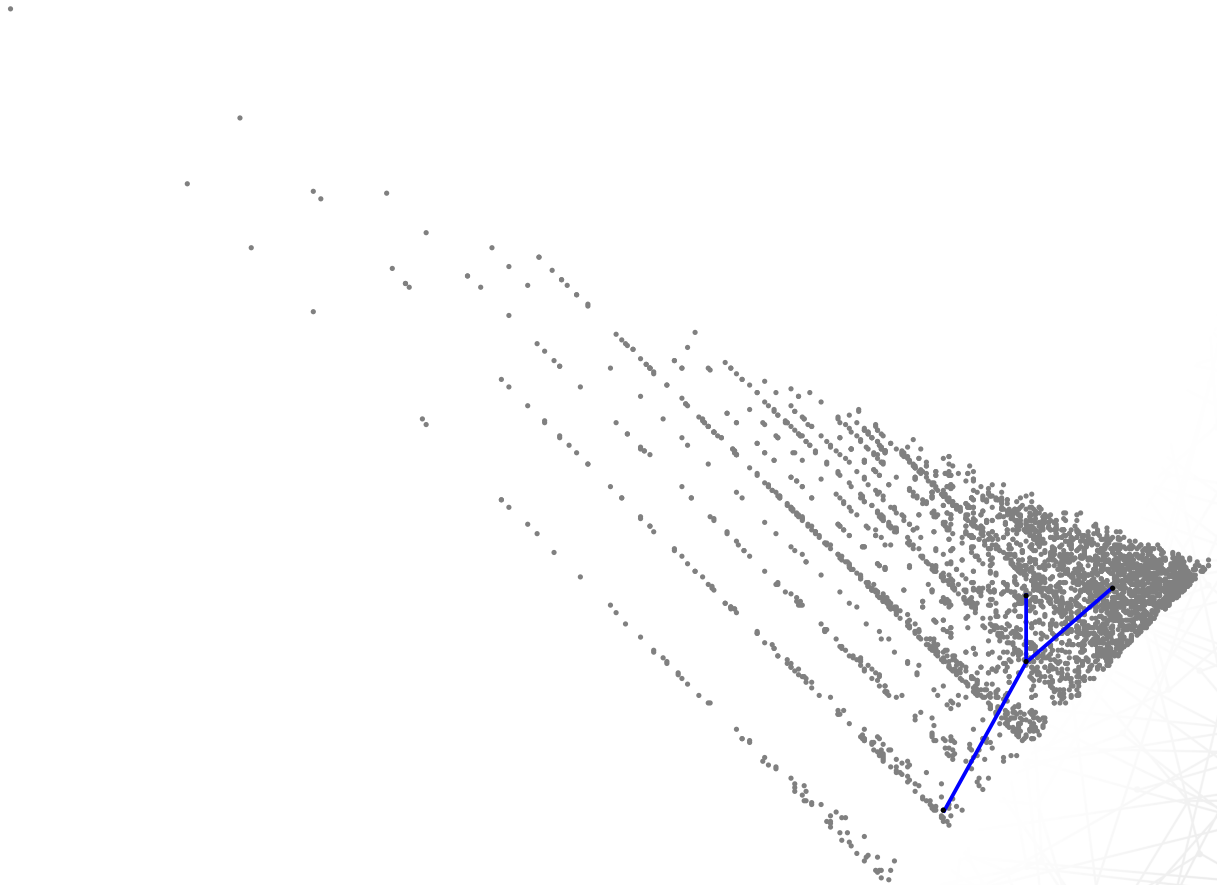
Image of $\mathcal{G}(p, 2)$:



- How long can the edges be?
- Why so many horizontal/vertical/45° edges?
- Why so many loops along that one diagonal?

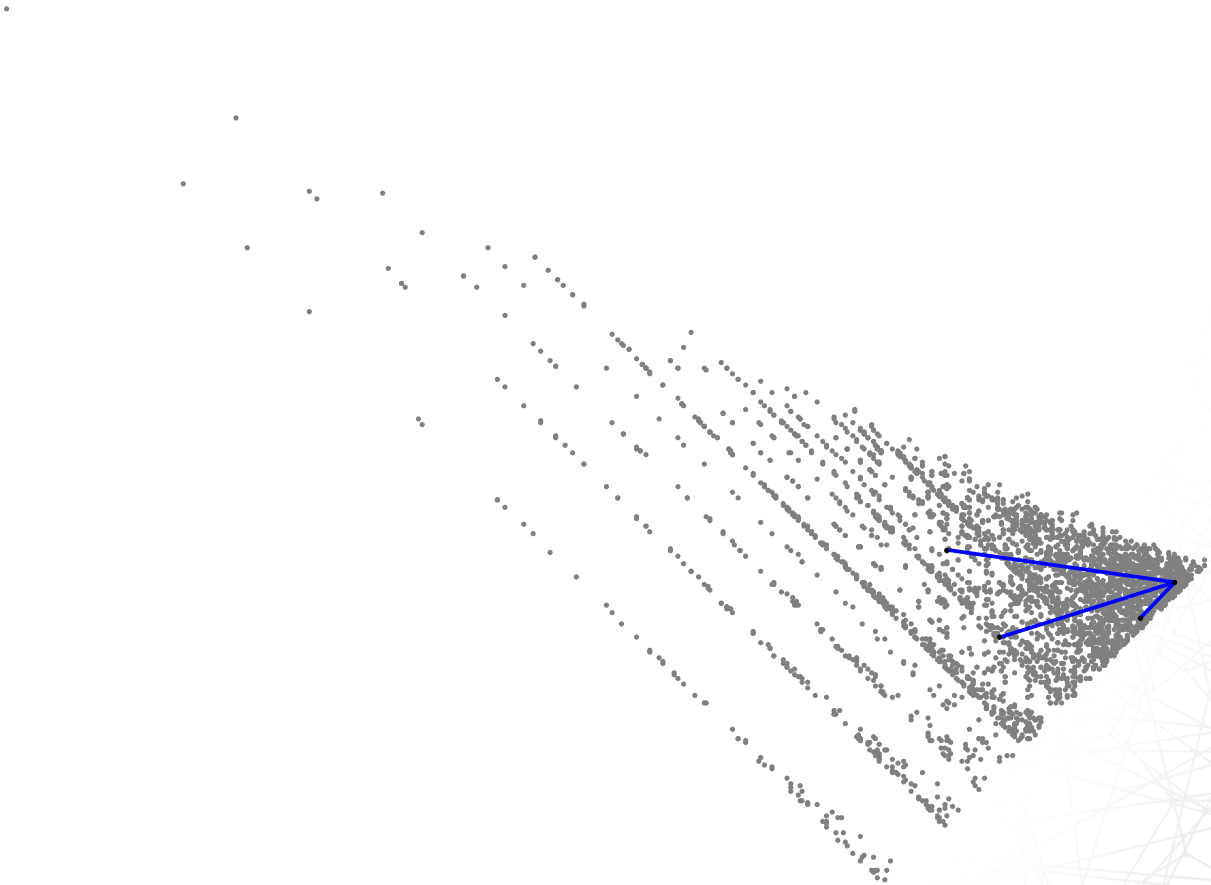
Which points are connected by isogenies?

Image of $\mathcal{G}(p, 2)$:



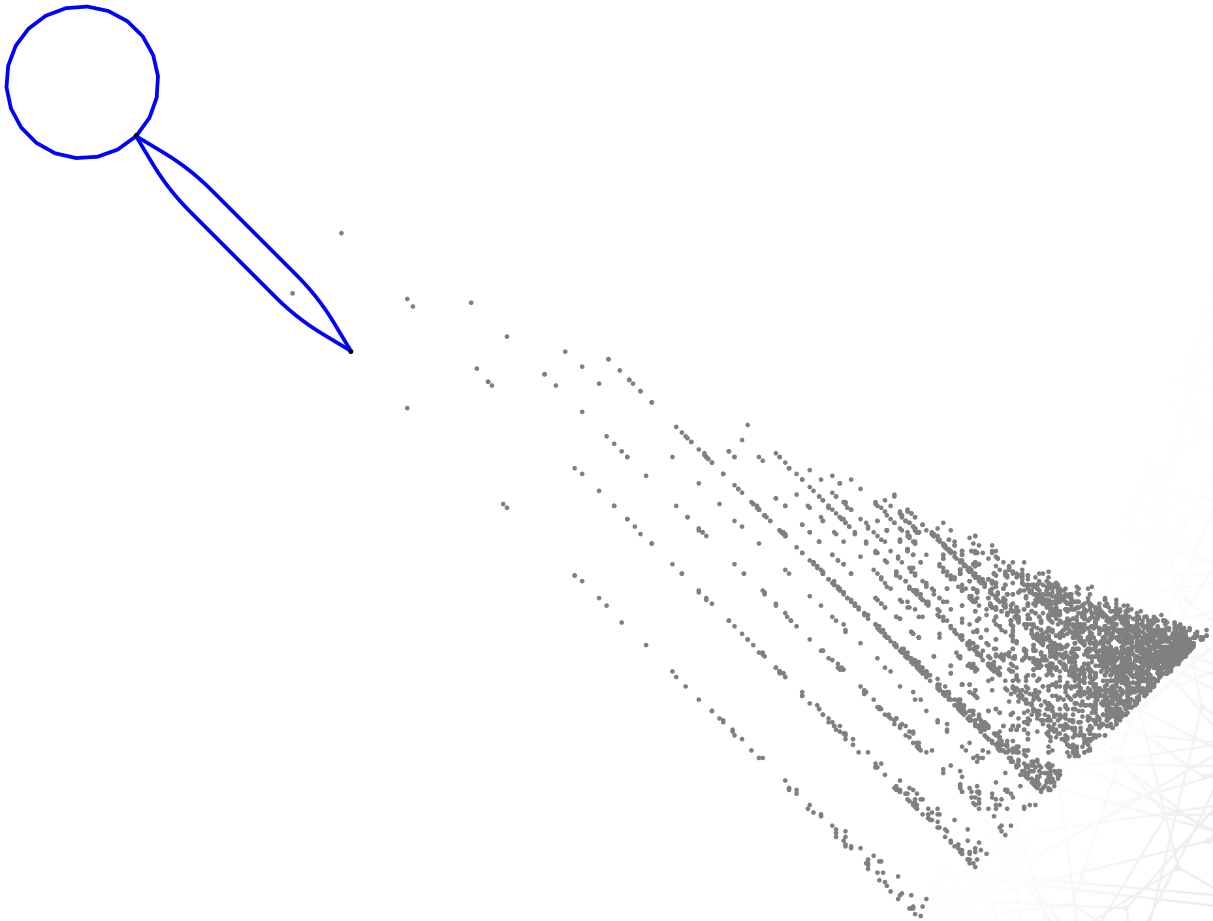
Which points are connected by isogenies?

Image of $\mathcal{G}(p, 2)$:



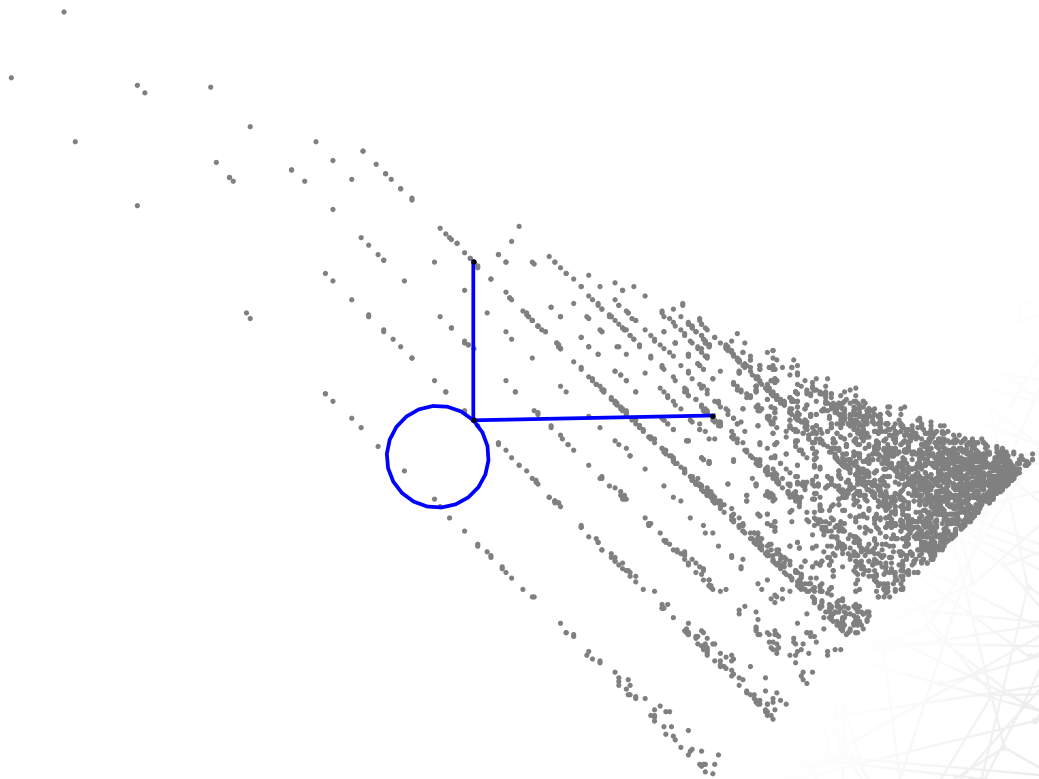
Which points are connected by isogenies?

Image of $\mathcal{G}(p, 2)$:



Which points are connected by isogenies?

Image of $\mathcal{G}(p, 2)$:



Which points are connected by isogenies?

Which points are connected by isogenies?

Each 2-isogeny corresponds to a pair $\mathcal{O}, \mathcal{O}'$ with a common index 2 sublattice.

Which points are connected by isogenies?

Each 2-isogeny corresponds to a pair $\mathcal{O}, \mathcal{O}'$ with a common index 2 sublattice.

In moving from $\mathcal{O}$ to $\mathcal{O}'$:

- β_1 could be replaced with $2\beta_1$ or $\frac{1}{2}\beta_1$;
- β_2 could be replaced with $2\beta_2$ or $\frac{1}{2}\beta_2$;

Which points are connected by isogenies?

Each 2-isogeny corresponds to a pair $\mathcal{O}, \mathcal{O}'$ with a common index 2 sublattice.

In moving from $\mathcal{O}$ to $\mathcal{O}'$:

- β_1 could be replaced with $2\beta_1$ or $\frac{1}{2}\beta_1$;
- β_2 could be replaced with $2\beta_2$ or $\frac{1}{2}\beta_2$;
- Other changes are possible, but D_1, D_2 never change by more than a factor of 2.

Which points are connected by isogenies?

Each 2-isogeny corresponds to a pair $\mathcal{O}, \mathcal{O}'$ with a common index 2 sublattice.

In moving from $\mathcal{O}$ to $\mathcal{O}'$:

- β_1 could be replaced with $2\beta_1$ or $\frac{1}{2}\beta_1$;
- β_2 could be replaced with $2\beta_2$ or $\frac{1}{2}\beta_2$;
- Other changes are possible, but D_1, D_2 never change by more than a factor of 2.

The distance between 2-isogenous vertices is bounded above by $\sqrt{2}\log 2$.

Which points are connected by isogenies?

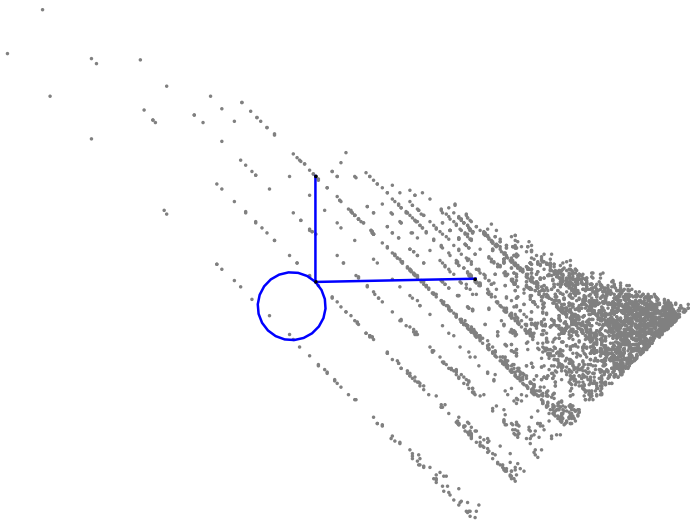
Each 2-isogeny corresponds to a pair $\mathcal{O}, \mathcal{O}'$ with a common index 2 sublattice.

In moving from $\mathcal{O}$ to $\mathcal{O}'$:

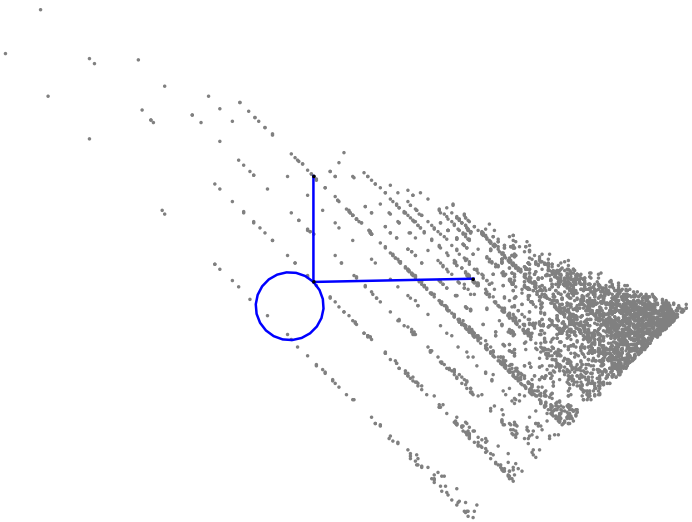
- β_1 could be replaced with $2\beta_1$ or $\frac{1}{2}\beta_1$;
- β_2 could be replaced with $2\beta_2$ or $\frac{1}{2}\beta_2$;
- Other changes are possible, but D_1, D_2 never change by more than a factor of 2.

The distance between 2-isogenous vertices is bounded above by $\sqrt{2}\log 2$.
Graph neighbors are close in successive minima space.

Which points are connected by isogenies?



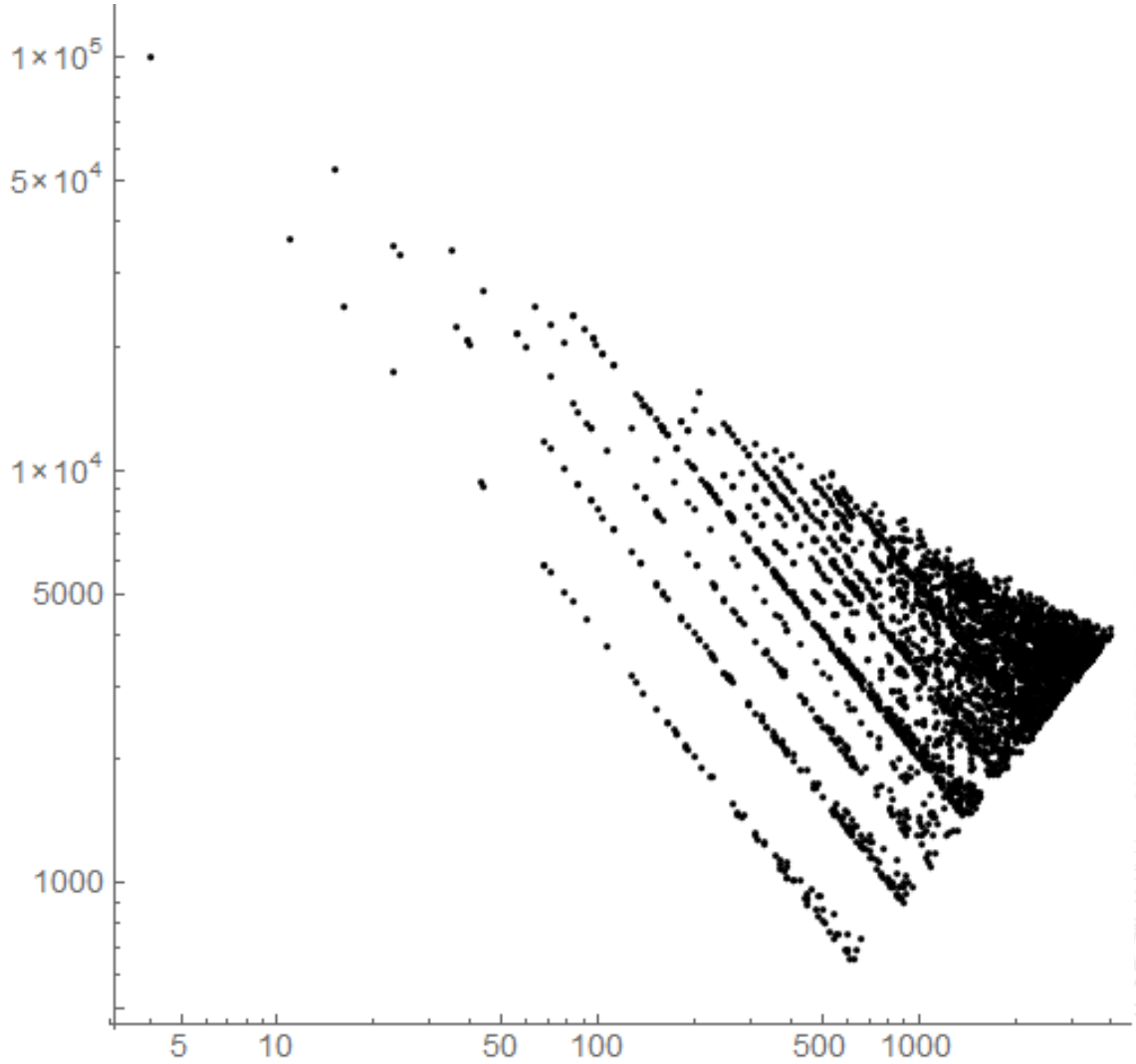
Which points are connected by isogenies?



$(207, 3895, 50248)$ (attained by $\beta_1, \beta_2, \beta_3$) has 2-isogenies to

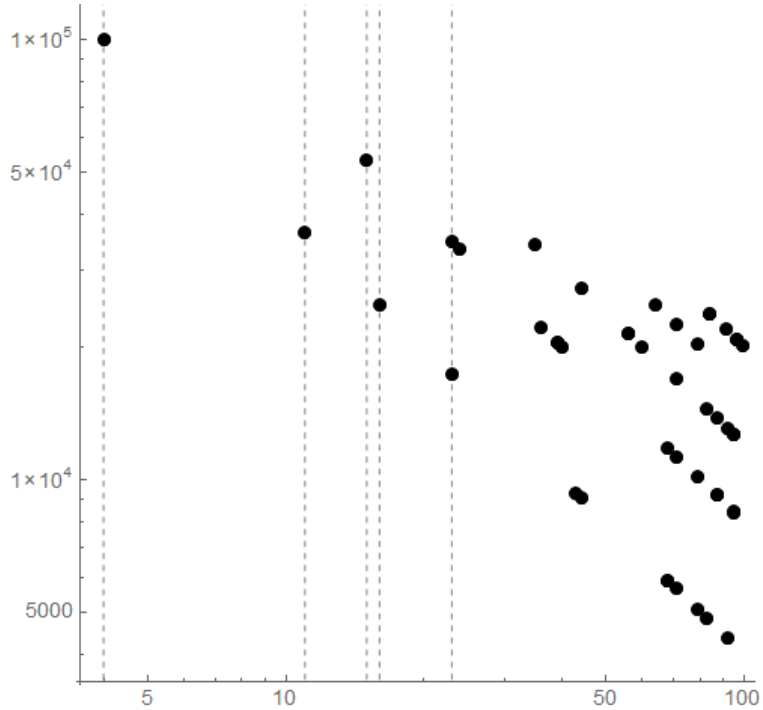
- itself (actually $E \to E^{(p)}$)
- $(828, 3895, 13055)$ (β_2 preserved)
- $(207, 15471, 15503)$ (β_1 preserved)

What do the sparse points represent?



What do the sparse points represent?

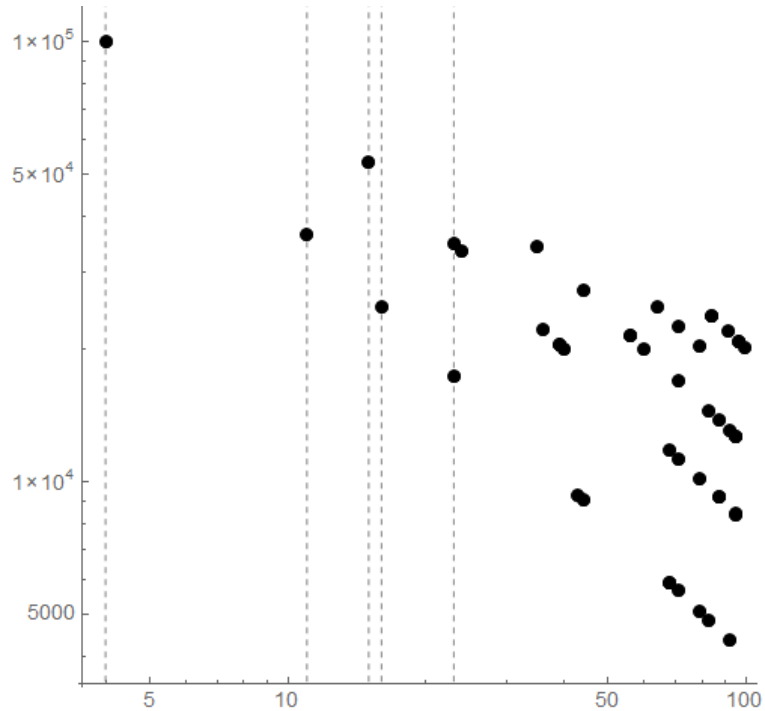
Vertices on a vertical line at $D_1 = D$ represent maximal orders $\mathcal{O}$ with an *optimal embedding* $\mathbb{Z}[\frac{D+\sqrt{-D}}{2}] \hookrightarrow \mathcal{O}$.



$D_1 = 4, 11, 15, 16, 23$:

What do the sparse points represent?

Vertices on a vertical line at $D_1 = D$ represent maximal orders $\mathcal{O}$ with an *optimal embedding* $\mathbb{Z}[\frac{D+\sqrt{-D}}{2}] \hookrightarrow \mathcal{O}$.



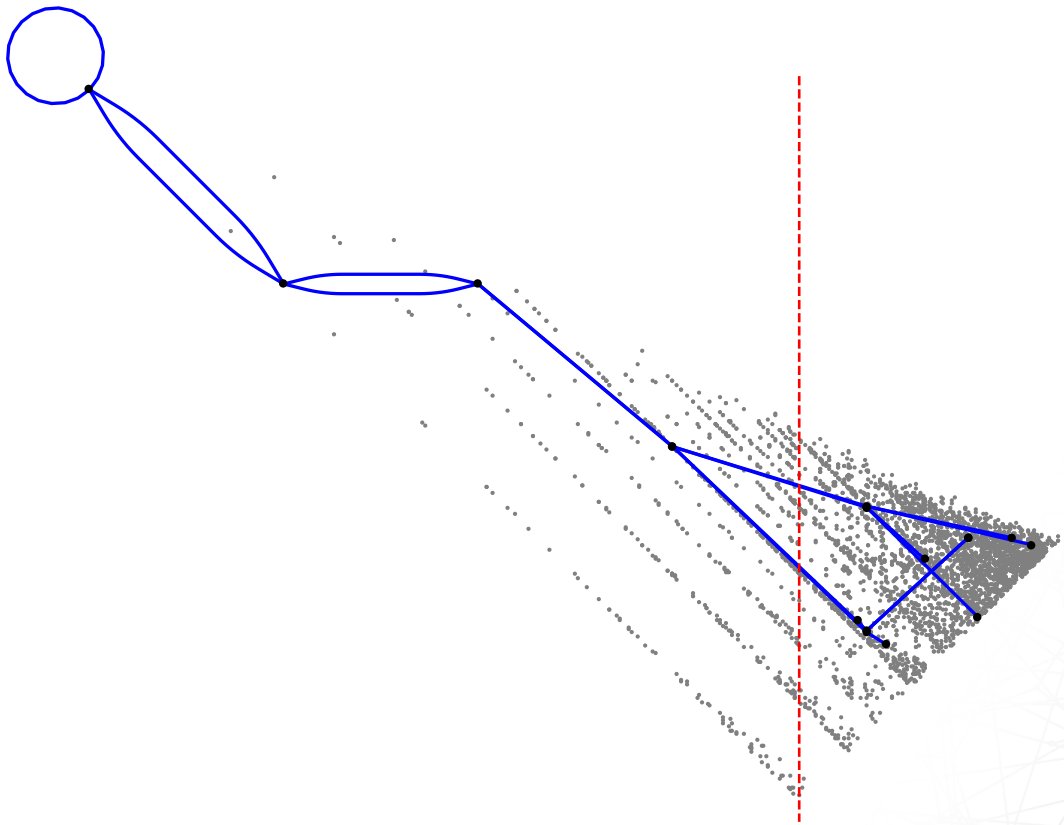
$D_1 = 4, 11, 15, 16, 23$:
$\mathbb{Z}[i]$, $\mathbb{Z}[\frac{1+\sqrt{-11}}{2}]$, $\mathbb{Z}[\frac{1+\sqrt{-15}}{2}]$, $\mathbb{Z}[2i]$, $\mathbb{Z}[\frac{1+\sqrt{-23}}{2}]$.

What do the sparse points represent?

Which "sparse points" are connected by 2-isogenies?

What do the sparse points represent?

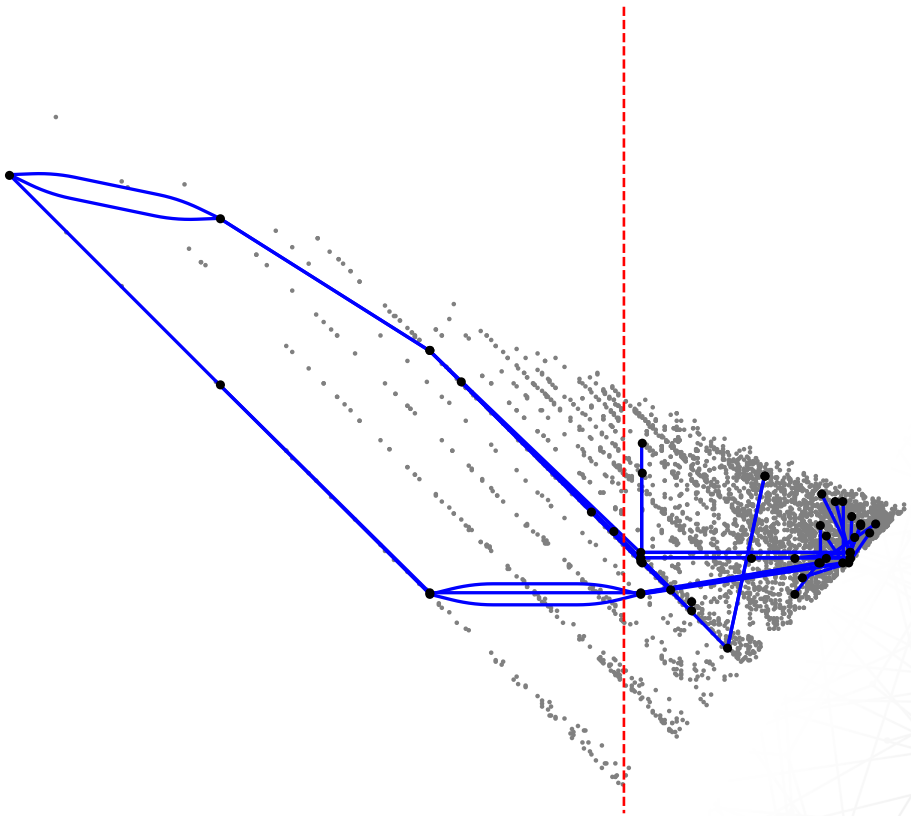
Which "sparse points" are connected by 2-isogenies?
5 steps from $(4, 100003, 100004)$:



(Red line: $D_1 = 2\sqrt{p}$)
$(4, 100003)$, $(16, 25003)$, $(64, 25007)$, $(256, 7839)$, $(256, 7860)$,...

What do the sparse points represent?

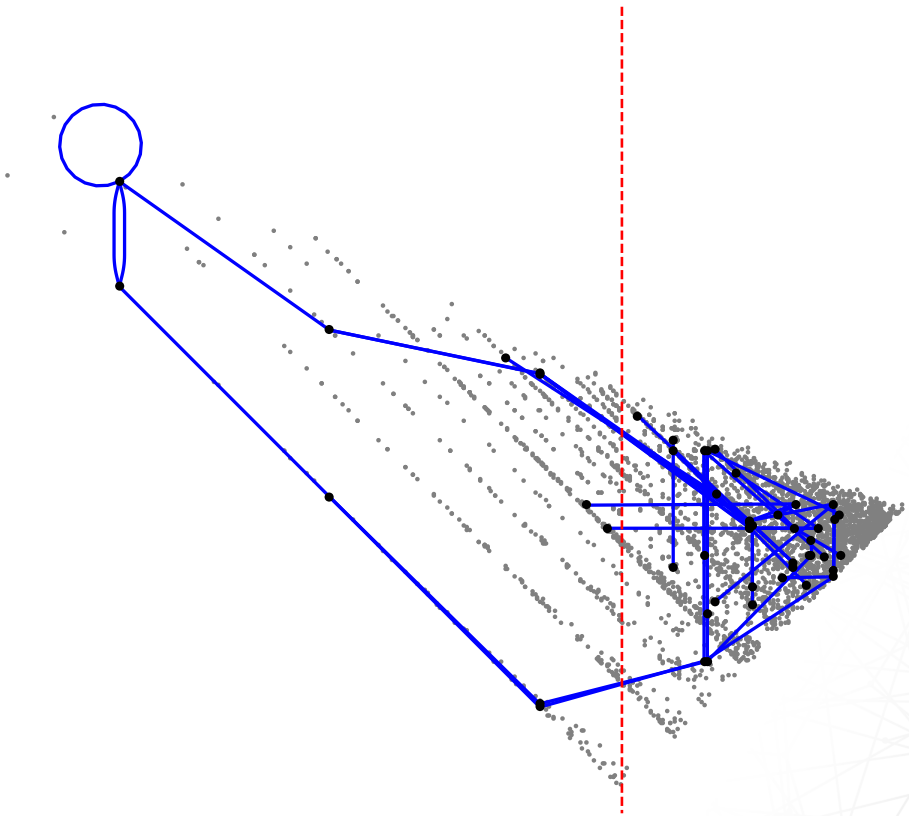
Which "sparse points" are connected by 2-isogenies?
5 steps from $(11, 36367, 109095)$:



(Red line: $D_1 = 2\sqrt{p}$)
$(11, 36367)$, $(44, 9092)$, $(44, 27275)$, $(176, 2311)$, $(176, 2287)\ldots$

What do the sparse points represent?

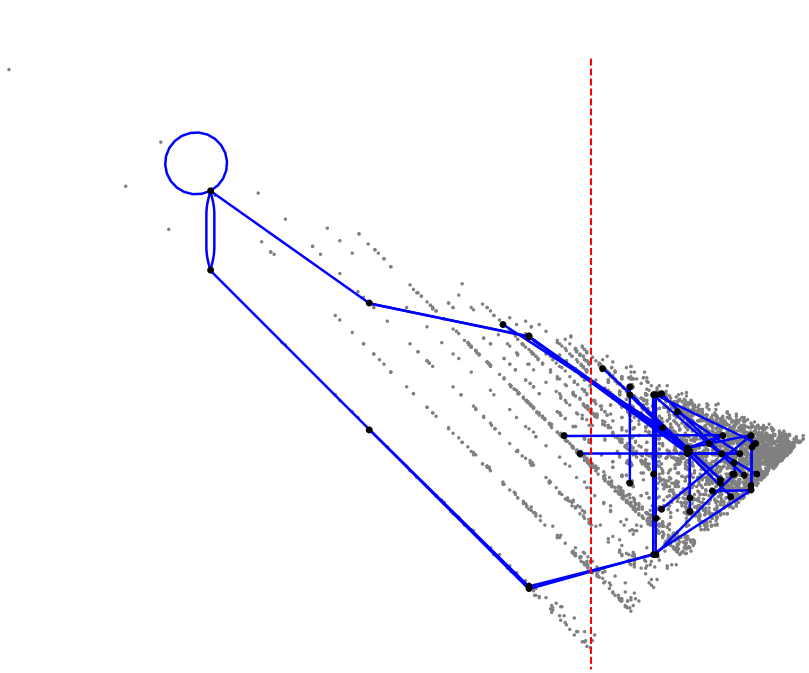
Which "sparse points" are connected by 2-isogenies?
5 steps from $(23, 17392, 104351)$ or $(23, 34788, 52179)$:

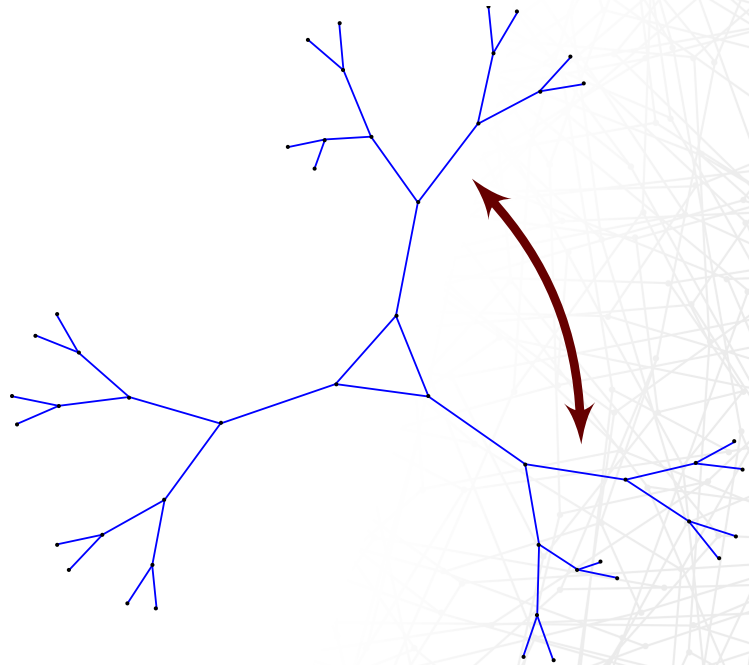


(Red line: $D_1 = 2\sqrt{p}$)
$(23, 17392)$, $(23, 34788)$, $(92, 4348)$, $(92, 13055)$, $(368, 1087)\ldots$

What do the sparse points represent?

5 steps from $(23, 17392, 104351)$ or $(23, 34788, 52179)$





(Red line: $D_1 = 2\sqrt{p}$)

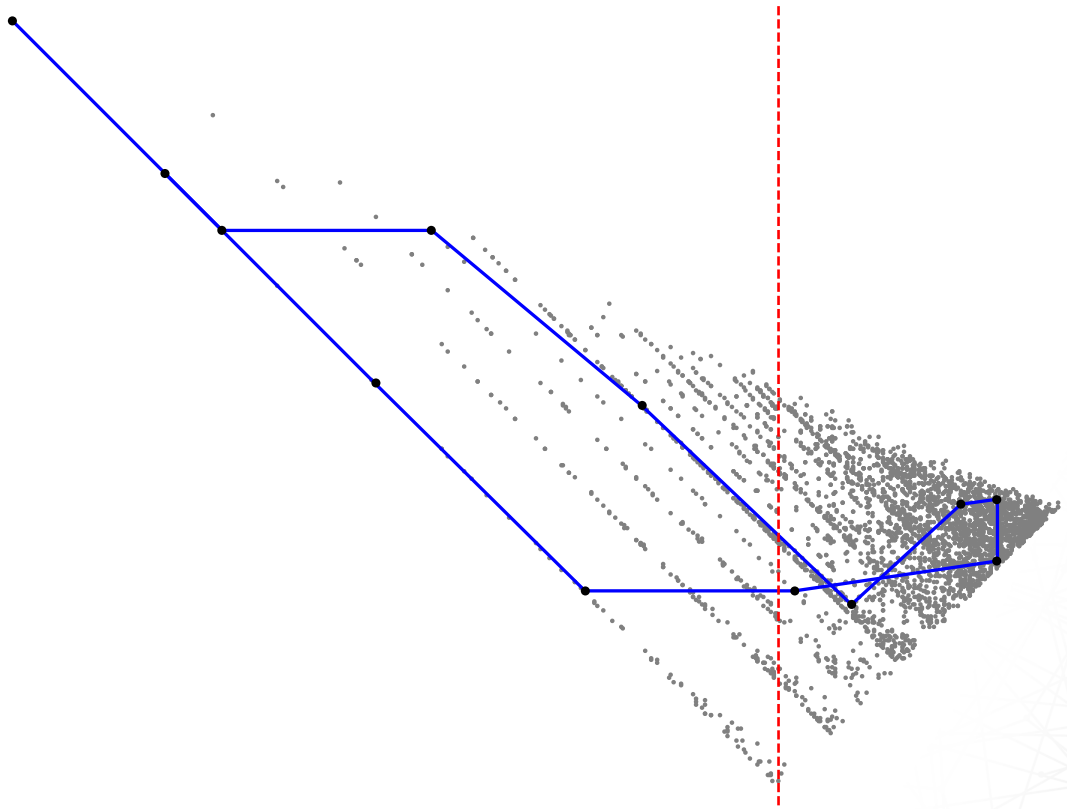
Each of these is an *isogeny volcano* (glued along Frobenius).

Points on the same vertical line have the same *level* (same optimally embedded quadratic order).

No backtracking until after crossing the red line.

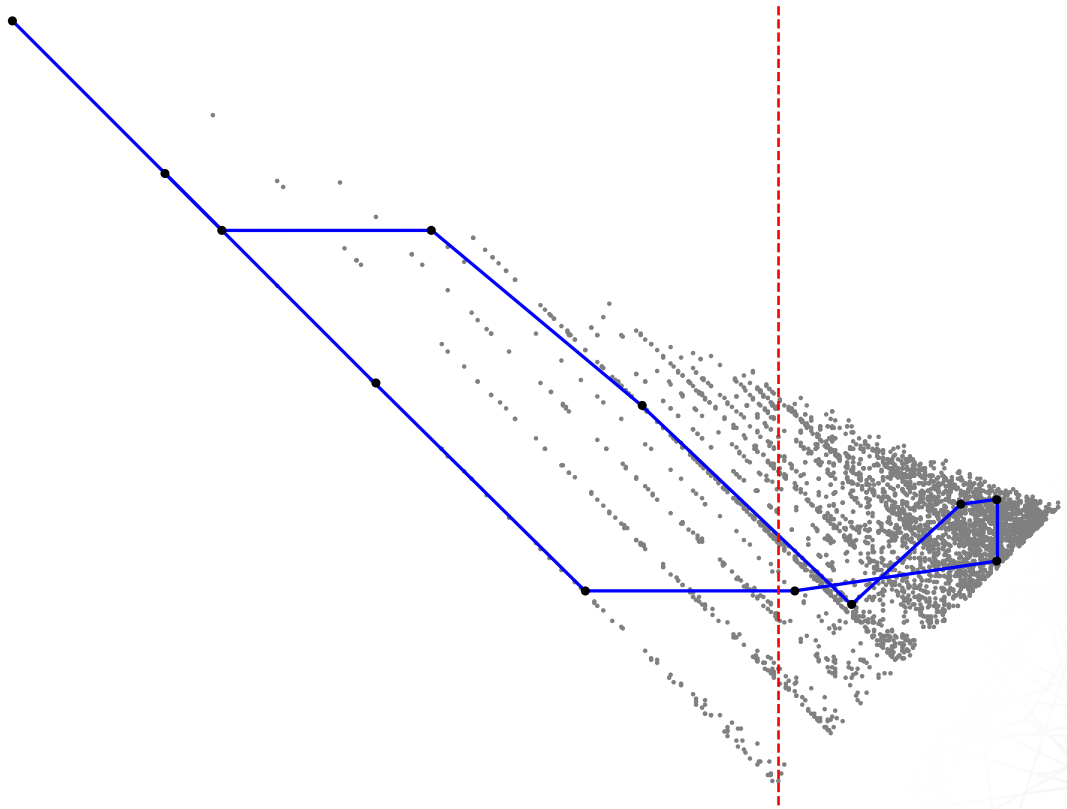
What do the sparse points represent?

Shortest path from $(4, 100003, 100004)$ to $(11, 36367, 109095)$:



What do the sparse points represent?

Shortest path from $(4, 100003, 100004)$ to $(11, 36367, 109095)$:



A path to a different volcano must descend into the depths of the isogeny graph.

What do the sparse points represent?

Take M such that $4M \ll 2\sqrt{p}$.

Theorem (L–Boneh '20)

The supersingular curves with $D_1 \leq 4M$ partition into sets T_D, for fundamental discriminants $-4M \leq D < 0$ with $\left(\frac{D}{p}\right) = -1$.

What do the sparse points represent?

Take M such that $4M \ll 2\sqrt{p}$.

Theorem (L–Boneh '20)

The supersingular curves with $D_1 \leq 4M$ partition into sets T_D, for fundamental discriminants $-4M \leq D < 0$ with $\left(\frac{D}{p}\right) = -1$.

- Any $E, E' \in T_D$ can be linked[a] by a sequence of isogenies between elements of T_D, each of degree at most $\frac{4}{\pi}\sqrt{M}$ (small!).

What do the sparse points represent?

Take M such that $4M \ll 2\sqrt{p}$.

Theorem (L–Boneh '20)

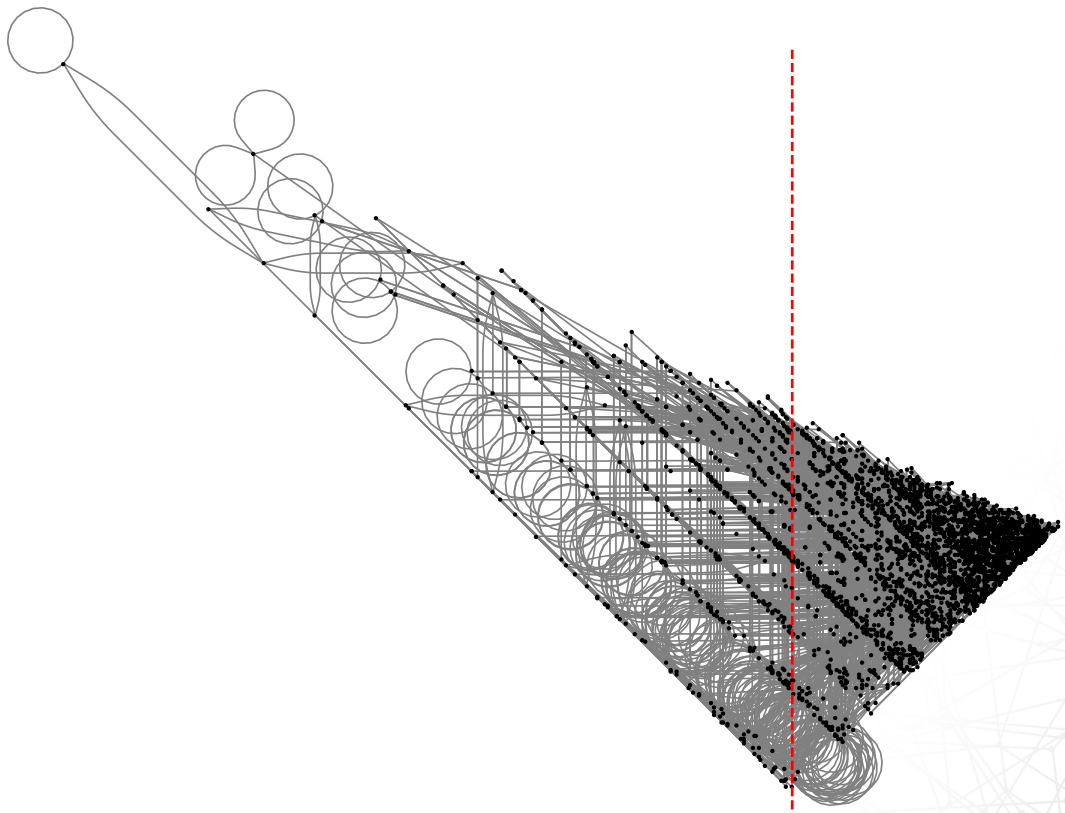
The supersingular curves with $D_1 \leq 4M$ partition into sets T_D, for fundamental discriminants $-4M \leq D < 0$ with $\left(\frac{D}{p}\right) = -1$.

- Any $E, E' \in T_D$ can be linked[a] by a sequence of isogenies between elements of T_D, each of degree at most $\frac{4}{\pi}\sqrt{M}$ (small!).
- If $E \in T_D$ and $E' \in T_{D'}$ with $D \neq D'$, any isogeny $E \to E'$ has degree at least $\frac{\sqrt{p}}{2M}$ (big!).

[a] Perhaps after replacing E by $E^{(p)}$

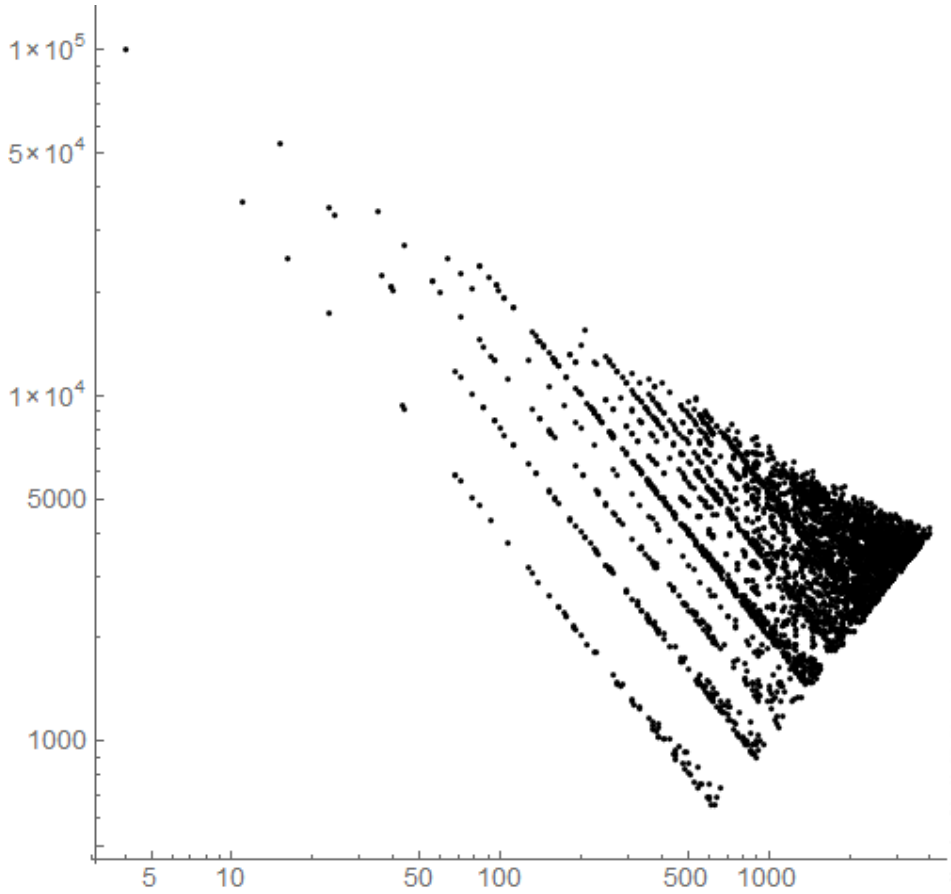
What do the sparse points represent?

The "sparse region" $D_1 < 2\sqrt{p}$ is a **disjoint union of isogeny volcanoes** (*oriented* isogeny graphs). These only meet in the "dense region" $D_1 > 2\sqrt{p}$.



What are the stripes?

What are the stripes?



What are the stripes?

The “rigidity law” for Gross lattices:

What are the stripes?

The "rigidity law" for Gross lattices:

Proposition (Kaneko '89)

Let $\mathcal{O}$ be a maximal order in $B_{p,\infty}$, and let β_1, β_2 be linearly independent elements of the Gross lattice. Then

$$\det\langle \beta_1, \beta_2 \rangle = N(\beta_1)N(\beta_2) - \frac{1}{4}\operatorname{Tr}(\beta_1\overline{\beta_2})^2 \tag{1}$$

is a positive integer multiple of $4p$.

What are the stripes?

The "rigidity law" for Gross lattices:

Proposition (Kaneko '89)

Let $\mathcal{O}$ be a maximal order in $B_{p,\infty}$, and let β_1, β_2 be linearly independent elements of the Gross lattice. Then

$$\det\langle \beta_1, \beta_2 \rangle = N(\beta_1)N(\beta_2) - \frac{1}{4}\operatorname{Tr}(\beta_1\overline{\beta_2})^2 \tag{1}$$

is a positive integer multiple of $4p$.

For any parallelogram in $\mathcal{O}^T$, its squared area is a multiple of $4p$.

What are the stripes?

The "rigidity law" for Gross lattices:

Proposition (Kaneko '89)

Let $\mathcal{O}$ be a maximal order in $B_{p,\infty}$, and let β_1, β_2 be linearly independent elements of the Gross lattice. Then

$$\det\langle \beta_1, \beta_2 \rangle = N(\beta_1)N(\beta_2) - \frac{1}{4}\operatorname{Tr}(\beta_1\overline{\beta_2})^2 \tag{1}$$

is a positive integer multiple of $4p$.

For any parallelogram in $\mathcal{O}^T$, its squared area is a multiple of $4p$.

This result is used to prove that successive minima of $\mathcal{O}^T$ determine $\mathcal{O}$ (Goren–L '24): we can recover *angle information* from knowledge of norms.

What are the stripes?

Proof idea: consider the lattice $L := \langle 1, \beta_1, \beta_2, \beta_1\beta_2 \rangle$.[1]

[1] To get the full result we actually need a slightly larger lattice

What are the stripes?

Proof idea: consider the lattice $L := \langle 1, \beta_1, \beta_2, \beta_1\beta_2 \rangle$.[1]

- L, a sublattice of $\mathcal{O}$, has determinant an integer multiple of $\frac{1}{16}p^2$.

[1] To get the full result we actually need a slightly larger lattice

What are the stripes?

Proof idea: consider the lattice $L := \langle 1, \beta_1, \beta_2, \beta_1\beta_2 \rangle$.[1]

- L, a sublattice of $\mathcal{O}$, has determinant an integer multiple of $\frac{1}{16}p^2$.
- The determinant can be computed explicitly in terms of the determinant of the 2-d lattice $\langle \beta_1, \beta_2 \rangle$.

[1] To get the full result we actually need a slightly larger lattice

What are the stripes?

What are the stripes?

If β_1, β_2 attain first two successive minima, they must be close to orthogonal:

$$\begin{aligned} N(\beta_2 \pm \beta_1) \geq N(\beta_2) &\Rightarrow \pm \operatorname{Tr}(\beta_1 \overline{\beta_2}) + N(\beta_1) \geq 0 \\ &\Rightarrow N(\beta_1) \geq |\operatorname{Tr}(\beta_1 \overline{\beta_2})|. \end{aligned}$$

So for $D_1 \ll \sqrt{p}$, $\operatorname{Tr}(\beta_1 \overline{\beta_2})^2 \ll p$.

What are the stripes?

If β_1, β_2 attain first two successive minima, they must be close to orthogonal:

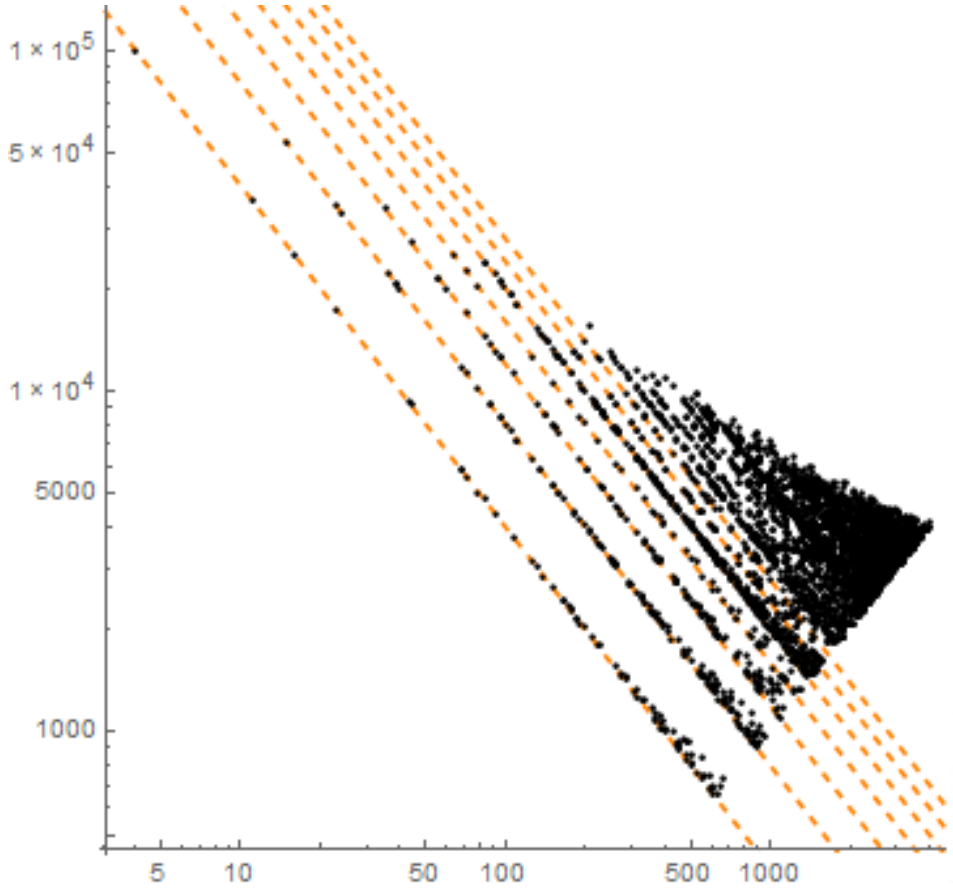
$$N(\beta_2 \pm \beta_1) \geq N(\beta_2) \Rightarrow \pm \operatorname{Tr}(\beta_1 \overline{\beta_2}) + N(\beta_1) \geq 0$$
$$\Rightarrow N(\beta_1) \geq |\operatorname{Tr}(\beta_1 \overline{\beta_2})|.$$

So for $D_1 \ll \sqrt{p}$, $\operatorname{Tr}(\beta_1 \overline{\beta_2})^2 \ll p$. Since

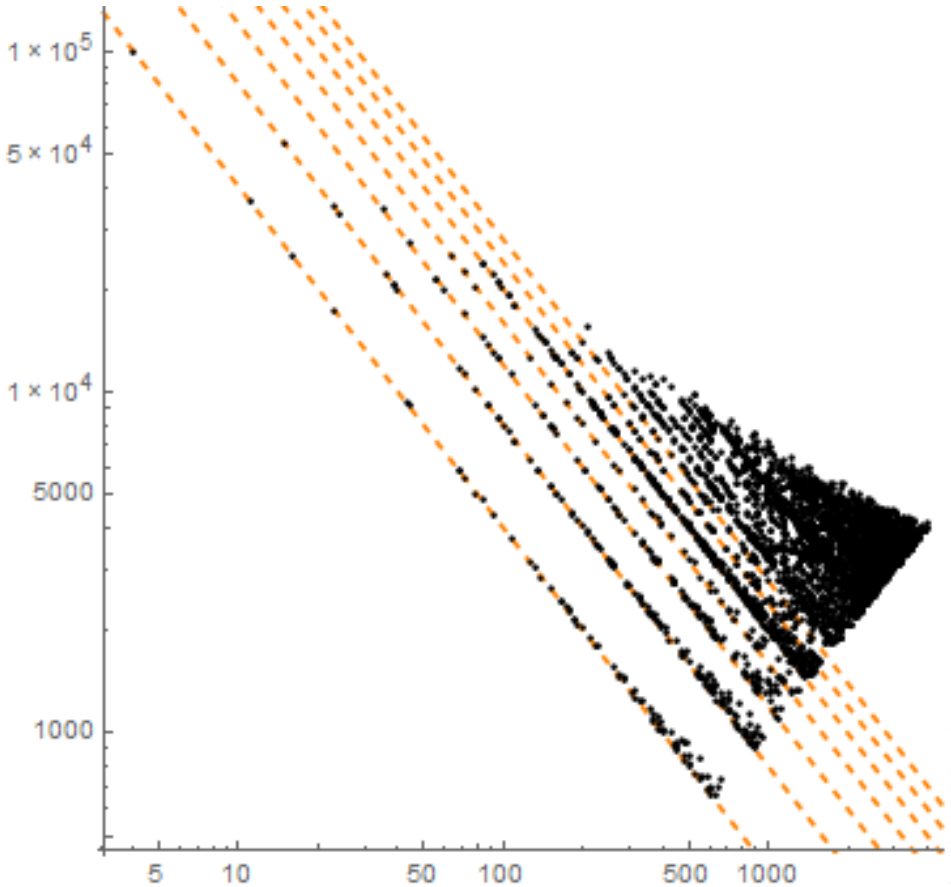
$$D_1 D_2 - \frac{1}{4} \operatorname{Tr}(\beta_1 \overline{\beta_2})^2$$

is a multiple of $4p$, $D_1 D_2$ is equal to, or just barely greater than, a multiple of $4p$.

What are the stripes?



What are the stripes?



$D_2 = \frac{4pn}{D_1}$ for $n = 1, 2, 3, \ldots$

What are the stripes?

Supersingular elliptic curves are defined over $\mathbb{F}_{p^2}$. The subgraph induced by those curves defined over $\mathbb{F}_p$ is called the spine of the supersingular isogeny graph.[2]

[2] Arpin–Camacho-Navarro–Lauter–Lim–Nelson–Scholl–Sotáková '21, *Adventures in Supersingularland*

What are the stripes?

Assume $p \geq 37$.

What are the stripes?

Assume $p \geq 37$.

Theorem (He–Korpal–Tran–Vincent '25+)

Let $E/\mathbb{F}_{p^2}$ be a supersingular elliptic curve. If E is defined over $\mathbb{F}_p$:

- $\mathcal{O}^T$ contains a rank 2 sublattice of discriminant $4p$
- D_3 is large ($p \leq D_3 \leq \frac{8}{7}p + \frac{7}{4}$)

What are the stripes?

Assume $p \geq 37$.

Theorem (He–Korpal–Tran–Vincent '25+)

Let $E/\mathbb{F}_{p^2}$ be a supersingular elliptic curve. If E is defined over $\mathbb{F}_p$:

- $\mathcal{O}^T$ contains a rank 2 sublattice of discriminant $4p$
- D_3 is large ($p \leq D_3 \leq \frac{8}{7}p + \frac{7}{4}$)

If E is *not* defined over $\mathbb{F}_p$:

- every rank 2 sublattice of $\mathcal{O}^T$ has discriminant $\geq 8p$;
- D_3 is small ($D_3 \leq \frac{3}{5}p + 5$).

What are the stripes?

Assume $p \geq 37$.

Theorem (He–Korpal–Tran–Vincent '25+)

Let $E/\mathbb{F}_{p^2}$ be a supersingular elliptic curve. If E is defined over $\mathbb{F}_p$:

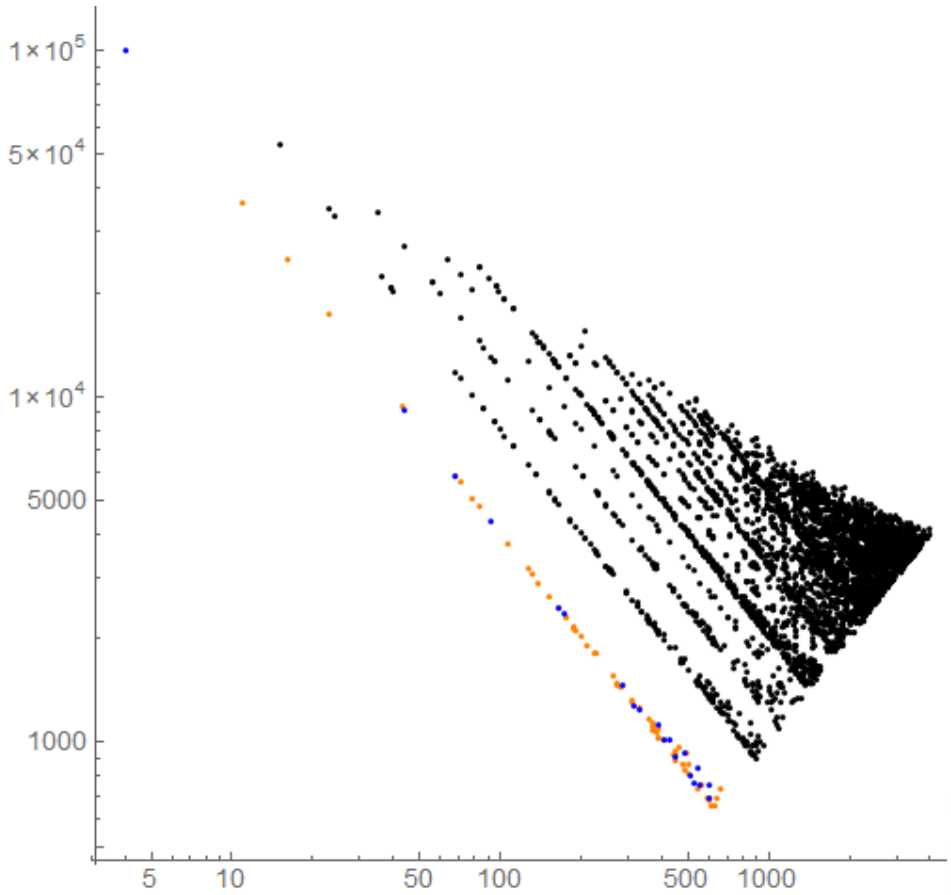
- $\mathcal{O}^T$ contains a rank 2 sublattice of discriminant $4p$
- D_3 is large ($p \leq D_3 \leq \frac{8}{7}p + \frac{7}{4}$)

If E is *not* defined over $\mathbb{F}_p$:

- every rank 2 sublattice of $\mathcal{O}^T$ has discriminant $\geq 8p$;
- D_3 is small ($D_3 \leq \frac{3}{5}p + 5$).

There is a "gap" beteen the spine and the rest of the isogeny graph.

What are the stripes?



- Blue: $\mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$ optimally embedded in $\mathrm{End}(E)$ $(E/\mathbb{F}_p)$.
- Orange: $\mathbb{Z}[\sqrt{-p}]$ optimally embedded in $\mathrm{End}(E)$ $(E/\mathbb{F}_p)$.
- Black: E not defined over $\mathbb{F}_p$.

What are the stripes?

Comparing two recent results:

What are the stripes?

Comparing two recent results:

- Eli Orvis ('24): Short cycles in $\mathcal{G}(p, \ell)$ are disproportionately likely to occur along the spine.

What are the stripes?

Comparing two recent results:

- Eli Orvis ('24): Short cycles in $\mathcal{G}(p, \ell)$ are disproportionately likely to occur along the spine.
- He–Korpal–Tran–Vincent ('25): For E along the spine, $\mathrm{End}(E)^T$ has rank 2 sublattices with determinant as small as possible.
  Endomorphisms of E are more "tightly packed" than usual.

What are the stripes?

Comparing two recent results:

- Eli Orvis ('24): Short cycles in $\mathcal{G}(p, \ell)$ are disproportionately likely to occur along the spine.
- He–Korpal–Tran–Vincent ('25): For E along the spine, $\mathrm{End}(E)^T$ has rank 2 sublattices with determinant as small as possible. Endomorphisms of E are more "tightly packed" than usual.

Both say that the spine has more small-degree endomorphisms than average. *Can we use either of these results to prove the other?*

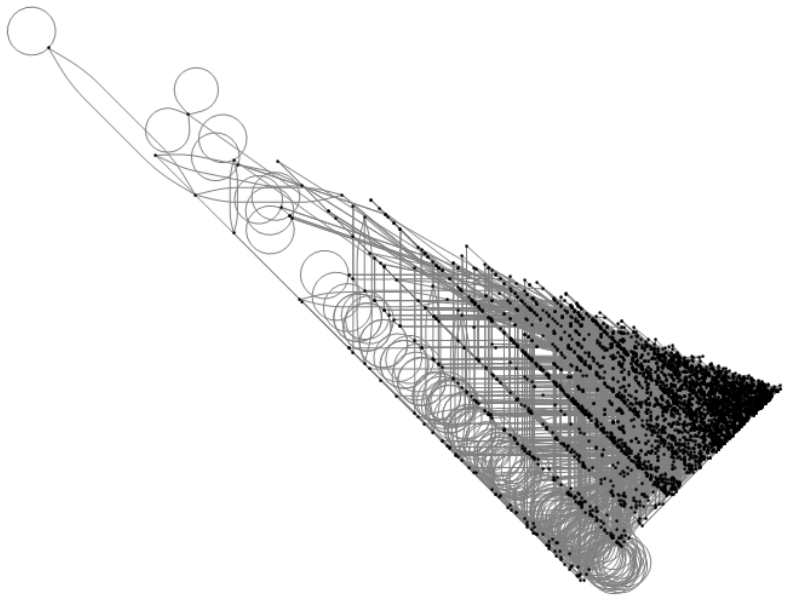
Summary: Plotting $\mathcal{G}(p, \ell)$ according to (D_1, D_2) allows us to identify special features.

- Points lie in a consistently-shaped zone, regardless of p;
- Sparse zone (to the left) captures curves with small non-integer endomorphisms (D_1 small);
- Curves over $\mathbb{F}_p$ occur as the bottom stripe ($D_1 D_2$ small);
- ℓ–isogenous curves are close to each other.

Open questions

Open questions

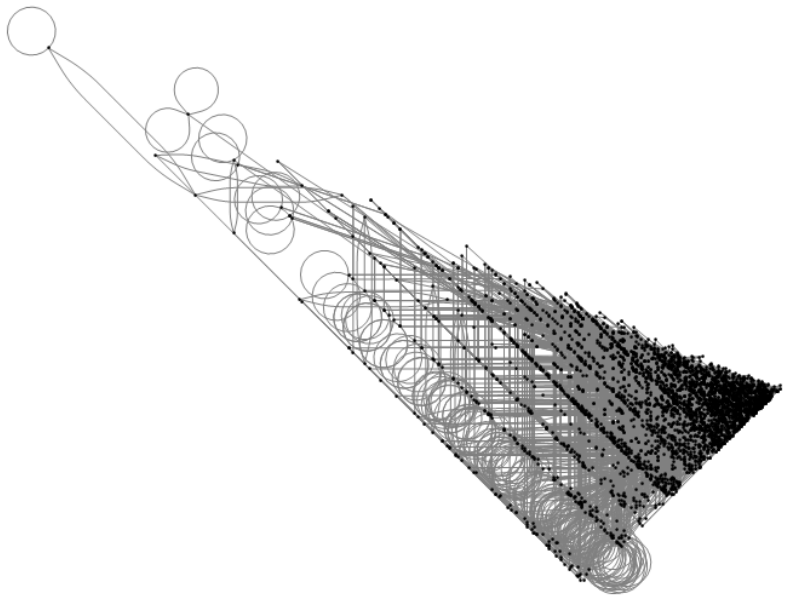
Image of $\mathcal{G}(p, 2)$:



- First stripe: defined over $\mathbb{F}_p$ ($E \to E^{(p)}$ of degree 1)
- Second stripe: $E \to E^{(p)}$ of degree 2

Open questions

Image of $\mathcal{G}(p, 2)$:



- First stripe: defined over $\mathbb{F}_p$ ($E \to E^{(p)}$ of degree 1)
- Second stripe: $E \to E^{(p)}$ of degree 2

Question

Does there exist an isogeny $E \to E^{(p)}$ of degree ℓ if and only if $\mathrm{End}(E)^T$ has a rank 2 sublattice of determinant $4\ell p$?

Open questions

Open questions

Question

Is it possible to take advantage of any of these structures without already knowing $\mathrm{End}(E)$?

Open questions

Question

Is it possible to take advantage of any of these structures without already knowing $\mathrm{End}(E)$?

Some of them, yes: e.g. there is a polynomial time algorithm to detect existence of small non-integer endomorphisms if they exist, and then to compute endomorphism ring (L–Boneh '20). What about other features?

Open questions

Question

Is it possible to take advantage of any of these structures without already knowing $\mathrm{End}(E)$?

Some of them, yes: e.g. there is a polynomial time algorithm to detect existence of small non-integer endomorphisms if they exist, and then to compute endomorphism ring (L–Boneh '20). What about other features?

Question

Is there a simple criterion to determine whether D_1, D_2, D_3 are the successive minima of $\mathrm{End}(E)^T$ for some supersingular E?

Open questions

Question

Is it possible to take advantage of any of these structures without already knowing $\mathrm{End}(E)$?

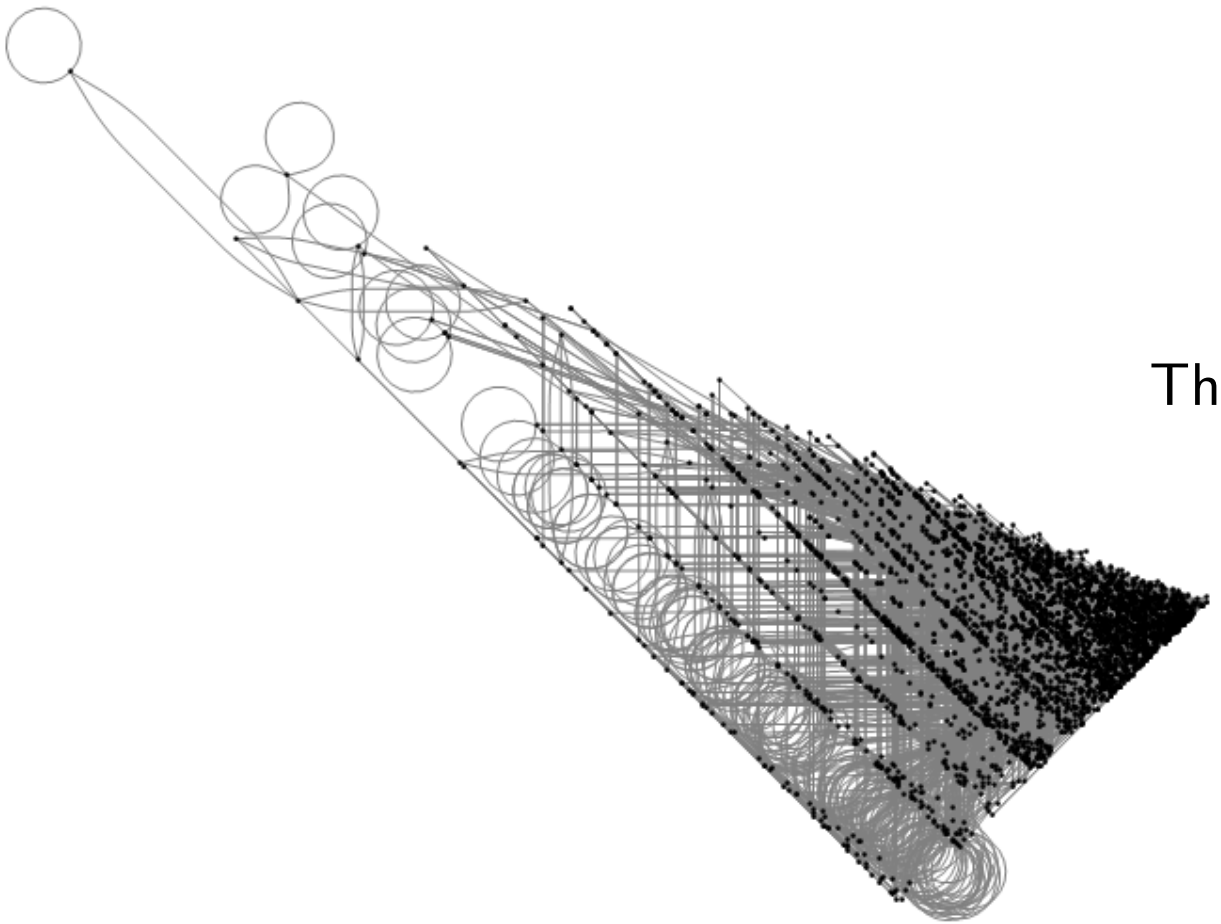
Some of them, yes: e.g. there is a polynomial time algorithm to detect existence of small non-integer endomorphisms if they exist, and then to compute endomorphism ring (L–Boneh '20). What about other features?

Question

Is there a simple criterion to determine whether D_1, D_2, D_3 are the successive minima of $\mathrm{End}(E)^T$ for some supersingular E?

Question

To what extent can this picture be generalized to higher-dimensional isogeny graphs?



Thank you for listening!