Computing endomorphism rings of supersingular elliptic curves

Travis Morrison

Institute for Quantum Computing, University of Waterloo

ANTS 2020

joint work with Eisenträger, Hallgren, Leonardi, and Park

Supersingular elliptic curves

Let E be an elliptic curve over $\mathbb{F}_q$. Then $\mathrm{End}(E)$ either has rank 2 or 4 as a $\mathbb{Z}$-module.

Definition

If $\mathrm{End}(E)$ is rank 2, E is called ordinary. If $\mathrm{End}(E)$ is rank 4, E is supersingular.

- If E is ordinary, then $\mathrm{End}(E) \otimes \mathbb{Q}$ is isomorphic to an imaginary quadratic field.
- If E is supersingular, then $\mathrm{End}(E) \otimes \mathbb{Q}$ is a quaternion algebra ramified at p and ∞. Moreover, $\mathrm{End}(E)$ is a maximal order in $\mathrm{End}(E) \otimes \mathbb{Q}$.

Computing the endomorphism ring of an elliptic curve

- Suppose $E/\mathbb{F}_q$ is ordinary and let π denote the Frobenius endomorphism.

$$\mathbb{Z}[\pi] \subseteq \mathrm{End}(E) \subseteq \mathcal{O}_{\mathbb{Q}(\pi)}$$

- Kohel 1996: $O(q^{1/3+\epsilon})$ algorithm
- Bisson-Sutherland 2009: subexponential algorithm
- When $E/\mathbb{F}_q$ is supersingular, there are (in general) no obvious quadratic orders $\mathbb{Z}[\alpha]$ which embed into $\mathrm{End}(E)$
- Moreover, $\mathrm{End}(E)$ is rank 4 as a $\mathbb{Z}$-module, so computing $\mathrm{End}(E)$ will be very different in the supersingular case

Connection to isogeny-based cryptography

An efficient algorithm for computing $\mathrm{End}(E)$ for supersingular E would break many isogeny-based cryptosystems

- The hash function of Charles-Goren-Lauter and de Feo, Jao, and Plût's SIDH
  - Kohel-Lauter-Petit-Tignol 2014, Galbraith-Petit-Shani-Ti 2016, Eisenträger-Hallgren-Lauter-Morrison-Petit 2018
- practical instantiations of Castryck-Lange-Martindale-Panny-Renes's CSIDH
  - Castryck-Panny-Vercauteren 2019

Computing the endomorphism ring of a supersingular elliptic curve

Theorem (Eisenträger-Hallgren-Leonardi-M-Park 2020)

Assuming several heuristics (including GRH), there is a $O(p^{1/2}(\log p)^2)$ time algorithm for computing the endomorphism ring of a supersingular elliptic curve.

Supersingular isogeny graphs

Definition

Let p, ℓ be distinct primes. Then $G(p, \ell)$ is the graph with

- Vertices: the isomorphism classes of supersingular elliptic curves
- Edges: one edge from E to E' for each ℓ-isogeny $\phi : E \to E'$ of degree ℓ.

Properties of $G(p, \ell)$

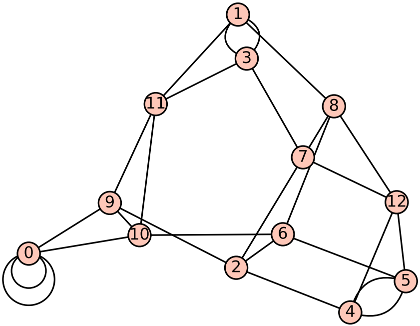


Figure: $G(157, 3)$

- $G(p, \ell)$ has roughly $p/12$ vertices
  - this is the number of supersingular j-invariants in $\overline{\mathbb{F}_p}$
- $G(p, \ell)$ is $\ell + 1$-regular
  - one outgoing edge for each of the $\ell + 1$ cyclic subgroups of $E[\ell]$
- $G(p, \ell)$ is connected, with diameter $O(\log p)$
- In fact, $G(p, \ell)$ is a Ramanujan graph ('rapid mixing')

Quaternionic orders from cycles in $G(p, \ell)$

- Compose the isogenies along a cycle starting at E to get an an endomorphism of E

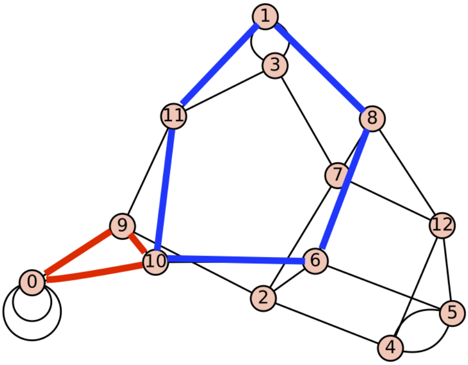


Figure: $\langle 1, \alpha, \beta, \alpha\beta \rangle$ is rank 4.

Computing endomorphisms using cycles in $G(p, \ell)$

Theorem (Kohel 1996)

There is a $\tilde{O}(p^{1+\epsilon})$ algorithm to compute a sub order $\Lambda = \langle 1, \alpha, \beta, \alpha\beta \rangle \subseteq End(E)$, where $E/\mathbb{F}_{p^2}$ is supersingular.

- Idea: construct a spanning tree in $G(p, \ell)$. Then α, β arise from cycles in $G(p, \ell)$ which begin and end at E.
- Delfs-Galbraith, 2016: $\tilde{O}(p^{1/2})$ time algorithm for computing endomorphisms (but not a cycle in $G(p, \ell)$)

Computing the endomorphism ring of a supersingular elliptic curve

Theorem (Eisenträger-Hallgren-Leonardiy-M-Park 2020)

Assuming several heuristics (including GRH), there is a $O(p^{1/2}(\log p)^2)$ time algorithm for computing the endomorphism ring of a supersingular elliptic curve.

Steps:

1. Compute two cycles in $G(p, 2)$ to get a suborder $\Lambda \subseteq \mathrm{End}(E)$
2. For each prime $q \mid \mathrm{discrd}(\Lambda)$, enumerate the q-maximal orders containing $\Lambda \otimes \mathbb{Z}_q$
3. Combine local superorders to get maximal orders containing Λ, check each if it is isomorphic to $\mathrm{End}(E)$.

Comparison to previous work

- Previous work (Galbraith-Petit-Shani-Ti): compute cycles in $G(p, 2)$ at E until the cycles generate $\mathrm{End}(E)$. Heuristically, $O(\log p)$ many cycles are required.
- Our work: compute a nice enough suborder $\Lambda \subseteq \mathrm{End}(E)$, and then enumerate maximal orders containing it until finding $\mathrm{End}(E)$. Heuristically, we require a constant number of calls to a cycle finding algorithm, rather than $O(\log p)$ calls.

Step 1: computing a suborder of End(E)

Theorem (EHLMP 2020)

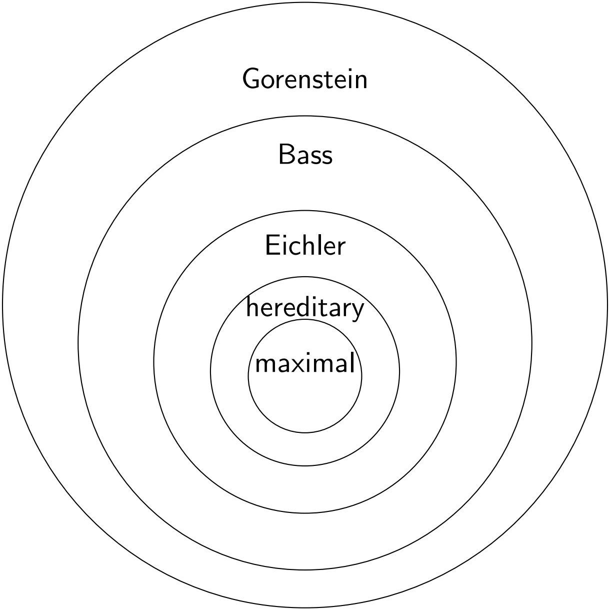
Assuming several heuristics (including GRH), there is a $O(p^{1/2}(\log p)^2)$ time (and poly $\log p$ storage) algorithm for computing two cycles in $G(p, \ell)$ which generate a suborder $\Lambda \subseteq End(E)$.

Using the geometry of $G(p,\ell)$ to compute cycles

$$\begin{tikzcd}
 & E_0 \arrow[dl] \arrow[dr] & \\
E_1' \arrow[d] & & E_1 \arrow[d] \\
(E_1')^{(p)} \arrow[ddr] & & E_2/\mathbb{F}_p \arrow[d] \\
 & & E_1^p \arrow[dl] \\
 & E_0^{(p)} &
\end{tikzcd}$$

- Given $E : y^2 = x^3 + ax + b$, define $E^{(p)}$ as $E^{(p)} : y^2 = x^3 + a^p x + b^p$.
- if E_1 is adjacent to E_2, then $E_1^{(p)}$ is adjacent to $E_2^{(p)}$ (Frobenius induces an automorphism of $G(p,\ell)$)
- Search for E defined over $\mathbb{F}_p$ (so $E^{(p)} = E$), or
- E such that E is adjacent to $E^{(p)}$
- This gives a $O((\log p)^2\sqrt{p})$ algorithm to compute a cycle in $G(p,\ell)$

A zoo of quaternionic orders



Enumerating local maximal superorders

For any order $\Lambda \subseteq M_2(\mathbb{Q}_q)$, the set of maximal orders containing Λ forms a subtree of the Bruhat-Tits tree. When Λ is Bass, this subtree is a path.

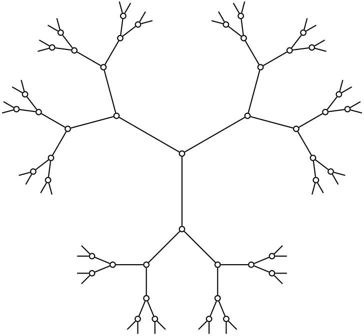


Figure: The 3-regular tree of maximal orders in $M_2(\mathbb{Q}_2)$

Enumerating global orders and finding $\mathrm{End}(E)$

Using knowledge of the local data $\{\Lambda' \supset \Lambda \otimes \mathbb{Z}_q : \Lambda' \text{ is maximal}\}$ for each prime $q \mid \mathrm{discrd}(\Lambda)$, and a local-global principle for quaternion orders, we can enumerate the global maximal orders containing Λ

$$\begin{tikzcd}
\mathcal{O}_1 & \mathcal{O}_2 & \mathrm{End}(E) & \cdots & \mathcal{O}_n \\
 & & \Lambda \arrow[ull] \arrow[ul] \arrow[u] \arrow[ur] \arrow[urr] & &
\end{tikzcd}$$

Given a maximal order $\mathcal{O}_i \supseteq \Lambda$, we can check if $\mathcal{O}_i \simeq \mathrm{End}(E)$ (Galbraith-Petit-Silva 2017).

Experimental data: how often is Λ Bass?

Given an order Λ in $B_{p,\infty}$ such that $\mathrm{discrd}(\Lambda) = p \prod_{i=1}^{m} q_i^{e_i}$, define $N(\Lambda) := \prod_{i=1}^{m}(e_i + 1)$. Then $N(\Lambda)$ is an upper bound on the number of maximal orders containing Λ.

p	orders	Bass orders	average $N(\Lambda)$
30,011	90	75	122.37
50,021	89	69	56.07
70,001	92	76	122.21
90,001	80	67	322.04
100,003	81	75	337.59

Figure: Results from computing 100 pairs of cycles in $G(p, 2)$ at random $j \in \mathbb{F}_{p^2} - \mathbb{F}_p$.

Number of maximal orders containing Λ