Adventures in Supersingularland: An Exploration of Supersingular Elliptic Curve Isogeny Graphs

Sarah Arpin
University of Colorado Boulder

Number Theory Series LA - Occidental College

October 26th, 2019

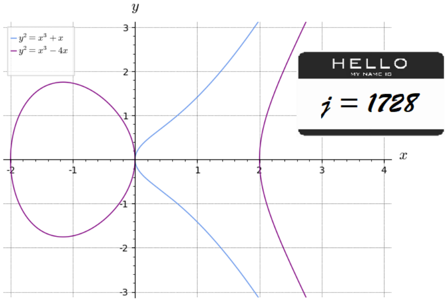
This is joint work with Catalina Camacho-Navarro, Kristin Lauter, Joelle Lim, Kristina Nelson, Travis Scholl, Jana Sotáková. [ACL$^+$19]

Overview

j-Invariants of Supersingular Elliptic Curves

Definition

For any elliptic curve E/K, j-**invariant** $j(E) \in K$ identifies E up to isomorphism over $\overline{K}$.



Isomorphism classes over $\mathbb{F}_{p^2}$: j-invariant uniquely identifies class
Isomorphism classes over $\mathbb{F}_p$: 2 classes of supersingular EC's per j-invariant

Isogenies

Definition

An **isogeny** $\phi : E_1 \to E_2$ is a group homomorphism of elliptic curves, which can be identified with (and computed from) its finite kernel.

Properties: [Sil09]

- The kernel of a nonzero isogeny is a finite group.
- The degree of an isogeny is equal to the size of the kernel.
- Every isogeny $\phi : E_1 \to E_2$ has a dual $\hat{\phi} : E_2 \to E_1$ of the same degree.
- ℓ: prime $\neq p$; there are $\ell + 1$ outgoing ℓ-isogenies from E

$\mathbb{F}_p$-Endomorphism Rings of Supersingular EC's

Theorem ([DG16])

For a supersingular elliptic curve E defined over $\mathbb{F}_p$, $End_{\mathbb{F}_p}(E)$ is an order in $\mathbb{Q}(\sqrt{-p})$ which contains $\mathbb{Z}[\sqrt{-p}]$.

$$\begin{array}{c} \mathcal{O}_{\mathbb{Q}(\sqrt{-p})} \\ \Big| \\ \mathbb{Z}[\sqrt{-p}] \end{array}$$

and $\mathcal{O}_{\mathbb{Q}(\sqrt{-p})} \cong \begin{cases} \mathbb{Z}[\sqrt{-p}] & \text{if } p \equiv 1 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right] & \text{if } p \equiv 3 \pmod 4 \end{cases}$

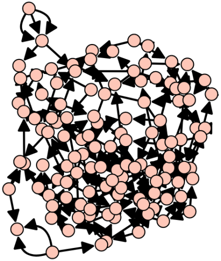
Cryptographic Motivation

WANT:

- Public Key: graph vertex; Private Key: a connected vertex
- A graph that's easy to navigate,
- But too tangled to re-trace steps.

Supersingular Isogeny Graphs:

- Vertices: $\overline{\mathbb{F}_p}$-isomorphism classes of supersingular elliptic curves
- Edges: degree-ℓ isogenies ($\Leftrightarrow$ subgroups of $E(\overline{\mathbb{F}_p})$ of size ℓ)



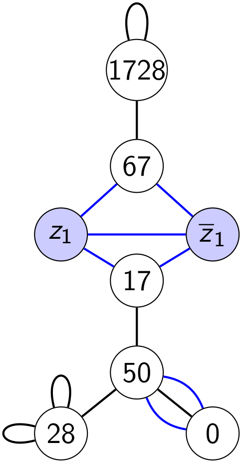
$p = 1409$

Three Graphs

- Full graph $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$
- Spine $\mathcal{S}$: subgraph taking only $\mathbb{F}_p$ vertices of $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$
- Graph generated over $\mathbb{F}_p$: $\mathcal{G}_\ell(\mathbb{F}_p)$

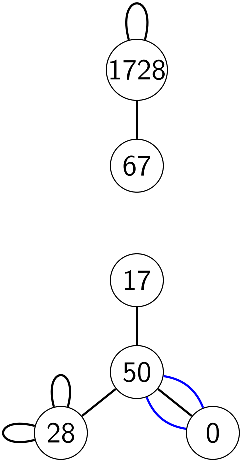
I: $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$: The full supersingular ℓ-isogeny graph

p: a fixed prime (BIG); ℓ: a fixed prime (small)



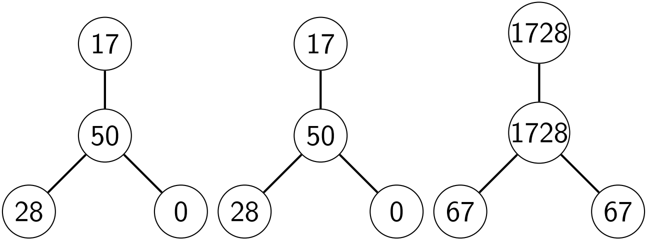
$p = 83, \ell = 2; z_1 = 17i + 38, \overline{z}_1 = 66i + 38$

II: The Spine $\mathcal{S}$: Subgraph of $\mathbb{F}_p$-vertices in $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$



$p = 83, \ell = 2$

III: $\mathcal{G}_\ell(\mathbb{F}_p)$: The supersingular ℓ-isogeny graph, over $\mathbb{F}_p$



$p = 83, \ell = 2$

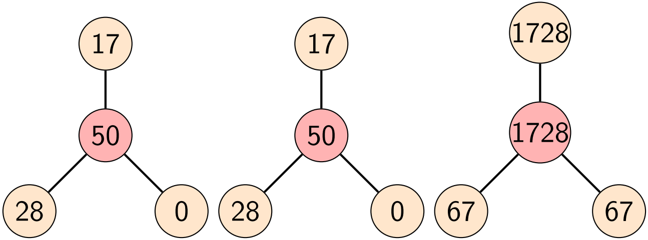
$\mathcal{G}_2(\mathbb{F}_p)$: Volcanoes

[Sut13]. p: a prime; E: supersingular elliptic curve over $\overline{\mathbb{F}_p}$

$$\mathrm{End}_{\mathbb{F}_p}(E) \cong \begin{cases} \mathbb{Z}[\sqrt{-p}] \\ \mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right] \end{cases}$$

Definition

If $\mathrm{End}_{\mathbb{F}_p}(E) \cong \mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$, then E lies on the surface of the volcano..
If $\mathrm{End}_{\mathbb{F}_p}(E) \cong \mathbb{Z}[\sqrt{-p}]$, then E lies on the floor of the volcano.

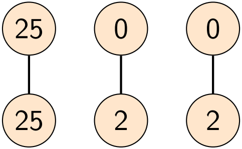


Structure of $\mathcal{G}_2(\mathbb{F}_p)$

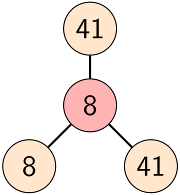
[DG16]. For $\ell = 2$:

Theorem (Theorem 2.7 [DG16])

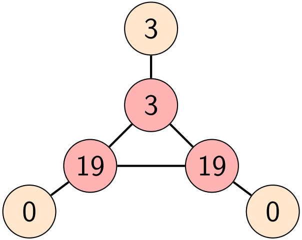
- $p \equiv 1 \pmod 4$: *Vertices paired together in isolated edges,*
- $p \equiv 3 \pmod 8$: *Vertices form a volcano; surface is one vertex, connected to three vertices on the floor,*
- $p \equiv 7 \pmod 8$: *Vertices form a volcano; each surface vertex is connected 1:1 with the floor.*



$p = 29 \equiv 1 \pmod 4$



$p = 43 \equiv 3 \pmod 8$



$p = 23 \equiv 7 \pmod 8$

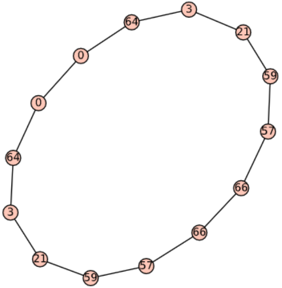
Structure of $\mathcal{G}_\ell(\mathbb{F}_p)$

For $\ell > 2$:

Theorem (Theorem 2.7 [DG16])

- $\left(\frac{-p}{\ell}\right) = 1$: *two ℓ-isogenies*
- $\left(\frac{-p}{\ell}\right) = -1$: *no ℓ-isogenies*

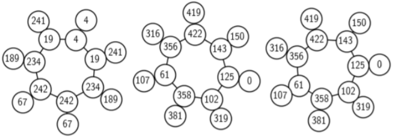
$p = 103, \ell = 3$:



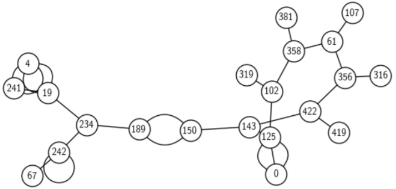
Possible changes, passing from $\mathcal{G}_\ell(\mathbb{F}_p)$ to $\overline{\mathbb{F}_p}$

Definition (3.13 [ACL+19])

- If two distinct components of $\mathcal{G}_\ell(\mathbb{F}_p)$ have exactly the same set of vertices up to j-invariant, then they will **stack** over $\overline{\mathbb{F}_p}$.
- A component of $\mathcal{G}_\ell(\mathbb{F}_p)$ will **fold** if it contains both vertices corresponding to each j-invariant in its vertex set.
- Two distinct components of $\mathcal{G}_\ell(\mathbb{F}_p)$ will **attach with a new edge**.
- Two distinct components of $\mathcal{G}_\ell(\mathbb{F}_p)$ will **attach along a j-invariant** if one vertex of each share a j-invariant (only possible for $\ell > 2$).



(a) The $\mathcal{G}_2(\mathbb{F}_p)$ for $p = 431$

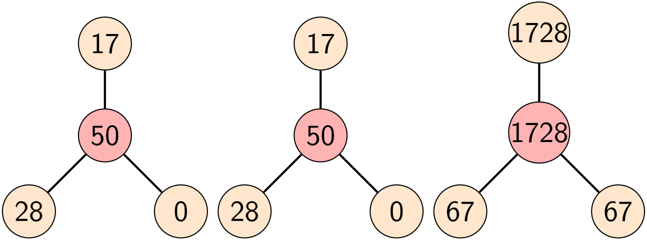


(b) The spine $\mathcal{S} \subset \mathcal{G}_2(\overline{\mathbb{F}_p})$ for $p = 431$.

Rules to pass from $\mathcal{G}_\ell(\mathbb{F}_p)$ to $\overline{\mathbb{F}_p}$

Observations:

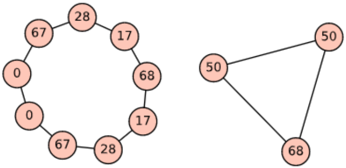
- (Corollary 3.9 [ACL$^+$19]) Twists are either both on the surface or both on the floor, except for $j = 1728$.
    - For $j \neq 1728$, $\mathrm{End}_{\mathbb{F}_p}(E) \cong \mathrm{End}_{\mathbb{F}_p}(E^t)$
- When $j = 1728$ is supersingular, one twist is on the surface, the other on the floor. They are 2-isogenous.
- (Lemma 3.11 [ACL$^+$19]) Edges from the same vertex don't collapse.
- (Corollary 3.12 [ACL$^+$19]) Twists have the same neighbor sets.



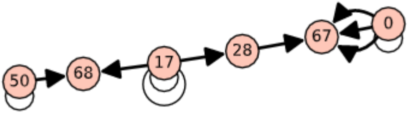
What actually happens for $\ell > 2$?

Theorem (Proposition 3.9 [ACL+19])

While passing from $\mathcal{G}_\ell(\mathbb{F}_p)$ to $\mathcal{S}$, the only possible events are stacking, folding and n attachments by a new edge and m attachments along a j-invariant with $m + 2n \leq 2\ell(2\ell - 1)$.



$\mathcal{G}_3(\mathbb{F}_{83})$:



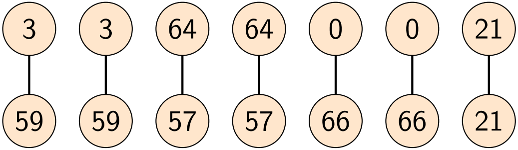
$\mathcal{S}$:

What actually happens for $\ell = 2$?

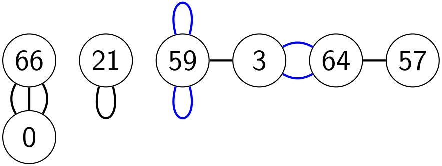
Theorem (Theorem 3.26 of [ACL+19])

Only stacking, folding or at most one attachment by a new edge are possible. In particular, no attachments by a j-invariant are possible.

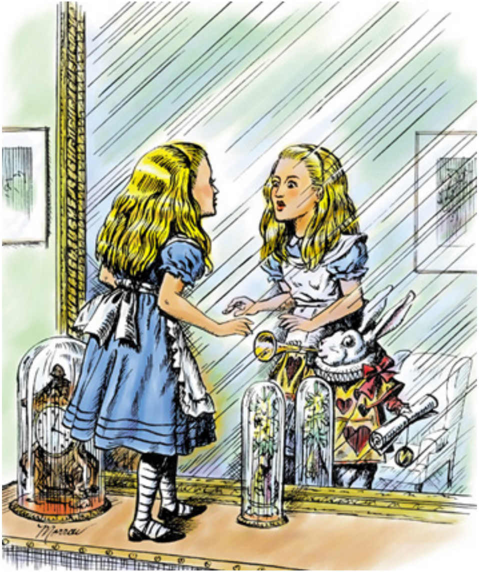
$\mathcal{G}_2(\mathbb{F}_{101})$:



$\mathcal{S}$:



Through the Looking Glass: Mirror Involution



Frobenius

$$\pi : E : y^2 = x^3 + ax + b \to E^{(p)} : y^2 = x^3 + a^p x + b^p$$
$$(x, y) \mapsto (x^p, y^p)$$
$$j(E) \mapsto j(E)^p$$

Definition (Mirror Involution)

If j is a supersingular j-invariant, so is its $\mathbb{F}_{p^2}$-conjugate j^p.
If $\exists$ ℓ-isogeny $\phi : E(j_1) \to E(j_2)$ then $\exists$ ℓ-isogeny $\phi' : E(j_1)^p \to E(j_2)^p$.
The p-power Frobenius map on $\mathbb{F}_{p^2}$ gives the **mirror involution** on $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$.

$$\cdots \to j_1 \to j_2 \to j_3 \to \cdots$$

Mirror Involution gives:

$$\cdots \to j_1^p \leftarrow j_2^p \leftarrow j_3^p \leftarrow \cdots$$

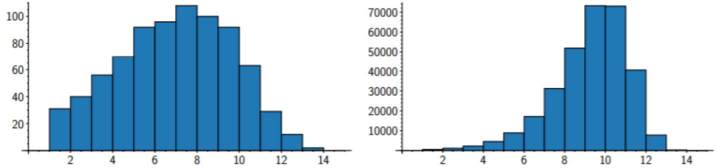
Mirror Paths

$$j_0 \to j_1 \to \cdots \to j_n \to \mathbf{j} \to j_n^p \to \cdots \to j_1^p \to j_0^p$$

$$j_0 \to j_1 \to \cdots \to j_n \to j_n^p \to \cdots \to j_1^p \to j_0^p$$

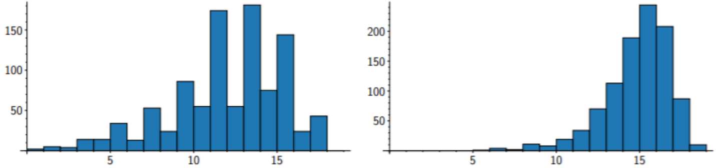
How often are paths of the first type? Second type?

How far are conjugate j-invariants in $\mathcal{G}_2(\overline{\mathbb{F}_p})$?



(a) *Distances between conjugate pairs.* ***(b)*** *Distances between arbitrary pairs.*

Figure 4.1: *Distances measured between conjugate pairs and arbitrary pairs of vertices not in* $\mathbb{F}_p$ *for the prime* $p = 19489$.



(a) *Distances between conjugate pairs.* ***(b)*** *Distances between arbitrary pairs.*

Figure 4.2: *Distances between* 1000 *randomly sampled pairs of arbitrary and conjugate vertices for the prime* $p = 1000003$.

How often are conjugate j-invariants 2-isogenous?

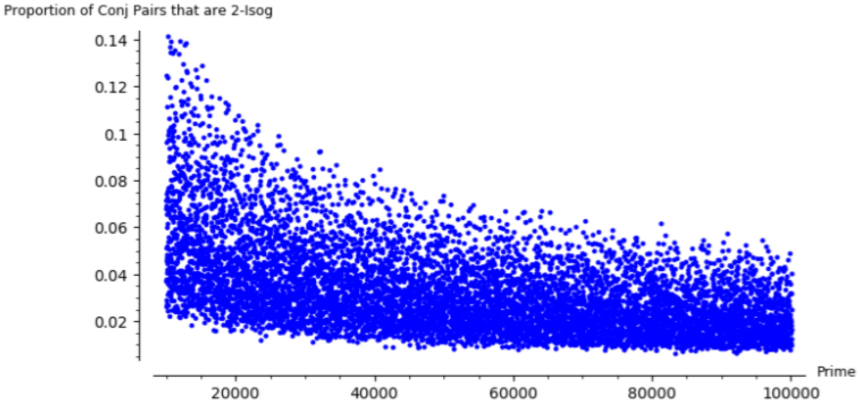


Figure 5.3: *Proportion of 2-isogenous conjugate pairs in* $\mathcal{G}_2(\overline{\mathbb{F}_p})$ *for* $p > 10000$

Summary

- We understand completely how to pass from $\mathcal{G}_\ell(\mathbb{F}_p)$ into $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$.
- Mirror involution gives a new perspective on supersingular isogeny graph structure.
- Vertices which are conjugate appear to be closer than random vertices, at least for $\ell = 2$.

Thank you.

Sarah Arpin, Catalina Camacho-Navarro, Kristin Lauter, Joelle Lim, Kristina Nelson, Travis Scholl, and Jana Sotáková.
Adventures in Supersingularland.
submitted, 2019.
https://arxiv.org/abs/1909.07779.

C. Delfs and S. D. Galbraith.
Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$.
Des. Codes Cryptography, 78(2):425–440, 2016.
https://arxiv.org/pdf/1310.7789.pdf.

Joseph H. Silverman.
The Arithmetic of Elliptic Curves, 2nd Edition.
Springer-Verlag, New York, N.Y., 2009.

Andrew Sutherland.
Isogeny volcanoes.
The Open Book Series, 1(1):507–530, Nov 2013.