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

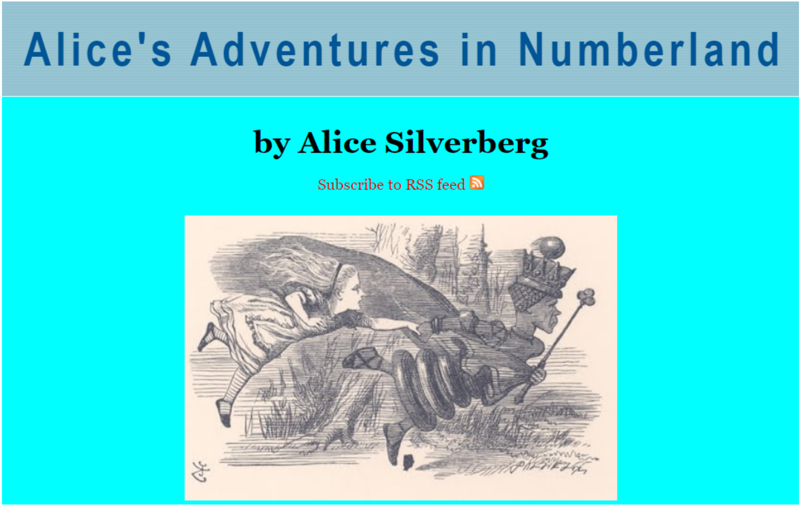
Sarah Arpin
University of Colorado Boulder

Slow Pitch - CU Boulder

October 9th, 2019

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

Alice Silverberg



https://sites.google.com/site/numberlandadventures/

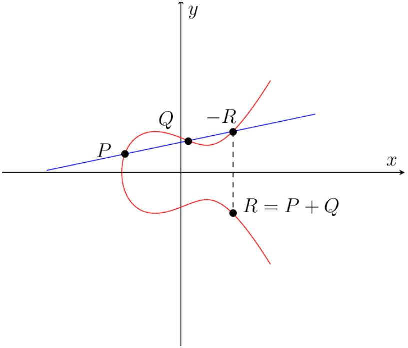
Overview

Elliptic Curves

Definition

An **elliptic curve** is a smooth, projective, algebraic curve of genus 1 with a fixed point, usually denoted $\mathcal{O}_E$.

$E : ZY^2 = X^3 + aXZ^2 + bZ^3$
$E : y^2 = x^3 + Ax + B$

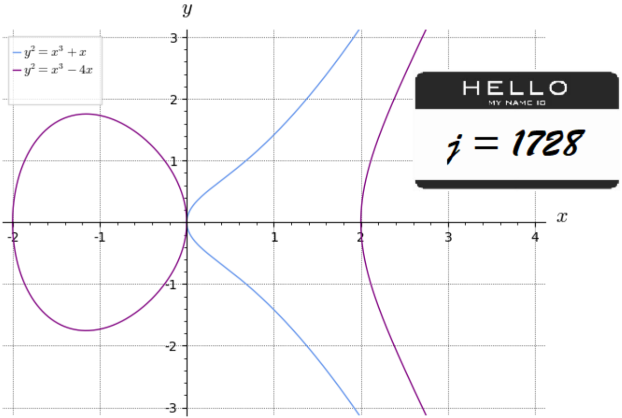


[Nas18]

j-Invariant

Definition

The j-**invariant** is a number which identifies an elliptic curve defined over a field K up to isomorphism over $\overline{K}$.



Supersingular Elliptic Curves

Definition ([Sil09])

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

- the multiplication-by-p map $[p] : E \to E$ is purely in separable and $j(E) \in \mathbb{F}_{p^2}$,
- $\text{End}_{\overline{K}}(E)$ is a maximal order in a quaternion algebra.

$\mathbb{F}_p$-Endomorphism Ring

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 $\mathbb{Z}[\sqrt{-p}]$.

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

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

Isogenies

Definition

An **isogeny** $\phi : E_1 \to E_2$ is a morphism between elliptic curves such that $\phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$.

Theorem (Corollary III.4.9 [Sil09])

The kernel of a nonzero isogeny is a finite group.

Theorem (Theorem III.4.10(c) [Sil09])

The degree of an isogeny is equal to the size of the kernel.

Isogenies, II

Theorem (Proposition III.4.12 [Sil09])

If E is an elliptic curve and Φ is a finite subgroup of E, then there are a unique elliptic curve E' and a separable isogeny ϕ such that

$$\phi : E \to E', \ \ker \phi = \Phi.$$

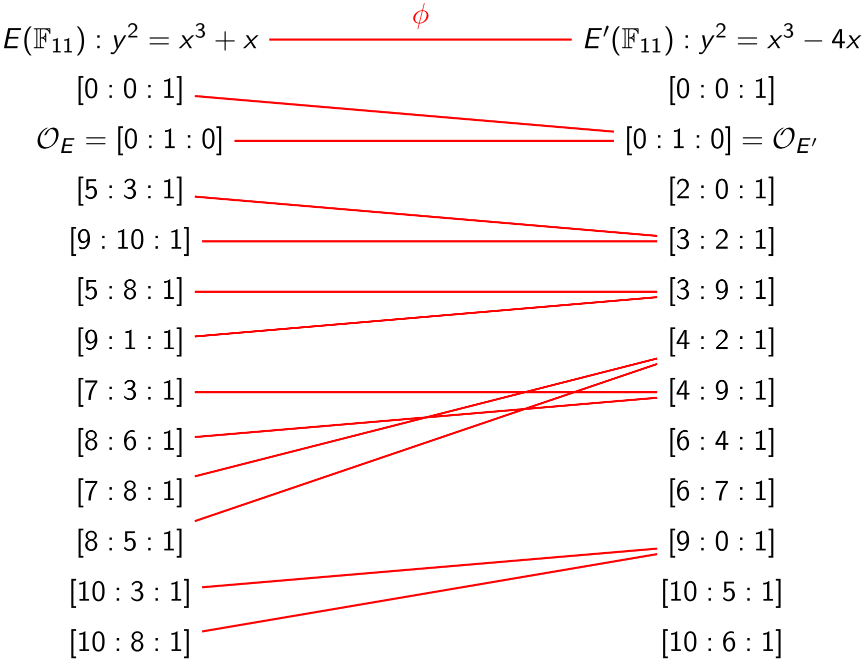
Isogenies, II

Theorem (Proposition III.4.12 [Sil09])

If E is an elliptic curve and Φ is a finite subgroup of E, then there are a unique elliptic curve E' and a separable isogeny ϕ such that

$$\phi : E \to E', \ \ker \phi = \Phi.$$

Let's do a quick example.


ϕ
$E(\mathbb{F}_{11}) : y^2 = x^3 + x$
$E'(\mathbb{F}_{11}) : y^2 = x^3 - 4x$
$[0 : 0 : 1]$
$\mathcal{O}_E = [0 : 1 : 0]$
$[5 : 3 : 1]$
$[9 : 10 : 1]$
$[5 : 8 : 1]$
$[9 : 1 : 1]$
$[7 : 3 : 1]$
$[8 : 6 : 1]$
$[7 : 8 : 1]$
$[8 : 5 : 1]$
$[10 : 3 : 1]$
$[10 : 8 : 1]$
$[0 : 0 : 1]$
$[0 : 1 : 0] = \mathcal{O}_{E'}$
$[2 : 0 : 1]$
$[3 : 2 : 1]$
$[3 : 9 : 1]$
$[4 : 2 : 1]$
$[4 : 9 : 1]$
$[6 : 4 : 1]$
$[6 : 7 : 1]$
$[9 : 0 : 1]$
$[10 : 5 : 1]$
$[10 : 6 : 1]$

Cryptographic Motivation

WANT:

- Public Key: graph vertex; Private Key: ℓ-isogenous graph vertex.
- A graph that's easy to navigate,
- ...but too tangled to re-trace steps.

Cryptographic Motivation

WANT:

- Public Key: graph vertex; Private Key: ℓ-isogenous graph vertex.
- A graph that's easy to navigate,
- ...but too tangled to re-trace steps.

Supersingular Isogeny Graphs have

- Vertices: $\overline{\mathbb{F}_p}$-isomorhism classes of supersingular elliptic curves
- Edges: degree-ℓ isogenies ($\Leftrightarrow$ subgroups of $E(\overline{\mathbb{F}_p})$ of size ℓ)
- *With a little extra information, isogenies commute!

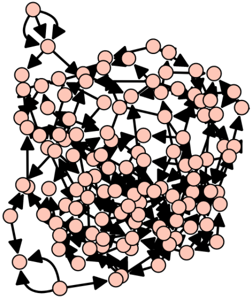
Cryptographic Motivation

WANT:

- Public Key: graph vertex; Private Key: ℓ-isogenous graph vertex.
- A graph that's easy to navigate,
- ...but too tangled to re-trace steps.

Supersingular Isogeny Graphs have

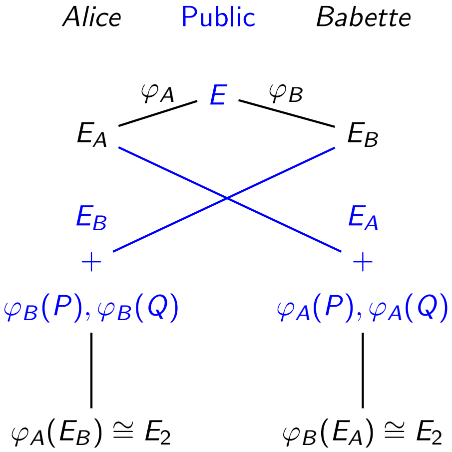
- Vertices: $\overline{\mathbb{F}_p}$-isomorhism classes of supersingular elliptic curves
- Edges: degree-ℓ isogenies ($\Leftrightarrow$ subgroups of $E(\overline{\mathbb{F}_p})$ of size ℓ)
- *With a little extra information, isogenies commute!



$p = 1409$

Quick-and-Dirty Supersingular Isogeny Diffie-Hellman (SIKE)

Quick-and-Dirty Supersingular Isogeny Diffie-Hellman (SIKE)

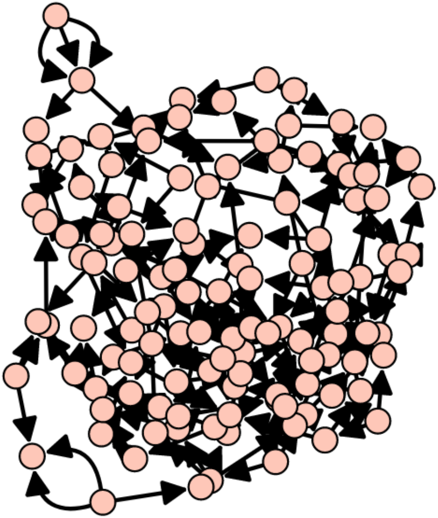


Hard Problems

1. Given E_1, E_2, find an ℓ^n-isogeny between them.
2. Given E, $\varphi_A(E)$, and $\varphi_B(E)$, find $\varphi_A(\varphi_B(E)) \cong \varphi_B(\varphi_A(E))$.

Hard Problems

1. Given E_1, E_2, find an ℓ^n-isogeny between them.
2. Given E, $\varphi_A(E)$, and $\varphi_B(E)$, find $\varphi_A(\varphi_B(E)) \cong \varphi_B(\varphi_A(E))$.



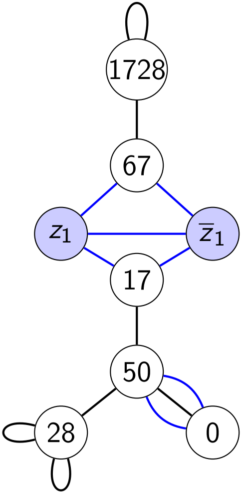
Hard Problems

1. Given E_1, E_2, find an ℓ^n-isogeny between them.
2. Given E, $\varphi_A(E)$, and $\varphi_B(E)$, find $\varphi_A(\varphi_B(E)) \cong \varphi_B(\varphi_A(E))$.

Three Graphs

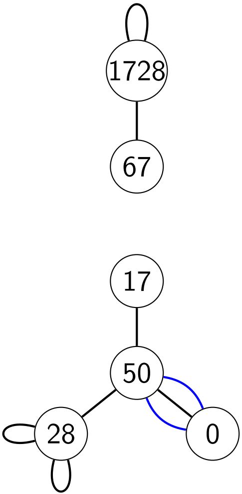
I: $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$: The full supersingular ℓ-isogeny graph

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



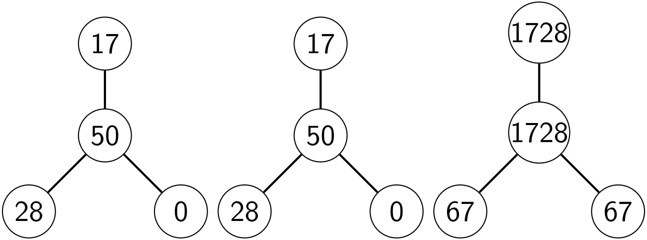
$p = 83, \ell = 2; z_1 = 17i + 38, \overline{z}_1 = 66i + 38$

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 $\mathbb{F}_p$



$p = 83, \ell = 2$

$$\mathcal{G}_\ell(\mathbb{F}_p) \not\subseteq \mathcal{S}!$$

- Vertices: Twists are separated and identified
- Edges: Field of definition of isogenies changes

The structure of $\mathcal{G}_\ell(\mathbb{F}_p)$ is well understood:

Volcanoes

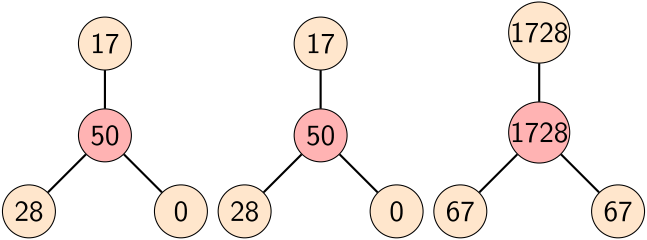
p: a prime; E: supersingular elliptic curve over $\overline{\mathbb{F}_p}$

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

If $p \equiv 1 \pmod 4$, $\mathrm{End}_{\mathbb{F}_p}(E) \cong \mathbb{Z}[\sqrt{-p}]$.

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.

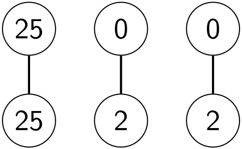


Structure of $\mathcal{G}_2(\mathbb{F}_p)$

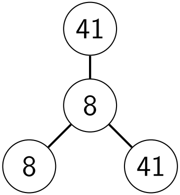
Well-studied by Delfs and Galbraith [DG16]. For $\ell = 2$:

Theorem (Theorem 2.7 [DG16])

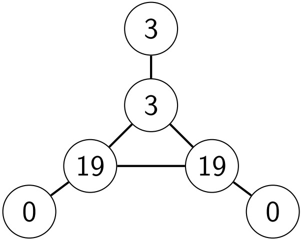
- $p \equiv 1 \pmod 4$: *Vertices paired together in isolated edges,*
- $p \equiv 3 \pmod 8$: *Vertices form a volcano; surface is one vertex, connected to three vertices on the floor,*
- $p \equiv 7 \pmod 8$: *Vertices form a volcano; each surface vertex is connected 1:1 with the floor.*



$p = 29 \equiv 1 \pmod 4$



$p = 43 \equiv 3 \pmod 8$



$p = 23 \equiv 7 \pmod 8$

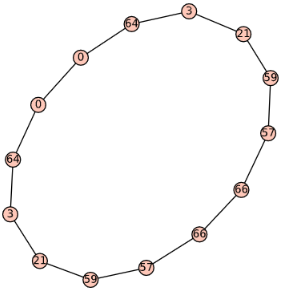
Structure of $\mathcal{G}_\ell(\mathbb{F}_p)$

For $\ell > 2$:

Theorem (Theorem 2.7 [DG16])

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

$p = 103, \ell = 3$:

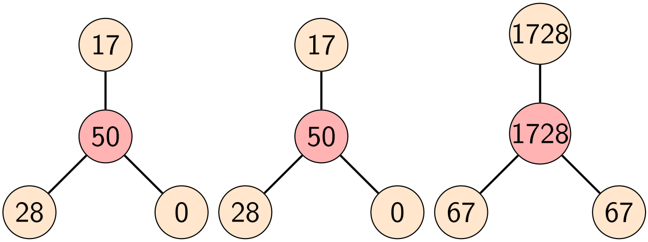


How does $\mathcal{G}_\ell(\mathbb{F}_p)$ change when we pass to $\overline{\mathbb{F}_p}$?

How does $\mathcal{G}_\ell(\mathbb{F}_p)$ change when we pass to $\overline{\mathbb{F}_p}$?

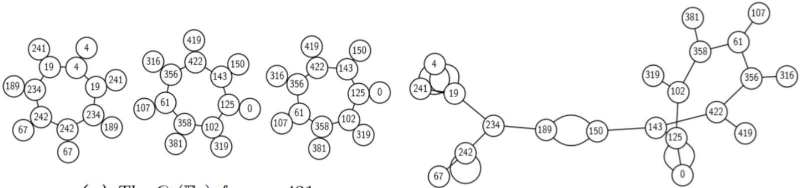
Observations:

- (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 don't collapse.
- (Corollary 3.12 [ACL+19]) Twists have the same neighbor sets.



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 $p = 431$*

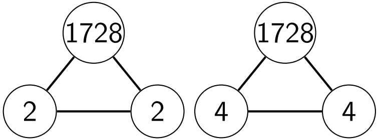
(b) *The spine $\mathcal{S} \subset \mathcal{G}_2(\overline{\mathbb{F}_p})$ for $p = 431$.*

What actually happens for $\ell > 2$?

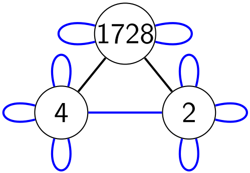
Theorem (Proposition 3.9 [ACL+19])

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 $m + 2n \leq 2\ell(2\ell - 1)$.

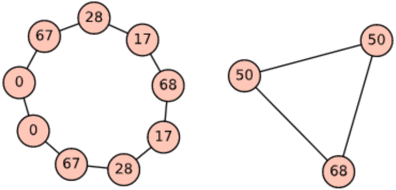
$\mathcal{G}_5(\mathbb{F}_{31})$:



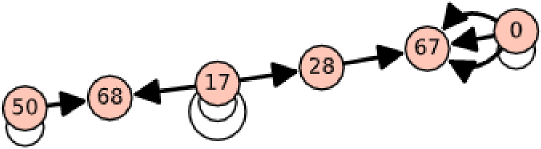
$\mathcal{S}$:



$p = 83, \ell = 3$



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



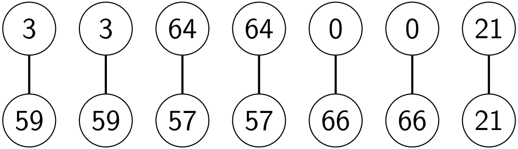
$\mathcal{S}$:

What actually happens for $\ell = 2$?

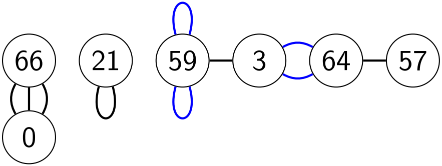
Theorem (Theorem 3.26 of [ACL+19])

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

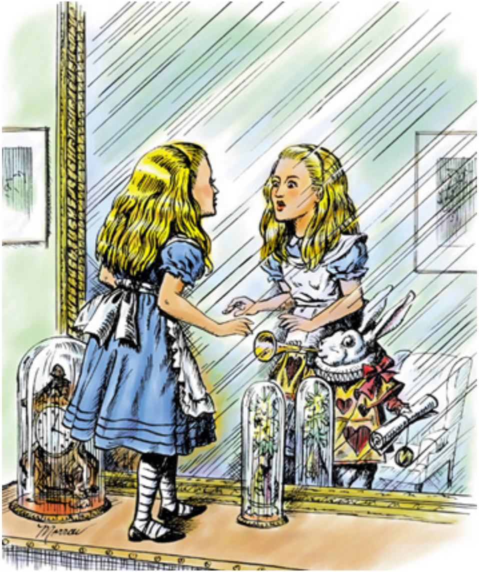
$\mathcal{G}_2(\mathbb{F}_{101})$:



$\mathcal{S}$:



Through the Looking Glass: Mirror Involution



Frobenius

p-power Frobenius π on $\mathbb{F}_{p^2}$:

$$\pi(a) = a^p$$

If $a \in \mathbb{F}_p$, then $a^p = a$.

Frobenius

p-power Frobenius π on $\mathbb{F}_{p^2}$:

$$\pi(a) = a^p$$

If $a \in \mathbb{F}_p$, then $a^p = a$.
On elliptic curves:

$$\pi : E : Y^2Z = X^3 + aXZ^2 + bZ^3 \to E^{(p)} : Y^2Z = X^3 + a^pXZ^2 + b^pZ^3$$

$$[X : Y : Z] \mapsto [X^p : Y^p : Z^p]$$

$j(E^{(p)}) = j(E)^p$
The Frobenius will also apply to **paths** in $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$:

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

Apply π to the vertices and get:

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

We call j^p the **conjugate** of j.

Mirror Involution

Definition

If j is a supersingular j-invariant, so is its $\mathbb{F}_{p^2}$-conjugate j^p. If there is an ℓ-isogeny $\phi : E(j_1) \to E(j_2)$ then there exists an ℓ-isogeny $\phi' : E(j_1)^p \to E(j_2)^p$.

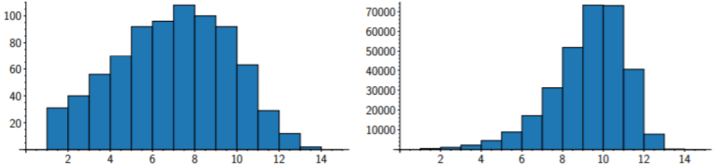
The p-power Frobenius map on $\mathbb{F}_{p^2}$ gives the **mirror involution** on $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$.

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

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

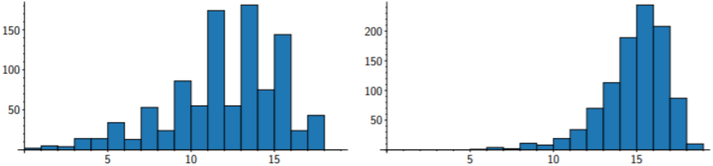
How often are paths of the first type? Second type?

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?

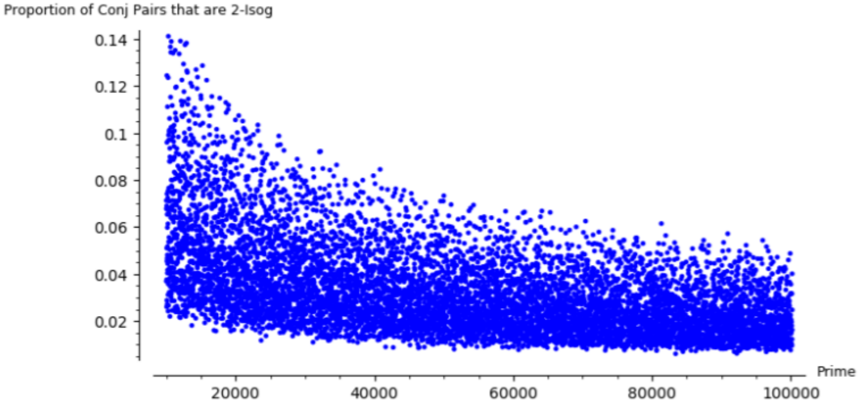


Figure 5.3: *Proportion of 2-isogenous conjugate pairs in* $\mathcal{G}_2(\overline{\mathbb{F}_p})$ *for* $p > 10000$

Modulo 12

	$p \equiv 1 \pmod{12}$	$p \equiv 5 \pmod{12}$
Total # of primes:	2079	2104
Mean:	0.043551	0.021969
Standard Deviation:	0.019815	0.010206
	$p \equiv 7 \pmod{12}$	$p \equiv 11 \pmod{12}$
Total # of primes:	2101	2094
Mean:	0.043375	0.022244
Standard Deviation:	0.020140	0.010512

Table 1: *Proportions of 2-isogenous conjugates,* $10007 \leq p \leq 100193$, *sorted by* $p \bmod 12$

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

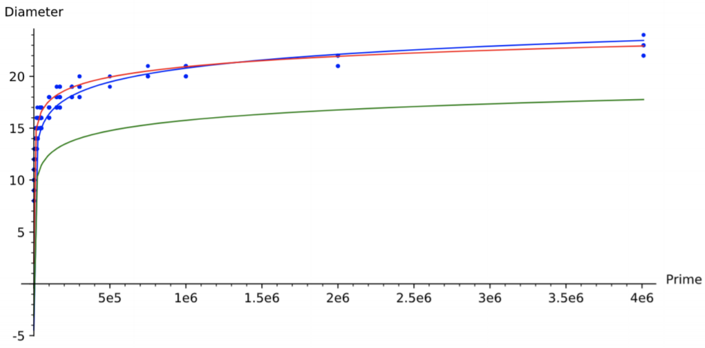


Figure 6.1: *Diameters of 2-isogeny graph over* $\overline{\mathbb{F}}_p$*, with* $y = \log_2(p/12) + \log_2(12) + 1$ *(red) and* $y = \frac{4}{3}\log_2(p/12) - 1$ *(blue).*

Isogeny graphs behave more like random Ramanujan graphs than LPS (Lubotzky-Phillips-Sarnak) graphs.

Trends Modulo 12

For $p \equiv 1, 7 \pmod{12}$:

- smaller 2-isogeny graph diameters
- larger number of spine components
- larger proportion of 2-isogenous conjugate j-invariants

For $p \equiv 5, 11 \pmod{12}$:

- larger 2-isogeny graph diameters
- smaller number of spine components
- smaller proportion of 2-isogenous conjugate j-invariants

Summary

- We understand completely how to pass from $\mathcal{G}_2(\mathbb{F}_p)$ into $\mathcal{G}_2(\overline{\mathbb{F}_p})$.
- Mirror involution gives a new perspective on supersingular isogeny graph structure.
- In terms of diameter, isogeny graphs behave more like random Ramanujan graphs than LPS (Lubotzky-Pizer-Sarnak) graphs.

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.

Christos Nasikas.
ccountable and privacy preserving data processing via distributed ledgers.
PhD thesis, 05 2018.

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