Adventures in Supersingularland: A Look at Supersingular Isogeny Graphs

Jana Sotáková

QuSoft / UvA

October 7, 2019, Eindhoven

This is joint work with Sarah Arpin, Catalina Camacho-Navarro, Kristin Lauter, Joelle Lim, Kristina Nelson and Travis Scholl.

Post-quantum cryptography

Most of the public-key encryption used nowadays is based on hard problems in number theory.

Post-quantum cryptography

Most of the public-key encryption used nowadays is based on hard problems in number theory.

Quantum computers can break these schemes.

Post-quantum cryptography

Most of the public-key encryption used nowadays is based on hard problems in number theory.

Quantum computers can break these schemes.

(Supersingular) Isogeny-based cryptography: make the number theory problems even harder.

Post-quantum cryptography

Most of the public-key encryption used nowadays is based on hard problems in number theory.

Quantum computers can break these schemes.

(Supersingular) Isogeny-based cryptography: make the number theory problems even harder.

Protocols:

- SIKE (`https://sike.org`),
- CSIDH (`https://csidh.isogeny.org/`),
- signature schemes (GPS, SeaSign, CSI-FiSh)

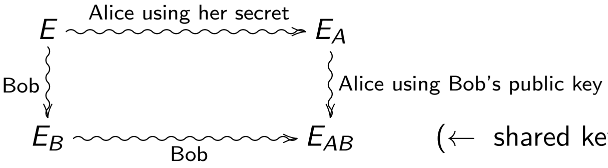
Bird's eye view of public key cryptography

Bird's eye view of public key cryptography

Key exchange after Diffie-Hellman

Bird's eye view of public key cryptography

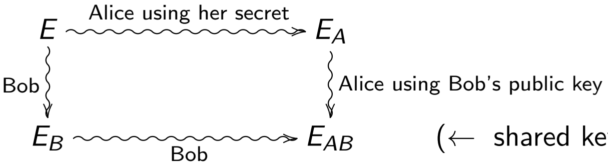
Key exchange after Diffie-Hellman



($\leftarrow$ shared key)

Bird's eye view of public key cryptography

Key exchange after Diffie-Hellman



(← shared key)

Isogeny crypto

The arrows correspond to paths in an isogeny graph

What are supersingular isogeny graphs

Definition

To define a supersingular isogeny graph, we need:

1. a suitable large prime p,

What are supersingular isogeny graphs

Definition

To define a supersingular isogeny graph, we need:

1. a suitable large prime p,

We will encounter

1. $\mathbb{F}_p$, finite field of p elements,

What are supersingular isogeny graphs

Definition

To define a supersingular isogeny graph, we need:

1. a suitable large prime p,

We will encounter

1. $\mathbb{F}_p$, finite field of p elements, same as $\mathbb{Z}/p\mathbb{Z}$ or $\mathbb{Z}_p$

What are supersingular isogeny graphs

Definition

To define a supersingular isogeny graph, we need:

1. a suitable large prime p,

We will encounter

1. $\mathbb{F}_p$, finite field of p elements, same as $\mathbb{Z}/p\mathbb{Z}$ or $\mathbb{Z}_p$
2. $\mathbb{F}_{p^2}$, finite field of p^2 elements, quadratic extension of $\mathbb{F}_p$,

What are supersingular isogeny graphs

Definition

To define a supersingular isogeny graph, we need:

1. a suitable large prime p,

We will encounter

1. $\mathbb{F}_p$, finite field of p elements, same as $\mathbb{Z}/p\mathbb{Z}$ or $\mathbb{Z}_p$
2. $\mathbb{F}_{p^2}$, finite field of p^2 elements, quadratic extension of $\mathbb{F}_p$,
3. $\overline{\mathbb{F}}_p$: It suffices to think that everything is defined over a finite field $\mathbb{F}_q$ with $q = p^n$ for some n.

What are supersingular isogeny graphs

Definition

To define a supersingular isogeny graph, we need:

1. a suitable large prime p,
2. the set of vertices: supersingular elliptic curves, *up to isomorphism*

What are supersingular isogeny graphs

Definition

To define a supersingular isogeny graph, we need:

1. a suitable large prime p,
2. the set of vertices: supersingular elliptic curves, *up to isomorphism*

We focus on supersingular elliptic curves: given by equations

$$E : y^2 = x^3 + ax + b \quad a, b \in \mathbb{F}_{p^2}$$

together with a point at infinity ∞ and such that

$$|\{(x, y) : x, y \in \mathbb{F}_{p^2} \text{ and } y^2 = x^3 = ax + b\} \cup \{\infty\}| = (p + 1)^2$$

What are supersingular isogeny graphs

Definition

To define a supersingular isogeny graph, we need:

1. a suitable large prime p,
2. the set of vertices: supersingular elliptic curves, *up to isomorphism*

We focus on supersingular elliptic curves: given by equations

$$E : y^2 = x^3 + ax + b \quad a, b \in \mathbb{F}_{p^2}$$

together with a point at infinity ∞ and such that

$$|\{(x, y) : x, y \in \mathbb{F}_{p^2} \text{ and } y^2 = x^3 = ax + b\} \cup \{\infty\}| = (p + 1)^2$$

If $a, b \in \mathbb{F}_p$, then we say that E is defined over $\mathbb{F}_p$.

Labels of vertices

For an elliptic curve

$$E : y^2 = x^3 + ax + b \quad a, b \in \mathbb{F}_{p^2}$$

Labels of vertices

For an elliptic curve

$$E : y^2 = x^3 + ax + b \quad a, b \in \mathbb{F}_{p^2}$$

define j-invariant $j(E) = 1728 \cdot \frac{4a^3}{4a^3+27b^2} \in \mathbb{F}_{p^2}$.

Labels of vertices

For an elliptic curve

$$E : y^2 = x^3 + ax + b \quad a, b \in \mathbb{F}_{p^2}$$

define j-invariant $j(E) = 1728 \cdot \frac{4a^3}{4a^3+27b^2} \in \mathbb{F}_{p^2}$.

j-invariant

is an isomorphism invariant over $\overline{\mathbb{F}}_p$.

Example

The two elliptic curves

$$E : y^2 = x^3 - x \qquad E' : y^2 = x^3 + 4x$$

both have $j(E) = j(E') = 1728$, so they are isomorphic

Labels of vertices

For an elliptic curve

$$E : y^2 = x^3 + ax + b \quad a, b \in \mathbb{F}_{p^2}$$

define j-invariant $j(E) = 1728 \cdot \frac{4a^3}{4a^3+27b^2} \in \mathbb{F}_{p^2}$.

j-invariant

is an isomorphism invariant over $\overline{\mathbb{F}}_p$.

Example

The two elliptic curves

$$E : y^2 = x^3 - x \qquad E' : y^2 = x^3 + 4x$$

both have $j(E) = j(E') = 1728$, so they are isomorphic but *not* over $\mathbb{F}_p$.

What are supersingular isogeny graphs

Definition

To define a supersingular isogeny graph, we need:

1. a suitable large prime p,
2. the set of vertices: supersingular elliptic curves, *up to isomorphism*
3. edges: isogenies of elliptic curves, *up to equivalence, up to dual isogenies, of a certain degree*

Example of isogenies

3. edges: isogenies of elliptic curves, *up to equivalence, up to dual isogenies, of a certain degree*

Example of isogenies

3. edges: isogenies of elliptic curves, *up to equivalence, up to dual isogenies, of a certain degree*

Isogenies in an example

Isogenies are maps of elliptic curves, given by rational maps:

$$\phi : E : y^2 = x^3 - x \longrightarrow E' : y^2 = x^3 + 4x$$
$$(x, y) \mapsto \left(\frac{x^2 - 1}{x}, y \cdot \frac{x^2 + 1}{x^2} \right)$$

Example of isogenies

3. edges: isogenies of elliptic curves, *up to equivalence, up to dual isogenies, of a certain degree*

Isogenies in an example

Isogenies are maps of elliptic curves, given by rational maps:

$$\phi : E : y^2 = x^3 - x \longrightarrow E' : y^2 = x^3 + 4x$$
$$(x, y) \mapsto \left(\frac{x^2 - 1}{x}, y \cdot \frac{x^2 + 1}{x^2} \right)$$

We see that the map is not defined at $x = 0$, so run into problems at $(0, 0)$:

Example of isogenies

3. edges: isogenies of elliptic curves, *up to equivalence, up to dual isogenies, of a certain degree*

Isogenies in an example

Isogenies are maps of elliptic curves, given by rational maps:

$$\phi : E : y^2 = x^3 - x \longrightarrow E' : y^2 = x^3 + 4x$$
$$(x, y) \mapsto \left(\frac{x^2 - 1}{x}, y \cdot \frac{x^2 + 1}{x^2} \right)$$

We see that the map is not defined at $x = 0$, so run into problems at $(0, 0)$: define

$$(0, 0),\ \infty \mapsto \infty$$

Example of isogenies

3. edges: isogenies of elliptic curves, *up to equivalence, up to dual isogenies, of a certain degree*

Isogenies in an example

Isogenies are maps of elliptic curves, given by rational maps:

$$\phi : E : y^2 = x^3 - x \longrightarrow E' : y^2 = x^3 + 4x$$
$$(x, y) \mapsto \left(\frac{x^2 - 1}{x}, y \cdot \frac{x^2 + 1}{x^2} \right)$$

We see that the map is not defined at $x = 0$, so run into problems at $(0, 0)$: define

$$(0, 0),\ \infty \mapsto \infty$$

There are two points mapping to ∞, so we say that this isogeny has degree 2.

Supersingular isogeny graphs

Fix a prime p (big) and a prime ℓ (small).

The supersingular isogeny graph $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$

1. vertices: all supersingular elliptic curves up to isomorphism: labels j-invariants (in $\mathbb{F}_{p^2}$)
2. edges: isogenies of degreee ℓ (we say ℓ-isogenies)

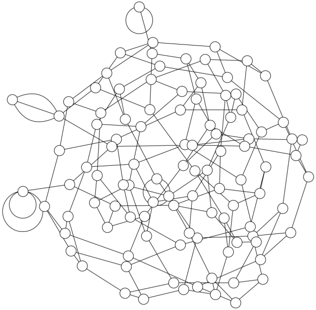
Supersingular isogeny graphs

Fix a prime p (big) and a prime ℓ (small).

The supersingular isogeny graph $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$

1. vertices: all supersingular elliptic curves up to isomorphism: labels j-invariants (in $\mathbb{F}_{p^2}$)
2. edges: isogenies of degreee ℓ (we say ℓ-isogenies)

$p = 1223$ and $\ell = 2$



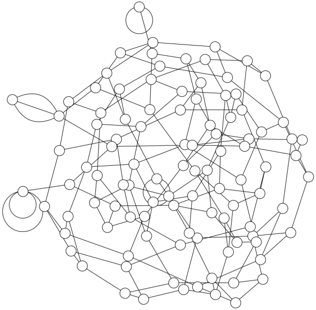
Supersingular isogeny graphs

Fix a prime p (big) and a prime ℓ (small).

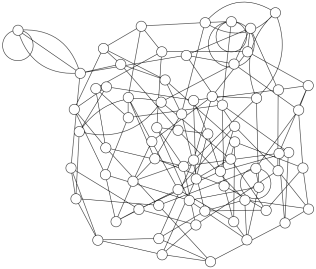
The supersingular isogeny graph $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$

1. vertices: all supersingular elliptic curves up to isomorphism: labels j-invariants (in $\mathbb{F}_{p^2}$)
2. edges: isogenies of degreee ℓ (we say ℓ-isogenies)

$p = 1223$ and $\ell = 2$



$p = 827$ and $\ell = 3$



Supersingular isogeny graphs as Ramanujan graphs

Fix a prime p (big) and a prime ℓ (small).

The supersingular isogeny graph $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$

1. vertices: all supersingular elliptic curves up to isomorphism: labels j-invariants (in $\mathbb{F}_{p^2}$)
2. edges: isogenies of degreee ℓ (we say ℓ-isogenies)

Properties

Supersingular isogeny graphs as Ramanujan graphs

Fix a prime p (big) and a prime ℓ (small).

The supersingular isogeny graph $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$

1. vertices: all supersingular elliptic curves up to isomorphism: labels j-invariants (in $\mathbb{F}_{p^2}$)
2. edges: isogenies of degreee ℓ (we say ℓ-isogenies)

Properties

1. exponentially-large graphs ($\approx p/12$ vertices)

Supersingular isogeny graphs as Ramanujan graphs

Fix a prime p (big) and a prime ℓ (small).

The supersingular isogeny graph $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$

1. vertices: all supersingular elliptic curves up to isomorphism: labels j-invariants (in $\mathbb{F}_{p^2}$)
2. edges: isogenies of degreee ℓ (we say ℓ-isogenies)

Properties

1. exponentially-large graphs ($\approx p/12$ vertices)
2. connected, $\ell + 1$-regular graphs,

Supersingular isogeny graphs as Ramanujan graphs

Fix a prime p (big) and a prime ℓ (small).

The supersingular isogeny graph $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$

1. vertices: all supersingular elliptic curves up to isomorphism: labels j-invariants (in $\mathbb{F}_{p^2}$)
2. edges: isogenies of degreee ℓ (we say ℓ-isogenies)

Properties

1. exponentially-large graphs ($\approx p/12$ vertices)
2. connected, $\ell + 1$-regular graphs,
3. short diameters: $d = \Theta(\log(p))$,

Supersingular isogeny graphs as Ramanujan graphs

Fix a prime p (big) and a prime ℓ (small).

The supersingular isogeny graph $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$

1. vertices: all supersingular elliptic curves up to isomorphism: labels j-invariants (in $\mathbb{F}_{p^2}$)
2. edges: isogenies of degreee ℓ (we say ℓ-isogenies)

Properties

1. exponentially-large graphs ($\approx p/12$ vertices)
2. connected, $\ell + 1$-regular graphs,
3. short diameters: $d = \Theta(\log(p))$,
4. expander graphs: taking random walks of length $\log(p)$ is almost as good as uniform sampling of vertices

Supersingular isogeny graphs as Ramanujan graphs

Fix a prime p (big) and a prime ℓ (small).

The supersingular isogeny graph $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$

1. vertices: all supersingular elliptic curves up to isomorphism: labels j-invariants (in $\mathbb{F}_{p^2}$)
2. edges: isogenies of degreee ℓ (we say ℓ-isogenies)

Properties

1. exponentially-large graphs ($\approx p/12$ vertices)
2. connected, $\ell + 1$-regular graphs,
3. short diameters: $d = \Theta(\log(p))$,
4. expander graphs: taking random walks of length $\log(p)$ is almost as good as uniform sampling of vertices
5. path finding is hard

Supersingular isogeny graphs as Ramanujan graphs

Fix a prime p (big) and a prime ℓ (small).

The supersingular isogeny graph $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$

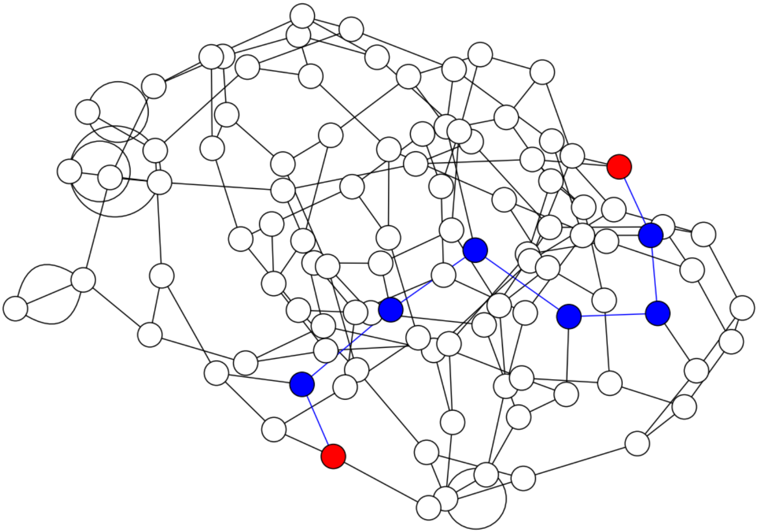
1. vertices: all supersingular elliptic curves up to isomorphism: labels j-invariants (in $\mathbb{F}_{p^2}$)
2. edges: isogenies of degreee ℓ (we say ℓ-isogenies)

Properties

1. exponentially-large graphs ($\approx p/12$ vertices)
2. connected, $\ell + 1$-regular graphs,
3. short diameters: $d = \Theta(\log(p))$,
4. expander graphs: taking random walks of length $\log(p)$ is almost as good as uniform sampling of vertices
5. path finding is hard (remember $E \rightsquigarrow E_A$)

Path finding is hard

For $p = 1223$ and $\ell = 2$, shortest path between two random vertices:



The Spine

Path finding is not always hard

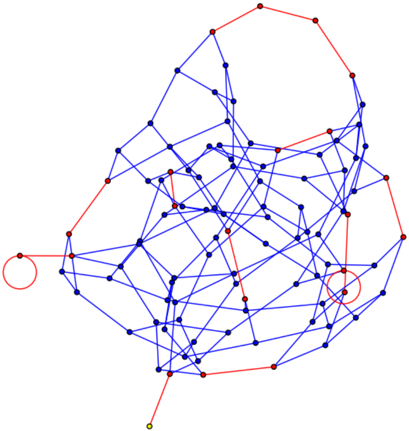
For vertices labelled with j-invariants $j \in \mathbb{F}_p$, path finding is easier.

The Spine

Path finding is not always hard

For vertices labelled with j-invariants $j \in \mathbb{F}_p$, path finding is easier.

For cryptanalysis, we typically assume that the spine is randomly distributed in the graph

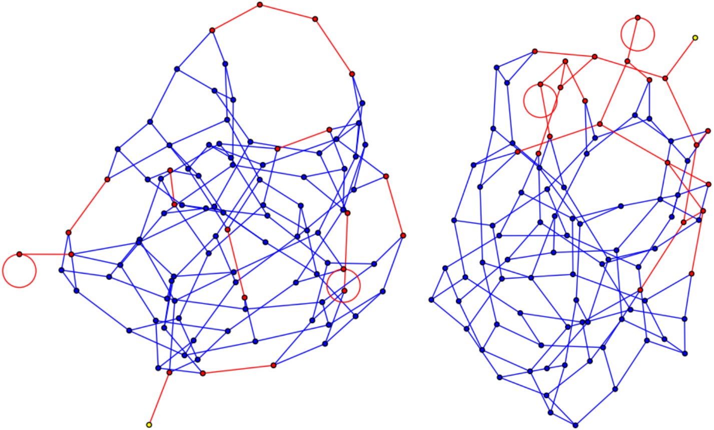


The Spine

Path finding is not always hard

For vertices labelled with j-invariants $j \in \mathbb{F}_p$, path finding is easier.

For cryptanalysis, we typically assume that the spine is randomly distributed in the graph



The Spine

Definition

The **spine** $\mathcal{S}$ is the induced subgraph of the isogeny graph with vertices

$$\{j : j \in \mathbb{F}_p\}$$

The Spine

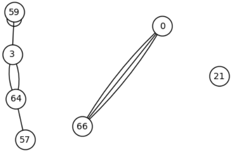
Definition

The **spine** $\mathcal{S}$ is the induced subgraph of the isogeny graph with vertices

$$\{j : j \in \mathbb{F}_p\}$$

It is a subgraph of size approximately $\sqrt{p}$.

The spine for $\ell = 2$



$p = 101$

The Spine

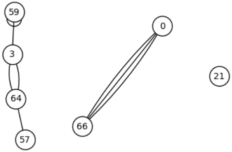
Definition

The **spine** $\mathcal{S}$ is the induced subgraph of the isogeny graph with vertices

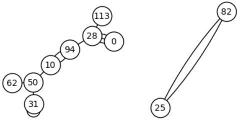
$$\{j : j \in \mathbb{F}_p\}$$

It is a subgraph of size approximately $\sqrt{p}$.

The spine for $\ell = 2$



$p = 101$



$p = 131$

The Spine

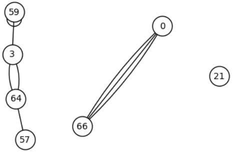
Definition

The **spine** $\mathcal{S}$ is the induced subgraph of the isogeny graph with vertices

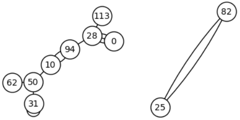
$$\{j : j \in \mathbb{F}_p\}$$

It is a subgraph of size approximately $\sqrt{p}$.

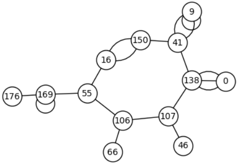
The spine for $\ell = 2$



$p = 101$



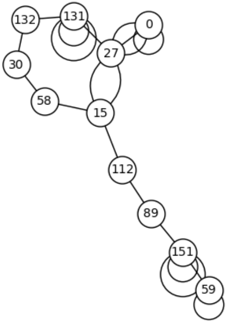
$p = 131$



$p = 191$

Examples of the spine

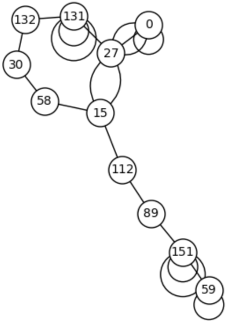
The spine for $\ell = 3$



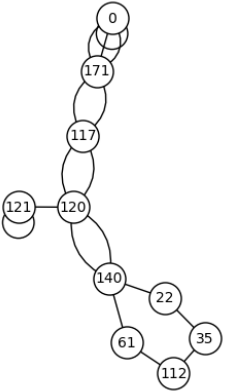
$p = 167$

Examples of the spine

The spine for $\ell = 3$



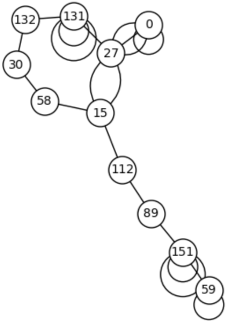
$p = 167$



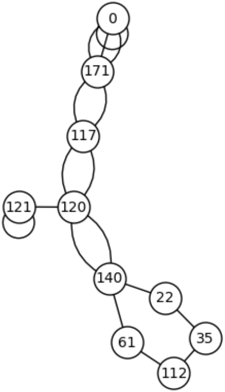
$p = 179$

Examples of the spine

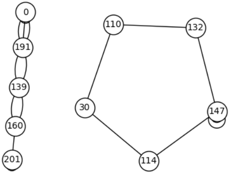
The spine for $\ell = 3$



$p = 167$



$p = 179$



$p = 227$

Visible structure

In the last picture, we see the nice cycle with 5 vertices and another component also with 5 vertices.

Everything over $\mathbb{F}_p$: the graph $\mathcal{G}_\ell(\mathbb{F}_p)$

Fix ℓ a small prime and p a large prime.

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

1. vertices: elliptic curves defined over $\mathbb{F}_p$, up to $\mathbb{F}_p$-isomorphism,

Everything over $\mathbb{F}_p$: the graph $\mathcal{G}_\ell(\mathbb{F}_p)$

Fix ℓ a small prime and p a large prime.

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

1. vertices: elliptic curves defined over $\mathbb{F}_p$, up to $\mathbb{F}_p$-isomorphism, (every j-invariant is there twice)

Everything over $\mathbb{F}_p$: the graph $\mathcal{G}_\ell(\mathbb{F}_p)$

Fix ℓ a small prime and p a large prime.

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

1. vertices: elliptic curves defined over $\mathbb{F}_p$, up to $\mathbb{F}_p$-isomorphism, (every j-invariant is there twice)
2. edges: ℓ-isogenies defined over $\mathbb{F}_p$.

Everything over $\mathbb{F}_p$: the graph $\mathcal{G}_\ell(\mathbb{F}_p)$

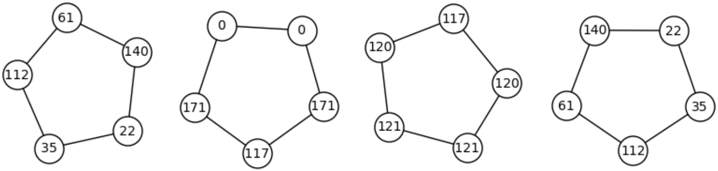
Fix ℓ a small prime and p a large prime.

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

1. vertices: elliptic curves defined over $\mathbb{F}_p$, up to $\mathbb{F}_p$-isomorphism, (every j-invariant is there twice)
2. edges: ℓ-isogenies defined over $\mathbb{F}_p$.

Example with $p = 179$ and $\ell = 3$

labels = j-invariants of the curves



Everything over $\mathbb{F}_p$: the graph $\mathcal{G}_\ell(\mathbb{F}_p)$

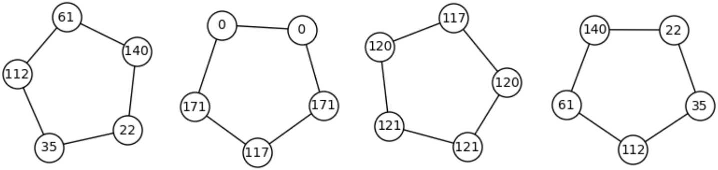
Fix ℓ a small prime and p a large prime.

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

1. vertices: elliptic curves defined over $\mathbb{F}_p$, up to $\mathbb{F}_p$-isomorphism, (every j-invariant is there twice)
2. edges: ℓ-isogenies defined over $\mathbb{F}_p$.

Example with $p = 179$ and $\ell = 3$

labels = j-invariants of the curves

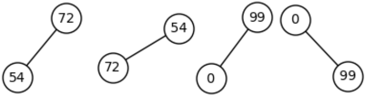


Any ℓ-isogeny graph $\mathcal{G}_\ell(\mathbb{F}_p)$ for $\ell > 2$ will be a union of cycles.

2-Isogenies: the graph $\mathcal{G}_2(\mathbb{F}_p)$

It depends on p mod 8:

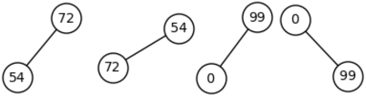
1. $p \equiv 1$ mod 4: bunch of edges



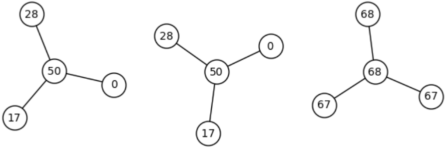
2-Isogenies: the graph $\mathcal{G}_2(\mathbb{F}_p)$

It depends on p mod 8:

1. $p \equiv 1 \bmod 4$: bunch of edges



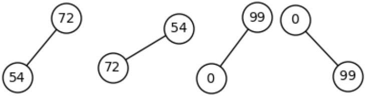
2. $p \equiv 3 \bmod 8$: claws



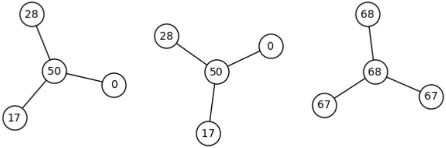
2-Isogenies: the graph $\mathcal{G}_2(\mathbb{F}_p)$

It depends on p mod 8:

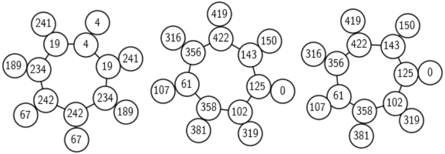
1. $p \equiv 1 \bmod 4$: bunch of edges



2. $p \equiv 3 \bmod 8$: claws



3. $p \equiv 7 \bmod 8$: volcanoes

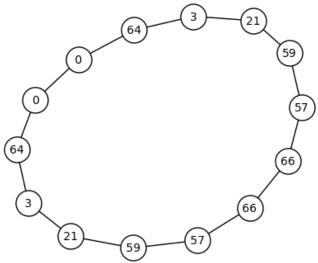


How to pass from $\mathcal{G}_\ell(\mathbb{F}_p)$ to the Spine $\mathcal{S}$

Two-step process

1. Identify vertices with the same j-invariant,
2. add edges that were not defined over $\mathbb{F}_p$.

For $\ell = 3$ and $p = 101$

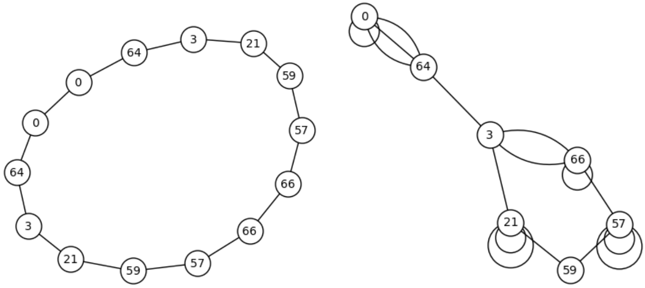


How to pass from $\mathcal{G}_\ell(\mathbb{F}_p)$ to the Spine $\mathcal{S}$

Two-step process

1. Identify vertices with the same j-invariant,
2. add edges that were not defined over $\mathbb{F}_p$.

For $\ell = 3$ and $p = 101$

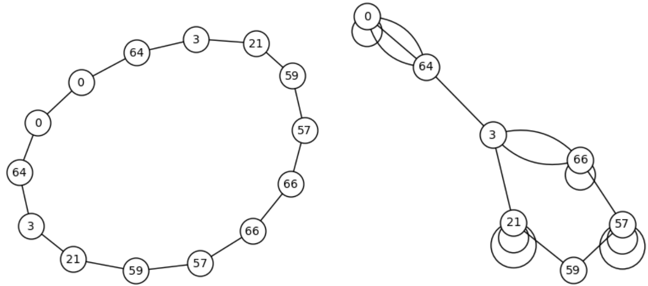


How to pass from $\mathcal{G}_\ell(\mathbb{F}_p)$ to the Spine $\mathcal{S}$

Two-step process

1. Identify vertices with the same j-invariant,
2. add edges that were not defined over $\mathbb{F}_p$.

For $\ell = 3$ and $p = 101$

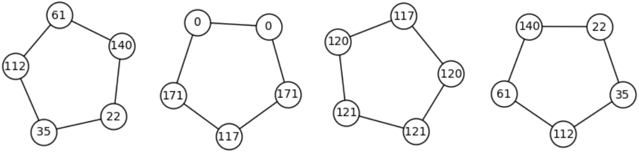


Lemma

Whenever we add an edge that does not correspond to an isogeny defined over $\mathbb{F}_p$, we get a double edge.

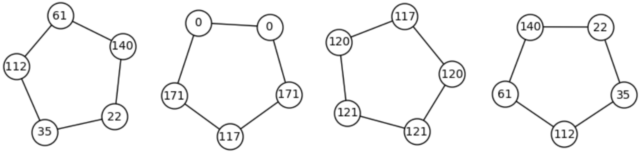
Neighbours

$\mathcal{G}_\ell(\mathbb{F}_p)$ for $p = 179, \ell = 3$



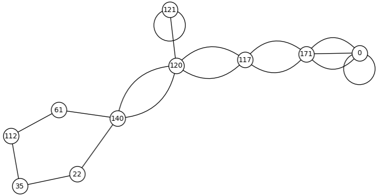
Neighbours

$\mathcal{G}_\ell(\mathbb{F}_p)$ for $p = 179, \ell = 3$



The Neighbour Lemma

Whenever the two vertices in $\mathcal{G}_\ell(\mathbb{F}_p)$ with j-invariant a do not have the same neighbours, there is a double edge from a in $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$.



Double edges using modular polynomials

Proposition

There exists a polynomial $\mathrm{Res}_\ell(X)$ of degree bounded by $2\ell(2\ell-1)$ such that there is a double edge from j in $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ if and only if $\mathrm{Res}_\ell(j) = 0$.

Double edges using modular polynomials

Proposition

There exists a polynomial $\mathrm{Res}_\ell(X)$ of degree bounded by $2\ell(2\ell-1)$ such that there is a double edge from j in $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ if and only if $\mathrm{Res}_\ell(j)=0$.

$\ell = 2$

There is a double edge from j if and only if it is a root of

$$\begin{aligned}\mathrm{Res}_2(X) = & -2^2 \cdot X^2 \cdot (X-1728) \cdot (X+3375)^2 \\ & \cdot (X^2 + 191025X - 121287375)^2\end{aligned}$$

This is a product of Hilbert class polynomials: whether the roots exist or don't depends on a congruence class of p!

Double edges using modular polynomials

Proposition

There exists a polynomial $\mathrm{Res}_\ell(X)$ of degree bounded by $2\ell(2\ell-1)$ such that there is a double edge from j in $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ if and only if $\mathrm{Res}_\ell(j)=0$.

$\ell = 2$

There is a double edge from j if and only if it is a root of

$$\begin{aligned}\mathrm{Res}_2(X) = &- 2^2 \cdot X^2 \cdot (X-1728)\cdot(X+3375)^2 \\ &\cdot (X^2+191025X-121287375)^2\end{aligned}$$

This is a product of Hilbert class polynomials: whether the roots exist or don't depends on a congruence class of p!

1. $p \equiv 1 \bmod 4$ then $j = 1728$ is not a supersingular j-invariant,
2. $p \equiv 1 \bmod 3$ then $j = 0$ is not a supersingular j-invariant, ...

Works the same for any ℓ.

Main theorem for $\ell = 2$

Stacking, folding, attaching for $\ell = 2$

Let $V \subset \mathcal{G}_2(\mathbb{F}_p)$ be a connected component.

Main theorem for $\ell = 2$

Stacking, folding, attaching for $\ell = 2$

Let $V \subset \mathcal{G}_2(\mathbb{F}_p)$ be a connected component.

1. If V does not contain 1728 or $j = 8000$, then there exists a connected component $W \subset \mathcal{G}_2(\mathbb{F}_p)$ with $V \neq W$ and identical labels. (*Stacking*)

Main theorem for $\ell = 2$

Stacking, folding, attaching for $\ell = 2$

Let $V \subset \mathcal{G}_2(\mathbb{F}_p)$ be a connected component.

1. If V does not contain 1728 or $j = 8000$, then there exists a connected component $W \subset \mathcal{G}_2(\mathbb{F}_p)$ with $V \neq W$ and identical labels. (*Stacking*)
2. For $j = 1728$ or 8000, there is only one connected component V containing both vertices j and this component is symmetric:

Main theorem for $\ell = 2$

Stacking, folding, attaching for $\ell = 2$

Let $V \subset \mathcal{G}_2(\mathbb{F}_p)$ be a connected component.

1. If V does not contain 1728 or $j = 8000$, then there exists a connected component $W \subset \mathcal{G}_2(\mathbb{F}_p)$ with $V \neq W$ and identical labels. (*Stacking*)
2. For $j = 1728$ or 8000, there is only one connected component V containing both vertices j and this component is symmetric: *(Folding)*

Main theorem for $\ell = 2$

Stacking, folding, attaching for $\ell = 2$

Let $V \subset \mathcal{G}_2(\mathbb{F}_p)$ be a connected component.

1. If V does not contain 1728 or $j = 8000$, then there exists a connected component $W \subset \mathcal{G}_2(\mathbb{F}_p)$ with $V \neq W$ and identical labels. (*Stacking*)
2. For $j = 1728$ or 8000, there is only one connected component V containing both vertices j and this component is symmetric: *(Folding)*
   2.1 it is either an edge $(8000, 8000)$,

Main theorem for $\ell = 2$

Stacking, folding, attaching for $\ell = 2$

Let $V \subset \mathcal{G}_2(\mathbb{F}_p)$ be a connected component.

1. If V does not contain 1728 or $j = 8000$, then there exists a connected component $W \subset \mathcal{G}_2(\mathbb{F}_p)$ with $V \neq W$ and identical labels. (*Stacking*)
2. For $j = 1728$ or 8000, there is only one connected component V containing both vertices j and this component is symmetric: *(Folding)*
    2.1 it is either an edge $(8000, 8000)$,
    2.2 a claw with 1728 on the surface and as one leaf, with the remaining leaves having the same label,

Main theorem for $\ell = 2$

Stacking, folding, attaching for $\ell = 2$

Let $V \subset \mathcal{G}_2(\mathbb{F}_p)$ be a connected component.

1. If V does not contain 1728 or $j = 8000$, then there exists a connected component $W \subset \mathcal{G}_2(\mathbb{F}_p)$ with $V \neq W$ and identical labels. (*Stacking*)
2. For $j = 1728$ or 8000, there is only one connected component V containing both vertices j and this component is symmetric: *(Folding)*
   2.1 it is either an edge $(8000, 8000)$,
   2.2 a claw with 1728 on the surface and as one leaf, with the remaining leaves having the same label,
   2.3 a volcano of depth 2 with 1728 on the surface and an edge $(8000, 8000)$ on the other side of the cycle on the surface, with identical paths from 1728 to 8000 from either side of the cycle.

Main theorem for $\ell = 2$

Stacking, folding, attaching for $\ell = 2$

Let $V \subset \mathcal{G}_2(\mathbb{F}_p)$ be a connected component.

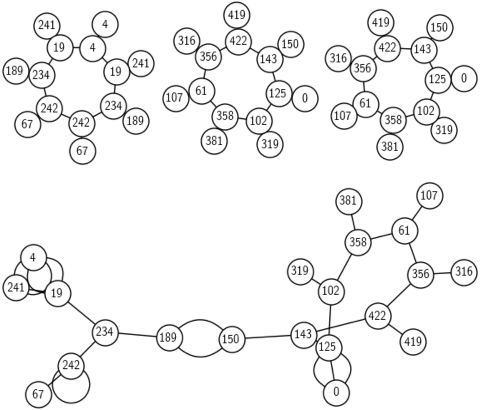
1. If V does not contain 1728 or $j = 8000$, then there exists a connected component $W \subset \mathcal{G}_2(\mathbb{F}_p)$ with $V \neq W$ and identical labels. (*Stacking*)
2. For $j = 1728$ or 8000, there is only one connected component V containing both vertices j and this component is symmetric: *(Folding)*
   - 2.1 it is either an edge $(8000, 8000)$,
   - 2.2 a claw with 1728 on the surface and as one leaf, with the remaining leaves having the same label,
   - 2.3 a volcano of depth 2 with 1728 on the surface and an edge $(8000, 8000)$ on the other side of the cycle on the surface, with identical paths from 1728 to 8000 from either side of the cycle.
3. At most one pair of vertices admits a new double edge. (*attaching.*)

Example for $\ell = 2$ and $p = 431$

Example

The graph above is $\mathcal{G}_2(\mathbb{F}_p)$ and the graph below is the spine in $\mathcal{G}_2(\overline{\mathbb{F}}_p)$.

We have
$1728 \bmod 431 = 4$
$8000 \bmod 431 = 242$
and 189 and 150 are the two roots of the polynomial $(X^2 + 191025X - 121287375)$ that we saw as a factor of $\mathrm{Res}_2(X)$.



Summary of what the Spine looks like for $\ell = 2$

The $\mathbb{F}_p$-subgraph $\mathcal{S} \subset \mathcal{G}_2(\overline{\mathbb{F}}_p)$:

1. for $p \equiv 1 \bmod 4$, we see single edges, with a possible vertex with a loop at $j = 8000$ and one possible component of size 4,
2. for $p \equiv 3 \bmod 8$, we see claws, with one claw collapsed to an edge ($j = 1728$), and a possible pair of claws joined by a double edge,
3. for $p \equiv 7 \bmod 8$, we see volcanoes, one of the volcanoes will be collapsed and possibly two volcanoes will get attached by a double edge to form a large component.

Why we call the Spine the Spine:

The finite field $\mathbb{F}_{p^2}$ has an involution: every j is sent to

$$j \mapsto j^p.$$

(we always have $j = j^{p^2} = (j^p)^p$).

Why we call the Spine the Spine:

The finite field $\mathbb{F}_{p^2}$ has an involution: every j is sent to

$$j \mapsto j^p.$$

(we always have $j = j^{p^2} = (j^p)^p$).

This extends to edges of $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$: if there is an edge (j, j') then we also have an edge $(j^p, (j')^p)$.

Why we call the Spine the Spine:

The finite field $\mathbb{F}_{p^2}$ has an involution: every j is sent to

$$j \mapsto j^p.$$

(we always have $j = j^{p^2} = (j^p)^p$).

This extends to edges of $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$: if there is an edge (j, j') then we also have an edge $(j^p, (j')^p)$.

The spine $\mathcal{S}$ is precisely the fixed set under this involution.

Why we call the Spine the Spine:

The finite field $\mathbb{F}_{p^2}$ has an involution: every j is sent to

$$j \mapsto j^p.$$

(we always have $j = j^{p^2} = (j^p)^p$).

This extends to edges of $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$: if there is an edge (j, j') then we also have an edge $(j^p, (j')^p)$.

The spine $\mathcal{S}$ is precisely the fixed set under this involution. We can build the graph starting from the spine and adding vertices j, j^p in pairs.

Why we call the Spine the Spine:

The finite field $\mathbb{F}_{p^2}$ has an involution: every j is sent to

$$j \mapsto j^p.$$

(we always have $j = j^{p^2} = (j^p)^p$).

This extends to edges of $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$: if there is an edge (j, j') then we also have an edge $(j^p, (j')^p)$.

The spine $\mathcal{S}$ is precisely the fixed set under this involution. We can build the graph starting from the spine and adding vertices j, j^p in pairs.
How accurate is this picture?

How central is the Spine?

Opposite vertices

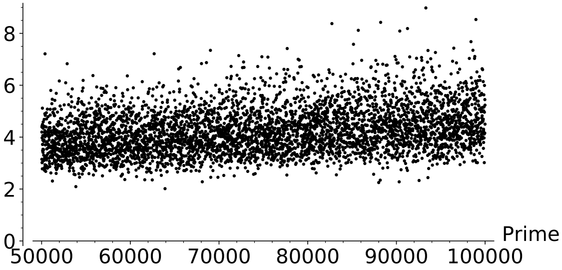
We say that j and j' are opposite vertices if the shortest path between j and j' passes through the spine.

How central is the Spine?

Opposite vertices

We say that j and j' are opposite vertices if the shortest path between j and j' passes through the spine.

Ratios of the number of opposite conjugate pairs (pairs j, j^p) to opposite arbitrary pairs. $(\ell = 2)$

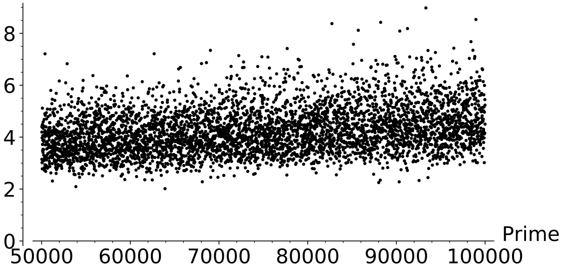


How central is the Spine?

Opposite vertices

We say that j and j' are opposite vertices if the shortest path between j and j' passes through the spine.

Ratios of the number of opposite conjugate pairs (pairs j, j^p) to opposite arbitrary pairs. ($\ell = 2$)



Conclusion: the spine is not in the *middle* of the graph.

Distances to the spine

Since the spine is a subgraph of size $\approx \sqrt{p}$, folklore is that we will reach the spine in approximately $\frac{1}{2}\log(p)$ steps.

Distances to the spine

Since the spine is a subgraph of size $\approx \sqrt{p}$, folklore is that we will reach the spine in approximately $\frac{1}{2}\log(p)$ steps.

More precisely, $\log_2(|\mathcal{G}_2(\overline{\mathbb{F}}_p)|/|\mathcal{S}|)$ is the expected distance to the spine from a random vertex.

Distances to the spine

Since the spine is a subgraph of size $\approx \sqrt{p}$, folklore is that we will reach the spine in approximately $\frac{1}{2}\log(p)$ steps.

More precisely, $\log_2(|\mathcal{G}_2(\overline{\mathbb{F}}_p)|/|\mathcal{S}|)$ is the expected distance to the spine from a random vertex.

We look at:

$$d_p = (\text{average distance to } \mathcal{S} \text{ for prime } p)/\log_2(|\mathcal{G}_2(\overline{\mathbb{F}}_p)|/|\mathcal{S}|)$$

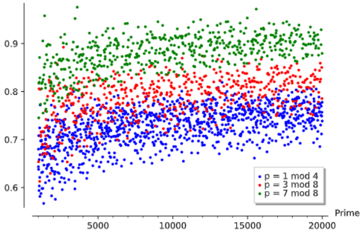
Distances to the spine

Since the spine is a subgraph of size $\approx \sqrt{p}$, folklore is that we will reach the spine in approximately $\frac{1}{2}\log(p)$ steps.

More precisely, $\log_2(|\mathcal{G}_2(\overline{\mathbb{F}}_p)|/|\mathcal{S}|)$ is the expected distance to the spine from a random vertex.

We look at:

$$d_p = (\text{average distance to } \mathcal{S} \text{ for prime } p)/\log_2(|\mathcal{G}_2(\overline{\mathbb{F}}_p)|/|\mathcal{S}|)$$



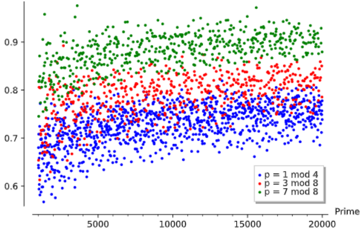
Distances to the spine

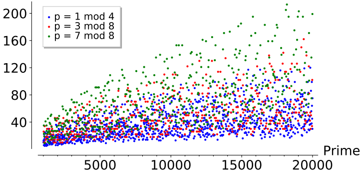
Since the spine is a subgraph of size $\approx \sqrt{p}$, folklore is that we will reach the spine in approximately $\frac{1}{2}\log(p)$ steps.

More precisely, $\log_2(|\mathcal{G}_2(\overline{\mathbb{F}}_p)|/|\mathcal{S}|)$ is the expected distance to the spine from a random vertex.

We look at:

$$d_p = (\text{average distance to } \mathcal{S} \text{ for prime } p)/\log_2(|\mathcal{G}_2(\overline{\mathbb{F}}_p)|/|\mathcal{S}|)$$





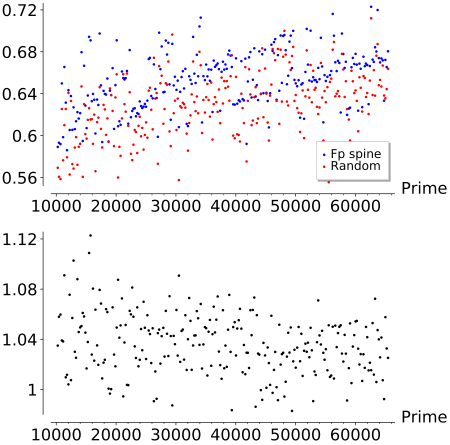
d_p for primes p mod 8

size of $\mathcal{S}$ for p mod 8.

Distances of components for $\ell = 2$ and $p \equiv 1 \bmod 4$

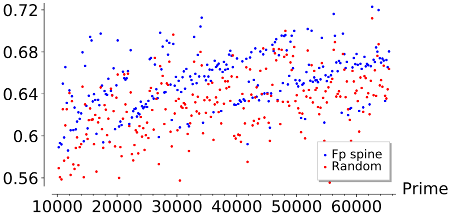
Normalized (by the diameter) distance between $\mathcal{S}$ components (blue) and random pairs (red)

Ratio of distances between components and the distances between random pairs

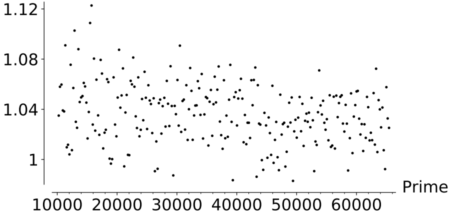


Distances of components for $\ell = 2$ and $p \equiv 1 \bmod 4$

Normalized (by the diameter) distance between $\mathcal{S}$ components (blue) and random pairs (red)



Ratio of distances between components and the distances between random pairs



Why is the distance of the edges between $\mathbb{F}_p$ vertices larger than the distance of random vertices?

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

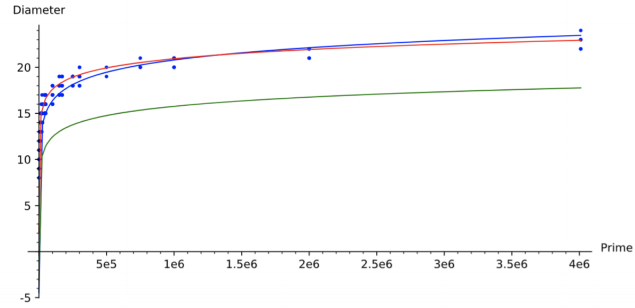


Figure 6.1: *Diameters of 2-isogeny graph over* $\overline{\mathbb{F}}_p$*, with* $y = \log_2(p/12) + \log_2(12) + 1$ *(red) and* $y = \frac{4}{3}\log_2(p/12) - 1$ *(blue).*

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

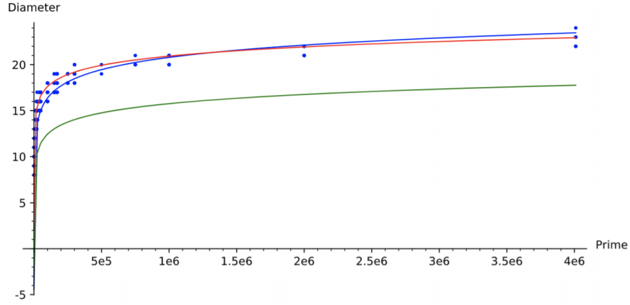


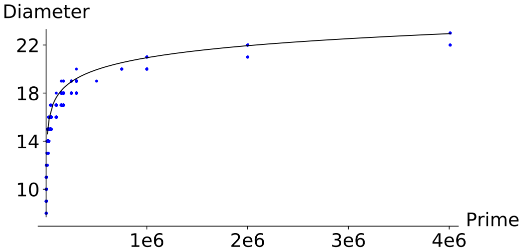
Figure 6.1: *Diameters of 2-isogeny graph over* $\overline{\mathbb{F}}_p$*, with* $y = \log_2(p/12) + \log_2(12) + 1$ *(red) and* $y = \frac{4}{3}\log_2(p/12) - 1$ *(blue).*

- Blue line: similar to LPS graphs (Lubotzky-Phillips-Sarnak)
- Red line: similar to random Ramanujan graphs

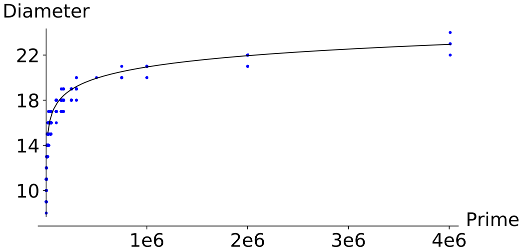
Diameters modulo 12

The line is $y = \log_2(p/12) + \log_2(12) + 1$.

$p \equiv$
$1, 7 \bmod 12$



$p \equiv$
$5, 11 \bmod 12$



Not just a picture

average diameter for $100,000 < p < 300,000$			
1 mod 12	17.2190476190476	5 mod 12	17.8761061946903
7 mod 12	17.7346938775510	11 mod 12	17.9919354838710
average diameter for $300,000 < p < 500,000$			
1 mod 12	18.4000000000000	5 mod 12	18.9230769230769
7 mod 12	18.8235294117647	11 mod 12	19.1000000000000

Average diameters sorted by primes modulo 12. The first data set contains around 100 primes in each congruence class, the latter between 10 to 17 primes.

Trends Modulo 12

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

- smaller 2-isogeny graph diameters,
- spine as disconnected as possible,
- fewer vertices in the spine.

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

- larger 2-isogeny graph diameters,
- fewer (but larger) connected components in the spine,
- more vertices in the spine.

Thank you for your attention!

For more, go to: eprint 2019/1056