Structure of Supersingular Elliptic Curve Isogeny Graphs

Renate Scheidler

UNIVERSITY OF CALGARY

Joint work with **Sarah Arpin** (Virginia Tech) and **Taha Hedayat** (U Calgary)

(arXiv:2502.03613v2 [math.NT]; to appear at LuCaNT 2025 Proceedings)

René 25
Université de la Polynèsie Française
Puna'auia, Tahiti, French Polynesia
August 18, 2025

The Dream Team

Happy 35^{th} Birthday, René!

Motivation

Why study supersingular elliptic curve isogeny graphs? 

Motivation

Why study supersingular elliptic curve isogeny graphs? 

- Interesting math, e.g. point counting (Fouquet-Morain 2002)

Motivation

Why study supersingular elliptic curve isogeny graphs? 

- Interesting math, e.g. point counting (Fouquet-Morain 2002)
- Post-quantum crypto (Charles-Goren-Lauter 2009, De Feo-Kohel-Leroux-Petit-Wesolowski 2020, De Feo-Fouotsa-Kutas-Leroux-Merz-Panny-Wesolowski 2023 etc.)

Motivation

UNIVERSITY OF CALGARY

Why study supersingular elliptic curve isogeny graphs? 

- Interesting math, e.g. point counting (Fouquet-Morain 2002)
- Post-quantum crypto (Charles-Goren-Lauter 2009, De Feo-Kohel-Leroux-Petit-Wesolowski 2020, De Feo-Fouotsa-Kutas-Leroux-Merz-Panny-Wesolowski 2023 etc.)
  - Hidden structures in these graphs could serve as attack vectors, resulting in security weaknesses in these systems
  - In fact, cryptographers typically assert that the behave "randomly"

Motivation

UNIVERSITY OF CALGARY

Why study supersingular elliptic curve isogeny graphs? 

- Interesting math, e.g. point counting (Fouquet-Morain 2002)
- Post-quantum crypto (Charles-Goren-Lauter 2009, De Feo-Kohel-Leroux-Petit-Wesolowski 2020, De Feo-Fouotsa-Kutas-Leroux-Merz-Panny-Wesolowski 2023 etc.)
    - Hidden structures in these graphs could serve as attack vectors, resulting in security weaknesses in these systems
    - In fact, cryptographers typically assert that the behave "randomly"

Our work herein analyzes some of the structure of

- supersingular elliptic curve isogeny graphs
- their subgraphs induced by the $\mathbb{F}_p$-vertices (the *spine*)

Supersingular Isogeny Graphs

For primes $\ell \neq p$, define the ℓ-isogeny graph $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ as follows:

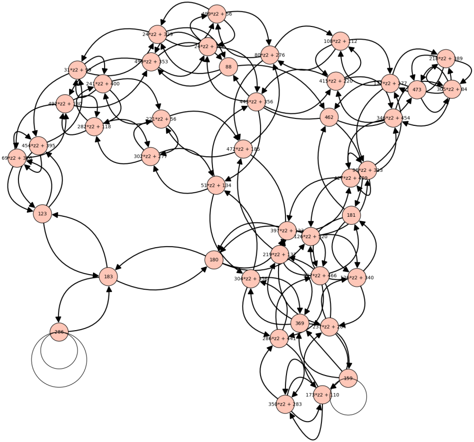
- *Vertices*: $\overline{\mathbb{F}}_p$-isomorphism classes (i.e. j-invariants) of curves
- *Edges*: ℓ-isogenies over $\overline{\mathbb{F}}_p$ (more or less)

Supersingular Isogeny Graphs

For primes $\ell \neq p$, define the ℓ-isogeny graph $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ as follows:

- *Vertices*: $\overline{\mathbb{F}}_p$-isomorphism classes (i.e. j-invariants) of curves
- *Edges*: ℓ-isogenies over $\overline{\mathbb{F}}_p$ (more or less)

Example: $\mathcal{G}_2(\overline{\mathbb{F}}_{523})$



Connection to Cryptography

Supersingular ℓ-Isogeny Path Finding Problem

Given two supersingular elliptic curves E, E', find a path from E to E' in $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$.

Connection to Cryptography

UNIVERSITY OF CALGARY

Supersingular ℓ-Isogeny Path Finding Problem

Given two supersingular elliptic curves E, E', find a path from E to E' in $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$.

Basis for the security of the aforementioned supersingular isogeny based cryptosystems.

In practice, the path contains a sub-path of $\mathbb{F}_p$-vertices.

Motivates the study of structural properties of the spine of $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$.

Isomorphic Supersingular Elliptic Curves

Every $\overline{\mathbb{F}}_p$-isomorphism class of supersingular elliptic curves has a representative defined over $\mathbb{F}_{p^2}$

- Some are defined over $\mathbb{F}_p$

Isomorphic Supersingular Elliptic Curves

Every $\overline{\mathbb{F}}_p$-isomorphism class of supersingular elliptic curves has a representative defined over $\mathbb{F}_{p^2}$

- Some are defined over $\mathbb{F}_p$

Every isogeny between supersingular elliptic curves is defined over $\mathbb{F}_{p^2}$

- Some are defined over $\mathbb{F}_p$

Isomorphic Supersingular Elliptic Curves

Every $\overline{\mathbb{F}}_p$-isomorphism class of supersingular elliptic curves has a representative defined over $\mathbb{F}_{p^2}$

- Some are defined over $\mathbb{F}_p$

Every isogeny between supersingular elliptic curves is defined over $\mathbb{F}_{p^2}$

- Some are defined over $\mathbb{F}_p$

Curves defined over $\mathbb{F}_p$ that are non-isomorphic over $\mathbb{F}_p$ can become isomorphic over $\mathbb{F}_{p^2}$:

- Example – quadratic twists: for $t^2 \in \mathbb{F}_p$, the curves

$$E : y^2 = x^3 + Ax + B \quad \text{and} \quad E_t : y^2 = x^3 + At^4x + Bt^6$$

are defined over $\mathbb{F}_p$ and isomorphic over $\mathbb{F}_{p^2}$ via $(x, y) \mapsto (t^2x, t^3y)$.

Isomorphic Supersingular Elliptic Curves

UNIVERSITY OF CALGARY

Every $\overline{\mathbb{F}}_p$-isomorphism class of supersingular elliptic curves has a representative defined over $\mathbb{F}_{p^2}$

- Some are defined over $\mathbb{F}_p$

Every isogeny between supersingular elliptic curves is defined over $\mathbb{F}_{p^2}$

- Some are defined over $\mathbb{F}_p$

Curves defined over $\mathbb{F}_p$ that are non-isomorphic over $\mathbb{F}_p$ can become isomorphic over $\mathbb{F}_{p^2}$:

- Example – quadratic twists: for $t^2 \in \mathbb{F}_p$, the curves

$$E : y^2 = x^3 + Ax + B \quad \text{and} \quad E_t : y^2 = x^3 + At^4x + Bt^6$$

  are defined over $\mathbb{F}_p$ and isomorphic over $\mathbb{F}_{p^2}$ via $(x, y) \mapsto (t^2x, t^3y)$. They are isomorphic over $\mathbb{F}_p$ if and only if $t \in \mathbb{F}_p$.

Graphs from Supersingular Isogenies

For primes $\ell \neq p$, we consider three graphs:

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

- *Vertices*: $\overline{\mathbb{F}}_p$-isomorphism classes (i.e. j-invariants) of supersingular elliptic curves over $\mathbb{F}_{p^2}$
- *Edges*: ℓ-isogenies* over $\overline{\mathbb{F}}_p$

*Up to post-composition by an automorphism over $\overline{\mathbb{F}}_p$

Graphs from Supersingular Isogenies

UNIVERSITY OF CALGARY

For primes $\ell \neq p$, we consider three graphs:

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

- *Vertices*: $\overline{\mathbb{F}}_p$-isomorphism classes (i.e. j-invariants) of supersingular elliptic curves over $\mathbb{F}_{p^2}$
- *Edges*: ℓ-isogenies* over $\overline{\mathbb{F}}_p$

Spine $\mathcal{S}_\ell^p \subset \mathcal{G}_\ell(\overline{\mathbb{F}}_p)$: subgraph induced by vertices in $\mathbb{F}_p$

- *Vertices*: $\overline{\mathbb{F}}_p$-isomorphism classes (i.e. j-invariants) of supersingular elliptic curves over $\mathbb{F}_p$
- *Edges*: ℓ-isogenies* **over** $\overline{\mathbb{F}}_p$ between these vertices

*Up to post-composition by an automorphism over $\overline{\mathbb{F}}_p$

Graphs from Supersingular Isogenies

UNIVERSITY OF CALGARY

For primes $\ell \neq p$, we consider three graphs:

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

- *Vertices*: $\overline{\mathbb{F}}_p$-isomorphism classes (i.e. j-invariants) of supersingular elliptic curves over $\mathbb{F}_{p^2}$
- *Edges*: ℓ-isogenies* over $\overline{\mathbb{F}}_p$

Spine $\mathcal{S}_\ell^p \subset \mathcal{G}_\ell(\overline{\mathbb{F}}_p)$: subgraph induced by vertices in $\mathbb{F}_p$

- *Vertices*: $\overline{\mathbb{F}}_p$-isomorphism classes (i.e. j-invariants) of supersingular elliptic curves over $\mathbb{F}_p$
- *Edges*: ℓ-isogenies* **over** $\overline{\mathbb{F}}_p$ between these vertices

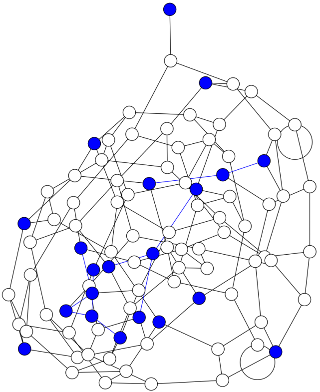
Restricted Supersingular ℓ-isogeny graph $\mathcal{G}_\ell(\mathbb{F}_p)$

- *Vertices*: $\mathbb{F}_p$-isomorphism classes (i.e. not necessarily distinct j-invariants) of supersingular elliptic curves **over** $\mathbb{F}_p$
- *Edges*: ℓ-isogenies **over** $\mathbb{F}_p$ between these vertices

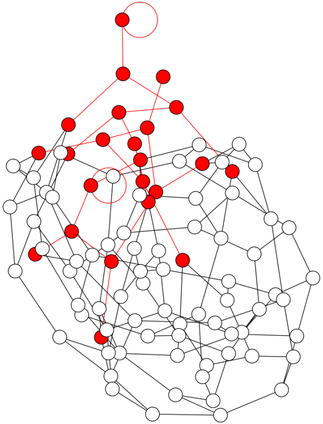
*Up to post-composition by an automorphism over $\overline{\mathbb{F}}_p$

Example: $p = 1103$, $\ell = 2$ (Courtesy Sotáková 2019)

A random graph of expected size in $\mathcal{G}_2(\overline{\mathbb{F}}_{1103})$



$\mathcal{S}_2^{1103}$

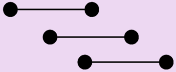
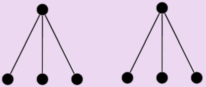
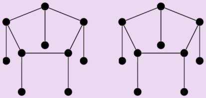


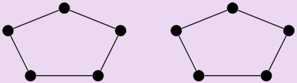
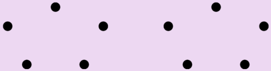
Structure of $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ (Kohel 1996)

- Connected with approximately $p/12$ vertices
- Optimal expander graph
- Every vertex has out-degree* $\ell + 1$
- Every vertex has in-degree $\ell + 1$ except 0 and 1728 which have smaller in-degree
- By identifying isogenies with their duals, $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ becomes an **undirected connected** graph that is $(\ell + 1)$-regular except in the neighbourhoods of vertices 0 and 1728.

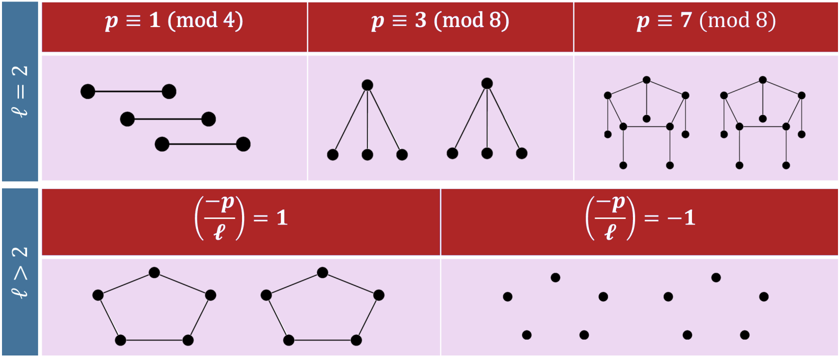
*Corresponding to the $\ell + 1$ subgroups of order ℓ of the ℓ-torsion $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ representing the kernels of the corresponding isogenies

Structure of $\mathcal{G}_\ell(\mathbb{F}_p)$ (Delfs & Galbraith 2013)

	$p \equiv 1 \pmod 4$	$p \equiv 3 \pmod 8$	$p \equiv 7 \pmod 8$
$\ell = 2$			

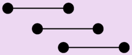
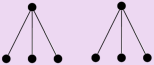
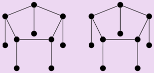
	$\left(\frac{-p}{\ell}\right) = 1$	$\left(\frac{-p}{\ell}\right) = -1$
$\ell > 2$		

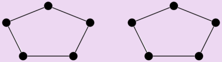
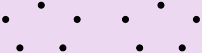
Structure of $\mathcal{G}_\ell(\mathbb{F}_p)$ (Delfs & Galbraith 2013)



Not quite .... doesn't characterize loops or multi-edges.

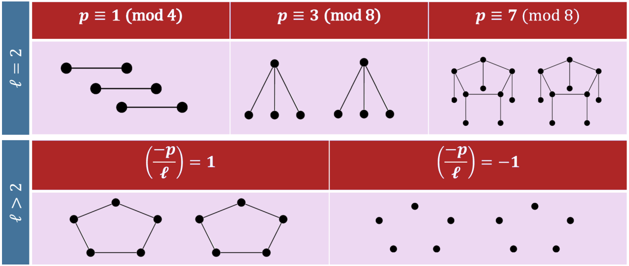
Structure of $\mathcal{G}_\ell(\mathbb{F}_p)$ (H-A-S 2015)

	$p \equiv 1 \pmod 4$	$p \equiv 3 \pmod 8$	$p \equiv 7 \pmod 8$
$\ell = 2$			

	$\left(\frac{-p}{\ell}\right) = 1$	$\left(\frac{-p}{\ell}\right) = -1$
$\ell > 2$		

Loops / Multi Edges	
ℓ	p
2	7
3	5, 11
5	11, 19
7	13, 19
11	13, 19, 43
13	17, 43
17	19, 43, 59, 67
⋮	⋮

Structure of $\mathcal{G}_\ell(\mathbb{F}_p)$ (H-A-S 2015)



Loops / Multi Edges	
ℓ	p
2	7
3	5, 11
5	11, 19
7	13, 19
11	13, 19, 43
13	17, 43
17	19, 43, 59, 67
⋮	⋮

Characterized by simple arithmetic conditions on ℓ and p.

Mapping $\mathcal{G}_\ell(\mathbb{F}_p)$ to $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$

$$\begin{array}{rcl} \mathbb{F}_p\text{-isomorphism classes} & \rightarrow & \overline{\mathbb{F}}_p\text{-isomorphism classes} \\ \mathbb{F}_p\text{-isogenies} & \rightarrow & \overline{\mathbb{F}}_p\text{-isogenies} \end{array}$$

Mapping $\mathcal{G}_\ell(\mathbb{F}_p)$ to $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$

$\mathbb{F}_p$-isomorphism classes $\rightarrow$ $\overline{\mathbb{F}}_p$-isomorphism classes

$\mathbb{F}_p$-isogenies $\rightarrow$ $\overline{\mathbb{F}}_p$-isogenies

What happens?

Mapping $\mathcal{G}_\ell(\mathbb{F}_p)$ to $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$

$$\mathbb{F}_p\text{-isomorphism classes} \rightarrow \overline{\mathbb{F}}_p\text{-isomorphism classes}$$
$$\mathbb{F}_p\text{-isogenies} \rightarrow \overline{\mathbb{F}}_p\text{-isogenies}$$

What happens?

- Pairs of vertices in $\mathcal{G}_\ell(\mathbb{F}_p)$ corresponding to quadratic twists merge into one vertex in $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$
- Isogenies defined over $\mathbb{F}_{p^2}$ but not $\mathbb{F}_p$ introduce new edges
- Disconnected components in $\mathcal{G}_\ell(\mathbb{F}_p)$ can merge into one component

Mapping $\mathcal{G}_\ell(\mathbb{F}_p)$ to $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$

$\mathbb{F}_p$-isomorphism classes $\rightarrow$ $\overline{\mathbb{F}}_p$-isomorphism classes

$\mathbb{F}_p$-isogenies $\rightarrow$ $\overline{\mathbb{F}}_p$-isogenies

What happens?

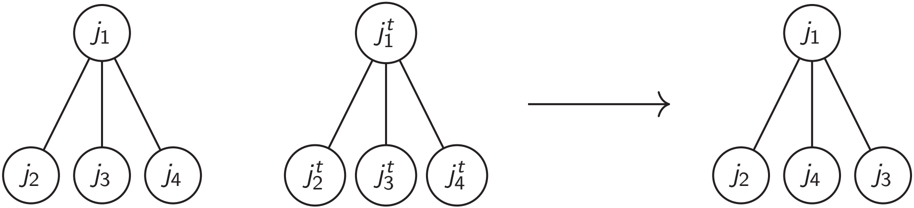
- Pairs of vertices in $\mathcal{G}_\ell(\mathbb{F}_p)$ corresponding to quadratic twists merge into one vertex in $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$
- Isogenies defined over $\mathbb{F}_{p^2}$ but not $\mathbb{F}_p$ introduce new edges
- Disconnected components in $\mathcal{G}_\ell(\mathbb{F}_p)$ can merge into one component

Theorem (Arpin, Camacho-Navarro, Lauter, Lim, Nelson, Scholl & Sotáková 2023)

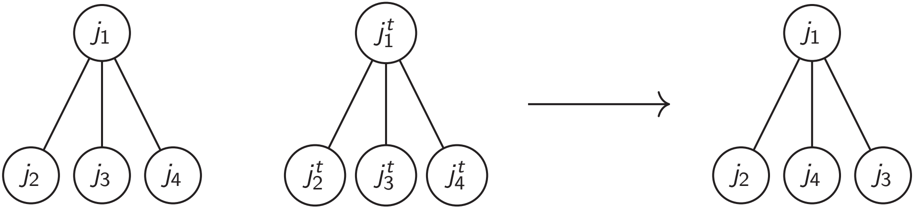
Mapping $\mathcal{G}_\ell(\mathbb{F}_p)$ to $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ happens in 4 ways:

- Stacking
- Folding
- Attachment at a vertex
- Attachment by a new edge

Stacking



Stacking



Stacking is the default. Almost everything stacks.

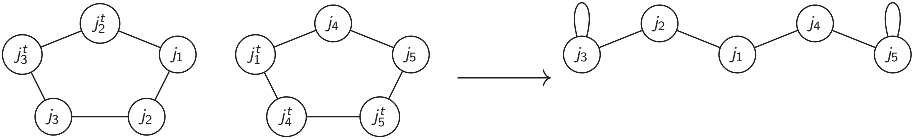
Folding

Folding

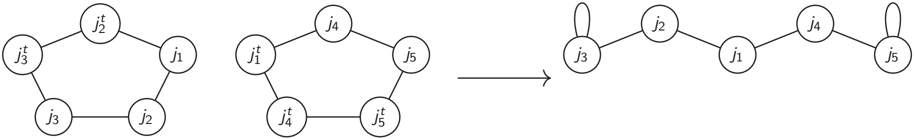
Folding and stacking are mutually exclusive.

For $\ell > 2$, only the two components of $\mathcal{G}_2(\mathbb{F}_p)$ containing 1728 fold.

Attachment at a Vertex



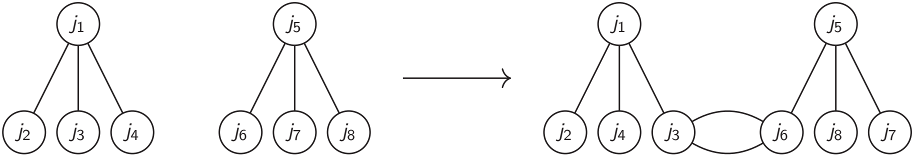
Attachment at a Vertex



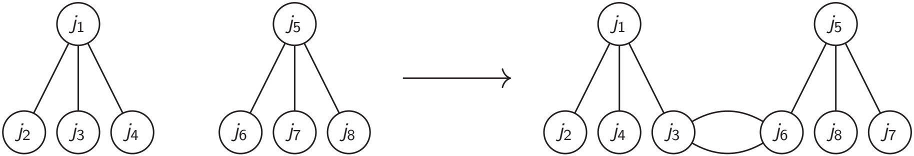
For $\ell = 2$, this does not happen.

For $\ell > 2$, the two folding components of $\mathcal{G}_2(\mathbb{F}_p)$ containing 1728 attach at 1728.

Attachment by a New Edge



Attachment by a New Edge



Two-for-one special: attaching edges come as double edges.

For $\ell = 2$, this happens at most once.

Mapping $\mathcal{G}_\ell(\mathbb{F}_p)$ to $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ (H-A-S 2025)

Explicitly characterized by congruence condition on

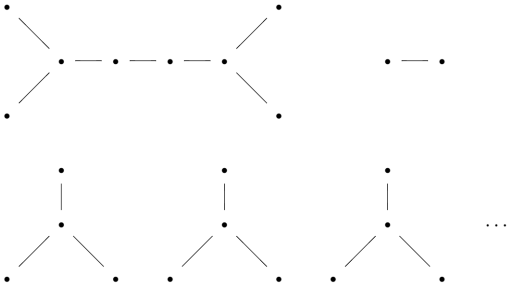
- $p \pmod{120}$ for $\ell = 2$
- $p \pmod{840}$ for $\ell = 3$

Mapping $\mathcal{G}_\ell(\mathbb{F}_p)$ to $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ (H-A-S 2025)

Explicitly characterized by congruence condition on

- $p \pmod{120}$ for $\ell = 2$
- $p \pmod{840}$ for $\ell = 3$

Case $\ell = 2$ and $p \equiv 11, 59 \pmod{120}$ with $p > 59$:



Mapping $\mathcal{G}_\ell(\mathbb{F}_p)$ to $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ (H-A-S 2025)

Explicitly characterized by congruence condition on

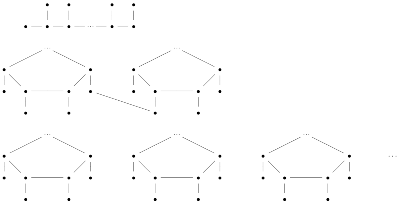
- $p \pmod{120}$ for $\ell = 2$ . . . *almost*
- $p \pmod{840}$ for $\ell = 3$

Mapping $\mathcal{G}_\ell(\mathbb{F}_p)$ to $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ (H-A-S 2025)

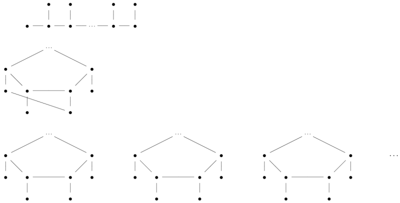
Explicitly characterized by congruence condition on

- $p \pmod{120}$ for $\ell = 2$ . . . *almost*
- $p \pmod{840}$ for $\ell = 3$

Case $\ell = 2$ and $p \equiv 71, 119 \pmod{120}$:



or

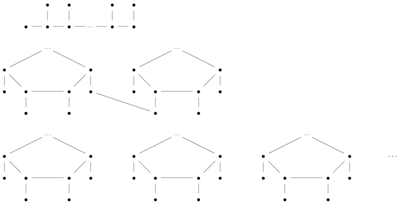


Mapping $\mathcal{G}_\ell(\mathbb{F}_p)$ to $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ (H-A-S 2025)

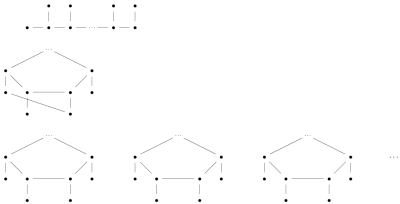
Explicitly characterized by congruence condition on

- $p \pmod{120}$ for $\ell = 2$ . . . *almost*
- $p \pmod{840}$ for $\ell = 3$

Case $\ell = 2$ and $p \equiv 71, 119 \pmod{120}$:



or



E.g. for $p = 71$ E.g. for $p = 1319$

Proof Ingredients

- ℓ-**th modular polynomial**: governs adjacency, including loops and multi-edges with multiplicities

Proof Ingredients

- **ℓ-th modular polynomial**: governs adjacency, including loops and multi-edges with multiplicities
- **Hilbert class polynomials**: governs endomorphism ring and supersingularity

Proof Ingredients

- **ℓ-th modular polynomial**: governs adjacency, including loops and multi-edges with multiplicities
- **Hilbert class polynomials**: governs endomorphism ring and supersingularity
- Supersingularity of 0 and 1728

Proof Ingredients

- **ℓ-th modular polynomial**: governs adjacency, including loops and multi-edges with multiplicities
- **Hilbert class polynomials**: governs endomorphism ring and supersingularity
- Supersingularity of 0 and 1728
- Occasional explicit isogeny computation (to see where they are defined)

Proof Ingredients

UNIVERSITY OF CALGARY

- ℓ**-th modular polynomial**: governs adjacency, including loops and multi-edges with multiplicities
- **Hilbert class polynomials**: governs endomorphism ring and supersingularity
- Supersingularity of 0 and 1728
- Occasional explicit isogeny computation (to see where they are defined)
- Going nuts with Chinese Remainder Theorem

Example: $\ell = 2$

$$\begin{aligned}\Phi_2(x,y) \;=\; & -x^2y^2 + x^3 + y^3 + 1488(x^2y + xy^2) \\ & - 162000(x^2 + y^2) + 40773375xy \\ & + 8748000000(x + y) - 157464000000000\end{aligned}$$

Example: $\ell = 2$

$$\begin{aligned}\Phi_2(x,y) &= -x^2y^2 + x^3 + y^3 + 1488(x^2y + xy^2) \\ &\quad - 162000(x^2 + y^2) + 40773375xy \\ &\quad + 8748000000(x + y) - 157464000000000\end{aligned}$$

$$\Phi_2(x,x) = -(x + 3375)^2(x - 1728)(x - 8000)$$

Two loops at j-invariant -3375, one loop each at 1728 and 8000

$$\begin{aligned}\Phi_2(x,y) \;=\; & -x^2y^2 + x^3 + y^3 + 1488(x^2y + xy^2) \\ & -162000(x^2+y^2) + 40773375xy \\ & +8748000000(x+y) - 157464000000000\end{aligned}$$

$$\Phi_2(x,x) \;=\; -(x+3375)^2(x-1728)(x-8000)$$

Two loops at j-invariant -3375, one loop each at 1728 and 8000

The resultant of Φ_2 and its derivative is

$$\mathrm{Res}_2(x) \;=\; -4H_{-3}(x)^2H_{-4}(x)H_{-7}(x)^2H_{-15}(x)^2 \text{ with}$$

$$H_{-3}(x) = x\;, \quad H_{-4}(x) = x - 1728\;, \quad H_{-7}(x) = x + 3375$$

$$H_{-15}(x) \;=\; x^2 + 191025x - 121287375$$

Example: $\ell = 2$

$$\begin{aligned}\Phi_2(x,y) &= -x^2y^2 + x^3 + y^3 + 1488(x^2y + xy^2)\\ &\quad - 162000(x^2+y^2) + 40773375xy\\ &\quad + 8748000000(x+y) - 157464000000000\end{aligned}$$

$$\Phi_2(x,x) = -(x+3375)^2(x-1728)(x-8000)$$

Two loops at j-invariant -3375, one loop each at 1728 and 8000

The resultant of Φ_2 and its derivative is

$$\mathrm{Res}_2(x) = -4H_{-3}(x)^2 H_{-4}(x) H_{-7}(x)^2 H_{-15}(x)^2 \text{ with}$$

$$H_{-3}(x) = x\ , \quad H_{-4}(x) = x - 1728\ , \quad H_{-7}(x) = x + 3375$$
$$H_{-15}(x) = x^2 + 191025x - 121287375$$

Double edges between 0, 1728, -3375 and the roots of $H_{-15}(x)$

For $\ell = 3$:

- The required Hilbert class polynomials for $D = -3, -4, -8, -11, -20, -32, -35$ are still all linear or quadratic

For $\ell = 3$:

- The required Hilbert class polynomials for $D = -3, -4, -8, -11, -20, -32, -35$ are still all linear or quadratic

For $\ell = 5$:

- Two of the required Hilbert class polynomials (for $D = -84, -96$) have degree 4 and are irreducible over $\mathbb{Z}$

$\mathcal{S}_\ell^p$ for $\ell > 2$

For $\ell = 3$:

- The required Hilbert class polynomials for $D = -3, -4, -8, -11, -20, -32, -35$ are still all linear or quadratic

For $\ell = 5$:

- Two of the required Hilbert class polynomials (for $D = -84, -96$) have degree 4 and are irreducible over $\mathbb{Z}$

For $\ell > 5$: 

Diameter of $\mathcal{S}_2^p$

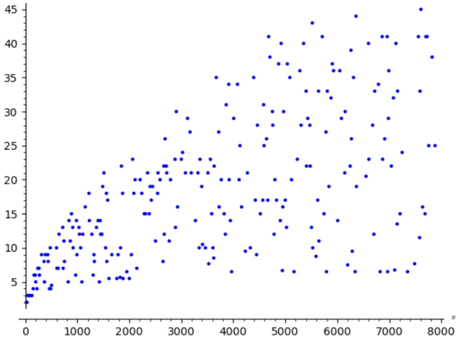
Diameters (lengths of longest directed path) of components of $\mathcal{S}_2^p$:

- $p \equiv 1 \pmod 4$ and $p \equiv 3 \pmod 8$: between 1 and 5
- $p \equiv 7 \pmod 8$ with $p \not\equiv 71, 119 \pmod{120}$: $(r+3)/2$ where r is order of the class of a prime $\mathbb{Z}[\sqrt{-p}]$-ideal above 2 in the class group
- $p \equiv 71, 119 \pmod{120}$: ???

UNIVERSITY OF CALGARY

Diameters (lengths of longest directed path) of components of $\mathcal{S}_2^p$:

- $p \equiv 1 \pmod 4$ and $p \equiv 3 \pmod 8$: between 1 and 5
- $p \equiv 7 \pmod 8$ with $p \not\equiv 71, 119 \pmod{120}$: $(r+3)/2$ where r is order of the class of a prime $\mathbb{Z}[\sqrt{-p}]$-ideal above 2 in the class group
- $p \equiv 71, 119 \pmod{120}$: ???



Mean component diameters in $\mathcal{S}_2^p$ for the first 250 primes $p \equiv 7 \pmod 8$

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

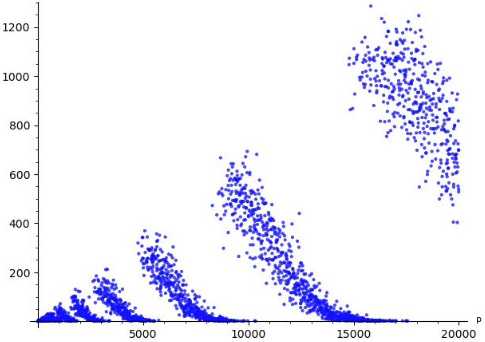
Radius: minimal length over all longest directed paths

Centre: collection of vertices for which the furthest distance to any other vertex is at most the radius

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

Radius: minimal length over all longest directed paths

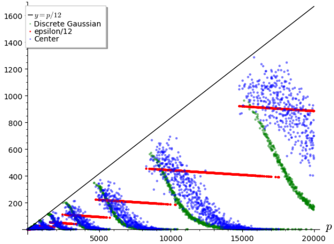
Centre: collection of vertices for which the furthest distance to any other vertex is at most the radius



Size of the center of $\mathcal{G}_2(\overline{\mathbb{F}}_p)$ for $5 \leq p \leq 20,000$

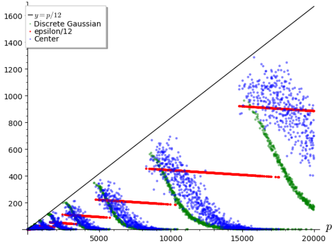
Picture for $\ell = 3$ is similar.

Centre Count Explained



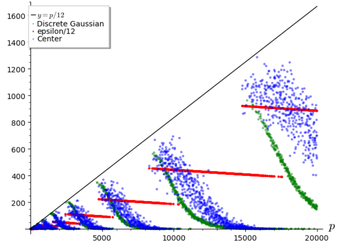
Centre Count Explained

UNIVERSITY OF CALGARY



- **Blue**: Centre size of $\mathcal{G}_2(\overline{\mathbb{F}}_p)$

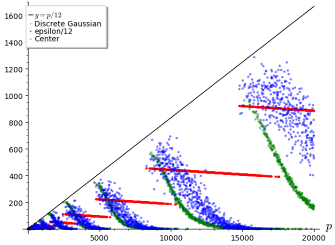
Centre Count Explained



- **Blue**: Centre size of $\mathcal{G}_2(\overline{\mathbb{F}}_p)$
- **Black**: $p/12$ (number of vertices in $\mathcal{G}_2(\overline{\mathbb{F}}_p)$)

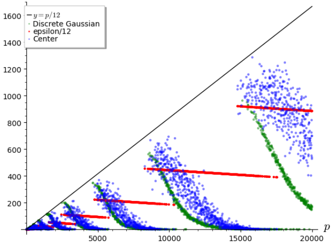
Centre Count Explained

UNIVERSITY OF CALGARY



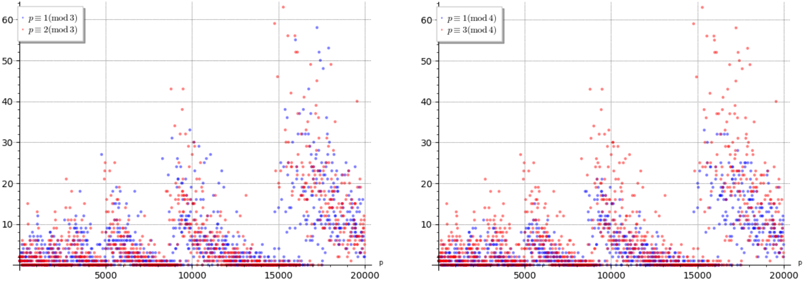
- **Blue**: Centre size of $\mathcal{G}_2(\overline{\mathbb{F}}_p)$
- **Black**: $p/12$ (number of vertices in $\mathcal{G}_2(\overline{\mathbb{F}}_p)$)
- **Green**: discrete Gauß sampling (mean $1.8\log(p)$, standard deviation 0.38) of longest path lengths for a 3-regular graph with $(p-1)/12$ vertices where $p \equiv 1 \pmod{12}$ (thank you, Jonathan Love!)

Centre Count Explained



- **Blue**: Centre size of $\mathcal{G}_2(\overline{\mathbb{F}}_p)$
- **Black**: $p/12$ (number of vertices in $\mathcal{G}_2(\overline{\mathbb{F}}_p)$)
- **Green**: discrete Gauß sampling (mean $1.8\log(p)$, standard deviation 0.38) of longest path lengths for a 3-regular graph with $(p-1)/12$ vertices where $p \equiv 1 \pmod{12}$ (thank you, Jonathan Love!)
- **Red**: discrepancy between the theoretically possible and the actual number of ways in which the furthest distance is at most the radius (thank you, Thomas Decru and Jonathan Komada Eriksen!)

UNIVERSITY OF CALGARY



Size of the center of $\mathcal{G}_2(\mathbb{F}_p)$ for $5 \leq p \leq 20,000$

$p \equiv 1 \pmod 3$ | $p \equiv 1 \pmod 4$
$p \equiv 2 \pmod 3$ | $p \equiv 3 \pmod 4$

Observations:

- Centre counts spread out across full range
- Higher centre counts for $p \equiv 3 \pmod 4$ (higher radius values)
- Similar wave pattern as $\mathcal{G}_2(\overline{\mathbb{F}}_p)$ despite Frobenius-conjugate paths

The End!

UNIVERSITY OF CALGARY

Merci! — Questions (ou Résponses)?