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]; conditionally accepted at LuCaNT 2025)

Arithmetic, Geometry, Cryptography and Coding Theory
CIRM Luminy, Marseille
June 10, 2025

Motivation

Why study supersingular elliptic curve isogeny graphs? 

- They have very interesting mathematical properties
- They form the basis of several post-quantum cryptographic systems (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

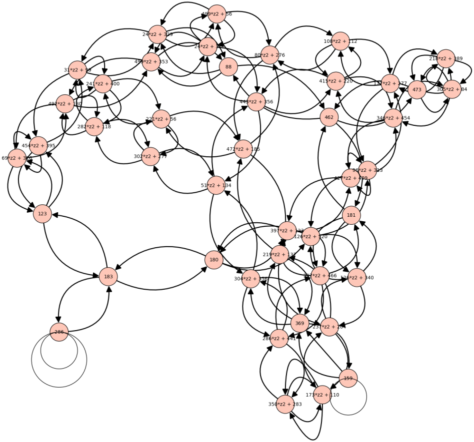
- supersingular elliptic curve isogeny graphs
- their subgraphs induced by the $\mathbb{F}_p$-vertices (the *spine*)

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)

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

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

In practice, the path endpoints are often $\mathbb{F}_p$-vertices.

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

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 $\overline{\mathbb{F}}_p$

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

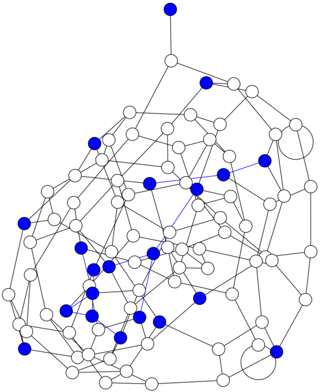
Restricted Supersingular ℓ-isogeny graph $\mathcal{G}_\ell(\mathbb{F}_p)$

- *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

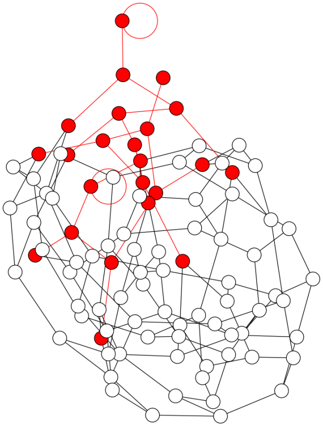
*Up to post-composition by an automorphism over $\overline{\mathbb{F}}_p$

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

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



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



Differences between $\mathcal{G}_\ell(\mathbb{F}_p)$ versus $\mathcal{S}_\ell^p$:

- $\mathcal{S}_\ell^p$ has half as many vertices as $\mathcal{G}_\ell(\mathbb{F}_p)$ because pairs of quadratic twists correspond to different vertices in $\mathcal{G}_\ell(\mathbb{F}_p)$ which merge in $\mathcal{S}_\ell^p$
- Non-adjacent vertices in $\mathcal{G}_\ell(\mathbb{F}_p)$ can become adjacent in $\mathcal{S}_\ell^p$ (if they are not ℓ-isogenous over $\mathbb{F}_p$ but ℓ-isogenous over $\mathbb{F}_{p^2}$)

The structures of $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ and $\mathcal{G}_\ell(\mathbb{F}_p)$ are well understood, but not $\mathcal{S}_\ell^p$.

- How exactly does $\mathcal{G}_\ell(\mathbb{F}_p)$ map into $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ when passing from isomorphism classes and isogenies over $\mathbb{F}_p$ to isomorphism classes and isogenies over $\mathbb{F}_{p^2}$, to become the spine $\mathcal{S}_\ell^p$?
  - Answered in this talk for $\ell = 2$ (also done for $\ell = 3$)
- Connectivity properties of $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ and of $\mathcal{S}_\ell^p$ located inside $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$
  - Presented in this talk for $\ell = 2$

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 $\mathcal{G}_\ell(\mathbb{F}_p)$, $\ell > 2$ (Delfs & Galbraith 2013)

Let $K = \mathbb{Q}(\sqrt{-p})$ and h_K the class number of K.

- Type 1 vertices have endomorphism ring $\mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$ (only for $p \equiv 3 \pmod 4$)
- Type 2 vertices have endomorphism ring $\mathbb{Z}[\sqrt{-p}]$

If ℓ is inert or ramified in K:

- No edges

If ℓ splits in K and $p \equiv 1 \pmod 4$:

- h_K vertices, all of type 2, that form a cycle*

If ℓ splits in K and $p \equiv 3 \pmod 4$:

- h_K type 1 vertices that form a cycle*
- h_K type 2 vertices that form a cycle*

*Cycles may be degenerate

Structure of $\mathcal{G}_2(\mathbb{F}_p)$ (Delfs & Galbraith 2013)

If $p \equiv 1 \pmod 4$:

- h_K vertices, all of type 2, that form a collection of edges

If $p \equiv 3 \pmod 8$:

- h_K vertices of type 1
- $3h_K$ vertices of type 2 that are joined three-to-one to the type 1 vertices (*claws* or *tripods*)

If $p \equiv 7 \pmod 8$:

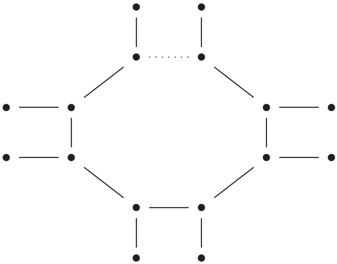
- h_K vertices of type 1 that form a cycle
- h_K vertices of type 2 that are joined one-to-one to the type 1 vertices

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

$p \equiv 1 \pmod 4$:

$p \equiv 3 \pmod 8$:

$p \equiv 7 \pmod 8$:



Mapping the components of $\mathcal{G}_\ell(\mathbb{F}_p)$ to become the spine $\mathcal{S}_\ell^p \subset \mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ is done by moving from isomorphism classes and ℓ-isogenies defined over $\mathbb{F}_p$ to isomorphism classes and ℓ-isogenies defined over $\mathbb{F}_{p^2}$:

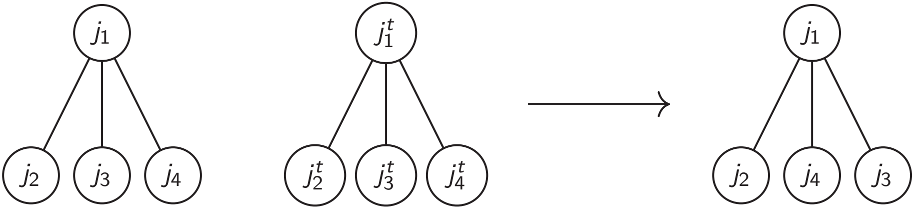
- Pairs of vertices in $\mathcal{G}_\ell(\mathbb{F}_p)$ corresponding to quadratic twists merge into one vertex in $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$
- Isogenies defined over $\mathbb{F}_{p^2}$ but not $\mathbb{F}_p$ introduce new edges
- Disconnected components in $\mathcal{G}_\ell(\mathbb{F}_p)$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

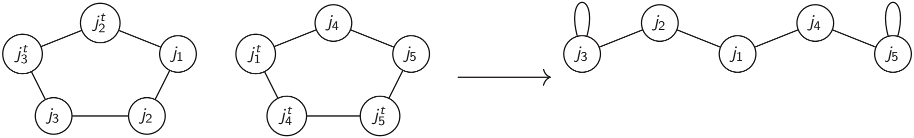
- Stacking
- Folding
- Attachment at a vertex
- Attachment by a new edge

Stacking

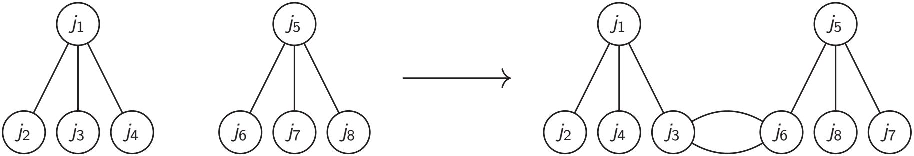


Folding

Attachment at a Vertex



Attachment by a New Edge



Theorem (Arpin, Hedayat, S. 2024)

Let $p \geq 17$ with $p \equiv 1 \pmod 4$. Then the transition $\mathcal{G}_2(\mathbb{F}_p) \to \mathcal{S}_2^p$ proceeds as follows:

- $p = 29$: the component containing $j = j^t = 8000$ folds and edge attaches to the other component.
- $p \equiv 29, 101 \pmod{120}$, $p \neq 29$: the component containing $j = j^t = 8000$ folds, all other components stack, two stacked components edge attach.
- $p \equiv 41, 89 \pmod{120}$: all components stack, and there is an edge attachment.
- $p \equiv 13, 37, 53, 61, 77, 109 \pmod{120}$: the component containing $j = j^t = 8000$ folds, all other components stack, no edge attachments.
- $p \equiv 1, 17, 49, 73, 97, 113 \pmod{120}$: all components stack, no edge attachments.

$\mathcal{G}_2(\mathbb{F}_p) \to \mathcal{S}_2^p$ for $p \equiv 3 \pmod 4$

UNIVERSITY OF CALGARY

Theorem (Arpin, Hedayat, S. 2024)

Let $p \geq 17$ with $p \equiv 3 \pmod 4$. Then the transition $\mathcal{G}_2(\mathbb{F}_p) \to \mathcal{S}_2^p$ proceeds as follows:

If $p \equiv 3 \pmod 8$, then the connected component containing $j = j^t = 1728$ always folds and we have the following:

- $p = 59$: the folded component gets edge attached to another component by an edge joining two type 2 vertices.
- $p \equiv 11, 59 \pmod{120}$ and $p \neq 11, 59$: two stacked components become edge attached by an edge joining two type 2 vertices.
- $p \equiv 19, 43, 67, 83, 91, 107 \pmod{120}$: no edge attachments.

If $p \equiv 7 \pmod 8$, then only the component containing $j = j^t = 1728$ and $j = j^t = 8000$ folds, and we have the following:

- $p \equiv 71, 119 \pmod{120}$: new double-edge in $\mathcal{S}_2^p$ incident with two type 2 vertices, which **may or may not** be an attachment.
- $p \equiv 7, 23, 31, 47, 79, 103 \pmod{120}$: no edge attachments.

Structure of $\mathcal{S}_2^p$ for $p \equiv 1 \pmod 4$

$p = 5$: $\bullet$

$p = 29$: $\bullet$ — $\bullet$ — $\bullet$

$p \equiv 29, 101 \pmod{120}$ and $p \neq 29$:

$\bullet$

$\bullet$ — $\bullet$ — $\bullet$ — $\bullet$

$\bullet$ — $\bullet$ $\quad$ $\bullet$ — $\bullet$ $\quad$ $\bullet$ — $\bullet$ $\quad$ $\bullet$ — $\bullet$ $\quad$ $\cdots$

Structure of $\mathcal{S}_2^p$ for $p \equiv 1 \pmod 4$ (contd)

$p \equiv 41, 89 \pmod{120}$:

$\bullet$ — $\bullet$ — $\bullet$ — $\bullet$

$\bullet$ — $\bullet$ $\quad$ $\bullet$ — $\bullet$ $\quad$ $\bullet$ — $\bullet$ $\quad$ $\bullet$ — $\bullet$ $\quad$ $\cdots$

$p \equiv 13, 37, 53, 61, 77, 109 \pmod{120}$:

$\bullet$

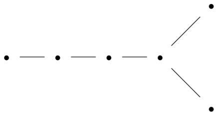
$\bullet$ — $\bullet$ $\quad$ $\bullet$ — $\bullet$ $\quad$ $\bullet$ — $\bullet$ $\quad$ $\bullet$ — $\bullet$ $\quad$ $\cdots$

$p \equiv 1, 17, 49, 73, 97, 113 \pmod{120}$:

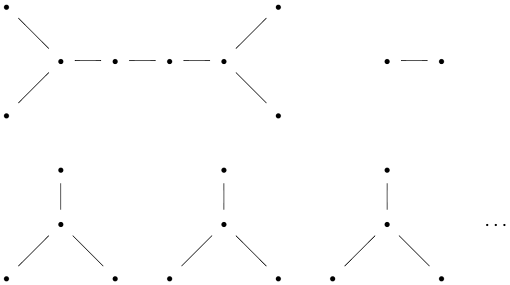
$\bullet$ — $\bullet$ $\quad$ $\bullet$ — $\bullet$ $\quad$ $\bullet$ — $\bullet$ $\quad$ $\bullet$ — $\bullet$ $\quad$ $\cdots$

Structure of $\mathcal{S}_2^p$ for $p \equiv 3 \pmod 8$

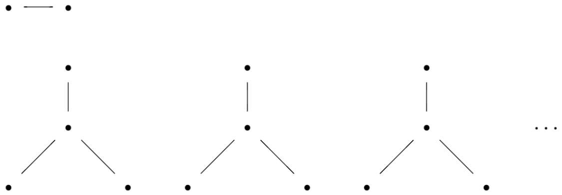
$p = 11$: 

$p = 59$: 

$p \equiv 11, 59 \pmod{120}$ and $p \neq 11, 59$:

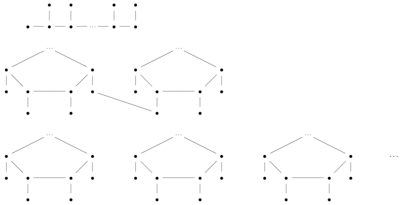


$p \equiv 19, 43, 67, 83, 91, 107 \pmod{120}$:

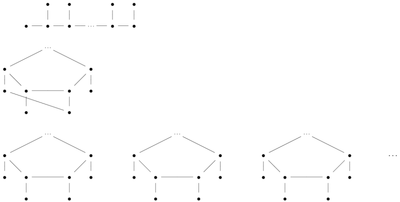


Structure of $\mathcal{S}_2^p$ for $p \equiv 7 \pmod 8$

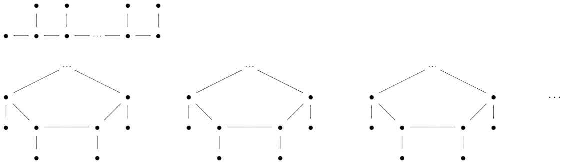
$p \equiv 71, 119 \pmod{120}$:



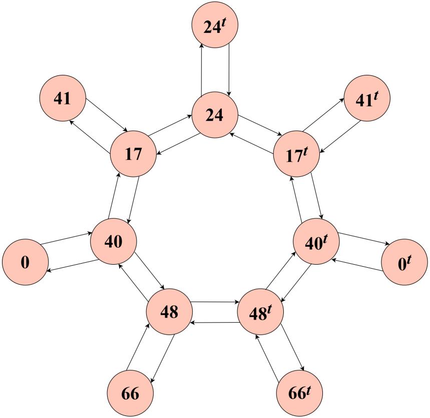
or



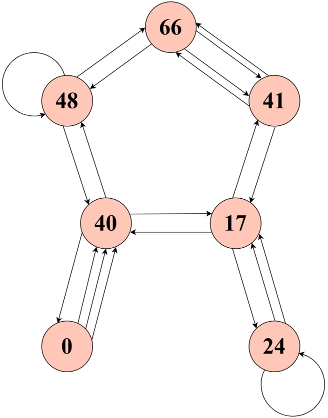
$p \equiv 7, 23, 31, 47, 79, 103 \pmod{120}$:



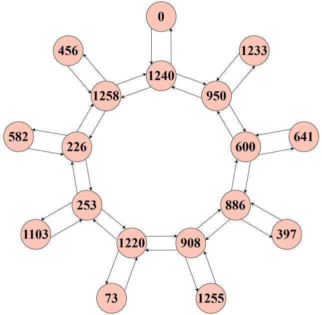
$p = 71$, no Edge Attachment



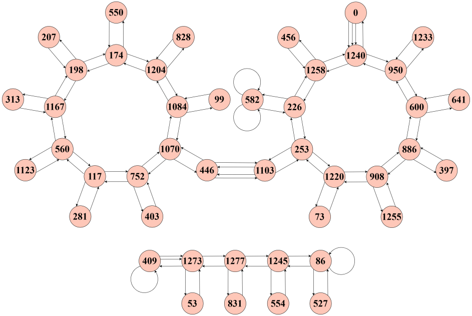
$\mathcal{G}_2(\mathbb{F}_{71})$



$\mathcal{S}_2^{71}$



One of 5 components of $\mathcal{G}_2(\mathbb{F}_{1319})$



$\mathcal{S}_2^{1319}$

The case $\ell = 3$

- Less difficult

- Three cases according to 0, 1 or 2 components folding

- Separation by $p \pmod{840}$

- I will spare you the details . . .

Proof Ingredient: Modular Polynomials

ℓ-**th modular polynomial** $\Phi_\ell(x,y) \in \mathbb{Z}[x,y]$:

$$\Phi_\ell(j,j') = 0 \quad \Longleftrightarrow \quad j \text{ and } j' \text{ are } \ell\text{-isogenous}$$

for all (ordinary and supersingular) j-invariants j, j'.

Properties:

- Loop edge j $\quad \Longleftrightarrow \quad \Phi_\ell(j,j) = 0$
- Double-edge $j \quad j'$ $\quad \Longleftrightarrow \quad \mathrm{Res}_\ell(j) = \mathrm{Res}_\ell(j') = 0$ where

$$\mathrm{Res}_\ell(x) = \mathrm{Res}\left(\Phi_\ell(x,y), \frac{d}{dy}\Phi_\ell(x,y); y\right) \in \mathbb{Z}[x]$$

Higher multiplicity edges can be found via resultants between higher derivatives of $\Phi_\ell(x,y)$.

Proof Ingredient: Hilbert Class Polynomials

Let $\mathcal{O}_D$ be the imaginary quadratic order of discriminant $D < 0$.

Hilbert class polynomial $H_D(x) \in \mathbb{Z}[x]$:

$$H_D(j) = 0 \iff j \text{ has endomorphism ring } \mathcal{O}_D$$

The polynomials $\Phi_\ell(x, x)$ and $\mathrm{Res}_\ell(x)$ factor into Hilbert class polynomials

$$j \text{ supersingular} \iff p \text{ does not split in } \mathbb{Q}(\sqrt{D})$$

UNIVERSITY OF CALGARY

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

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

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

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

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

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

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

Proof Idea for $\ell = 2$

$$\mathcal{G}_\ell(\mathbb{F}_p) \to \mathcal{S}_\ell^p \quad \longleftrightarrow \quad \text{Structure of } \mathcal{G}_\ell(\mathbb{F}_p) \text{ and } \mathcal{G}_\ell(\overline{\mathbb{F}}_p)$$

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

Considerations and requirements for explicit descriptions via congruence conditions on p:

- Roots of $\Phi_2(x, x) \pmod{p}$
- Roots of $\mathrm{Res}_2(x) \pmod{p}$
- Explicit isogeny computations (in some cases)
- 0 and 1728 supersingular
- Roots of $H_{-15}(x)$ in $\mathbb{F}_p$ (quadratic formula)
- $\left(\frac{-3}{p}\right) = \left(\frac{-4}{p}\right) = \left(\frac{-7}{p}\right) = \left(\frac{-15}{p}\right) = -1$

The first three govern the behaviour of how $\mathcal{G}_2(\mathbb{F}_p)$ maps into $\mathcal{G}_2(\overline{\mathbb{F}}_p)$

The last three impose additional congruence conditions on p

$\mathcal{S}_\ell^p$ 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

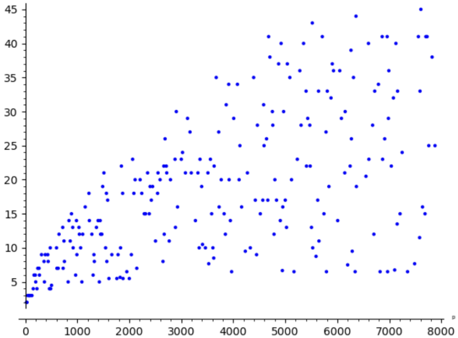
For $\ell = 5$:

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

For $\ell > 5$: 

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
- $p \equiv 71, 119 \pmod{120}$: ???

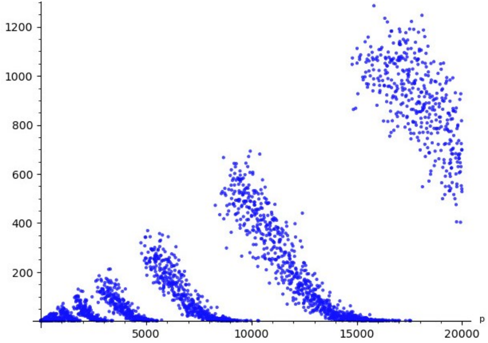


Mean component diameters in $\mathcal{S}_2^p$ for the first 250 primes $p \equiv 7 \pmod 8$

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

Radius: minimal length over all longest directed paths

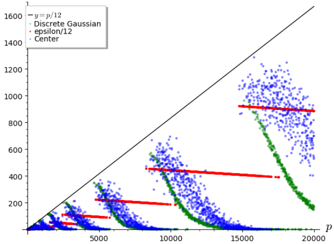
Centre: collection of vertices for which the furthest distance to any other vertex is at most the radius



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

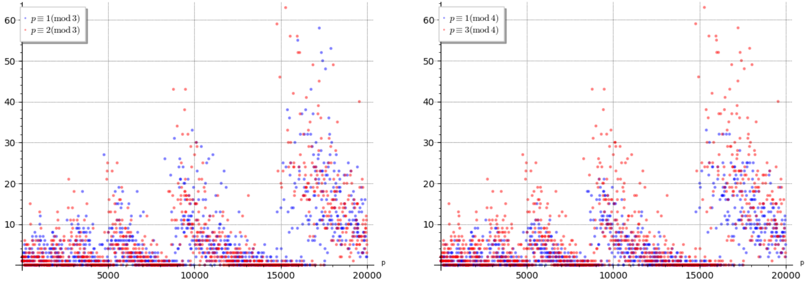
Picture for $\ell = 3$ is similar.

Centre Count Explained



- **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!)

Centre Count of $\mathcal{S}_2^p$



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, lower connectivity of 1728)
- Similar wave pattern as $\mathcal{G}_2(\overline{\mathbb{F}}_p)$ despite Frobenius-conjugate paths

The End!

Merci! — Questions (ou Résponses)?