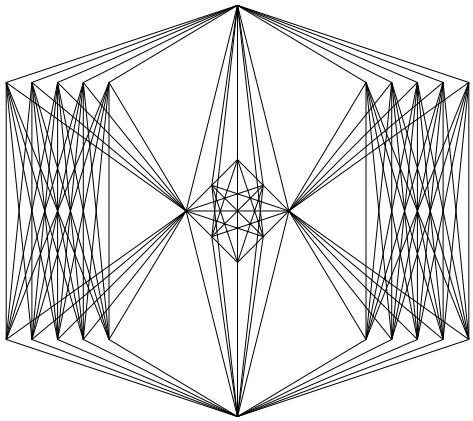
The spine of a supersingular ℓ-isogeny graph

Taha Hedayat, Sarah Arpin, and Renate Scheidler

Abstract. Supersingular elliptic curve ℓ-isogeny graphs over finite fields offer a setting for a number of quantum-resistant cryptographic protocols. The security analysis of these schemes typically assumes that these graphs behave randomly. Motivated by this debatable assertion, we explore structural properties of these graphs. We detail the behavior, governed by congruence conditions on p, of the ℓ-isogeny graph over $\mathbb{F}_p$ when passing to the spine, i.e. the subgraph induced by the $\mathbb{F}_p$-vertices in the full ℓ-isogeny graph. We describe the diameter of the spine and offer numerical data on the number of vertices, over both $\mathbb{F}_p$ and $\overline{\mathbb{F}}_p$, in the center of the ℓ-isogeny graph. Our plots of these counts exhibit a wave-shaped pattern which supports the assertion that centers of supersingular ℓ-isogeny graphs exhibit the same behavior as those of random $(\ell+1)$-regular graphs.



1. Introduction

Supersingular elliptic curve isogeny graphs have undergone a surge of research activity in recent years, in part due to their suitability as a mathematical foundation for quantum-safe cryptographic applications. In particular, the path-finding

2020 *Mathematics Subject Classification.* 14H52, 11G20, 11-04, 11-11, 05C40.

Key words and phrases. Supersingular elliptic curve ℓ-isogeny graph, spine, graph diameter, graph center.

The first and third author acknowledge the support of the *Natural Sciences and Engineering Research Council of Canada* (NSERC).

The second author is a faculty fellow of the Commonwealth Cyber Initiative and is supported by an AMS-Simons Travel Grant.

problem in these graphs seems to be intractable even on a quantum computer. For a prime p, the supersingular isogeny graph $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ has as its vertex set the $\overline{\mathbb{F}}_p$-isomorphism classes of supersingular elliptic curves, labeled by their j-invariants in $\mathbb{F}_{p^2}$. The directed edges of $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ are the ℓ-isogenies between elliptic curves representing vertices, where ℓ is a (usually small) prime. Given two vertices, represented by two elliptic curves E, E' over $\overline{\mathbb{F}}_p$, the path-finding problem in $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ asks to find a path from E to E' comprised of ℓ-isogenies. The presumed intractability of this problem provides security for a number of cryptographic protocols, including [**CLG09**, **DFKL+20**, **FFK+23**] and their variants.

It is well-known that supersingular ℓ-isogeny graphs are optimal expander graphs, and are in fact Ramanujan graphs when $p \equiv 1 \pmod{12}$. The security analysis of supersingular isogeny based cryptographic schemes typically assumes that $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ behaves like a "random" Ramanujan graph, a supposition that has since been called into question. For example, the p-power Frobenius acting on $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ pairs up paths with their Frobenius conjugate paths. It also fixes vertices in $\mathbb{F}_p$ and those ℓ-isogenies between them that are defined over $\mathbb{F}_p$. Moreover, path-finding becomes substantially easier when the start and end vertices belong to $\mathbb{F}_p$ [**DG16**, **CJS14**]. Such special structural features exhibited by the subgraph of $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ induced by the $\mathbb{F}_p$-vertices, referred to as the *spine* of $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$, may make it possible to distinguish a supersingular elliptic curve ℓ-isogeny graph from a random optimal expander or Ramanujan graph.

These questions prompted the authors of [**ACNL+23**] to launch a thorough investigation into the spine $\mathcal{S}_\ell^p$ of $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$. To that end, they considered the supersingular isogeny $\mathbb{F}_p$-graph $\mathcal{G}_\ell(\mathbb{F}_p)$, where the vertices are now $\mathbb{F}_p$-isomorphism classes of supersingular elliptic curves and the edges are $\mathbb{F}_p$-rational ℓ-isogenies. The structure of this graph is well understood and was described in detail in [**DG16**]. There is a natural two-step process of passing from $\mathcal{G}_\ell(\mathbb{F}_p)$ to the spine $\mathcal{S}_\ell^p \subset \mathcal{G}_\ell(\overline{\mathbb{F}}_p)$: vertices in $\mathcal{G}_\ell(\mathbb{F}_p)$ corresponding to twists of curves are identified in $\mathcal{S}_\ell^p$ (with any $\mathbb{F}_p$-isogenies between them turning into loop edges), and edges arising from ℓ-isogenies not defined over $\mathbb{F}_p$ are then added. In [**ACNL+23**], the possible behaviors exhibited by the connected components of $\mathcal{G}_\ell(\mathbb{F}_p)$ under this process were analyzed in detail. Here, we expand on this exploration, refining the results of [**ACNL+23**] and offering new findings.

Our contribution herein is two-fold. In Section 4, we describe all the ways, characterized by explicit congruence conditions on p, in which components of $\mathcal{G}_\ell(\mathbb{F}_p)$ can behave when passing to $\mathcal{S}_\ell^p$ for the arguably most interesting case of $\ell = 2$. In Section 5, we do the same for $\ell = 3$ and give a road map of how to extend our approach to isogeny degrees $\ell \geq 5$.

Leveraging our spine structure results, we describe the diameter (the largest possible directed distance between any pair of vertices) in any component of $\mathcal{S}_\ell^p$ in Section 6. This is followed by an extensive numerical investigation of the center of $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$, i.e. the set of vertices for which the largest distance to any other vertex is minimal. Center vertices can be thought of as having increased connectivity to the rest of the graph compared to the vertices outside the center. The fact that Frobenius is a graph automorphism on $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ that fixes precisely the $\mathbb{F}_p$-vertices might suggest that spine vertices are more prominently represented in the center of $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ than vertices not defined over $\mathbb{F}_p$. Our numerical experiments for $\ell = 2, 3$ and the first 2260 primes $p \neq 2, 3$ (i.e. $5 \leq p < 20000$) demonstrate that this is in

fact not the case for this range of parameters, thereby providing evidence against this claim. Plots of counts of $\mathbb{F}_p$-vertices belonging to the center of $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ exhibit a wave pattern, where wave peaks become higher and are spaced increasingly far apart for larger values of p. Similar wave shapes appear for $\ell = 3$, and this behavior is more pronounced when plotting the size of the entire center of $\mathcal{G}_2(\overline{\mathbb{F}}_p)$ rather than just the number of its spine vertices. Although visually striking, this pattern is in fact evidence that the center size of $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ behaves like that of a random $(\ell+1)$-regular graph.

1.1. Accompanying data and code. The data used to create the figures in this work, as well as the SageMath [**S$^+$25**] code used to generate that data, can be found at the GitHub repository [**Hed25**]. Consult the README.md file for a list of the included files and their functionalies. This code is modified from its original version, which was created by the first author in the summer of 2023. Data collected in `.csv` files was generated using SageMath 10.4 [**S$^+$25**] on a MacBook Pro, Apple M3, with 16 GB of memory, running macOS Sonoma 14.6.1.

1.2. Acknowledgments. We thank Jonathan Love, Jonathan Komada Eriksen and Thomas Decru for their observations and comments in Section 6.3. We are also grateful to our anonymous referees for their comprehensive reviews and their constructive and helpful comments.

2. Supersingular elliptic curve isogeny graphs

Let p be a prime, $\mathbb{F}_p$ the finite field of p elements and $\overline{\mathbb{F}}_p$ a fixed algebraic closure of $\mathbb{F}_p$. We consider supersingular elliptic curves over $\overline{\mathbb{F}}_p$ and recall that every $\overline{\mathbb{F}}_p$-isomorphism class of such curves contains a representative that is defined over $\mathbb{F}_{p^2}$. Isomorphism classes of supersingular elliptic curves are classified by their j-invariant, which is thus an element of $\mathbb{F}_{p^2}$. The j-invariants of curves with extra automorphisms may or may not be supersingular; specifically, $j = 1728$ is supersingular if and only if $p \equiv 3 \pmod 4$, and $j = 0$ is supersingular if and only if $p \equiv 2 \pmod 3$.

While the endomorphism ring of a supersingular elliptic curve defined over $\overline{\mathbb{F}}_p$ is isomorphic to a maximal order in a quaternion algebra, the ring of endomorphisms defined over $\mathbb{F}_p$ of any elliptic curve over $\mathbb{F}_p$ is isomorphic to an imaginary quadratic order. Specifically, when $p \equiv 1 \pmod 4$, all supersingular elliptic curves defined over $\mathbb{F}_p$ have $\mathbb{F}_p$-endomorphism ring isomorphic to the maximal order $\mathbb{Z}[\sqrt{-p}]$ of discriminant $-4p$. When $p \equiv 3 \pmod 4$, all such curves have $\mathbb{F}_p$-endomorphism ring isomorphic to either the maximal order $\mathbb{Z}[(1+\sqrt{-p})/2]$ of discriminant $-p$ or its index 2 suborder $\mathbb{Z}[\sqrt{-p}]$ of discriminant $-4p$. For any quadratic discriminant Δ, denote by $h(\Delta)$ the class number (i.e. the size of the class group) of the quadratic order of discriminant Δ.

Proposition 2.1 (Class number parity, $p \equiv 3 \pmod 4$). If $p \equiv 3 \pmod 4$, then $h(-p)$ is odd.

Proof. For any fundamental discriminant $\Delta < 0$, the 2-rank of the class group of the quadratic order $\mathcal{O}_\Delta$ of discriminant Δ, i.e. its number of 2-Sylow factors, is one less than the number of prime factors of Δ by genus theory (see [**JW09**, p. 170] for example). Hence $h(-p)$ is odd when $p \equiv 3 \pmod 4$. □

When $p \equiv 1 \pmod 4$, the 2-rank of the class group of $\mathbb{Q}(\sqrt{-p})$ is 1, so $h(-4p)$ is even. But this does not determine the 2-adic valuation of $h(-4p)$.

Now fix a prime ℓ. We associate two directed graphs to the set of supersingular elliptic curves and their ℓ-isogenies. For both graphs, the set of vertices does not depend on ℓ, but the set of edges does. Two isogenies are said to be $\mathbb{F}_p$-*equivalent* (resp., $\overline{\mathbb{F}}_p$-*equivalent*) if they are equal up to post-composition with an $\mathbb{F}_p$-automorphism (resp., an $\overline{\mathbb{F}}_p$-automorphism).

DEFINITION 2.2 (Supersingular elliptic curve isogeny graphs). Let p and ℓ be primes. Define the following two graphs.

- The *supersingular elliptic curve ℓ isogeny graph over* $\mathbb{F}_p$, denoted $\mathcal{G}_\ell(\mathbb{F}_p)$, is the directed graph whose vertices are $\mathbb{F}_p$-isomorphism classes of supersingular elliptic curves and whose edges are ℓ-isogenies of these curves up to $\mathbb{F}_p$-equivalence.
- The *supersingular elliptic curve ℓ-isogeny graph over* $\overline{\mathbb{F}}_p$, denoted $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$, is the directed graph whose vertices are $\overline{\mathbb{F}}_p$-isomorphism classes of supersingular elliptic curves and whose edges are ℓ-isogenies of these curves up to $\overline{\mathbb{F}}_p$-equivalence.

By identifying ℓ-isogenies with their duals, the two graphs become undirected. Note that due to post-composition by the extra automorphisms at j-invariants 0 and 1728, this process may identify two or three directed edges in $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ with the same edge in the other direction; see [**ACNL+23**, Rem. 2.3]. We will work with the undirected variants when it is convenient and edge direction does not matter.

It is well-known that the undirected variant of $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ is an optimal expander graph, and is in fact an $(\ell+1)$-regular Ramanujan graph when $p \equiv 1 \pmod{12}$. We recall three key results governing the structure of $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$:

- For any j-invariant j, the neighbors of j in $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ are precisely the roots of $\Phi_\ell(j, Y) \pmod p$. The multiplicity of an edge joining j to j' is the multiplicity of the root j' of $\Phi_\ell(j, Y) \pmod p$. An explicit list of modular polynomials of can be found at [**Sut**].
- Two (not necessary distinct) j-invariants j, j' are joined by a multi-edge in $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ if both are roots of the polynomial $\mathrm{Res}_\ell(X) \pmod p$, where

$$\mathrm{Res}_\ell(X) = \mathrm{Res}\left(\Phi_\ell(X,Y), \frac{\partial}{\partial Y}\Phi_\ell(X,Y);\ Y\right), \tag{2.1}$$

  the resultant of the level ℓ modular polynomial $\Phi_\ell(X, Y)$ and its partial derivative with respect to Y when both are considered as polynomials in Y with coefficients in $\mathbb{Z}[X]$.
- The roots of the Hilbert class polynomial $H_\Delta(X)$ for the imaginary quadratic order $\mathcal{O}_\Delta$ of discriminant Δ are precisely the j-invariants with endomorphism ring isomorphic to $\mathcal{O}_\Delta$. Such a j-invariant is supersingular if and only if p does not split in $\mathcal{O}_\Delta$ (see [**Lan87**, Ch. 13, Thm. 12].

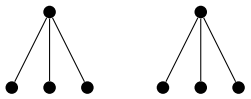
The structure of $\mathcal{G}_\ell(\mathbb{F}_p)$ for $p \geq 5$ was first described in [**DG16**]. Following volcano terminology first introduced in [**FM02**], vertices in $\mathcal{G}_\ell(\mathbb{F}_p)$ corresponding to elliptic curves with $\mathbb{F}_p$-endomorphism ring $\mathbb{Z}[(1+\sqrt{-p})/2]$ are said to lie on the *surface*; those with $\mathbb{F}_p$-endomorphism rings $\mathbb{Z}[\sqrt{-p}]$ lie on the *floor*. When $p \equiv 1 \pmod 4$, all vertices are on the floor. We restate the main structure theorem of [**DG16**] here. Recall that two vertices of a graph are *adjacent* if they are joined by

an edge, in which case each vertex is said to be *incident* with the edge. Adjacent vertices are also referred to as *neighbors*.

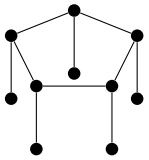
THEOREM 2.3. [DG16, Thm. 2.7], Structure of $\mathcal{G}_\ell(\mathbb{F}_p)$ Let $p \geq 5$ be a prime.

(1) If $\ell = 2$ and $p \equiv 1 \pmod 4$, then $\mathcal{G}_2(\mathbb{F}_p)$ consists of $h(-4p)$ vertices joined in adjacent pairs.

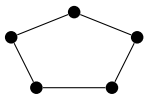
(2) If $\ell = 2$ and $p \equiv 3 \pmod 8$, then $\mathcal{G}_2(\mathbb{F}_p)$ consists of $4h(-p)$ vertices organized into $h(-p)$ *tripod* formations. Each tripod consists of a single vertex on the surface that is adjacent to three distinct vertices on the floor.



(3) If $\ell = 2$ and $p \equiv 7 \pmod 8$, then $\mathcal{G}_2(\mathbb{F}_p)$ consists of $2h(-p)$ vertices, organized into *volcanoes*. Each volcano contains a (possibly degenerate) cycle consisting of vertices on the surface, each of which is adjacent to a unique vertex on the floor.



(4) If $\ell > 2$, with $\ell \neq p$, then $\mathcal{G}_\ell(\mathbb{F}_p)$ is a disoint union of (possibly degenerate) cycles. If $p \equiv 3 \pmod 4$, then each cycle contains either surface vertices or floor vertices, but not both.



In cases (3) and (4), the length of each cycle is the order of the class generated by a prime ideal above ℓ in the class group of the corresponding quadratic order. When $p \equiv 3 \pmod 4$, vertices on the surface may be incident with loop edges.

Note that cycles may be degenerate, i.e. consist of one vertex only. In particular, for $\ell > 2$, $\mathcal{G}_\ell(\mathbb{F}_p)$ may consist of isolated vertices (possibly with loops); for example, when the Legendre symbol $(\frac{-p}{\ell}) = -1$ or $\mathbb{Q}(\sqrt{-p})$ has class number 1.

We characterize loops and multi-edges in $\mathcal{G}_\ell(\mathbb{F}_p)$ when $p > \ell$.

PROPOSITION 2.4 (Loops in $\mathcal{G}_\ell(\mathbb{F}_p)$). Suppose $p > \ell$.

(1) If $p \equiv 3 \pmod 4$, then a vertex on the surface of $\mathcal{G}_\ell(\mathbb{F}_p)$ is incident with a loop if and only if $4\ell - p$ is a perfect square. In this case, every vertex on the surface is incident with two distinct loops, corresponding to dual degree ℓ endomorphisms.

(2) No vertex of $\mathcal{G}_\ell(\mathbb{F}_p)$ on the floor is incident with a loop.

PROOF. Loops in $\mathcal{G}_\ell(\mathbb{F}_p)$ correspond to degree ℓ endomorphisms over $\mathbb{F}_p$, which in turn correspond to elements of norm ℓ in the appropriate quadratic order.

(1) For brevity, put $\omega = (1+\sqrt{-p})/2$ and let $\alpha = a + b\omega \in \mathbb{Z}[\omega]$ be the element of norm ℓ corresponding to loop incident with a vertex on the surface of $\mathcal{G}_\ell(\mathbb{F}_p)$. Since $p > \ell$, we obtain
$$4p > 4\ell = 4N(\alpha) = (2a+b)^2 + b^2 p \geq b^2 p.$$
so $|b| \leq 1$. If $b = 0$, then $\ell = N(\alpha) = a^2$ which is impossible since ℓ is prime. This forces $b = \pm 1$, so $4\ell - p = (2a \pm 1)^2$ is a perfect square. Conversely, if $4\ell - p = m^2$ with $m \in \mathbb{Z}$, then m must be odd. Thus, $\alpha = a + \omega \in \mathbb{Z}[\omega]$ with $a = (m-1)/2$ is an element of norm ℓ. Note that $\alpha = (m + \sqrt{-p})/2$, so the two loops at j correspond to the conjugate elements $(m \pm \sqrt{-p})/2 \in \mathbb{Z}[\omega]$ of norm ℓ.

(2) Now let $\alpha = a + b\sqrt{-p} \in \mathbb{Z}[\sqrt{-p}]$. Then $N(\alpha) = a^2 + b^2 p$. If $b \neq 0$, then $N(\alpha) \geq p > \ell$, whereas if $b = 0$, then $N(\alpha) = a^2$ which is not prime and hence also distinct from ℓ. Hence $\mathbb{Z}[\sqrt{-p}]$ contains no elements of norm ℓ. □

In particular, $\mathcal{G}_\ell(\mathbb{F}_p)$ can only contain loops if $p \equiv 3 \pmod 4$ and $4\ell - p$ is a perfect square. Applying this to $\ell = 2, 3$ immediately yields the following.

Corollary 2.5 (Loops in $\mathcal{G}_\ell(\mathbb{F}_p)$ for $\ell = 2, 3$). For $\ell = 2, 3$ and $p > \ell$, the graph $\mathcal{G}_\ell(\mathbb{F}_p)$ contains no loops except when $(\ell, p) \in \{(2, 7), (3, 11)\}$, where $\mathcal{G}_\ell(\mathbb{F}_p)$ has one vertex that is incident with two pairs of loops.

We now turn to multi-edges in $\mathcal{G}_\ell(\mathbb{F}_p)$ that are not loops.

Proposition 2.6 (Multi-edges in $\mathcal{G}_\ell(\mathbb{F}_p)$). Suppose $p > \ell$.

(1) If $p \equiv 3 \pmod 4$, then $\mathcal{G}_\ell(\mathbb{F}_p)$ contains no directed multi-edges except possibly loops unless $(\ell, p) = (2, 3)$. Here, $\mathcal{G}_2(\mathbb{F}_3)$ has one directed triple edge.

(2) If $p \equiv 1 \pmod 4$, then $\mathcal{G}_\ell(\mathbb{F}_p)$ contains directed multi-edges if and only if it has at least two vertices and $2\ell - p$ is a perfect square. In this case, the vertices in $\mathcal{G}_\ell(\mathbb{F}_p)$ are joined pairwise by pairs of double edges in opposite directions.

Proof. A directed multi-edge in $\mathcal{G}_\ell(\mathbb{F}_p)$ that is not a loop corresponds to multiple $\mathbb{F}_p$-non-equivalent ℓ-isogenies $\phi, \psi : E \to E'$ where E and E' are not isomorphic over $\mathbb{F}_p$. Then $\hat{\phi}\psi$ is an endomorphism on E of degree ℓ^2, and we have a multi-edge if and only if $\hat{\phi}\psi$ is not the multiplication by ℓ map on E. Thus, multi-edges arise from elements $\alpha \neq \pm\ell$ of norm ℓ^2 in the corresponding quadratic order which are not squares up to sign.

(1) Assume $p \equiv 3 \pmod 4$. Note that ℓ does not ramify in $\mathbb{Z}[\omega]$ as $\ell \neq p$. Suppose first that ℓ splits in $\mathbb{Z}[\omega]$, and write $(\ell) = \mathfrak{l}\bar{\mathfrak{l}}$ with prime ideals $\mathfrak{l}, \bar{\mathfrak{l}}$ of $\mathbb{Z}[\omega]$. Note that this precludes the case $p = 3$, as $\ell < p$ implies $\ell = 2$ in this case, but 2 is inert in $\mathbb{Q}(\sqrt{-3})$. Let $\alpha \in \mathbb{Z}[\omega]$ with $\alpha \neq \pm\ell$ and $N(\alpha) = \ell^2$. Unique prime ideal factorization, together with $(\alpha) \neq (\ell)$, forces $(\alpha) = \mathfrak{l}^2$

or $(\alpha) = \bar{\mathfrak{l}}^2$. Assume the former; the case $(\alpha) = \bar{\mathfrak{l}}^2$ is entirely analogous. Then $\mathfrak{l}^2$ is principal. Since $h(-p)$ is odd by Proposition 2.1, $\mathfrak{l}$ must be principal. This means that α is a square in $\mathbb{Z}[\omega]$ up to sign, which we precluded.

Now assume that ℓ is inert in $\mathbb{Z}[\omega]$. Since (ℓ) is the only prime ideal of norm ℓ^2, unique prime ideal factorization implies $(\alpha) = (\ell)$. The assumption $\alpha \neq \ell$ now forces $p = 3$ (the only case where $\mathbb{Z}[\omega]$ has non-trivial units) and hence $\ell = 2$ since $\ell < p$. Thus, $\alpha = \pm 2\zeta^k$ where $k = 1, 2$ and ζ is a primitive cube root of unity, so $\pm\alpha \in \{1+\sqrt{-3}, 1-\sqrt{-3}\}$. Indeed, among the four $\mathbb{F}_3$-isomorphism classes of supersingular elliptic curves over $\mathbb{F}_3$, exactly two, represented by the curves $E_\pm : y^2 = x^3 \pm x$, are 2-isogenous over $\mathbb{F}_3$. The curve E_+ is on the floor, whereas E_- is on the surface and has, up to sign, three $\mathbb{F}_3$-rational automorphisms $(x, y) \mapsto (x + i, y)$ for $i = 0, 1, 2$. So there are three $\mathbb{F}_3$-inequivalent 2-isogenies from E_- to E_+, producing three directed edges. Their duals differ only by post-composition by an automorphism on E_- and are hence equivalent, yielding one edge in the opposite direction.

(2) Now suppose $p \equiv 1 \pmod 4$. Let $\alpha \in \mathbb{Z}[\sqrt{-p}]$ with $N(\alpha) = \ell^2$, $\alpha \neq \pm\ell$ and $\pm\alpha$ not a square in $\mathbb{Z}[\sqrt{-p}]$. Write $\alpha = a + b\sqrt{-p}$ with $a, b \in \mathbb{Z}$. Then $a^2 + b^2 p = \ell^2$ and $b \neq 0$, so $|a| < \ell$. We have

$$b^2 p = \ell^2 - a^2 = (\ell - |a|)(\ell + |a|), \tag{2.2}$$

so p divides $\ell - |a|$ or $\ell + |a|$. Since $1 \leq \ell - |a| \leq \ell < p$, the first of these possibilities cannot happen; hence $p \mid \ell + |a|$. Write $\ell + |a| = kp$ for some $k \in \mathbb{Z}$. Then $k \geq 1$ and $k\ell < kp = \ell + |a| < 2\ell$, forcing $k = 1$ and hence $p = \ell + |a|$. By (2.2), we have $b^2 = \ell - |a| = 2\ell - p$, so $2\ell - p$ is a perfect square. Conversely, if $2\ell - p = b^2$ for some $b \in \mathbb{Z}$, then the 4 elements $\alpha = \pm(p - \ell) \pm b\sqrt{-p}$ all have norm ℓ^2, are distinct from $\pm\ell$, and are not squares in $\mathbb{Z}[\sqrt{-p}]$.

Note that as in the case $p \equiv 3 \pmod 4$, we have $(\alpha) = \mathfrak{l}^2$ or $(\alpha) = \bar{\mathfrak{l}}^2$, where $\mathfrak{l}$ and $\bar{\mathfrak{l}}$ are the two prime ideals above (ℓ) in $\mathbb{Z}[\sqrt{-p}]$. So the ideal class of $\mathfrak{l}$ has order 2 in the class group of $\mathbb{Q}(\sqrt{-p})$. This means that if $\mathcal{G}_\ell(\mathbb{F}_p)$ has more than one vertex and $2\ell - p$ is a perfect square (which rules out $\ell = 2$ as $p \geq 5$), all the cycles in $\mathcal{G}_\ell(\mathbb{F}_p)$ as described in part (4) of Theorem 2.3 have length 2. They correspond to two pairs of directed edges and their respective duals. □

Proposition 2.6 shows that if $p > \ell > 2$, then $\mathcal{G}_\ell(\mathbb{F}_p)$ can only contain directed double edges when $p \equiv 1 \pmod 4$ and $p \leq 2\ell - 1$. The cases $\ell = 2, 3$ can now once again be easily deduced.

Corollary 2.7 (Multi-edges in $\mathcal{G}_\ell(\mathbb{F}_p)$ for $\ell = 2, 3$). For $\ell = 2, 3$ and $p > \ell$, apart from the loops of Corollary 2.5, $\mathcal{G}_\ell(\mathbb{F}_p)$ contains no directed multi-edges except when $(\ell, p) \in \{(2, 3), (3, 5)\}$.

A list of prime pairs (ℓ, p) with $2 \leq \ell < 100$ and $p > \ell$ for which $\mathcal{G}_\ell(\mathbb{F}_p)$ has directed multi-edges, including loops, can be found in the file called `loops & multi-edges in G_l(Fp).pdf` at the GitHub repository [**Hed25**]. A notebook with code to generate visual depictions of $\mathcal{G}_\ell(\mathbb{F}_p)$ and $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$, under the name `Graph_Viz.ipynb`, is also available at [**Hed25**].

18 Jun 2025 06:21:36 PDT
250201-Scheidler Version 2 - Submitted to LuCaNT

3. The spine of $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$

In this section, we review the relationship between $\mathcal{G}_\ell(\mathbb{F}_p)$ and $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$; specifically the process of moving from $\mathbb{F}_p$-isomorphism classes of elliptic curves to $\overline{\mathbb{F}}_p$-isomorphism classes, and from ℓ-isogenies defined over $\mathbb{F}_p$ to those defined over $\overline{\mathbb{F}}_p$. This material is a summary of [ACNL+23].

Definition 3.1 (Spine). The *spine* $\mathcal{S}_\ell^p$ is the subgraph of $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ induced by the vertices in $\mathbb{F}_p$. Specifically, the vertices of $\mathcal{S}_\ell^p$ are the $\overline{\mathbb{F}}_p$-isomorphism classes of supersingular elliptic curves defined over $\mathbb{F}_p$, and its edges are all the ℓ-isogenies joining these vertices.

The terminology was first introduced in [ACNL+23] and stems from the fact that $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ can be obtained from $\mathcal{S}_\ell^p$ by adding pairs of conjugate j-invariants and the corresponding conjugate ℓ-isogenies for any j-invariant in $\mathbb{F}_p$, conjuring an image of a ribcage anchored at a spine. There are natural maps between the graphs $\mathcal{G}_\ell(\mathbb{F}_p)$, $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$, and $\mathcal{S}_\ell^p$:

Definition 3.2. Define $\Gamma : \mathcal{G}_\ell(\mathbb{F}_p) \to \mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ to take vertices of $\mathcal{G}_\ell(\mathbb{F}_p)$ to their $\overline{\mathbb{F}}_p$-isomorphism classes and edges to their $\overline{\mathbb{F}}_p$-equivalence classes.

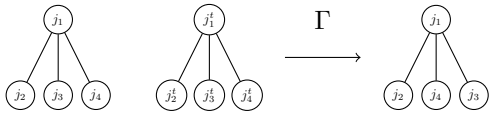
Next, define $\Theta : \mathrm{Im}(\Gamma) \to \mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ to add edges between vertices in $\mathrm{Im}(\Gamma)$ that correspond to isogenies defined over $\overline{\mathbb{F}}_p$ and not defined over $\mathbb{F}_p$. In particular, $\Theta(\mathrm{Im}(\Gamma)) = \mathcal{S}_\ell^p$.

Lastly, define $\Omega = \Theta \circ \Gamma : \mathcal{G}_\ell(\mathbb{F}_p) \to \mathcal{S}_\ell^p \subseteq \mathcal{G}_\ell(\overline{\mathbb{F}}_p)$.

The following graph structural changes are possible under Ω:

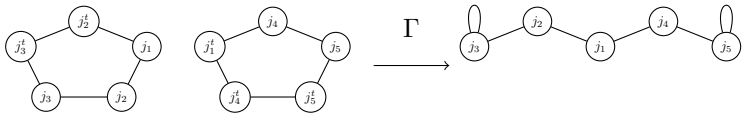
Definition 3.3.

- **Stacking:** Two connected components of $\mathcal{G}_\ell(\mathbb{F}_p)$ *stack* under the map Γ of Definition 3.2 if they are the same graph when labeled by j-invariants.

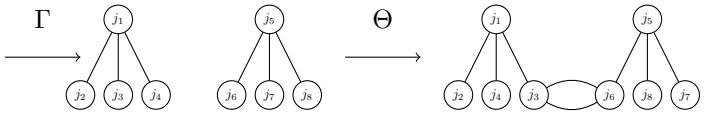


- **Folding:** A connected component of $\mathcal{G}_\ell(\mathbb{F}_p)$ *folds* under the map Γ if it only contains vertices corresponding to both quadratic twists for every j-invariant appearing as a vertex in the component.

- **Attachment at a vertex:** Two components of $\mathcal{G}_\ell(\mathbb{F}_p)$ have a *vertex attachment* under the map Γ if they both contain a vertex with the same j-invariant but the neighbors of that shared j-invariant are different in the two components.



- **Attachment by a new edge:** Two connected components of $\mathcal{G}_\ell(\mathbb{F}_p)$ have an *edge attachment* if a new edge appears under the map Θ of Definition 3.2 which connects these two components.



The map Γ is always 2-to-1 on vertices, and also 2-to-1 on edges outside of the neighborhoods of $j = 0, 1728$. Definition 3.3 immediately implies the following.

LEMMA 3.4. Folding and stacking are mutually exclusive.

PROOF. If two components stack, then one component's vertices correspond to the quadratic twists of the other component's vertices. If a component folds, then the quadratic twists of its vertices belong to that same component. □

As shown in [**ACNL+23**, Prop. 3.16 and Cor. 3.24], vertex attachment is only possible at the j-invariant 1728 and only for $\ell > 2$. Attachment by a new edge implies a double edge in $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ by [**ACNL+23**, Cor. 3.15]. We recall the precise theorems from [**ACNL+23**] describing the changes to $\mathcal{G}_\ell(\mathbb{F}_p)$ under the map Ω:

THEOREM 3.5 ([**ACNL+23**, Thm. 3.29]). Let $\ell = 2$. Under the map $\Gamma : \mathcal{G}_2(\mathbb{F}_p) \to \mathcal{G}_2(\overline{\mathbb{F}}_p)$ of Definition 3.2, only stacking and folding are possible. Under the map $\Theta : \mathrm{Im}(\Gamma) \to \mathcal{G}_2(\overline{\mathbb{F}}_p)$, at most one attachment by a new edge is possible. In particular, attachment by a vertex is not possible.

THEOREM 3.6 ([**ACNL+23**, Thm. 3.18]). Let p and $\ell > 2$ be distinct primes such that the order of a prime ideal $\mathfrak{l}$ above ℓ in the class group of $\mathbb{Q}(\sqrt{-p})$ is odd. Under the map $\Gamma : \mathcal{G}_\ell(\mathbb{F}_p) \to \mathcal{G}_\ell(\overline{\mathbb{F}}_p)$:

- the two components containing vertices corresponding to $j = 1728$ fold and attach at the vertex $j = 1728$;
- all other components stack.

Under the map $\Theta : \mathrm{Im}(\Gamma) \to \mathcal{G}_\ell(\overline{\mathbb{F}}_p)$, the number of new edges is bounded by the degree of $\mathrm{Res}_\ell(X) \pmod p$, with $\mathrm{Res}_\ell(X)$ given in (2.1).

In the next two sections, building on the results of [**ACNL+23**, Sec. 3], we explicitly describe the structure of $\mathcal{S}_2^p$ and and $\mathcal{S}_3^p$ in terms of specific congruence conditions on p. We also provide a road map for extending this approach in principle to any ℓ and outline obstacles one might encounter. Small primes are treated separately elsewhere: a detailed description of the graphs $\mathcal{G}_\ell(\mathbb{F}_p)$, $\mathcal{S}_\ell^p$ and $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ for $2 \le p \le 31$ can be found under the file name `SmallCharacteristic-GraphDescription.pdf`. This information can also be generated with the notebook `Small_Prime_Information.ipynb`, and the notebook `Graph_Viz.ipynp` generates images of all three graphs. All these sources are available at [**Hed25**].

4. Structure of the spine $\mathcal{S}_2^p$

In this section, we provide congruence conditions on p that govern the structure of $\mathcal{S}_2^p$, the spine for $\ell = 2$. This case carries the most interest, especially when $p \equiv 3 \pmod 4$, due to the volcano structure of $\mathcal{G}_2(\mathbb{F}_p)$. For much of this section, we only consider primes $p \ge 17$; for details on the primes $2 \le p \le 13$, consult the sources cited at the end of Section 3.

As expected, our investigation makes extensive use of the modular polynomial $\Phi_2(X, X)$ and the polynomial $\mathrm{Res}_2(X)$ defined in (2.1). Explicitly:

$$\Phi_2(X, X) = -(X - 1728)(X - 8000)(X + 3375)^2, \tag{4.1}$$

$$\mathrm{Res}_2(X) = -2^2X^2(X - 1728)(X + 3375)^2(X^2 + 191025X - 121287375)^2. \tag{4.2}$$

By Corollary 2.5, $\mathcal{G}_2(\mathbb{F}_p)$ contains loops only for $p = 7$. We recall a well-known result about loops in $\mathcal{G}_2(\overline{\mathbb{F}}_p)$, cf. [**Gha24**, Ex. 3].

LEMMA 4.1 (Loops in $\mathcal{G}_2(\overline{\mathbb{F}}_p)$). Let $p \neq 2, 7$. Loops occur in $\mathcal{G}_2(\overline{\mathbb{F}}_p)$ at vertices corresponding to precisely the following j-invariants, all belonging to $\mathbb{F}_p$:

$$\begin{aligned} 1728 &\text{ if } p \equiv 3 \pmod 4, \\ 8000 &\text{ if } p \equiv 5, 7 \pmod 8, \\ -3375 &\text{ if } p \equiv 3, 5, 6 \pmod 7. \end{aligned}$$

PROOF. The loops in $\mathcal{G}_2(\overline{\mathbb{F}}_p)$ are precisely the roots of the polynomial $\Phi_2(X, X)$ of (4.1). Its linear factors are the Hilbert class polynomials $H_{-4}(X)$, $H_{-8}(X)$ and $H_{-7}(X)$. The congruence conditions on p characterize when p is inert in the corresponding imaginary quadratic fields. □

The j-invariants listed in Lemma 4.1 need not be distinct for primes $p \leq 5$; these small primes are handled explicitly in the document `SmallCharacteristic-GraphDescription.pdf` at [**Hed25**].

LEMMA 4.2. [**ACNL+23**, Prop. 3.22] Let $j \in \mathbb{F}_p$ be a supersingular j-invariant, and denote by v_j, w_j the two distinct vertices of $\mathcal{G}_2(\mathbb{F}_p)$ representing isomorphism classes with j-invariant j. If $j \neq 1728$, then v_j and w_j have neighbors in $\mathcal{G}_2(\mathbb{F}_p)$ that correspond to identical j-invariants. Specifically:

(1) If $p \equiv 1 \pmod 4$, then the unique neighbor of v_j and the unique neighbor of w_j are vertices representing the same j-invariant j'.
(2) If $p \equiv 3 \pmod 4$ and the vertices v_j, w_j are on the floor, then the unique neighbor of v_j and the unique neighbor of w_j are vertices with the same j-invariant j'.
(3) If $p \equiv 3 \pmod 4$ and the vertices v_j, w_j are on the surface, then v_j has three neighbors with distinct j-invariants j_1, j_2, j_3 and w_j has three neighbors with the same j-invariants j_1, j_2, j_3.

The following proposition corrects [**ACNL+23**, Cor. 3.28].

PROPOSITION 4.3 (Folding for $\ell = 2$). Let $p > 7$ be prime. The only connected components of $\mathcal{G}_2(\mathbb{F}_p)$ which fold are those containing vertices with $j = 8000$ (if $p \equiv 5, 7 \pmod 8$) and/or $j = 1728$ (if $p \equiv 3 \pmod 4$).

PROOF. A component folds if and only if it contains only vertices corresponding to both $\mathbb{F}_p$-twists of a single supersingular elliptic curve j-invariant when $\ell = 2$, see [**ACNL+23**, Cor. 3.28]. Such a component necessarily contains two adjacent vertices corresponding to a pair of twists which are 2-isogenous over $\mathbb{F}_p$. The roots of $\Phi_2(X, X)$ are precisely $8000, 1728, -3375$; see (4.1).

Since -3375 is a double root of $\Phi_2(X, X)$, there are two distinct 2-isogenies between elliptic curves with j-invariant $j = -3375$. There are no loops or multi-edges in $\mathcal{G}_2(\mathbb{F}_p)$ for $p > 7$ by Corollaries 2.5 and 2.7, so these isogenies do not correspond to edges in $\mathcal{G}_2(\mathbb{F}_p)$.

18 Jun 2025 06:21:36 PDT
250201-Scheidler Version 2 - Submitted to LuCaNT

In [ACNL+23], the authors mistakenly declare that $j = 8000$ is only supersingular for $p \equiv 5 \pmod 8$, when in fact $j = 8000$ is supersingular for $p \equiv 5, 7 \pmod 8$. The two models that the authors list for the curve over $\mathbb{Z}$:

$$E_{8000} : y^2 = x^3 - 4320x + 96768, \quad E^t_{8000} : y^2 = x^3 - 17280x - 774144$$

are twists by $\sqrt{-2}$ (not $\sqrt{2}$, as stated by the authors). Since -2 is not a square modulo p for $p \equiv 5, 7 \pmod 8$, E and E' reduce to supersingular quadratic twists over $\mathbb{F}_p$ for such primes p. Moreover, E and E' have a $\mathbb{Z}$-rational 2-isogeny between them, so they represent adjacent vertices on a connected component of $\mathcal{G}_2(\mathbb{F}_p)$.

Likewise, $\mathbb{Z}$-models for $j = 1728$ show that the $\mathbb{F}_p$-isomorphism classes are 2-isogenous over $\mathbb{F}_p$. □

Since edge attachment forces a double edge, we need to identify double edges in $\mathcal{G}_2(\overline{\mathbb{F}}_p)$ that join two vertices in $\mathbb{F}_p$. This amounts to ascertaining when the roots of the polynomial $\mathrm{Res}_2(X)$ in (4.2) are supersingular and belong to $\mathbb{F}_p$. For $j = 0$, this requires $p \equiv 2 \pmod 3$, and for the roots 1728 and -3375 of $\mathrm{Res}_2(X)$, this was addressed in Lemma 4.1. So we need only consider the quadratic factor of $\mathrm{Res}_2(X)$, which is in fact the Hilbert class polynomial $H_{-15}(X)$.

LEMMA 4.4 (Multi-edges in $\mathcal{G}_2(\overline{\mathbb{F}}_p)$). Let $p \geq 7$. In addition to the loops in Lemma 4.1, $\mathcal{G}_2(\overline{\mathbb{F}}_p)$ has multi-edges when $p = 7, 13$ or $p \equiv 11, 14 \pmod{15}$.

PROOF. By (4.2), additional double edges correspond to the roots modulo p of $H_{-15}(X) = X^2 + 191025X - 121287375$, which are $(-191025 \pm 85995\sqrt{5})/2$. For p odd, their reductions modulo p belong to $\mathbb{F}_p$ if and only if $p \mid 85995 = 3^3 \cdot 5 \cdot 7^2 \cdot 13$ or 5 is a quadratic residue modulo p. So assuming $p \geq 7$, $H_{-15} \pmod p$ has roots in $\mathbb{F}_p$ if and only if $p = 7, 13$ or $(\frac{5}{p}) = 1$. The latter condition holds if and only if $p \equiv \pm 1 \pmod 5$.

For $p \geq 7$, the roots of $H_{-15}(X) \pmod p$ are j-invariants of supersingular elliptic curves if and only if $(\frac{-15}{p}) = -1$. Note that this holds for $p = 7$ and $p = 13$, in which case $H_{-15}(X)$ has the double root $-191025/2 \in \mathbb{F}_p$; else it has two distinct roots in $\mathbb{F}_p$. Assuming $(\frac{5}{p}) = 1$, the condition $(\frac{-15}{p}) = -1$ reduces to $(\frac{-3}{p}) = -1$, or equivalently, $p \equiv 2 \pmod 3$. Finally, $p \equiv \pm 1 \pmod 5$ and $p \equiv 2 \pmod 3$ if and only if $p \equiv 11$ or $14 \pmod{15}$. □

PROPOSITION 4.5 (New edges and edge attachment for $\ell = 2$). Suppose $p \geq 17$.

(1) If $p \not\equiv 7 \pmod 8$, then new edges appear at the supersingular j-invariants which are roots of $H_{-15}(X)$. The new edge joining the two distinct roots of $H_{-15}(X)$ is attaching. Thus, edge attachment happens when $p \equiv 11$, 29, 41, 59, 89, 101 $\pmod{120}$.
(2) If $p \equiv 7 \pmod 8$, then attachment by an edge can only happen between vertices distinct from -3375, 1728 and 0 whose j-invariants are roots of $H_{-15}(X)$.

PROOF. Part (1) is an extension of [ACNL+23, Cor. 3.30], where the authors proved the result under the assumption that $p > 101$. We contribute the computations for $p \leq 101$ to complete the result.

New edges correspond to distinct roots of $H_{-15}(x)$ that are supersingular j-invariants in $\mathbb{F}_p$. Since $p \neq 7, 13$, the roots of $H_{-15}(x)$ are distinct modulo p and are supersingular for $p \equiv 11$ or $14 \pmod{15}$ by Lemma 4.4. Combining these congruence conditions with $p \not\equiv 7 \pmod 8$ results in the set of congruence classes

listed in part (1). It thus suffices to verify this for $p = 29, 41, 59, 71, 89$, and 101. For $p = 29, 41$ and 59, edge attachment holds by the connectivity of $\mathcal{G}_2(\overline{\mathbb{F}}_p)$ and the fact that all the supersingular j-invariants belong to $\mathbb{F}_p$. For $p = 89$ and 101, direct computation of $\mathcal{S}_2^p$ confirms the edge attachment.

The case $p \equiv 7 \pmod 8$ is covered in [ACNL+23, Prop. 3.25]. □

For $p \equiv 11, 14 \pmod{15}$ with $p \equiv 7 \pmod 8$, or equivalently, $p \equiv 71$ or $119 \pmod{120}$, the new edges of Proposition 4.5 may or may not be attaching.

Triple edges in $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ also play a role in ascertaining edge attachment. The following theorem characterizes the occurrence of triple edges in $\mathcal{G}_2(\overline{\mathbb{F}}_p)$.

PROPOSITION 4.6 (Triple edges in $\mathcal{G}_2(\overline{\mathbb{F}}_p)$). For brevity, let $\mathcal{P}_2 = \{2, 3, 5, 7, 13\}$.

(1) If $p \in \mathcal{P}_2$, then $\mathcal{G}_2(\overline{\mathbb{F}}_p)$ is identical to the spine $\mathcal{S}_2^p$ and consists of a single vertex with a triple loop.
(2) If $p \notin \mathcal{P}_2$, and $p \equiv 2 \pmod 3$, then there is a triple edge from the vertex corresponding to $j = 0$ to the vertex corresponding to $j = 54000$.
(3) For all other primes p, $\mathcal{G}_2(\overline{\mathbb{F}}_p)$ does not contain triple edges.

PROOF. A proof for the primes $p \in \mathcal{P}_2$ can be found in the document Small-CharacteristicGraphDescription.pdf at [Hed25], so suppose $p \notin \mathcal{P}_2$. The primes p for which $\mathcal{S}_2^p$ contains a triple edge are those for which the polynomials $\mathrm{Res}_2(X)$ of (4.2) and the polynomial

$$\begin{aligned}\mathrm{Res}_2^{(2)}(X) &= \mathrm{Res}\left(\Phi_2(X,Y), \frac{\partial^2}{\partial Y^2}\Phi_2(X,Y);\ Y\right)\\ &= -2^2 \cdot 3X(X-405)(X^2 - 2571X + 1492425)\end{aligned}$$

share a common root in $\mathbb{F}_p$. The respective sets of roots of these two polynomials:

$$\left\{0, 1728, -3375, \frac{-191025 \pm 85995\sqrt{5}}{2}\right\}, \quad \left\{0, 405, \frac{2571 \pm 39\sqrt{421}}{2}\right\}.$$

The j-invariant 0 is a common root of both polynomials, so when $j = 0$ is supersingular (i.e. $p \equiv 2 \pmod 3$), the graph $\mathcal{S}_2^p$ has a triple edge from $j = 0$. Solving $\Phi_2(0, Y) = 0$ for Y over $\mathbb{Z}$, we see that this triple edge is to the vertex $j = 54000$ and is hence not a loop (as $54000 \not\equiv 0 \pmod p$ for $p \geq 7$). We show that $\mathrm{Res}_2(X)$ and $\mathrm{Res}_2^{(2)}(X)$ have no other shared roots when $p \notin \mathcal{P}_2$, thus ruling out any other triple edges in $\mathcal{S}_2^p$.

For brevity, let $f(X) = X^2 - 2571X + 1492425$ denote the quadratic factor of $\mathrm{Res}_2^{(2)}(X)$. We observe that the root $j = 1728$ of $\mathrm{Res}_2(X)$ is not a root of $\mathrm{Res}_2^{(2)}(X)$. For $p \notin \mathcal{P}_2$, note that $1728 \not\equiv 0, 405 \pmod p$ and $f(1728) = 3^6 \cdot 7^2 \not\equiv 0 \pmod p$. Similarly, the root $j = -3375$ of $\mathrm{Res}_2(X)$ is not a root of $\mathrm{Res}_2^{(2)}(X)$, as $-3375 \not\equiv 0$ or 405 modulo p and $f(-3375) = 3^6 \cdot 5^2 \cdot 7 \cdot 13^2 \not\equiv 0 \pmod p$ when $p \notin \mathcal{P}_2$.

Finally, we establish that $H_{-15}(X)$ and $f(X)$ have no shared root. Equating the roots of these two polynomials modulo p yields the following sequence of

implications:

$$\begin{aligned}
\frac{-191025 \pm 85995\sqrt{5}}{2} &\equiv \frac{2571 \pm 39\sqrt{421}}{2} \pmod{p},\\
(85995)^2 \cdot 5 &\equiv \left(193596 \pm 39\sqrt{421}\right)^2 \pmod{p},\\
-504351432 &\equiv \pm 15100488\sqrt{421} \pmod{p},\\
(-504351432)^2 &\equiv (15100488)^2 \cdot 421 \pmod{p},\\
158371952330592000 &\equiv 0 \pmod{p}.
\end{aligned}$$

The only prime $p \notin \mathcal{P}_2$ that divides 158371952330592000 is $p = 11$. The constant coefficients of $H_{-15}(X)$ and $f(X)$ are both multiples of 11, and it is now easy to verify that the only common root of these two polynomials modulo 11 is 0. □

With these ingredients, we are ready to explicitly describe the graph structure of $\mathcal{S}_2^p$. As in Theorem 2.3, we consider three cases according to the structure of $\mathcal{G}_2(\mathbb{F}_p)$, in Theorems 4.7, 4.8, and 4.9, respectively. We refer to `Small-CharacteristicGraphDescription.pdf` at [**Hed25**] for primes p with $2 \le p \le 13$.

THEOREM 4.7 (Spine structure, $p \equiv 1 \pmod 4$ and $\ell = 2$). Let $p \ge 17$ with $p \equiv 1 \pmod 4$. When mapping $\mathcal{G}_2(\mathbb{F}_p)$ into the spine $\mathcal{S}_2^p$, there may be stacking, folding, or attachment by new edges. The following congruence conditions on p determine precisely which of these occur and how often.

(1) $p = 29$: $\mathcal{G}_2(\mathbb{F}_{29})$ has two components: the component containing the two vertices with $j = 8000$ folds, and there is an edge attachment connecting this folded component to the other component. The spine $\mathcal{S}_2^p$ is the entire 2-isogeny graph $\mathcal{G}_2(\overline{\mathbb{F}}_p)$.
(2) $p \equiv 29, 101 \pmod{120}$, $p \neq 29$: the component containing the two vertices with $j = 8000$ folds, all other components stack, and there is an edge attachment connecting two stacked components. The spine $\mathcal{S}_2^p$ consists of one isolated vertex with $j = 8000$ with a loop, one component with four vertices, and the remaining $h(-4p)/2 - 5$ vertices are joined in pairs.
(3) $p \equiv 41, 89 \pmod{120}$: all components stack, and there is an edge attachment. The spine $\mathcal{S}_2^p$ consists of one connected component with four vertices, and the remaining $h(-4p)/2 - 4$ vertices are joined in pairs.
(4) $p \equiv 13, 37, 53, 61, 77, 109 \pmod{120}$: the component containing the two vertices with $j = 8000$ folds, all other components stack, and there are no edge attachments. The spine $\mathcal{S}_2^p$ consists of one isolated vertex with $j = 8000$ with a loop, and the remaining $h(-4p)/2 - 1$ vertices connect in pairs.
(5) $p \equiv 1, 17, 49, 73, 97, 113 \pmod{120}$: all components stack and there are no edge attachments. The spine $\mathcal{S}_2^p$ is $h(-4p)/2$ vertices joined in pairs.

The five cases are summarized in Table 4.1.

PROOF. The case $p = 29$ can be verified by directly computing $\mathcal{S}_2^{29}$.

We consider the cases for stacking and folding first, followed by those of edge attachment. The individual congruence conditions can be combined by the Chinese Remainder Theorem to provide the statements in this theorem.

Folding and stacking: By Proposition 4.3, the only connected components which could possibly fold are those containing $j = 8000$ and $j = 1728$. Since $p \equiv 1$

<table>
<tr><th></th><th colspan="2">Edge attachment</th><th>No edge attachment</th></tr>
<tr><td>No fold</td><td colspan="2">$p \equiv 41, 89 \pmod{120}$</td><td>$p \equiv 1, 17, 49, 73, 97, 113 \pmod{120}$</td></tr>
<tr><td rowspan="2">One fold</td><td>w/ folded comp.</td><td>not w/ folded comp.</td><td rowspan="2">$p \equiv 13, 37, 53, 61, 77, 109 \pmod{120}$</td></tr>
<tr><td>$p = 29$</td><td>$p \equiv 29, 101 \pmod{120}$, $p \neq 29$</td></tr>
</table>

TABLE 4.1. Spine structure for $p \equiv 1 \pmod 4$

(mod 4), $j = 1728$ is not a supersingular j-invariant. The j-invariant 8000 is supersingular over $\mathbb{F}_p$ whenever $p \equiv 5, 7 \pmod 8$. Combining this with our assumption that $p \equiv 1 \pmod 4$, the connected component with vertices having j-invariant 8000 will fold whenever $p \equiv 5 \pmod 8$. The rest of the components necessarily stack.

Edge attachment: Every edge that appears in $\mathcal{G}_2(\overline{\mathbb{F}}_p)$ but does not already belong to $\mathcal{G}_2(\mathbb{F}_p)$ results in a double edge by [**ACNL+23**, Lem. 3.14]. If a new edge is not attaching, this would result in a triple edge in the case of $p \equiv 1 \pmod 4$ since the connected components of $\mathcal{G}_2(\mathbb{F}_p)$ are precisely edges, see Theorem 2.3. By Proposition 4.6, a triple edge only occurs when a double edge is added between vertices with an existing $\mathbb{F}_p$-edge between them, there are no attaching triple edges for $p > 13$, $p \equiv 1 \pmod 4$.

By Proposition 4.5, attachment by a new edge happens when $p \equiv 11, 29, 41, 59, 89, 101 \pmod{120}$. Combining this with our assumption that $p \equiv 1 \pmod 4$ yields the congruence conditions $p \equiv 29, 41 \pmod{60}$.

To ascertain whether or not this edge attaches to the folding component (corresponding to $j = 8000$), we observe that if $p \equiv 1 \pmod 4$, $j = 8000$ is supersingular if and only if $p \equiv 5 \pmod 8$. Since $p > 13$, $j = 8000$ is a root of $H_{15}(X)$ only for $p = 29$. This explains the second column of Table 4.1. The third column is obtained by sorting the remaining congruence classes modulo 120 by their congruence classes modulo 8. □

THEOREM 4.8 (Spine structure, $p \equiv 3 \pmod 8$ and $\ell = 2$). Let $p \geq 17$ with $p \equiv 3 \pmod 8$. When mapping $\mathcal{G}_2(\mathbb{F}_p)$ into the spine $\mathcal{S}_2^p$, there may be stacking, folding, or attachment by new edges. The connected component of $\mathcal{G}_2(\mathbb{F}_p)$ containing the two vertices with $j = 1728$ always folds. The following congruence conditions on p determine precisely which of these occur and how often.

(1) $p = 59$: the folded component gets edge attached to another component by an edge between two vertices on the floor.
(2) $p \equiv 11, 59 \pmod{120}$ and $p \neq 11, 59$: an edge attachment takes place between two stacked components with the attaching edge being incident to two vertices on the floor.
(3) $p \equiv 19, 43, 67, 83, 91, 107 \pmod{120}$: no edge attachment takes place.

The three cases are summarized in Table 4.2.

No edge attachment	$p \equiv 19, 43, 67, 83, 91, 107 \pmod{120}$
EA w/ folded comp.	$p = 59$
EA not w/ folded comp.	$p \equiv 11, 59 \pmod{120}$ and $p \neq 11, 59$

TABLE 4.2. Spine structure for $p \equiv 3 \pmod 8$

PROOF. The case $p = 59$ can be again be observed directly by computing $\mathcal{S}_2^{59}$.

As before, we consider stacking and folding first, followed by edge attachment. Chinese remaindering again produces the specified congruence conditions on p.

Folding and stacking: By Proposition 4.3, the only connected components which could possibly fold are those containing $j = 8000$ or $j = 1728$. Since $p \equiv 3 \pmod 8$, $j = 8000$ is not a supersingular j-invariant, but $j = 1728$ is supersingular, and folding happens for the component containing the two vertices with $j = 1728$.

Edge attachment: By Proposition 4.5, attachment by a new edge happens when $p \equiv 11, 29, 41, 59,\ 89, 101 \pmod{120}$. Combining this with $p \equiv 3 \pmod 8$ yields $p \equiv 11, 59 \pmod{120}$.

We can determine when the new edge attaches to the folded component. The folded component is a tripod whose surface vertex corresponds to $j = 1728$ and whose floor vertices have j-invariants $1728, 287496$, and 287496, by Theorem 2.3, Proposition 4.3, and the factorization $\Phi_2(1728, X) = (X - 1728)(X - 287496)^2$. For $p > 13$, the j-invariant $j = 1728$ is not a root of $H_{-15}(X)$, and $j = 287496$ is a root of $H_{-15}(X)$ precisely when $p = 59$. In the remaining cases, the edge attachment occurs between stacking components. This produces Table 4.2. □

THEOREM 4.9 (Spine structure, $p \equiv 7 \pmod 8$ and $\ell = 2$). Let $p \geq 17$ with $p \equiv 7 \pmod 8$. When mapping $\mathcal{G}_2(\mathbb{F}_p)$ into the spine $\mathcal{S}_2^p$, there may be stacking, folding, or attachment by new edges. Only the unique connected component of $\mathcal{G}_2(\mathbb{F}_p)$ containing $j = 1728$ and $j = 8000$ folds. The following congruence conditions on p determine the presence of new edges.

(1) $p \equiv 71, 119 \pmod{120}$: there is a new double-edge in $\mathcal{S}_2^p$ which may or may not be an attachment.
(2) $p \equiv 7, 23, 31, 47, 79, 103 \pmod{120}$: edge attachment does not occur.

PROOF. We proceed as in the proofs of the previous two theorems. By Proposition 4.3, the only components of $\mathcal{G}_2(\mathbb{F}_p)$ which could possibly fold are those containing $j = 8000$ and $j = 1728$. For $p \equiv 7 \pmod 8$, both these are supersingular, and are distinct for $p > 13$. By [**ACNL+23**, Ex. 3.8], exactly one of the occurrences of 1728 in $\mathcal{G}_2(\mathbb{F}_p)$ lies on the surface of a volcano. Since $h(-p)$ is odd by Proposition 2.1, any volcano surface contains an odd number of vertices. The two vertices with $j = 1728$ are adjacent by a 2-isogeny over $\mathbb{F}_p$, with one vertex on the surface and the other on the floor of the connected component. In order for folding to occur, this surface (with an odd number of vertices) must also contain two adjacent vertices with the same j-invariant. This is only possible for $j = 8000$ by Lemma 4.1 (vertices with $j = -3375$ are ruled out since the 2-isogeny joining curves with $j = -3375$ is not defined over $\mathbb{F}_p$ by the proof of Proposition 4.3). Hence the unique component containing $j = 1728$ and $j = 8000$ folds.

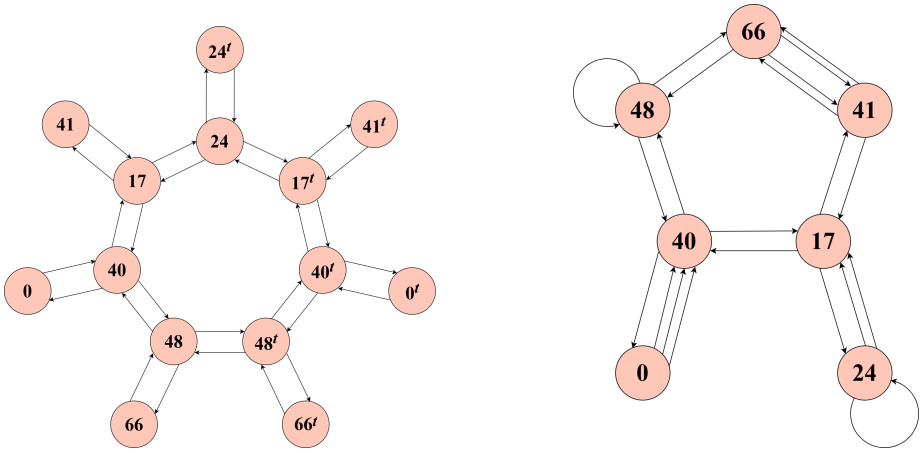
A new edge is added when $p \equiv 11, 14 \pmod{15}$ by Proposition 4.5, but this may or may not be an edge attachment. Other than this edge, there are no new non-loop edges, so no further edge attachment can occur. Combining $p \equiv 11, 14 \pmod{15}$ with $p \equiv 7 \pmod 8$ gives $p \equiv 71, 119 \pmod{120}$. □

REMARK 4.10. Theorem 4.9 shows that precisely one connected component of $\mathcal{G}_2(\mathbb{F}_p)$ folds for $p \equiv 7 \pmod 8$. The structure of this folding component tells us that the smallest positive integer k such that there exists an $\mathbb{F}_p$-rational isogeny of degree 2^k between an elliptic curve with $j = 8000$ and an elliptic curve with

$j = 1728$ is $k = (r-1)/2$, where r is the (necessarily odd) order of the class of a prime ideal above 2 in the class group of $\mathbb{Q}(\sqrt{-p})$.

REMARK 4.11. Whether or not the new edge of Theorem 4.9 (1) produces an edge attachment depends entirely on whether the roots of $H_{-15}(X)$ belong to the same connected component of $\mathcal{G}_2(\mathbb{F}_p)$. When $p \equiv 7 \pmod 8$, the volcano structure of this graph leaves too many possibilities. There is no single simple condition to establish the existence of an endomorphism, so we are not able to determine if the new (double) edge is attaching or not. We provide examples for each case.

EXAMPLE 4.12 ($p = 71$, no edge attachment). For $p = 71$, edge attachment is in principle possible by Theorem 4.9; however, it does not occur. The graph $\mathcal{G}_2(\mathbb{F}_{71})$ consists of a single component. It has 7 vertices on the surface joined to 7 vertices on the floor. This component folds and there is a new edge, but clearly this cannot be an edge attachment: any time $\mathcal{G}_2(\mathbb{F}_p)$ consists of a single connected component, edge attachment is not possible. See Figure 4.1.



(A) (B)

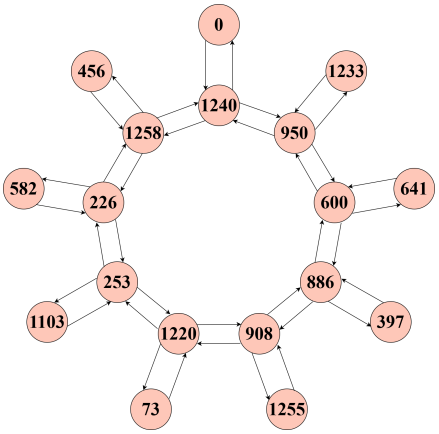
FIGURE 4.1. (A): The graph $\mathcal{G}_2(\mathbb{F}_{71})$. Vertex labels j, j^t represent the j-invariant of a curve and its quadratic twist. (B): The spine graph $\mathcal{S}_2^{71}$.

EXAMPLE 4.13 ($p = 1319$, edge attachment). For $p = 1319 \equiv 71 \pmod{120}$, edge attachment is possible by Theorem 4.9, and in fact it occurs. The graph $\mathcal{G}_2(\mathbb{F}_{1319})$ has five connected components. Each component is a volcano with 9 vertices on the surface and 9 vertices on the floor. Two pairs of connected components stack and the remaining connected component folds. The two stacked components attach at a new edge at the vertices with j-invariants 446 and 1103. See Figure 4.2.

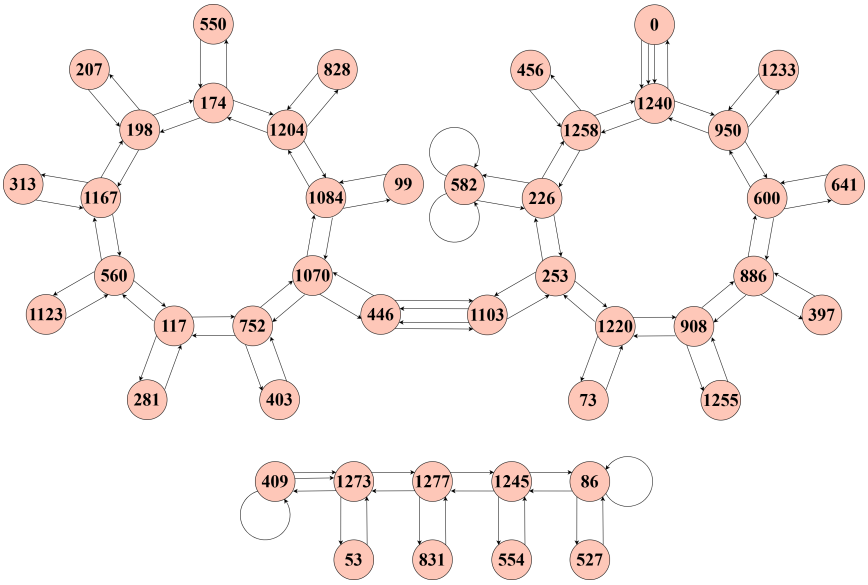
5. Structure of $\mathcal{S}_\ell^p$ for $\ell \geq 3$

The process of moving from $\mathcal{G}_\ell(\mathbb{F}_p)$ to $\mathcal{S}_\ell^p$ for $\ell \geq 3$ is less involved than the analogous procedure for $\ell = 2$ due to the substantially simpler structure of $\mathcal{G}_\ell(\mathbb{F}_p)$ as a collection of disjoint cycles. Note that if $(\frac{-p}{\ell}) = -1$, then $\mathcal{G}_\ell(\mathbb{F}_p)$ has no edges,

18 Jun 2025 06:21:36 PDT
250201-Scheidler Version 2 - Submitted to LuCaNT



(A)



(B)

FIGURE 4.2. (A): One (of five) connected components of $\mathcal{G}_2(\mathbb{F}_{1319})$. (B): The spine graph $\mathcal{S}_2^{1319}$.

including loops, by Theorem 2.3 and Corollary 2.5. In this case, all components (i.e. isolated vertices) stack, none fold, there is no vertex attachment, and only new edges are introduced. We provide an overview of the general method for computing spine structures, with particular focus on the case $\ell = 3$, where we describe the structure of $\mathcal{S}_3^p$ in a manner similar to Theorems 4.7-4.9.

Step 1: Loops. Determine the vertices in $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ belonging to $\mathbb{F}_p$ that are incident with loops by factoring $\Phi_\ell(X, X)$ over $\mathbb{F}_p$ and determining the congruence conditions on p such that these vertices correspond to supersingular j-invariants in $\mathbb{F}_p$.

For edge attachment (investigated in step 3), also ascertain which of these loops belong to $\mathcal{G}_\ell(\mathbb{F}_p)$ via Proposition 2.4.

By Corollary 2.5, $\mathcal{G}_3(\mathbb{F}_p)$ contains loops only for $p = 11$. The loops in $\mathcal{G}_3(\overline{\mathbb{F}}_p)$ are given as follows.

LEMMA 5.1 (Loops in $\mathcal{G}_3(\overline{\mathbb{F}}_p)$). Let $p \neq 2, 3, 11$. Loops occur in $\mathcal{G}_3(\overline{\mathbb{F}}_p)$ at vertices corresponding to precisely the following j-invariants, all belonging to $\mathbb{F}_p$:

$$\begin{aligned} 0 \text{ and } 54000 &\text{ if } p \equiv 2 \pmod 3, \\ 8000 &\text{ if } p \equiv 5, 7 \pmod 8, \\ -32768 &\text{ if } p \equiv 2, 3, 6, 7, 8, 10 \pmod{11}. \end{aligned}$$

PROOF. We have

$$\Phi_3(X, X) = -X(X-54000)(X-8000)^2(X+32768)^2 = H_{-3}H_{-12}H_{-8}^2(X)H_{-11}(X)^2.$$

The congruence conditions on p come from the inertness of p in the corresponding quadratic fields. □

The j-invariants of Lemma 5.1 are not all distinct for $p \leq 5$.

Step 2: Folding and vertex attachment. If $p \equiv 3 \pmod 4$, then there are two different components containing 1728 by Theorem 3.6. The two components fold and get attached at vertex $j = 1728$, and all other components stack.

If $p \equiv 1 \pmod 4$, then the components that can fold are those containing two adjacent vertices in $\mathcal{G}_\ell(\mathbb{F}_p)$ with the same j-invariant, where $\mathcal{G}_\ell(\mathbb{F}_p)$ does not have a loop by Corollary 2.5 (but of course $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ does). These vertices, along with loops (see step 1), correspond to vertices $j \in \mathbb{F}_p$ such that $\Phi_\ell(j, j) = 0$.

PROPOSITION 5.2 (Folding and vertex attachment for $\ell = 3$). If $p \equiv 11 \pmod{12}$, then only the two components containing $j = 1728$ fold and attach at 1728. If $p \equiv 5 \pmod{12}$, then only the component containing $j = 0$ folds and there is no vertex attachment. Else there is neither folding nor vertex attachment.

PROOF. For $p \equiv 11 \pmod{12}$, this is Theorem 3.6. Suppose $p \equiv 5 \pmod{12}$. Then $j = 0$ and $j = 54000$ are supersingular (they are the roots of $H_{-3}(X)$ and $H_{-12}(X)$, respectively), whereas 1728 is not. Two elliptic curves defined over $\mathbb{F}_p$ with $j = 0$ are $E_0 : y^2 = x^3 + 1$ and $E_0^t : y^2 = x^3 - 3$, its twist by a cube root of $\sqrt{-3}$ in $\mathbb{F}_{p^2}$. Since -3 is not a square in $\mathbb{F}_p$, they are non-isomorphic over $\mathbb{F}_p$. There is a 3-isogeny from E_0 to E_0^t with kernel $\langle(0, 1)\rangle$ and hence defined over $\mathbb{F}_p$, i.e. corresponding to an edge in $\mathcal{G}_3(\mathbb{F}_p)$.

By [**ACNL+23**, Ex. 3.20], the only elliptic curves over $\mathbb{F}_p$ with an $\mathbb{F}_p$-rational 3-isogeny to their twist are those with j-invariants 0 and 54000. Using the same reasoning as in the proof of [**ACNL+23**, Thm. 3.18], we see that all their occurrences in $\mathcal{G}_3(\mathbb{F}_p)$ belong to the same component, and this is the only component that folds.

For all other primes p, we have $(\frac{-p}{3}) = -1$, so $\mathcal{G}_3(\mathbb{F}_p)$ contains no edges. □

Step 3: New edges and edge attachment. From the factorization of the polynomial $\mathrm{Res}_\ell(X)$ into Hilbert class polynomials, determine the new edges; it may not be possible to ascertain whether or not they attach. All new edges are multi-edges by [**ACNL+23**, Cor. 3.15], but not all multi-edges are new edges.

Loops cannot be attaching edges. We sketch the idea for characterizing multi-edges and loops for $\ell = 3$. Consider the resultant

$$\begin{aligned}\mathrm{Res}_3(X) = -3^3X^2(X-8000)^2(X-1728)^2(X+32768)^2 \\ \times H_{-20}(X)H_{-32}(X)H_{-35}(X).\end{aligned} \tag{5.1}$$

The roots of (5.1) are j-invariants represented by vertices incident with multi-edges in $\mathcal{G}_3(\overline{\mathbb{F}}_p)$. We find the roots and generate congruence conditions on p under which these roots are supersingular and in $\mathbb{F}_p$. Furthermore, we determine values of p for which distinct roots in $\mathbb{Z}$ coincide modulo p and place them into a list of excluded p-values, denoted $\mathcal{P}_3$.

To determine which multi-edges are loops, we note that loops occur precisely at the j-invariants listed in Lemma 5.1. Substituting these j-values into the polynomial (5.1), we find the values of p for which multi-edges are loops and add these p-values to the list of excluded primes $\mathcal{P}_3$.

We obtain three spine structure theorems, differentiated by number of folding components, for all primes p outside the following set of excluded small values:

$$\mathcal{P}_3 = \{5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59, 61, 71, 79, 89, 101, 139, 151, 199, 271\}.$$

The spines for primes p with $2 \le p \le 31$, along with the graphs $\mathcal{G}_\ell(\mathbb{F}_p)$ and $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$, are explicitly described in the document `SmallCharacteristicGraph-Description.pdf` at [**Hed25**]. For the remaining primes in $\mathcal{P}_3$, the corresponding information can be produced with the notebook `Small_Prime_Information.ipynb`. The notebook `Graph_Viz.ipynp` generates images of all three graphs. These sources are all available at [**Hed25**]. For the remainder of this section, we only consider primes $p \notin \mathcal{P}_3$.

THEOREM 5.3 (Spine structure, $\ell = 3$, no folding). Suppose $p \notin \mathcal{P}_3$. In the following cases, no connected component of $\mathcal{G}_3(\mathbb{F}_p)$ folds and no vertex attachment takes place. In addition to new loops, new edges are added as follows.

(1) None when

$$\begin{aligned}p \equiv\ & 1, 13, 37, 43, 67, 73, 97, 109, 121, 157, 163, 169, 187, 193, \\ & 253, 277, 283, 289, 307, 313, 337, 361, 373, 397, 403, 421, \\ & 433, 457, 493, 517, 523, 529, 541, 547, 577, 589, 613, 643, \\ & 667, 673, 697, 709, 733, 757, 781, 787, 793, 817 \pmod{840}\end{aligned}$$

(2) One when

$$\begin{aligned}p \equiv\ & 61, 103, 127, 181, 211, 223, 229, 241, 247, 331, 349, 367, \\ & 379, 409, 463, 481, 487, 499, 571, 583, 601, 607, 649, 661, \\ & 703, 727, 739, 769, 823, 829 \pmod{840}.\end{aligned}$$

(3) Two that do no share any vertices when

$$p \equiv 19, 79, 139, 151, 319, 451, 619, 631, 691, 751, 799, 811 \pmod{840}$$

(4) Three that do no share any vertices when

$$p \equiv 31, 199, 271, 391, 439, 559 \pmod{840}.$$

THEOREM 5.4 (Spine structure, $\ell = 3$, one component folds). Suppose $p \notin \mathcal{P}_3$. In the following cases, the connected component of $\mathcal{G}_3(\mathbb{F}_p)$ containing $j = 0$ folds

and no vertex attachment takes place. In addition to new loops, new edges are added as follows.

(1) None when

$$p \equiv 17, 29, 53, 113, 137, 149, 173, 197, 221, 233, 257, 281, 293, 317, 353, 377, 389, 401, 437, 449, 473, 533, 557, 569, 593, 617, 641, 653, 677, 701, 713, 737, 773, 797, 809, 821 \pmod{840}.$$

(2) One when

$$p \equiv 41, 89, 101, 209, 269, 341, 461, 509, 521, 629, 689, 761 \pmod{840}$$

THEOREM 5.5 (Spine structure, $\ell = 3$, two components folds). Suppose $p \notin \mathcal{P}_3$. In the following cases, the two connected components of $\mathcal{G}_3(\mathbb{F}_p)$ containing $j = 1728$ fold and get attached at $j = 1728$. In addition to new loops, new edges are added as follows.

(1) None when

$$p \equiv 83, 107, 227, 323, 347, 443, 467, 563, 587, 683, 803, 827 \pmod{840}.$$

(2) One when

$$p \equiv 11, 23, 47, 143, 167, 179, 263, 383, 407, 491, 503, 527, 611, 647, 659, 743, 767, 779 \pmod{840}.$$

(3) Two that do no share any vertices when

$$p \equiv 59, 71, 131, 191, 239, 251, 299, 359, 419, 431, 599, 731 \pmod{840}.$$

(4) Three that do no share any vertices when

$$p \equiv 311, 479, 551, 671, 719, 839 \pmod{840}.$$

Note that Theorem 5.3 covers exactly the setting when $\mathcal{G}_\ell(\mathbb{F}_p)$ has no edges. Theorem 5.4 deals with the case when $j = 0$ is supersingular and $j = 1728$ is not, while in Theorem 5.5, both $j = 0$ and $j = 1728$ are supersingular.

One obstacle to obtaining general explicit structure results about $\mathcal{S}_\ell^p$ for $p \geq 5$, stated only in terms of congruence conditions on p, is the fact that degrees of Hilbert class polynomials grow as the corresponding discriminant increases in absolute value. Already for $\ell = 5$, this becomes a problem: the polynomial $\mathrm{Res}_5(X)$ has degree 54 and decomposes over $\mathbb{Z}$ into linear, quadratic and quartic irreducible factors. While formulas exist for the roots of degree 4 polynomials, the conditions on p become increasingly complicated, and for irreducible factors of degree 5 and higher, such root formulas may no longer exist.

6. Experiments on the Structural Properties of Isogeny Graphs

As mentioned in the introduction, $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ is an optimal expander graph and in fact a Ramanujan graph for $p \equiv 1 \pmod{12}$ (when neither 0 nor 1728 is supersingular). The fact that we can partition the vertices of $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ into two categories, namely the $\mathbb{F}_p$-vertices and the $(\mathbb{F}_{p^2} \setminus \mathbb{F}_p)$-vertices, casts doubt upon the assumption that $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ behaves like a random graph. To shed further light on this question, we gathered a substantial amount of data on graph-theoretic invariants of spines $\mathcal{S}_\ell^p$ for $\ell \leq 5$ and many primes p. We provide an in-depth study of a selection of these invariants in this section.

6.1. Relevant notions and definitions. Let G be a directed graph with vertex set $V(G)$ and edge set $E(G)$. Recall that G is said to be *strongly connected* if it contains a directed path between any two vertices. The *distance* $d(v, w)$ from a vertex v to a vertex w is the length (i.e. the number of edges) in a shortest path from v to w in G. If no such path exists, we set $d(v, w) = \infty$. Also, $d(v, v) = 0$.

DEFINITION 6.1 (Eccentricity). Let $v \in V(G)$. The *(out-)eccentricity* of v is the quantity

$$ecc^+(v) = \max\{d(v, w) : w \in V(G) \text{ and } d(v, w) \neq \infty\},$$

This notion captures the furthest distance required to travel from v to any other vertex of G.

DEFINITION 6.2 (Diameter). If every component of G is strongly connected, then the *diameter* of G is the quantity

$$diam(G) = \max\{ecc^+(v) : v \in V(G)\}.$$

Otherwise, the diameter of G is infinite, i.e. $diam(G) = \infty$.

The diameter is the largest distance between any two vertices of G. Similarly, the radius is the smallest distance between any two vertices of G.

DEFINITION 6.3 (Radius). If every component of G is strongly connected, then the *radius* of G is the quantity

$$rad(G) = \min\{ecc^+(v) : v \in V(G)\}.$$

Otherwise, the radius of G is infinite, i.e. $rad(G) = \infty$.

Finally, the center of G is the set of vertices of G for which the distance to any other vertex is minimal (i.e. takes on the value of the radius).

DEFINITION 6.4 (Center). If the radius of G exists, then the *center* of G is the set

$$cen(G) = \{v \in V(G) : ecc^+(v) = rad(G)\}.$$

As suggested by the name, center vertices can be thought of as "central" in the sense that they are better connected to the entire graph compared to vertices outside the center.

6.2. Diameter of the spine $\mathcal{S}_2^p$. In light of the structure theorems from Section 4, the diameters of the connected components of $\mathcal{S}_2^p$ can be explicitly computed in almost all cases. Again, for this entire section assume $p > 13$.

REMARK 6.5 (Diameters for $\ell > 2$). One could use the structure theorems from Section 5 to make similar statements about the diameter of $\mathcal{S}_3^p$ (or even $\mathcal{S}_\ell^p$ for $p \geq 5$). However, compared to the case $\ell = 2$, less is known about the order r of an ideal class of a prime ideal above an odd prime ℓ in the appropriate class group, and it is harder to obtain concrete statements. Indeed, the $\ell > 2$ case is similar to the $p \equiv 7 \pmod 8$ case for $\ell = 2$ (Theorem 6.8), where the lengths of the cycles in $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ depend on the quantity r.

Following the structure theorems in Section 4, we determine the diameters of the connected components of $\mathcal{S}_2^p$ in the cases $p \equiv 1 \pmod 4$ and $p \equiv 3 \pmod 8$. Examples illustrating each case can be found in `SpineDiameter_examples.ipynb` at [**Hed25**]. For $p \equiv 7 \pmod 8$, we cannot determine edge attachments, which prevents us from classifying the diameter of $\mathcal{S}_2^p$ completely in this case.

Recall that (the undirected version of) $\mathcal{G}_2(\mathbb{F}_p)$ consists of pairs of vertices joined by a single edge when $p \equiv 1 \pmod 4$. Mapping into the spine $\mathcal{S}_2^p$, the generic behavior for these components is to stack. The diameters of the connected components of $\mathcal{S}_2^p$ thus depend on the number of folds and edge attachments.

THEOREM 6.6 (Spine Diameters, $p \equiv 1 \pmod 4$ and $\ell = 2$). Let $p \geq 17$ with $p \equiv 1 \pmod 4$. There are $h(-4p)/2$ vertices in $\mathcal{S}_2^p$. The following congruence conditions on p completely determine the diameters of the components of $\mathcal{S}_2^p$:

(1) If $p = 29$, then $\mathcal{S}_2^p = \mathcal{G}_2(\overline{\mathbb{F}}_p)$, so it contains three vertices (diameter 2).
(2) If $p \equiv 29, 101 \pmod{120}$, then one connected component of $\mathcal{S}_2^p$ has a single vertex with a loop, one connected component has four vertices (diameter 3), and the remaining $h(-4p)/2 - 5$ vertices are joined in pairs (diameter 1).
(3) If $p \equiv 41, 89 \pmod{120}$, then one connected component of $\mathcal{S}_2^p$ has four vertices (diameter 3), and the remaining $h(-4p)/2 - 4$ vertices are joined in pairs (diameter 1).
(4) If $p \equiv 13, 37, 53, 61, 77, 109 \pmod{120}$, then one connected component of $\mathcal{S}_2^p$ is a single vertex with a loop, and the remaining $h(-4p)/2 - 1$ vertices are joined in pairs (diameter 1).
(5) If $p \equiv 1, 17, 49, 73, 97, 113 \pmod{120}$, then $\mathcal{S}_2^p$ consists of $h(-4p)/2$ vertices joined in pairs, so each connected component of $\mathcal{S}_2^p$ has diameter 1.

PROOF. This is a direct result of applying Theorem 4.7 to the possible graph structure of $\mathcal{G}_2(\mathbb{F}_p)$ given in Theorem 2.3. □

THEOREM 6.7 (Spine Diameters, $p \equiv 3 \pmod 8$ and $\ell = 2$). Let $p \geq 17$ with $p \equiv 3 \pmod 8$. There are $2h(-p)$ vertices in $\mathcal{S}_2^p$. The following congruence conditions on p completely determine the diameters of the components of $\mathcal{S}_2^p$:

(1) If $p = 59$, then $\mathcal{S}_2^p$ is a single connected component formed by a tripod edge joined by an edge to a folded tripod component (diameter 4).
(2) If $p \equiv 11, 59 \pmod{120}$ ($p \neq 59$), then one connected component of $\mathcal{S}_2^p$ consists of two adjacent vertices (diameter 1), one connected component is 8 vertices in two tripod shapes joined by a double edge (diameter 5), and the remaining $2h(-p) - 9$ vertices are adjacent in groups of four in tripod formation.
(3) If $p \equiv 19, 43, 67, 83, 91, 107 \pmod{120}$, then one connected component of $\mathcal{S}_2^p$ consists of two adjacent vertices (diameter 1) and the remaining $2h(-p) - 2$ vertices are joined in groups of four in tripods from case (2) of Theorem 2.3 (diameter 2).

PROOF. Follows directly from applying Theorem 4.8 to Theorem 2.3. □

THEOREM 6.8 (Spine Diameters, $p \equiv 7 \pmod 8$ and $\ell = 2$). Let $p \geq 17$ with $p \equiv 7 \pmod 8$. There are $h(-p)$ vertices in $\mathcal{S}_2^p$. Let r denote the order of the ideal class generated by either of the prime ideals above 2 in the class group of $\mathbb{Q}(\sqrt{-p})$. If $p \equiv 7, 23, 31, 47, 79, 103 \pmod{120}$, then the diameter of the spine is $(r+3)/2$.

18 Jun 2025 06:21:36 PDT
250201-Scheidler Version 2 - Submitted to LuCaNT

PROOF. Follows directly from applying Theorem 4.9 to Theorem 2.3. □

If $p \equiv 71, 119 \pmod{120}$, then the diameter of $\mathcal{S}_2^p$ is uncertain. Attaching edges will approximately double the diameter of the resulting connected component, but there are no clear congruence conditions for when this occurs. See Figure 6.1 for a plot visualizing the mean diameters of the components of $\mathcal{S}_2^p$ for a range of primes $p \equiv 7 \pmod 8$. The notebook used to collect the data in this figure can be found in the file `SpineDiameter.ipynb` at [**Hed25**].

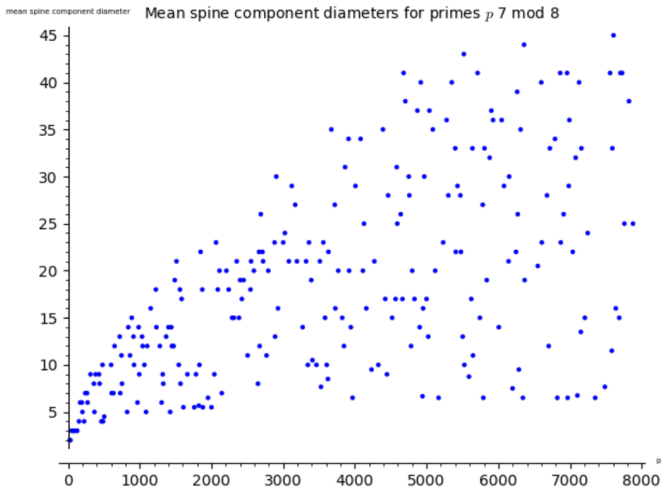


FIGURE 6.1. Mean spine component diameters in $\mathcal{G}_2(\overline{\mathbb{F}}_p)$, for 250 primes $p \equiv 7 \pmod 8$ with $23 \leq p \leq 7879$.

6.3. Center of $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$. In this work, we computed the centers of supersingular elliptic curve 2- and 3-isogeny graphs and counted the number of center vertices belonging to their respective spines. The accompanying data are listed in the file `center012925.csv`. They were generated with the notebook `Center_Data-Generation.ipynb` and plotted using `Center_DataProcessing.ipynb`. All these sources can be found at [**Hed25**].

Recall that the center of a graph (Definition 6.4) is the set of vertices with minimal out-eccentricity. These vertices are well-connected to every other vertex in the graph. Considering that the p-power Frobenius map is a graph automorphism on $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ that fixes the vertices of $\mathcal{S}_\ell^p$, one might expect the spine vertices to be over-represented in the center of $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$. To see this, we note that for any vertex $v \in \mathbb{F}_p$, the set of distances from v displays a symmetry whereby distances can be paired up. Specifically, if w is any vertex of $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ and w^p its Frobenius conjugate, then $d(v, w) = d(v, w^p)$. This property does not hold for vertices $v \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$. So the set of distances from vertices in $\mathbb{F}_p$ only supports "half the randomness" of the set of distances from vertices outside $\mathbb{F}_p$.

In our first experiment, we counted the number of $\mathbb{F}_p$-vertices in the center of $\mathcal{G}_2(\overline{\mathbb{F}}_p)$ as p ranges through the 2260 primes from 5 to 19997. Immediately, a striking wave-like pattern emerged. In order to ascertain whether this behavior

was particular to just the $\mathbb{F}_p$-vertices in the center, we repeated the experiment for the entire center of $\mathcal{G}_2(\overline{\mathbb{F}}_p)$ using the same range of primes. This produced a very similar pattern where the wave shapes are even more pronounced. The results are plotted in blue in Figure 6.2. Analogous results for $\ell = 3$ look similar.

We are indebted to Jonathan Love for the following explanation. The observed wave pattern in Figure 6.2 closely matches the expected behavior of the minimum value of an integer-valued distribution with slow growing mean – in this case, the out-eccentricity whose minimum value (which is the radius) grows approximately as $\log(p/12)$ – and very small standard deviation. Each wave corresponds to primes p for which $\mathcal{G}_2(\overline{\mathbb{F}}_p)$ has a fixed radius r. As p grows, so does $p/12$ (the number of vertices in $\mathcal{G}_2(\overline{\mathbb{F}}_p)$), allowing fewer and fewer vertices with out-eccentricity r until no more such vertices exist. At this point, the radius of $\mathcal{G}_2(\overline{\mathbb{F}}_p)$ jumps to $r+1$, an out-eccentricity value taken on by many more vertices, which starts the next wave. Our experiments confirm that the radius of $\mathcal{G}_2(\overline{\mathbb{F}}_p)$ is generally only slightly larger than $\log_2(p/12)$ in the range of primes under investigation. Thus, if a wave corresponding to a given radius r peaks at a prime p, then the peak of the next wave, corresponding to radius $r+1$, should be located close to $2p$; in other words, the distance between consecutive wave crests doubles each time. Our data bears this out as well.

The green 'Discrete Gaussian' points in Figure 6.2 were obtained via a Discrete Gaussian sampler as follows. For any prime p with $p \equiv 1 \pmod{12}$, simulate a 3-regular graph G with $(p-1)/12$ vertices. Assign an out-eccentricity to any vertex of G by sampling from a normal distribution with mean $1.8\log(p)$ and standard deviation 0.38 and plot the floor function of the sampled values. Although out-eccentricities of adjacent vertices in $\mathcal{G}_2(\overline{\mathbb{F}}_p)$ are in actuality not independent, it is evident that this model matches our observed center size data quite closely.

Additionally, we thank Thomas Decru and Jonathan Komada Eriksen for the observation that the likelihood of a vertex v of $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ to belong to the center can be estimated by the discrepancy between the theoretically possible and the actual number of ways in which it can achieve $ecc^+(v) = r$, where r is the radius of $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$. Let T_ℓ be the tree rooted at v where v has $\ell+1$ children, all other interior vertices have ℓ children, and all leaf nodes are located at level r. Then T_ℓ models an idealized version of the possible paths of length at most r from v in $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$, assuming no cycles are encountered. The difference $\epsilon = |V(T_p)| - |(\mathcal{G}_\ell(\overline{\mathbb{F}}_p))|$ is a measure of the likelihood for a vertex of $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ to lie in the center. For $\ell = 2$, the number of vertices in T_2 is $|V(T_2)| = 1 + 3(2^r - 1)$. The quantity $\epsilon = |V(T_2)| - |V(\mathcal{G}_2(\overline{\mathbb{F}}_p))|$, scaled by $1/12$ for best fit, is plotted in red in Figure 6.2.

To ascertain if elliptic curves with extra automorphisms had any effect on the size of the center of $\mathcal{G}_2(\mathbb{F}_2)$, we separated our data into congruence classes of $p \pmod 4$ and $p \pmod 3$, and the resulting plots are found in Figure 6.3. No definitive pattern emerges for the congruence classes of $p \pmod 3$. While the data points for both congruences classes of p modulo 4 are spread out over the entire data range, higher center size counts (i.e. more data points in the wave peaks) appear for $p \equiv 3 \pmod 4$. This is to be expected because the radius r of $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ tends to be larger in this case and hence easier to attain. In particular, the vertex associated to $j = 1728$ has only one neighbor distinct from itself, whereas a generic vertex of $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ is expected to have three neighbors. A larger radius r makes it

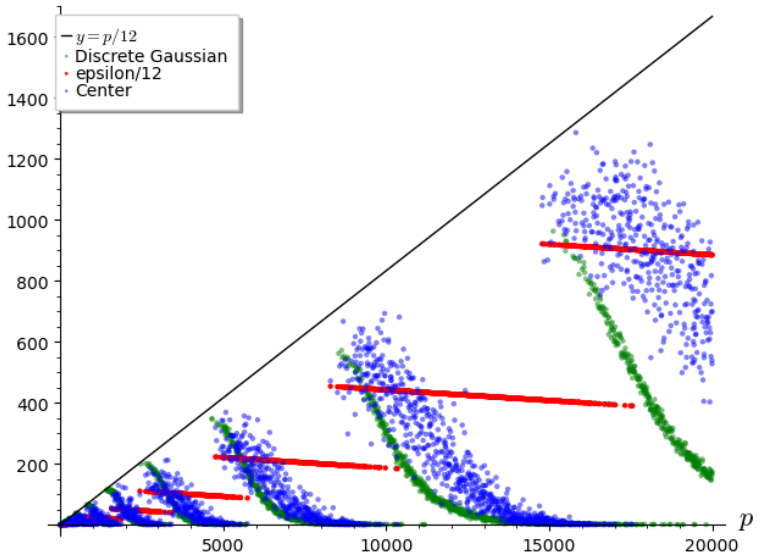
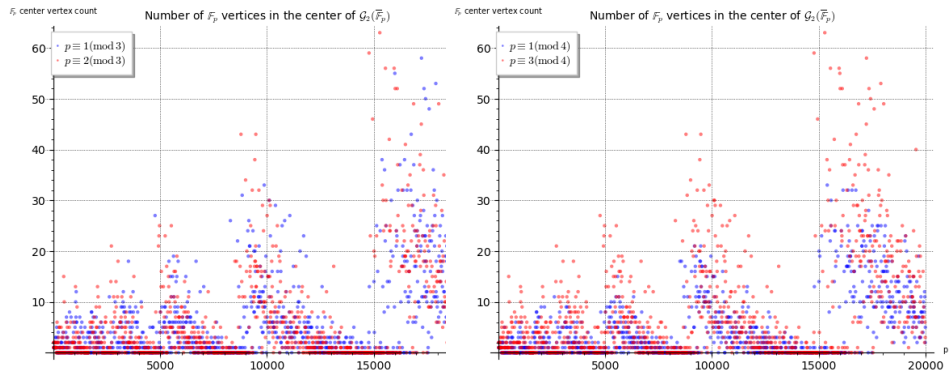


FIGURE 6.2. Size of the center of $\mathcal{G}_2(\overline{\mathbb{F}}_p)$ (in blue) and discrete Gauss sampling with $\mu = 1.8\log(p)$, $\sigma = 0.38$, (in green). The red segments represent the estimate $\epsilon/12$ for a vertex of $\mathcal{G}(\overline{\mathbb{F}}_p)$ to belong to the center, and the line $y = p/12$ (in black) approximates the total number of vertices in $\mathcal{G}_2(\overline{\mathbb{F}}_p)$.

easier for a random vertex to achieve out-eccentricity at most r and thus belong to the center of $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$.



(A) $p \pmod 3$ (B) $p \pmod 4$

FIGURE 6.3. Number of $\mathbb{F}_p$-vertices in the center, sorted by congruence class of p. On the left, blue and red represent $p \equiv 1 \pmod 3$ and $p \equiv 2 \pmod 3$, respectively. On the right, blue and red correspond to $p \equiv 1 \pmod 4$ and $p \equiv 3 \pmod 4$, respectively.

We also investigated the likelihood of 1728 belonging to the center of $\mathcal{G}_2(\overline{\mathbb{F}}_p)$. Overwhelmingly, this is not the case: out of the 1135 primes $p \equiv 3 \pmod 4$ with $5 \leq p < 20000$, the only primes p for which 1728 lies in the center of $\mathcal{G}_2(\overline{\mathbb{F}}_p)$ are $p = 7, 11, 19$.

7. Conclusions and future work

The spine $\mathcal{S}_\ell^p$ of the supersingular ℓ-isogeny graph $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$, our main protagonist, is obtained by mapping the supersingular ℓ-isogeny graph $\mathcal{G}_\ell(\mathbb{F}_p)$ into $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ via a natural two-step process. When passing from $\mathbb{F}_p$-isomorphism classes of curves to $\overline{\mathbb{F}}_p$-isomorphism classes, vertices of $\mathcal{G}_\ell(\mathbb{F}_p)$ representing j-invariants of twists are identified, leading to either stacking or folding of connected components of $\mathcal{G}_\ell(\mathbb{F}_p)$. Components may be joined via attachment at a vertex (for $\ell > 2$ only, and only for j-invariant 1728) or an edge. Passing from ℓ-isogenies over $\mathbb{F}_p$ to those over $\overline{\mathbb{F}}_p$ subsequently introduces new edges.

The authors of [**ACNL+23**] provided the first major insight into this arguably surprisingly predictable process. Our structure theorems in Sections 4 and 5 offer a refinement of their work by characterizing this behavior almost completely in the cases $\ell = 2, 3$ via congruence conditions on p, and outlining a general road map for determining $\mathcal{S}_\ell^p$ for larger primes ℓ. For any particular pair (ℓ, p), the graphs $\mathcal{G}_\ell(\mathbb{F}_p)$, $\mathcal{S}_\ell^p$ and $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ can be explicitly generated using our code at [**Hed25**]; for small primes p and $\ell = 2, 3$, they are described explicitly in a separate document there and cited throughout this paper.

Our structure theorems make it possible to determine the diameter of $\mathcal{S}_2^p$, i.e. the largest distance between any two vertices of $\mathcal{S}_2^p$. This is entirely explicit, and shows that the diameter tends to be very small when $p \not\equiv 7 \pmod 8$; in the case $p \equiv 7 \pmod 8$, the diameter is determined by the order of the ideal class represented by a prime ideal above 2 in the class group of $\mathbb{Q}(\sqrt{-p})$.

It is natural to ask how the spine is situated inside the full ℓ-isogeny graph. To that end, we considered the centers of both $\mathcal{S}_2^p$ and $\mathcal{G}_2(\mathbb{F}_p)$, i.e. the collection of vertices whose furthest distance to any other vertex is minimal. We found that the count of center vertices in $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ defined over $\mathbb{F}_p$, as well as the size of the full center of $\mathcal{G}(\overline{\mathbb{F}}_p)$, follow a remarkable wave-like pattern as p grows. A similar pattern was observed for $\ell = 3$. The community-sourced explanation shows that this pattern is evidence of supersingular elliptic curve isogeny graphs behaving as random graphs.

Our continuing exploration of graph theoretic features of $\mathcal{S}_\ell^p$ gives us new insight into the cryptographically relevant heuristic assumptions we make about $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$. Beyond the findings reported herein, we conducted extensive numerical experiments generating a substantial volume of data on both internal and external connectivity properties of $\mathcal{S}_\ell^p$, as well as counts and proportions of vertices in the periphery of $\mathcal{S}_\ell^p$ and $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$. Our findings raise a number intriguing questions (and answers, thanks to our community); analyzing and understanding the results of our experiments is very much a work in progress as we strive to shed further light on the structural features and patters found in supersingular elliptic curve ℓ-isogeny graphs.

18 Jun 2025 06:21:36 PDT
250201-Scheidler Version 2 - Submitted to LuCaNT

References

[ACNL+23] Sarah Arpin, Catalina Camacho-Navarro, Kristin Lauter, Joelle Lim, Kristina Nelson, Travis Scholl, and Jana Sotáková, *Adventures in Supersingularland*, Exp. Math. **32** (2023), no. 2, 241–268. MR 4592945

[CJS14] Andrew Childs, David Jao, and Vladimir Soukharev, *Constructing elliptic curve isogenies in quantum subexponential time*, J. Math. Cryptol. **8** (2014), no. 1, 1–29. MR 3163097

[CLG09] Denis X. Charles, Kristin E. Lauter, and Eyal Z. Goren, *Cryptographic hash functions from expander graphs*, J. Cryptology **22** (2009), no. 1, 93–113. MR 2496385

[DFKL+20] Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski, *SQISign: compact post-quantum signatures from quaternions and isogenies*, Advances in cryptology—ASIACRYPT 2020. Part I, Lecture Notes in Comput. Sci., vol. 12491, Springer, Cham, [2020] ©2020, pp. 64–93. MR 4210303

[DG16] Christina Delfs and Steven D. Galbraith, *Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$*, Des. Codes Cryptogr. **78** (2016), no. 2, 425–440. MR 3451433

[FFK+23] Luca De Feo, Tako Boris Fouotsa, Péter Kutas, Antonin Leroux, Simon-Philipp Merz, Lorenz Panny, and Benjamin Wesolowski, *SCALLOP: scaling the CSI-FiSh*, Public-key cryptography—PKC 2023. Part I, Lecture Notes in Comput. Sci., vol. 13940, Springer, Cham, [2023] ©2023, pp. 345–375. MR 4591147

[FM02] Mireille Fouquet and François Morain, *Isogeny volcanoes and the SEA algorithm*, Algorithmic number theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 276–291. MR 2041091

[Gha24] Wissam Ghantous, *Loops, multi-edges and collisions in supersingular isogeny graphs*, Advances in Mathematics of Communications **18** (2024), no. 4, 935–955.

[Hed25] Taha Hedayat, *Lucant-2025-supersingular-ell-isogeny-spine*, https://github.com/TahaHedayat/LUCANT-2025-Supersingular-Ell-Isogeny-Spine, 2025.

[JW09] Michael J. Jacobson, Jr. and Hugh C. Williams, *Solving the Pell equation*, CMS Books in Mathematics/Ouvrages de Mathématiques de la SMC, Springer, New York, 2009. MR 2466979

[Lan87] Serge Lang, *Elliptic functions*, second ed., Graduate Texts in Mathematics, vol. 112, Springer-Verlag, New York, 1987, With an appendix by J. Tate. MR 890960

[S+25] William A. Stein et al., *Sage Mathematics Software (Version 10.4)*, The Sage Development Team, 2025, http://www.sagemath.org.

[Sut] Andrew V. Sutherland, *Modular polynomials*, https://math.mit.edu/~drew/ClassicalModPolys.html, Accessed: 2025-01-17.

Department of Mathematics and Statistics, University of Calgary, 2500 University Drive NW, Calgary, AB T2N 1N4, Canada

Email address: taha.hedayat@ucalgary.ca

Virginia Tech Department of Mathematics, 225 Stanger Street, Blacksburg, VA 24061, USA

Email address: sarpin@vt.edu

Department of Mathematics and Statistics, University of Calgary, 2500 University Drive NW, Calgary, AB T2N 1N4, Canada

Email address: rscheidl@ucalgary.ca