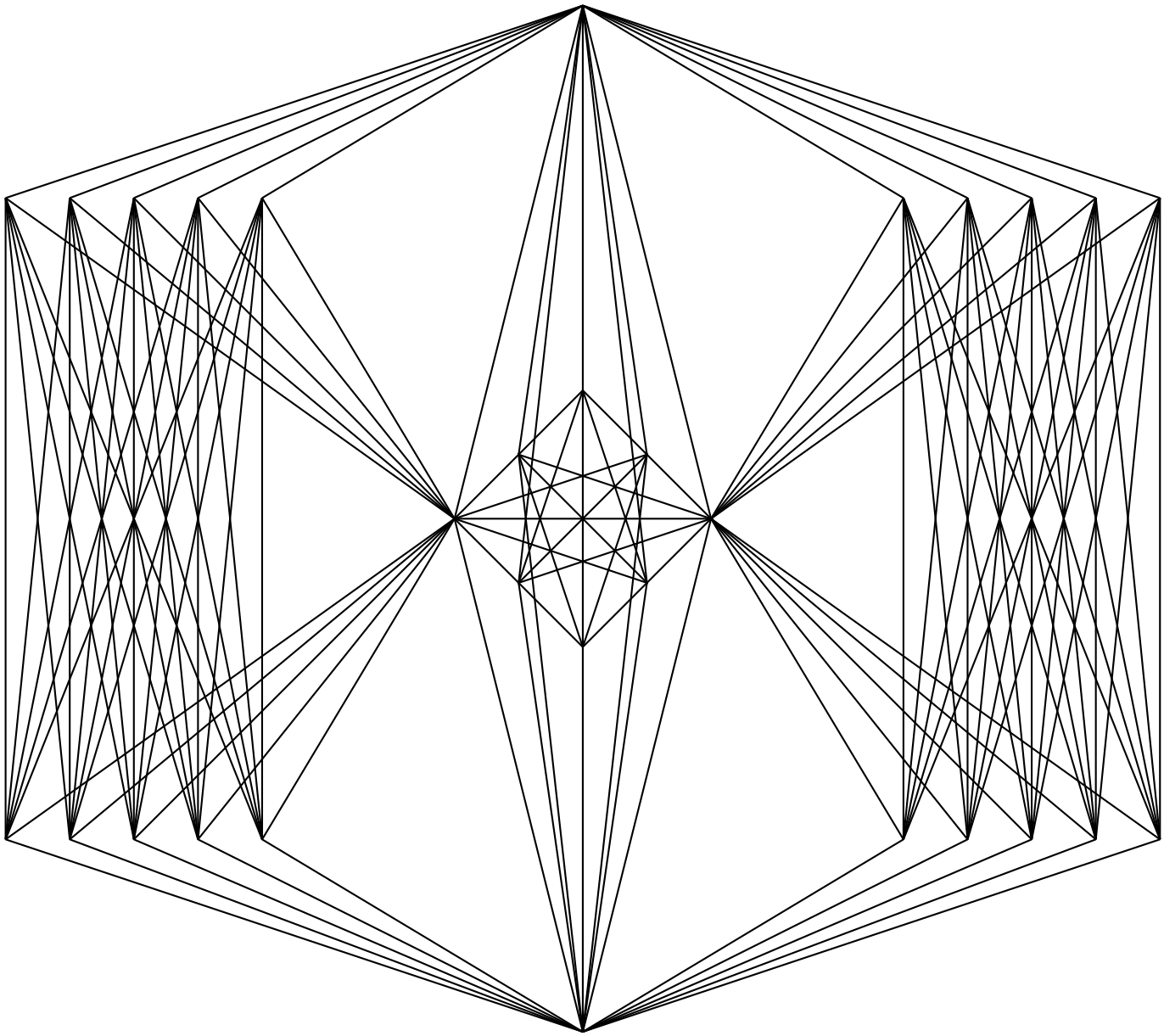
The Spine of Supersingular Ell Isogeny graphs

Describing the explicit structure of the Spine of the Supersingular Ell Isogeny Graph for Ell = 2 and Ell = 3

Taha Hedayat, Dr. Renate Scheidler, Dr. Sarah Arpin



1 Introduction:

1.1 Graph Theoretic Definitions and Notations:

Definition 1.1.1: A *Graph* $\mathcal{G}$ is a finite collection of vertices (dots/circles), and edges (lines) between those vertices.

Definition 1.1.2: An *non-directional graph* is a graph comprised of edges that do not have a direction (no arrows).

Definition 1.1.3: A *directional graph* is a graph comprised of edges that do have a direction (edges are one-way arrows between vertices).

Definition 1.1.4: a *mixed graph* is a graph comprised of edges that may or may not be directional.

Definition 1.1.5: A *multi-edge graph* is a graph that allows more than one edge (of the same direction) to exist between the same two vertices.

Definition 1.1.6: A *loop (*or *looped) graph* is a graph that allows there to exist an edge from a vertex to itself. (Note that loops do not have a direction)

Definition 1.1.7: A graph that is mixed, multi-edged, and looped will be called an *MML graph*.

From now on let $\mathcal{G}$ be an MML graph.

Definition 1.1.8: (The notation of edges in $\mathcal{G}$): Let v and w be vertices in $\mathcal{G}$

- Define (v,w) to be an edge from v to w.
  - Let the edge $e=(v,w)$ be in the graph $\mathcal{G}$.
    - we call v the *tail* of e
    - we call w the *head* of e
    - we say that e *leaves* v
    - we say that e *enters* w
  - if $v=w$, we have a *loop*. A loop is an edge that leaves and enters v. For this reason, we may denote the loop (v,v) by (v).
- Define $\{v,w\}$ to be an edge between v and w. (If you see this notation, assume v and w are distinct vertices.)

Note that $(v,w)\neq(w,v)$ in general. However, $\{v,w\}=\{w,v\}$.

If we have an edge e going to or from a vertex v (the edge can be directed, undirected, or a loop), then we say that v is *incident* to e and vice-versa. Furthermore, if w is the other (not necessarily distinct in the case of loops) vertex incident to e, we say that v and w are *adjacent*. And we call v and w the *end-vertices* of e.

Definition 1.1.9: Define $V(\mathcal{G})$ as the *set of vertices* in $\mathcal{G}$. Similarly, define $E(\mathcal{G})$ as the *set of edges* in $\mathcal{G}$.

Definition 1.1.10: We say that a graph G is a *subgraph* of a graph $\mathcal{G}$ if $V(G) \subseteq V(\mathcal{G})$ and $E(G) \subseteq E(\mathcal{G})$. In this case, we write $G \subseteq \mathcal{G}$. If we wish to stress that G is a proper subgraph of $\mathcal{G}$, then we write $G \subsetneq \mathcal{G}$

Definition 1.1.11: Let $R \subseteq E(\mathcal{G})$. Define $\mathcal{G} - R$ as the graph such that $V(\mathcal{G} - R) = V(\mathcal{G})$, and $E(\mathcal{G} - R) = E(\mathcal{G}) \setminus R$.

Let $S \subseteq V(\mathcal{G})$. Define $\mathcal{G} - S$ as a graph such that $V(\mathcal{G} - S) = V(\mathcal{G}) \setminus S$ and

$$E(\mathcal{G} - S) = \{(v,w), \{v,w\} \in E(\mathcal{G}) : v,w \in V(\mathcal{G}) \setminus S\}$$

Definition 1.1.12: Let $v \in V(\mathcal{G})$. Define the following notations:

- *out-edges:* ${}_{+}E_v := \{(v,w) \in E(\mathcal{G}) : w \in V(\mathcal{G})\}$, note that this includes loops on v.
- *in-edges:* ${}_{-}E_v := \{(w,v) \in E(\mathcal{G}) : w \in V(\mathcal{G})\}$, note that this includes loops on v.
- *non-directed-edges:* ${}_{ND}E_v := \{\{v,w\} \in E(\mathcal{G}) : w \in V(\mathcal{G})\}$, note that this does not include loops on v.
- *loop edges:* ${}_{\circ}E_v := \{(v,v) \in E(\mathcal{G}) : v \in V(\mathcal{G})\}$
- *directed-edges:* ${}_{\pm}E_v := {}_{+}E_v \cup {}_{-}E_v$
- *total-edges* $E_v := {}_{\pm}E_v \cup {}_{ND}E_v$

Note that if the context is not enough we can denote the above by having $\mathcal{G}$ in parenthesis right afterwards. Ex.) ${}_{\pm}E_v(G)$ denotes the set of directed edges coming in or out of the vertex v that exist within the set $E(G)$, for a graph G, this includes the loops on v (loops are only counted once since the union of sets does not result in repetition).

Definition 1.1.13: Let $v \in V(\mathcal{G})$. Define the following notations:

- *out-degree:* ${}_{+}d_v := |{}_{+}E_v|$
- *in-degree:* ${}_{-}d_v := |{}_{-}E_v|$
- *non-directed-degree:* ${}_{ND}d_v := |{}_{ND}E_v| + 2|{}_{\circ}E_v|$
- *directed-degree:* ${}_{\pm}d_v := |{}_{\pm}E_v| + |{}_{\circ}E_v|$
- *total-degree:* $d_v := |E_v| + |{}_{\circ}E_v|$

Note that if the context is not enough we can denote the above by having $\mathcal{G}$ in parenthesis right afterwards. Ex.) ${}_{\pm}d_v(G)$ denotes the cardinality of the set of directed edges coming in or out of the vertex v (loops counted twice, once for being an in-edge, and another time for being an out-edge) that exist within the set $E(G)$, for a graph G.

Definition 1.1.14: Let $v \in V(\mathcal{G})$. Define the following notations:

- *out-neighbourhood:* ${}_{+}N_v := \{w \in V(\mathcal{G}) : (v,w) \in {}_{+}E_v\}$
- *closed out-neighbourhood:* ${}_{+}\overline{N}_v := {}_{+}N_v \cup \{v\}$
- *in-neighbourhood:* ${}_{-}N_v := \{w \in V(\mathcal{G}) : (w,v) \in {}_{-}E_v\}$
- *closed in-neighbourhood:* ${}_{-}\overline{N}_v := {}_{-}N_v \cup \{v\}$
- *non-directional-neighbourhood:* ${}_{ND}N_v := \{w \in V(\mathcal{G}) : \{v,w\} \in {}_{ND}E_v\}$
- *closed non-directional-neighbourhood:* ${}_{ND}\overline{N}_v := {}_{ND}N_v \cup \{v\}$
- *neighbourhood:* $N_v := {}_{+}N_v \cup {}_{-}N_v \cup {}_{ND}N_v$
- *closed neighbourhood:* $\overline{N}_v := {}_{+}N_v \cup {}_{-}N_v \cup {}_{ND}N_v \cup \{v\}$

Note that if the context is not enough we can denote the above by having $\mathcal{G}$ in parenthesis right afterwards.

Definition 1.1.15: a *walk*,$\mathcal{W}$, is an ordered sequence of edges of the form

$$\mathcal{W} = \{e_1, e_2, \ldots, e_n\}$$

where $n \in \mathbb{N}$, $e_i \in E(\mathcal{G})$ for all $1 \leq i \leq n$, and for all $1 \leq i \leq n-1$, e_i enters the same vertex that e_{i+1} leaves.

If $\mathcal{W}$ is a walk notated as above, v_1 is the tail of e_1, and v_{n+1} is the head of e_n, then we say that $\mathcal{W}$ is a walk form v_1 to v_{n+1}, or a (v_1, v_{n+1})-walk. Furthermore, we define the *initial vertex* of the walk $\mathcal{W}$ to be v_1, and the *terminal vertex* of the walk $\mathcal{W}$ to be v_{n+1}.

Note that if it is required we may write $\mathcal{W}(\mathcal{G})$ to emphasize the fact that $\mathcal{W}$ is a walk made up of vertices and edges within $\mathcal{G}$.

Furthermore, we define a *closed walk*, as a walk such that the initial and terminal vertices of the walk are the same.

Definition 1.1.16: We define the *vertices of a walk* $\mathcal{W} = \{e_1, e_2, \ldots, e_n\}$, to be the ordered sequence $V(\mathcal{W}) := \{v_1, v_2, \ldots, v_{n+1}\}$. where e_j leaves v_j and enters v_{j+1} for all $1 \leq j \leq n$

Similarly we define the *edges of the walk* $\mathcal{W}$ to be the ordered sequence $E(\mathcal{W}) := \{e_1, e_2, \ldots, e_n\}$.

Definition 1.1.17: The *subgraph of $\mathcal{G}$ produced by the walk $\mathcal{W}$* is defined as the subgraph of $\mathcal{G}$ made up of vertices $V(\mathcal{W})$ and edges $E(\mathcal{W})$. We will denote this subgraph by $\mathcal{W}$ and make it clear through the context whether we are talking about the walk $\mathcal{W}$ or the subgraph $\mathcal{W}$.

Definition 1.1.18: A walk $\mathcal{W}$ is called a *path* if every vertex of $\mathcal{W}$ is distinct

Note that similar to walks, if $\mathcal{P}$ is a path from the vertex v_1 to the vertex v_n, then we say that $\mathcal{P}$ is a (v_1, v_n)-path.

Furthermore, we define a *cycle* as a closed walk that is a path except at the initial and terminal vertices of the walk. A cycle is usually denoted by $\mathcal{C}$

Definition 1.1.19: Let G and H be subgraphs of $\mathcal{G}$. We say that G and H are *strongly connected* in $\mathcal{G}$ if for every vertex v in G and for every vertex w in H, there exists a (v,w)-path, $\mathcal{P}_1(\mathcal{G})$, and a (w,v)-path, $\mathcal{P}_2(\mathcal{G})$.

Definition 1.1.20: We say that $\mathcal{G}$ is a *disconnected* if there exist subgraphs G, H of $\mathcal{G}$ such that there exists vertices $v \in V(G)$ and $w \in V(H)$ such that there is no (v,w)-path.

Definition 1.1.21: Let G be a subgraph of $\mathcal{G}$. We say that G is a *strongly connected component (of $\mathcal{G}$)* if it is a maximally strongly connected. By "maximally" we mean that if we add any vertex of $V(\mathcal{G} - G)$ (and any associated edges) to G, then G would now no longer be strongly connected.

If the context is clear, we may call a strongly connected component, a *component*.

Definition 1.1.22: The *length* of a walk $\mathcal{W}$ is defined as $|\mathcal{W}| := |E(\mathcal{W})|$.

Note that for a path $\mathcal{P}$, $|\mathcal{P}| = |V(\mathcal{P})| - 1$. Furthermore, for a cycle $\mathcal{C}$, $|\mathcal{C} = |V(\mathcal{C})|$.

Definition 1.1.23: Let $v, w \in V(\mathcal{G})$. We define the *distance from v to w*, denoted $d(v,w)$, as the value $\min(\{|\mathcal{P}| : \mathcal{P} \text{ is a } (v,w)\text{-path}\})$ if there exists a path from v to w. If there does not exist a path from v to w, then the distance from v to w is infinite, and we write $d(v,w) = \infty$.

Note $d(v,w) \neq d(w,v)$ in general. However, if $d(v,w) = d(w,v) \in \mathbb{N}_0$, then we may write $d\{v,w\}$, and call it the *distance between v and w*. If $d(v,w) = d(w,v) = \infty$, then we say that the distance between v and w is infinite and we write $d\{v,w\} = \infty$.

Definition 1.1.24: Let $v \in V(\mathcal{G})$. We define the *out-eccentricity of v* as $ecc^+(v) := \max(\{d(v,w) : w \in V(\mathcal{G}) \text{ and } d(v,w) \neq \infty\})$.

Similarly, we define the *in-eccentricity of v* as $ecc^-(v) := \max(\{d(w,v) : w \in V(\mathcal{G}) \text{ and } d(w,v) \neq \infty\})$.

Note that $ecc^+(v) \neq ecc^-(v)$ in general. However, if $ecc^+(v) = ecc^-(v)$, then we may write $ecc(v)$, and call it the *eccentricity of* v.

Note that there always exists a path from v to itself. Namely the trivial path $\mathcal{P} = \emptyset$. In this way, $0 \leq ecc^+(v), ecc^-(v), ecc(v)$.

Definition 1.1.25: The *diameter* of a graph $\mathcal{G}$ is defined as follows:

- If there exists a component of $\mathcal{G}$ that is not strongly connected, then we say that the diameter of $\mathcal{G}$ is infinite and write $diam(\mathcal{G}) = \infty$.
- If every component of $\mathcal{G}$ is strongly connected, then we define the diameter of $\mathcal{G}$ as:

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

Definition 1.1.26: Let $\mathcal{V}$ be the set of components of $\mathcal{G}$. We define the *mean (component) diameter* of $\mathcal{G}$ to be:

$$\overline{diam}(\mathcal{G}) := \frac{\sum_{G \in \mathcal{V}} diam(G)}{|\mathcal{V}|}$$

Definition 1.1.27: Similar to the diameter, the *radius* $\mathcal{G}$ is defined as follows:

- If there exists a component of $\mathcal{G}$ that is not strongly connected, then we say that the radius of $\mathcal{G}$ is infinite and write $rad(\mathcal{G}) = \infty$.
- If every component of $\mathcal{G}$ is strongly connected, then we define the radius of $\mathcal{G}$ as:

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

Definition 1.1.28: Let $\mathcal{V}$ be the set of components of $\mathcal{G}$. We define the *mean (component) radius* of $\mathcal{G}$ to be:

$$\overline{rad}(\mathcal{G}) := \frac{\sum_{G \in \mathcal{V}} rad(G)}{|\mathcal{V}|}$$

Definition 1.1.29: We define the *girth* of $\mathcal{G}$ as follows:

- If there exists at least one cycle in $\mathcal{G}$, then the girth of $\mathcal{G}$ is defined as $gir(\mathcal{G}) = \min(\{|C(\mathcal{G})|\})$.
- If there does not exists any cycles in $\mathcal{G}$, then we say that the girth of $\mathcal{G}$ is infinite, and we write $gir(\mathcal{G}) = \infty$.

Note that if the girth exists, its value is at least 1.

Definition 1.1.30: Let $\mathcal{V}$ be the set of components of $\mathcal{G}$. We define the *mean (component) girth* of $\mathcal{G}$ to be:

$$\overline{gir}(\mathcal{G}) := \frac{\sum_{G \in \mathcal{V}} gir(G)}{|\mathcal{V}|}$$

Definition 1.1.31: If the radius of $\mathcal{G}$ exists, then we define the *center* of $\mathcal{G}$ to be the set of vertices in $\mathcal{G}$ that have an out-eccentricity value equal to the radius of $\mathcal{G}$. In other words,

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

Definition 1.1.32: If the diameter of $\mathcal{G}$ exists, then we define the *periphery* of $\mathcal{G}$ to be the set of vertices in $\mathcal{G}$ that have an out-eccentricity value equal to the diameter of $\mathcal{G}$. In other words,

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

Definition 1.1.33: Let $\mathcal{V}$ be an arbitrary set of vertices and let $\mathcal{E}$ be all possible edges between vertices in $\mathcal{V}$ (including directed, undirected, looped, and multi edges). Lastly, let $\mathcal{E}_S$ be the set of all possible undirected edges between vertices in $\mathcal{V}$ excluding loops and multi edges. We define the *simplification map*

$$\Upsilon : (\mathcal{V}, \mathcal{E}) \to (\mathcal{V}, \mathcal{E}_S)$$

such that for a mixed, multi-edged, looped graph $\mathcal{G}$, the following hold:

- $\Upsilon(v) = v$ for all $v \in V(\mathcal{G})$,
- for all $v, w \in V(\mathcal{G})$, if $e_1, e_2, \ldots, e_n \in E(\mathcal{G})$ are all edges of the forms (v,w), (w,v) or $\{v,w\}$, then $\Upsilon(e_i) = \{v,w\}$ for all $1 \leq i \leq n$, $i \in \mathbb{N}$, and
- for all $v \in V(\mathcal{G})$, if $e_1, e_2, \ldots, e_n \in E(\mathcal{G})$ are all the edges of the form (v), then $\Upsilon(e_i) = \emptyset$ for all $1 \leq i \leq n$, $i \in \mathbb{N}$.

Note that the simplification map turns any graph into a simple graph by making all directed edges into undirected edges and getting rid of any multi-edges or loops.

1.2 General Definitions of Elliptic curves and the ℓ-Isogeny Graph

Let us first define the notation that we will be using in this paper. Most of the notation is borrowed from [Arpin, Et al.]. For this entire document, let p and l be prime numbers with $p > 3$, and let k be a finite field of characteristic p (which is greater than 3).

Definition 1.2.1: In this paper we will use $\subseteq$ and $\subset$ as equivalent notions of a "subset which may or may not be equal". We use $\subsetneq$ to identify a "proper subset". Lastly, $\nsubseteq$ and $\not\subset$ are equivalent notions of "not a subset".

In this paper $\mathbb{N} = \{1, 2, 3, \ldots\}$, and $\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$.

We also denote the *cardinality* of a set S, as $|S|$

Definition 1.2.2: The *algebraic closure*, $\bar{k}$, of the finite field k is defined to be the field extension of k such that all irreducible polynomials over k have degree 1.

An equivalent definition of $\bar{k}$ is the union of all finite algebraic extensions of k.

Definition 1.2.3: In this document, we say E is an *(affine) elliptic curve defined over a finite field k* if E is the set of points defined by the affine form elliptic equation $y^2 = x^3 + ax + b$ with $a, b \in k$, $4a^3 + 27b^2 \neq 0$, and the valid inputs of (x, y) reside in $\overline{k}^2$. This set has the natural binary operation notated with "+", and an additional point called the *point at infinity* of the elliptic curve E denoted as $\mathcal{O}_E$. This creates an abelian group $(E, +)$ with the identity element being $\mathcal{O}_E$.

If we wish to emphasize the fact that E is defined over the finite field k, then we may notate E as E/k. Furthermore, if we wish to keep things general we may write $E/\overline{k}$ to denote the elliptic curve E defined over an unspecified finite field extension of k. If we do not specify what field E is defined over, then we assume that we are working over $\overline{k}$.

Definition 1.2.4: Let L superfield of k and a subfield of $\overline{k}$. We notate the *L-rational points* of an elliptic curve E defined over k as $E(L) = \{(x, y) \in E : x, y \in L\} \cup \{\mathcal{O}_E\}$

Definition 1.2.5: Let $k \subseteq L \subseteq \overline{k}$ be a field. We say that two elliptic curves E/k and E'/k are *isomorphic over L (as groups)* if there exists $u \in L$ such that the map $\phi : E \to E'$ where $(x, y) \mapsto (u^2 x, u^3 y)$ is a group isomorphism. In this case, we write $E \simeq_L E'$.

Definition 1.2.6: Let $E/k : y^2 = x^3 + ax + b$ be an elliptic curve. We define the *j-invariant of E* as the following:

$$j(E) := 1728 \frac{4a^3}{4a^3 + 27b^2}$$

Theorem 1.2.7: Two elliptic curves E/k and E'/k are isomorphic over $\overline{k}$ if and only if $j(E) = j(E')$.

Proof: Proof done in [Sil09, III, 1.4] ■

Definition 1.2.8: Let E/k and E'/k be two elliptic curves such that $E \simeq_{\overline{k}} E'$ (or $j(E) = j(E')$). This by definition implies that there exists $u \in \overline{k}$ such that the function ϕ as defined in **1.2.5** is an isomorphism. If it is the case that $u \notin k$, but $u^n \in k$ for some minimal $n \in \mathbb{N}_{>1}$, then we call E and E' *twists* of each other. If $n = 2$, then we say E and E' are *quadratic twists*. Moreover, there exist *cubic twists*, $(n = 3)$, *quartic twists* $(n = 4)$, and *sextic twists* $(n = 6)$.

Note that twists, are isomorphic over $\overline{k}$, but not isomorphic over k.

Definition 1.2.9: We call a surjective group homomorphism between two elliptic curves E and E' an *isogeny*.

Theorem 1.2.10: Any non-zero homomorphism between two elliptic curves is an isogeny. In other words, any non-zero homomorphism between two elliptic curves is surjective.

Proof: Proof done in [Har77, II, 6.8] ■

Theorem 1.2.11: Let $\phi : E/k \to E'/k$ be an isogeny. Then there exists polynomials $u,v,s,t \in \overline{k}[x]$ such that

$$\phi(x,y) = \left(\frac{u(x)}{v(x)}, y\frac{r(x)}{s(x)}\right)$$

Proof: Proof done in [Sut22, 4.26]. ■

Definition 1.2.12: Let $k \subseteq L \subseteq \overline{k}$ be a field. We say that an isogeny ϕ is defined over L if $\phi(x,y) = \left(\frac{u(x)}{v(x)}, y\frac{r(x)}{s(x)}\right)$ where $u,v,r,s \in L[x]$.

Let us look at some important isogenies from an elliptic curve to its self (*endomorphisms*)

Definition 1.2.13: Let $n \in \mathbb{N}$. We denote the *multiplication by n map* of an elliptic curve E as $[n] : E \to E$, such that

$$[n](P) := [n]P = \overbrace{P+P+\cdots+P}^{n \text{ times}}$$

for $P \in E$.

Definition 1.2.14: Recall that p is the characteristic of the finite field k. Let $q = p^n$ where $n \in \mathbb{N}$ such that $q = |k|$. We define the *q-power Frobenius endomorphism* as the map $\pi_q : E/k \to E/k$ such that $(x,y) \mapsto (x^q, y^q)$.

Note that these are not the only endomorphisms of elliptic curves, but they are specifically important. There is also a general isogeny which is not always an endomorphism.

Definition 1.2.15: If k is a finite field of order $q = p^n \neq p$, and characteristic p, then for every elliptic curve $E/k : y^2 = x^3 + ax + b$, the map $\pi_p : E \to E'$ where $(x,y) \mapsto (x^p, y^p)$ is an isogeny with its image being the elliptic curve $E'/k : y^2 = x^3 + a^p x + b^p$. We call this the p-power Frobenius isogeny.

Note that we differentiate when π_p is an endomorphism ($|k| = p$), and when it is not ($|k| \neq p$), by calling it the p-power Frobenius endomorphism, versus, the p-power Frobenius isogeny, respectively.

Definition 1.2.16: Let $m \in \mathbb{N}$. We denote the *m torsion subgroup of an elliptic curve E* by $E[m] := \{P \in E : [m]P = \mathcal{O}_E\}$

Theorem 1.2.17: Let $l,e \in \mathbb{N}$, then

$$E[l^e] \simeq \begin{cases} \mathbb{Z}/l^e\mathbb{Z} \times \mathbb{Z}/l^e\mathbb{Z} & \text{if } l \neq p \\ \mathbb{Z}/l^e\mathbb{Z} \text{ or } \{\mathcal{O}_E\} & \text{if } l = p \end{cases}$$

Furthermore, the two possible cases for $E[p^e]$ are mutually exclusive.

Proof: This is proven in [Sil09, VI, 5.4]. ■

Definition 1.2.18: Let $e \in \mathbb{N}$. If $E[p^e] \simeq {}^{\mathbb{Z}}/_{p^e\mathbb{Z}}$, then we call E an *ordinary* elliptic curve. However, if $E[p^e] \simeq \{\mathcal{O}_E\}$, then we call E a *supersingular* elliptic curve.

Theorem 1.2.19: If $E/\mathbb{F}_p$ is supersingular, then $|E(\mathbb{F}_p)| = p+1$.

Proof: Follows from **1.2.30**. ■

Theorem 1.2.20: If $E/\mathbb{F}_p$ is a supersingular elliptic curve, then it only has one twist $E^t/\mathbb{F}_p$ which is supersingular.

Proof: Shown in [DG16, 2.3]. ■

Definition 1.2.21: Let E be an elliptic curve defined over the finite field k. The *k-function field* of E is defined as

$$k(E) = \left\{ \left[\frac{f(x,y)}{g(x,y)}\right]_\sim : f,g \in {}^{k[x_1,x_2]}/_{I(E)}, g \notin I(E), f,g \text{ are homogeneous of degree } d, \text{ and } \frac{f_1}{g_1} \sim \frac{f_2}{g_2} \iff f_1g_2 - f_2g_1 \in I(E) \right\}$$

Where $I(E) = \{f \in \bar{k}[x_1,x_2] : f(P) = 0 \,\forall\, P \in E\}$. Note that $I(E)$ is generated by the definition equation of E (and hence is a subset of $k[x,y]$), and is always a prime ideal. Hence the above is well defined.

Note that a function $f(x,y)$ is *homogeneous* of degree d if for all $\lambda \in \bar{k}$, $f(\lambda x, \lambda y) = \lambda^d f(x,y)$, for some $d \in \mathbb{N}$.

Note that for our purposes if $f \in k(E)$, then we consider f as a map from E to k

Let E and E' be elliptic curves defined over the finite field k. Furthermore, let $k(E)$ and $k(E')$ be the associated function fields. Lastly, let $\phi : E \to E'$ be an isogeny defined over k.

Define ϕ^* such that $\phi^*(f) = f \circ \phi$ for all $f \in k(E')$. Note that in this case $\phi^* : k(E') \to k(E)$, since for $f \in k(E')$, $\phi^*(f) = f \circ \phi : E \to k$. Therefore, $\phi^*(k(E'))$ is a subfield of $k(E)$.

Definition 1.2.22: Let $\phi : E/k \to E'/k$ be an isogeny defined over k. We say that ϕ is *separable*, *inseparable*, or *purely inseparable* corresponding to whether the field extension ${}^{k(E)}/_{\phi^*(k(E'))}$ is separable, inseparable, or purely inseparable.

Definition 1.2.23: Let $\phi : E/k \to E'/k$ be an isogeny defined over k. We define the *degree of* ϕ to be the degree of the extension $[k(E) : \phi^*(k(E'))]$.

Let F and I be fields such that ${}^I/_F$ is a field extension. Recall that there always exists a unique subextension $F \subseteq J \subseteq I$ such that ${}^J/_F$ is a separable extension and ${}^I/_J$ is a purely inseparable field extension. And along with that we have the *separable degree* of ${}^I/_F$ as:

$$[I : F]_s = [J : F]$$

along with the *inseparable degree* of I/F as:

$$[I:F]_i = [I:J]$$

Furthermore, recall that $[I:F] = [I:F]_s[I:F]_i$.

Definition 1.2.24: Let $\phi : E/k \to E'/k$ be an isogeny defined over k. We define the *separable degree of* ϕ as the separable degree of the field extension $k(E)/\phi^*(k(E'))$, denoted as $\deg_s(\phi) = [k(E) : \phi^*(k(E'))]_s$.

Similarly, we define the *inseparable degree of* ϕ as the inseparable degree of the field extension $k(E)/\phi^*(k(E'))$, denoted as $\deg_i(\phi) = [k(E) : \phi^*(k(E'))]_i$.

Note that if ϕ is separable then $\deg(\phi) = \deg_s(\phi)$. Similarly, if ϕ is purely inseparable, then $\deg(\phi) = \deg_i(\phi)$.

Theorem 1.2.25: Let $\phi : E/k \to E'/k$ be an isogeny defined over k. Then the following holds:

(a) If ϕ is separable, then $\deg(\phi) = |ker(\phi)|$.

(b) If ϕ is purely inseparable, then $\deg(\phi) = p^e$ for some $e \in \mathbb{N}$.

(c) If ϕ is the multiplication by $m \in \mathbb{Z}$ endomorphism $[m]$ then ϕ is separable, and $\deg(\phi) = m^2$.

(d) If ϕ is the p^e-th Frobenius isogeny, π_{p^e}, for any $e \in \mathbb{Z}$, then ϕ is purely inseparable and $\deg(\phi) = p^e$.

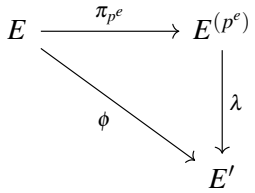
(e) There exists $e \in \mathbb{N}$, elliptic curve denoted $E^{(p^e)}$, Frobenius isogeny $\pi_{p^e} : E \to E^{(p^e)}$, and isogeny $\lambda : E^{(p^e)} \to E'$ such that the following hold:

i. $\phi = \lambda \circ \pi_{p^e}$

ii. λ is separable and $\deg_s(\phi) = \deg(\lambda)$

iii. $p^e = \deg_i(\phi)$

Diagram describing the situation:



Proof: (a) Proof done in [Sil09, III, 4.10]

(b) Proof done in [Sil09, II, 2.11]

(c) Proof done in [Sil09, III, 6.2]

(d) follows from **1.2.25(e)**

(e) Proof done in [Sil09, II, 2.12]

■

Definition 1.2.26: Let E/k be an elliptic curve, and let $\mathrm{End}(E)$ be the set of all endomorphisms of E. Or in other words:

$$\mathrm{End}(E) := \{\phi : E \to E | \phi \text{ is an isogeny}\}$$

Note that isogenies in $\text{End}(E)$ can be defined over any superfield of k. Now, if we let $\phi, \psi \in \text{End}(E)$, then we can define the binary operation $+ : \text{End}(E) \times \text{End}(E) \to \text{End}(E)$ such that $(\phi + \psi)(P) = \phi(P) + \psi(P)$ for all $P \in E$. Furthermore, we can define another binary operation $\circ : \text{End}(E) \times \text{End}(E) \to \text{End}(E)$, such that $(\phi \circ \psi)(P) = \phi(\psi(P))$ for all $P \in E$. We claim that this structure $(\text{End}(E), +, \circ)$ is a ring. We call this ring the *endomorphism ring of* E.

If we wish to only look at the endomorphisms of E defined over a specific super field of k, say L, then we define

$$\text{End}_L(E) = \{\phi : E \to E | \phi \text{ is an isogeny defined over } L\}$$

$(\text{End}_L(E), +, \circ)$ is subring of $\text{End}(E)$, and is called the *endomorphism ring of E defined over L.*

Definition 1.2.27: Let E/k be an elliptic curve. We define the *endomorphism algebra of* E as

$$\mathcal{K}_E := \text{End}(E) \otimes \mathbb{Q}$$

Note that $\mathcal{K}_E$ is a scalar extension of $\mathbb{Q}$, and hence is a number field and a finitely generated $\mathbb{Q}$-algebra! If the context is clear of what elliptic curve we are talking about, then we may write $\mathcal{K}$ instead of $\mathcal{K}_E$

Definition 1.2.28: Let K be a finitely generated $\mathbb{Q}$-algebra. An *order* $\mathcal{O} \subseteq K$ is a subring of K that is a finitely generated $\mathbb{Z}$-module of maximal dimension.

Theorem 1.2.29: Let E/k be an elliptic curve, and let $\mathcal{K}$ be its associated endomorphism algebra. Then $\text{End}(E)$ is an order in $\mathcal{K}$.

Proof: Shown in [DG16, 2.1] ■

Theorem 1.2.30: Let E/k be an elliptic curve and let $\mathcal{K}$ be its associated endomorphism algebra. If $|k| = p^n = q$, for some $n \in \mathbb{N}$. Then there exists $t \in \mathbb{Z}$ such that $|E(k)| = q + 1 - t$, and $|t| \leq 2\sqrt{q}$. Furthermore, one of the following must be true:

(a) n is even and $t = \pm 2\sqrt{q}$

(b) n is even and $p \not\equiv 1 \pmod 3$ and $t = \pm\sqrt{q}$

(c) n is even and $p \not\equiv 1 \pmod 4$ and $t = 0$

(d) n is odd and $t = 0$

Lastly, we know that in case (a), $\mathcal{K}$ is a quaternion algebra over $\mathbb{Q}$, and in cases (b), (c), and (d), $\mathcal{K}$ is an imaginary quadratic field over $\mathbb{Q}$.

Proof: Shown in [DG16, 2.1] ■

Theorem 1.2.31: Let $\phi : E/k \to E'/k$ be a non-zero isogeny defined over k of degree m. Then, there exists a map $\widehat{\phi} : E'/k \to E/k$ that is a non-zero isogney defined over k and $\widehat{\phi} \circ \phi = [m] \in \text{End}(E)$

Proof: This is proven in [Sil09, III, 6.1] ■

Definition 1.2.32: The map $\widehat{\phi}$ in **1.2.31** is called the *dual (isogeny) of* ϕ.

Theorem 1.2.33: Let $\phi : E \to E'$ be a non-zero isogeny, then

(a) Let $m = \deg(\phi)$. Then

$$\widehat{\phi} \circ \phi = [m] \in \mathrm{End}(E) \qquad \text{and} \qquad \phi \circ \widehat{\phi} = [m] \in \mathrm{End}(E')$$

(b) Let $\lambda : E_2 \to E_3$ be another isogeny. Then

$$\widehat{\lambda \circ \phi} = \hat{\phi} \circ \hat{\lambda}$$

(c) Let $\psi : E_1 \to E_2$ be another isogeny. Then

$$\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$$

(d) $\deg(\widehat{\phi}) = \deg(\phi)$.

(e) $\widehat{\widehat{\phi}} = \phi$.

Proof: This is proven in [Sil09, III, 6.2] ■

Definition 1.2.34: Let E_1/k, E_2/k, E_1'/k, E_2'/k be elliptic curves such that $E_1 \neq E_2$, let $\phi_1 : E_1 \to E_1'$, and $\phi_2 : E_2 \to E_2'$ be separable isogenies, and let L be a superfield of k. We say that ϕ_1 and ϕ_2 are *equivalent over the field* L if there exists L-isomorphisms $\lambda : E_1 \to E_2$, and $\lambda' : E_1' \to E_2'$ such that $\phi_2 \circ \lambda = \lambda' \circ \phi_1$. In other words, ϕ_1 and ϕ_2 are equivalent over L if there exists L-isogmorphism λ and λ' such that the following diagram commutes:

$$\begin{array}{ccc} E_1 & \xrightarrow{\lambda} & E_2 \\ \downarrow{\scriptstyle \phi_1} & & \downarrow{\scriptstyle \phi_2} \\ E_1' & \xrightarrow[\lambda']{} & E_2' \end{array}$$

Note that in the definition above since λ and λ' are L-isogenies, and hence E_1, E_2 are in the same isomorphism class of elliptic curves, and the same holds for E_1' and E_2'. This implies that ϕ and ϕ' are doing "basically the same thing" up to L-isomorphism.

Theorem 1.2.35: Equivalent separable isogenies have the same degree.

Proof: Let E_1/k, E_2/k, E_1'/k, E_2'/k be elliptic curves. Let $\phi_1 : E_1 \to E_1'$ and $\phi_2 : E_2 \to E_2'$ be separable isogenies. Suppose that ϕ is equivalent to ϕ' over the superfield $L \supseteq k$. By definition, this implies that there exists L-isomorphisms $\lambda : E_1 \to E_2$, and $\lambda' : E_1' \to E_2'$ such that $\phi_2 \circ \lambda = \lambda' \circ \phi_1$. To prove the theorem we need only to show that the cardinality of the kernels of ϕ_1 and ϕ_2 are the same and use **1.2.25**.

Consider $ker(\phi_2 \circ \lambda) := \{P \in E_1 : \phi_2 \circ \lambda(P) = \mathcal{O}_{E_2'}\}$ which we can write as $ker(\phi_2 \circ \lambda) = \{P \in E_1 : \lambda(P) \in ker(\phi_2)\}$. We can define the map $\alpha : ker(\phi_2 \circ \lambda) \to ker(\phi_2)$ such that $P \mapsto \lambda(P)$. We claim

that α is a bijection. We can check injectivity by looking at the kernel of α. Let $P \in ker(\alpha)$. By definition this implies that $\alpha(P) = \lambda(P) = \mathcal{O}_{E_2}$. Now since λ is an isomorphism we know that $P = \mathcal{O}_{E_1}$. By the arbitrary choice of P we know that $Ker(\alpha) = \{\mathcal{O}_{E_1}\}$, and hence α is injective. We can show surjectivity of α by looking at $ker(\phi_2)$. Let $P \in ker(\phi_2)$. By definition, we know that $P \in E_2$. Furthermore, since λ is an isomorphism we know that it has an inverse. Therefore we know that $\lambda^{-1}(P)$ is well defined and is in E_1. Note that $\phi_2 \circ \lambda(\lambda^{-1}(P)) = \phi_2(P) = \mathcal{O}_{E_2'}$. Hence $\lambda^{-1}(P) \in ker(\phi_2 \circ \lambda)$. With this, we can consider $\alpha(\lambda^{-1}(P)) = \lambda(\lambda^{-1}(P)) = P \in ker(\phi_2)$. Hence α is surjective. As a result we know that α is a bijection, and therefore we know that $|ker(\phi_2 \circ \lambda)| = |ker(\phi_2)|$.

On the other hand, we can consider $ker(\lambda' \circ \phi_1) := \{P \in E_1 : \lambda' \circ \phi_1(P) = \mathcal{O}_{E_2'}\}$ which we can write as $ker(\lambda' \circ \phi_1) = \{P \in E_1 : \phi_1(P) \in ker(\lambda')\}$. Note however, that since λ' is an isomorphism we know that $ker(\lambda') = \{\mathcal{O}_{E_1'}\}$. Therefore we have $ker(\lambda' \circ \phi_1) = \{P \in E_1 : \phi_1(P) = \mathcal{O}_{E_1'}\}$. This by definition is the kernel of ϕ_1. Hence we have $|ker(\lambda' \circ \phi_1)| = |ker(\phi_1)|$.

Adding ontop of these results our supposition that $\phi_2 \circ \lambda = \lambda' \circ \phi_1$ (which implies that $|ker(\phi_2 \circ \lambda)| = |ker(\lambda' \circ \phi_1)|$), we have the following result:

$$\begin{aligned} deg(\phi_1) &= |ker(\phi_1)| && \text{(by } \mathbf{1.2.25}\text{)} \\ &= |ker(\lambda' \circ \phi_1)| \\ &= |ker(\phi_2 \circ \lambda)| \\ &= |ker(\phi_2)| \\ &= deg(\phi_2) && \text{(by } \mathbf{1.2.25}\text{)} \end{aligned}$$

Thus $deg(\phi_1) = deg(\phi_2)$. By the arbitrary choice of ϕ_1 and ϕ_2, we have proven the statement. ■

Definition 1.2.36: Let $\phi : E/k \to E'/k$ be an isogeny defined over k, and let L be a superfield of k. We define the *equivilance class of isogenies of ϕ over L* to be the following set:

$$[\phi]_L = \{\psi : E \to E' | \exists \text{ isomorphism } \lambda : E' \to E' \text{ such that } \psi = \lambda \circ \phi\}$$

Note that by combining **1.2.34**, **1.2.35**, and **1.2.36** we can understand that an equivalence class of isogenies, $[\phi]_L$, is a collection of isogenies with, the same degree, the same domain (up to L-isomorphism), the same codomain (up to L-isomorphism), and they all "basically do the same thing".

Definition 1.2.37: The *(general) ℓ-isogeny graph over the field k* is the graph made by the following:

- The vertices are k-isomorphism classes of (ordinary or supersingular) elliptic curves defined over k,
- The edges are k-equivalence classes of isogenies between the k-isomorphism classes of elliptic curves defined over k, such that the isogeny is defined over k and has a degree of ℓ.

Definition 1.2.38: The *supersingular ℓ-isogeny graph over the field k* is the graph made by the following:

- The vertices are k-isomorphism classes of supersingular elliptic curves defined over k,
- The edges are k-equivalence classes of isogenies between the k-isomorphism classes of supersingular elliptic curves defined over k, such that the isogeny is defined over k and has a degree of ℓ.

We denote this graph as $\mathcal{G}_\ell(k)$.

Note that for all fields k, it can be shown that $\mathcal{G}_\ell(k)$ is a proper subgraph of the general ℓ isogeny graph.

Definition 1.2.39: A polynomial $\Phi_\ell(X,Y) \in \mathbb{Z}[X,Y]$ is called the *ℓ-modular polynomial* if the following hold:

(a) $deg(\Phi_\ell) = \ell + 1$

(b) $\Phi_\ell(X,Y) = \Phi_\ell(Y,X)$

(c) There exists an ℓ-isogeny over $\overline{\mathbb{F}_p}$, $\phi : E_1 \to E_2$ with $j(E_1) = j_1$, $j(E_2) = j_2$ if and only if $\Phi_\ell(j_1, j_2) = 0$

Definition 1.2.40: Let $A, B \in \mathbb{Z}[X_1, X_2, \ldots, X_n]$. We define the *resultant polynomial of A and B with respect to X_i*, for some $i \in \{1, 2, \ldots, n\}$, as

$$Res_{X_i}(A,B) = a_0^e b_0^d \prod_{\substack{1 \le l \le d \\ 1 \le m \le e}} (\lambda_l - \mu_m)$$

Where e, d is the degrees of A and B respectively, a_0, b_0 are the leading coefficients of A and B respectively, and μ_l, λ_m are roots of A and B respectively. All with respect to X_i.

Definition 1.2.41: We define the *ℓ-resultant polynomial* as

$$Res_\ell(X) := Res_Y\left(\Phi_\ell, \frac{\partial}{\partial Y}\Phi_\ell\right)$$

Theorem 1.2.42: j is a root of $Res_\ell(X)$ if and only if the vertex $j \in \mathcal{G}_\ell(\overline{\mathbb{F}_p})$ is incident to a double edge.

Proof: This is proven in [Arp+23, Lemma 2.14] ■

1.3 Notation of $\mathcal{G}_\ell(\mathbb{F}_p)$ and $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$, and the definition of $\mathcal{S}_\ell^p$

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

Note that in this case, the vertices are $\overline{\mathbb{F}_p}$ isomorphism classes of elliptic curves defined over $\overline{\mathbb{F}_p}$. We know by **Theorem 1.2.7** that any two elliptic curves that are isomorphic to each other over $\overline{\mathbb{F}_p}$ must share j-invariants. Thus as a result we notate a vertex by the j-invariant of the elliptic curves in this isomorphism class represented by the vertex. All edges in $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$ are directed. Since there may be multi-edges in this graph, we stick with the same notation of edges introduced in section **1.1**.

Note that it can be shown that if j is supersingular, then $j \in \mathbb{F}_{p^2}$. If we wish to emphasize that a j-invariant is in a particular field we use the following notation

- If $j \in \mathbb{F}_{p^2}$, then we use the standard notation j.

- If $j \in \mathbb{F}_p$, then we use the notation $\mathbf{j}$.
- If $j \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$, then we use the notation $\boldsymbol{j}$
- If $j \in V(\mathcal{G}_\ell(\overline{\mathbb{F}_p}))$, then we call j supersingular.
- If $j \in V(\mathcal{G}_\ell(k)) \setminus V(\mathcal{G}_\ell(\overline{\mathbb{F}_p}))$, then we call j, ordinary.

Consider $\mathcal{G}_\ell(\mathbb{F}_p)$:

Note that in this case, the vertices are $\mathbb{F}_p$ isomorphism classes of elliptic curves defined over $\mathbb{F}_p$. Let $E/\mathbb{F}_p$ and $E^t/\mathbb{F}_p$ be supersingular elliptic curves such that E^t is the twist of E (we know that there is only one twist of E by **Theorem 1.2.20**). Furthermore, let $[E]$ and $[E^t]$ be the $\mathbb{F}_p$-isomorphism classes of the relative curves. Note that for any two curves in an $\mathbb{F}_p$ isomorphism class are isomorphic over $\overline{\mathbb{F}_p}$. Therefore by **Theorem 1.2.7** we know that all elliptic curves in an $\mathbb{F}_p$-isomorphism class have the same j-invariant. Let $j = j([E]) = j(E)$, and let $j^t = j([E^t]) = j(E^t)$. However, note that E and E^t are isomorphic over $\overline{\mathbb{F}_p}$ therefore we know that $j = j^t$. Thus come to the realization that a j invariant does not identify only one $\mathbb{F}_p$-isomorphism class, but rather two $\mathbb{F}_p$-isomorphism classes.

To distinguish between vertices with the same j-invariant, we will denote one of them as u_j and the other w_j. Note that in this case if $j \neq 1728$, then w_j is the vertex representing the $\mathbb{F}_p$ isomorphism class of the quadratic twist of an elliptic curve in the $\mathbb{F}_p$ isomorphism class represented by the vertex u_j. If $j = 1728$, then w_j is instead the vertex representing the $\mathbb{F}_p$ isomorphism class of the quartic twist of an elliptic curve in the $\mathbb{F}_p$ isomorphism class represented by the vertex u_j.

We will soon cover this in section 1.4, however, in $\mathcal{G}_\ell(\mathbb{F}_p)$ there are rarely any multi-edges or loops. Furthermore, it is most common that for every outgoing edge, there is only one incoming edge. Therefore, in most cases, if $u, w \in V(\mathcal{G}_\ell(\mathbb{F}_p))$ are adjacent, then we can identify the pair (u,w) and (w,u) with the singular edge $\{u,w\}$. Therefore, if we say that "v and w are connected by an isogeny" we mean they are adjacent by the pair (u,w) and (w,u). If we wish to be specific about which version of $\mathcal{G}_\ell(\mathbb{F}_p)$ we are talking about, we will use the simplified version of $\mathcal{G}_\ell(\mathbb{F}_p)$, $\Upsilon(\mathcal{G}_\ell(\mathbb{F}_p))$ to show that we are talking about a graph with undirected edges, no loops, and no multi-edges.

Lastly, we will generally notate distinct components of $\mathcal{G}_\ell(\mathbb{F}_p)$ by U and W. However, this may be partially misleading. We will come to find that it is not true that u_a and w_a are always on distinct components U and W, and it is also not true that u_a and w_a will always be on the same component. However, (later we will find that) in most cases u_a and w_a are on distinct components. Hence, we use the notation for U and W as distinct components.

The spine:

Definition 1.3.1: Let $F = \{\boldsymbol{j} \in V(\mathcal{G}_\ell(\overline{\mathbb{F}_p}))\}$. The *spine of the supersingular ℓ-isogeny graph over the field k* is defined as the following subgraph of $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$:

$$\mathcal{S}_\ell^p := \mathcal{G}_\ell(\overline{\mathbb{F}_p}) - F$$

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

Delfs and Galbraith in their 2013 paper [DG16] described the shape of $\mathcal{G}_\ell(\mathbb{F}_p)$ using notions as defined below.

Definition 1.4.1: The $\mathbb{F}_p$-isomorphism class of a supersingular elliptic curve E is said to be on the *surface* if $\text{End}_{\mathbb{F}_p}(E) = \mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$. On the other hand, the $\mathbb{F}_p$-isomorphism class of a supersingular elliptic curve E is said to be on the *floor* if $\text{End}_{\mathbb{F}_p}(E) = Z[\sqrt{-p}]$. We think of the floor and surface as being *levels* of the $\mathcal{G}_\ell(\mathbb{F}_p)$ graph.

Definition 1.4.2: A supersingular $\mathbb{F}_p$-isogeny $\phi : E \to E'$ is said to be *horizontal* if $\text{End}_{\mathbb{F}_p}(E) \simeq \text{End}_{\mathbb{F}_p}(E')$. If this equality does not hold, the isogeny is said to be *vertical*.

Using this we can identify the structure of $\mathcal{G}_\ell(\mathbb{F}_p)$ as described in [DG16].

Definition 1.4.3: Let $\mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field over $\mathbb{Q}$. We denote that *class number of* $\mathbb{Q}(\sqrt{-d})$ by $h(-d)$.

Theorem 1.4.4: The following cases describe the structure of $\mathcal{G}_\ell(\mathbb{F}_p)$:

1.) Suppose $p \equiv 1 \pmod 4$. Then there are $h(-p)$ $\mathbb{F}_p$-isomorphism classes of supersingular elliptic curves over $\mathbb{F}_p$, all being on the floor.

i. If $\ell = 2$, then for every vertex there is a horizontal 2-isogeny going to a (not necessarily distinct) vertex.

ii. If $\ell > 2$ and the Legendre symbol $\left(\frac{-p}{\ell}\right) = 1$, then for every vertex there are two horizontal ℓ-isogenies going to (not necessarily distinct) vertices.

2.) Suppose $p \equiv 3 \pmod 4$. Then there are two levels in the supersingular isogeny graph.

i. If $\ell = 2$, then we have two cases. One where $p \equiv 3 \pmod 8$, and another where $p \equiv 7 \pmod 8$.

A. Suppose $p \equiv 7 \pmod 8$. In this case, there exists $h(-p)$ vertices on each level of the graph. The surface and the floor are connected 1-to-1 with 2-isogenies, and on the surface, we have two horizontal 2-isogenies from each vertex going to (not necessarily distinct) vertices.

B. Suppose $p \equiv 3 \pmod 8$. In this case, there exist $h(-p)$ vertices on the surface and $3h(-p)$ vertices on the floor. For every isogeny on the surface, there are three 2-isogenies to (not necessarily distinct) vertices on the floor. Furthermore, there are no horizontal isogenies.

ii. If $\ell > 2$ and the Legendre symbol $\left(\frac{-p}{\ell}\right) = 1$, then from each vertex there are two horizontal ℓ-isogenies to (not necessarily distinct) vertices. There may or may not be vertical ℓ-isogenies.

Proof: This is proven in [DG16, 2.7] ■

Theorem 1.4.5: Let $u \in V(\mathcal{G}_\ell(\mathbb{F}_p))$ such that $p > \ell$, p is a prime, ℓ is a prime, and $\left(\frac{-p}{\ell}\right) = 1$. If u is on the floor, then u has no loops. If u is on the surface, then u has a loop if and only if $4\ell \geq p$, $p = 4c+3$ for some $c \in \mathbb{Z}_{>0}$, and $\ell = a^2 + a + 1 + c$ for some $a \in \mathbb{Z}$.

Proof: Let $E/\mathbb{F}_p$ be an elliptic curve. Let $\phi : E \to E$ be a degree ℓ isogeny defined over $\mathbb{F}_p$. By definition we know that $\phi \in \text{End}_{\mathbb{F}_p}(E)$. We know by [DG16] that if E is defined over $\mathbb{F}_p$ then $\text{End}_{\mathbb{F}_p}(E) = \mathbb{Z}[\sqrt{-p}]$ or $\text{End}_{\mathbb{F}_p}(E) = \mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$. Let us explore these two cases.

Case 1: Suppose that $\text{End}_{\mathbb{F}_p}(E) = \mathbb{Z}[\sqrt{-p}]$. As a result, we know that $[E]_{\mathbb{F}_p}$ is on the floor of $\mathcal{G}_\ell(\mathbb{F}_p)$. Since $\phi \in \text{End}_{\mathbb{F}_p}(E) = \mathbb{Z}[\sqrt{-p}]$, we know that there exists $a, b \in \mathbb{Z}$ such that $\phi = a + b\sqrt{-p}$. recall the fact that $deg(\phi) = N(\phi) = \phi\overline{\phi}$. Thus in our case we have

$$\begin{aligned} deg(\phi) &= \phi\overline{\phi} \\ \ell &= (a + b\sqrt{-p})(a - b\sqrt{-p}) \\ \ell &= a^2 + b^2 p \end{aligned}$$

Now, suppose in hopes of reaching a contradiction that $b^2 \geq 1$. Then

$$\ell = a^2 + b^2 p \geq a^2 + p \geq p$$

This contradicts our hypothesis of $\ell < p$. Thus it must be that $b^2 = 0 \Rightarrow b = 0$. Hence

$$\ell = a^2 + (0)^2 p = a^2$$

However, since ℓ is a prime number we know that ℓ cannot be a square of an integer. Hence we have a contradiction. Thus we conclude that there are no loops in this case.

Case 2: Suppose that $\text{End}_{\mathbb{F}_p}(E) = \mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$. As a result, we know that $[E]_{\mathbb{F}_p}$ is on the surface of $\mathcal{G}_\ell(\mathbb{F}_p)$. Since $\phi \in \text{End}_{\mathbb{F}_p}(E) = \mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$ we know that there exists $a, b \in \mathbb{Z}$ such that $\phi = a + b\left(\frac{1+\sqrt{-p}}{2}\right)$.

Recall the fact that $deg(\phi) = N(\phi) = \phi\overline{\phi}$. Thus in our case we have

$$\begin{aligned}
deg(\phi) &= \phi\overline{\phi} \\
\ell &= \left[a + b\left(\frac{1+\sqrt{-p}}{2}\right)\right]\left[a + b\left(\frac{1-\sqrt{-p}}{2}\right)\right] \\
\ell &= a^2 + ab\left(\frac{1+\sqrt{-p}}{2}\right) + ab\left(\frac{1-\sqrt{-p}}{2}\right) + b^2\left(\frac{(1+\sqrt{-p})(1-\sqrt{-p})}{2}\right) \\
\ell &= a^2 + ab\left(\frac{1+\sqrt{-p}+1-\sqrt{-p}}{2}\right) + b^2\left(\frac{1+p}{4}\right) \\
\ell &= a^2 + ab + \frac{b^2(1+p)}{4} \qquad (1) \\
4\ell &= 4a^2 + 4ab + b^2(1+p) \\
0 &= 4a^2 + 4ab + b^2(1+p) - 4\ell \\
&\Downarrow \text{(by quadratic formula)} \\
a &= \frac{-4b \pm \sqrt{(4b)^2 - 4(4)(b^2(1+p) - 4\ell)}}{2(4)} \\
a &= \frac{-4b \pm 4\sqrt{b^2 - (b^2(1+p) - 4\ell)}}{8} \\
a &= \frac{-b \pm \sqrt{b^2 - b^2 - b^2p + 4\ell}}{2} \\
2a &= -b \pm \sqrt{4\ell - b^2p}
\end{aligned}$$

As a result we know $\sqrt{4\ell - b^2p} \in \mathbb{Z}$. Since $\sqrt{4\ell - b^2p} \in \mathbb{Z} \subseteq \mathbb{R}$ we know

$$\begin{aligned}
4\ell - b^2p &\geq 0 \\
4\ell &\geq b^2p
\end{aligned}$$

Now, suppose in hopes of reaching a contradiction that $b^2 \geq 4$. As a result of this supposition we know that $4\ell \geq b^2p \geq 4p \Rightarrow \ell \geq p$ which contradicts our supposition that $p > \ell$. Now instead, suppose in hopes of reaching a contradiction that $b = 0$. Then from (1) we know that

$$\ell = a^2 + ab + \frac{b^2(1+p)}{4} = a^2 + a(0) + \frac{(0)^2(1+p)}{4} = a^2$$

Which contradicts the primality of ℓ. Hence we know that $b = \pm 1$ and $4\ell \geq p$.

Case 2.1 Suppose that $b = 1$ and $2a = -b + \sqrt{4\ell - b^2p}$. In this case we know

$$\begin{aligned}
2a &= -1 + \sqrt{4\ell - p} \\
2a + 1 &= \sqrt{4\ell - p} \qquad (2) \\
(2a+1)^2 &= 4\ell - p \\
4a^2 + 4a + 1 &= 4\ell - p
\end{aligned}$$

Now, recall that E is on the surface. From Theorem **1.4.4** we know that $p \equiv 3 \pmod 4$.

Hence we know that there exists $c \in \mathbb{Z}_{>0}$ (since $p > 3$) such that $p = 4c+3$. Thus we have

$$\begin{aligned} 4\ell - p &= 4a^2 + 4a + 1 \\ 4\ell - (4c+3) &= 4a^2 + 4a + 1 \\ 4\ell - 4c - 3 &= 4a^2 + 4a + 1 \\ 4\ell &= 4a^2 + 4a + 4 + 4c \\ \ell &= a^2 + a + 1 + c \end{aligned}$$

Note that (2) implies that $a \geq 0$. Hence we know that in this case, if ϕ is a loop on E, then there exists $a \in \mathbb{Z}_{\geq 0}$, $c \in \mathbb{Z}_{>0}$ such that $p = 4c+3$ and

$$\phi = a + \frac{1+\sqrt{-p}}{2} \qquad \text{and} \qquad \ell = a^2 + a + 1 + c$$

Case 2.2: Suppose $b = -1$ and $2a = -b + \sqrt{4\ell - b^2 p}$. In this case we have:

$$\begin{aligned} 2a &= 1 + \sqrt{4\ell - p} \\ 2a - 1 &= \sqrt{4\ell - p} \\ 2a - 2 + 1 &= \sqrt{4\ell - p} \\ 2(a-1) + 1 &= \sqrt{4\ell - p} \end{aligned}$$

Note that if we replace $a-1$ with d, then we know $2d+1 = \sqrt{4\ell - p}$. This is exactly Case 2.1. Hence we know that there exists $c \in \mathbb{Z}_{>0}$, $d \in \mathbb{Z}_{\geq 0}$ $a - 1 \in \mathbb{Z}_{\geq 0} \Rightarrow a \in \mathbb{Z}_{\geq 1}$ such that $p = 4c+3$, $\phi = a - \frac{1+\sqrt{-p}}{2}$, and

$$\begin{aligned} \ell &= d^2 + d + 1 + c \\ &= (a-1)^2 + (a-1) + 1 + c \\ &= a^2 - 2a + 1 + a - 1 + 1 + c \\ &= a^2 - a + 1 + c \end{aligned}$$

Case 2.3 Suppose $b = 1$ and $2a = -b - \sqrt{4\ell - b^2 p}$. In this case we have

$$\begin{aligned} 2a &= -1 - \sqrt{4\ell - p} \\ 2a + 1 &= -\sqrt{4\ell - p} \\ -2a - 1 &= \sqrt{4\ell - p} \\ -2a - 2 + 1 &= \sqrt{4\ell - p} \\ 2(-a-1) + 1 &= \sqrt{4\ell - p} \end{aligned} \tag{3}$$

Note that by (3) we know that $a \in \mathbb{Z}_{\leq -1} \Rightarrow -a - 1 \in \mathbb{Z}_{\geq 0}$. Thus if we replace $-a-1$ with d, we would again be in Case 2.1. Hence we know that there exists $c \in \mathbb{Z}_{>0}$, $a \in \mathbb{Z}_{\leq -1}$ such that $p = 4c+3$, $\phi = a + \frac{1+\sqrt{-p}}{2}$, and

$$\begin{aligned} \ell &= (-a-1)^2 + (-a-1) + 1 + c \\ &= a^2 + a + 1 + c \end{aligned}$$

Case 2.4: Suppose $b = -1$ and $2a = -b - \sqrt{4\ell - b^2 p}$. In this case we have

$$\begin{aligned} 2a &= 1 - \sqrt{4\ell - p} \\ 2a - 1 &= -\sqrt{4\ell - p} \\ -2a + 1 &= \sqrt{4\ell - p} \\ 2(-a) + 1 &= \sqrt{4\ell - p} \end{aligned}$$

Note that if we replace $-a$ with d, then we know that we are in Case 2.1, and hence we know that there exists $c \in \mathbb{Z}_{>0}$, $a \in \mathbb{Z}_{\leq 0}$ such that $p = 4c+3$, $\phi = a - \frac{1+\sqrt{-p}}{2}$, and

$$\begin{aligned} \ell &= d^2 + d + 1 + c \\ &= (-a)^2 + (-a) + 1 + c \\ &= a^2 - a + 1 + c \end{aligned}$$

Putting all of our results together, we know that if ϕ is a loop on a vertex on the surface, then $4\ell > p$ and there exists $x, y \in \mathbb{Z}$, $z \in \mathbb{Z}_{>0}$ such that $p = 4z+3$ and

$$\phi = x + \frac{1+\sqrt{-p}}{2} \qquad \text{and} \qquad \ell = x^2 + x + 1 + z \tag{4}$$

or,

$$\phi = y - \frac{1+\sqrt{-p}}{2} \qquad \text{and} \qquad \ell = y^2 - y + 1 + z \tag{5}$$

However, note that if we find an $x \in \mathbb{Z}$ such that $\ell = x^2 + x + 1 + z$, then we have

$$\begin{aligned} (x+1)^2 - (x+1) + 1 + z &= x^2 + 2x + 1 - x - 1 + 1 + z \\ &= x^2 + x + 1 + z \\ &= \ell \end{aligned}$$

hence (4) implies (5). Similarly, if we find a $y \in \mathbb{Z}$ such that $\ell = y^2 - y + 1 + z$, then we have

$$\begin{aligned} (y-1)^2 + (y-1) + 1 + z &= y^2 - 2y + 1 + y - 1 + 1 + z \\ &= y^2 - y + 1 + z \\ &= \ell \end{aligned}$$

hence (5) implies (4).

Note that since our proof in this section has only had a progression of if and only if statements, we know that we have proven this case.

Thus we can conclude that we have proven the statement in all of its cases.

■

Corollary 1.4.6: If $E/\mathbb{F}_p$ is an elliptic curve, then there either exists exactly 0 endomorphisms of degree ℓ, or there exists exactly 4 endomorphisms of degree ℓ.

Proof: The proof follows from the separate cases in the proof of 1.4.5. ■

Corollary 1.4.7: Let $p > \ell$ both primes ($p > 3$) such that $p \equiv 3 \pmod 4$. Let $c \in \mathbb{Z}_{>0}$ such that $p = 4c+3$. Suppose we try to find a solution to one of the following Diophantine equations

$$\ell = x^2 + x + 1 + c \qquad \ell = x^2 - x + 1 + c \tag{6}$$

If there does not exist a solution to one of the above Diophantine equations, then there are no loops in $\mathcal{G}_\ell(\mathbb{F}_p)$. If there exists $a \in \mathbb{Z}$ that satisfied one of the Diophantine equations above, then the following are endomorphisms of degree ℓ

$$\phi = x_\phi + \frac{1+\sqrt{-p}}{2}, \qquad \psi = x_\psi + \frac{1+\sqrt{-p}}{2}, \qquad \gamma = x_\gamma - \frac{1+\sqrt{-p}}{2}, \qquad \delta = x_\delta - \frac{1+\sqrt{-p}}{2}$$

where $x_\phi, x_\psi, x_\gamma, x_\delta$ can be found by following the following table:

Which diophantine equations did you find a solution for?	**which of the two stemming options is true for the solution you found?**	x_ϕ	x_ψ	x_γ	x_δ
$\ell = x^2 + x + 1 + c$	$a \geq 0$	a	$-a-1$	$a+1$	$-a$
	$a \leq -1$	$-a-1$	a	$-a$	$a+1$
$\ell = x^2 - x + 1 + c$	$a \geq 1$	$a-1$	$-a$	a	$-a+1$
	$a \leq 0$	$-a$	$a-1$	$-a+1$	a

Proof: If there was no solution to any of the Diophantine equations then we know that the conditions for **Theorem 1.4.5** are not satisfied and hence there are no loops in $\mathcal{G}_\ell(\mathbb{F}_p)$. In the other case where we were able to find a solution to one of the Diophantine equations, we then would be in one of the cases in the proof of **Theorem 1.4.5**, namely Case 2.1 through Case 2.4. From there we simply need to find the approapriate transformation to find ourselves in each of the other cases. We can verify that the variable transformations provided in *Table 1.4.7* put us in the appropriate cases. ■

Corollary 1.4.8: Let $p > \ell$ and $p \equiv 3 \pmod 4$. If $u \in V(\mathcal{G}_\ell(\mathbb{F}_p))$ has a loop, then u has exactly two loops and these two loops are duals of each other.

Proof: Suppose $p > \ell$, $p \equiv 4 \pmod 4$, and $u \in V(\mathcal{G}_\ell(\mathbb{F}_p))$ has a loop. By **Theorem 1.4.5** we know that there exists $x \in \mathbb{Z}$ such that $\ell = x^2 + x + 1 + c$, where $c \in \mathbb{N}$, $p = 4c+1$. By **Corollary 1.4.7** we can restrict x such that $x \in \mathbb{N}_0$. This way we know that the only endomorphisms of degree ℓ are

$$\phi = x + \frac{1+\sqrt{-p}}{2}, \qquad \psi = -x - 1 + \frac{1+\sqrt{-p}}{2}, \qquad \gamma = x + 1 - \frac{1+\sqrt{-p}}{2}, \qquad \delta = -x - \frac{1+\sqrt{-p}}{2}$$

Note that $\phi = -\delta$ and $\gamma = -\psi$. Hence ϕ is equivalent to δ and γ is equivalent to ψ. Hence u has a maximum of 2 loops. Furthermore, note that ϕ and γ are not equivalent to each other since they are not the same element of $\mathrm{End}_{\mathbb{F}_p}(u)$, nor are they negatives of each other. Hence u has exactly two loops.

Consider the following:

$$\begin{aligned}
\phi\gamma &= \left(x+\frac{1+\sqrt{-p}}{2}\right)\left(x+1-\frac{1+\sqrt{-p}}{2}\right)\\
&= x(x+1)-x\left(\frac{1+\sqrt{-p}}{2}\right)+(x+1)\left(\frac{1+\sqrt{-p}}{2}\right)-\left(\frac{1+\sqrt{-p}}{2}\right)^2\\
&= x^2+x+\frac{1+\sqrt{-p}}{2}-\frac{1-p+2\sqrt{-p}}{4}\\
&= x^2+x+\frac{1+\sqrt{-p}}{2}+\frac{p-1}{4}-\frac{\sqrt{-p}}{2}\\
&= x^2+x+\frac{1+\sqrt{-p}}{2}+\frac{p-1}{4}-\frac{\sqrt{-p}}{2}-\frac{1}{2}+\frac{1}{2}\\
&= x^2+x+\frac{1+\sqrt{-p}}{2}-\frac{1+\sqrt{-p}}{2}+\frac{p+1}{4}\\
&= x^2+x+\frac{p+1}{4}\\
&= x^2+x+\frac{4c+3+1}{4}\\
&= x^2+x+c+1\\
&= \ell
\end{aligned}$$

Hence we know that ϕ and γ are duals of each other. ■

Lemma 1.4.9: For $\alpha \in \mathbb{Z}_{>0}$, $f(x) = x^2+x-\alpha$ has integer roots if and only if $\alpha = \lfloor\sqrt{\alpha}\rfloor(\lfloor\sqrt{\alpha}\rfloor+1)$.

Proof: Let $\alpha \in \mathbb{Z}_{>0}$. Note that $0 = x^2+x-\alpha \Leftrightarrow \alpha = x(x+1)$. Hence α has integer factors that are one apart. This implies that the backward direction of the statement holds. Now let us prove the forward direction. Let $x \in \mathbb{Z}$ such that $x(x+1) = \alpha$. Note that it must be that $x > 0$ since $\alpha > 0$. Consider $\lfloor\sqrt{\alpha}\rfloor$. Note that if $\alpha = 1$ then we would have a contradiction on the fact that $1 \neq x(x+1)$ for any positive integer x. Similarly, we know that α cannot be equal to 3. If $\alpha = 2$ then $2 = \lfloor\sqrt{2}\rfloor(\lfloor\sqrt{2}\rfloor+1)$. Thus we see that for $\alpha = 1,2,3$, the forward direction is true. Thus, let us suppose $\alpha > 3$. As a result we know that $\lfloor\sqrt{\alpha}\rfloor > 1 \Rightarrow \lfloor\sqrt{\alpha}\rfloor - 1 > 0$. An important fact to recall is

$$\sqrt{\alpha}-1 < \lfloor\sqrt{\alpha}\rfloor \leq \sqrt{\alpha}$$

Now by the ordering of the real numbers, we know that $x < \lfloor\sqrt{\alpha}\rfloor, x > \lfloor\sqrt{\alpha}\rfloor$, or $x = \lfloor\sqrt{\alpha}\rfloor$.

Suppose in hopes of reaching a contradiction that $x < \lfloor\sqrt{\alpha}\rfloor$. Then we have

$$\begin{aligned}
\alpha &= x(x+1)\\
&< \lfloor\sqrt{\alpha}\rfloor(\lfloor\sqrt{\alpha}\rfloor+1)\\
&= \lfloor\sqrt{\alpha}\rfloor^2+\lfloor\sqrt{\alpha}\rfloor\\
&\leq \sqrt{\alpha}^2+\lfloor\sqrt{\alpha}\rfloor\\
&= \alpha+\lfloor\sqrt{\alpha}\rfloor\\
&< \alpha
\end{aligned}$$

hence we get $\alpha < \alpha$ which is a contradiction.

Now instead, suppose in hopes of reaching a contradiction that $x > \lfloor\sqrt{\alpha}\rfloor$. Then we have

$$\begin{aligned}\alpha &= x(x+1)\\ &> \lfloor\sqrt{\alpha}\rfloor(\lfloor\sqrt{\alpha}\rfloor+1)\\ &> (\sqrt{\alpha}-1)(\sqrt{\alpha}-1+1)\\ &= \alpha-\sqrt{\alpha}\\ &> \alpha\end{aligned}$$

hence we get $\alpha > \alpha$ which is a contradiction.

Thus we conclude that $x = \lfloor\sqrt{\alpha}\rfloor$ and thus the lemma is proven. ■

Corollary 1.4.10: Let p and ℓ be primes satisfying $\ell < p < 4\ell$ and $p > 3$. $\mathcal{G}_\ell(\mathbb{F}_p)$ has loops if and only if

$$\ell - c - 1 = \lfloor\sqrt{\ell-c-1}\rfloor \cdot \left(\lfloor\sqrt{\ell-c-1}\rfloor + 1\right)$$

where $c \in \mathbb{Z}_{>0}$ such that $p = 4c+3$.

Proof: The corollary follows from combining **Lemma 1.4.9** and **Theorem 1.4.5**. ■

Using the easy computation provided by **Corollary 1.4.10** we can compute the p values which would result in $\mathcal{G}_\ell(\mathbb{F}_p)$ having loops for a given ℓ value. We have computed the list of p values which result in $\mathcal{G}_\ell(\mathbb{F}_p)$ having loops for all ℓ less than 100 in the following table

ℓ	**Which values of p result in $\mathcal{G}_\ell(\mathbb{F}_p)$ having loops**
2	7
3	11
5	11, 19
7	19
11	19, 43
13	43
17	19, 43, 59, 67
19	67
23	43, 67, 83
29	67, 107
31	43
37	67, 139
41	43, 83, 139, 163
43	163
47	67, 107, 139, 163, 179
53	131, 163, 211
59	67, 211, 227
61	163
67	No such p values exist
71	163, 283
73	211, 283
79	307
83	107, 163, 211, 251, 283, 307, 331
89	131, 307, 331, 347
97	163, 307, 379

Table 1: List of p values which result in $\mathcal{G}_\ell(\mathbb{F}_p)$ having a loop given a particular ℓ value for all ℓ smaller than 100.

Now instead of only loops we will expand our view to multi-edges. Suppose that $E/\mathbb{F}_p, E'/\mathbb{F}_p$ are supersingular elliptic curves. Furthermore, suppose that there exist two nonequivalent isogenies of degree ℓ both having domain E and codomain E' and both being defined over $\mathbb{F}_p$, call these isogenies ϕ and ψ. Recall that we know a dual isogeny exists for both ϕ and ψ, notated $\widehat{\phi}$ and $\widehat{\psi}$. Note that we know that each dual is unique, hence we know $\widehat{\phi}$ is nonequivalent to $\widehat{\psi}$.

Recall that by definition $\widehat{\phi}$ is the unique map such that $\phi\widehat{\phi} = \ell$, and the same is true form $\psi\widehat{\psi} = \ell$. Therefore, it must be true that $\phi\widehat{\psi} \neq \ell$. Therefore there must exist an element of $\mathrm{End}_{\mathbb{F}_p}(E)$ that is not the ℓ multiplication map and has degree ℓ^2. Using this we can use the norm equation for each endomorphism ring to find which values of p and ℓ imply a multi-edge within $\mathcal{G}_\ell(\mathbb{F}_p)$. If there exists a multi-edge with the domain being on the floor, then there must exist $a, b \in \mathbb{Z}$ such that

$$\ell^2 = a^2 + b^2 p \qquad (1)$$

And if there exists a multi-edge with the domain being on the surface, then there must exist $a, b \in \mathbb{Z}$ such that

$$\ell^2 = a^2 + ab + b^2(1+c) \qquad (2)$$

where $p = 4c+3$. With this we can find bounds for (1) and (2). We find that in order for there exist a solution for (1), we require $0 < a \leq \ell$ and $0 < b \leq \sqrt{\ell}$, and $\ell < p < \ell^2$. On the other hand, we find that in order for there to exist a solution for (2), we require $0 < a \leq \ell$ and $-\sqrt{\ell} \leq b < 0$ or $0 < b \leq \sqrt{\ell}$, and $\ell < p < 4\ell^2$. Using these bounds we can find p and ℓ values that would result in a multi-edge in $\mathcal{G}_\ell(\mathbb{F}_p)$, as given in *table 2*.

Note that by *table 2* we can see that surface multi-edges happen only when loops happen. Furthermore, we can also see that multi edges happen on the surface only when $p \equiv 3 \pmod 4$. However, this we have not proven. An thus we provide the following three conjectures:

Conjecture 1: If there exists a multi-edge of degree ℓ on the floor of $\mathcal{G}_\ell(\mathbb{F}_p)$, then $p \equiv 1 \pmod 4$.

Conjecture 2: There exists a multi-edge of degree ℓ on the surface of $\mathcal{G}_\ell(\mathbb{F}_p)$ if and only if the multi-edge is created from loops.

Conjecture 3: If there exists a solution to the Diophantine equation $\ell^2 = a^2 + ab + b^2(1+c)$ for $p = 4c+3$, then b is odd.

The reason we state the third conjecture is because if b could be even then we would have a multi-edge in the surface and the floor at the same time which would contradict conjectures 1 and 2.

1.5 Miscellaneous facts

Let us look at some well-known facts about $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$.

Theorem 1.5.1: The following are information that are well known about $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$

(a) $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$ is a directed graph with loops and no non-directional edges.

(b) Let $j \in V(\mathcal{G}_\ell(\overline{\mathbb{F}_p}))$, then ${}_+d_j = \ell + 1$. If $j \notin \overline{N}_0$ and $j \notin \overline{N}_{1728}$ then ${}_-d_j = \ell + 1$. In this way (in most cases), most vertices in $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$ have the same out-degree and in-degree. Hence $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$ is referred to as an $(\ell+1)$-*regular graph*[1].

[1]Note that $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$ is not a true $(\ell+1)$-regular graph. For an integer n, G is an n-regular directed graph if for every vertex $v \in V(G)$, ${}_+d_v = {}_-d_v = n$. This is not the case for $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$. However, $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$ is a true $(\ell+1)$-*out-regular graph.*

Value of ℓ	p values which result in a multi-edge with domain in the floor	p values which result in a multi-edge with domain on the surface
2	NA	7
3	NA	11
5	NA	11, 19
7	13	19
11	13	19, 43
13	17	43
17	NA	19, 43, 59, 67
19	29, 37	67
23	37	43, 67, 83
29	NA	67, 107
31	37, 53, 61	43
37	73	67, 139
41	73	43, 83, 139, 163
43	61	163
47	NA	67, 107, 139, 163, 179
53	97	131, 163, 211
59	109	67, 211, 227
61	73, 97, 113	163
67	109	NA
71	NA	163, 283
73	97, 137	211, 283
79	109, 149, 157	307
83	157	107, 163, 211, 251, 283, 207, 311
89	97	131, 307, 331, 347
97	113, 193	163,307,379

Table 2: List of values of ℓ and p that result in a multi-edge in $\mathcal{G}_\ell(\mathbb{F}_p)$. Note that "NA" means that no such combinations exist

(c) $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$ is a strongly connected component of the general ℓ isogeny graph.

(d) $\mathcal{S}_\ell^p$ is a strongly connected subgraph of $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$

(e) The number of vertices in $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$ are as follows:

$$|V(\mathcal{G}_\ell(\overline{\mathbb{F}_p}))| = \left\lfloor \frac{p}{12} \right\rfloor + \begin{cases} 0 & \text{if } p \equiv 1 \pmod{12} \\ 1 & \text{if } p \equiv 5,7 \pmod{12} \\ 2 & \text{if } p \equiv 11 \pmod{12} \end{cases}$$

Note that as a result of **Theorem 1.5.1 (c)** and **(d)** we know that $ecc^+(u) = ecc^-(u)$ for all $u \in V(\mathcal{G}_\ell(\overline{\mathbb{F}_p}))$. Hence we can simply refer to *the* eccentricity of a vertex and *the* distance between two vertices in this graph.

Now let us look at some other facts about $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$.

Theorem 1.5.2: Let $j_0 \in \overline{k}$. Then there exists an elliptic curve E defined over the field $k(j_0)$ such that $j(E) = j_0$.

Theorem 1.5.3: $0 \in V(\mathcal{G}_\ell(\overline{\mathbb{F}_p})) \iff p \equiv 2 \pmod 3$, otherwise 0 is ordinary. Furthermore, $1728 \in V(\mathcal{G}_\ell(\overline{\mathbb{F}_p})) \iff p \equiv 3 \pmod 4$, otherwise 1728 is ordinary.

Proof: This is proven in [Sil09, V, 4.4] and [Sil09, V, 4.5]. ■

Theorem 1.5.4: $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$ has no loops if and only if the Legendre symbol $\left(\frac{s^2-4\ell}{p}\right) = 1$ for all $s \in \mathbb{N}_0$ such that $s^2 \leq 4\ell$.

Proof: This is proven in [Gha24, Theorem 3.1] ■

Corollary 1.5.5: $\mathcal{G}_2(\overline{\mathbb{F}_p})$ has no loops if and only if:

$$p \equiv 1, 9, \text{ or } 25 \pmod{56}$$

Proof: This is proven in [Gha24, Example 3.3] ■

Corollary 1.5.6: $\mathcal{G}_3(\overline{\mathbb{F}_p})$ has no loops if and only if:

$$p \equiv 1, 25, 49, 67, 91, 97, 115, 163, 169, \text{ or } 235 \pmod{264}$$

Proof: This is proven in [Gha24, Example 3.4] ■

Theorem 1.5.7: $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$ has no multi-edges if and only if $p \equiv 1 \pmod{12}$ and $\left(\frac{s^2-4\ell^2}{p}\right) = 1$ for all $s \in \mathbb{N}$ such that $s^2 < 4\ell^2$

Proof: This is proven in [Gha24, Theorem 3.5] ■

Corollary 1.5.8: $\mathcal{G}_2(\overline{\mathbb{F}_p})$ has no multi-edges if and only if:

$$p \equiv 1, 109, 121, 169, 289, \text{ or } 361 \pmod{420}$$

Proof: This is proven in [Gha24, Example 3.5] ■

Corollary 1.5.9: $\mathcal{G}_3(\overline{\mathbb{F}_p})$ has no multi-edge if and only if:

$$\begin{aligned} p \equiv 1, 169, 289, 361, 529, 841, 961, 1369, 1681, 1849, 2209, 2641, 2689, \\ 2809, 3481, 3529, 3721, 4321, 4489, 5041, 5329, 5569, 6169, 6241, \\ 6889, 7561, 7681, 7921, 8089, \text{ or } 8761 \pmod{9240} \end{aligned}$$

Proof: This is proven in [Gha24, Example 3.6] ■

Corollary 1.5.10: $\mathcal{G}_2(\overline{\mathbb{F}_p})$ has no loops nor multi-edges if and only if:

$$p \equiv 1, 121, 169, 289, 361, \text{ or } 529 \pmod{840}$$

Proof: Let p be a prime such that the following hold:

$$p \equiv m \pmod{420} \qquad \text{and} \qquad p \equiv n \pmod{56}$$

for some $m, n \in \mathbb{Z}$ such that $0 \leq m \leq 419$, and $0 \leq n \leq 55$. This by the definition of modulo classes implies that there exists $a, b \in \mathbb{Z}$ such that:

$$p = 420a + m \qquad \text{and} \qquad p = 56b + n$$

From this we get the following:

$$\begin{aligned} p &= p \\ 420a + m &= 56b + n \\ n - m &= 420a - 56b \\ n - m &= 28(15a - 2b) \\ n &= 28(15a - 2b) + m \end{aligned}$$

Let $15a - 2b = c$. Now since $0 \leq n \leq 55$, we have the following

$$\begin{aligned} 0 \leq \quad & n \quad \leq 55 \\ 0 \leq & 28c + m \leq 55 \\ -m \leq \quad & 28c \quad \leq 55 - m \\ \tfrac{-m}{28} \leq \quad & c \quad \leq \tfrac{55-m}{28} \end{aligned}$$

Therefore, if we now know m, then we can find c, and hence we can find n.

Suppose that $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$ has no multiedges. Then we have the following cases:

Case 1: Suppose $p \equiv 1 \pmod{420}$ (AKA: $m = 1$). We know that $\frac{-1}{28} \leq c \leq \frac{55-1}{28} \Rightarrow -0.0357\ldots \leq c \leq 1.928\ldots \Rightarrow$ $c = 0$ or 1. If $c = 0$, then $n = 28(0)+1 = 1$. If $c = 1$, then $n = 28(1)+1 = 29$. Since we wish to have n such that $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$ has no loops as well as no multi-edges, then it must be that $n = 1$.

Case 2: Suppose $m = 109$. Via a similar approach as in Case 1 we find that $n = 25$

Case 3: Suppose $m = 121$. Then $n = 9$

Case 4: Suppose $m = 169$. Then $n = 1$

Case 5: Suppose $m = 289$. Then $n = 9$

Case 6: Suppose $m = 261$. Then $n = 25$

Now in order solve the system of equations $p \equiv m \pmod{420} \iff p = 420x+m$, $p \equiv n \pmod{56} \iff p = 56y+n$, we need only to solve the Diophantine equations

$$15x + 2y = \frac{m-n}{28}$$

By solving the Diophantine equation in each case we have the following:

Case 1: $15x+2y = 0 \Rightarrow x = -2d, y = 15d, d \in \mathbb{Z}$. Thus $p = 420x+1 = 420(-2d)+1 = 840(-d)+1 \Rightarrow$ $p \equiv 1 \pmod{840}$

Case 2: $15x+2y = 3 \Rightarrow x = 3+2d, y = -21-15d, d \in \mathbb{Z}$. Thus $p = 420(3+2d)+109 = 840(d+1)+$ $529 \Rightarrow p \equiv 529 \pmod{840}$

Case 3: $15x+2y = 4 \Rightarrow x = 4+2d, y = -28-15d, d \in \mathbb{Z}$. Thus $p = 420(4+2d)+121 = 840(d+2)+$ $121 \Rightarrow p \equiv 121 \pmod{840}$

Case 4: $15x+2y = 6 \Rightarrow x = 6+2d, y = -42-15d, d \in \mathbb{Z}$. Thus $p = 420(6+2d)+169 = 840(d+3)+$ $169 \Rightarrow p \equiv 169 \pmod{840}$

Case 5: $15x+2y = 10 \Rightarrow x = 10+2d, y = -70-15d, d \in \mathbb{Z}$. Thus $p = 420(10+2d)+289 = 840(d+$ $5)+289 \Rightarrow p \equiv 289 \pmod{840}$

Case 6: $15x+2y = 12 \Rightarrow x = 12+2d, y = -84-15d, d \in \mathbb{Z}$. Thus $p = 420(12+2d)+361 = 840(d+$ $6)+361 \Rightarrow p \equiv 361 \pmod{840}$

Putting all the cases together we get $p \equiv 1, 121, 169, 289, 361,$ or $529 \pmod{840}$. Thus we have shown the forward implication. The backwards implication is easy to see. Hence we have proven the statement. ■

Corollary 1.5.11: If $\mathcal{G}_3(\overline{\mathbb{F}_p})$ has no multi-edges, then $\mathcal{G}_3(\overline{\mathbb{F}_p})$ has no loops.

Proof: Note that the conditions of $\mathcal{G}_3(\overline{\mathbb{F}_p})$ not having any loops is encompassed by the conditions of $\mathcal{G}_3(\overline{\mathbb{F}_p})$ not having any multi-edges. Hence if $\mathcal{G}_3(\overline{\mathbb{F}_p})$ has no multi-edges, then it has no loops. ■

Corollary 1.5.12: $\mathcal{G}_3(\overline{\mathbb{F}_p})$ has no loops nor multi-edges if and only if:

$$p \equiv 1, 169, 289, 361, 529, 841, 961, 1369, 1681, 1849, 2209, 2641, 2689,$$
$$2809, 3481, 3529, 3721, 4321, 4489, 5041, 5329, 5569, 6169, 6241,$$
$$6889, 7561, 7681, 7921, 8089, \text{ or } 8761 \pmod{9240}$$

Proof: The proof follows from **Corollary 1.5.11**. ■

Theorem 1.5.13: In $\mathcal{G}_2(\overline{\mathbb{F}_p})$, only the following j-invariants have loops:

$j = -3375$: This j-invariant has two distinct loops. Note that -3375 is supersingular if and only if $p \equiv 3, 5,$ or $6 \pmod 7$.

$j = 1728$: This j-invariant has a singular loop. (refer to **Theorem 1.5.3** for when 1728 is supersingular).

$j = 8000$: This j-invariant has a singular loop. Note that 8000 is supersingular if and only if $p \equiv 5$ or $7 \pmod 8$.

Furthermore, in $\mathcal{G}_2(\overline{\mathbb{F}_p})$, on the following j-invariants have multi-edges:

$j = -3375$: This j-invariant has two distinct loops.

$j = 0$: There exist three distinct edges of the form $(0, 54000)$.

$j = 1728$: There exists two distinct edges of the form $(1728, 287496)$

j: If j is a root of the polynomial

$$x^2 + 191025x - 121287375$$

then j has two outgoing edges to the same vertex.

Proof: This is proven in [Arp+23, Section 2.2] ■

Theorem 1.5.14: Let $p > 5$, and let $E/\mathbb{F}_p$ be a supersingular elliptic curve. Then

$$\mathrm{End}_{\mathbb{F}_p}(E) = \mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right] \iff E[2] \subseteq E(\mathbb{F}_p)$$

Proof: This is proven in [Arp+23, Lemma 3.6] ■

Corollary 1.5.15: Let $p > 5$, and let $E/\mathbb{F}_p$ be supersingular. If $p \equiv 1 \pmod 4$, then $E[2] \not\subseteq E(\mathbb{F}_p)$.

Proof: This is followed by combining **Theorem 1.5.14** and **Theorem 1.4.4**. ■

Theorem 1.5.16: Let $E/\mathbb{F}_p$ be an elliptic curve and let $E^t/\mathbb{F}_p$ be its quadratic twist. Then

$$\mathrm{End}_{\mathbb{F}_p}(E) \simeq \mathrm{End}_{\mathbb{F}_p}(E^t)$$

Proof: This is proven in [Arp+23, Corollary 3.7] ■

Theorem 1.5.17: If $p \equiv 3 \pmod 4$, then $u_{1728}, w_{1728} \in V(\mathcal{G}_\ell(\mathbb{F}_p))$ are places such that u_{1728} is on the floor and w_{1728} is on the surface.

Proof: This is proven in [Arp+23, Example 3.8] ■

Corollary 1.5.18: If $j \neq 1728$, then either both $u_j, w_j \in V(\mathcal{G}_\ell(\mathbb{F}_p))$ are on the surface, or they are both on the floor.

Proof: We know from **Theorem 1.2.20** that for each $u_j \in V(\mathcal{G}_\ell(\mathbb{F}_p))$, there exists exactly one twist $w_j \in V(\mathcal{G}_\ell(\mathbb{F}_p))$. If $j \neq 1728$, then w_j is the quadratic twist of u_j, and if $j = 1728$, then w_j is the quartic twist of v_j. Then the statement follows from **Theorem 1.5.16** and **Theorem 1.5.17**. ■

1.6 Structure of the Spine

Note that we defined the spine to be a subgraph of $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$ by removing all vertices not in $\mathbb{F}_p$ and their incident edges. However, we can make the spine using $\mathcal{G}_\ell(\mathbb{F}_p)$ in the following way:

1. Construct the graph $\mathcal{G}_\ell(\mathbb{F}_p)$,
2. Identify each pair of vertices with the same j-invariant, v_j, w_j as a singular vertex j.
3. Identify the existing equivalent edges (isogenies) with their equivalent edges over $\overline{\mathbb{F}_p}$.
4. Add any edges defined over $\overline{\mathbb{F}_p}$ that have both end vertices in $\mathbb{F}_p$.

There is a strong relationship between the structure of the spine and the $\mathcal{G}_\ell(\mathbb{F}_p)$ graph. To be able to describe the structure of the spine we need to understand what happens when we go from $\mathcal{G}_\ell(\mathbb{F}_p)$ to $\mathcal{S}_\ell^p$. In order to communicate this let us define the following.

Definition 1.6.1: Let $\Gamma : \mathcal{G}_\ell(\mathbb{F}_p) \to \mathcal{G}_\ell(\overline{\mathbb{F}_p})$ such that $\Gamma([E]_{\mathbb{F}_p}) = [E]_{\overline{\mathbb{F}_p}}$ and $\Gamma([\phi]_{\mathbb{F}_p}) = [\phi]_{\overline{\mathbb{F}_p}}$. Furthermore, define $\Theta : Im(\Gamma) \to \mathcal{G}_\ell(\overline{\mathbb{F}_p})$ such that if two vertices in $Im(\Gamma)$ have isogenies of degree ℓ between them that are not defined over $\mathbb{F}_p$, then Θ adds those edges into the graph $Im(\Gamma)$. Lastly define $\Omega : \mathcal{G}_\ell(\mathbb{F}_p) \to \mathcal{S}_\ell^p$ such that $\Omega = \Theta \circ \Gamma$.

Note in the process of going from $\mathcal{G}_\ell(\mathbb{F}_p)$ to $\mathcal{S}_\ell^p$, Γ is describing steps 2 and 3, while Θ is describing step 4.

Theorem 1.6.2: Let $E/\mathbb{F}_p$ be an elliptic curve with $j(E) \neq 0, 1728$. Suppose that there are two ℓ-isogenies, ϕ and ψ, defined over $\mathbb{F}_p$ with domain E. Then ϕ is equivalent to ψ over $\mathbb{F}_p$ if and only if ϕ is equivalent to ψ over $\overline{\mathbb{F}_p}$.

Proof: This is proved in [Arp+23, Lemma 3.10]. ■

Note that this theorem implies that for any $u_{\mathbf{j}}, u_{\mathbf{b}}, u_{\mathbf{c}} \in \mathcal{G}_\ell(\mathbb{F}_p)$, if $\{u_{\mathbf{j}}, u_{\mathbf{b}}\}, \{u_{\mathbf{j}}, u_{\mathbf{c}}\} \in E(\mathcal{G}_\ell(\mathbb{F}_p))$, are distinct edges (where $\mathbf{b}$ and $\mathbf{c}$ are not necessarily distinct), then there exist distinct edges $(\mathbf{j}, \mathbf{b})$ and $(\mathbf{j}, \mathbf{c})$ in $E(\mathcal{G}_\ell(\overline{\mathbb{F}_p}))$ and vice versa.

Definition 1.6.3: Define the map

$$\Lambda : \Upsilon(\mathcal{G}_\ell(\mathbb{F}_p)) \to \Upsilon(\mathcal{G}_\ell(\mathbb{F}_p)) \text{ such that } u_a \mapsto w_a, \text{ and } \{u_a, u_b\} \mapsto \{w_a, w_b\}$$

for all supersingular $a, b \in \mathbb{F}_p$. Let U and W be distinct components of $\Upsilon(\mathcal{G}_\ell(\mathbb{F}_p))$.

(a) If $\Lambda|_U$ is a graph isomorphism and $Im(\Lambda|_U) = W$, then we say that U and W *stack*.

(b) If there exists $u \in V(U)$ such that $\Lambda(u) \in V(U)$, then we say that U *folds*.

(c) Suppose a and b are distinct supersingular j invariants in $\mathbb{F}_p$. Furthermore, suppose G and H are distinct components of $\Gamma(\mathcal{G}_\ell(\mathbb{F}_p))$ such that $a \in V(G)$ and $b \in V(H)$. If it is the case such that $(a,b) \notin E(\Gamma(\mathcal{G}_\ell(\mathbb{F}_p)))$, but $(a,b) \in E(\mathcal{S}_\ell^p)$, then we say that the two components U and W become *attached by a new edge*.

(d) If $u_a \in V(U)$, $w_a \in V(w)$, and $j(N_{u_a}) \neq j(N_{w_a})$, then we say that the two components U and W become *attached along a j-invariant a*.

Remark: Notice the following result from the above definitions:

- Definitions (a), (b), and (d) describe what happens to the structure of $\mathcal{G}_\ell(\mathbb{F}_p)$ as Γ is applied to it.
- Definition (c) is describing what happens to $\Gamma(\mathcal{G}_\ell(\mathbb{F}_p))$ as Θ is applied to it.
- Suppose two components $U, W \subseteq \mathcal{G}_\ell(\mathbb{F}_p)$ stack with each other. As a result we know that for any $a,b \in \mathbb{F}_p$ not equal to 0 or 1728, $u_a, u_b \in V(U)$, if $(u_a,u_b) \in E(U)$, then $(w_a,w_b) \in E(W)$. Furthermore, we know that there only exists one edge of the form $(a,b) \in \Gamma(U \cup W)$. In other words, edges stack.
- Suppose $U \subseteq \mathcal{G}_\ell(\mathbb{F}_p)$ is a component which folds. Due to a result in [Arp+23] we know that U is a symmetric component. Hence we know that for any $a,b \in \mathbb{F}_p$ not equal to 0 or 1728, $u_a, u_b \in V(U)$ if $(u_a,u_b) \in E(U)$, then $(w_a,w_b) \in E(U)$. Furthermore, we know that there exists a single edge (in the case where (u_a,u_b) is not a multi-edge) of the form $(a,b) \in E(\Gamma(U))$. In other words, when a component folds, the edges fold as well.

Theorem 1.6.4: A component of $\mathcal{G}_\ell(\mathbb{F}_p)$ stacks if and only if it does not fold

Proof: Let us prove the statement in both directions:

($\Rightarrow$) Let U be a component of $\mathcal{G}_\ell(\mathbb{F}_p)$, and suppose U stacks. This by definition implies that there exists a distinct component W of $\mathcal{G}_\ell(\mathbb{F}_p)$ such that $\Lambda|_U$ is an isomorphism from U to W which sends a vertex to its unique twist. Hence we know that for all $u \in V(U)$, the twist of u exists on a distinct component. Now suppose in hopes of reaching a contradiction that U folds. By definition, this supposition implies that there exists a vertex $u_0 \in V(U)$ such that $\Lambda(u_0) \in V(U)$. In other words, a vertex exists that has a twist on the same component. This contradicts our earlier result that every vertex on U has its twist on a distinct component. Thus we conclude that if U stacks, then U cannot fold.

($\Leftarrow$) Let U be a component of $\mathcal{G}_\ell(\mathbb{F}_p)$, and suppose U folds. This by definition implies that there exists a vertex $u_0 \in V(U)$ such that $\Lambda(u_0) \in V(U)$. In other words, there exists a vertex in U such that its twist is also in U. Now, suppose in hopes of reaching a contradiction that U stacks. By definition, this supposition implies that there exists a distinct component W of $\mathcal{G}_\ell(\mathbb{F}_p)$ such that $\Lambda|_U$ is a graph isomorphism from U to W. In other words, every vertex of U has its twist on a distinct component W. This contradicts our result with u_0. Hence we conclude that if U folds, then it cannot stack.

■

Theorem 1.6.5: Let $a,b \in V(\Gamma(\mathcal{G}_\ell(\mathbb{F}_p)))$ be two vertices such that when Θ is applied, there exists a new edge $e=(a,b)$, with $a \neq 0,1728$. Then there exist two distinct edges of the form (a,b).

Proof: This is proved in [Arp+23, Lemma 3.14]. ■

Corollary 1.6.6: For $j \in V(\Gamma(\mathcal{G}_\ell(\mathbb{F}_p)))$, $j \neq 0,1728$, a maximum of $\frac{\ell+1}{2}$ edge attachments involving j can take place.

Proof: If there are more than $\frac{\ell+1}{2}$ edge attachments incident to the same vertex $j \neq 0,1728$, then j would need to have an out-degree larger than $\ell+1$, by **Theorem 1.6.5**. This violates the maximum out-degree property of $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$. ■

Theorem 1.6.7: The only p values that result in $\mathcal{S}_\ell^p$ being a graph of a single vertex are $p=2,3,5,7,13,37$.

Proof: We know by [DG16] that if $p>3$ then

$$\left|V(\mathcal{S}_\ell^p)\right| = \begin{cases} \frac{1}{2}h(-4p) & \text{if } p \equiv 1 \pmod 4 \\ h(-p) & \text{if } p \equiv 7 \pmod 8 \\ 2h(-p) & = \text{if } p \equiv 3 \pmod 8 \end{cases}$$

where $h(d)$ is the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{d})$. It has been proved by Baker, Stark, and Heegner that the square free numbers which result in a discriminant d such that $h(d)=1$ are the numbers

$$\{-1,-2,-3,-7,-11,-19,-43,-67,-163\}$$

Furthermore, it was proved by Baker and Stark that the square free numbers which result in a discriminant d such that $h(d)=2$ are the numbers:

$$\{-5,-6,-10,-13,-15,-22,-35,-37,-51,-58,-91,-115,-123,-187,-235,-267,-403,-427\}$$

Note that the potential p values in the first set are $\{2,3,7,11,19,43,67,163\}$. However, by the above, we know that each prime would result in a single vertex if and only if $p \equiv 7 \pmod 8$, and the only prime in this set which has that property is 7. Thus we know that $\mathcal{S}_\ell^7$ is a single vertex. On the other hand, the potential values of p in the set of square-free numbers which result in a discriminant d such that $h(d)=2$ are $\{5,13,37\}$. By the above, we know that each prime would result in a single vertex if and only if $p \equiv 1 \pmod 4$ which holds true for all of them. Hence we know that $\mathcal{S}_\ell^5, \mathcal{S}_\ell^{13}, \mathcal{S}_\ell^{37}$ are single vertices. Hence the p values that result in $\mathcal{S}_\ell^p$ having only one vertex are $p=5,7,13,37$. We know that these will be the only such primes, due to the fact that we would need $h(-4p)=2$ or $h(-p)=1$ depending on the congruence class of p.

Now suppose $p=2$, we know that there exists only one supersingular elliptic curve shown by [Sil09, p. V4. 148]. Furthermore, we also know that for $p=3$ there only exists a singular supersingular elliptic curve as shown by [Sil09, V4, 4.1]. Thus in both of those cases, $\mathcal{S}_\ell^p = \mathcal{G}_\ell(\mathbb{F}_p)$, and there only exists one vertex. ■

For this subsection suppose $\ell > 2$:

Theorem 1.6.8: Suppose an attachment along a j-invariant has taken place. Then:

(a) The attachment happened for $j = 1728$.

(b) $N_{u_{1728}}(\mathcal{G}_\ell(\mathbb{F}_p)) = \{u_a, w_a\}$, and $N_{u_{1728}}(\mathcal{G}_\ell(\mathbb{F}_p)) = \{u_b, w_b\}$ for some $a, b \in \mathbb{F}_{p^2}$.

Proof: This is proved in [Arp+23, Proposition 3.16]. ■

Theorem 1.6.9: Let $a \neq 0, 1728$. If $N_{u_a}(\mathcal{G}_\ell(\mathbb{F}_p)) = \{u_b, u_c\}$ then $N_{w_a}(\mathcal{G}_\ell(\mathbb{F}_p)) = \{w_b, w_c\}$.

Proof: This is proved in [Arp+23, Lemma 3.17]. ■

Theorem 1.6.10: If $\left(\frac{-p}{\ell}\right) = -1$, then all components stack. On the other hand, if $\left(\frac{-p}{\ell}\right) = 1$ and $p \equiv 3 \pmod 4$ then the components containing 1728 fold and get (vertex) attached by 1728.

Proof: This was proved in [Arp+23, Theorem 3.18] ■

Theorem 1.6.11: $\left(\frac{-p}{3}\right) = -1$ if and only if all components stack. On the other hand, if $\left(\frac{-p}{3}\right) = 1$ then while passing from $\mathcal{G}_\ell(\mathbb{F}_p)$ to $\mathcal{S}_\ell^p$ the following hold:

(a) $p \equiv 3 \pmod 4$ if and only if the distinct components containing u_{1728}, w_{1728} fold and then get attached along the j invariant 1728. The component containing u_{1728} contains both u_0 and w_0, and the component containing w_{1728} contains both u_{54000} and w_{54000}. These two components are the only components that get attached by a vertex, and they are the only components which fold.

(b) $p \equiv 1 \pmod 4$ if and only if there is a single component that contains u_0, w_0, u_{54000}, and w_{54000}. This component is the only component that folds.

(c) All other components stack.

Proof: This is proved in [Arp+23, Theorem 3.21]. ■

Corollary 1.6.12: If vertex attachment takes place for $\ell = 3$, then at least one component is folded. But the converse does not hold true.

Proof: This fact follows from combining (a) and (b). ■

Corollary 1.6.13: No component folds or stacks if and only if there are no edges in $\mathcal{G}_3(\mathbb{F}_p)$.

Proof: Note that this follows from the above and the fact that $\left(\frac{-p}{3}\right) = -1$ if and only if there are no edges in $\mathcal{G}_3(\mathbb{F}_p)$ as proved in **Theorem 1.4.4**. ■

Corollary 1.6.14: Suppose $\left(\frac{-p}{\ell}\right) = -1$. If there exists **j**, **j'**$\in \mathbb{F}_p$ such that (**j**,**j'**) is an edge in $\mathcal{S}_\ell^p$, then a new edge was added between **j** and **j'** by Θ. Hence (**j**,**j'**) is a multi-edge.

Proof: Suppose $\left(\frac{-p}{\ell}\right) = -1$. This results in there being no isogenies of degree ℓ defined over $\mathbb{F}_p$ in $\mathcal{G}_\ell(\mathbb{F}_p)$. In other words, there are no edges in $\mathcal{G}_\ell(\mathbb{F}_p)$. As a result, we know that there are also no edges in $\Gamma(\mathcal{G}_\ell(\mathbb{F}_p))$. Now, suppose that there is an isogeny between two vertices in $\mathcal{S}_\ell^p$. We know that this edge is not defined over $\mathbb{F}_p$, hence Θ must have added it. By **Theorem 1.6.5** we know that this edge is actually a multi-edge. ■

Remark: Note **Corollary 1.6.14** tells us that if there are any edges in $\mathcal{S}_\ell^p$ when $\left(\frac{-p}{\ell}\right) = -1$, then an edge attachment has taken place.

For this subsection suppose $\ell = 2$:

Theorem 1.6.15: If $(u_a, u_b) \in E(\mathcal{G}_\ell(\mathbb{F}_p))$, then $(w_a, w_b) \in E(\mathcal{G}_\ell(\mathbb{F}_p))$.

Proof: This is proved in [Arp+23, Corollary 3.23]. ■

Theorem 1.6.16: In the process of going from $\mathcal{G}_\ell(\mathbb{F}_p)$ to $\mathcal{S}_\ell^p$, the following happen:

(a) Stacking (if there is a component that does not fold)

(b) Folding:

i. If $p \equiv 1 \pmod 4$, then the only component that folds is U where U is an edge (u_{8000}, w_{8000}).

ii. If $p \equiv 3 \pmod 4$, then the only component that folds is U where U contains both vertices of 1728, and U is symmetric (with respect to j-invariants) with symmetry line going through the 1728 vertices.

(c) If there exists a supersingular root in $\mathbb{F}_p$ of the polynomial

$$R_{2,1}(x) = x^2 + 191025x - 121287375$$

then there may or may not be an edge attachment. Otherwise, no edge attachment will take place.

(d) no attachments along a j-invariant.

Proof: This is proved in [Arp+23, Section 3.4]. ■

Note that just because there is a root of $R_{2,1}(x)$ that is supersingular and in $\mathbb{F}_p$ it does not mean that the implied edge is an edge attachment. $R_{2,1}(x)$ is a factor of $Res_2(x)$ and hence the roots of $R_{2,1}(x)$ only categorize multi-edges within $\mathcal{S}_\ell^p$. This does encapsulate edge attachments due to **Theorem 1.6.5**.

Theorem 1.6.17: If $p \equiv 3 \pmod 8$, $p > 101$, and $R_{2,1}(x)$ has a supersingular root in $\mathbb{F}_p$, then there is an edge attachment. On the other hand, if $p \equiv 7 \pmod 8$ then a supersingular root in $\mathbb{F}_p$ of the polynomial does not necessarily imply an edge attachment.

Proof: This is proved in [Arp+23, Corollary 3.30]. ■

In these next few pages we will build an explicit structure of the spine for $\ell = 2$ and $\ell = 3$.

$\ell = 2$:

Lemma 1.6.18: Let p be an odd prime. Then

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

Proof: This result follows by Euler's Criterion. ■

Lemma 1.6.19: Let p be an odd prime not equal to 3. Then

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 11 \pmod{12} \\ -1 & \text{if } p \equiv 5 \text{ or } 7 \pmod{12} \end{cases}$$

Proof: Let p be an odd prime not equal to 3. Consider $\left(\frac{3}{p}\right)$. Note that by Quadratic Reciprocity we have

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{3-1}{2}} = (-1)^{\frac{p-1}{2}}$$

Hence we fall into two cases, one where $p \equiv 1 \pmod 4$, and another where $p \equiv 3 \pmod 4$. Let us explore these cases.

Case 1: Suppose $p \equiv 1 \pmod 4$. In this case, we know that

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = 1 \implies \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$$

Hence we know that 3 is a quadratic residue mod p if and only if p is a quadratic residue mod 3. By an exhaustive search, we can see that p is a quadratic residue mod 3 if and only if $p \equiv 1 \pmod 3$, and p is not a quadratic residue mod 3 if and only if $p \equiv -1 \pmod 3$. Combining these congruence conditions along with our supposition of $p \equiv 1 \pmod 4$ using the Chinese Remainder Theorem (CRT) we find that

- if $p \equiv 1 \pmod{12}$, then $\left(\frac{3}{p}\right) = 1$.
- if $p \equiv 5 \pmod{12}$, then $\left(\frac{3}{p}\right) = -1$.

Case 2: Suppose $p \equiv 3 \pmod 4$. In this case, we know that

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = -1 \implies \left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right)$$

Hence we know that 3 is a quadratic residue mod p if and only if p is not a quadratic residue mod 3. Recall that we know p is a quadratic residue mod 3 if and only if $p \equiv 1 \pmod 3$, and p is not a quadratic residue mod 3 if and only if $p \equiv -1 \pmod 3$. Combining these congruence conditions along with our supposition of $p \equiv 3 \pmod 4$ using the Chinese Remainder Theorem (CRT) we find that

- if $p \equiv 11 \pmod{12}$, then $\left(\frac{3}{p}\right) = 1$.
- if $p \equiv 7 \pmod{12}$, then $\left(\frac{3}{p}\right) = -1$.

Since the two cases cover all possible values of p we know that we have covered every possible value of p. Hence we have proved the statement. ■

Lemma 1.6.20: Let p be an odd prime not equal to 5. Then

$$\left(\frac{5}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 4 \pmod{5} \\ -1 & \text{if } p \equiv 2 \text{ or } 3 \pmod{5} \end{cases}$$

Proof: Suppose p is an odd prime not equal to 5. Then by Quadratic Reciprocity we know

$$\left(\frac{5}{p}\right)\left(\frac{p}{5}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{5-1}{2}} = 1$$

Hence we know that 5 is a quadratic residue mod p if and only if p is a quadratic residue mod 5. By doing an exhaustive search we see that p is a quadratic residue mod 5 if and only if $p \equiv \pm 1 \pmod{5}$. Hence the statement follows. ■

Corollary 1.6.21: Let p be an odd prime not equal to 3 or 5. Then

$$\left(\frac{-15}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1,17,19,23,31,47,49, \text{ or } 53 \pmod{60} \\ -1 & \text{if } p \equiv 7,11,13,29,37,41,43, \text{ or } 59 \pmod{60} \end{cases}$$

Proof: Suppose p is an odd prime not equal to 3 or 5. Then by the multiplicative property of the Legendre symbol we have

$$\left(\frac{-15}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)\left(\frac{5}{p}\right)$$

Define the tuple $(a, \quad b, \quad c) = \left(\left(\frac{-1}{p}\right), \quad \left(\frac{3}{p}\right), \quad \left(\frac{5}{p}\right)\right)$. Note that by looking at each one of these tuples we can determine the value of $\left(\frac{-15}{p}\right)$. Using **Lemma 1.6.18**, **Lemma 1.6.19**, **Lemma 1.6.20**, and CRT we get the following table of values:

$(a, \quad b, \quad c)$	$p \pmod{60}$
$(1, \quad 1, \quad 1)$	1, 49
$(1, \quad 1, \quad -1)$	13, 37
$(1, \quad -1, \quad 1)$	29, 41
$(1, \quad -1, \quad -1)$	17, 53
$(-1, \quad 1, \quad 1)$	11, 59
$(-1, \quad 1, \quad -1)$	23, 47
$(-1, \quad -1, \quad 1)$	19, 31
$(-1, \quad -1, \quad -1)$	7, 43

The statement follows from the above table. ■

Lemma 1.6.22: The Hilbert class polynomial $H_{15}(x)$ has a supersingular root in $\mathbb{F}_p$ if and only if $p = 7, 13$ or $p \equiv 11$ or $14 \pmod{15}$.

Proof: We know that $H_{15}(x)$ has a supersingular root if and only if $\left(\frac{-15}{p}\right) = -1$. By **corollary 1.6.21** we know that $H_{15}(x)$ has a supersingular root if and only if $p \equiv 7, 11, 13, 29, 37, 41, 43,$ or $59 \pmod{60}$.

Note that $H_{15}(x) = x^2 + 191025x - 121287375$ hence by the quadratic formula we know

$$H_{15}(x) = 0 \iff \frac{-191025 \pm 85995\sqrt{5}}{2} = 0$$

Hence we know that $H_{15}(x)$ has a root in $\mathbb{F}_p$ if and only if $p|85995$ or 5 is a quadratic residue modulo p. Let us explore each case.

Case 1: Suppose $p|85995 \Leftrightarrow p|(3^3 \cdot 5 \cdot 7^2 \cdot 13)$ Hence $p = 3, 5, 7,$ or 13.

Case 2: Suppose 5 is a quadratic residue modulo p. By **Lemma 1.6.20** we know that this is true if and only if $p \equiv \pm 1 \pmod{5}$.

Hence $H_{15}(x)$ has a root in $\mathbb{F}_p$ if and only if $p = 3, 5, 7, 13$ or $p \equiv \pm 1 \pmod{5}$.

Combining the conditions for supersingular roots and roots in $\mathbb{F}_p$ we find that $H_{15}(x)$ has a supersingular root in $\mathbb{F}_p$ if and only if $p = 7, 13$ or $p \equiv 11, 29, 41, 59 \pmod{60}$

Claim: $\{p > 2 : p \in [11]_{60} \cup [41]_{60}\} = \{p > 2 : p \in [11]_{15}\}$ and $\{p > 2 : p \in [29]_{60} \cup [59]_{60}\} = \{p > 2 : p \in [14]_{15}\}$.

proof: Suppose $x \equiv 11 \pmod{15}$. By definition, we know that there exists $n \in \mathbb{Z}$ such that $x = 15n + 11$. Since $n \in \mathbb{Z}$ we know that either n is congruent to 0, 1, 2, or 3 modulo 4. Let us explore each case:

- Suppose $n = 4m$ for some $m \in \mathbb{Z}$. Then we have

$$x = 15n + 11 = 15(4m) + 11 = 60m + 11$$

and hence $x \in [11]_{60}$.

- Suppose $n = 4m + 1$ for some $m \in \mathbb{Z}$. Then we have

$$x = 15n + 11 = 15(4m + 1) + 11 = 60m + 15 + 11 = 60m + 26$$

and hence $x \in [26]_{60}$

- Suppose $n = 4m + 2$ for some $m \in \mathbb{Z}$. Then we have

$$x = 15n + 11 = 15(4m + 2) + 11 = 60m + 30 + 11 = 60m + 41$$

and hence $x \in [41]_{60}$

- Suppose $n = 4m + 3$ for some $m \in \mathbb{Z}$. Then we have

$$x = 15n + 11 = 15(4m + 3) + 11 = 60m + 45 + 11 = 60m + 56$$

and hence $x \in [56]_{60}$

Hence $[11]_{15} = [11]_{60} \cup [26]_{60} \cup [41]_{60} \cup [56]_{60}$. However, if we only consider odd prime numbers, we know that p cannot be in $[26]_{60} \cup [56]_{60}$. Hence any primes in $[11]_{15}$ are in $[11]_{60} \cup [41]_{60}$ and vice versa. Thus $\{p > 2 : p \in [11]_{60} \cup [41]_{60}\} = \{p > 2 : p \in [11]_{15}\}$.

Now instead suppose $y \in [14]_{15}$. By definition, we know that there exists $r \in \mathbb{Z}$ such that $y = 15r + 14$. Since $r \in \mathbb{Z}$ we know that either n is congruent to 0, 1, 2, or 3 modulo 4. Let us explore each case:

- Suppose $r = 4s$ for some $s \in \mathbb{Z}$. Then we have

$$x = 15r + 14 = 15(4s) + 14 = 60s + 14$$

  and hence $x \in [14]_{60}$.
- Suppose $r = 4s + 1$ for some $s \in \mathbb{Z}$. Then we have

$$x = 15r + 14 = 15(4s + 1) + 14 = 60s + 15 + 14 = 60s + 29$$

  and hence $x \in [29]_{60}$.
- Suppose $r = 4s + 2$ for some $s \in \mathbb{Z}$. Then we have

$$x = 15r + 14 = 15(4s + 2) + 14 = 60s + 30 + 14 = 60s + 44$$

  and hence $x \in [44]_{60}$.
- Suppose $r = 4s + 3$ for some $s \in \mathbb{Z}$. Then we have

$$x = 15r + 14 = 15(4s + 3) + 14 = 60s + 45 + 14 = 60s + 59$$

  and hence $x \in [59]_{60}$.

Hence $[14]_{15} = [14]_{60} \cup [29]_{60} \cup [44]_{60} \cup [59]_{60}$. However, if we only consider odd prime numbers, we know that p cannot be in $[14]_{60} \cup [44]_{60}$. Hence any primes in $[14]_{15}$ are in $[29]_{60} \cup [59]_{60}$ and vice versa. Thus $\{p > 2 : p \in [29]_{60} \cup [59]_{60}\} = \{p > 2 : p \in [14]_{15}\}$

Thus by the claim we conclude that $H_{15}(x)$ has a supersingular root in $\mathbb{F}_p$ if and only if $p = 7, 13$ or $p \equiv 11, 14 \pmod{15}$. ■

Theorem 1.6.23: In $\mathcal{S}_2^p$ the following statements are true:

(a) If $p = 2$, then $\mathcal{S}_2^p$ is a single vertex with j-invariant 0. And this vertex has a triple multi-edge loop with itself.

(b) If $p = 3$, then $\mathcal{S}_2^p$ is a single vertex with j-invariant 0. And this vertex has a triple multi-edge loop with itself.

(c) If $p = 5$, then $\mathcal{S}_2^p$ is a single vertex with j-invariant 0. And this vertex has a triple multi-edge loop with itself.

(d) If $p = 7$, then $\mathcal{S}_2^p$ is a single vertex with j-invariant 6. And this vertex has a triple multi-edge loop with itself.

(e) If $p = 13$, then $\mathcal{S}_2^p$ is a single vertex with j-invariant 5. And this vertex has a triple multi-edge loop with itself.

(f) Suppose $p \neq 2, 3, 5, 7$, and 13.

i. If $p \equiv 1 \pmod 3$, then there does not exist any triple edges in $\mathcal{S}_2^p$ nor $\mathcal{G}_2(\overline{\mathbb{F}_p})$.

ii. If $p \equiv 2 \pmod 3$, then there exists a unique triple multi-edge of the form $(0, 54000)$ in $\mathcal{G}_2(\overline{\mathbb{F}_p})$ (and hence $\mathcal{S}_2^p$) and this edge is not a loop.

Proof: Suppose that there exists $v \in \mathcal{G}_2(\overline{\mathbb{F}_p})$ such that v is incident to an out-triple-multi-edge. By the definition of the modular polynomial, we know that $\Phi_2(v,X) = (X-j)^3 g(v,X)$ where $j \in \overline{\mathbb{F}_p}$, and $g \in \overline{\mathbb{F}_p}[Y,X]$. However, we know that Φ_2 is a polynomial of degree 3 for both of its variables. Hence $g(v,X)$ must be equal to a constant. In fact, due to the properties of non-square modular polynomials, we know that $g(v,X)$ must be ± 1, and hence we can simply ignore it. Hence we have $\Phi_2(v,X) = (X-j)^3$. As a result we have:

$$\Phi_2(v,X) = (X-j)^3$$
$$\frac{\partial}{\partial X}\Phi_2(v,X) = 3(X-j)^2$$
$$\frac{\partial^2}{\partial X^2}\Phi_2(v,X) = 6(X-j)$$

Hence (if $6 \neq 0$), j is a root of $\Phi_2(v,X)$, $\frac{\partial}{\partial X}\Phi_2(v,X)$, and $\frac{\partial^2}{\partial X^2}\Phi_2(v,X)$. As such, by definition we know that v is a root of both of the following polynomials:

$$\mathcal{R}es_1(Y) := Res_X\left(\Phi_2(X,Y), \frac{\partial}{\partial X}\Phi_2(X,Y)\right)$$

$$\mathcal{R}es_2(Y) := Res_X\left(\frac{\partial}{\partial X}\Phi_2(X,Y), \frac{\partial^2}{\partial X^2}\Phi_2(X,Y)\right)$$

A simple computation reveals that the explicit forms of $\mathcal{R}es_1$ and $\mathcal{R}es_2$ are:

$$\mathcal{R}es_1(Y) = (-4)(Y-1728)(Y+3375)^2(Y)^2(Y^2+191025Y-121287375)^2$$

$$\mathcal{R}es_2(Y) = (-12)(Y)(Y-405)(Y^2-2571Y+1492425)$$

For simplification purposes, let the symbolic variable Y be represented by x for the rest of the duration of this proof. Furthermore, let the following notation stand:

$$f_1(x) = -4 \qquad g_1(x) = -12$$
$$f_2(x) = x - 1728 \qquad g_2(x) = x$$
$$f_3(x) = x \qquad g_3(x) = x - 405$$
$$f_4(x) = x + 3375 \qquad g_4(x) = x^2 - 2571x + 1492425$$
$$f_5(x) = x^2 + 191025x - 121287375$$

Note that if $f_i(x_0) = 0$ and $g_l(x_0) = 0$ for some $x_0 \in \overline{\mathbb{F}_p}$, then x_0 is a root of both $\mathcal{R}es_1(x)$ and $\mathcal{R}es_2(x)$. Hence by definition, x_0 is a root of $\Phi_2(v,X)$, $\frac{\partial}{\partial X}\Phi_2(v,X)$, and $\frac{\partial^2}{\partial X^2}\Phi_2(v,X)$, making it have a triple edge in the isogeny graph.

Thus we are interested in x_0 which is a root of f_i and g_l for some i,l. On top of that, we want to know when x_0 is supersingular so that we know when $x_0 \in V(\mathcal{G}_\ell(\overline{\mathbb{F}_p}))$.

Firstly, let us find the potential x_0 values. In order to find all possible x_0 values we must solve all systems of the form $f_i(x) = g_l(x) = 0$. Therefore we have the following cases:

1.) $f_1(x) = g_1(x) = 0$	2.) $f_1(x) = g_2(x) = 0$	3.) $f_1(x) = g_3(x) = 0$	4.) $f_1(x) = g_4(x) = 0$
5.) $f_2(x) = g_1(x) = 0$	6.) $f_2(x) = g_2(x) = 0$	7.) $f_2(x) = g_3(x) = 0$	8.) $f_2(x) = g_4(x) = 0$
9.) $f_3(x) = g_1(x) = 0$	10.) $f_3(x) = g_2(x) = 0$	11.) $f_3(x) = g_3(x) = 0$	12.) $f_3(x) = g_4(x) = 0$
13.) $f_4(x) = g_1(x) = 0$	14.) $f_4(x) = g_2(x) = 0$	15.) $f_4(x) = g_3(x) = 0$	16.) $f_4(x) = g_4(x) = 0$
17.) $f_5(x) = g_1(x) = 0$	18.) $f_5(x) = g_2(x) = 0$	19.) $f_5(x) = g_3(x) = 0$	20.) $f_5(x) = g_4(x) = 0$

Note, however, that this is all dependent on the fact that $6 \neq 0$. We know that $6 = 0$ in $\overline{\mathbb{F}_p}$ if and only if $p = 2$ or $p = 3$. So let us consider those cases first.

Suppose $p = 2$. We know that in this case 0 is the only supersingular j-invariant. Hence if we look at the 2-modular polynomial at 0 we get $\Phi_2(0,x) = x^3$. Hence we know that 0 has a triple loop to its self.

Now, suppose $p = 3$. We know that in this case 0 is the only supersingular j-invarant. Hence if we look at the 2-modular polynomial at 0 we again get $\Phi_2(0,x) = x^3$. Hence we know that 0 has a triple loop to its self.

Note that for cases 1.) , 2.) , 3.) , 4.) , 5.) , 9.) , 13.) , 17.) , we either have $f_1(x) = 0$ or $g_1(x) = 0$ which would result in $4 = 0$ or $12 = 0$ respectively. Both of these would land us in the $p = 2,3$ case which we have already covered. Hence we skip these cases.

Case 6: Suppose $f_2(x) = g_2(x) = 0$. Hence we have the system:

$$\begin{cases} f_2(x) = 0 \\ g_2(x) = 0 \end{cases} \longrightarrow \begin{cases} x - 1728 = 0 \\ x = 0 \end{cases} \longrightarrow \begin{cases} x = 1728 \\ x = 0 \end{cases} \Rightarrow 0 = 1728$$

We can see that the system is true in $\overline{\mathbb{F}_p}$ when $p|1728 \Leftrightarrow p|(2^6 \cdot 3^3) \Rightarrow p = 2$ or 3.
Thus Case 6: results in a triple edge for $x_0 = 0 \in \overline{\mathbb{F}_2}$, and $x_0 = 0 \in \overline{\mathbb{F}_3}$.

Case 7: Suppose $f_2(x) = g_3(x) = 0$. Hence we have the system:

$$\begin{cases} f_2(x) = 0 \\ g_3(x) = 0 \end{cases} \longrightarrow \begin{cases} x - 1728 = 0 \\ x - 405 = 0 \end{cases} \longrightarrow \begin{cases} x = 1728 \\ x = 405 \end{cases} \Rightarrow 1728 = 405 \Leftrightarrow 1323 = 0$$

We can see that the system is true in $\overline{\mathbb{F}_p}$ when $p|1323 \Leftrightarrow p|(3^3 \cdot 7^2) \Rightarrow p = 3$ or 7. Note that $1728 \equiv 405 \equiv 0 \pmod 3$ and $1728 \equiv 405 \equiv 6 \pmod 7$.
Thus Case 7: results in a triple edge or $x_0 = 0 \in \overline{\mathbb{F}_3}$, and $x_0 = 6 \in \overline{\mathbb{F}_7}$.

Case 8: Suppose $f_2(x) = g_4(x) = 0$. Hence we have the system:

$$\begin{cases} f_2(x) = 0 \\ g_4(x) = 0 \end{cases} \longrightarrow \begin{cases} x - 1728 = 0 \\ g_4(x) = 0 \end{cases} \longrightarrow \begin{cases} x = 1728 \\ g_4(x) = 0 \end{cases} \longrightarrow \begin{cases} x = 1728 \\ g_4(1728) = 0 \end{cases} \longrightarrow \begin{cases} x = 1728 \\ 35721 = 0 \end{cases}$$

We can see that the system is true in $\overline{\mathbb{F}_p}$ when $p|35721 \Leftrightarrow p|(3^5 \cdot 7^2) \Rightarrow p = 3$ or $p = 7$.
Thus similar to the last case, Case 8: results in a triple edge or $x_0 = 0 \in \overline{\mathbb{F}_3}$, and $x_0 = 6 \in \overline{\mathbb{F}_7}$.

Case 10: Suppose $f_3(x) = g_2(x) = 0$. Hence we have the system:

$$\begin{cases} f_3(x) = 0 \\ g_2(x) = 0 \end{cases} \longrightarrow \begin{cases} x = 0 \\ x = 0 \end{cases}$$

Note that there are no restrictions on p. Thus Case 10: results in a triple edge for $x_0 = 0 \in \overline{\mathbb{F}_p}$ for any prime p.

Case 11: Suppose $f_3(x) = g_3(x) = 0$. Hence we have the system:

$$\begin{cases} f_3(x) = 0 \\ g_3(x) = 0 \end{cases} \longrightarrow \begin{cases} x = 0 \\ x - 405 = 0 \end{cases} \longrightarrow \begin{cases} x = 0 \\ x = 405 \end{cases} \Rightarrow 405 = 0$$

We can see that the system is true in $\overline{\mathbb{F}_p}$ when $p|405 \Leftrightarrow p|(3^4 \cdot 5) \Rightarrow p = 3, 5$.
Thus Case 11: results in a triple edge for $x_0 = 0 \in \overline{\mathbb{F}_3}$ and $x_0 = 0 \in \overline{\mathbb{F}_5}$.

Case 12: Suppose $f_3(x) = g_4(x) = 0$. Hence we have the system:

$$\begin{cases} f_3(x) = 0 \\ g_4(x) = 0 \end{cases} \longrightarrow \begin{cases} x = 0 \\ g_4(x) = 0 \end{cases} \longrightarrow \begin{cases} x = 0 \\ g_4(0) = 0 \end{cases} \longrightarrow \begin{cases} x = 0 \\ 1492425 = 0 \end{cases}$$

We can see that the system is true in $\overline{\mathbb{F}_p}$ when $p|1492425 \Leftrightarrow p|(3^3 \cdot 5^2 \cdot 11 \cdot 67) \Rightarrow p = 3, 5, 11,$ or 67.
Thus Case 12: results in a triple edge for $x_0 = 0$ in $\overline{\mathbb{F}_3}, \overline{\mathbb{F}_5}, \overline{\mathbb{F}_{11}}, \overline{\mathbb{F}_{67}}$.

Case 14: Suppose $f_4(x) = g_2(x) = 0$. Hence we have the system:

$$\begin{cases} f_4(x) = 0 \\ g_2(x) = 0 \end{cases} \longrightarrow \begin{cases} x + 3375 = 0 \\ x = 0 \end{cases} \longrightarrow \begin{cases} x = -3375 \\ x = 0 \end{cases} \Rightarrow 0 = -3375 \Leftrightarrow 3375 = 0$$

We can see that the system is true in $\overline{\mathbb{F}_p}$ when $p|3375 \Leftrightarrow p|(3^3 \cdot 5^3) \Rightarrow p = 3$ or 5.
Thus Case 14: results in a triple edge for $x_0 = 0 \in \overline{\mathbb{F}_3}$ and $x_0 = 0 \in \overline{\mathbb{F}_5}$.

Case 15: Suppose $f_4(x) = g_3(x) = 0$. Hence we have the system:

$$\begin{cases} f_4(x) = 0 \\ g_3(x) = 0 \end{cases} \longrightarrow \begin{cases} x + 3375 = 0 \\ x - 405 = 0 \end{cases} \longrightarrow \begin{cases} x = -3375 \\ x = 405 \end{cases} \Rightarrow 405 = -3375 \Leftrightarrow 3780 = 0$$

We can see that the system is true in $\overline{\mathbb{F}_p}$ when $p|3780 \Leftrightarrow p|(2^2 \cdot 3^3 \cdot 5 \cdot 7) \Rightarrow p = 2, 3, 5,$ or 7. Note that

$$x \equiv -3375 \equiv 405 \equiv \begin{cases} 1 & (\text{mod } 2) \\ 0 & (\text{mod } 3) \\ 0 & (\text{mod } 5) \\ 6 & (\text{mod } 7) \end{cases}$$

Thus Case 15: results in a triple edge for $x_0 = 1 \in \overline{\mathbb{F}_2}, x_0 = 0 \in \overline{\mathbb{F}_3}, x_0 = 0 \in \overline{\mathbb{F}_5}$, and $x_0 = 6 \in \overline{\mathbb{F}_7}$.

Case 16: Suppose $f_4(x) = g_4(x) = 0$. Hence we have the system:

$$\begin{cases} f_4(x) = 0 \\ g_4(x) = 0 \end{cases} \longrightarrow \begin{cases} x + 3375 = 0 \\ g_4(x) = 0 \end{cases} \longrightarrow \begin{cases} x = -3375 \\ g_4(x) = 0 \end{cases} \longrightarrow \begin{cases} x = -3375 \\ g_4(-3375) = 0 \end{cases} \longrightarrow \begin{cases} x = -3375 \\ 21560175 = 0 \end{cases}$$

We can see that the system is true in $\overline{\mathbb{F}_p}$ when $p|21560175 \Leftrightarrow p|(3^5 \cdot 5^2 \cdot 7 \cdot 13^2) \Rightarrow p = 3, 5, 7,$ or 13. Note that

$$x \equiv -3375 \equiv \begin{cases} 0 & (\text{mod } 3) \\ 0 & (\text{mod } 5) \\ 6 & (\text{mod } 7) \\ 5 & (\text{mod } 13) \end{cases}$$

Thus Case 16: results in a triple edge for $x_0 = 0 \in \overline{\mathbb{F}_3}, x_0 = 0 \in \overline{\mathbb{F}_5}, x_0 = 6 \in \overline{\mathbb{F}_7}$, and $x_0 = 5 \in \overline{\mathbb{F}_{13}}$.

Case 18: Suppose $f_5(x) = g_2(x) = 0$. Hence we have the system:

$$\begin{cases} f_5(x) = 0 \\ g_2(x) = 0 \end{cases} \longrightarrow \begin{cases} f_5(x) = 0 \\ x = 0 \end{cases} \longrightarrow \begin{cases} f_5(0) = 0 \\ x = 0 \end{cases} \longrightarrow \begin{cases} -121287375 = 0 \\ x = 0 \end{cases}$$

We can see that the system is true in $\overline{\mathbb{F}_p}$ when $p|121287375 \Rightarrow p|(3^5 \cdot 5^3 \cdot 11^3) \Rightarrow p = 3, 5, 11$. Thus Case 18: results in a triple edge for $x_0 = 0 \in \overline{\mathbb{F}_3}, \overline{\mathbb{F}_5}$, and $\overline{\mathbb{F}_{11}}$.

Case 19: Suppose $f_5(x) = g_3(x) = 0$. Hence we have the system:

$$\begin{cases} f_5(x) = 0 \\ g_3(x) = 0 \end{cases} \longrightarrow \begin{cases} f_5(x) = 0 \\ x - 405 = 0 \end{cases} \longrightarrow \begin{cases} f_5(405) = 0 \\ x = 405 \end{cases} \longrightarrow \begin{cases} -43758225 = 0 \\ x = 405 \end{cases}$$

We can see that the system is true in $\overline{\mathbb{F}_p}$ when $p|43758225 \Rightarrow p|(3^6 \cdot 5^2 \cdot 7^4) \Rightarrow p = 3, 5, 7$. Note that

$$x \equiv 405 \equiv \begin{cases} 0 & (\text{mod } 3) \\ 0 & (\text{mod } 5) \\ 6 & (\text{mod } 7) \end{cases}$$

Thus Case 19: results in a triple edge for $x_0 = 0 \in \overline{\mathbb{F}_3}, x_0 = 0 \in \overline{\mathbb{F}_5}$, and $x_0 = 6 \in \overline{\mathbb{F}_7}$.

Case 20: Suppose $f_5(x) = g_3(x) = 0$. Hence we have the system:

$$\begin{cases} f_5(x) = 0 \\ g_4(x) = 0 \end{cases} \longrightarrow \begin{cases} x^2 + 191025x - 121287375 = 0 \\ x^2 - 2571x + 1492425 = 0 \end{cases}$$

$$\longrightarrow \begin{cases} x = \frac{-191025 \pm 85995\sqrt{5}}{2} \\ x = \frac{2571 \pm 39\sqrt{421}}{2} \end{cases} \qquad \text{(suppose } p \neq 2\text{)}$$

$$\Rightarrow \frac{-191025 \pm 85995\sqrt{5}}{2} = \frac{2571 \pm 39\sqrt{421}}{2}$$

$$-191025 \pm 85995\sqrt{5} = 2571 \pm 39\sqrt{421}$$

$$\pm 85995\sqrt{5} = 193596 \pm 39\sqrt{421}$$

$$(85995)^2 \cdot 5 = \left(193596 \pm 39\sqrt{421}\right)^2$$

$$36975700125 = 37480051557 \pm 15100488\sqrt{421}$$

$$-504351432 = \pm 15100488\sqrt{421}$$

$$(-504351432)^2 = (15100488)^2 \cdot 421$$

$$254370366960450624 = 95998414629858624$$

$$-158371952330592000 = 0$$

$$158371952330592000 = 0$$

We can see that the system is true in $\overline{\mathbb{F}_p}$ when $p | 158371952330592000 \Rightarrow p | (2^8 \cdot 3^8 \cdot 5^3 \cdot 7^3 \cdot 11 \cdot 13) \Rightarrow p = 2, 3, 5, 7, 11, 13$. Note that for $p = 2$ our original system is

$$\begin{cases} x^2 + x + 1 = 0 \\ x^2 + x + 1 = 0 \end{cases} \Rightarrow x^2 + x + 1 = 0 \Rightarrow x = z_2$$

where $z_2 \notin \mathbb{F}_2$ but $(z_2)^2 \in \mathbb{F}_2$. In the other cases, we have:

$$x = \frac{-191025 \pm 85995\sqrt{5}}{2} = \begin{cases} 0 & (\text{mod } 3) \\ 0 & (\text{mod } 5) \\ 6 & (\text{mod } 7) \\ 0, 1 & (\text{mod } 11) \\ 5 & (\text{mod } 13) \end{cases} \quad \text{and} \quad x = \frac{2571 \pm 39\sqrt{421}}{2} = \begin{cases} 0 & (\text{mod } 3) \\ 0, 1 & (\text{mod } 5) \\ 3, 6 & (\text{mod } 7) \\ 0, 8 & (\text{mod } 11) \\ 5 & (\text{mod } 13) \end{cases}$$

Thus Case 20: results in a triple edge for $x_0 = z_2 \in \overline{\mathbb{F}_2}, x_0 = 0 \in \overline{\mathbb{F}_3}, x_0 = 0 \in \overline{\mathbb{F}_5}, x_0 = 6 \in \overline{\mathbb{F}_7}, x_0 = 0 \in \overline{\mathbb{F}_{11}}$, and $x_0 = 5 \in \overline{\mathbb{F}_{13}}$.

As a final result, we see that the following j invariants have triple edges in $\mathcal{G}_2(\overline{\mathbb{F}_p})$:

p	j-invariant
5	0
7	$0, 6$
11	0
13	$0, 5$
any other	0

It is easy to check which of the j invariants is supersingular and in $\mathbb{F}_p$. We know from **Theorem 1.6.7** that $p = 5, 7, 13$ result in $\mathcal{S}_2^p$ being a single vertex. For $p = 5$, 0 is supersingular, for $p = 7$, 6 is supersingular, and for $p = 13$, 5 is supersingular. Hence, these cases result in $\mathcal{S}_2^p$ being a single vertex with three multi-edge loops.

Note that all remaining cases, 0 is the only vertex which implies a triple edge. In fact by factoring $\Phi_2(0, X) = (X - 54000)^3$, and factoring $54000 = 2^4 \cdot 3^3 \cdot 5^3$, we see that any prime other than 2, 3, or 5, would not result in 0 having loops. To finish the proof of the statement we simply have to recall that 0 is supersingular if and only if $p \equiv 2 \pmod 3$. Thus, we have proved every aspect of the statement. ■

Theorem 1.6.24: The following conditions characterize all possible structures of the spine for $\ell = 2$:

(a) $p = 5$. Then $\Upsilon(\mathcal{S}_\ell^p)$ is a single vertex.

(b) $p \equiv 1 \pmod 4$.

i. $p = 29$ if and only if there is an edge attachment, the unique component which can fold does so, and the edge attachment connects the folded component to another component.

ii. $p \equiv 29, 101 \pmod{120}$, $p \neq 29$ if and only if there is an edge attachment, the unique component which can fold does so, and the edge attachment does not connect the folded component to another component.

iii. $p \equiv 41, 89 \pmod{120}$ if and only if there is an edge attachment and no component folds.

iv. $p \equiv 13, 37, 53, 61, 77, 109 \pmod{120}$ if and only if no edge attachment takes place and the unique component which can fold does so.

v. $p \equiv 1, 17, 49, 73, 97, 113 \pmod{120}$ if and only if no edge attachment takes place and no component folds.

(c) $p \equiv 3 \pmod 8$. Folding always happens.

i. $p = 11$ if and only if there is a new multi-edge, however, it is incident to vertices originally from the same component.

ii. $p = 59$ if and only if the folded component gets edge attached to another component by an edge between two vertices on the floor.

iii. $p \equiv 11, 59 \pmod{120}$ and $p \neq 11, 59$ if and only if an edge attachment takes place between two stacked components with the attaching edge being incident to two vertices on the floor.

iv. $p \equiv 19, 43, 67, 83, 91, 107 \pmod{120}$ if and only if no edge attachment takes place.

(d) $p \equiv 7 \pmod 8$. Folding always happens.

i. $p \equiv 71, 119 \pmod{120}$ if and only if there is a new multi-edge in $\mathcal{S}_\ell^p$. This *may* imply that there is an edge attachment, though it is not a necessary result. In either case, the new edge is incident to two vertices on the floor.

ii. $p \equiv 7, 23, 31, 47, 79, 103 \pmod{120}$ if and only if there are no new multi-edges in $\mathcal{S}_\ell^p$. This implies that there are no edge attachments.

Proof: We will go through each of the cases of the theorem and prove each case in order. Suppose $\ell = 2$. For each of the cases we need to keep in mind that **Theorem 1.6.16(a)** tells us that if there is a component that does not fold, then that component stacks. Furthermore, **Theorem 1.6.16(b)** tells us that there is only one component that folds. Hence we know that if there is a component that is not the folding component, then that component will stack. Lastly, **Theorem 1.6.16(d)** tells us that no vertex attachments take place. Thus, the only things that distinguish the structure of the spine are when folding happens, and when edge attachment happens. Let us explore these cases.

Case (a) Suppose $p = 5$. By **Theorem 1.6.7** we know that the spine is comprised of a single vertex. There may be loops on that vertex, but we know that $\Upsilon(\mathcal{S}_2^5)$ is a single vertex with no edges. Thus proving the statement in this case.

From now on, suppose $p > 5$.

Case (b) Suppose $p \equiv 1 \pmod 4$. Let us first look at when folding and edge attachment occur separately, then combine our results afterward.

Folding: Recall that **Theorem 1.6.16(b.i)** tells us that folding happens if and only if the component (u_{8000}, w_{8000}) exists. In other words, folding happens if and only if 8000 is supersingular. By **Theorem 1.5.13** we know that 8000 is supersingular if and only if $p \equiv 5$ or $7 \pmod 8$. Since we are in the case that $p \equiv 1 \pmod 4$, we gather that 8000 is supersingular if and only if $p \equiv 5 \pmod 8$.

Edge Attachment: Recall that **Theorem 1.6.16(c)** tells us that if there is a supersingular root of $R_{2,1}(x)$ in $\mathbb{F}_p$, then an edge attachment *may or may not* take place. However, we know that if $R_{2,1}(x)$ has a supersingular root in $\mathbb{F}_p$ then a new double edge is added to the graph.
Note that $R_{2,1}(x) = H_{15}(x)$. Hence by **Lemma 1.6.22** we know that $R_{2,1}$ has a supersingular root in $\mathbb{F}_p$ if and only if $p = 7, 13$ or $p \equiv 11, 14 \pmod{15}$. Combining this with the fact that we supposed $p \equiv 1 \pmod 4$ by CRT, we know that there is a new double edge if $p = 13$ or $p \equiv 29, 41 \pmod{60}$.
Suppose j is a supersingular root of $R_{2,1}(x)$ in $\mathbb{F}_p$, however, the implied edge is not an attaching edge. This implies that ${}_+d_j(\mathcal{S}_\ell^p) = 3$. Hence we know that j is one of the vertices with triple edges mentioned in **Theorem 1.6.23** (while recalling that we are assuming $p > 3$). The theorem tells us that the only j invariants with a triple edge are $j = 0, 5, 6$. However, since the j invariant 6 is associated with $p = 7$, we exclude it (since $p \equiv 1 \pmod 4$). Hence $j = 0$, or 5 where $j = 5 \Leftrightarrow p = 13$. Note that in $\mathbb{F}_{13}$, $\Phi_2(5, x) = (x-5)^3$. Hence we know that two new edges were added, but as loops. Thus $p = 13$ is a case where there is a new double edge, but no new edge attachment. Now consider $j = 0$, note that $R_{2,1}(0) = -121287375$ which is equal to zero if and only if $p | 121287375 \Leftrightarrow p | 3^6 \cdot 5^3 \cdot 11^3 \Leftrightarrow p = 3, 5, 11$. Since $p > 3$ and $p \equiv 1 \pmod 4$ $p = 5$ is the only possibility, which we have already covered in (a).
Thus we conclude that if $p = 13$ then there is a new double edge, but no edge attachment, and if $p \equiv 29, 41 \pmod{60}$, then there is a new double edge and this double edge is an attaching edge.

Thus, we now know when there is a component which folds, and when there is an edge attachment. Note, however, that the folded component contains only one vertex, 8000. Hence we can find when the folded component is involved in an edge attachment. Consider $Res_{2,1}(8000) = 1470912625$. Hence we know that 8000 is incident to a double edge if $p | 1470912625 \Leftrightarrow p | (5^3 \cdot 7^4 \cdot 13^2 \cdot 29) \Rightarrow p = 5, 7, 13, 29$. Note that the only p value which results in an edge attachment is 29. Hence we know that the folded component is involved in an edge attachment if and only if $p = 29$.

Note that we know that an edge attachment happens if and only if $p \equiv 29, 41 \pmod{60}$, which implies that an edge attachment does not happen if $p \not\equiv 29, 41 \pmod{60} \Leftrightarrow p \equiv 1, 13, 17, 37, 49, 53 \pmod{60}$ (since $p \equiv 1 \pmod 4$ the number of equivalence classes not equivalent to 29 or 41 is restricted). Furthermore, we know that a component folds if and only if $p \equiv 5 \pmod 8$, which implies that a component does not fold if $p \not\equiv 5 \pmod 8 \Leftrightarrow p \equiv 1 \pmod 8$ (again taking into account that $p \equiv 1 \pmod 4$). Define the tuple $(a, \quad b)$ such that $a \equiv p \pmod{60}$ and $b \equiv p \pmod 8$. The following table shows our computations using CRT:

Description	Accepted Tuple	Resulting $p \pmod{120}$
attachment and fold	$(29, \ 5)$	29
	$(41, \ 5)$	101
attachment and no fold	$(29, \ 1)$	89
	$(41, \ 1)$	41
no attachment and fold	$(1, \ 5)$	61
	$(13, \ 5)$	13
	$(17, \ 5)$	77
	$(37, \ 5)$	37
	$(49, \ 5)$	109
	$(53, \ 5)$	53
no attachment and no fold	$(1, \ 1)$	1
	$(13, \ 1)$	73
	$(17, \ 1)$	17
	$(37, \ 1)$	97
	$(49, \ 1)$	49
	$(53, \ 1)$	113

Hence with the fact that we consider $p = 29$ as a different case than when attachment and folding happen, we have proved this case of the statement.

Case (c) Suppose $p \equiv 3 \pmod 8$. First, let us look at when folding and edge attaching happen.

Folding: We know by **Theorem 1.6.16(c,ii)** that folding happens when 1728 is supersingular, which only happens when $p \equiv 1 \pmod 4$. This will always happen since $p = [3]_8 \Rightarrow p = [3]_4$. Hence, folding always happens in this case.

Edge Attachment: We know by **Theorem 1.6.16** that edge attachment can only happen if there is a supersingular root of $R_{2,1}(x)$ in $\mathbb{F}_p$, and even then it may not happen. However, **Theorem 1.6.17** tells us that if $p > 101$ and $R_{2,1}(x)$ has a supersingular root in $\mathbb{F}_p$, then there is an edge attachment. Note that $R_{2,1}(x) = H_{15}(x)$, and hence by **Lemma 1.6.22** we know that $R_{2,1}(x)$ has supersingular roots in $\mathbb{F}_p$ if and only if $p = 7, 13$ or $p \equiv 11, 14 \pmod{15}$. In our case, we can rule out $p = 7$ and 13. If we combine the condition $p = 11, 14 \pmod{15}$ and the assumption that $p \equiv 3 \pmod 8$, by CRT we get the condition $p \equiv 11, 59 \pmod{120}$.
We know that if $p > 101$ then a supersingular root of $R_{2,1}(x)$ in $\mathbb{F}_p$ would imply an edge attachment has taken place. But if $p = 11, 59$ then we do not know. However, this can be fixed by simply computing $\mathcal{S}_2^{11}$ and $\mathcal{S}_2^{59}$. By doing so we see that no edge attachment takes place for $p = 11$, but the folded component attaches to another component when $p = 59$.

Thus we know when folding and edge attachment happen. Consider the folded component for a moment. We know by the structure of $\mathcal{G}_\ell(\mathbb{F}_p)$ that the folded component (when put through the simplification map) is just an edge. By factoring $\Phi_2(1728, x) = (x - 1728)(x - 287496)^2$ we see that the component is comprised of the vertices 1728 and 287496 (since we know that there exists a vertex in the component of $\mathcal{G}_\ell(\mathbb{F}_p)$ containing 1728, that does not have a j-invariant of 1728). Note that the 2-modular polynomial tells us that ${}_+d_{1728}(Im(\Gamma)) = 3$. Hence edge attachment cannot happen for 1728, otherwise, 1728 would have an out-degree of 5 which cannot happen. Now suppose that the folded component got attached. That would mean that 287496 is a supersingular root of $R_{2,1}(x)$. Note that $R_{2,1}(287496) = 137451586041$ which is zero if and only if $p | 137451586041 \Leftrightarrow p | (3^6 \cdot 7^4 \cdot 11^3 \cdot 59)$. The only one which works in this case is $p = 59$.

Hence $p = 59$ is the only prime value which results in the folded component getting attached by an edge.

One important thing to note is where an edge attachment can happen. Note that for every supersingular $j \in \mathbb{F}_p$, if $j \neq 1728$, then both u_j and w_j are on the same level of $\mathcal{G}_\ell(\mathbb{F}_p)$. Hence in most cases, we can identify a j-invariant as being on the floor or the surface. Recall that every component that does not fold, stacks. Therefore we know that the components of $\mathcal{G}_\ell(\mathbb{F}_p)$ keep their structure (other than the folded component). Hence we know that every j on the surface of $\mathcal{S}_\ell^p$ cannot get attached to any new vertices since it is already incident to three out-edges. Therefore we know that any edge attachment happens between vertices on the floor. This extends to the folded component, due to the fact that the only vertex that can attach in the folded component is 287496 which we know to be on the floor of $\mathcal{G}_\ell(\mathbb{F}_p)$.

Note that we have shown that if $p = 11$ then there is a new edge but it resides within the same component, if $p = 59$ then the folded component gets attached, and if $p \equiv 11, 59 \pmod{120}$ and $p \neq 11, 59$ then there is an attaching edge between floor vertices of stacked components. Hence the only section of the statement we have not shown is when there is not an edge attachment. In this case an edge attachment not happening means $p \not\equiv 11, 59 \pmod{120}$ and $p \equiv 3 \pmod 8$.

Note that $p \not\equiv 11, 59 \pmod{120}$ means that p is congruent to an integer between 0 and 119 modulo 120. However, we know that we are excluding any number which has a common divisor with 120 (other than 1) since then that would imply that p is divisible by a non-identity element. Hence p would have to be congruent to a number within the set

$$\{1,7,13,17,19,23,29,31,37,41,43,47,49,53,61,67,71,73,77,\\ 79,83,89,91,97,101,103,107,109,113,119\}$$

Then taking into account that we have supposed $p \equiv 3 \pmod 8$, our set restricts to

$$\{11,19,43,59,67,83,91,107\}$$

Which matches the claim in the statement. Thus we have proved this section of the statement.

Case (d) Suppose $p \equiv 7 \pmod 8$. Let us see when folding and edge attaching take place.

Folding: By **Theorem 1.6.16(c, ii)** we know that folding takes place when 1728 is supersingular. In this case, 1728 is always supersingular since $p = [7]_8 \Rightarrow p = [3]_4$. Hence the component containing both u_{1728} and w_{1728} folds.

Edge Attachment: By **Theorem 1.6.16(d)** we know that there an edge attachment may or may not happen when $R_{2,1}(x)$ has a supersingular root in $\mathbb{F}_p$. Note that $R_{2,1}(x) = H_{15}(x)$, and by **Lemma 1.6.22** we know that $R_{2,1}(x)$ has a supersingular root in $\mathbb{F}_p$ if and only if $p = 7, 13$ or $p \equiv 11, 14 \pmod{15}$. By our supposition that $p \equiv 7 \pmod 8$, we exclude $p = 13$. Now, suppose $p = 7$. By **Theorem 1.6.7** we know that $\mathcal{S}_2^7$ is a single vertex hence we know that no edge attachment can happen. However, we know that the only supersingular j-invariant in $\mathcal{S}_2^7$ is 6, and in $\mathbb{F}_7$, $R_{2,1}(x) = (x+1)^2$ of which 6 is a root of. Hence, when $p = 7$, there is a supersingular root of $R_{2,1}(x)$ in $\mathbb{F}_p$, but no edge attachment takes place.

Now let us combine the condition that $p = 11, 14 \pmod{15}$ with our supposition that $p \equiv 7 \pmod 8$. By CRT we conclude that an edge attachment *can* happen if and only if $p \equiv 71, 119 \pmod{120}$. This congruence condition is a necessary condition for an edge attachment to happen, however, it is not a sufficient condition to guarantee edge attachment, as shown in the remark after [Arp+23, corollary 3.30].

Hence we know that folding always occurs, and edge attachment can only happen if $p \equiv 71$, $119 \pmod{120}$. However, we do not know exactly when edge attachment happens, nor when the folded component attaches to a stacked component.

Recall that any component that does not fold, stacks. Hence we know that the structure of the (simplified) components of $\mathcal{S}_\ell^p$ are identical to the (simplified) components of $\mathcal{G}_\ell(\mathbb{F}_p)$ except for the folded component. Hence we know that the surface vertices in stacked components of $\mathcal{S}_\ell^p$ cannot get attached to any vertex as they already are incident to three out-edges. Furthermore, if we look at the stacked component, all vertices on the surface (including 1728) have an out-degree of either 2 or 3. Hence no edge attachment can happen through vertices on the surface of the folded component as a new edge would imply two new edges which would supersede the maximum out-degree of $\mathcal{S}_\ell^p$. Thus we know that if there is a new edge, then it must have happened between two floor vertices (excluding 0 since it has extra automorphisms).

Note that we don't know much information about when edge attachment definitvely happens, nor where it happens, however, we can determine when it will certainly not happen. That is when $p \not\equiv 71, 119 \pmod{120}$. Similar to the previous case we know that this means that p must be congruent to one of the following natural numbers:

$$\{1,7,11,13,17,19,23,29,31,37,41,43,47,49,53,59,61,67,$$
$$73,77,79,83,89,91,97,101,103,107,109,113\}$$

However, taking into account our supposition that $p \equiv 7 \pmod{8}$, our set restricts to:

$$\{7,23,31,47,79,103\}$$

This encapsulates the case where $p = 7$, hence we do not need to mention it in a different case. We see that this matches our statement. Hence we have proved this case of the statement.

Note that we have proved every case of this statement. Thus we conclude that the statement is proved to be true.

■

$\ell = 3$:

Lemma 1.6.25: For an odd prime p,

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1,7 \pmod 8 \\ -1 & \text{if } p \equiv 3,5 \pmod 8 \end{cases}$$

Proof: This is an elementary number theory result which the reader can find in any introductory number theory textbook. ■

Lemma 1.6.26: For an odd prime p not equal to 7, then

$$\left(\frac{7}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1,3,9,19,25,27 \pmod{28} \\ -1 & \text{if } p \equiv 5,11,13,15,17,23 \pmod{28} \end{cases}$$

Proof: Let p be an odd prime. By quadratic reciprocity we have

$$\left(\frac{7}{p}\right)\left(\frac{p}{7}\right) = (-1)^{\frac{p-1}{2}\frac{7-1}{2}} = (-1)^{\frac{p-1}{2}}$$

Hence we have two cases depending on if $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$.

Case 1: Suppose $p \equiv 1 \pmod 4$. Then we know that $\left(\frac{7}{p}\right)\left(\frac{p}{7}\right) = 1$, and hence $\left(\frac{7}{p}\right) = \left(\frac{p}{7}\right)$. In other words, 7 is a quadratic residue modulo p if and only if p is a quadratic residue modulo 7. By exhaustively searching we find that the quadratic residues modulo 7 are 1, 2, and 4. Hence we know that if $p \equiv 1,2,4 \pmod 7$ then 7 is a quadratic residue modulo p. By letting $(a, \quad b) = ([p]_4, \quad [p_7])$ we combine the conditions of p modulo 7 and 4 using CRT in the following table:

$(a, \quad b)$	$p \pmod{28}$
$(1, \quad 1)$	1
$(1, \quad 2)$	9
$(1, \quad 4)$	25
$(1, \quad 3)$	17
$(1, \quad 5)$	23
$(1, \quad 6)$	13

Hence we know that 7 is a quadratic residue modulo p if $p \equiv 1,9,25 \pmod{28}$, and 7 is not a quadratic residue modulo p if $p \equiv 13,17,23 \pmod{28}$

Case 2: Suppose $p \equiv 3 \pmod 4$. By this we know that $\left(\frac{7}{p}\right)\left(\frac{p}{7}\right) = -1$, and hence $\left(\frac{7}{p}\right) = -\left(\frac{p}{7}\right)$. In other words, 7 is a quadratic residue modulo p if and only if p is not a quadratic residue modulo 7. We have already seen that 1, 2, and 4 are the only quadratic residues modulo 7. Hence by letting $(a, \quad b) = ([p]_4, \quad [p_7])$ we combine the conditions of p modulo 7 and 4 using CRT in the following table: Hence we know that 7 is a quadratic residue modulo p if $p \equiv 3,19,27 \pmod{28}$, and 7 is not a quadratic residue modulo p if $p \equiv 11,15,23 \pmod{28}$.

Putting our two cases together, we see that we have proved the statement. ■

$(a,\ b)$	$p \pmod{28}$
$(3,\ 3)$	3
$(3,\ 5)$	19
$(3,\ 6)$	27
$(3,\ 1)$	15
$(3,\ 2)$	23
$(3,\ 4)$	11

Lemma 1.6.27: Suppose p is an odd prime not equal to 11. Then

$$\left(\frac{-11}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1,3,4,5,9 \pmod{11} \\ -1 & \text{if } p \equiv 2,6,7,8,10 \pmod{11} \end{cases}$$

Proof: Suppose p is an odd prime not equal to 11. Then we have the following:

$$\begin{aligned} \left(\frac{-11}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{11}{p}\right) && \text{(by the multiplicative property)} \\ &= (-1)^{\frac{p-1}{2}}\left(\frac{11}{p}\right) && \text{(by Euler's Criterion)} \\ &= (-1)^{\frac{p-1}{2}}\left((-1)^{\frac{p-1}{2}\cdot\frac{11-1}{2}}\left(\frac{p}{11}\right)\right) && \text{(by quadratic reciprocity)} \\ &= (-1)^{\frac{p-1}{2}}\cdot(-1)^{\frac{p-1}{2}}\cdot\left(\frac{p}{11}\right) \\ &= \left(\frac{p}{11}\right) \end{aligned}$$

Hence we conclude that -11 is a quadratic residue modulo p if and only if p is a quadratic residue modulo 11. We know the quadratic residues of 11 to be 1, 3, 4, 5, and 9. Hence we conclude that $\left(\frac{-11}{p}\right) = 1$ if and only if $p \equiv 1,3,4,5,9 \pmod{11}$ and $\left(\frac{-11}{p}\right) = -1$ if and only if $p \equiv 2,6,7,8,10 \pmod{11}$. This proves our statement. ■

Lemma 1.6.28: Suppose p is an odd prime not equal to 5. Then

$$\left(\frac{-20}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1,3,7,9 \pmod{20} \\ -1 & \text{if } p \equiv 11,13,17,19 \pmod{20} \end{cases}$$

Proof: Suppose p is an odd prime not equal to 5. By the multiplicative property of the Legendre symbol we have:

$$\left(\frac{-20}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)^2\left(\frac{5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right)$$

By **Lemma 1.6.18** and **Lemma 1.6.20** we know that

$$\left(\frac{-1}{2}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases} \quad \text{and} \quad \left(\frac{5}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 4 \pmod 5 \\ -1 & \text{if } p \equiv 2 \text{ or } 3 \pmod 5 \end{cases}$$

And since $\left(\frac{-20}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right)$ we know that if both $\left(\frac{-1}{p}\right)$ and $\left(\frac{5}{p}\right)$ are positive or both negative, then $\left(\frac{-20}{p}\right)$ is positive, and $\left(\frac{-20}{p}\right)$ is negative other wise. If we use the tuple $([p]_4,\ \ [p]_5)$ then we have

Value of $\left(\frac{-20}{p}\right)$	$([p]_4, \quad [p]_5)$	Resulting $p \pmod{20}$
1	$(1, \quad 1)$	1
	$(1, \quad 4)$	9
	$(3, \quad 2)$	7
	$(3, \quad 3)$	3
-1	$(1, \quad 2)$	17
	$(1, \quad 3)$	13
	$(3, \quad 1)$	11
	$(3, \quad 4)$	19

Table 3: Scenarios which provide a value for $\left(\frac{-20}{p}\right)$

the scenarios provided in Table 3. Thus we see that $\left(\frac{-20}{p}\right) = 1$ if and only if $p \equiv 1,3,7,9 \pmod{20}$ and $\left(\frac{-20}{p}\right) = -1$ if and only if $p \equiv 11,13,17,19 \pmod{20}$. Hence we have proved the statement. ■

Lemma 1.6.29: Let p be an odd prime. Then

$$\left(\frac{-32}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1,3 \pmod 8 \\ -1 & \text{if } p \equiv 5,7 \pmod 8 \end{cases}$$

Proof: Note that by the multiplicative property of the Legendre symbol, we know:

$$\left(\frac{-32}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)^5 = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$$

By **Lemma 1.6.18** and **Lemma 1.6.25** we know that

$$\left(\frac{-1}{2}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases} \quad \text{and} \quad \left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1,7 \pmod 8 \\ -1 & \text{if } p \equiv 3,5 \pmod 8 \end{cases}$$

And since $\left(\frac{-32}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$ we know that if both $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$ are positive or both negative, then $\left(\frac{-32}{p}\right)$ is positive, and $\left(\frac{-32}{p}\right)$ is negative other wise. If we use the tuple $([p]_4, \quad [p]_8)$ then we have the scenarios provided in Table 4. Hence we know that $\left(\frac{-32}{p}\right) = 1$ if and only if $p \equiv 1,3 \pmod 8$ and $\left(\frac{-32}{p}\right) = -1$ if and only if $p \equiv 5,7 \pmod 8$. Thus we have proved the statement. ■

Lemma 1.6.30: Let p be a prime such that $p \neq 2,5,7$. Then

$$\left(\frac{-35}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1,3,4,9,11,12,13,16,17,27,29,33 \pmod{35} \\ -1 & \text{if } p \equiv 2,6,8,18,19,22,23,24,26,31,32,34 \pmod{35} \end{cases}$$

Proof: Suppose p is a prime such that $p \neq 2,5,7$. Then by the multiplicative property of the Legendre symbol we have:

$$\left(\frac{-35}{p}\right) = \left(\frac{-7}{p}\right)\left(\frac{5}{p}\right)$$

Value of $\left(\frac{-32}{p}\right)$	$([p]_4, \quad [p]_8)$	Resulting $p \pmod 8$
1	$(1, \quad 1)$	1
	$(1, \quad 7)$	$\emptyset$
	$(3, \quad 3)$	3
	$(3, \quad 5)$	$\emptyset$
-1	$(1, \quad 3)$	$\emptyset$
	$(1, \quad 5)$	5
	$(3, \quad 1)$	$\emptyset$
	$(3, \quad 7)$	7

Table 4: Scenarios which result in a value for $\left(\frac{-32}{p}\right)$

Let us consider $\left(\frac{-7}{p}\right)$ for a moment. Note that we have the following:

$$\begin{aligned}
\left(\frac{-7}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{7}{p}\right) \\
&= (-1)^{\frac{p-1}{2}}\left(\frac{7}{p}\right) && \text{(by Euler's Criterion)} \\
&= (-1)^{\frac{p-1}{2}}\left((-1)^{\frac{p-1}{2}\cdot\frac{7-1}{2}}\cdot\left(\frac{p}{7}\right)\right) && \text{(by quadratic reciprocity)} \\
&= (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}}\left(\frac{p}{7}\right) \\
&= \left(\frac{p}{7}\right)
\end{aligned}$$

Hence we know that $\left(\frac{-7}{p}\right) = \left(\frac{p}{7}\right)$. In other words, -7 is a quadratic residue modulo p if and only if p is a quadratic residue modulo 7. We know that quadratic residues of 7 to be $1, 2$, and 4. Hence we conclude that

$$\left(\frac{-7}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1,2,4 \pmod 7 \\ -1 & \text{if } p \equiv 3,5,6 \pmod 7 \end{cases}$$

If we recall **Lemma 1.6.20** we remember that

$$\left(\frac{5}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1,4 \pmod 5 \\ -1 & \text{if } p \equiv 2,3 \pmod 5 \end{cases}$$

Since $\left(\frac{-35}{p}\right) = \left(\frac{-7}{p}\right)\left(\frac{5}{p}\right)$ we know that $\left(\frac{-35}{p}\right)$ is positive if both $\left(\frac{-7}{p}\right)$ and $\left(\frac{5}{p}\right)$ are positive or both are negative. Additionally, we know that $\left(\frac{-35}{p}\right)$ is negative in any other case. By considering the tuple $([p]_5, \quad [p]_7)$ we have the scenarios shown in Table 5. Thus we conclude that $\left(\frac{-35}{p}\right) = 1$ if and only if $p \equiv 1,3,4,9,11,12,13,16,17,27,29,33 \pmod{35}$ and $\left(\frac{-35}{p}\right) = -1$ if and only if $p \equiv 2,6,8,18,19,22,23,24,26,31,32,34 \pmod{35}$. Hence we have proved the statement true. ■

Lemma 1.6.31: Suppose p is a prime such that $p \neq 2, 3$, then

$$\left(\frac{-36}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

Value of $\left(\frac{-35}{p}\right)$	$([p]_5,\ [p]_7)$	Resulting $p \pmod{35}$
1	$(1,\ 1)$	1
	$(1,\ 2)$	16
	$(1,\ 4)$	11
	$(4,\ 1)$	29
	$(4,\ 2)$	9
	$(4,\ 4)$	4
	$(2,\ 3)$	17
	$(2,\ 5)$	12
	$(2,\ 6)$	27
	$(3,\ 3)$	3
	$(3,\ 5)$	33
	$(3,\ 6)$	13
-1	$(1,\ 3)$	31
	$(1,\ 5)$	26
	$(1,\ 6)$	6
	$(4,\ 3)$	24
	$(4,\ 5)$	19
	$(4,\ 6)$	34
	$(2,\ 1)$	22
	$(2,\ 2)$	2
	$(2,\ 4)$	32
	$(3,\ 1)$	8
	$(3,\ 2)$	23
	$(3,\ 4)$	18

Table 5: all possible scenarios that result in a value for $\left(\frac{-35}{p}\right)$

Proof: Suppose that p is a prime such that $p \neq 2,3$. By the multiplicative property of the Legendre symbol and **Lemma 1.6.18** we have

$$\left(\frac{-36}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)^2\left(\frac{3}{p}\right)^2 = \left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

Which proves the statement. ■

Lemma 1.6.32: Suppose p is a prime such that $p \neq 2,3,11$. Then

$$\left(\frac{-99}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1,3,4,5,9 \pmod{11} \\ -1 & \text{if } p \equiv 2,6,7,8,10 \pmod{11} \end{cases}$$

Proof: Suppose p is a prime such that $p \neq 2,3,11$. Then by the multiplicative property of the Legendre symbol and **Lemma 1.6.27** we have

$$\left(\frac{-99}{p}\right) = \left(\frac{-11}{p}\right)\left(\frac{3}{p}\right)^2 = \left(\frac{-11}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1,3,4,5,9 \pmod{11} \\ -1 & \text{if } p \equiv 2,6,7,8,10 \pmod{11} \end{cases}$$

This proves our statement. ■

Lemma 1.6.33: Let E_a and E'_a be elliptic curves defined over a field k such that $j(E_a) = j(E'_a) = a$ and $E_a \neq E'_a$. Additionally, let E_b and E'_b be elliptic curves defined over k such that $j(E_b) = j(E'_b) = b$. Suppose that there exist isogenies

$$\phi : E_a \to E_b \qquad \text{and} \qquad \psi : E'_a \to E'_b$$

such that ϕ and ψ are defined over k. Then ϕ is equivalent to ψ over a superfield $L \supseteq k$ if and only if there exist group isomorphism defined over L

$$\eta : E_a \to E'_a$$

such that

$$\eta(\ker(\phi)) = \ker(\psi)$$

Proof: Suppose that ϕ and ψ are equivalent over L. By definition this implies that there exists isomorphisms defined over L

$$\eta_a : E_a \to E'_a \qquad \text{and} \qquad \eta_b : E_b \to E'_b$$

such that

$$\psi \circ \eta_a = \eta_b \circ \phi$$

Since (we are generally working with separable isogenies) we know that $\psi \circ \eta_a$ and $\eta_b \circ \phi$ are determined by their kernels. Hence we know that ϕ is equivalent to ψ over L if and only if $\ker(\psi \circ \eta_a) = \ker(\eta_b \circ \phi)$. Hence we have the following:

$$\begin{aligned}
\ker(\psi \circ \eta_a) &= \ker(\eta_b \circ \phi) \\
\left\{P \in E_a : \psi \circ \eta_a(P) = \mathcal{O}_{E'_b}\right\} &= \left\{P \in E_a : \eta_b \circ \phi(P) = \mathcal{O}_{E'_b}\right\} \\
\{P \in E_a : \eta_a(P) \in \ker(\psi)\} &= \left\{P \in E_a : \phi(P) = \mathcal{O}_{E'_b}\right\} \\
\{P \in E_a : \eta_a(P) \in \ker(\psi)\} &= \ker(\phi)
\end{aligned}$$

Hence, by the fact that η_a is an isomorphism we know that the last equality holds if and only if

$$\ker(\psi) = \eta_a(\ker(\phi))$$

Thus proving the statement. ■

Lemma 1.6.34: Let $p \equiv 2 \pmod 3$. Then the following elliptic curves defined over $\mathbb{F}_p$

$$u_0 : y^2 = x^3 + 1$$

$$w_0 : y^2 = x^3 - 3$$

are elliptic curves with j invariant 0 and they are not isomorphic to each other over $\mathbb{F}_p$, but are isomorphic to each other over $\mathbb{F}_{p^2}$ via the isomorphism η such that $(x,y) \mapsto (u^2x, u^3y)$ where u is a sixth root of -3 in $\mathbb{F}_{p^2}$.

Proof: Suppose $p \equiv 2 \pmod 3$. By using the formula for the j invariant we have:

$$j(u_0) = 1728 \cdot \frac{4(0)^3}{4(0)^3 + 27(1)^2} = 0 = 1728 \cdot \frac{4(0)^3}{4(0)^3 + 27(-3)^2} = j(w_0)$$

Define $\mathbb{F}_{p^2}$ such that $\mathbb{F}_{p^2} \simeq {}^{\mathbb{F}_p[t]}/_{t^2+t+1}$. Note that t^2+t+1 is an irreducible polynomial in $\mathbb{F}_p[t]$ due to the fact that

$$t^2 + t + 1 = 0 \Leftrightarrow t = \frac{-1 \pm \sqrt{-3}}{2}$$

Hence we know that $t \in \mathbb{F}_p$ if and only if $\left(\frac{-3}{p}\right) = 1$. Note that

$$\begin{aligned}
\left(\frac{-3}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) \\
&= (-1)^{\frac{p-1}{2}}\left(\frac{3}{p}\right) && \text{(by Euler's Criterion)} \\
&= (-1)^{\frac{p-1}{2}}\left((-1)^{\frac{p-1}{2}\cdot\frac{3-1}{2}}\left(\frac{p}{3}\right)\right) && \text{(by quadratic reciprocity)} \\
&= \left(\frac{p}{3}\right) \\
&= \begin{cases} 1 & \text{if } p \equiv 1 \pmod 3 \\ -1 & \text{if } p \equiv 2 \pmod 3 \end{cases}
\end{aligned}$$

Hence we know that $t \in \mathbb{F}_p$ if and only if $p \equiv 1 \pmod 3$, which we know not to be the case by our supposition of $p \equiv 2 \pmod 3$. Consider the isomorphism η such that $(x,y) \mapsto (u^2x, u^3y)$ where u is an element of $\mathbb{F}_{p^2}$. We see that $y^2 = x^3 - 3 \mapsto u^6 \cdot y^2 = u^6 \cdot x^3 - 3 \Leftrightarrow y^2 = x^3 - \frac{3}{u^6}$. Since we know (x,y) satisfies $y^2 = x^3 + 1$, we must have $-\frac{3}{u^6} = 1 \Leftrightarrow -3 = u^6 \Leftrightarrow -3 = \left(u^3\right)^2$. However, we know that -3 is not a square in this case, and hence we know that η is not defined over $\mathbb{F}_p$, and hence u_0 and w_0 are non-isomorphic elliptic curves over $\mathbb{F}_p$. ■

Note that since $p > 3$ we know that there are exactly six isomorphisms between two elliptic curves of j invariant 0.

Lemma 1.6.35: Let ζ_3 be the primitive third root of unity. Table 6 lists all isomorphisms of the form $\eta : u_0 \to w_0$ defined over $\mathbb{F}_{p^2}$:

Proof: Note that in this section we have supposed the $p \equiv 2 \pmod 3$. Hence we know $3|(p+1)$. Further note that we previously defined $\mathbb{F}_{p^2}$ as ${}^{\mathbb{F}_p[t]}/_{t^2+t+1}$. With this definition, we have the following:

$$\begin{aligned}
(2t+1)^2 &= 4t^2 + 4t + 1 \\
&= 4t^2 + 4t + 4 - 4 + 1 \\
&= 4\left(t^2 + t + 1\right) - 3 \\
&= -3
\end{aligned}$$

Hence we know that $\sqrt{-3} = 2t + 1 \in \mathbb{F}_{p^2}$. Recall that the cube root of any element exists in $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$. The only difference that could exist is the potential for there to be multiple cube roots of a single

Name	Input	Output
$\eta_{0,1}$	(x,y)	$\left(-\sqrt[3]{3}x, \sqrt{-3}y\right)$
$\eta_{0,2}$	(x,y)	$\left(-\sqrt[3]{3}x, -\sqrt{-3}y\right)$
$\eta_{0,3}$	(x,y)	$\left(-\sqrt[3]{3}\zeta_3 x, \sqrt{-3}y\right)$
$\eta_{0,4}$	(x,y)	$\left(-\sqrt[3]{3}\zeta_3 x, -\sqrt{-3}y\right)$
$\eta_{0,5}$	(x,y)	$\left(-\sqrt[3]{3}\zeta_3^2 x, \sqrt{-3}y\right)$
$\eta_{0,6}$	(x,y)	$\left(-\sqrt[3]{3}\zeta_3^2 x, -\sqrt{-3}y\right)$

Table 6: Isomorphisms of the form $\eta_{0,i} : u_0 \to w_0$ defined over $\mathbb{F}_{p^2}$.

item. This difference depends solely on the existence of the primitive cube root of unity. In this situation, since $3|(p+1)$, $(p+1)|(p^2-1)$, and $(p^2+1) = \left|\mathbb{F}_{p^2}^{\times}\right|$, we know that the primitive cube root of unity exists in $\mathbb{F}_{p^2}$. Putting these conclusions together we see that

$$T := \left\{ \pm\sqrt[3]{\sqrt{-3}}, \pm\sqrt[3]{\sqrt{-3}}\cdot\zeta_3, \pm\sqrt[3]{\sqrt{-3}}\cdot\zeta_3^2 \right\} \subseteq \mathbb{F}_{p^2}^{\times}$$

Hence for every $u \in T$, we know that the map $(x,y) \mapsto \left(u^2x, u^3y\right)$ is an isomorphism. We know that an isomorphism which sends $(x,y) \mapsto \left(u^2x, u^3y\right)$ goes from $y^2 = x^3 + Ax + B$ to $y^2 = x^3 + Au^4x + Bu^6$. Hence we know that for each $u \in T$, the implied isomorphism is going from u_0 to w_0. Explicitly calculating u^2 and u^3 for each $u \in T$ yields the result presented in Table 6. Lastly, since these are all distinct isomorphisms and there are 6 of them, we know that these are the only isomorphisms between the two elliptic curves. ■

Lemma 1.6.36: Let $p \equiv 3 \pmod 4$. The two curves defined over $\mathbb{F}_p$:

$$u_{1728} : y^2 = x^3 + x,$$

$$w_{1728} : y^2 = x^3 - x$$

both have j-invariant 1728 and are not isomorphic over $\mathbb{F}_p$, but are isomorphic over $\mathbb{F}_{p^2}$. The explicit isomorphism $\eta : u_{1728} \to w_{1728}$ is given by $(x,y) \mapsto (u^2x, u^3y)$, where u is a primitive 4-th root of unity in $\mathbb{F}_{p^2}$.

Proof: The j-invariants can be computed using the general formula for curves in short Weierstrass form $y^2 = x^3 + Ax + B$:

$$j = 1728\frac{4A^3}{4A^3 + 27B^2}.$$

Isomorphisms between curves in short Weierstrass form must be of the form $(x,y) \mapsto (u^2x, u^3y)$, for some u in the field of definition of the isomorphism. An isomorphism $\eta : u_{1728} \to w_{1728}$, $\eta(x,y) =$

(u^2x, u^3y) must then satisfy:

$$\begin{aligned}(u^3y)^2 &= (u^2x)^3 - (u^2x)\\ u^6y^2 &= u^6x^3 - u^2x\\ y^2 &= x^3 - (1/u^4)x\end{aligned}$$

since (x,y) satisfies $y^2 = x^3 + x$, we can conclude that u must be such that $-(1/u^4) = 1$, or equivalently $u^4 = -1$. Since $p \equiv 3 \pmod 4$, we know $u^2 = -1$ has no solution in $\mathbb{F}_p$, which implies that $u^4 = -1$ has no solution in $\mathbb{F}_p$. This establishes that the curves are not isomorphic over $\mathbb{F}_p$. To show that they are isomorphic over $\mathbb{F}_{p^2}$, we first fix $\mathbb{F}_{p^2} = \mathbb{F}_p[s]/(s^2+1)$. The field $\mathbb{F}_{p^2}$ contains a primitive 4-th root of unity (i.e., an element x such that $x^4 = 1$ and $x^k \neq 1$ for any $1 \leq k < 4$), because the group $\mathbb{F}_{p^2}^\times$ of invertible elements is cyclic and of order p^2-1. Since $p \equiv 3 \pmod 4$, $4 \mid (p+1) \mid (p^2-1)$ and so if y is a generator of $\mathbb{F}_{p^2}^\times$, then $y^{(p^2-1)/4}$ is an element of exact order 4. ■

Lemma 1.6.37: The 3-torsion subgroups of $u_0 : y^2 = x^3 + 1$ are

$$\langle (0,1) \rangle = \{(0,1), (0,-1), \mathcal{O}_{u_0}\}$$

$$\left\langle \left(-\sqrt[3]{4}, \sqrt{-3}\right) \right\rangle = \left\{ \left(-\sqrt[3]{4}, \sqrt{-3}\right), \left(-\sqrt[3]{4}, -\sqrt{-3}\right), \mathcal{O}_{u_0} \right\}$$

$$\left\langle \left(\frac{1+\sqrt{-3}}{\sqrt[3]{2}}, \sqrt{-3}\right) \right\rangle = \left\{ \left(\frac{1+\sqrt{-3}}{\sqrt[3]{2}}, \sqrt{-3}\right), \left(\frac{1+\sqrt{-3}}{\sqrt[3]{2}}, -\sqrt{-3}\right), \mathcal{O}_{u_0} \right\}$$

$$\left\langle \left(\frac{1-\sqrt{-3}}{\sqrt[3]{2}}, \sqrt{-3}\right) \right\rangle = \left\{ \left(\frac{1-\sqrt{-3}}{\sqrt[3]{2}}, \sqrt{-3}\right), \left(\frac{1-\sqrt{-3}}{\sqrt[3]{2}}, -\sqrt{-3}\right), \mathcal{O}_{u_0} \right\}$$

Proof: By a quick computation, we see that the third division polynomial of u_0 is

$$3x(x^3+4)$$

We know that roots of x^3+4 to be $\sqrt[3]{-4}$, however, there are three elements in $\overline{\mathbb{Q}}$ that are cube roots of -4. By some simple complex analysis, we have

$$\begin{aligned}\sqrt[3]{-4} &= \left\{ \sqrt[3]{4}\exp\left(i\frac{\pi}{3}\right)\exp\left(i\frac{2k\pi}{3}\right) : k = 0,1,2 \right\}\\ &= \left\{ \sqrt[3]{4}\exp\left(i\frac{\pi}{3}\right), \sqrt[3]{4}\exp(i\pi), \sqrt[3]{4}\exp\left(i\frac{5\pi}{3}\right) \right\}\\ &= \left\{ -2^{\frac{2}{3}}, 2^{\frac{2}{3}}\left(\frac{1}{2} + i\frac{\sqrt{3}}{2}\right), 2^{\frac{2}{3}}\left(\frac{1}{2} - i\frac{\sqrt{3}}{2}\right) \right\}\end{aligned}$$

Now instead of working over $\mathbb{Q}$ we are working over $\mathbb{F}_p$ hence technically we have $i\sqrt{3}$ representing $\sqrt{-3}$. Due to this, we have

$$\begin{aligned}\sqrt[3]{-4} &= \left\{ -2^{\frac{2}{3}}, 2^{\frac{2}{3}}\left(\frac{1}{2} + \frac{\sqrt{-3}}{2}\right), 2^{\frac{2}{3}}\left(\frac{1}{2} - \frac{\sqrt{-3}}{2}\right) \right\}\\ &= \left\{ -2^{\frac{2}{3}}, 2^{\frac{2}{3}}\left(2^{-1} + (-3)^{\frac{1}{2}} \cdot 2^{-1}\right), 2^{\frac{2}{3}}\left(2^{-1} - (-3)^{\frac{1}{2}} \cdot 2^{-1}\right), \right\}\\ &= \left\{ -2^{\frac{2}{3}}, 2^{\frac{-1}{3}} + (-3)^{\frac{1}{2}} \cdot 2^{\frac{-1}{3}}, 2^{\frac{-1}{3}} - (-3)^{\frac{1}{2}} \cdot 2^{\frac{-1}{3}} \right\}\\ &= \left\{ -\sqrt[3]{4}, \frac{1+\sqrt{-3}}{\sqrt[3]{2}}, \frac{1-\sqrt{-3}}{\sqrt[3]{2}} \right\}\end{aligned}$$

Hence we know that $x = 0, -\sqrt[3]{4}, \frac{1+\sqrt{-3}}{\sqrt[3]{2}}, \frac{1-\sqrt{-3}}{\sqrt[3]{2}}$ will result in a point of u_0 that has order 3. Note that

$$y^2 = (0)^3 + 1 \Leftrightarrow y^2 = 1 \Leftrightarrow y = \pm 1$$

Let $a = -\sqrt[3]{4}, \frac{1+\sqrt{-3}}{\sqrt[3]{2}}, \frac{1-\sqrt{-3}}{\sqrt[3]{2}}$. Since for any value a takes, it is a cube root of -4 we know that $a^3 = -4$. Hence we have

$$y^2 = a^3 + 1 \Leftrightarrow y^2 = -4 + 1 \Leftrightarrow y^2 = -3 \Leftrightarrow y = \pm\sqrt{-3}$$

Thus the points

$$\left\{(0,1),(0,-1),\left(-\sqrt[3]{4},\sqrt{-3}\right),\left(-\sqrt[3]{4},-\sqrt{-3}\right),\left(\frac{1+\sqrt{-3}}{\sqrt[3]{2}},\sqrt{-3}\right),\right.$$
$$\left.\left(\frac{1+\sqrt{-3}}{\sqrt[3]{2}},-\sqrt{-3}\right),\left(\frac{1-\sqrt{-3}}{\sqrt[3]{2}},\sqrt{-3}\right),\left(\frac{1-\sqrt{-3}}{\sqrt[3]{2}},-\sqrt{-3}\right)\right\}$$

have order 3 in u_0.

Now we wish to find the subgroups of u_0 of order 3. We know that they must be generated by the points above. We also know that for every element its negative must be in the group as well. For elliptic curve points, that means that if (x,y) is in our subgroup, then so is $(x,-y)$. Thus we realize the four subgroups of u_0 of order 3 to be

$$\langle(0,1)\rangle = \{(0,1),(0,-1),\mathcal{O}_{u_0}\}$$
$$\left\langle\left(-\sqrt[3]{4},\sqrt{-3}\right)\right\rangle = \left\{\left(-\sqrt[3]{4},\sqrt{-3}\right),\left(-\sqrt[3]{4},-\sqrt{-3}\right),\mathcal{O}_{u_0}\right\}$$
$$\left\langle\left(\frac{1+\sqrt{-3}}{\sqrt[3]{2}},\sqrt{-3}\right)\right\rangle = \left\{\left(\frac{1+\sqrt{-3}}{\sqrt[3]{2}},\sqrt{-3}\right),\left(\frac{1+\sqrt{-3}}{\sqrt[3]{2}},-\sqrt{-3}\right),\mathcal{O}_{u_0}\right\}$$
$$\left\langle\left(\frac{1-\sqrt{-3}}{\sqrt[3]{2}},\sqrt{-3}\right)\right\rangle = \left\{\left(\frac{1-\sqrt{-3}}{\sqrt[3]{2}},\sqrt{-3}\right),\left(\frac{1-\sqrt{-3}}{\sqrt[3]{2}},-\sqrt{-3}\right),\mathcal{O}_{u_0}\right\}$$

■

Lemma 1.6.38: The 3-torsion subgroups of $w_0 : y^2 = x^3 - 3$ are

$$\left\langle\left(0,\sqrt{-3}\right)\right\rangle = \left\{\left(0,\sqrt{-3}\right),\left(0,-\sqrt{-3}\right),\mathcal{O}_{w_0}\right\}$$
$$\left\langle\left(\sqrt[3]{12},3\right)\right\rangle = \left\{\left(\sqrt[3]{12},3\right),\left(\sqrt[3]{12},-3\right),\mathcal{O}_{w_0}\right\}$$
$$\left\langle\left(\frac{-\sqrt[3]{3}+\sqrt[3]{3}\sqrt{-3}}{\sqrt[3]{2}},3\right)\right\rangle = \left\{\left(\frac{-\sqrt[3]{3}+\sqrt[3]{3}\sqrt{-3}}{\sqrt[3]{2}},3\right),\left(\frac{-\sqrt[3]{3}+\sqrt[3]{3}\sqrt{-3}}{\sqrt[3]{2}},-3\right),\mathcal{O}_{w_0}\right\}$$
$$\left\langle\left(\frac{-\sqrt[3]{3}-\sqrt[3]{3}\sqrt{-3}}{\sqrt[3]{2}},3\right)\right\rangle = \left\{\left(\frac{-\sqrt[3]{3}-\sqrt[3]{3}\sqrt{-3}}{\sqrt[3]{2}},3\right),\left(\frac{-\sqrt[3]{3}-\sqrt[3]{3}\sqrt{-3}}{\sqrt[3]{2}},-3\right),\mathcal{O}_{w_0}\right\}$$

Proof: By a quick computation, we see that the third division polynomial of w_0 is

$$3x(x^3-12)$$

We know the roots of this polynomial to be $x=0$ and $x=\sqrt[3]{12}$. Similar to the previous case, we first find the cube roots using complex analysis, then switch back into $\mathbb{F}_p$:

$$\begin{aligned}
\sqrt[3]{12} &= \left\{\sqrt[3]{12}\cdot\exp\left(i\frac{2k\pi}{3}\right) : k=0,1,2\right\}\\
&= \left\{\sqrt[3]{12}, \sqrt[3]{12}\exp\left(i\frac{2\pi}{3}\right), \sqrt[3]{12}\exp\left(i\frac{4\pi}{3}\right)\right\}\\
&= \left\{\sqrt[3]{12}, \sqrt[3]{12}\left(-\frac{1}{2}+i\frac{\sqrt{3}}{2}\right), \sqrt[3]{12}\left(-\frac{1}{2}-i\frac{\sqrt{3}}{2}\right)\right\}\\
&= \left\{\sqrt[3]{12}, 2^{\frac{2}{3}}3^{\frac{1}{3}}\left(-2^{-1}+2^{-1}(-3)^{\frac{1}{2}}\right), 2^{\frac{2}{3}}3^{\frac{1}{3}}\left(-2^{-1}-2^{-1}(-3)^{\frac{1}{2}}\right)\right\}\\
&= \left\{\sqrt[3]{12}, -2^{\frac{-1}{3}}3^{\frac{1]}{3}}+2^{\frac{-1}{3}}3^{\frac{1}{3}}(-3)^{\frac{1}{2}}, -2^{\frac{-1}{3}}3^{\frac{1]}{3}}-2^{\frac{-1}{3}}3^{\frac{1}{3}}(-3)^{\frac{1}{2}}\right\}\\
&= \left\{\sqrt[3]{12}, \frac{-\sqrt[3]{3}+\sqrt[3]{3}\sqrt{-3}}{\sqrt[3]{2}}, \frac{-\sqrt[3]{3}-\sqrt[3]{3}\sqrt{-3}}{\sqrt[3]{2}}\right\}
\end{aligned}$$

Hence we know that the values $x=0, \sqrt[3]{12}, \frac{-\sqrt[3]{3}+\sqrt[3]{3}\sqrt{-3}}{\sqrt[3]{2}}, \frac{-\sqrt[3]{3}-\sqrt[3]{3}\sqrt{-3}}{\sqrt[3]{2}}$ will result in a point of w_0 having order 3.

Note that when $x=0$, we have $y^2=(0)^3-3=-3$. Hence we know that the points $\left(0,\sqrt{-3}\right), \left(0,-\sqrt{-3}\right)$ are on w_0 and they have order 3.

Furthermore, note that for $x=\sqrt[3]{12}, \frac{-\sqrt[3]{3}+\sqrt[3]{3}\sqrt{-3}}{\sqrt[3]{2}}, \frac{-\sqrt[3]{3}-\sqrt[3]{3}\sqrt{-3}}{\sqrt[3]{2}}$, the value of x^3 is always 12 by definition. Hence we know that for all of them, $y^2=x^3-3=12-3=9$. Hence the points $(x,\pm 3)$ is a point on w_0 with order 3.

Thus we conclude that the points of order 3 on w_0 are

$$\begin{aligned}
\left\{\left(0,\sqrt{-3}\right), \left(0,-\sqrt{-3}\right), \left(\sqrt[3]{12},3\right), \left(\sqrt[3]{12},-3\right), \left(\frac{-\sqrt[3]{3}+\sqrt[3]{3}\sqrt{-3}}{\sqrt[3]{2}},3\right),\right.\\
\left.\left(\frac{-\sqrt[3]{3}+\sqrt[3]{3}\sqrt{-3}}{\sqrt[3]{2}},-3\right), \left(\frac{-\sqrt[3]{3}-\sqrt[3]{3}\sqrt{-3}}{\sqrt[3]{2}},3\right), \left(\frac{-\sqrt[3]{3}-\sqrt[3]{3}\sqrt{-3}}{\sqrt[3]{2}},-3\right)\right\}
\end{aligned}$$

We know that the subgroups of order three must be generated by the points above. We also know that for an element in a subgroup, its negative is also in the subgroup. For elliptic curves this means that if (x,y) is in the subgroup, then so is $(x,-y)$. Hence we know that the subgroups of order 3 of w_0 are

$$\left\langle\left(0,\sqrt{-3}\right)\right\rangle = \left\{\left(0,\sqrt{-3}\right), \left(0,-\sqrt{-3}\right), \mathcal{O}_{w_0}\right\}$$

$$\left\langle\left(\sqrt[3]{12},3\right)\right\rangle = \left\{\left(\sqrt[3]{12},3\right), \left(\sqrt[3]{12},-3\right), \mathcal{O}_{w_0}\right\}$$

$$\left\langle\left(\frac{-\sqrt[3]{3}+\sqrt[3]{3}\sqrt{-3}}{\sqrt[3]{2}},3\right)\right\rangle = \left\{\left(\frac{-\sqrt[3]{3}+\sqrt[3]{3}\sqrt{-3}}{\sqrt[3]{2}},3\right), \left(\frac{-\sqrt[3]{3}+\sqrt[3]{3}\sqrt{-3}}{\sqrt[3]{2}},-3\right), \mathcal{O}_{w_0}\right\}$$

$$\left\langle \left(\frac{-\sqrt[3]{3}-\sqrt[3]{3}\sqrt{-3}}{\sqrt[3]{2}}, 3 \right) \right\rangle = \left\{ \left(\frac{-\sqrt[3]{3}-\sqrt[3]{3}\sqrt{-3}}{\sqrt[3]{2}}, 3 \right), \left(\frac{-\sqrt[3]{3}-\sqrt[3]{3}\sqrt{-3}}{\sqrt[3]{2}}, -3 \right), \mathcal{O}_{w_0} \right\}$$

■

Recall that we know an isogeny is defined over $\mathbb{F}_p$ if the Frobenius endomorphism preserves the kernel. Further recall that the Frobenius map permutes the roots of an irreducible quadratic polynomial. As a result we know that the isogenies generated by $\langle (0,1) \rangle$, $\left\langle \left(-\sqrt[3]{4}, \sqrt{-3} \right) \right\rangle$, $\langle (0, \sqrt{-3}) \rangle$, $\left\langle \left(\sqrt[3]{12}, 3 \right) \right\rangle$ are the only isogenies defined over $\mathbb{F}_p$. Note that Table 7 describes the isogenies generated by these kernels:

Name	Domain	Codomain	Kernel
$\phi_{3,1}$	u_0	w_0	$\langle (0,1) \rangle$
$\phi_{3,2}$	u_0	$u_{-12288000}$	$\left\langle \left(-\sqrt[3]{4}, \sqrt{-3} \right) \right\rangle$
$\psi_{3,1}$	w_0	u_0	$\langle (0, \sqrt{-3}) \rangle$
$\psi_{3,2}$	w_0	$w_{-12288000}$	$\left\langle \left(\sqrt[3]{12}, 3 \right) \right\rangle$

Table 7: Description of the isogenies of degree 3 with domain u_0 and w_0 defined over $\mathbb{F}_p$ by the use of Velu's formula.

Lemma 1.6.39: $\phi_{3,1}$ is equivalent to $\psi_{3,1}$ over $\mathbb{F}_{p^2}$.

Proof: Note the following:

$$\begin{aligned} \eta_{0,1}\langle (0,1) \rangle &= \langle \eta_{0,1}(0,1) \rangle \\ &= \left\langle \left(-\sqrt[3]{3} \cdot 0, \sqrt{-3} \cdot 1 \right) \right\rangle \\ &= \left\langle \left(0, \sqrt{-3} \right) \right\rangle \end{aligned}$$

Hence we can realize that

$$\eta_{0,1}(\ker(\phi_{3,1})) = \eta_{0,1}\langle (0,1) \rangle = \left\langle \left(0, \sqrt{-3} \right) \right\rangle = \ker(\psi_{3,1})$$

Thus by **Lemma 1.6.33**, we conclude that $\phi_{3,1}$ is equivalent to $\psi_{3,1}$ which proves the statement. ■

Lemma 1.6.40: $\psi_{3,2}$ is equivalent to $\psi_{3,2}$ over $\mathbb{F}_{p^2}$.

Proof: Note the following:

$$\begin{aligned} \eta_{0,2} \left\langle \left(-\sqrt[3]{4}, \sqrt{-3} \right) \right\rangle &= \left\langle \eta_{0,2} \left(-\sqrt[3]{4}, \sqrt{-3} \right) \right\rangle \\ &= \left\langle \left(\left(-\sqrt[3]{3} \right) \left(-\sqrt[3]{4} \right), \left(-\sqrt{-3} \right) \left(\sqrt{-3} \right) \right) \right\rangle \\ &= \left\langle \left(\sqrt[3]{12}, 3 \right) \right\rangle \end{aligned}$$

Hence we can realize that

$$\eta_{0,2}(\ker(\phi_{3,2})) = \eta_{0,2}\left\langle\left(-\sqrt[3]{4}, \sqrt{-3}\right)\right\rangle = \left\langle\left(\sqrt[3]{12}, 3\right)\right\rangle = \ker(\psi_{3,2})$$

Thus by **Lemma 1.6.33**, we conclude that $\phi_{3,2}$ is equivalent to $\psi_{3,2}$ which proves the statement. ■

Theorem 1.6.41: All isogenies that leave an elliptic curve with j-invariant of 0 in $\mathcal{G}_3(\mathbb{F}_p)$ fold.

Proof: The statement follows by **Lemma 1.6.39** and **Lemma 1.6.40**. ■

Lemma 1.6.42: The 3-torsion subgroups of $u_{1728} : y^2 = x^3 + x$ are

$$\left\langle\left(\frac{\sqrt{3}+1}{\sqrt{2}\sqrt[4]{3}}, \frac{2^{\frac{1}{4}}(\sqrt{3}-1)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right)\right\rangle = \left\{\left(\frac{\sqrt{3}+1}{\sqrt{2}\sqrt[4]{3}}, \frac{2^{\frac{1}{4}}(\sqrt{3}-1)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right), \left(\frac{\sqrt{3}+1}{\sqrt{2}\sqrt[4]{3}}, -\frac{2^{\frac{1}{4}}(\sqrt{3}-1)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right), \mathcal{O}_{u_{1728}}\right\}$$

$$\left\langle\left(-\frac{\sqrt{3}+1}{\sqrt{2}\sqrt[4]{3}}, i\frac{2^{\frac{1}{4}}(\sqrt{3}-1)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right)\right\rangle = \left\{\left(-\frac{\sqrt{3}+1}{\sqrt{2}\sqrt[4]{3}}, i\frac{2^{\frac{1}{4}}(\sqrt{3}-1)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right), \left(-\frac{\sqrt{3}+1}{\sqrt{2}\sqrt[4]{3}}, -i\frac{2^{\frac{1}{4}}(\sqrt{3}-1)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right), \mathcal{O}_{u_{1728}}\right\}$$

$$\left\langle\left(\frac{i(\sqrt{3}+1)}{\sqrt{2}\sqrt[4]{3}}, \frac{i^{\frac{3}{4}}\cdot 2^{\frac{1}{4}}\cdot\left(3^{\frac{1}{2}}+1\right)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right)\right\rangle = \left\{\left(\frac{i(\sqrt{3}+1)}{\sqrt{2}\sqrt[4]{3}}, \frac{i^{\frac{3}{4}}\cdot 2^{\frac{1}{4}}\cdot\left(3^{\frac{1}{2}}+1\right)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right), \left(\frac{i(\sqrt{3}+1)}{\sqrt{2}\sqrt[4]{3}}, -\frac{i^{\frac{3}{4}}\cdot 2^{\frac{1}{4}}\cdot\left(3^{\frac{1}{2}}+1\right)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right), \mathcal{O}_{u_{1728}}\right\}$$

$$\left\langle\left(-\frac{i(\sqrt{3}+1)}{\sqrt{2}\sqrt[4]{3}}, \frac{i^{\frac{1}{4}}\cdot 2^{\frac{1}{4}}\cdot\left(3^{\frac{1}{2}}+1\right)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right)\right\rangle = \left\{\left(-\frac{i(\sqrt{3}+1)}{\sqrt{2}\sqrt[4]{3}}, \frac{i^{\frac{1}{4}}\cdot 2^{\frac{1}{4}}\cdot\left(3^{\frac{1}{2}}+1\right)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right), \left(-\frac{i(\sqrt{3}+1)}{\sqrt{2}\sqrt[4]{3}}, -\frac{i^{\frac{1}{4}}\cdot 2^{\frac{1}{4}}\cdot\left(3^{\frac{1}{2}}+1\right)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right), \mathcal{O}_{u_{1728}}\right\}$$

Proof: Via a quick computation, we can find that the third division polynomial of u_{1728} is

$$3x^4 + 6x^2 - 1$$

We can find the roots by:

$$
\begin{aligned}
3x^4+6x^2-1=3\left(x^2\right)^2+6\left(x^2\right)-1=0 \\
\Rightarrow x^2=\frac{-6\pm\sqrt{36-4(3)(-1)}}{2(3)} \\
x^2=\frac{-6\pm\sqrt{48}}{6} \\
x^2=\frac{-6\pm4\sqrt{3}}{6} \\
x^2=\frac{-3\pm2\sqrt{3}}{3} \\
x=\pm\sqrt{\frac{-3\pm2\sqrt{3}}{3}} \\
x=\frac{\pm\sqrt{-3\pm2\sqrt{3}}}{\sqrt{3}} \\
x=\begin{cases}\frac{\pm\sqrt{-3+2\sqrt{3}}}{\sqrt{3}}\\ \frac{\pm\sqrt{-3-2\sqrt{3}}}{\sqrt{3}}\end{cases} \\
x=\begin{cases}\pm\frac{\sqrt[4]{3}\sqrt{-\sqrt{3}+2}}{\sqrt{3}}\\ \pm\frac{i\sqrt[4]{3}\sqrt{\sqrt{3}+2}}{\sqrt{3}}\end{cases} \\
x=\begin{cases}\pm\frac{\sqrt[4]{3}\sqrt{\left(\frac{\sqrt{3}-1}{\sqrt{2}}\right)^2}}{\sqrt{3}}\\ \pm\frac{i\sqrt[4]{3}\sqrt{\left(\frac{\sqrt{3}+1}{\sqrt{2}}\right)^2}}{\sqrt{3}}\end{cases} \\
x=\begin{cases}\pm\frac{\sqrt{3}-1}{\sqrt{2}\sqrt[4]{3}}\\ \pm\frac{i\left(\sqrt{3}+1\right)}{\sqrt{2}\sqrt[4]{3}}\end{cases}
\end{aligned}
$$

Hence we can find the y values in the following cases:

$$\begin{aligned}
y^2 &= \left(\pm\frac{\sqrt{3}-1}{\sqrt{2}\sqrt[4]{3}}\right)^3 + \left(\pm\frac{\sqrt{3}-1}{\sqrt{2}\sqrt[4]{3}}\right) \\
&= \pm\left(\frac{\left(\sqrt{3}-1\right)^3}{2^{\frac{3}{2}}\cdot 3^{\frac{3}{4}}} + \frac{\left(\sqrt{3}-1\right)}{2^{\frac{1}{2}}\cdot 3^{\frac{1}{4}}}\right) \\
&= \pm\frac{\sqrt{3}-1}{2^{\frac{1}{2}}\cdot 3^{\frac{1}{4}}}\left(\frac{\left(\sqrt{3}-1\right)^2}{2\sqrt{3}}+1\right) \\
&= \pm\frac{\sqrt{3}-1}{2^{\frac{1}{2}}\cdot 3^{\frac{1}{4}}}\left(\frac{4-2\sqrt{3}}{2\sqrt{3}}+1\right) \\
&= \pm\frac{\sqrt{3}-1}{2^{\frac{1}{2}}\cdot 3^{\frac{1}{4}}}\left(\frac{2}{\sqrt{3}}\right) \\
&= \pm\frac{2^{\frac{1}{2}}\left(\sqrt{3}-1\right)}{3^{\frac{3}{4}}} \\
\Rightarrow y &= \begin{cases} \pm\frac{2^{\frac{1}{4}}\left(\sqrt{3}-1\right)^{\frac{1}{2}}}{3^{\frac{3}{8}}} \\ \pm i\frac{2^{\frac{1}{4}}\left(\sqrt{3}-1\right)^{\frac{1}{2}}}{3^{\frac{3}{8}}} \end{cases}
\end{aligned}$$

In the other case we have:

$$\begin{aligned}
y^2 &= \left(\pm\frac{i\left(\sqrt{3}+1\right)}{\sqrt{2}\sqrt[4]{3}}\right)^3 + \left(\pm\frac{i\left(\sqrt{3}+1\right)}{\sqrt{2}\sqrt[4]{3}}\right) \\
&= \pm\left(\frac{i^3\left(\sqrt{3}+1\right)^3}{2^{\frac{3}{2}}\cdot 3^{\frac{3}{4}}} + \frac{i\left(\sqrt{3}+1\right)}{2^{\frac{1}{2}}\cdot 3^{\frac{1}{4}}}\right) \\
&= \pm\frac{i\left(\sqrt{3}+1\right)}{2^{\frac{1}{2}}\cdot 3^{\frac{1}{4}}}\left(\frac{i^2\left(\sqrt{3}+1\right)^2}{2\sqrt{3}}+1\right) \\
&= \pm\frac{i\left(\sqrt{3}+1\right)}{2^{\frac{1}{2}}\cdot 3^{\frac{1}{4}}}\left(\frac{-4-2\sqrt{3}}{2\sqrt{3}}+1\right) \\
&= \pm\frac{i\left(\sqrt{3}+1\right)}{2^{\frac{1}{2}}3^{\frac{1}{4}}}\left(\frac{-2}{\cdot}\sqrt{3}\right) \\
&= \pm\frac{-i\sqrt{2}\left(\sqrt{3}+1\right)}{3^{\frac{3}{4}}}
\end{aligned}$$

$$\Rightarrow y = \begin{cases} \pm\frac{i^{\frac{3}{2}}\cdot 2^{\frac{1}{4}}\cdot\left(3^{\frac{1}{2}}+1\right)^{\frac{1}{2}}}{3^{\frac{3}{8}}} \\ \pm\frac{i^{\frac{1}{2}}\cdot 2^{\frac{1}{4}}\cdot\left(3^{\frac{1}{2}}+1\right)^{\frac{1}{2}}}{3^{\frac{3}{8}}} \end{cases}$$

Thus we conclude that the points of order 3 of u_{1728} are:

$$\left\{\left(\frac{\sqrt{3}+1}{\sqrt{2}\sqrt[4]{3}},\frac{2^{\frac{1}{4}}\left(\sqrt{3}-1\right)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right),\left(\frac{\sqrt{3}+1}{\sqrt{2}\sqrt[4]{3}},-\frac{2^{\frac{1}{4}}\left(\sqrt{3}-1\right)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right),\right.$$
$$\left(-\frac{\sqrt{3}+1}{\sqrt{2}\sqrt[4]{3}},i\frac{2^{\frac{1}{4}}\left(\sqrt{3}-1\right)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right),\left(-\frac{\sqrt{3}+1}{\sqrt{2}\sqrt[4]{3}},-i\frac{2^{\frac{1}{4}}\left(\sqrt{3}-1\right)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right),$$
$$\left(\frac{i\left(\sqrt{3}+1\right)}{\sqrt{2}\sqrt[4]{3}},\frac{i^{\frac{3}{2}}\cdot 2^{\frac{1}{4}}\cdot\left(3^{\frac{1}{2}}+1\right)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right),\left(\frac{i\left(\sqrt{3}+1\right)}{\sqrt{2}\sqrt[4]{3}},-\frac{i^{\frac{3}{2}}\cdot 2^{\frac{1}{4}}\cdot\left(3^{\frac{1}{2}}+1\right)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right),$$
$$\left.\left(-\frac{i\left(\sqrt{3}+1\right)}{\sqrt{2}\sqrt[4]{3}},\frac{i^{\frac{1}{2}}\cdot 2^{\frac{1}{4}}\cdot\left(3^{\frac{1}{2}}+1\right)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right),\left(-\frac{i\left(\sqrt{3}+1\right)}{\sqrt{2}\sqrt[4]{3}},-\frac{i^{\frac{1}{2}}\cdot 2^{\frac{1}{4}}\cdot\left(3^{\frac{1}{2}}+1\right)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right)\right\}$$

Now, since we know that every subgroup of order 3 in u_{1728} is generated by one of the above, and we also know that if (x,y) is in our subgroup, then so is $(x,-y)$, we conclude that the following are the subgroups of order 3 in u_{1728}:

$$\left\langle\left(\frac{\sqrt{3}+1}{\sqrt{2}\sqrt[4]{3}},\frac{2^{\frac{1}{4}}\left(\sqrt{3}-1\right)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right)\right\rangle=\left\{\left(\frac{\sqrt{3}+1}{\sqrt{2}\sqrt[4]{3}},\frac{2^{\frac{1}{4}}\left(\sqrt{3}-1\right)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right),\left(\frac{\sqrt{3}+1}{\sqrt{2}\sqrt[4]{3}},-\frac{2^{\frac{1}{4}}\left(\sqrt{3}-1\right)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right),\mathcal{O}_{u_{1728}}\right\}$$

$$\left\langle\left(-\frac{\sqrt{3}+1}{\sqrt{2}\sqrt[4]{3}},i\frac{2^{\frac{1}{4}}\left(\sqrt{3}-1\right)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right)\right\rangle=\left\{\left(-\frac{\sqrt{3}+1}{\sqrt{2}\sqrt[4]{3}},i\frac{2^{\frac{1}{4}}\left(\sqrt{3}-1\right)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right),\left(-\frac{\sqrt{3}+1}{\sqrt{2}\sqrt[4]{3}},-i\frac{2^{\frac{1}{4}}\left(\sqrt{3}-1\right)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right),\mathcal{O}_{u_{1728}}\right\}$$

$$\left\langle\left(\frac{i\left(\sqrt{3}+1\right)}{\sqrt{2}\sqrt[4]{3}},\frac{i^{\frac{3}{4}}\cdot 2^{\frac{1}{4}}\cdot\left(3^{\frac{1}{2}}+1\right)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right)\right\rangle=\left\{\left(\frac{i\left(\sqrt{3}+1\right)}{\sqrt{2}\sqrt[4]{3}},\frac{i^{\frac{3}{4}}\cdot 2^{\frac{1}{4}}\cdot\left(3^{\frac{1}{2}}+1\right)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right),\left(\frac{i\left(\sqrt{3}+1\right)}{\sqrt{2}\sqrt[4]{3}},-\frac{i^{\frac{3}{4}}\cdot 2^{\frac{1}{4}}\cdot\left(3^{\frac{1}{2}}+1\right)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right),\mathcal{O}_{u_{1728}}\right\}$$

$$\left\langle\left(-\frac{i\left(\sqrt{3}+1\right)}{\sqrt{2}\sqrt[4]{3}},\frac{i^{\frac{1}{4}}\cdot 2^{\frac{1}{4}}\cdot\left(3^{\frac{1}{2}}+1\right)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right)\right\rangle=\left\{\left(-\frac{i\left(\sqrt{3}+1\right)}{\sqrt{2}\sqrt[4]{3}},\frac{i^{\frac{1}{4}}\cdot 2^{\frac{1}{4}}\cdot\left(3^{\frac{1}{2}}+1\right)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right),\left(-\frac{i\left(\sqrt{3}+1\right)}{\sqrt{2}\sqrt[4]{3}},-\frac{i^{\frac{1}{4}}\cdot 2^{\frac{1}{4}}\cdot\left(3^{\frac{1}{2}}+1\right)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right),\mathcal{O}_{u_{1728}}\right\}$$

■

Lemma 1.6.43: The outgoing isogenies of u_{1728} do not fold.

Proof: If we would like to find out which of the following subgroups are defined over $\mathbb{F}_p$, we have to apply the Frobenius endomorphism to the points. Recall that the Frobenius endomorphism permutes the roots of irreducible quadratics and fixes the roots of elements in $\mathbb{F}_p$. Note that for any y in any of the subgroups, y^p since the y values were found via a quadratic. Further note that since $p\equiv 3 \pmod 4$ we know that $\left(\frac{-1}{p}\right)=-1$, which implies that $i\notin\mathbb{F}_p$. Hence we know that

$$\pm\frac{i\left(\sqrt{3}+1\right)}{\sqrt{2}\sqrt[4]{3}}\notin\mathbb{F}_p$$

And hence we know that frobenius switches the two values $\pm\frac{i(\sqrt{3}+1)}{\sqrt{2}\sqrt[4]{3}}$ which lie in different subgroups. Hence we know that the subgroups

$$\left\langle\left(\frac{i(\sqrt{3}+1)}{\sqrt{2}\sqrt[4]{3}}, \frac{i^{\frac{3}{4}}\cdot 2^{\frac{1}{4}}\cdot\left(3^{\frac{1}{2}}+1\right)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right)\right\rangle \quad \text{and} \quad \left\langle\left(-\frac{i(\sqrt{3}+1)}{\sqrt{2}\sqrt[4]{3}}, \frac{i^{\frac{1}{4}}\cdot 2^{\frac{1}{4}}\cdot\left(3^{\frac{1}{2}}+1\right)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right)\right\rangle$$

Are not the kernels of isogenies defined over $\mathbb{F}_p$.

Now, suppose that $p \equiv 2 \pmod 3 \Leftrightarrow \left(\frac{-p}{3}\right) = 1$, which by **Theorem 1.4.4** implies that there are isogenies defined over $\mathbb{F}_p$. In this case we have $p \equiv 11 \pmod{12}$ we know that $\sqrt{3}$, $\sqrt[4]{3}$, and $\sqrt{2}$ are defined over $\mathbb{F}_p$. Hence we know that Frobenius fixes the values

$$\pm\frac{\sqrt{3}+1}{\sqrt{2}\sqrt[4]{3}}$$

As a result we conclude that if $p \equiv 11 \pmod{12}$, then the isogenies with kernels

$$\left\langle\left(\frac{\sqrt{3}+1}{\sqrt{2}\sqrt[4]{3}}, \frac{2^{\frac{1}{4}}\left(\sqrt{3}-1\right)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right)\right\rangle \quad \text{and} \quad \left\langle\left(-\frac{\sqrt{3}+1}{\sqrt{2}\sqrt[4]{3}}, i\frac{2^{\frac{1}{4}}\left(\sqrt{3}-1\right)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right)\right\rangle$$

are defined over $\mathbb{F}_p$.

We know by [Arp+23] that the codomains of these isogenies have the same j-invariant (1728 partakes in vertex attachment). Hence By the definition of equivalence, we know that these two isogenies cannot be equivalent over $\overline{\mathbb{F}_p}$. Hence we know that the isogenies going out of u_{1728} do not fold. ■

Lemma 1.6.44: The 3-torsion subgroups of $w_{1728} : y^2 = x^3 - x$ are

$$\left\langle\left(\frac{\sqrt{3}+1}{\sqrt{2}\sqrt[4]{3}}, \frac{2^{\frac{1}{4}}\cdot(\sqrt{3}+1)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right)\right\rangle = \left\{\left(\frac{\sqrt{3}+1}{\sqrt{2}\sqrt[4]{3}}, \frac{2^{\frac{1}{4}}\cdot(\sqrt{3}+1)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right), \left(\frac{\sqrt{3}+1}{\sqrt{2}\sqrt[4]{3}}, -\frac{2^{\frac{1}{4}}\cdot(\sqrt{3}+1)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right), \mathcal{O}_{w_{1728}}\right\}$$

$$\left\langle\left(-\frac{\sqrt{3}+1}{\sqrt{2}\sqrt[4]{3}}, \frac{i\cdot 2^{\frac{1}{4}}\cdot(\sqrt{3}+1)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right)\right\rangle = \left\{\left(-\frac{\sqrt{3}+1}{\sqrt{2}\sqrt[4]{3}}, \frac{i\cdot 2^{\frac{1}{4}}\cdot(\sqrt{3}+1)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right), \left(-\frac{\sqrt{3}+1}{\sqrt{2}\sqrt[4]{3}}, -\frac{i\cdot 2^{\frac{1}{4}}\cdot(\sqrt{3}+1)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right), \mathcal{O}_{w_{1728}}\right\}$$

$$\left\langle\left(i\frac{\sqrt{3}-1}{\sqrt{2}\sqrt[4]{3}}, \frac{i^{\frac{3}{2}}\cdot 2^{\frac{1}{4}}\cdot(\sqrt{3}-1)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right)\right\rangle = \left\{\left(i\frac{\sqrt{3}-1}{\sqrt{2}\sqrt[4]{3}}, \frac{i^{\frac{3}{2}}\cdot 2^{\frac{1}{4}}\cdot(\sqrt{3}-1)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right), \left(i\frac{\sqrt{3}-1}{\sqrt{2}\sqrt[4]{3}}, -\frac{i^{\frac{3}{2}}\cdot 2^{\frac{1}{4}}\cdot(\sqrt{3}-1)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right), \mathcal{O}_{w_{1728}}\right\}$$

$$\left\langle\left(-i\frac{\sqrt{3}-1}{\sqrt{2}\sqrt[4]{3}}, \frac{i^{\frac{1}{2}}\cdot 2^{\frac{1}{4}}\cdot(\sqrt{3}-1)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right)\right\rangle = \left\{\left(-i\frac{\sqrt{3}-1}{\sqrt{2}\sqrt[4]{3}}, \frac{i^{\frac{1}{2}}\cdot 2^{\frac{1}{4}}\cdot(\sqrt{3}-1)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right), \left(-i\frac{\sqrt{3}-1}{\sqrt{2}\sqrt[4]{3}}, -\frac{i^{\frac{1}{2}}\cdot 2^{\frac{1}{4}}\cdot(\sqrt{3}-1)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right), \mathcal{O}_{w_{1728}}\right\}$$

Proof: Via a quick computation, we can find that the third division polynomial of w_{1728} is

$$3x^4 - 6x^2 - 1$$

We can find the roots by:

$$
\begin{aligned}
3x^4 - 6x^2 - 1 &= 0 \\
x^2 &= \frac{6 \pm \sqrt{36 - 4(3)(-1)}}{2(3)} \\
x^2 &= \frac{3 \pm 2\sqrt{3}}{3} \\
x^2 &= \frac{\sqrt{3} \pm 2}{\sqrt{3}} \\
x &= \begin{cases} \pm \frac{\sqrt{\sqrt{3}+2}}{\sqrt[4]{3}} \\ \pm \frac{\sqrt{\sqrt{3}-2}}{\sqrt[4]{3}} \end{cases} \\
x &= \begin{cases} \pm \frac{\sqrt{\left(\frac{\sqrt{3}+1}{\sqrt{2}}\right)^2}}{\sqrt[4]{3}} \\ \pm \frac{\sqrt{\left(i\frac{\sqrt{3}-1}{\sqrt{2}}\right)^2}}{\sqrt[4]{3}} \end{cases} \\
x &= \begin{cases} \pm \frac{\sqrt{3}+1}{\sqrt{2}\sqrt[4]{3}} \\ \pm i\frac{\sqrt{3}-1}{\sqrt{2}\sqrt[4]{3}} \end{cases}
\end{aligned}
$$

Hence since we have $y^2 = x^3 - x = x(x^2-1)$, we can find the y values as:

$$
\begin{aligned}
y^2 &= \pm \frac{\sqrt{3}+1}{\sqrt{2}\sqrt[4]{3}} \left(\frac{(\sqrt{3}+1)^2}{2\sqrt{3}} - 1 \right) \\
y^2 &= \pm \frac{\sqrt{3}+1}{\sqrt{2}\sqrt[4]{3}} \left(\frac{4+2\sqrt{3}}{2\sqrt{3}} - 1 \right) \\
y^2 &= \pm \frac{\sqrt{3}+1}{\sqrt{2}\sqrt[4]{3}} \left(\frac{2}{\sqrt{3}} \right) \\
y^2 &= \pm \frac{\sqrt{2}\left(\sqrt{3}+1\right)}{3^{\frac{3}{4}}} \\
y &= \begin{cases} \pm \frac{2^{\frac{1}{4}} \cdot \left(\sqrt{3}+1\right)^{\frac{1}{2}}}{3^{\frac{3}{8}}} \\ \pm \frac{i \cdot 2^{\frac{1}{4}} \cdot \left(\sqrt{3}+1\right)^{\frac{1}{2}}}{3^{\frac{3}{8}}} \end{cases}
\end{aligned}
$$

And in the other case:

$$y^2 = \pm i\frac{\sqrt{3}-1}{\sqrt{2}\sqrt[4]{3}}\left(\frac{(i(\sqrt{3}-1))^2}{2\sqrt{3}}-1\right)$$
$$y^2 = \pm i\frac{\sqrt{3}-1}{\sqrt{2}\sqrt[4]{3}}\left(\frac{-4+2\sqrt{3}}{2\sqrt{3}}-1\right)$$
$$y^2 = \pm i\frac{\sqrt{3}-1}{\sqrt{2}\sqrt[4]{3}}\left(\frac{-2}{\sqrt{3}}\right)$$
$$y^2 = \pm i\frac{\sqrt{2}(\sqrt{3}-1)}{3^{\frac{3}{4}}}$$
$$y = \begin{cases} \pm\frac{i^{\frac{3}{2}}\cdot 2^{\frac{1}{4}}\cdot(\sqrt{3}-1)^{\frac{1}{2}}}{3^{\frac{3}{8}}} \\ \pm\frac{i^{\frac{1}{2}}\cdot 2^{\frac{1}{4}}\cdot(\sqrt{3}-1)^{\frac{1}{2}}}{3^{\frac{3}{8}}} \end{cases}$$

Hence we can see that the points of order three in w_{1728} are:

$$\left\{\left(\frac{\sqrt{3}+1}{\sqrt{2}\sqrt[4]{3}}, \frac{2^{\frac{1}{4}}\cdot(\sqrt{3}+1)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right), \left(\frac{\sqrt{3}+1}{\sqrt{2}\sqrt[4]{3}}, -\frac{2^{\frac{1}{4}}\cdot(\sqrt{3}+1)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right),\right.$$
$$\left(-\frac{\sqrt{3}+1}{\sqrt{2}\sqrt[4]{3}}, \frac{i\cdot 2^{\frac{1}{4}}\cdot(\sqrt{3}+1)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right), \left(-\frac{\sqrt{3}+1}{\sqrt{2}\sqrt[4]{3}}, -\frac{i\cdot 2^{\frac{1}{4}}\cdot(\sqrt{3}+1)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right),$$
$$\left(i\frac{\sqrt{3}-1}{\sqrt{2}\sqrt[4]{3}}, \frac{i^{\frac{3}{2}}\cdot 2^{\frac{1}{4}}\cdot(\sqrt{3}-1)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right), \left(i\frac{\sqrt{3}-1}{\sqrt{2}\sqrt[4]{3}}, -\frac{i^{\frac{3}{2}}\cdot 2^{\frac{1}{4}}\cdot(\sqrt{3}-1)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right),$$
$$\left.\left(-i\frac{\sqrt{3}-1}{\sqrt{2}\sqrt[4]{3}}, \frac{i^{\frac{1}{2}}\cdot 2^{\frac{1}{4}}\cdot(\sqrt{3}-1)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right), \left(-i\frac{\sqrt{3}-1}{\sqrt{2}\sqrt[4]{3}}, -\frac{i^{\frac{1}{2}}\cdot 2^{\frac{1}{4}}\cdot(\sqrt{3}-1)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right)\right\}$$

By the same reasoning in the u_{1728} case we realize that the subgroups of order 3 of w_{1728} are

$$\left\langle\left(\frac{\sqrt{3}+1}{\sqrt{2}\sqrt[4]{3}}, \frac{2^{\frac{1}{4}}\cdot(\sqrt{3}+1)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right)\right\rangle = \left\{\left(\frac{\sqrt{3}+1}{\sqrt{2}\sqrt[4]{3}}, \frac{2^{\frac{1}{4}}\cdot(\sqrt{3}+1)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right), \left(\frac{\sqrt{3}+1}{\sqrt{2}\sqrt[4]{3}}, -\frac{2^{\frac{1}{4}}\cdot(\sqrt{3}+1)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right), \mathcal{O}_{w_{1728}}\right\}$$
$$\left\langle\left(-\frac{\sqrt{3}+1}{\sqrt{2}\sqrt[4]{3}}, \frac{i\cdot 2^{\frac{1}{4}}\cdot(\sqrt{3}+1)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right)\right\rangle = \left\{\left(-\frac{\sqrt{3}+1}{\sqrt{2}\sqrt[4]{3}}, \frac{i\cdot 2^{\frac{1}{4}}\cdot(\sqrt{3}+1)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right), \left(-\frac{\sqrt{3}+1}{\sqrt{2}\sqrt[4]{3}}, -\frac{i\cdot 2^{\frac{1}{4}}\cdot(\sqrt{3}+1)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right), \mathcal{O}_{w_{1728}}\right\}$$
$$\left\langle\left(i\frac{\sqrt{3}-1}{\sqrt{2}\sqrt[4]{3}}, \frac{i^{\frac{3}{2}}\cdot 2^{\frac{1}{4}}\cdot(\sqrt{3}-1)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right)\right\rangle = \left\{\left(i\frac{\sqrt{3}-1}{\sqrt{2}\sqrt[4]{3}}, \frac{i^{\frac{3}{2}}\cdot 2^{\frac{1}{4}}\cdot(\sqrt{3}-1)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right), \left(i\frac{\sqrt{3}-1}{\sqrt{2}\sqrt[4]{3}}, -\frac{i^{\frac{3}{2}}\cdot 2^{\frac{1}{4}}\cdot(\sqrt{3}-1)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right), \mathcal{O}_{w_{1728}}\right\}$$
$$\left\langle\left(-i\frac{\sqrt{3}-1}{\sqrt{2}\sqrt[4]{3}}, \frac{i^{\frac{1}{2}}\cdot 2^{\frac{1}{4}}\cdot(\sqrt{3}-1)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right)\right\rangle = \left\{\left(-i\frac{\sqrt{3}-1}{\sqrt{2}\sqrt[4]{3}}, \frac{i^{\frac{1}{2}}\cdot 2^{\frac{1}{4}}\cdot(\sqrt{3}-1)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right), \left(-i\frac{\sqrt{3}-1}{\sqrt{2}\sqrt[4]{3}}, -\frac{i^{\frac{1}{2}}\cdot 2^{\frac{1}{4}}\cdot(\sqrt{3}-1)^{\frac{1}{2}}}{3^{\frac{3}{8}}}\right), \mathcal{O}_{w_{1728}}\right\}$$

■

Lemma 1.6.45: The outgoing isogenies of w_{1728} do not fold.

Proof: By the same reasoning provided in the u_{1728} we conclude that the outgoing isogenies defined over $\mathbb{F}_p$ of w_{1728} are the ones with kernels

$$\left\langle \left(\frac{\sqrt{3}+1}{\sqrt{2}\sqrt[4]{3}}, \frac{2^{\frac{1}{4}} \cdot (\sqrt{3}+1)^{\frac{1}{2}}}{3^{\frac{3}{8}}} \right) \right\rangle \quad \text{and} \quad \left\langle \left(-\frac{\sqrt{3}+1}{\sqrt{2}\sqrt[4]{3}}, \frac{i \cdot 2^{\frac{1}{4}} \cdot (\sqrt{3}+1)^{\frac{1}{2}}}{3^{\frac{3}{8}}} \right) \right\rangle$$

Additionally, these isogenies are not equivalent over $\overline{\mathbb{F}_p}$, and thus they do not fold. ■

Theorem 1.6.46: The edge $e \in E(\mathcal{G}_3(\mathbb{F}_p))$ does not fold nor stack if and only if e is of the form $(1728, \mathbf{j})$ for some $\mathbf{j} \in \mathbb{F}_p$.

Proof: We know by [Arp+23, Lemma 3.10] that any isogeny that is not leaving an elliptic curve with j-invariant with value 0 or 1728 must fold or stack. Hence We know that if an isogeny does not fold or stack it must be leaving an elliptic curve with j-invariant 0 or 1728. By **Theorem 1.6.41** that the ougoing isogenies of u_0 and w_0 fold. Additionally by **Lemma 1.6.43** and **Lemma 1.6.45** we know that the outgoing isogenies of u_{1728} and w_{1728} do not fold. This proves the statement. ■

Lemma 1.6.47: $H_{20}(x)$ has a supersingular root in $\mathbb{F}_p$ if and only if $p = 5, 13, 17$ or $p \equiv 11, 19 \pmod{20}$

Proof: First let us find out when $H_{20}(x)$ has a root in $\mathbb{F}_p$, then when it has a supersingular root.

$\mathbb{F}_p$ root: Suppose $H_{20}(x) = 0 \Leftrightarrow x^2 - 1264000x - 681472000 = 0$. By the quadratic formula, we have

$$x = 632000 \pm 282880\sqrt{5}$$

Hence we know that x is a root in $\mathbb{F}_p$ if and only if $p|282880$ or $\left(\frac{5}{p}\right) = 1$.

Case 1: Suppose $p|282880 \Leftrightarrow p|\left(2^8 \cdot 5 \cdot 13 \cdot 17\right) \Leftrightarrow p = 2, 5, 13, 17$. However, since we have supposed $p > 3$ we exclude 2. Thus we know that $H_{20}(x)$ has a root in $\mathbb{F}_p$ if $p = 5, 13, 17$.

Case 2: Suppose $\left(\frac{5}{p}\right) = 1$. By **Lemma 1.6.20** we know that $\left(\frac{5}{p}\right) = 1 \Leftrightarrow p \equiv 1, 4 \pmod{5}$. Hence we know that $H_{20}(x)$ has a root in $\mathbb{F}_p$ if $p \equiv 1, 4 \pmod{5}$.

Putting our results together we conclude that $H_{20}(x)$ has a root in $\mathbb{F}_p$ if and only if $p = 5, 13, 17$ or $p \equiv 1, 4 \pmod{5}$.

Supersingular roots: Recall that we know $H_{20}(x)$ has a supersingular root if and only if $\left(\frac{-20}{p}\right) = -1$. By **Lemma 1.6.28** we know that for an odd prime not equal to 5 $\left(\frac{-20}{p}\right) = -1$ if and only if $p \equiv 11, 13, 17, 19 \pmod{20}$. Thus we conclude that $H_{20}(x)$ has a supersingular root if and only if $p \equiv 11, 13, 17, 19 \pmod{20}$.

Thus we know that $H_{20}(x)$ has a supersingular root in $\mathbb{F}_p$ if and only if $p = 5, 13, 17$ or $p \equiv 1, 4 \pmod{5}$, and $p \equiv 11, 13, 17, 19 \pmod{20}$. Note that $p = 13, 17$ satisfy the supersingularity condition. Further note that $H_{20}(x)$ has a root of 0 in $\mathbb{F}_p$ and we know 0 to be supersingular when $p = 5$. Hence we know that $H_{20}(x)$ does have a supersingular root in $\mathbb{F}_p$ if $p = 5, 13, 17$. Now, suppose $p \neq 5, 13, 17$, $p \equiv 1, 4 \pmod{5}$, and $p \equiv 11, 13, 17, 19 \pmod{20}$. Note that since $5|20$, we know that if $p \equiv \alpha \pmod{20}$, then $\alpha \equiv 1, 4 \pmod{5}$ must be true. However, this holds for $p \equiv 11, 19 \pmod{20}$, but does not not hold for $p \equiv 13, 17 \pmod{20}$.

Thus we conclude that $H_{20}(x)$ has a supersingular root in $\mathbb{F}_p$ if and only if $p = 13, 17$ or $p \equiv 11, 19 \pmod{20}$. Thus we have proved the statement. ■

Lemma 1.6.48: $H_{32}(x)$ has a supersingular root in $\mathbb{F}_p$ if and only if $p = 5, 13, 29$ or $p \equiv 7 \pmod 8$.

Proof: First let us show when $H_{23}(x)$ has a root in $\mathbb{F}_p$, then when it has a supersingular root.

$\mathbb{F}_p$ root: Consider $H_{32}(x) = 0 \Leftrightarrow x^2 - 52250000x + 12167000000 = 0$. By the quadratic formula this results in

$$x = 26125000 \pm 18473000\sqrt{2}$$

Hence we know that x is a value in $\mathbb{F}_p$ if and only if $p|18473000$ or $\left(\frac{2}{p}\right) = 1$.

Case 1: Suppose that $p|18473000 \Leftrightarrow p|\left(2^3 \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 29\right) \Leftrightarrow p = 2, 5, 7, 13, 29$. Since we suppose $p > 3$ we exclude $p = 2$. Hence we know that $H_{32}(x)$ has a root in $\mathbb{F}_p$ if $p = 5, 7, 13, 29$.

Case 2: Suppose $\left(\frac{2}{p}\right) = 1$. By **Lemma 1.6.25** we know that for an odd prime $\left(\frac{2}{p}\right) = 1 \Leftrightarrow p \equiv 1, 7 \pmod 8$. Hence we know that $H_{32}(x)$ has a root in $\mathbb{F}_p$ if $p \equiv 1, 7 \pmod 8$.

Thus we conclude that $H_{32}(x)$ has a root in $\mathbb{F}_p$ if and only if $p = 5, 13, 29$ or $p \equiv 7 \pmod 8$.

Supersingular root: Recall that we know $H_{32}(x)$ has a supersingular root if and only if $\left(\frac{-32}{p}\right) = -1$. Hence we know by **Lemma 1.6.29** that $\left(\frac{-32}{p}\right) = -1$ if and only if $p \equiv 5, 7 \pmod 8$. Hence we know that $H_{32}(x)$ has a supersingular root if and only if $p \equiv 5, 7 \pmod 8$

Combining our condition for $H_{32}(x)$ having a root in $\mathbb{F}_p$ and a root in $\mathbb{F}_p$ and a supersingular root, we find that $H_{32}(x)$ has a supersingular root in $\mathbb{F}_p$ if and only if $p = 5, 13, 29$ or $p \equiv 7 \pmod 8$. Hence we have proved the statement. ■

Lemma 1.6.49: $H_{35}(x)$ has a supersingular root in $\mathbb{F}_p$ if and only if $p = 5, 7, 23$ or $p \equiv 6, 19, 24, 26, 31, 34 \pmod{35}$

Proof: Let us first find out when $H_{35}(x)$ has a root in $\mathbb{F}_p$, then find when $H_{35}(x)$ has a supersingular root.

$\mathbb{F}_p$ root: Suppose $H_{35}(x) = 0 \Leftrightarrow x^2 + 117964800x - 134217728000 = 0$. By the quadratic formula we arrive at the value

$$x = -58982400 \pm 26378240\sqrt{5}$$

Hence we know that x is a root in $\mathbb{F}_p$ if and only if $p|26378240$ or $\left(\frac{5}{p}\right) = 1$.

Case 1: Suppose $p|26378240 \Leftrightarrow p|\left(2^{15} \cdot 5 \cdot 7 \cdot 23\right) \Leftrightarrow p = 2, 5, 7, 23$. By our supposition that $p > 3$ we exclude 2. Hence we know that $H_{35}(x)$ has a root in $\mathbb{F}_p$ if $p = 5, 7, 23$.

Case 2: Suppose $\left(\frac{5}{p}\right) = 1$. By **Lemma 1.6.20** we know that this supposition is true if and only if $p \equiv 1, 4 \pmod 5$.

Putting our cases together, we conclude that $H_{35}(x)$ has a supersingular root if and only if $p = 5, 7, 23$ or $p \equiv 1, 4 \pmod 5$

Supersingular root: Recall that $H_{35}(x)$ has a supersingular root if and only if $\left(\frac{-35}{p}\right) = -1$. By **Lemma 1.6.30** we know that for a prime p such that $p \neq 2, 5, 7$, $\left(\frac{-35}{p}\right) = -1$ if and only if $p \equiv 2, 6, 8, 18, 19, 22, 23, 24, 26, 31, 32, 34 \pmod{35}$. Thus we conclude that $H_{35}(x)$ has a supersingular root if and only if $p \equiv 2, 6, 8, 18, 19, 22, 23, 24, 26, 31, 32, 34 \pmod{35}$.

Putting the conditions together we see that $H_{35}(x)$ has a supersingular root in $\mathbb{F}_p$ if and only if $p = 5,7,23$ or $p \equiv 1,4 \pmod 5$ and $p \equiv 2,6,8,18,19,22,23,24,26,31,32,34 \pmod{35}$ for $p \neq 5,7$. In $\mathbb{F}_5$, $H_{35}(x) = x^2$ which has a supersingular root 0, and in $\mathbb{F}_7$, $H_{35}(x) = (x-6)^2$ which has supersingular root 6. On the other hand if $p = 23$, then we see that the condition for a root in $\mathbb{F}_p$ and the condition for supersingular root are satisfied, hence we have a supersingular root in $\mathbb{F}_p$ when $p = 23$. Now suppose $p \neq 5,7,23$. Note that $5|35$, hence we know that if $p \equiv \alpha \pmod{35}$ then $\alpha \equiv 1,4 \pmod 5$. However, $p \equiv 2,8,18,22,32 \pmod{35}$ fail this condition.

Hence we conclude that $H_{35}(x)$ has a supersingular root in $\mathbb{F}_p$ if and only if $p = 5,7,23$ or $p \equiv 6,19,24,26,31,34 \pmod{35}$ which proves the statement. ■

Lemma 1.6.50: Let $p > 3$ be a prime. Then

(a) $H_{20}(x)$ has a supersingular root of Value
   i. 0 if and only if $p = 5,11$,
   ii. 1728 if and only if $p = 11,19$,
   iii. 8000 if and only if $p = 5,13,31$,
   iv. -32768 if and only if $p = 11,13,17,19$,
   v. 54000 if and only if $p = 5,11,17,59$.

(b) $H_{32}(x)$ has a supersingular root of Value
   i. 0 if and only if $p = 5,23$,
   ii. 1728 if and only if $p = 7,23,31$,
   iii. 8000 if and only if $p = 5,7,13$,
   iv. -32768 if and only if $p = 7,13,29,79$,
   v. 54000 if and only if $p = 5,29,47,71$.

(c) $H_{35}(x)$ has a supersingular root of Value
   i. 0 if and only if $p = 5$,
   ii. 1728 if and only if $p = 7,19,31$,
   iii. 8000 if and only if $p = 5,7,23,61$,
   iv. -32768 if and only if $p = 7,19$,
   v. 54000 if and only if $p = 5,23,41,89,101$.

(d) $H_{20}(x)$ and $H_{32}(x)$ share at least one root in $\mathbb{F}_p$ if and only if $p = 5,13,79,151$.

(e) $H_{20}(x)$ and $H_{35}(x)$ share at least one root in $\mathbb{F}_p$ if and only if $p = 5,19,31,139$.

(f) $H_{32}(x)$ and $H_{35}(x)$ share at least one root in $\mathbb{F}_p$ if and only if $p = 5,7,31,199,271$.

(g) $H_{20}(x)$, $H_{32}(x)$, and $H_{35}(x)$ share at least one root in $\mathbb{F}_p$ if and only if $p = 5$

Proof: Note that for statements (a), (b), and (c) we simply have to plug in the appropriate value $x_0 \in \{0,1728,8000,-32768,54000\}$ into each Hilbert Class Polynomial $H_r(x)$ for $r \in \{20,32,35\}$, then see which primes p divide $H_r(x_0)$ while excluding $p = 2,3$. These steps are shown in Table 8.

We can see that the values in the 5-th column of Table 8 match the ones stated within the lemma, hence we know that sections (a), (b), and (c) are proved. Thus let us prove the remaining sections.

$H_r(x)$	x_0	$H_r(x_0)$	$H_r(x_0)$ factored	Valid p
$H_{20}(x)$	0	-681472000	$-1\cdot 2^{12}\cdot 5^3\cdot 11^3$	$5,11$
	1728	-2862678016	$-1\cdot 2^{16}\cdot 11^2\cdot 19^2$	$11,19$
	8000	-10729472000	$-1\cdot 2^{14}\cdot 5^3\cdot 13^2\cdot 31$	$5,13,31$
	-32768	41811021824	$2^{12}\cdot 11\cdot 13^2\cdot 17^2\cdot 19$	$11,13,17,19$
	54000	-66021472000	$-1\cdot 2^8\cdot 5^3\cdot 11^2\cdot 17^2\cdot 59$	$5,11,17,59$
$H_{32}(x)$	0	12167000000	$2^6\cdot 5^6\cdot 23^3$	$5,23$
	1728	-78118014016	$-1\cdot 2^6\cdot 7^4\cdot 23^2\cdot 31^2$	$7,23,31$
	8000	-405769000000	$-1\cdot 2^6\cdot 5^6\cdot 7^4\cdot 13^2$	$5,7,13$
	-32768	1725368741824	$2^6\cdot 7^4\cdot 13^2\cdot 29^2\cdot 79$	$7,13,29,79$
	54000	-2806417000000	$-1\cdot 2^6\cdot 5^6\cdot 29^2\cdot 47\cdot 71$	$5,29,47,71$
$H_{35}(x)$	0	-134217728000	$-1\cdot 2^{30}\cdot 5^3$	5
	1728	69628432384	$2^{12}\cdot 7^2\cdot 19^2\cdot 31^2$	$7,19,31$
	8000	809564672000	$2^{12}\cdot 5^3\cdot 7^2\cdot 23^2\cdot 61$	$5,7,23,61$
	-32768	-3998614552576	$-1\cdot 2^{32}\cdot 7^2\cdot 19$	$7,19$
	54000	6238797472000	$2^8\cdot 5^3\cdot 23^2\cdot 41\cdot 89\cdot 101$	$5,23,41,89,101$

Table 8: Finding when $H_{20}(x)$, $H_{32}(x)$, and $H_{35}(x)$ have special roots.

(d): Suppose we have the following system of equations:

$$\begin{cases} 0 = H_{20}(x) \\ 0 = H_{32}(x) \end{cases} \iff \begin{cases} 0 = x^2 - 1264000x - 681472000 \\ 0 = x^2 - 52250000x + 12167000000 \end{cases}$$

By the quadratic formula we have

$$\begin{cases} x = 632000 \pm 282880\sqrt{5} \\ x = 26125000 \pm 18473000\sqrt{2} \end{cases}$$

Hence we have the following:

$$\begin{aligned}
26125000 \pm 18473000\sqrt{2} &= 632000 \pm 282880\sqrt{5} \\
\pm 18473000\sqrt{2} &= -25493000 \pm 282880\sqrt{5} \\
682503458000000 &= 650293154472000 \pm 14422919680000\sqrt{5} \\
32210303528000 &= \pm 14422919680000\sqrt{5} \\
1037503653365889246784000000 &= 1040103060478656512000000000 \\
0 &= 259940711276726521600000 0 \\
0 &= 2^{12} \cdot 5^6 \cdot 13^4 \cdot 31 \cdot 37^2 \cdot 53^2 \cdot 79 \cdot 151
\end{aligned}$$

Looking at our original system of equations modulo 5, 13, 31, 37, 53, 79, and 151, we see that they all result in at least one solution, but $p = 5, 13, 79$, and 151 are the only primes which result in a shared root in $\mathbb{F}_p$. This proves this section of the lemma.

(e): Suppose we have the following system of equations:

$$\begin{cases} 0 = H_{20}(x) \\ 0 = H_{35}(x) \end{cases} \iff \begin{cases} 0 = x^2 - 1264000x - 681472000 \\ 0 = x^2 + 117964800x - 134217728000 \end{cases}$$

By the quadratic formula we have

$$\begin{cases} x = 632000 \pm 282880\sqrt{5} \\ x = -58982400 \pm 26378240\sqrt{5} \end{cases}$$

Hence we have the following:

$$\begin{aligned}
&\Leftrightarrow 632000 \pm 282880\sqrt{5} = -58982400 \pm 26378240\sqrt{5} \\
&\Leftrightarrow 59614400 \pm 282880\sqrt{5} = \pm 26378240\sqrt{5} \\
&\Leftrightarrow \begin{cases} 59614400 + 282880\sqrt{5} = 26378240\sqrt{5} \\ 59614400 + 282880\sqrt{5} = -26378240\sqrt{5} \\ 59614400 - 282880\sqrt{5} = 26378240\sqrt{5} \\ 59614400 - 282880\sqrt{5} = -26378240\sqrt{5} \end{cases} \\
&\Leftrightarrow \begin{cases} 59614400 = 26095360\sqrt{5} \\ 59614400 = -26661120\sqrt{5} \\ 59614400 = 26661120\sqrt{5} \\ 59614400 = -26095360\sqrt{5} \end{cases} \\
&\Leftrightarrow \begin{cases} 59614400 = \pm 26095360\sqrt{5} \\ 59614400 = \pm 26661120\sqrt{5} \end{cases} \\
&\Leftrightarrow \begin{cases} 3553876687360000 = 3404839067648000 \\ 3553876687360000 = 3554076598272000 \end{cases} \\
&\Leftrightarrow \begin{cases} 0 = 149037619712000 \\ 0 = 199910912000 \end{cases} \\
&\Leftrightarrow \begin{cases} 0 = 2^{12} \cdot 5^3 \cdot 19^3 \cdot 31 \cdot 37^2 \\ 0 = 2^{12} \cdot 5^3 \cdot 53^2 \cdot 139 \end{cases}
\end{aligned}$$

Checking the original system of equations for $p = 5, 19, 31, 37, 53$, and 139, we see that all of these cases result in $H_{20}(x)$ and $H_{35}(x)$ sharing at least one root, however, $p = 5, 19, 31$, and 139 result in the system having at least one solution in $\mathbb{F}_p$.

(f): Suppose we have the following system of equations:

$$\begin{cases} 0 = H_{32}(x) \\ 0 = H_{35}(x) \end{cases} \iff \begin{cases} 0 = x^2 - 52250000x + 12167000000 \\ 0 = x^2 + 117964800x - 134217728000 \end{cases}$$

By the quadratic formula we have

$$\begin{cases} x = 26125000 \pm 18473000\sqrt{2} \\ x = 632000 \pm 282880\sqrt{5} \end{cases}$$

Hence we have the following:

$$\begin{aligned} 26125000 \pm 18473000\sqrt{2} &= 632000 \pm 282880\sqrt{5} \\ 85107400 \pm 18473000\sqrt{2} &= \pm 282880\sqrt{5} \\ 7925772992760000 + 3144378000400000\sqrt{2} &= 3479057727488000 \\ 3144378000400000\sqrt{2} &= -4446715265272000 \\ 19774226018799004800320000000000 &= 19773276650403033329233984000000 \\ 0 &= 949368395971471086016000000 \\ 0 &= 2^{12} \cdot 5^6 \cdot 7^4 \cdot 31^3 \cdot 37^2 \cdot 53^2 \cdot 199 \cdot 271 \end{aligned}$$

Checking the original system of equations for $p = 5, 7, 31, 37, 53, 199$, and 271, we see that all of these cases result in $H_{32}(x)$ and $H_{35}(x)$ sharing at least one root, however, $p = 5, 7, 31, 199$, and 271 result in the system having at least one solution in $\mathbb{F}_p$.

(g): Using the results in cases (d), (e), and (f), we see that the only potential time that all three $H_{20}(x)$, $H_{32}(x)$, $H_{35}(x)$ share a root is when $p = 5$, and this results in all three equations being x^2 which implies that they all have the same root.

Hence we see that we have covered every case of this lemma. Thus the lemma is proved true. ■

Lemma 1.6.51: Suppose $\ell = 3$ and $p > 3$. The following holds true:

(a) if $p = 5, 7, 13$, then 8000 has exactly four loops in $\mathcal{S}_\ell^p$

(b) if $p = 31, 61$, then 8000 has a new edge to a distinct vertex and two new loops in $\mathcal{S}_\ell^p$

(c) if $p \equiv 5, 7 \pmod 8$ and $p \neq 5, 7, 13, 31, 61$, then 8000 has two new loops and no other new edges.

Proof: Suppose that Ω implies a new edge $(8000, j)$ when $\Gamma(\mathcal{G}_3(\mathbb{F}_p))$, $p > 3$, is inputted. then either

1. $j = 0$
2. $j = 1728$
3. $(8000, j)$ is a multi-edge

This follows from **Theorem 1.6.5**. Let us explore when each case happens. To be able to do so, we need to recall that

$$\Phi_3(8000,x) = (x-8000)^2\left(x^2 - 377674768000x + 232381513792000000\right)$$

For convenience sake, let $A(x) = x^2 - 377674768000x + 232381513792000000$

Case 1: Suppose that there exists an edge of the form $(8000,0)$ in $\mathcal{S}_3^p$. By the definition of the modular polynomial, we know that this implies $\Phi_3(8000,0) = 0$. By this we we know that either $(800 - 0) = 8000 = 0$ or $A(0) = 0$.

Case 1.1 Suppose $8000 = 0$, this is only possible if and only if $p|8000 \Leftrightarrow p|\left(2^6 \cdot 5^3\right) \Leftrightarrow p = 2,5$. However, by our supposition that $p > 3$ we conclude that $(8000,0)$ is an edge in this case if and only if $p = 5$.

Case 1.2 Suppose $A(0) = 0 \Leftrightarrow 232381513792000000 = 0$. This is only possible if and only if $p|232381513792000000 \Leftrightarrow p|\left(2^{12} \cdot 5^6 \cdot 29^3 \cdot 53^3\right) \Leftrightarrow p = 2,5,29,53$. Similar to the last case, our supposition that $p > 3$ implies that $(8000,0)$ is an edge in this case if and only if $p = 5,29,53$

Hence $(8000,0)$ is an edge in $\mathcal{S}_3^p$ if and only if $p = 5,29,53$. Computing $\mathcal{G}_3(\mathbb{F}_p)$, $\mathcal{S}_3^p$ and comparing the two graphs, we see that for $p = 29$ and 53, the edge $(8000,0)$ is not new. Hence $p = 5$ is the only case where there is a new edge of the form $(8000,0)$. In computing $\mathcal{S}_3^p$ we also see that this new edge is a loop, resulting in there existing 4 loops on 8000.

Case 2: Suppose that there exists an edge of the $(8000,1728)$ in $\mathcal{S}_3^p$. By definition of the modular polynomial, we know that this implies $\Phi_3(8000,1728) = 0$. By this we know that either $(8000 - 1728) = 0 \Leftrightarrow 6272 = 0$ or $A(1728) = 0$.

Case 2.1 Suppose $6272 = 0$. This is only possible if and only if $p|6272 \Leftrightarrow p|\left(2^7 \cdot 7^2\right) \Leftrightarrow p = 2,7$. Similar to previous cases, we exclude $p = 2$ and are left with only $p = 7$.

Case 2.2 Suppose $A(1728) = 0 \Leftrightarrow 231728891795881984 = 0$. We know that this is possible if and only if $p|231728891795881984 \Leftrightarrow p|\left(2^{14} \cdot 7^4 \cdot 23^2 \cdot 47^2 \cdot 71^2\right) \Leftrightarrow p = 2,7,23,47,71$. Again, we exclude $p = 2$ and are left with $p = 7,23,47,71$.

Hence $(8000,1728)$ is an edge in $\mathcal{S}_3^p$ if and only if $p = 7,23,47,71$. Computing $\mathcal{G}_3(\mathbb{F}_p)$, $\mathcal{S}_3^p$, and comparing the two graphs, we see that for $p = 23,47,71$ the edge $(8000,1728)$ is not a new edge. Hence $p = 7$ is the only case where there is a new edge of the form $(8000,1728)$. Furthermore, in our calculations, we see that this edge is a loop, resulting in 4 loops on 8000.

Case 3: Suppose $(8000,j)$ is a multi edge. This implies that $\Phi_3(8000,j)$ has a root of multiplicity 2. By the structure of $\Phi_3(8000,j)$ this means that either $j = 8000$ or $A(x)$ is a square. Note that when $j = 8000$, then the edge $(8000,j)$ is a loop. Now, let us consider the other case. Note that

$$A(x) = 0 \Leftrightarrow x = 188837384000 \pm 77092288000\sqrt{6}$$

Hence we know that $A(x)$ is a square if and only if $p|77092288000$ or $p|\sqrt{6}$. In the first case $p|77092288000 \Leftrightarrow p|\left(2^9 \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 31 \cdot 61\right) \Leftrightarrow p = 2,5,7,13,31,61$. In the second case $p|sqrt6 \Leftrightarrow p|6 \Leftrightarrow p|(2 \cdot 3) \Leftrightarrow p = 2,3$. Hence we know that there is a multi-edge between 8000 and j if $j = 8000$ or $p = 5,7,13,31,61$, since $p > 3$. By computing $\mathcal{G}_3(\mathbb{F}_p)$, $\mathcal{S}_3^p$, and comparing the two graphs, we see that all of these p values result in a new edge. Furthermore, the edges in the case $p = 5,7,13$ are new loops (resulting in 4 loops on 8000), whereas the edges for $p = 31,61$ are new edges to distinct vertices.

Thus we see that if $p = 5,7,13$ then 8000 has 4 loops in $\mathcal{S}_3^p$, if 8000 is supersingular and $p \neq 5,7,13,31,61$, then 8000 has exactly two loops and no new edges, and if $p = 31,61$, then 8000 has a new (double) edge to a distinct vertex. ■

Lemma 1.6.52: Θ always adds a new edge incident to 0 when inputted $\Gamma(\mathcal{G}_3(\mathbb{F}_p))$, so long as 0 is supersingular. However, this new edge is also incident to a vertex 0 was adjacent to in $\Gamma(\mathcal{G}_3(\mathbb{F}_p))$.

Proof: Note that

$$\Phi_3(0,x) = x(x+12288000)^3$$

However, we know by **Theorem 1.4.4** that u_0 is either incident to no edges or to 2 out-edges. Hence we know that there must be a new edge added by Θ, so long as 0 is supersingular.

Recall that we know the edge (u_0, w_0) is defined over $\mathbb{F}_p$ hence we know that 0 has a loop in $\Gamma(\mathcal{G}_3(\mathbb{F}_p))$. Furthermore, we know that there are edges $(u_0, u_{-12288000})$ and $(w_0, w_{-12288000})$ in $\mathcal{G}_3(\mathbb{F}_p)$ when 0 is supersingular. Thus we know that there is an edge of the form $(0,-12288000)$ in $\Gamma(\mathcal{G}_3(\mathbb{F}_p))$. Note that if Θ were to add an edge incident to 0, then that edge must also be incident to 0 (forming a loop), or -12288000. However, since these edges already exist in $\Gamma(\mathcal{G}_3(\mathbb{F}_p))$ we know that the edge Θ is adding is incident to a vertex which 0 was already adjacent to in $\Gamma(\mathcal{G}_3(\mathbb{F}_p))$. Thus prooving the statement. ■

Lemma 1.6.53: 1728 is incident to a new edge if and only if $p = 7,19,31$.

Proof: Suppose $p \equiv 2 \pmod 3$. In this case, we know that $\left(\frac{-p}{3}\right) = 1$ and hence there are edges in $\mathcal{G}_3(\mathbb{F}_p)$. Note that by **Theorem 1.4.4** we know that ${}_+d_{u_{1728}}(\mathcal{G}_3(\mathbb{F}_p)) = {}_+d_{w_{1728}}(\mathcal{G}_3(\mathbb{F}_p)) = 2$. Furthermore, we know that the out-edges of 1728 do not fold by **Theorem 1.6.46**, hence we know that ${}_+d_{1728}(\Gamma(\mathcal{G}_3(\mathbb{F}_p))) = 4$. Which is the maximum out-degree of any vertex in $\mathcal{G}_3(\overline{\mathbb{F}_p})$. Hence we know that no new edges can be added by Θ that are incident to 1728.

On the other hand, suppose now that $p \equiv 1 \pmod 3$. In this case, we know that $\left(\frac{-p}{3}\right) = -1$ and hence there are no edges in $\mathcal{G}_3(\mathbb{F}_p)$ by **Theorem 1.4.4**. Thus, if there are any supersingular roots of $\Phi_3(1728,x)$ that are in $\mathbb{F}_p$, then 1728 has a new edge induced by Θ. Note that

$$\Phi_3(1728,x) = (x^2 - 153542016x - 1790957481984)^2$$

Let $A(x) = x^2 - 153542016x - 1790957481984$. We would like to know when $A(x)$ has roots in $\mathbb{F}_p$ that are supersingular. Let us find out when each happens.

$\mathbb{F}_p$ roots: Suppose $A(x) = 0$. By the quadratic formula we arrive at a solution

$$x = 76771008 \pm 44330496\sqrt{3}$$

Hence we know that x is a value in $\mathbb{F}_p$ if and only if $p|44330496$ or $\left(\frac{3}{p}\right) = 1$.

Case 1: Suppose $p|44330496 \Leftrightarrow p|\left(2^9 \cdot 3 \cdot 7^2 \cdot 19 \cdot 31\right) \Leftrightarrow p = 2,3,7,19,31$. From our supposition that $p > 3$ we exclude $p = 2,3$. Hence we know $A(x)$ has a root in $\mathbb{F}_p$ if $p = 7,19,31$.

Case 2: Suppose $\left(\frac{3}{p}\right) = 1$. By **Lemma 1.6.19** we know that $\left(\frac{3}{p}\right) = 1$ if and only if $p \equiv 1,11 \pmod{12}$.

Putting the two cases together we see that $A(x)$ has a root in $\mathbb{F}_p$ if and only if $p = 7, 19, 31$ or $p \equiv 1, 11 \pmod{12}$. Additionally, adding our supposition that $p \equiv 1 \pmod 3$ we in fact get rid of $p \equiv 11 \pmod{12}$. Thus we conclude that in this case $A(x)$ has a root in $\mathbb{F}_p$ if and only if $p \equiv 1 \pmod{12}$ or $p = 7, 19, 31$.

Supersingular root: Note that if $A(x) = H_{36}(x)$ which we know to have a supersingular root if and only if $\left(\frac{-36}{p}\right) = -1$. By **Lemma 1.6.31** we know that $\left(\frac{-36}{p}\right) = -1$ if and only if $p \equiv 3 \pmod 4$. Combining this condition with our supposition that $p \equiv 1 \pmod 3$, we see that 1728 has a new edge if $p \equiv 7 \pmod{12}$.

Putting our two conditions together we see that $A(x)$ has a supersingular root in $\mathbb{F}_p$ if and only if $p \equiv 7 \pmod{12}$, and $p \equiv 1 \pmod{12}$ or $p = 7, 19, 31$. This is only possible if $p = 7, 19, 31$. Hence these are the only times that $A(x)$ has a supersingular root in $\mathbb{F}_p$ while $\left(\frac{-p}{3}\right) = -1$.

Thus we conclude that the only time 1728 is incident to a new edge is when $p = 7, 19, 31$. ■

Lemma 1.6.54: Suppose $\ell = 3$ and $p > 3$. Then the following hold true:

(a) If $p = 7, 13$, then -32768 has 4 new loops added by Ω,

(b) If $p = 11$, then -32768 has 2 loops that are *not* new and two out-edges to distinct vertices that are also not new.

(c) If $p = 19, 79$, then -32768 has two new loops and a new edge to a distinct vertex.

(d) If $p \equiv 2, 6, 7, 8, 10 \pmod{11}$ and $p \neq 7, 13, 19, 79$, then -32768 has exactly two new loops and no other new edges.

Proof: Suppose $\ell = 3$ and $p > 3$. Note that if $(-32768, j)$ is a new edge then we know that one of the following must hold:

1. $j = 0$,
2. $j = 1728$,
3. $(-32768, j)$ is a multi-edge.

Before we explore each case, notice that

$$\Phi_3(-32768, x) = (x + 32768)^2(x^2 + 37616060956672x - 56171326053810176)$$

Let $A(X) = x^2 + 37616060956672x - 56171326053810176$ for convenience sake.

Case 1: Suppose $\Phi_3(-32768, 0) = 0$. Then we know that $32768 = 0$ or $A(0) = 0$.

Case 1.1: Suppose $32768 = 0$. We know that this is only possible if and only if $p | 32769 \Leftrightarrow p | (2^{15}) \Leftrightarrow p = 2$. We know this to be a contradiction to our supposition of $p > 3$, hence we know that this case cannot happen.

Case 1.2: Suppose $A(0) = 0 \Leftrightarrow -56171326053810176 = 0 \Leftrightarrow p | 56171326053810176 \Leftrightarrow p | (2^{33} \cdot 11^3 \cdot 17^2)$ $\Leftrightarrow p = 2, 11, 17$. By our supposition $p > 3$ we exclude $p = 2$. Hence we know that $A(x) = 0$ if and only if $p = 11, 17$ 17 has new loops. By computing $\mathcal{G}_3(\mathbb{F}_p)$, $\mathcal{S}_3^p$ and comparing the two graphs for $p = 11, 17$ we see that $p = 11$ results in -32768 having two loops and two out-edges in $\mathcal{S}_2^p$, however, none of these are new edges. On the other hand $p = 17$ results in -32768 having two new loops added to it by Ω.

Thus we conclude that there are no cases where $(-32768, 0)$ is a new edge. However, we do know that when $p = 11$, -32768 has two loops in $\mathcal{S}_3^p$ that are not new, and two out-edges to 0 that are also not new. Furthermore, we know that when $p = 17$, -32768 has two new loops in $\mathcal{S}_3^p$, and an edge to 0 that is not new.

Case 2: Suppose $\Phi_3(-32768, 1728) = 0$. Then we know that $1728 + 32768 = 34496 = 0$ or $A(1728) = 0$.

Case 2.1: Suppose $34496 = 0$. We know this to be true if and only if $p|34496 \Leftrightarrow p|\left(2^6 \cdot 7^2 \cdot 11\right) \Leftrightarrow p = 2, 7, 11$. Similar to previous cases, we exclude $p = 2$. Thus we know that there is an edge of the form $(-32768, 1728)$ if $p = 7, 11$. By computing $\mathcal{G}_3(\mathbb{F}_p)$, $\mathcal{S}_3^p$ and comparing the two graphs for $p = 7, 11$, we see that $p = 7$ is the only case that has a new edge of the form $(-32768, 1728)$. This new edge is a double-loop.

Case 2.2: Suppose $A(1728) = 0 \Leftrightarrow p|8829227282305024 \Leftrightarrow p|\left(2^{12} \cdot 7^4 \cdot 19^4 \cdot 83^2\right) \Leftrightarrow p = 2, 7, 19, 83$. Again, we exclude $p = 2$. We already know that $p = 7$ results in two new loops. By computing $\mathcal{G}_3(\mathbb{F}_p)$, $\mathcal{S}_3^p$, and comparing the two graphs for $p = 19, 83$, we see that for $p = 19$ results in -32768 getting two new loops and two new edges to a distinct vertex by Ω. Furthermore, we see that for $p = 83$, -32768 gets two new loops and is incident to two distinct vertices via edges that are not new.

Thus we conclude that $(-32768, 1728)$ is a new edge if and only if $p = 7, 19$. Otherwise, we know that for $p = 11, 83$ the edge $(-32768, 1728)$ is not new, but we know that for $p = 83$, -32768 gets two new loops.

Case 3: Suppose $(-32768, j)$ is a multi-edge. By this supposition, we know that $\Phi_3(-32768, x)$ has a root of multiplicity 2. By the structure of $\Phi_3(-32768, x)$ which we provided before, we see that $\Phi_3(-32768, x)$ has a root of multiplicity 2 if and only if $(x + 32768)$ has a supersingular root in $\mathbb{F}_p$ or $A(x)$ has a supersingular root in $\mathbb{F}_p$ of multiplicity 2. Let us explore each case.

Case 3.1: We wish to find when $(x + 32768)$ has a supersingular root in $\mathbb{F}_p$. $(x + 32768)$ always has a root in $\mathbb{F}_p$, which has a value -32768, however, we need to find out when this value is supersingular. Note that $(x + 32768) = H_{11}(x)$, and we know when a Hilbert class polynomial has a supersingular root. Hence we know that $(x + 32768)$ has a supersingular root if and only if $\left(\frac{-11}{p}\right) = -1$. By **Lemma 1.6.27** we conclude that for an odd prime p not equal to 11, $(x + 32768)$ has a supersingular root in $\mathbb{F}_p$ if and only if $p \equiv 2, 6, 7, 8, 10 \pmod{11}$. For the case where $p = 11$ we see that $(x + 32768) = (x + 10)$ which has a root of 1. In the case where $p = 11$ we know 1 to be supersingular. Hence we know that this is an additional case where $(x + 32768)$ has a supersingular root in $\mathbb{F}_p$.

Case 3.2: In this case we wish to find when $A(x)$ has a supersingular root in $\mathbb{F}_p$ of multiplicity 2.

Supersingular root: Note that $A(x) = H_{99}(x)$. Hence we know that $A(x)$ has a supersingular root if and only if $\left(\frac{-99}{p}\right) = -1$. By **Lemma 1.6.32** we know that for an odd prime p not equal to 11, $A(x)$ has a supersingular root if and only if $p \equiv 2, 6, 7, 8, 10 \pmod{11}$. For when $p = 11$ we can explicitly see that $A(x) = x^2$ in $\mathbb{F}_{11}$, and we know 0 to be supersingular in this case.

$\mathbb{F}_p$ root (mult. 2): Consider $A(x) = 0$. By the quadratic formula, we get

$$x = -18808030478336 \pm 3274057859072\sqrt{33}$$

Note that $A(x)$ has a root in $\mathbb{F}_p$ of multiplicity 2 if and only if $p|3274057859072$ or $p|\sqrt{33}$. The latter case results in $p = 3, 11$, and since we have suppose $p > 3$ we exclude 3, and hence $p = 11$ is a valid case. In Former case we have $p|3274057859072 \Leftrightarrow$

$p|\left(2^{14}\cdot 7^2\cdot 11\cdot 13\cdot 19^2\cdot 79\right) \Leftrightarrow p=2,7,11,13,19,79$. Similar to the previous case we exclude $p=2$. Hence we know that $A(x)$ has a root in $\mathbb{F}_p$ of multiplicity 2 if and only if $p=7,11,13,19,79$.

Putting the two conditions together we see that $A(x)$ has a supersingular root in $\mathbb{F}_p$ of multiplicity 2 if and only if $p=7,11,13,19,79$ or $p\equiv 2,6,7,8,10 \pmod{11}$. Note that -32768 always has at least two loops, as seen from the structure of $\Phi_3(-32768,x)$. Hence the only new edges that are incident to distinct edges come from Case 3.2. However, for $p=7,13$, we know that there is only one vertex by **Theorem 1.6.7**, and hence the edges implied by this case are loops. In other words, for $p=7,13$, -32768 has four loops. In the case where $p=11$, $1728=-32768$, and hence we know that the edges ${}_+E_{-32768}(\mathcal{G}_3(\mathbb{F}_p))$ do not fold by **Theorem 1.6.46**, and hence the implied multi-edge is not a new edge implemented by Θ. Thus the only cases left are $p=19,79$, and by computing $\mathcal{G}_3(\mathbb{F}_p)$, $\mathcal{S}_3^p$ and comparing the two graphs we see that indeed, when $p=19,79$, -32768 becomes incident to a new edge which going to a distinct vertex.

Note that we have shown that for $p=7,13$, -32768 becomes incident to four new loops. When $p=11$ no new edges are added to -32768 even though $\mathcal{S}_\ell^p$ has two loops on -32768. Furthermore, we have shown that when $p=19,79$, then -32768 is incident to a new edge going to a distinct vertex and two new loops. Lastly, we have shown that when $p=17,83$ or $p\equiv 2,6,7,8,10 \pmod{11}$, which is equivalent to $p\equiv 2,6,7,8,10 \pmod{11}$, then -32768 gets two new loops, and no new outgoing edges which go to distinct vertices. Thus we have proved the statement. ■

Definition 1.6.55: For the rest of this section let us use the following notation for these special polynomials

$$\begin{aligned}
R_{3,1}(x) &= x\\
R_{3,2}(x) &= x-8000\\
R_{3,3}(x) &= x-1728\\
R_{3,4}(x) &= x+32768\\
R_{3,5}(x) &= x^2-52250000x+12167000000\\
R_{3,6}(x) &= x^2-1264000x-681472000\\
R_{3,7}(x) &= x^2+117964800x-134217728000
\end{aligned}$$

The reason that these polynomials are special is due to the fact that

$$\mathcal{R}e_{\mathcal{S}_3}(x) = -27\prod_{n=1}^{7}(R_{3,n}(x))^2$$

Corollary 1.6.56: The following statements stand true:

(a) If $R_{3,1}(x)$ has a supersingular root in $\mathbb{F}_p$ that becomes incident to a new edge by Θ, then this new edge will be incident to a distinct vertex.

(b) If $R_{3,1}(x)$ has a supersingular root in $\mathbb{F}_p$, then the root is not incident to an edge which results in an edge attachment.

Proof: Note that the root of $R_{3,1}$ is 0. Let us go through the proof of each section:

(a) This is proved in **Lemma 1.6.52** by using the structure of $\Phi_3(0,x)$.

(b) This follows from the fact that **Lemma 1.6.52** tells us that if $e = (0, j)$ is a new edge in $\mathcal{S}_3^p$, then $(0, j)$ is a distinct edge that exists in $\mathcal{G}_\ell(\mathbb{F}_p)$, and hence this new edge is not connecting any vertices that were not already connected. Thus, no edge attachment.

■

Corollary 1.6.57: $R_{3,2}(x)$ has a supersingular root in $\mathbb{F}_p$ which results in an edge attachment if and only if $p = 31, 61$.

Proof: Note that the root of $R_{3,2}(x)$ is 8000. We know by **Lemma 1.6.51** that 8000 becomes incident to a new edge which is not a loop only when $p = 31, 61$. Now, if we compute $\mathcal{G}_3(\mathbb{F}_p)$, $\mathcal{S}_3^p$, and compare these two graphs for $p = 31, 61$, we see that these new edges are in fact edge attachments. ■

Corollary 1.6.58: $R_{3,3}(x)$ has a root which results in an edge attachment if and only if $p = 19, 31$.

Proof: Note that the root of $R_{3,3}(x)$ is 1728. By **Lemma 1.6.53** we know that 1728 is incident to a new edge if and only if $p = 7, 19, 31$. However, we know by **Theorem 1.6.7** that there is only one vertex when $p = 7$, hence edge attachment cannot take place. We can easily check that when $p = 19, 31$, 1728 becomes adjacent to a distinct vertex. This proves the statement. ■

Corollary 1.6.59: $R_{3,4}(x)$ has a supersingular root in $\mathbb{F}_p$ which results in an edge attachment if and only if $p = 19, 79$.

Proof: Note that the root of $R_{3,4}(x)$ is -32768. By **Lemma 1.6.54** we know that -32768 becomes incident to a new non-loop edge if and only if $p = 19, 79$. By computing $\mathcal{G}_3(\mathbb{F}_p)$, $\mathcal{S}_3^p$, and comparing the two graphs for $p = 19, 79$ we see that this new edge is in fact an edge-attaching edge. ■

Corollary 1.6.60: The following statements stand true:

(a) $R_{3,5}(x)$ has a supersingular root in $\mathbb{F}_p$ if and only if $p \equiv 7 \pmod 8$ or $p = 5, 13, 29$.

(b) $R_{3,5}(x)$ has a supersingular root in $\mathbb{F}_p$, and all of its roots are incident to a new edge (not necessarily the same edge) if and only if $p \equiv 7 \pmod 8$ such that $p \neq 23$ or $p = 5, 13, 29$.

(c) $R_{3,5}(x)$ has a supersingular root in $\mathbb{F}_p$, all of its roots become incident to a new edge (not necessarily the same edge), and this edge is not a loop if and only if $p \equiv 7 \pmod 8$ and $p \neq 7, 23, 47, 71, 79$

Proof: Let us prove each statement one at a time:

(a) Note that $R_{3,5}(x) = H_{32}(x)$. Hence by **Lemma 1.6.48** we know that $R_{3,5}(x)$ has a supersingular root in $\mathbb{F}_p$ if and only if $p = 5, 13, 29$ or $p \equiv 7 \pmod 8$. This proves the statement.

(b) Suppose $R_{3,5}(x)$ has a supersingular root in $\mathbb{F}_p$, however, the root is not incident to a new edge in $\mathcal{S}_3^p$. Let j be such a root. Note that since j is a root of $R_{3,5}(x)$ we know that j is a root of $\mathcal{R}e_3(x)$, and hence we know that j is incident to an out-multi-edge. By our supposition, it is assumed that this multi-edge exists in $\Gamma(\mathcal{G}_3(\mathbb{F}_p))$. However, the only time there can be an out-multi-edge

in $\Gamma(\mathcal{G}_3(\mathbb{F}_p))$ is when this multi-edge existed in $\mathcal{G}_\ell(\mathbb{F}_p)$ or $j = 1728$ since out-edges of 1728 does not result in folding by **Theorem 1.6.46**. In the former case, we know by **Theorem 1.4.5** that the only graph which has a multi-edge and has $\ell = 3$ is $\mathcal{G}_3(\mathbb{F}_{11})$, however, $p = 11$ does not result in $R_{3,2}(x)$ having a supersingular root. In the latter case, if we suppose 1728 is a root of $R_{3,5}(x)$, then we have $R_{3,5}(1728) = 0 \Leftrightarrow p = 2, 7, 23, 31$ by **Lemma 1.6.50(b.ii)**. By the proof of **Lemma 1.6.53** we know that if $p \equiv 7 \pmod{12}$ then 1728 is incident to a new edge. Thus that only leaves us with $p = 23$. Thus we know that the only time $R_{3,5}(x)$ has a supersingular root in $\mathbb{F}_p$ but the root is not incident to a new vertex is when $p = 23$, and a quick computation confirms this.

(c) Suppose $p \equiv 7 \pmod{8}$ such that $p \neq 23$ or $p = 5, 13, 29$. In this case we know that $R_{3,5}(x)$ has a supersingular root in $\mathbb{F}_p$. Now, suppose that this root has a loop. By factoring

$$\Phi_3(x,x) = (-1) \cdot x \cdot (x - 54000) \cdot (x - 8000)^2 \cdot (x + 32768)^2$$

we realize that the root has to be $0, 54000, 8000$, or -32768. By **Lemma 1.6.50(b)** we know that one of these can only happen if and only if $p = 5, 7, 13, 23, 29, 47, 71$, or 79. Taking into consideration our supposed restrictions on p we see that $p = 5, 7, 29, 47, 71, 79$ are the only possible primes that result in $R_{3,5}(x)$ having a root that could be incident to a loop. Hence if we exclude these primes, we know that the root of $R_{3,5}$ will not have a root which could be incident to a loop.

■

Corollary 1.6.61: The following statements stand true:

(a) $R_{3,6}(x)$ has a supersingular root in $\mathbb{F}_p$ if and only if $p \equiv 11, 19 \pmod{20}$ or $p = 5, 13, 17$.

(b) $R_{3,6}(x)$ has a supersingular root in $\mathbb{F}_p$, and all its roots are incident to a new edge (not necessarily the same edge) if and only if $p \equiv 11, 19 \pmod{20}$ such that $p \neq 11, 19$ or $p = 5, 13, 17$.

(c) $R_{3,6}(x)$ has a supersingular root in $\mathbb{F}_p$, all of its roots are incident to a new edge (not necessarily the same edge) and this new edge is not a loop if and only if $p \equiv 11, 19 \pmod{20}$ such that $p \neq 11, 19, 31, 59$.

Proof: Let us prove each statement one at a time.

(a) Note that $R_{3,6}(x) = H_{20}(x)$. Hence by **Lemma 1.6.47** we know that $R_{3,6}(x)$ has a supersingular root in $\mathbb{F}_p$ if and only if $p = 5, 13, 17$ or $p = 11, 19 \pmod{20}$. Hence we have proved this statement.

(b) Suppose that $R_{3,6}(x)$ has root x_0 such that this edge is not incident to a new edge. Since $R_{3,6}(x)$ is a factor of $\mathcal{R}e\mathcal{J}_3(x)$ we know that x_0 is incident to a multi-edge, however, by assumption, this edge cannot be new. Thus we know that x is incident to a multi-edge in $\Gamma(\mathcal{G}_3(\mathbb{F}_p))$. We know by Table 2 and **Theorem 1.6.46** that there is a multi-edge in $\Gamma(\mathcal{G}_3(\mathbb{F}_p))$ if and only if $p = 11$ or 1728 is supersingular and the multi-edge is leaving 1728. Note that $p = 11$ does result in $R_{3,6}(x)$ having a supersingular root by (a), hence we know that the root of $R_{3,6}(x)$ could be incident to a multi-edge that is not new in this case. On the other hand, $R_{3,6}(x)$ needs to have a root of 1728 to be able to be incident to an out-going multi-edge. BY **Lemma 1.6.50(a)** we know that $R_{3,6}(x)$ has a root of 1728 if and only if $p = 11, 19$, and we know that when $p = 11, 19$, $R_{3,6}(x)$ has a supersingular root in $\mathbb{F}_p$. Hence we know that the only times $R_{3,6}(x)$ has a supersingular root in

$\mathbb{F}_p$ that is not incident to a new edge is when $p = 11, 19$. Thus we conclude that if $p \neq 11, 19$ and $R_{3,6}(x)$ has a supersingular root in $\mathbb{F}_p$ then the root will be incident to a new edge. Hence we have proved the statement.

(c) Recall that as shown in the proof of **Corollary 1.6.60 (c)** we know that the only vertices in $\mathcal{S}_3^p$ that are incident to a loop are $0, 54000, 8000$, and -32768. By **Lemma 1.6.50** we know that $R_{2,6}(x)$ has one of $0, 54000, 8000$, or -32768 as a root if and only if $p = 5, 11, 13, 17, 19, 31, 59$. Hence if we exclude these prime values we know that the if $R_{3,6}(x)$ still has a supersingular root in $\mathbb{F}_p$ and this root is incident to a new edge then the root cannot be incident to a loop. Hence we have proved the statement.

Note that we have proved each individual statement in this corollary. Hence we have proved the corollary. ■

Corollary 1.6.62: The following statements stand true:

(a) $R_{3,7}(x)$ has a supersingular root in $\mathbb{F}_p$ if and only if $p \equiv 6, 19, 24, 26, 31, 34 \pmod{35}$ or $p = 5, 7, 23$.

(b) $R_{3,7}(x)$ has a supersingular root in $\mathbb{F}_p$, and all its roots are incident to a new edge (not necessarily the same edge) if and only if $p \equiv 6, 19, 24, 26, 31, 34 \pmod{35}$ such that $p \neq 19, 31$ or $p = 5, 23$.

(c) $R_{3,7}(x)$ has a supersingular root in $\mathbb{F}_p$, all its roots are incident to a new edge (note necessarily the same edge), and these edges are not loops if and only if $p \equiv 6, 19, 24, 26, 31, 34 \pmod{35}$ such that $p \neq 19, 31, 41, 61, 89, 101$.

Proof: Let us each statement one at a time.

(a) Note that $R_{3,7}(x) = H_{35}(x)$. Hence by **Lemma 1.6.49** we know that $R_{3,7}(x)$ has a supersingular root in $\mathbb{F}_p$ if and only if $p \equiv 6, 19, 24, 26, 31, 34 \pmod{35}$ or $p = 5, 7, 23$. This proves this statement.

(b) Suppose $p \equiv 6, 19, 24, 26, 31, 34 \pmod{35}$ or $p = 5, 7, 23$. By (a) we know that this implies that $R_{3,7}(x)$ has a supersingular root in $\mathbb{F}_p$. Further suppose that the root of $R_{3,7}(x)$ is not incident to a new edge. Let x_0 be such a root. Note that since x_0 is a root of $R_{3,7}(x)$, by definition we know that x_0 is a root of $\mathcal{R}e\mathcal{S}_3(x)$. Hence we know that x_0 is incident to a multi-edge in $\mathcal{S}_3^p$, however, this multi-edge is not new. Thus we know that x_0 has to be incident to a multi-edge in $\Gamma(\mathcal{G}_3(\mathbb{F}_p))$. By Table 2 and **Theorem 1.6.46** we know that the only multi edges possible are when $p = 11$ or when $x_0 = 1728$. However, note that $p = 11$ does not satisfy the necessary conditions for $R_{3,7}(x)$ to have a supersingular root in $\mathbb{F}_p$, and hence this case is not possible. On the other hand if we suppose that 1728 is a root of $R_{3,7}(x)$ then by **Lemma 1.6.50(c)** we know that this is possible if and only if $p = 7, 19, 31$. Hence if we exclude these primes, then we know that the root of $R_{3,5}(x)$ must be incident to a new edge. Thus we have proved the statement.

(c) Suppose $p \equiv 6, 19, 24, 26, 31, 34 \pmod{35}$ such that $p \neq 19, 31$ or $p = 5, 23$.. By (a) we know that this implies that $R_{3,7}(x)$ has a supersingular root in $\mathbb{F}_p$. Further suppose that the root of $R_{3,7}(x)$ is incident to a loop. We know by the proof of **Corollary 1.6.60(c)** that the only vertices in $\mathcal{S}_3^p$ that have loops are are $0, 54000, 8000$, and -32768. By **Lemma 1.6.50(c)** we know that $R_{3,7}(x)$ has one of $0, 54000, 8000$, or -32768 as a root if and only if $p = 5, 7, 19, 23, 41, 61, 89, 101$. Note if we exclude these prime values then we know that if $R_{3,7}(x)$ has a root, then that root cannot be incident to a loop. This proves the statement.

■

Lemma 1.6.63: A component of $\mathcal{G}_3(\mathbb{F}_p)$ folds if and only if there exist an edge in $\mathcal{G}_3(\mathbb{F}_p)$

Proof: ($\Rightarrow$): Suppose a component of $\mathcal{G}_3(\mathbb{F}_p)$ folds. Let U be such a component. We know by **Theorem 1.6.11** that this component must either contain 0 or 54000. We know that 0 and 54000 are supersingular if and only if $p \equiv 2 \pmod 3$. $p \equiv 2 \pmod 3$ is true if and only if $\left(\frac{-p}{3}\right) = 1$. Thus by **Theorem 1.4.4** there are edges in $\mathcal{G}_3(\mathbb{F}_p)$.

($\Leftarrow$): Suppose there are no edges in $\mathcal{G}_3(\mathbb{F}_p)$. We know by **Theorem 1.4.4** that $\left(\frac{-p}{3}\right) = -1$. We know this to be true if and only if $p \equiv 1 \pmod 3$. As a result we know that 0 and 54000 are not supersingular. By **Theorem 1.6.11** we know that no component can fold in this case.

Hence we have proved the statement. ■

Theorem 1.6.64: This theorem either explicitly gives the structure of $\Upsilon\left(\mathcal{S}_3^p\right)$ or describes what happens to $\mathcal{G}_\ell(\mathbb{F}_p)$ as Ω is applied.

(a) for $\ell = 3$, a maximum of two components can fold, and either no components become attached by a vertex or exactly two components become attached by a single vertex.

(b) The following are explicit descriptions of $\Upsilon\left(\mathcal{S}_3^p\right)$:

$$\Upsilon\left(\mathcal{S}_3^5\right) = \bullet$$

$$\Upsilon\left(\mathcal{S}_3^7\right) = \bullet$$

$$\Upsilon\left(\mathcal{S}_3^{11}\right) = \bullet \text{——} \bullet$$

$$\Upsilon\left(\mathcal{S}_3^{13}\right) = \bullet$$

$$\Upsilon\left(\mathcal{S}_3^{17}\right) = \bullet \text{——} \bullet$$

$$\Upsilon\left(\mathcal{S}_3^{19}\right) = \bullet \text{——} \bullet$$

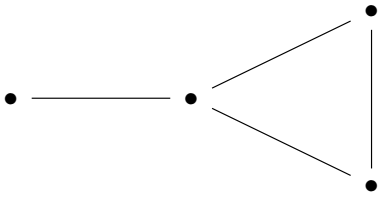
$$\Upsilon\left(\mathcal{S}_3^{23}\right) = \bullet \text{——} \bullet \text{——} \bullet$$

$$\Upsilon\left(\mathcal{S}_3^{29}\right) = \bullet \text{——} \bullet \text{——} \bullet$$

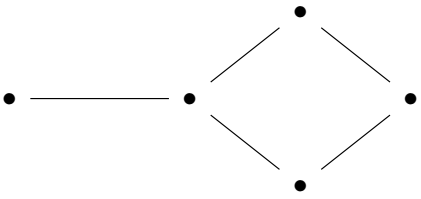
$\Upsilon(\mathcal{S}_3^{31}) =$

$\Upsilon(\mathcal{S}_3^{37}) =$

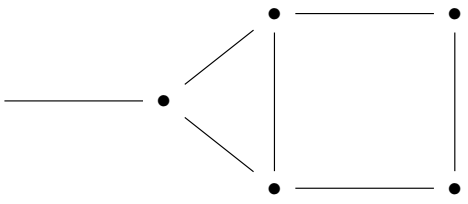
$\Upsilon(\mathcal{S}_3^{41}) =$



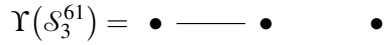
$\Upsilon(\mathcal{S}_3^{47}) =$



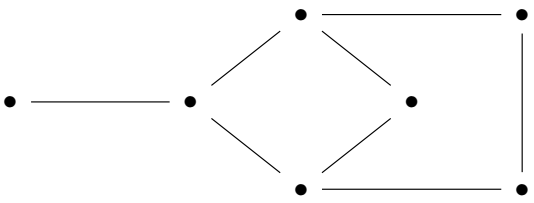
$\Upsilon(\mathcal{S}_3^{59}) =$



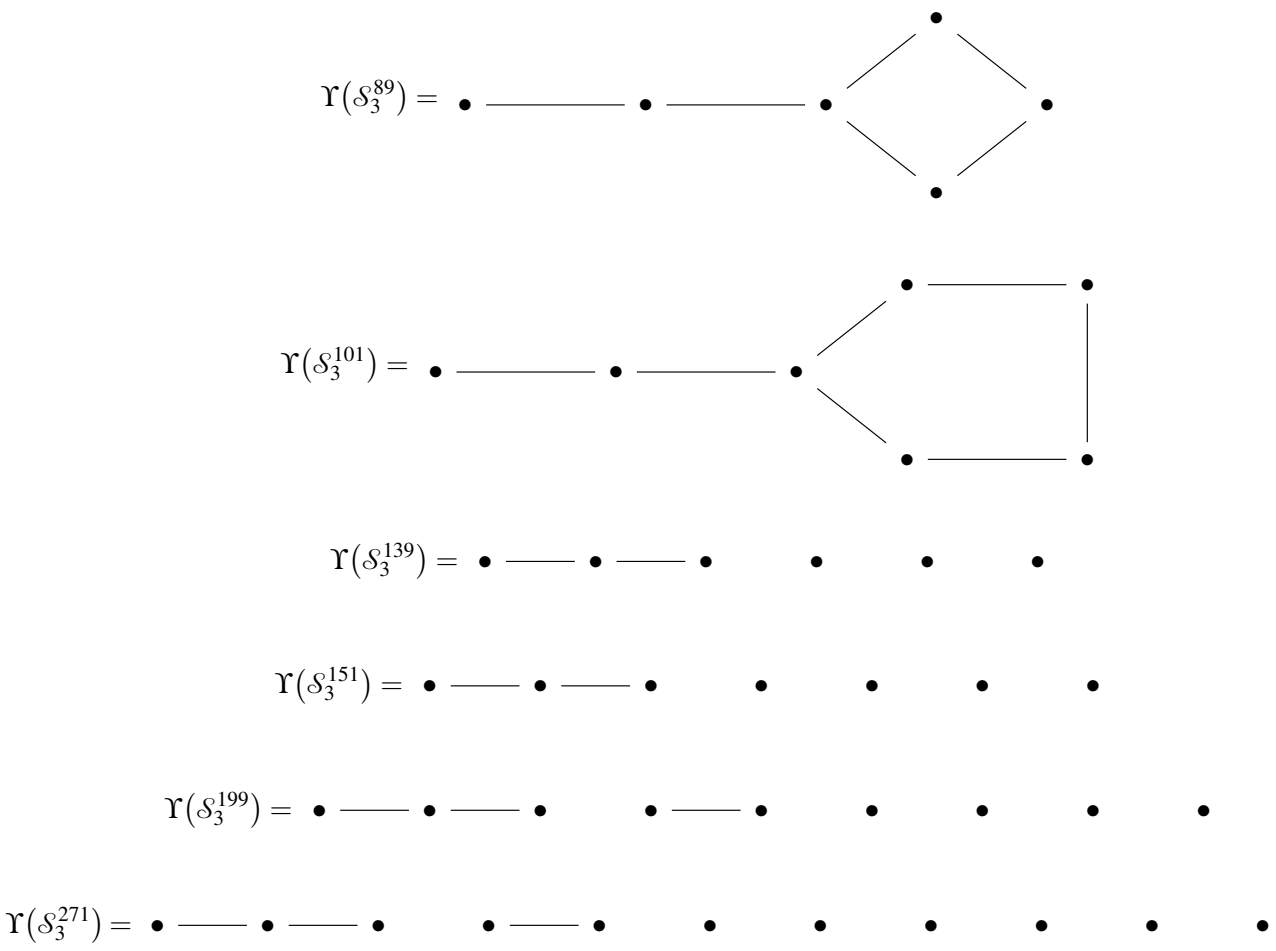
$\Upsilon(\mathcal{S}_3^{61}) =$



$\Upsilon(\mathcal{S}_3^{71}) =$



$\Upsilon(\mathcal{S}_3^{79}) =$



(c) Suppose $p \neq 5,7,11,13,17,19,23,29,31,41,47,59,61,71,79,89,101,139,151,199,271$. In this case, we will use the following terminology:

- *0 new edges*: This implies that if Ω adds any new edges to $\mathcal{G}\ell(\mathbb{F}_p)$ then they are loops.
- *1 new edge*: This implies that there exists a unique new multi-edge e that was added by Ω, and this edge is not a loop.
- *2 new edges*: This implies that there exist two new multi-edges e_1 and e_2 that were added by Ω such that neither e_1 nor e_2 are loops and they do not share any vertex between them.
- *3 new edges*: This implies that there exist three new multi-edges e_1, e_2, and e_3 that were added by Ω such that none of them are loops and do not share any vertex.

i. There does not exist any value of p such that $\mathcal{S}_3^p$ is made from one component folding, no vertex attachment happening, and 2 new edges being added.

ii. There does not exist any value of p such that $\mathcal{S}_3^p$ is made from one component folding, no vertex attachment happening, and 3 new edges being added.

iii. No folding happens, no vertex attachment happens, and 0 new edges are added iff

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

iv. No folding happens, no vertex attachment happens, and 1 new edge is added iff

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

v. No folding happens, no vertex attachment happens, and 2 new edges are added iff

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

vi. No folding happens, no vertex attachment happens, and 3 new edges are added iff

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

vii. One component folds, no vertex attachment happens, and 0 new edges are added iff

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

viii. One component folds, no vertex attachment happens, and 1 new edge is added iff

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

ix. Two components fold, they get attached by a vertex, and 0 new edges are added iff

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

x. Two components fold, they get attached by a vertex, and 1 new edge is added iff

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

xi. Two components fold, they get attached by a vertex, and 2 new edges are added iff

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

xii. Two components fold, they get attached by a vertex, and 3 new edges are added iff

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

xiii. No other edges (other than loops) can be added.

Proof: Let us go through one by one and prove the statement.

- This follows directly from **Theorem 1.6.11** and the description provided.
- We can check these values by a simple computation of the spine.
- Consider **Corollory 1.6.56** through **Corollory 1.6.62** along with 1.6.11 and the congruence conditions provided by each corollary. Note that we have excluded all primes that get removed in each corollary, and we have gotten rid of any finite cases in part (b). Hence by using the last congruence condition of each of those corollaries, we can use CRT to find the above-described situations based on how many polynomials have roots, and whether or not a component folds or not.

■

References

[Har77] Robin Hartshorne. *Algebraic geometry*. Vol. No. 52. Graduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg, 1977, pp. xvi+496. ISBN: 0-387-90244-9. URL: https://www.math.stonybrook.edu/~kamenova/homepage_files/Hartshorne_engl.pdf.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*. Second. Vol. 106. Graduate Texts in Mathematics. Springer, Dordrecht, 2009, pp. xx+513. ISBN: 978-0-387-09493-9. DOI: 10.1007/978-0-387-09494-6. URL: https://doi.org/10.1007/978-0-387-09494-6.

[DG16] Christina Delfs and Steven D. Galbraith. "Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$". In: *Des. Codes Cryptogr.* 78.2 (2016), pp. 425–440. ISSN: 0925-1022,1573-7586. DOI: 10.1007/s10623-014-0010-1. URL: https://doi.org/10.1007/s10623-014-0010-1.

[Sut22] Andrew Sutherland. *18.783 Elliptic Curves*. Lecture Notes. 2022. URL: https://math.mit.edu/classes/18.783/2022/lectures.html.

[Arp+23] Sarah Arpin et al. "Adventures in supersingularland". In: *Exp. Math.* 32.2 (2023), pp. 241–268. ISSN: 1058-6458,1944-950X. DOI: 10.1080/10586458.2021.1926009. URL: https://doi.org/10.1080/10586458.2021.1926009.

[Gha24] Wissam Ghantous. "Loops, multi-edges and collisions in supersingular isogeny graphs". In: *Advances in Mathematics of Communications* 18.4 (2024), pp. 935–955. ISSN: 1930-5346. DOI: 10.3934/amc.2022038. URL: https://www.aimsciences.org/article/id/62a94b882d80b75d2b6d8238.