ADDING LEVEL STRUCTURE TO SUPERSINGULAR ELLIPTIC CURVE ISOGENY GRAPHS

SARAH ARPIN

Abstract. Supersingular elliptic curve isogeny graphs are an interesting new direction for post-quantum cryptography. In this paper, we add the information of level structure to supersingular elliptic curves and study these objects with the motivation of isogeny-based cryptography. Supersingular elliptic curves with level structure map to Eichler orders in a quaternion algebra, just as supersingular elliptic curves map to maximal orders in a quaternion algebra. We study this map and the Eichler orders themselves. We also look at isogeny graphs of supersingular elliptic curves with level structure, and how they relate to supersingular isogeny graphs used in post-quantum cryptography.

1. Introduction

The emergence of quantum computers with the ability to break or weaken current cryptographic protocols has mathematicians and computer scientists alike searching for the next successful protocol to keep our secrets safe. Supersingular elliptic curve isogeny graphs have spawned a number of protocols, beginning with a hash function designed by Charles, Goren, and Lauter in 2006 [CGL09]. The CGL hash function [CGL09] is based on the hard problem of path-finding in the supersingular ℓ-isogeny graph, $\mathcal{G}_{\overline{\mathbb{F}}_p}$. A few years later came the SIDH key exchange protocol SIKE designed by De Feo, Jao, and Plût proposed in [DFJP14], followed by variants such as CSIDH [CLM$^+$18] and OSIDH [CK20]. SIKE is based on a slight modification of the path-finding hard problem in which the images of torsion points under certain isogenies are made public. This modification motivates the study of isogeny graphs of supersingular elliptic curves with level structure.

Definition 1.1. Let N and p be distinct primes. Let $|\mathcal{S}_N|$ denote the set of $\overline{\mathbb{F}}_p$-isomorphism classes of *supersingular elliptic curves with level-N structure*, which are represented by pairs (E, G) where E is a supersingular elliptic curve over $\overline{\mathbb{F}}_p$ and $G \subseteq E[N]$ is a cyclic subgroup of order N.

Each supersingular elliptic curve with level-N structure $(E, G) \in |\mathcal{S}_N|$ has an endomorphism ring $\mathcal{O}(E, G)$ respecting the level structure, which we define and describe in Section 3.1. The rings $\mathcal{O}(E, G)$ are isomorphic to Eichler orders in a quaternion algebra, which we prove in Theorem 3.5. In fact, every Eichler order of level-N is isomorphic to $\mathcal{O}(E, G)$ for some pair $(E, G) \in |\mathcal{S}_N|$. This association between endomorphism rings of supersingular elliptic curves with level-N structure and Eichler orders of level-N is remniscent of the association between endomorphism rings of supersingular elliptic curves and maximal orders, which we recall in Section 2.3. The map $\mathcal{O}(\cdot, \cdot)$ from $|\mathcal{S}_N|$ to isomorphism classes of Eichler orders allows us to study supersingular elliptic curves with level structure via studying Eichler orders in a quaternion algebra. In particular, ℓ-isogenies of supersingular elliptic curves can be identified with ideals of their corresponding endomorphism

Date: March 8, 2022.
Sarah Arpin was supported by NSF-CAREER CNS-1652238 (P.I. Katherine E. Stange).

rings. We recall this association in Section 2.2. A similar identification holds for ℓ-isogenies of supersingular elliptic curves with level-N structure, and we construct these ideals in Section 3.3.

In Section 4, we study the map $\mathcal{O}(\cdot,\cdot)$ from the set $|\mathcal{S}_N|$ of supersingular elliptic curves with level-N structure to isomorphism classes of Eichler orders of level N. This map is not injective, and the failure of injectivity of $\mathcal{O}(\cdot,\cdot)$ brings to light properties of the pairs (E,G). In particular, if we know the size of the fiber above $\mathcal{O}(E,G)$, we can discern different properties of E and the isogeny from E with kernel G. In Section 4.1, we describe two involutions on the set $|\mathcal{S}_N|$, corresponding to dual isogenies and the p-power Frobenius isogeny. These involutions help us understand the fibers of $\mathcal{O}(\cdot,\cdot)$. In Theorem 4.9, we describe the possible fiber sizes for the fibers along $\mathcal{O}(\cdot,\cdot)$. For $p \equiv 1 \pmod{12}$, the situation is simplified by the restriction to supersingular elliptic curves with automorphism group $\{[\pm 1]\}$. In this case, Propositions 4.11 and 4.13 provide a detailed analysis for what the fiber above $\mathcal{O}(E,G)$ can tell us about the supersingular elliptic curve E and the isogeny with kernel given by the group G.

In Section 5, we apply our understanding of the failure of injectivity of $\mathcal{O}(\cdot,\cdot)$ to provide an approximate upper-bound for the number of supersingular elliptic curves over $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$ which have degree-N isogenies to their p-power Frobenius conjugate. First described in [ACNL$^+$21], this question relates to path-finding strategies described in [EHL$^+$20]. The initial motivation for considering such isogenies was the appearance of *mirror paths* in the ℓ-isogeny graph. These are (undirected) paths in the ℓ-isogeny graph which are invariant under the p-power Frobenius isogeny. Such paths necessarily have a central reflection point consisting of either a pair of N-isogenous conjugate curves or a single curve defined over $\mathbb{F}_p$. In [ACNL$^+$21], we were interested in counting paths of the first kind, and so we computed heuristics of the numbers of supersingular elliptic curves defined over $\mathbb{F}_{p^2}$ (and not defined over $\mathbb{F}_p$) which had a degree-N isogeny to their Frobenius conjugate. The lower bound provided by [EHL$^+$20] for this count included supersingular elliptic curves defined over $\mathbb{F}_p$ which have a degree-N endomorphism. This lower bound proves the existence of mirror paths in any ℓ-isogeny graph, but it does not allow us to distinguish between the two types of mirror path as described above. Using information from the fiber sizes of $\mathcal{O}(\cdot,\cdot)$, we give an approximate upper-bound specifically for the N-isogenies between distinct Frobenius conjugates. Additionally, we provide an exact count for the number of N-isogenies between a supersingular elliptic curve and its Frobenius conjugate, removing our restriction to curves which are defined over $\mathbb{F}_{p^2}$ and not $\mathbb{F}_p$.

In Section 6, we build the category $\mathcal{S}_N$ with objects given by the isomorphism classes in $|\mathcal{S}_N|$ and morphisms given by isogenies. This categorical point of view is inspired by the classical Deuring correspondence, which we recall in Section 2.1. In Section 6.1, we prove a categorical equivalence between the category of supersingular elliptic curves with level-N structure and the category of invertible left $\mathcal{O}(E,G)$-modules, for a fixed $(E,G) \in \mathcal{S}_N$. The equivalence is obtained via the functor $\mathscr{h}_{(E,G)}$ which maps any pair $(E',G') \in \mathcal{S}_N$ to $\mathrm{Hom}((E',G'),(E,G))$. The proof strategy for this equivalence centers on the development of the properties of invertible left modules of the objects $\mathcal{O}(E,G)$. The properties of Eichler orders are integral to understanding the structure of these modules.

In Section 7, we restrict the morphisms of $\mathcal{S}_N$ to isogenies of degree-ℓ to create an ℓ-isogeny graph of supersingular elliptic curves with level-N structure:

Definition 1.2. In the graph $\mathcal{E}^N_{p,\ell}$, vertices are $\overline{\mathbb{F}}_p$-isomorphism classes of pairs (E,G), where E is a supersingular elliptic curve and G is a subgroup of $E[N]$ of order N. An edge from vertex (E,G) to vertex (E',G') is a degree-ℓ isogeny $\varphi : E \to E'$ such that $\varphi(G) = G'$.

The set of vertices of the graph $\mathcal{E}_{p,\ell}^N$ is the set $|\mathcal{S}_N|$ of isomorphism classes of supersingular elliptic curves with level-N structure. The properties of $\mathcal{E}_{p,\ell}^N$ mirror those of the supersingular ℓ-isogeny graph used in post-quantum cryptography. In particular, $\mathcal{E}_{p,\ell}^N$ is a connected graph. We also provide an example of the corresponding graph of Eichler orders.

1.1. **Acknowledgments.** The author is deeply indebted to her advisor, Katherine E. Stange, for continuous guidance on this paper from the very start. The author would like to thank John Voight for promptly answering emails to provide very helpful exposition and clarification. Additional thanks to Leo Herr and Soumya Sankar for helpful discussions.

1.2. **Conventions.** In this paper, p is a cryptographic size prime, and N and ℓ are distinct small ($\leq \log p$) primes, unless otherwise noted.

2. Background

Let $B_{p,\infty}$ denote the unique (up to isomorphism) quaternion algebra ramified precisely at p and infinity.

2.1. **The Classical Deuring Correspondence.** Deuring provides a correspondence between the endomorphism rings of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ and maximal orders in the appropriate quaternion algebra. The connection to the quaternions provides an important avenue for studying the structure of the isogeny graphs.

Theorem 2.1 (Deuring Correspondence)**.** *Fix a maximal order R of the quaternion algebra $B_{p,\infty}$. There is a bijection between isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ and the left class set of the maximal order R.*

Deuring's original statement depends on a choice of maximal order R in $B_{p,\infty}$, which is implicitly a choice of supersingular elliptic curve whose endomorphism ring is isomorphic to R. For every maximal order, the right orders of ideals in the left ideal class set of that order will run through all of the maximal orders of the quaternion algebra. In this way, one can think of associating the supersingular elliptic curves over $\overline{\mathbb{F}}_p$ to the maximal orders of $B_{p,\infty}$, which is either a one-to-one or two-to-one map, depending on the field of definition of the supersingular elliptic curve, or equivalently the size of the two-sided ideal class group of the maximal order. This perspective removes the necessity of an initial choice of maximal order, but it no longer describes a bijection: If E is defined over $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$, then $E \ncong E^p$, but $\mathrm{End}(E) \cong \mathrm{End}(E^p)$ map to the same maximal order of $B_{p,\infty}$. If E is defined over $\mathbb{F}_p$, then $E \cong E^p$ and $\mathrm{End}(E)$ is the maximal order uniquely identified with the isomorphism class of E.

Ribet [Rib89] credits an unpublished manuscript of Mestre–Osterlé for this basepoint-free version of the Deuring Correspondence: He writes that Mestre–Osterlé take a perspective of "oriented" maximal orders to achieve this result. The basepoint-free perspective is also how Kohel presents the Deuring correspondence in his thesis [Koh96]:

Theorem 2.2 (Theorem 44 [Koh96])**.** *Given a maximal order of the quaternion algebra $B_{p,\infty}$, there exist one or two supersingular j-invariants over $\overline{\mathbb{F}}_p$ such that the corresponding endomorphism ring is isomorphic to a maximal order of the given type.*

Kohel also presents the basepoint dependent version of the Deuring Correspondence as a categorical equivalence [Koh96, Theorem 45]. In Section 6, we prove a categorical equivalence in the level structure context.

2.2. **Translating Isogenies to the Quaternion Algebra Side.** Isogenies of supersingular elliptic curves also have a corresponding object in the quaternion algebra $B_{p,\infty}$. A thorough reference for the correspondence between isogenies and left ideals of a maximal order $\mathcal{O} \cong \mathrm{End}(E)$ is described in detail in [Voi21, 42.2]. We briefly recall this theory here: suppose $\varphi : E \to E'$ is a separable isogeny between supersingular elliptic curves over $\overline{\mathbb{F}}_p$. Let I_φ be the left ideal of $\mathrm{End}(E)$ in $B_{p,\infty}$ which corresponds to φ in the following way:

$$\ker(\varphi) = \bigcap_{\alpha \in I_\varphi} \ker(\alpha).$$

The norm of I_φ is equal to the degree of φ. The ideal I_φ is also a right $\mathrm{End}(E')$ ideal, by the same theory.

2.3. **Embedding Multiple Endomorphism Rings in $B_{p,\infty}$.** If one wishes to compare more than one supersingular elliptic curve over $\overline{\mathbb{F}}_p$ to the corresponding maximal order in $B_{p,\infty}$, one must be careful to choose compatible maps into the same copy of $B_{p,\infty}$. A detailed discussion is found in [Voi21, Section 42.2], and we provide a summary of the details which will be necessary for this paper. Fix a supersingular elliptic curve $E/\overline{\mathbb{F}}_p$. The endomorphism ring of E, $\mathrm{End}(E)$, is a maximal order in the quaternion algebra $B^E_{p,\infty} := \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q} \cong B_{p,\infty}$. All supersingular elliptic curves are isogenous. To map the endomorphism ring $\mathrm{End}(E')$ of another supersingular elliptic curve $E'/\overline{\mathbb{F}}_p$ into $B^E_{p,\infty}$, we choose an isogeny $\varphi : E \to E'$. As described above, φ corresponds to a left ideal I of the maximal order $\mathrm{End}(E)$. Any left ideal in the class of I corresponds to an isogeny $E \to E'$. We map the endomorphisms of E' into $B^E_{p,\infty}$ via

$$\begin{aligned} \mathrm{End}(E') &\hookrightarrow B^E_{p,\infty} \\ \beta &\mapsto \frac{1}{\deg \varphi}(\widehat{\varphi}\beta\varphi). \end{aligned} \tag{1}$$

The image of $\mathrm{End}(E')$ is the maximal order of $B^E_{p,\infty}$ which is the right order of I. In this way, we are viewing the endomorphism rings of E and E' inside the same copy of $B_{p,\infty}$, namely $B^E_{p,\infty}$ as defined above. Note that this map depends on a choice of φ: if instead we had chosen an isogeny $\eta \circ \varphi : E \to E'$, where $\eta \in \mathrm{Aut}(E')$, the image of $\mathrm{End}(E')$ in $B^E_{p,\infty}$ would remain the same, but the map itself would be different.

2.4. **$\mathbb{F}_p$-Endomorphism Rings.** While computing the full endomorphism ring of a given supersingular elliptic curve is generically a hard problem, this is not the case for computing the subset of endomorphisms which are defined over $\mathbb{F}_p$, for curves which are defined over $\mathbb{F}_p$. Delfs and Galbraith [DG16] show that $\mathrm{End}_{\mathbb{F}_p}(E) \cong \mathbb{Z}[\sqrt{-p}]$ or $\mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$, depending on the congruence class of p modulo 4 and the action of the p-power Frobenius on the two-torsion points of E. We condense and re-state this theorem below for ease of reference:

Proposition 2.3 (Section 2 [DG16])**.** Let $E/\mathbb{F}_p$ be a supersingular elliptic curve, and let π_p denote the p-power Frobenius map on E. If $p \equiv 1 \pmod 4$, then $\mathrm{End}(E) \cong \mathbb{Z}[\sqrt{-p}]$. If $p \equiv 3 \pmod 4$, then there are two possibilities for $\mathrm{End}_{\mathbb{F}_p}(E)$: if $\pi_p(P) = P$ for all $P \in E[2]$, then $\mathrm{End}_{\mathbb{F}_p}(E) \cong \mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$. Otherwise, $\mathrm{End}_{\mathbb{F}_p}(E) \cong \mathbb{Z}[\sqrt{-p}]$.

2.5. **Historical context of level structure.** The notion of extending the Deuring correspondence to a supersingular ℓ-isogeny graph with level structure is not new. However, there has yet to appear a detailed description of an equivalence of categories for supersingular elliptic curves with level structure. The idea has been called "folklore" [FKL+20, Section 4]: Papers have been written about related concepts in the context of modular forms (Ribet), or different choices of level structure (Goren–Kassaei [GK17], with a choice of torsion point, Roda's thesis [Rod19] with full level structure). In this paper, the author hopes to provide the details of theorems that many have suspected, as well as some which are perhaps less expected. To begin this work, we provide a brief overview of what we have found in the literature, to date.

Voight [Voi21, Remark 42.3.10] also notes that a generalization of the Deuring correspondence is possible through mild adjustments. Ribet, in [Rib89], also notes that the Deuring correspondence as phrased by Mestre–Osterlé can be extended to "oriented" Eichler orders, but does not prove the correspondence explicitly.

Eichler [Eic55] [Eic73] and Pizer [Piz73] provide the foundational theory of Eichler orders.

More recently, work of Goren and Kassaei [GK17] takes the perspective of Hecke operators to prove properties of the supersingular ℓ-isogeny graph with the added level-N structure of a choice of N-torsion point.

The SqiSign authors [FKL$^+$20] have most recently published a version of the Eichler order Deuring correspondence, motivated by commutative isogeny diagrams of supersingular elliptic curves: Under suitable conditions for p, the authors prove a bijection between the class set of a fixed Eichler order of square-free level N and the set of all N-isogenies between supersingular elliptic curves over $\overline{\mathbb{F}}_p$. This bijection is essentially the same as the underlying bijection on objects of the equivalence of categories proved in Section 6.

3. Elliptic Curves with Level Structure and Their Endomorphism Rings

Definition 3.1. Let $|\mathcal{S}_N|$ denote the set of pairs (E, G), up to equivalence $\sim$, where E is a supersingular elliptic curve over $\overline{\mathbb{F}}_p$ and $G \subseteq E[N]$ is a subgroup of order N. Two pairs $(E_1, G_1), (E_2, G_2)$ are equivalent under the equivalence relation $\sim$ if there exists an isomorphism $\rho : E_1 \to E_2$ such that $\rho(G_1) = G_2$. The pairs in $|\mathcal{S}_N|$ are *supersingular elliptic curves with level-N structure.*

We define the notion of an endomorphism ring of a pair in $|\mathcal{S}_N|$ (Section 3.1) and describe the structure of this endomorphism ring as an object in the quaternion algebra $B_{p,\infty}$ (Section 3.2).

3.1. Endomorphism Rings $\mathcal{O}(E, G)$.

Definition 3.2 ($\mathcal{O}(E, G)$)**.** As a subring of $\mathrm{End}(E)$, we define the ring of endomorphisms of the pair $(E, G) \in |\mathcal{S}_N|$ as follows:

$$\mathcal{O}(E, G) := \{\alpha \in \mathrm{End}(E) : \alpha(G) \subseteq G\}.$$

Since $|\mathcal{S}_N|$ is a set of equivalence classes, we need to check that $\mathcal{O}(\cdot, \cdot)$ is well-defined on these equivalence classes.

Proposition 3.3. Suppose $(E, G) \sim (F, H)$ for some $(E, G), (F, H) \in |\mathcal{S}_N|$. By definition, this means that there exists an isomorphism $\eta : E \to F$ such that $\eta(G) = H$. Then, the map $\mathcal{O}(F, H) \to \mathcal{O}(E, G)$ defined $\alpha \mapsto \eta^{-1}\alpha\eta$ is an isomorphism.

Proof. If $\eta : E \to F$ is an isomorphism, then we have an isomorphism $\mathrm{End}(F) \to \mathrm{End}(E)$ given by $\alpha \mapsto \eta^{-1}\alpha\eta$. Since $\eta(G) = H$, $\alpha(H) \subseteq H$ is equivalent to $\eta^{-1}\alpha\eta(G) \subseteq G$. We have:

$$\begin{aligned}\mathcal{O}(F, H) &= \{\alpha \in \mathrm{End}(F) : \alpha(H) \subseteq H\} \\ &\cong \{\beta \in \mathrm{End}(E) : \beta(G) \subseteq G\} \\ &= \mathcal{O}(E, G).\end{aligned}$$

□

In Theorem 3.5, we show that $\mathcal{O}(E,G)$ is an Eichler order of level N of $B_{p,\infty}$. We consider $\mathcal{O}(\cdot,\cdot)$ as a map that we apply to elements (E,G) of $|\mathcal{S}_N|$. Just as supersingular elliptic curves are mapped to the set of maximal orders of $B_{p,\infty}$, we map elements of $|\mathcal{S}_N|$ to Eichler orders of level N of $B_{p,\infty}$. By Proposition 3.6, the map $\mathcal{O}(\cdot,\cdot)$ is surjective onto isomorphism classes of Eichler orders of level N in $B_{p,\infty}$, but injectivity fails in an interesting way. We describe this completely in Section 4.

Proposition 3.4. *Let (E,G) be an element of $|\mathcal{S}_N|$. Let $\varphi : E \to E/G$ be an isogeny with $\ker(\varphi) = G$. Then, $\mathcal{O}(E,G) = \mathrm{End}(E) \cap (\frac{1}{\deg\varphi}\widehat{\varphi}\mathrm{End}(E/G)\varphi)$ where the intersection is taken in $B^E_{p,\infty}$, and is independent of choice of φ.*

Proof. We proceed by showing containment in both directions. To see $\mathcal{O}(E,G) \supseteq \mathrm{End}(E) \cap (\frac{1}{\deg\varphi}\widehat{\varphi}\mathrm{End}(E/G)\varphi)$, take $\alpha \in \mathrm{End}(E) \cap (\frac{1}{\deg\varphi}\widehat{\varphi}\mathrm{End}(E/G)\varphi)$. Immediately we have $\alpha \in \mathrm{End}(E)$, so it remains to show $\alpha(G) \subseteq G$. There exists $\beta \in \mathrm{End}(E/G)$ such that $\varphi\circ\alpha = \beta\circ\varphi$. This guarantees that $\alpha(G) \subseteq G$, as $\varphi\circ\alpha(G) = \beta\circ\varphi(G) = \{id_{E/G}\}$.

To see $\mathcal{O}(E,G) \subseteq \mathrm{End}(E)\cap(\frac{1}{\deg\varphi}\widehat{\varphi}\mathrm{End}(E/G)\varphi)$, take $\alpha \in \mathcal{O}(E,G)$. To show $\alpha \in \frac{1}{\deg\varphi}\widehat{\varphi}\mathrm{End}(E/G)\varphi$, we will show that there exists a $\beta \in \mathrm{End}(E/G)$ such that $\varphi\circ\alpha = \beta\circ\varphi$. Since $\alpha(G) \subseteq G$, we have $\ker(\varphi) = G \subseteq \ker(\varphi\circ\alpha)$. We apply Corollary III.4.11 of [Sil09] to guarantee the existence of a (unique) $\beta : E/G \to E/G$ such that $\varphi\circ\alpha = \beta\circ\varphi$.

Our choice of $\varphi : E \to E/G$ is unique up to post-composition with an automorphism of E/G. If we replace φ above with $\psi := \eta\circ\varphi$ for some $\eta \in \mathrm{Aut}(E/G)$, we obtain the object:

$$\frac{1}{\deg\psi}\widehat{\psi}\mathrm{End}(E/G)\psi = \frac{1}{\deg\eta\cdot\deg\varphi}\widehat{\varphi}\widehat{\eta}\mathrm{End}(E/G)\eta\varphi.$$

Since η is an automorphism of E/G, $\widehat{\eta}\mathrm{End}(E/G)\eta = \mathrm{End}(E/G)$ and $\deg\eta = 1$. This gives an equality:

$$\frac{1}{\deg\psi}\widehat{\psi}\mathrm{End}(E/G)\psi = \frac{1}{\deg\varphi}\widehat{\varphi}\mathrm{End}(E/G)\varphi.$$

□

3.2. **Eichler Orders.** The classical origins of Eichler orders can be traced to papers of Eichler himself [Eic55], [Eic73]. The theory of Eichler orders was further developed by Pizer [Piz73]. Eichler orders of prime level are called *hereditary*. For relevant properties and background on Eichler and hereditary orders, see [Voi21].

Any Eichler order in a quaternion algebra is the intersection of two (not necessarily distinct) maximal orders. The level of an Eichler order in $B_{p,\infty}$ is given by its index in one of the maximal orders whose intersection defines the order (this index will be the same for either order). In [KLPT14, Lemma 8], the authors describe how an Eichler order of level N is equivalent data to two maximal orders with a connecting ideal of reduced norm N. We let $\mathrm{Nrd}(I)$ denote the reduced norm of the ideal I.

Theorem 3.5. *$\mathcal{O}(E,G)$ is isomorphic to an Eichler order of level $|G| = N$.*

Proof. Proposition 3.4 shows that $\mathcal{O}(E,G) \cong \mathrm{End}(E) \cap (\frac{1}{\deg\varphi}\widehat{\varphi}\mathrm{End}(E/G)\varphi)$, where E/G is the codomain of φ. Fix $B^E_{p,\infty} \cong \mathrm{End}(E)\otimes_{\mathbb{Z}}\mathbb{Q}$. By the Deuring correspondence $\mathrm{End}(E)$ and $\frac{1}{\deg\varphi}\widehat{\varphi}\mathrm{End}(E/G)\varphi$ are maximal orders in the quaternion algebra $B^E_{p,\infty}$. The intersection of two maximal orders is an Eichler order, so it remains to show that the level of $\mathcal{O}(E,G)$ is N.

In Proposition 3.4, we introduced the isogeny $\varphi : E \to E/G$ with kernel G. This isogeny corresponds to a left ideal I of the maximal order $\mathrm{End}(E)$, where $\mathrm{Nrd}(I) = \deg\varphi = N$. See

Section 2.2 for a detailed description of this association between isogenies and left ideals. The left order of I, which we denote $O_L(I)$, is $\mathrm{End}(E)$. $\mathrm{End}(E/G)$ embeds into $B_{p,\infty}^E$ as the right order of I. Together with Proposition 3.4, this shows that $\mathcal{O}(E,G) \cong O_L(I) \cap O_R(I)$. By [KLPT14, Lemma 8], this is an Eichler order of level $\mathrm{Nrd}(I) = N$. □

The following proposition shows that our map $\mathcal{O}(\cdot,\cdot)$ to Eichler orders of level N of $B_{p,\infty}$ is surjective.

Proposition 3.6. Every Eichler order $\mathcal{O}$ of level N in $B_{p,\infty}$ is isomorphic to $\mathcal{O}(E,G)$ for some pair (E,G) in $|\mathcal{S}_N|$.

Proof. Every local Eichler order $\mathcal{O}$ of prime level N is the intersection of two uniquely determined maximal orders $\mathcal{O}_1, \mathcal{O}_2$ such that $\mathcal{O}$ is of index N in both $\mathcal{O}_1$ and $\mathcal{O}_2$ [Voi21, Proposition 23.4.3]. Eichler orders of prime level are only non-maximal at the prime which is their level, so all three orders $\mathcal{O}, \mathcal{O}_1, \mathcal{O}_2$ lift uniquely to the global setting [Voi21, Theorem 9.1.1]. By the Deuring correspondence, fix an isomorphism $\mathrm{End}(E_1) \cong \mathcal{O}_1$ for a supersingular elliptic curve $E_1/\overline{\mathbb{F}}_p$. Let $B_{p,\infty}^{E_1} = \mathrm{End}(E_1) \otimes_{\mathbb{Z}} \mathbb{Q}$.

By [KLPT14, Lemma 8], there exists a unique ideal I of $B_{p,\infty}^{E_1}$ which is a left $\mathcal{O}_1$-ideal and a right $\mathcal{O}_2$-ideal of reduced norm N. This ideal determines a group G of order N given by the scheme theoretic intersection

$$G := \bigcap_{\alpha \in I} E_1[\alpha]$$

where $E_1[\alpha]$ is the kernel of the endomorphism α. By equation (1) of Section 2.3, the right order of I is given by $\frac{1}{\deg\varphi}\widehat{\varphi}\mathrm{End}(E_2)\varphi$. Since $\mathcal{O}_2$ is the right order of I, we have $\mathcal{O}_2 = \frac{1}{\deg\varphi}\widehat{\varphi}\mathrm{End}(E_2)\varphi$.

By Proposition 3.4, $\mathcal{O}(E_1,G) = \mathrm{End}(E_1) \cap \frac{1}{\deg\varphi}\widehat{\varphi}\mathrm{End}(E_2)\varphi \cong \mathcal{O}_1 \cap \mathcal{O}_2 = \mathcal{O}$. □

The failure of injectivity of $\mathcal{O}(\cdot,\cdot)$ reveals structural properties of both the supersingular elliptic curves with level-N structure and the Eichler orders of level N. We address this completely in the following section.

3.3. ℓ-isogenies on the Quaternion Side.

The correspondence between ℓ-isogenies and left ideals of a maximal order $\mathcal{O} \cong \mathrm{End}(E)$ of reduced norm ℓ is well-known, as we recalled in Section 2.2. Let $\varphi : E \to E/G$ be a degree-ℓ isogeny between supersingular elliptic curves over $\overline{\mathbb{F}}_p$. Then $G \subset E[N], \varphi(G) \subset (E/G)[N]$ and $|G| = |\varphi(G)| = N$. Let I_G be the left ideal of the maximal order isomorphic to $\mathrm{End}(E)$ in $B_{p,\infty}^E$ which corresponds to φ. The degree of the isogeny is the norm of the ideal. The isogeny $\varphi : E \to E/G$ is also a morphism between elements of $|\mathcal{S}_N|$, as $\varphi : (E,G) \to (E/G, \varphi(G))$. In this section, we describe isogenies between elements of $|\mathcal{S}_N|$ as quaternion objects.

Proposition 3.7. Let $\mathcal{O}$ be an Eichler order of level-N specified by the intersection $M_1 \cap M_2$ of two maximal orders M_1 and M_2. The integral left ideals I of a maximal order M_1 are in bijection with the left ideals of $\mathcal{O}$ of norm coprime to N. This bijection is realized by the map $I \mapsto I \cap \mathcal{O}$ and if $Nrd(I)$ is coprime to N, then $Nrd(I) = Nrd(\mathcal{O})$.

Proof. This property can be proven locally. The left ideals are lattices in the quaternion algebra. Let $\mathcal{O}$ be an Eichler order, and let MO be a maximal order containing $\mathcal{O}$. At every prime q dividing neither p nor the level of $\mathcal{O}$, the order $\mathcal{O}_q \cong MO_q$. By [Voi21, Theorem 9.1.1], it follows that there is a bijection between the lattices of reduced norm ℓ of a maximal order and those of any Eichler order contained in that maximal order.

To see that this bijection is realized by intersecting the ideals of the maximal order with the Eichler order, see the proof provided in [FKL+20, Lemma 5]. □

We have a way of associating the ideals I of maximal orders with isogenies $E \to E'$. To extend this picture to $\mathcal{O}(E, G)$, we need to show that a left ideal of $\mathcal{O}(E, G)$ will have right order $\mathcal{O}(E', G')$, where I corresponds to an isogeny $\varphi_I : E \to E'$ such that $\varphi_I(G) = G'$.

By Proposition 3.7, every left-ideal of $\mathcal{O}(E, G)$ of norm prime to N is of the form $I \cap \mathcal{O}(E, G)$.

Proposition 3.8. Let $I \cap \mathcal{O}(E, G)$ be a left ideal of $\mathcal{O}(E, G)$ of norm prime to N. Then,

$$O_R(I \cap \mathcal{O}(E, G)) \cong \frac{1}{\deg \varphi_I} \widehat{\varphi}_I \mathcal{O}(E', G')\varphi_I.$$

Proof. We proceed by showing containment in both directions. By [FKL+20, Lemma 5] $I \cap \mathcal{O}(E, G)$ is a left ideal of the Eichler order $\mathcal{O}(E, G)$.

Take $\frac{1}{\deg \varphi_I}\widehat{\varphi}_I \alpha \varphi_I \in \frac{1}{\deg \varphi_I}\widehat{\varphi}_I \mathcal{O}(E', G')\varphi_I$, for some $\alpha \in \mathcal{O}(E', G')$. To show that $(I \cap \mathcal{O}(E, G))\frac{1}{\deg \varphi_I}\widehat{\varphi}_I \alpha \varphi_I \subseteq I \cap \mathcal{O}(E, G)$, note that the elements of $I \cap \mathcal{O}(E, G)$ are characterized by the following two properties:

(i) Every $\nu \in I \cap \mathcal{O}(E, G)$ must be of the form $\beta \circ \varphi_I$, for some $\beta \in \mathrm{Hom}(E', E)$. This property is equivalent to being in I, by [Voi21, Lemma 42.2.7].

(ii) Every $\nu \in I \cap \mathcal{O}(E, G)$ must satisfy $\nu(G) \subseteq G$. This property is equivalent to being in $\mathcal{O}(E, G)$, by definition. Note that this is equivalent to requiring that $\beta(G') \subseteq G$, when we write ν in the form $\nu = \beta \circ \varphi_I$.

For any $\beta \circ \varphi_I \in I \cap \mathcal{O}(E, G)$ we have:

$$\beta \circ \varphi_I \circ \left(\frac{1}{\deg \varphi_I}\widehat{\varphi}_I \circ \alpha \circ \varphi_I\right) = \beta \circ \alpha \circ \varphi_I$$

So our element $\frac{1}{\deg \varphi_I}\widehat{\varphi}_I \alpha \varphi_I$ satisfies condition (i). To check condition (ii):

$$\beta \circ \varphi_I \circ \left(\frac{1}{\deg \varphi_I}\widehat{\varphi}_I \circ \alpha \circ \varphi_I\right)(G) = \beta \circ \alpha \circ \varphi_I(G) = \beta \circ \alpha(G') \subseteq \beta(G') \subseteq G$$

To see $O_R(I \cap \mathcal{O}(E, G)) \subseteq \frac{1}{\deg \varphi_I}\widehat{\varphi}_I \mathcal{O}(E', G')\varphi_I$, recall that $I \cap \mathcal{O}(E, G)$ is a left ideal of an Eichler order of level N, and the right order of this ideal must also be an Eichler order of level N (see [Voi21, Lemma 17.4.11]). Since $O_R(I \cap \mathcal{O}(E, G))$ contains the Eichler order $\frac{1}{\deg \varphi_I}\widehat{\varphi}_I \mathcal{O}(E', G')\varphi_I$ of level N, this containment is equality. □

4. Failure of Injectivity of $\mathcal{O}(\cdot, \cdot)$

We have shown how to associate supersingular elliptic curves with level-N structure to Eichler orders of $B_{p,\infty}$ of level N via the map $\mathcal{O}(\cdot, \cdot)$. This map is not usually bijective, and we study the properties of supersingular elliptic curves with level structure which result in the various possible fiber sizes. In Section 4.1 we describe two involutions corresponding to a dualizing action and the p-power Frobenius action. These involutions help us determine the fibers of $\mathcal{O}(E, G)$ in Theorem 4.9 of Section 4.2. In Section 4.3, we assume $p \equiv 1 \pmod{12}$ and completely describe the failure of injectivity by classifying elements of $|\mathcal{S}_N|$ which result in one-to-one, two-to-one, and four-to-one maps, which are the only possibilities for this congruence class of p. An example of the potentially more complicated case $p \not\equiv 1 \pmod{12}$ is provided in Section 4.4.

4.1. **Involutions.** In this section, we will define two group involutions on the set $|\mathcal{S}_N|$ of equivalence classes of supersingular elliptic curves with level-N structure. For this approach, it is useful to consider the following construction of representatives for the equivalence classes in $|\mathcal{S}_N|$: For each supersingular j-invariant, fix a particular Weierstrass model. In $|\mathcal{S}_N|$, it suffices to only consider pairs (E, G) where E has the Weierstrass model fixed for $j(E)$. In each equivalence class, there exists at least one pair (E, G) where E has the desired Weierstrass equation. For $j(E) \neq 0, 1728$, this pair is necessarily unique. For $j(E) = 0, 1728$, there may be multiple pairs (E, G) in the same equivalence class, due to extra automorphisms $\eta : E \to E$ which may act nontrivially on subgroups. Equivalence classes corresponding to $j(E) = 0, 1728$ may have one, two, or three representative elements with the fixed Weierstrass equation. We fix the Weiestrass equations for all supersingular j-invariants over $\overline{\mathbb{F}}_p$ once and for all, and let $[(E, G)]$ denote the equivalence class in $|\mathcal{S}_N|$ specified by:

$$[(E, G)] = \{(E, \alpha(G))\}_{\alpha\in \mathrm{Aut}(E)}.$$

Moreover, we can choose all of these Weierstrass equations to be defined over $\mathbb{F}_{p^2}$, since $j(E) \in \mathbb{F}_{p^2}$ for every supersingular j-invariant.

We begin by defining a dualizing involution on the equivalence classes $[(E, G)] \in |\mathcal{S}_N|$: For every element $[(E, G)] \in |\mathcal{S}_N|$, we form the associated family $\{\eta \circ \varphi_G\}_{\eta\in \mathrm{Aut}(E')}$ of isogenies from E with kernel equal to G, where $\varphi_G : E \to E/G$ is a fixed representative isogeny. Consider the set of kernels

$$\{\ker \widehat{\eta \circ \varphi_G}\}_{\eta\in \mathrm{Aut}(E/G)} = \{\ker(\widehat{\varphi}_G \circ \widehat{\eta})\}_{\eta\in \mathrm{Aut}(E/G)} = \{\widehat{\eta}^{-1}(\ker(\widehat{\varphi}_G))\}_{\eta\in \mathrm{Aut}(E')}.$$

Let $\widehat{G} := \ker(\widehat{\varphi}_G)$. Since $\mathrm{Aut}(E/G)$ is a group, $\{\widehat{\eta}^{-1}\widehat{G})\}_{\eta\in \mathrm{Aut}(E/G)} = \{\eta(\widehat{G})\}_{\eta\in \mathrm{Aut}(E/G)}$. If $j(E/G) \neq 0, 1728$, then $\mathrm{Aut}(E/G) = \{[\pm 1]\}$, and $\eta(\widehat{G}) = \widehat{G}$, since the automorphisms $[\pm 1]$ fix subgroups. If $j(E/G) = 0, 1728$, it is possible that $\eta(\widehat{G}) \neq \widehat{G}$. The set $\{\eta(\widehat{G})\}_{\eta\in \mathrm{Aut}(E/G)}$ is a single orbit under the action of $\mathrm{Aut}(E/G)$, so we can define a dualizing action on the set of equivalence classes $|\mathcal{S}_N|$:

Definition 4.1 (Dualizing Involution on $|\mathcal{S}_N|$)**.**

$$D([(E, G)]) := [(E/G, \widehat{G})],$$

where $\varphi_G : E \to E/G$ is an isogeny with kernel G, and $\widehat{G}$ denotes the kernel of the dual isogeny $\widehat{\varphi}_G : E/G \to E$.

Lemma 4.2. The dualizing involution D is a well-defined involution on $|\mathcal{S}_N|$.

Proof. Take $(E, G), (E, \alpha(G))$, for any $\alpha \in \mathrm{Aut}(E)$. These pairs lie in the same equivalence class $[(E, G)] \in |\mathcal{S}_N|$. We need to show that $[(E/G, \widehat{G})] = [(E/\alpha(G), \widehat{\alpha(G)})]$, where $\widehat{\alpha(G)} = \ker \widehat{\varphi}_{\alpha(G)}$. Begin by noticing that $\ker \varphi_{\alpha(G)} = \alpha(\ker(\varphi_G))$, so we must have $\varphi_{\alpha(G)} = \eta \circ \varphi_G \circ \alpha^{-1}$, where η is an automorphism of E/G. Taking the dual, we have $\widehat{\varphi}_{\alpha(G)} = \widehat{\alpha^{-1}} \circ \widehat{\varphi}_G \circ \widehat{\eta}$. Since $\widehat{\alpha^{-1}}$ is an automorphism, we have:

$$\begin{aligned}\widehat{\alpha(G)} &= \ker(\widehat{\varphi}_{\alpha(G)})\\ &= \ker(\widehat{\varphi}_G \circ \widehat{\eta})\\ &= \widehat{\eta}^{-1}(\ker(\widehat{\varphi}_G))\\ &= \widehat{\eta}^{-1}(\widehat{G}).\end{aligned}$$

Since $\widehat{\eta}^{-1} \in \mathrm{Aut}(E/G)$, we have $[(E/G, \widehat{G})] = [(E/G, \widehat{\alpha(G)})]$ and D is well-defined on $|\mathcal{S}_N|$.

$$\begin{tikzcd}
E \arrow[r, "\alpha"] \arrow[d, "\pi_p^E"'] & E \arrow[d, "\pi_p^E"] \\
E^p \arrow[r, dashed, "\beta"'] & E^p
\end{tikzcd}$$

FIGURE 4.1. Behavior of p-power Frobenius composed with an automorphism.

To see that D is an involution, we check that $D(D([(E,G)])) = [(E,G)]$. By the definition of D, $D(D([(E,G)])) = D([(E/G,\widehat{G})])$. The isogeny $\widehat{\varphi}_G : E/G \to E$ has dual φ_G with $\ker \varphi_G = G$, so we have $D(D([(E,G)])) = [(E,G)]$. □

The p-power Frobenius map $\pi_p^E : E \to E^p$ defines another involution map F_p on supersingular elliptic curves with level-N structure in the following manner:

$$F_p(E,G) := (E^p, G^p),$$

where E^p is the codomain of $\pi_p^E : E \to E^p$ and $G^p = \pi_p^E(G)$. Lemma 4.4 shows that this definition also gives an involution F_p on the set of equivalence classes $|\mathcal{S}_N|$:

Definition 4.3 (Frobenius Involution on $|\mathcal{S}_N|$)**.**

$$F_p([(E,G)]) := [(E^p, G^p)].$$

Lemma 4.4. The Frobenius involution F_p is a well-defined involution on $|\mathcal{S}_N|$.

Proof. Take (E,G), $(E,\alpha(G))$, for any $\alpha \in \mathrm{Aut}(E)$. These pairs lie in the same equivalence class $[(E,G)] \in |\mathcal{S}_N|$. We need to show that $[(E^p,G^p)] = [(E^p,\alpha(G)^p)]$. Consider the diagram in Figure 4.1. In this figure, $\alpha \in \mathrm{Aut}(E)$ implies that $\beta \in \mathrm{Aut}(E^p)$. We have $\pi_p^E \circ \alpha = \beta \circ \pi_p^E$, and in particular $\alpha(G)^p = \beta(G^p)$, so $[(E^p,G^p)] = [(E^p,\alpha(G)^p)]$.

To check $F_p(F_p([(E,G)])) = [(E,G)]$, note that $(E^p)^p = E$, since $E/\mathbb{F}_{p^2}$. Since $\widehat{\pi}_p$ is purely inseparable, it can be written as $\alpha \circ \pi_p^{E/G}$. Then,

$$\pi_p^{E/G}(\pi_p^E(G)) = \pi_p^{E/G}(G^p) = \alpha^{-1}(G),$$

and we have $F_p(F_p([(E,G)])) = [(E,G)]$, as desired. □

Lemma 4.5. Let (E,G) be a supersingular elliptic curve with level-N structure G. We have $\varphi_G : E \to E/G$ with $\ker \varphi_G = G$ and $\varphi_{G^p} : E^p \to (E/G)^p$ with $\ker \varphi_{G^p} = G^p$. Let π_p^E denote the p-power Frobenius morphism $\pi_p^E : E \to E^p$ and let $\pi_p^{E/G}$ denote the p-power Frobenius morphism $\pi_p^{E/G} : E/G \to (E/G)^p$. Then,

$$\varphi_{G^p} \circ \pi_p^E = \alpha \circ \pi_p^{E/G} \circ \varphi_G,$$

where $\alpha \in \mathrm{Aut}((E/G)^p)$.

Proof. Since $\ker \varphi_G \subset \ker(\varphi_{G^p} \circ \pi_p^E)$ and φ_G is a separable isogeny, by [Sil09, Corollary III.4.11] there exists a unique isogeny $\lambda : E/G \to (E/G)^p$ such that

$$\varphi_{G^p} \circ \pi_p^E = \lambda \circ \varphi_G.$$

By degree comparison on the left and right sides above, we see λ must be degree-p and inseparable degree-p, and so $\lambda = \alpha \circ \pi_p^{E/G}$ for some $\alpha \in \mathrm{Aut}((E/G)^p)$, where $\pi_p^{E/G}$ denotes the p-power Frobenius map on E/G. □

$$\begin{tikzcd}
E \arrow[r, "\varphi_G"] \arrow[d, "\pi_p^E"'] & E/G \arrow[d, "\pi_p^{E/G}"] \\
E^p \arrow[r, "\varphi_{G^p}"'] & E^p/G^p
\end{tikzcd}$$

(A) Commutative diagram proven in Lemma 4.5, up to automorphism on $(E/G)^p = E^p/G^p$.

$$\begin{tikzcd}
E & E/G \arrow[l, "\widehat{\varphi}_G"'] \\
E^p \arrow[u, "\widehat{\pi}_p^E"] & E^p/G^p \arrow[l, "\widehat{\varphi}_{G^p}"] \arrow[u, "\widehat{\pi}_p^{E/G}"']
\end{tikzcd}$$

(B) Commutative diagram obtained by taking duals of isogenies in Figure 4.2a.

Figure 4.2

The above lemma implies the commutative diagram in Figure 4.2. In particular, we note that $E^p/G^p = (E/G)^p$, up to automorphism.

Lemma 4.6.

$$D(F_p([(E,G)])) = F_p(D([(E,G)])).$$

Proof. By definition, on the right side of the equation we have:

$$F_p(D([(E,G)])) = F_p([(E/G,\widehat{G})]) = [((E/G)^p, \widehat{G}^p)].$$

Also by definition, on the left side of the equation we have:

$$D(F_p([(E,G)])) = D([(E^p, G^p)]) = [(E^p/G^p, \widehat{G^p})].$$

To see that $(E/G)^p = E^p/G^p$ and $\widehat{G}^p = \widehat{G^p}$, see Figure 4.2 which immediately gives $(E/G)^p = E^p/G^p$, up to automorphism. For the kernels, we use the fact that the p-power Frobenius isogeny and its dual both have trivial kernel together with Lemma 4.5:

$$\begin{aligned}
\widehat{G^p} &= \ker \widehat{\varphi}_{G^p} \\
&= \ker \widehat{\pi}_p^E \circ \widehat{\varphi}_{G^p} \\
&= \ker \widehat{\varphi}_G \circ \widehat{\pi}_p^{E/G} \\
&= \pi_p^{E/G}(\ker \widehat{\varphi}_G) \\
&= (\ker \widehat{\varphi}_G)^p \\
&= \widehat{G}^p.
\end{aligned}$$

□

4.2. **Fibers of $\mathcal{O}(\cdot,\cdot)$.** Recall from the discussion at the beginning of Section 4.1 that we fix a Weierstrass equation over $\mathbb{F}_{p^2}$ for each supersingular j-invariant and use this curve to determine our representatives of the equivalence classes $[(E,G)]$. The involutions D, and F_p descend to well-defined involutions on isomorphism classes of Eichler orders via the map $\mathcal{O}(\cdot,\cdot)$. We will show that these descended involutions are both trivial.

Lemma 4.7. The map $\mathcal{O}(\cdot,\cdot) \circ D$ is the identity map on isomorphism classes of Eichler orders.

Proof. For any $(E/G, \alpha(\widehat{G})) \in D([(E,G)])$ where $\alpha \in \mathrm{Aut}(E)$, we wish to show that $\mathcal{O}(E/G, \alpha(\widehat{G})) = \mathcal{O}(E,G)$. Since the map $\mathcal{O}(\cdot,\cdot)$ is well-defined on equivalence classes, we may simply take $\alpha = [1]$. By Proposition 3.4,

$$\mathcal{O}(E,G) = \mathrm{End}(E) \cap \left(\frac{1}{\deg \varphi_G} \widehat{\varphi}_G \mathrm{End}(E/G) \varphi_G\right) \subseteq B_{p,\infty}^E,$$

where $\varphi_G : E \to E/G$ is an isogeny with $\ker \varphi_G = G$. Likewise,

$$\mathcal{O}(E/G, \widehat{G}) = \mathrm{End}(E/G) \cap \left(\frac{1}{\deg \widehat{\varphi}_G} \varphi_G \mathrm{End}(E) \widehat{\varphi}_G \right) \subseteq B_{p,\infty}^{E/G}.$$

The map from $\mathrm{End}(E/G) \to B_{p,\infty}^{E}$ is given by conjugation by $\frac{1}{\deg \varphi_G} \widehat{\varphi}_G(-)\varphi_G$. Mapping $\mathcal{O}(E/G, \widehat{G})$ into $B_{p,\infty}^{E}$ by this map, we have

$$\mathcal{O}(E/G, \widehat{G}) \cong \left(\frac{1}{\deg \varphi} \widehat{\varphi}_G \mathrm{End}(E/G) \varphi_G \right) \cap \mathrm{End}(E) = \mathcal{O}(E, G).$$

□

Lemma 4.8. The map $\mathcal{O}(\cdot, \cdot) \circ F_p$ is the identity map on isomorphism classes of Eichler orders.

Proof. For any $(E^p, \alpha(G^p)) \in F_p([(E, G)])$ where $\alpha \in \mathrm{Aut}(E^p)$, we wish to show that $\mathcal{O}(E^p, \alpha(G^p)) = \mathcal{O}(E, G)$. Since the map $\mathcal{O}(\cdot, \cdot)$ is well-defined on equivalence classes, we may simply take $\alpha = [1]$. By Proposition 3.4,

$$\mathcal{O}(E, G) = \mathrm{End}(E) \cap \left(\frac{1}{\deg \varphi_G} \widehat{\varphi}_G \mathrm{End}(E/G) \varphi_G \right) \subseteq B_{p,\infty}^{E},$$

where $\varphi_G : E \to E/G$ is an isogeny with $\ker \varphi_G = G$. Likewise,

$$\mathcal{O}(E^p, G^p) = \mathrm{End}(E^p) \cap \left(\frac{1}{\deg \varphi_{G^p}} \widehat{\varphi}_{G^p} \mathrm{End}((E/G)^p) \varphi_{G^p} \right) \subseteq B_{p,\infty}^{E^p},$$

where $\varphi_{G^p} : E^p \to (E/G)^p$ is an isogeny with $\ker \varphi_{G^p} = G^p = \pi_p(G)$, where π_p is the p-power Frobenius isogeny from E to E^p. By Lemma 4.5, we have a relationship between φ_G and φ_{G^p}:

$$\varphi_{G^p} \circ \pi_p^E = \lambda \circ \varphi_G,$$

where $\lambda = \alpha \circ \pi_p^{E/G}$ for some $\alpha \in \mathrm{Aut}((E/G)^p)$.

Next, we map $\mathcal{O}(E^p, G^p)$ into $B_{p,\infty}^{E}$. Since $\pi_p : E \to E^p$, we have $\widehat{\pi}_p : E^p \to E$. This map gives an isomorphism $\frac{1}{p}\widehat{\pi}_p \mathrm{End}(E^p) \pi_p = \mathrm{End}(E)$. Conjugating $\mathcal{O}(E^p, G^p)$ by this map, we obtain the image of $\mathcal{O}(E^p, G^p)$ in $B_{p,\infty}^{E}$:

$$\begin{aligned}
\mathcal{O}(E^p, G^p) &= \frac{1}{p}\widehat{\pi}_p \left(\mathrm{End}(E^p) \cap \left(\frac{1}{\deg \varphi_{G^p}} \widehat{\varphi}_{G^p} \mathrm{End}((E/G)^p) \varphi_{G^p}\right) \right) \pi_p \subseteq B_{p,\infty}^{E} \\
&= \frac{1}{p}\widehat{\pi}_p \mathrm{End}(E^p) \pi_p \cap \left(\frac{1}{p \deg \varphi_{G^p}} \widehat{\varphi_{G^p} \circ \pi_p} \mathrm{End}((E/G)^p) \varphi_{G^p} \circ \pi_p\right) \\
&= \mathrm{End}(E) \cap \left(\frac{1}{p \deg \varphi_G} \widehat{\lambda \circ \varphi_G} \mathrm{End}((E/G)^p) \lambda \circ \varphi_G\right)
\end{aligned}$$

Since $\varphi_{G^p} \circ \pi_p = \lambda \circ \varphi_G$, $\lambda : E/G \to (E/G)^p$ gives:

$$\frac{1}{\deg \lambda} \widehat{\lambda} \mathrm{End}((E/G)^p) \lambda = \mathrm{End}(E/G),$$

and we have recovered $\mathcal{O}(E^p, G^p) = \mathcal{O}(E, G)$. □

Theorem 4.9. The fiber above $\mathcal{O}(E, G)$ along the map $\mathcal{O}(\cdot, \cdot)$ contains precisely the equivalence classes $[(E, G)]$, $D([(E, G)])$, $F_p([(E, G)])$, and $D(F_p([(E, G)]))$.

Proof. Lemmas 4.7 and 4.8 show that the fiber above $\mathcal{O}(E,G)$ contains $[(E,G)]$, $D([(E,G)])$, $F_p([(E,G)])$, and $D(F_p([(E,G)]))$. To see that these are the only possibilities, consider the choices made in the proof of Proposition 3.6. The Eichler order $\mathcal{O}(E,G)$ uniquely determines an intersection of maximal orders $\mathcal{O}(E,G) = \mathcal{O}_1 \cap \mathcal{O}_2$. By the Deuring correspondence (see Section 2.1), $\mathcal{O}_1$ must be one of the following:

(i) $\mathcal{O}_1 = \mathrm{End}(E)$
(ii) $\mathcal{O}_1 = \mathrm{End}(E^p)$
(iii) $\mathcal{O}_1 = \mathrm{End}(E/G)$
(iv) $\mathcal{O}_1 = \mathrm{End}((E')^p)$.

As in the proof of Proposition 3.6, the intersection $\mathcal{O}_1 \cap \mathcal{O}_2$ uniquely determines an ideal I of norm N with left order $\mathcal{O}_1$ and right order $\mathcal{O}_2$. This ideal I determines an isogeny as in Section 2.2. Depending on the choice of $\mathcal{O}_1$ above, the isogeny will be one of the following:

(i) $\mathcal{O}_1 \cong \mathrm{End}(E)$: The isogeny is $\varphi_G : E \to E/G$ with
$$G = \cap_{\alpha \in I} E[\alpha],$$
as defined in Proposition 3.6.
(ii) $\mathcal{O}_1 \cong \mathrm{End}(E^p)$: We obtain an isogeny $\varphi : E^p \to (E/G)^p$, where $F_p([(E,G)]) = [(E^p, \ker\varphi)] = [(E^p, G^p)]$.
(iii) $\mathcal{O}_1 \cong \mathrm{End}(E/G)$: We obtain an isogeny $\varphi : E/G \to E$, where $D([(E,G)]) = [(E/G, \ker\varphi)]$.
(iv) $\mathcal{O}_1 \cong \mathrm{End}((E/G)^p)$.: We obtain an isogeny $\varphi : (E/G)^p \to E^p$, where $D(F_p([(E,G)])) = [((E/G)^p, \ker\varphi)]$.

□

4.3. **Explicit Fibers for Primes $p \equiv 1 \pmod{12}$.** Recall from the discussion at the beginning of Section 4.1 that we fix a Weierstrass equation over $\mathbb{F}_{p^2}$ for each supersingular j-invariant and use this curve to determine our representatives of the equivalence classes $[(E,G)]$.

In this section, fix a prime $p \equiv 1 \pmod{12}$. Each equivalence class $[(E,G)] \in |\mathcal{S}_N|$ has precisely one element corresponding to our fixed Weierstrass equation, so we will simply denote $[(E,G)]$ by (E,G). By Theorem 4.9, the fiber along $\mathcal{O}(\cdot,\cdot)$ above $\mathcal{O}(E,G)$ contains four, not necessarily distinct, pairs in $|\mathcal{S}_N|$:

(1) (E,G),
(2) $(E/G, \widehat{G})$,
(3) (E^p, G^p),
(4) $((E/G)^p, \widehat{G}^p)$,

with the notation from Theorem 4.9.

Example 4.10 ($p = 61$, $N = 2$)**.** Let $\mathbb{F}_{61^2} = \mathbb{F}_{61}[s]/(s^2 + 60s + 2)$. Table 1 lists supersingular j-invariants and Weierstrass equations.

Table 2 sorts the pairs (E,G) into sets of the form $\{(E,G), (E/G, \widehat{G}), (E^p, G^p), ((E/G)^p, \widehat{G}^p)\}$. The last column indicates the size of the set $\{(E,G), (E/G, \widehat{G}), (E^p, G^p), ((E/G)^p, \widehat{G}^p)\}$, i.e., the size of the fiber above the corresponding image under $\mathcal{O}(\cdot,\cdot)$.

Proposition 4.11 (Fibers of size 1)**.** The fiber above $\mathcal{O}(E,G)$ is size one if and only if G is the kernel of a degree-N self-dual endomorphism of E.

$j(E)$	Weierstrass Equation
9	$E_9 : y^2 = x^3 + 53x + 18$
41	$E_{41} : y^2 = x^3 + 6x + 34$
50	$E_{50} : y^2 = x^3 + 14x + 36$
$20s + 32$	$E_{20s+32} : y^2 = x^3 + (30s + 47)x + (48s + 49)$
$41s + 52$	$E_{41s+52} : y^2 = x^3 + (31s + 16)x + (13s + 36)$

Table 1. j-invariants and Weierstrass equations for the computations of Example 4.10.

(E, G)	$(E/G, \widehat{G})$	(E^p, G^p)	$((E/G)^p, \widehat{G}^p)$	$\lvert\text{Set}\rvert$
$(E_{50}, \langle(59, 0)\rangle)$	$(E_{41}, \langle(4, 0)\rangle)$	$(E_{50}, \langle(59, 0)\rangle)$	$(E_{41}, \langle(4, 0)\rangle)$	2
$(E_{50}, \langle(60s + 32, 0)\rangle)$	$(E_{20s+32}, \langle(2s + 58, 0)\rangle)$	$(E_{50}, \langle(s + 31, 0)\rangle)$	$(E_{41s+52}, \langle(59s + 60, 0)\rangle)$	4
$(E_{41}, \langle(43s + 7, 0)\rangle)$	$(E_{41}, \langle(18s + 50, 0)\rangle)$	$(E_{41}, \langle(18s + 50, 0)\rangle)$	$(E_{41}, \langle(43s + 7, 0)\rangle)$	2
$(E_{20s+32}, \langle(40s + 6, 0)\rangle)$	$(E_{41s+52}, \langle(21s + 46, 0)\rangle)$	$(E_{41s+52}, \langle(21s + 46, 0)\rangle)$	$(E_{20s+32}, \langle(40s + 6, 0)\rangle)$	2
$(E_{20s+32}, \langle(19s + 58, 0)\rangle)$	$(E_9, \langle(50s + 2, 0)\rangle)$	$(E_{41s+52}, \langle(42s + 16, 0)\rangle)$	$(E_9, \langle(11s + 52, 0)\rangle)$	4
$(E_9, \langle(7, 0)\rangle)$	$(E_9, \langle(7, 0)\rangle)$	$(E_9, \langle(7, 0)\rangle)$	$(E_9, \langle(7, 0)\rangle)$	1

Table 2. Table of the sets $\{(E, G), (E/G, \widehat{G}), (E^p, G^p), ((E/G)^p, \widehat{G}^p)\} \subset |\mathcal{S}_N|$ for $p = 61$, $N = 2$

Proof. If the fiber above $\mathcal{O}(E, G)$ is size one, then $(E, G) = (E/G, \widehat{G}) = (E^p, G^p) = ((E/G)^p, \widehat{G}^p)$. Then E is defined over $\mathbb{F}_p$, and G is the kernel of an endomorphism $\varphi_G : E \to E/G$ whose dual has kernel $\widehat{G} = G$, and so φ_G is self-dual up to post-composition with an automorphism.

For the reverse direction, if G is the kernel of a degree-N endomorphism defined over $\mathbb{F}_p$, then $E = E^p = E/G$ and $G = G^p$. Since φ_G is self-dual, we also have $\widehat{G} = G$. □

Remark 4.12. In Proposition 4.11, the endomorphism φ_G with kernel G must be defined over a nontrivial extension of $\mathbb{F}_p$. This is because $\operatorname{End}_{\mathbb{F}_p}(E) \cong \mathbb{Z}[\sqrt{-p}]$, and if φ_G were an $\mathbb{F}_p$-endomorphism of $E/\mathbb{F}_p$, then $\mathbb{Z}[\sqrt{-p}]$ would contain an element of norm N. Since $N < p$ and the norm form equation of $\mathbb{Z}[\sqrt{-p}]$ is $x^2 + py^2$, there is no such element. Since $G = G^p$, it must be that G determines an isogeny ψ_G to the quadratic twist of the curve E, which we denote E^t. Of course E and E^t are isomorphic by some map $\eta : E^t \to E$, but by the definition of quadratic twist η is defined over $\mathbb{F}_{p^2}$ and in particular η is not defined over $\mathbb{F}_p$. Then, $\varphi_G = \eta \circ \psi_G$. See Figure 4.3.

$$\begin{tikzcd}
E \arrow[r, "\psi_G/\mathbb{F}_p"] \arrow[dr, "\varphi_G/\mathbb{F}_{p^2}"'] & E^t \arrow[d, "\eta/\mathbb{F}_{p^2}"] \\
 & E
\end{tikzcd}$$

Figure 4.3. Diagram to accompany field of definition discussion in Remark 4.12

Proposition 4.13 (Fibers of size 2)**.** The fiber above $\mathcal{O}(E, G)$ is size two if and only if it corresponds to one of the following cases:

(1) $(E, G) = (E^p, G^p) \neq (E/G, \widehat{G}) = ((E/G)^p, \widehat{G}^p)$,

(2) $(E,G)=(E/G,\widehat{G})\neq(E^p,G^p)=((E/G)^p,\widehat{G}^p)$,
(3) $(E,G)=((E/G)^p,\widehat{G}^p)\neq(E/G,\widehat{G})=(E^p,G^p)$.

These cases correspond to (respectively):

(1) Two options:
   (a) If $E\neq E/G$, then G is the kernel of an isogeny $E\to E/G$ over $\mathbb{F}_p$ between two distinct curves defined over $\mathbb{F}_p$.
   (b) If $E=E/G$, then $G\neq\widehat{G}$ and G is the kernel of an endomorphism $\varphi_G : E\to E$ and φ_G is defined over $\mathbb{F}_p$ and is not self-dual.

(2) G is the kernel of a self-dual endomorphism of E, and E is not defined over $\mathbb{F}_p$.

(3) Two options:
   (a) If $E=E^p$, then $G\neq G^p$ and G is the kernel of an endomorphism which is not defined over $\mathbb{F}_p$ of a curve which is defined over $\mathbb{F}_p$.
   (b) If $E\neq E^p$, then G is the kernel of an isogeny between two distinct curves whose j-invariants are Frobenius conjugate.

Proof. (1) If $E\neq E/G$, then G is the kernel of an isogeny in $\operatorname{Hom}_{\mathbb{F}_p}(E,E/G)$.

If $E=E/G$ but $G\neq\widehat{G}$, then $G/\mathbb{F}_p$ defines an endomorphism $\varphi_G : E\to E$ which is not self-dual. Since the norm form of $\operatorname{End}_{\mathbb{F}_p}(E)\cong\mathbb{Z}[\sqrt{-p}]$ (see 2.4) does not represent the integer N, this isogeny is not an endomorphism of $E/\mathbb{F}_p$.

(2) $E=E/G$ tells that G defines an endomorphism of the $\overline{\mathbb{F}}_p$-isomorphism class of E. This endomorphism cannot be defined over $\mathbb{F}_p$, as $G\neq G^p$.

(3) If E is defined over $\mathbb{F}_p$, then $E=E^p=E/G=(E/G)^p$. Then $G\neq G^p$, and G must correspond to an endomorphism which is not defined over $\mathbb{F}_p$.

If E is not defined over $\mathbb{F}_p$, then $E/G=E^p$ shows that G is the kernel of an isogeny from E to its conjugate.

□

If none of the special cases of the previous two propositions occur, then the fibers are of size 4, as described in Theorem 4.9. Fibers of size 3 are not possible by the symmetry of the involutions D and F_p defined in Section 4.1.

The following proposition characterizes the fiber size on the quaternion side.

Proposition 4.14. *Let $\mathcal{O}$ be an Eichler order of $B_{p,\infty}$ of prime level N. The size of the two-sided ideal class group of $\mathcal{O}$ is equal to the number of distinct pairs (E,G) of $|\mathcal{S}_N|$ for which $\mathcal{O}(E,G)\cong\mathcal{O}$.*

Proof. By [Voi21, 23.3.19], above each of the two primes p and N dividing the discriminant of $\mathcal{O}$, we get a unique two-sided maximal ideal of order two in the two-sided ideal class group of $\mathcal{O}$. Let $\mathfrak{p}$ be the two-sided ideal of $\mathcal{O}$ such that $\mathfrak{p}^2=p\mathcal{O}$, and let $\mathfrak{n}$ be the two-sided ideal of $\mathcal{O}$ such that $\mathfrak{n}^2=N\mathcal{O}$. The size of the two-sided ideal class group of $\mathcal{O}$ is either 1, 2, or 4, as each of these ideals has at most order two. To see how this number relates to the identification of elements of $|\mathcal{S}_N|$, consider the possible coincidences of $(E,G),(E^p,G^p),(E/G,\widehat{G}),((E/G)^p,\widehat{G}^p)$:

- If $(E,G)=(E^p,G^p)$, then the p-power Frobenius map is an endomorphism, and the ideal $\mathfrak{p}$ is principally generated by that endomorphism. As long as no other coincidences of $|\mathcal{S}_N|$ pairs occur, this case corresponds to the two sided ideal class group of the Eichler order being size 2, generated by [1] and $[\mathfrak{n}]$.
- If $(E,G)=(E/G,\widehat{G})$, then $\mathfrak{n}$, the two-sided ideal corresponding to $\varphi_G : E\to E/G$, is principally generated by the endomorphism φ_G. As long as no other coincidences of $|\mathcal{S}_N|$

pairs occur, this case corresponds to the two sided ideal class group of the Eichler order being size 2, generated by [1] and $[\mathfrak{p}]$.

- If $(E, G) = ((E/G)^p, \widehat{G}^p)$, then $(E^p, G^p) = (E/G, \widehat{G})$. This means that the Frobenius map and φ_G have the same domain and codomain, and thus the corresponding ideals $\mathfrak{p}$ and $\mathfrak{n}$ belong to the same class. As long as no other coincidences of $|\mathcal{S}_N|$ pairs occur, this case corresponds to the two sided ideal class group of the Eichler order being size 2, generated by [1] and $[\mathfrak{n}] = [\mathfrak{p}]$. This is the case of N-isogenous conjugate pairs.
- Finally, if $(E, G) = (E^p, G^p) = (E/G, \widehat{G}) = ((E/G)^p, \widehat{G}^p)$, then $\mathfrak{p}$ and $\mathfrak{n}$ are both principal ideals, yielding a two-sided ideal class group of size one.

□

4.4. **Fibers for Primes** $p \not\equiv 1 \pmod{12}$**.** The list of elements of $|\mathcal{S}_N|$ in the fiber above $\mathcal{O}(E, G)$ is more complicated by the presence of automorphisms of E if $j(E) = 0$ or 1728. The list of these elements provided in Theorem 4.9 may contain more than four distinct elements, and the sizes of the fibers above a given $\mathcal{O}(E, G)$ may be a variety of sizes between one and eight. We provide an example, but leave more detailed classification to the reader.

Example 4.15 ($p = 23$, $N = 3$)**.** We describe the level-3 structure on supersingular elliptic curves defined over $\overline{\mathbb{F}}_{23}$. Let $\mathbb{F}_{23^2} = \mathbb{F}_{23}[s]/(s^2 + 21s + 5)$. There are three supersingular j-invariants, and we use the Weierstrass models given in Table 3.

$j(E)$	Weierstrass Equation
0	$E_0 : y^2 = x^3 + 1$
3	$E_3 : y^2 = x^3 + 6x$
19	$E_{19} : y^2 = x^3 + 8x + 1$

Table 3. j-invariants and Weierstrass equations for the computations in Example 4.15

There are five fibers of $\mathcal{O}(\cdot, \cdot)$, which we list and describe below:

(1) $\{(E_0, \langle(0, 1)\rangle)\}$:
The group $\langle(1, 0)\rangle \subset E_0[3]$ defines a 3-isogeny to the supersingular elliptic curve $y^2 = x^3+19$, which also has j-invariant 0 and is the quadratic twist of $y^2 = x^3 + 1$.

(2) $\{(E_0, \langle(20, 15s+8)\rangle), (E_0, \langle(12s+1, 155s+8)\rangle), (E_0, \langle(11s+2, 15s+8)\rangle), (E_3, \langle(9, 1)\rangle), (E_3, \langle(14, 11s+12)\rangle)\}$:
The three groups $\langle(20, 15s+8)\rangle, \langle(12s+1, 155s+8)\rangle, \langle(11s+2, 15s+8)\rangle \subset E_0[3]$ map to each other under the automorphisms of E_0. They define 3-isogenies to E_3, which also has extra automorphisms. The three 3-isogenies $E_0 \to E_3$ all have duals with kernel $\langle(9, 1)\rangle$, and post-composition with a different automorphism of E_0. The groups $\langle(9, 1)\rangle, \langle(14, 11s + 12)\rangle \subset E_3[3]$ map to each other under the automorphisms of E_3. The dual of the 3-isogeny $E_3 \to E_0$ with kernel $\langle(14, 11s + 12)\rangle$ has kernel $\langle(11s + 2, 15s + 8)\rangle$.

(3) $\{(E_3, \langle(11s + 12, 10s + 10)\rangle), (E_3, \langle(12s + 11, 13s + 7)\rangle), (E_{19}, \langle(16, 4)\rangle)\}$:
The groups $\langle(11s + 12, 10s + 10)\rangle, \langle(12s + 11, 13s + 7)\rangle \subset E_3[3]$ map to each other under the automorphisms of E_3 and the p-power Frobenius endomorphism of E_3. They both define isogenies to E_{19}, and their duals each have kernel $\langle(16, 4)\rangle$. The duals differ by post-composition with an automorphism of E_3.

(4) $\{(E_{19}, \langle(20, s+22)\rangle)\}$:
The group $\langle(20, s+22)\rangle \subset E_{19}$ is stable under the p-power Frobenius endomorphism of E_{19}. It defines a self-dual degree-3 endomorphism of E_{19}.

(5) $\{(E_{19}, \langle(12s+16, 8s+19)\rangle), (E_{19}, \langle(11s+17, 15s+12)\rangle)\}$:
The groups $\langle(12s+16, 8s+19)\rangle, \langle(11s+17, 15s+12)\rangle \subset E_{19}[3]$ map to each other under the p-power Frobenius endomorphism of E_{19}. They define endomorphisms of E_{19} which are each others' duals.

5. Counting N-isogenies $E \to E^{(p)}$

We apply the results of Section 4 to provide a new approximate upper bound on the number of N-isogenies between pairs of distinct supersingular elliptic curves with conjugate j-invariants. We contrast this to approximate counts and bounds provided in [CGL09, Lemma 6] and [EHL$^+$20, Theorem 3.9] in Section 5.2.

As in Section 4.1, we fix Weierstrass equations over $\mathbb{F}_{p^2}$ for each supersingular j-invariant and work exclusively with this set of representative curves, instead of isomorphism classes of curves. This is to make our counting statements easier.

Let α_N denote the number of pairs (E, ψ) where $\psi : E \to E^p$ is a degree-N isogeny from E to its p-power Frobenius conjugate E^p. Let $\alpha'_N \leq \alpha_N$ be the count of the subset of pairs (E, ψ) as above with E defined over $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$.

5.1. An Approximate Upper-Bound From Eichler Orders.

Restrict to the case $p \equiv 1 \pmod{12}$ for this section, for ease of fiber size counts. Let $\mathcal{F}_1, \mathcal{F}_2, \mathcal{F}_4$ denote the number of isomorphism classes of Eichler orders whose fibers along $\mathcal{O}(\cdot,\cdot)$ are sizes 1, 2, and 4, respectively. Let T denote the number of isomorphism classes of Eichler orders of level N of $B_{p,\infty}$. Let $\#(\mathbf{S}_p)$ denote the number of supersingular j-invariants over $\overline{\mathbb{F}}_p$.

Proposition 5.1. The following relations hold between the quantities $\mathcal{F}_1, \mathcal{F}_2, \mathcal{F}_4, T, (\#\mathbf{S}_p)$:

$$\mathcal{F}_1 + \mathcal{F}_2 + \mathcal{F}_4 = T \tag{2}$$

$$\mathcal{F}_1 + 2\mathcal{F}_2 + 4\mathcal{F}_4 = (N+1)(\#\mathbf{S}_p). \tag{3}$$

Proof. For (2): every Eichler order of level N has fiber size 1, 2, or 4 along $\mathcal{O}(\cdot,\cdot)$ by Theorem 4.9. For (3): the size of $|\mathcal{S}_N|$ is $(N+1)(\#\mathbf{S}_p)$, and every element of $|\mathcal{S}_N|$ lies in a fiber above some isomorphism class of Eichler order of level N along $\mathcal{O}(\cdot,\cdot)$. □

Combine the equations in Proposition 5.1 to solve for $\mathcal{F}_2$:

$$\mathcal{F}_2 = 2T - \frac{N+1}{2}(\#\mathbf{S}_p) - \frac{3}{2}\mathcal{F}_1. \tag{4}$$

As shown in Proposition 4.11, the fiber size one case corresponds to a rare case. For small N, degree-N endomorphisms are rare. By work of Love and Boneh [LB20], the number of curves with an endomorphism of degree less than or equal to N is $O(N^{3/2})$. Assuming $\mathcal{F}_1 = 0$, we obtain an approximate upper bound for $\mathcal{F}_2$ from Equation (4):

$$2T - \frac{N+1}{2}(\#\mathbf{S}_p). \tag{5}$$

The number of degree-N isogenies between conjugate curves α'_N is also generically counted in $\mathcal{F}_2$. To see this, begin by noting that if E is defined over $\mathbb{F}_{p^2}$ and not $\mathbb{F}_p$, then the fiber above $\mathcal{O}(E, G)$ is either of size 2 or 4. Furthermore, if G is the kernel of an N-isogeny from E to E^p, then $E/G = E^p$.

From here, either $G^p = \widehat{G}$ or $G^p \neq \widehat{G}$. In the first case, the fiber above $\mathcal{O}(E, G)$ is size 2. If $G^p \neq \widehat{G}$, then there are two separate degree-N isogenies from E^p to E: one with kernel G^p and the other with kernel $\widehat{G}$. This corresponds to a double-edge in the N-isogeny graph, which is a rare occurrence (as discussed in [ACNL$^+$21]). Therefore, Equation (5) gives an approximate upper-bound for the number of conjugate pairs of supersingular curves over $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$ connected by an N-isogeny, namely $\alpha'_N/2$. We conclude that an approximate upper-bound for α'_N is:

$$4T - (N+1)(\#\mathbf{S}_p). \tag{6}$$

This approximate upper-bound for α'_N can be compared with the data computed in [ACNL$^+$21], which we discuss in Section 5.2.

5.2. **Comparison With Other Bounds.** The author's first interest in the question of counting N-isogenous conjugate curves began with research as part of the collaborative work in [ACNL$^+$21]. We wished to identify the frequency of *mirror paths*, which are invariant under the Frobenius conjugate. These mirror paths necessarily have a central point of symmetry, which either corresponds to a j-invariant defined over $\mathbb{F}_p$, or a pair of N-isogenous conjugate j-invariants both defined over $\mathbb{F}_{p^2}$ and not $\mathbb{F}_p$. We posed a question about counting the number of N-isogenous conjugate pairs, as described in the second mirror path scenario. This corresponds to estimating α'_N. In [ACNL$^+$21], we computed α'_N for a wide range of values p. Most other work focuses on estimations of the value of α_N.

Subsequently, [EHL$^+$20] considered the question of counting the number α_N of supersingular j-invariants with an N-isogeny to their p-power Frobenius conjugate. They pointed out that an upper-bound for this value, which they denote $|S^p|$, could be computed using [CGL09, Lemma 6], which provides an approximation for this value. The authors also provided a lower-bound [EHL$^+$20, Theorem 3.9]:

$$|S^p| \geq \frac{\sqrt{Np}}{6(N+1)\log\log(Np)}.$$

This lower-bound is an easily computed function which provides a lower-bound on the class number of the order $\mathbb{Z}[\sqrt{-Np}]$. In Figure 5.1, which is a lower bound for α_N. We plot this rational function for $N = 3$ against the data for 3-isogenous conjugates provided in [ACNL$^+$21] and the upper-bound for α'_3 in Equation (6) is plotted.

The big-O notation approximation provided in [CGL09, Lemma 6] can be adjusted to give an exact count of N-isogenous conjugate curves. To begin this analysis, we provide the statement of [CGL09, Lemma 6]:

Lemma 5.2 (Lemma 6 [CGL09])**.** Let i be a non-negative integer. The number $\alpha(i)$ of supersingular j-invariants such that $\mathrm{dist}_G(j, j^p) \leq i$ is the number of pairs (E, g) consisting of a supersingular elliptic curve E and an endomorphism g of E of degree $p \cdot \ell^j$, $j \leq i$, up to isomorphism. Assume that $i \leq \log_\ell(p/4)$. Then

$$\alpha(i) = \ell^{i/2}\widetilde{O}(\sqrt{p}).$$

Inspired by Lemma 5.2, we prove the precise value of α_N. Chenu and Smith [CS21, Theorem 2] provide an alternative proof of this proposition.

Proposition 5.3. The value $2\alpha_N$ is equal to the number of pairs consisting of a supersingular elliptic curve E and an embedding $\mathbb{Z}[\sqrt{-pN}]$ into $\mathrm{End}(E)$.

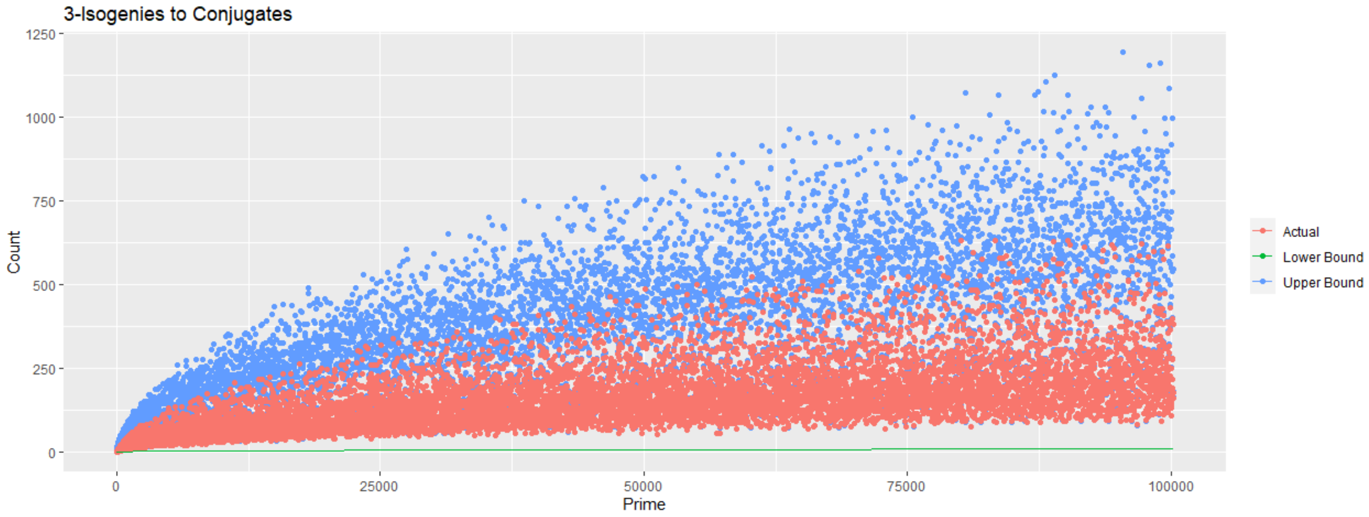


FIGURE 5.1. For primes between 5 and 100000, we plot the actual count α'_3 of 3-isogenies between distinct p-power Frobenius conjugate curves, the upper bound for α'_3 provided in Equation (6), and the lower bound for α_3 provided by [EHL+20]

Furthermore,

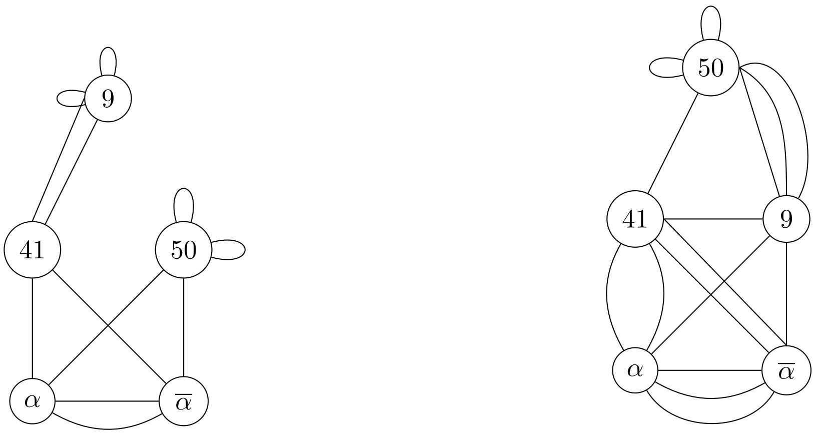
$$2\alpha_N = \begin{cases} |\, \mathcal{C}\ell(\mathbb{Z}[\frac{1+\sqrt{-pN}}{2}])\,| + |\, \mathcal{C}\ell(\mathbb{Z}[\sqrt{-pN}])\,| & \text{if } -pN \equiv 3 \pmod 4 \\ |\, \mathcal{C}\ell(\mathbb{Z}[\sqrt{-pN}])\,| & \text{if } -pN \equiv 1 \pmod 4 \end{cases}$$

The factor of two appears because two embeddings which differ by a factor of -1 on the generator $\sqrt{-pN}$ are counted as distinct, whereas the two isogenies $\psi, -\psi$ are not considered distinct.

Proof. By definition the number $\alpha(1)$ counts pairs (E, h) where E is a supersingular elliptic curve and $h : E^p \to E$ is a degree-N isogeny between E and its conjugate E^p. Every endomorphism of E can be factored into separable and purely inseparable parts. In particular, every endomorphism g of E of degree pN can be factored uniquely into $\pi_p \circ h$, where π_p is the Frobenius map and h is an isogeny of degree N.

$$\begin{tikzcd} E \arrow[r, "\pi_p"] \arrow[rr, bend right, "g"'] & E^p \arrow[r, "h"] & E \end{tikzcd}$$

The data (E, g) is equivalent to the data (E, h). To count pairs (E, g), we are looking to count embeddings of $\mathbb{Z}[\sqrt{-pN}]$ into $\mathrm{End}(E)$. The action of the class group of $\mathbb{Z}[\sqrt{-pN}]$ is free and transitive on a subset of the primitively $\mathbb{Z}[\sqrt{-pN}]$-oriented supersingular elliptic curves, by [Onu21]. By [CS21, Theorem 2], this subset actually contains all primitively $\mathbb{Z}[\sqrt{-pN}]$-oriented supersingular elliptic curves. By this free and transitive action, the number of such embeddings is equal to the class number of $\mathbb{Z}[\sqrt{-pN}]$. The number of primitive embeddings is $\mathbb{Z}[\sqrt{-pN}]$, but if $\mathbb{Z}[\sqrt{-pN}]$ is properly contained in the maximal order of $\mathbb{Q}(\sqrt{-pN})$, then this is not the full picture. If $\mathcal{O}_{\mathbb{Q}(\sqrt{-pN})} = \mathbb{Z}[\frac{1+\sqrt{-pN}}{2}] \supsetneq \mathbb{Z}[\sqrt{-pN}]$, then we will also want to count primitive embeddings of $\mathcal{O}_{\mathbb{Q}(\sqrt{-pN})}$.



(A) $p = 61$, supersingular $N = 3$-isogeny graph (B) $p = 61$, supersingular $N = 5$-isogeny graph

Figure 5.2. Illustrative examples for Proposition 5.3.

The total number of embeddings (and thus, N-isogenies to a conjugate curve) is:

$$\begin{cases} | \mathcal{C}\ell(\mathbb{Z}[\frac{1+\sqrt{-pN}}{2}]) \mid + \mid \mathcal{C}\ell(\mathbb{Z}[\sqrt{-pN}]) \mid & \text{if } -pN \equiv 3 \pmod 4 \\ | \mathcal{C}\ell(\mathbb{Z}[\sqrt{-pN}]) \mid & \text{if } -pN \equiv 1 \pmod 4 \end{cases}$$

Note that this count includes embeddings which differ by an automorphism of the field, in particular the automorphisms ±1. Since the field $\mathbb{Q}(\sqrt{-pN})$ is quadratic, we always have Galois group $\cong \mathbb{Z}/2\mathbb{Z}$. The endomorphisms corresponding to $\pm\sqrt{-pN}$ are not distinct, so we divide this embedding count by two to get the number of pairs $(j(E), \psi)$ where $\psi : E \to E^p$ is an N-isogeny. This divided count is what we see if we look at the supersingular N-isogeny graph. □

Example 5.4 ($-pN \equiv 1 \pmod 4$)**.** Let $p = 61$, $N = 3$. By Proposition 5.3,

$$\alpha_N = \frac{1}{2}|\mathcal{C}\ell(\mathbb{Z}[\sqrt{-61 \cdot 3}])| + \frac{1}{2}\left|\mathcal{C}\ell\left(\mathbb{Z}\left[\frac{1+\sqrt{-61 \cdot 3}}{2}\right]\right)\right| = \frac{8}{2} + \frac{8}{2} = 8.$$

We provide the supersingular 3-isogeny graph over $\overline{\mathbb{F}}_{61}$ in Figure 5.2a. Since $61 \equiv 1 \pmod{12}$, this graph can be presented as undirected by identifying isogenies and their duals. We see the eight 3-isogenies to a conjugate curve:

- Two 3-isogenies $E_{50} \to E_{50}$
- Two 3-isogenies $E_9 \to E_9$
- Two 3-isogenies $E_\alpha \to E_{\overline{\alpha}}$
- Two 3-isogenies $E_{\overline{\alpha}} \to E_\alpha$

Example 5.5 ($-pN \equiv 3 \pmod 4$)**.** Let $p = 61$, $N = 5$. By Proposition 5.3,

$$\alpha_N = \frac{1}{2}|\mathcal{C}\ell(\mathbb{Z}[\sqrt{-61 \cdot 5}])| = \frac{16}{2} = 8.$$

We provide the supersingular 5-isogeny graph over $\overline{\mathbb{F}}_{61}$ in Figure 5.2b. Since $61 \equiv 1 \pmod{12}$, this graph can be presented as undirected by identifying isogenies and their duals. We see the eight 5-isogenies to a conjugate curve:

- Two 5-isogenies $E_{50} \to E_{50}$
- Three 5-isogenies $E_\alpha \to E_{\overline{\alpha}}$
- Three 5-isogenies $E_{\overline{\alpha}} \to E_\alpha$

6. The Category $\mathcal{S}_N$

The Deuring correspondence was rephrased as a categorical equivalence by Kohel [Koh96]. In this categorical version, the supersingular elliptic curve objects are enhanced by the data of a Frobenius isogeny, as are the quaternion objects. Voight [Voi21] presents a variation of this equivalence of categories, without this additional enhancement:

Theorem 6.1 (Theorem 42.3.2 [Voi21])**.** Fix a supersingular elliptic curve E_0 with endomorphism ring O_0. The functor $\mathrm{Hom}(\cdot, E_0)$ defines an equivalence of categories from the category of isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ under isogenies and the category of invertible left-O_0-modules, under nonzero left O_0-module homomorphisms.

We present an equivalence of categories for supersingular elliptic curves with level-N structure.

6.1. Equivalence of Categories.

We begin by defining the categories in question:

Definition 6.2 (Supersingular elliptic curves with level-N structure)**.** Let $\mathcal{S}_N$ denote the category with objects given by pairs (E_1, G_1), where E_1 is a supersingular elliptic curve over $\overline{\mathbb{F}}_p$ up to $\overline{\mathbb{F}}_p$-isomorphism and $G_1 \subset E_1[N]$ is fixed order-N subgroup. A morphism between two objects (E_1, G_1) and (E_2, G_2) is a nonzero isogeny $\psi : E_1 \to E_2$ such that $\psi(G_1) \subseteq G_2$.

We fix $(E, G) \in \mathcal{S}_N$ and the Eichler order $\mathcal{O}(E, G)$ for the remainder of this section. Define the following category:

Definition 6.3 (Invertible left $\mathcal{O}(E, G)$-modules)**.** Let $\mathcal{LM}$ denote the category with objects invertible left $\mathcal{O}(E, G)$-modules. A morphism between objects is given by a nonzero left $\mathcal{O}(E, G)$-module homomorphism.

It is straightforward to check that these are well-defined categories.

Definition 6.4. We let $\mathscr{h}_{(E,G)}$ denote the functor $\mathrm{Hom}(-, (E, G))$, so

$$\mathscr{h}_{(E,G)}(E', G') = \mathrm{Hom}((E', G'), (E, G)).$$

Theorem 6.5 (Equivalence of Categories)**.** Fix a supersingular elliptic curve E defined over $\overline{\mathbb{F}}_p$ and a subgroup $G \subset E[N]$ of prime order N. $\mathscr{h}_{(E,G)}$ is a contravariant functor from the category $\mathcal{S}_N$ to the category $\mathcal{LM}$. This functor defines an equivalence of categories.

Proof. Lemma 6.6 shows that $\mathscr{h}_{(E,G)}$ is well-defined as a functor. To see that $\mathscr{h}_{(E,G)}$ defines an equivalence of categories, it remains to show that $\mathscr{h}_{(E,G)}$ is essentially surjective and fully faithful.

First, we show that $\mathscr{h}_{(E,G)}$ is essentially surjective. Consider the objects I of $\mathcal{LM}$: Since I is an invertible left $\mathcal{O}(E, G)$-module, it is a rank-1 $\mathcal{O}(E, G)$-module. $\mathcal{O}(E, G)$ is rank-4 over $\mathbb{Z}$, so I is also rank-4 over $\mathbb{Z}$. Since I is a rank-1 $\mathcal{O}(E, G)$-module gives a local isomorphism with $\mathcal{O}(E, G)$. This local isomorphism extends to an isomorphism $I \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathcal{O}(E, G) \otimes_{\mathbb{Z}} \mathbb{Q}$, which gives an inclusion of I into $B^E_{p,\infty} := \mathcal{O}(E, G) \otimes_{\mathbb{Z}} \mathbb{Q}$. By [Voi21, Theorem 9.3.6] I is a fractional ideal of $\mathcal{O}(E, G)$ in $B^E_{p,\infty}$. Scaling by an integer prime to N, we can assume I is an integral left ideal of $\mathcal{O}(E, G)$ of norm $\mathrm{Nrd}(I)$. $\mathrm{Nrd}(I)$ must be prime to N, otherwise it would violate the invertibility of the original left $\mathcal{O}(E, G)$-module. By Lemma 6.7, $I = \mathscr{h}_{(E,G)}(E_I, G_I)\varphi_I$ such that $\varphi_I : E \to E_I$ is a degree $\mathrm{Nrd}(I)$ and $\varphi_I(G) \subseteq G_I$. This identification shows $\mathscr{h}_{(E,G)}$ is essentially surjective.

Lastly, we show that $\mathscr{h}_{(E,G)}$ is fully faithful. In particular, we need to show that the map

$$\mathrm{Hom}_{\mathcal{S}_N}((E_{I'}, G_{I'}), (E_I, G_I)) \to \mathrm{Hom}_{\mathscr{LM}}(\mathscr{h}_{(E,G)}(E_I, G_I), \mathscr{h}_{(E,G)}(E_{I'}, G_{I'}))$$

from morphisms in $\mathcal{S}_N$ to morphisms in $\mathscr{LM}$ is bijective. This is accomplished in Lemma 6.9. □

Lemma 6.6. Let $(E', G') \in \mathcal{S}_N$. Then, $\mathscr{h}_{(E,G)}(E', G')$ is a $\mathbb{Z}$-module of rank 4 that is invertible as a left $\mathcal{O}(E, G)$-module under post-composition.

Proof. By [Voi21, Lemma 42.1.11], $\mathrm{Hom}(E', E)$ is a rank 4 $\mathbb{Z}$-module. To show that $\mathscr{h}_{(E,G)}(E', G') \subset \mathrm{Hom}(E', E)$ is also rank 4, we will show that $\mathscr{h}_{(E,G)}(E', G')$ contains a sublattice which is rank 4. Let $G_0, G_1, ..., G_N$ denote the $N + 1$ subgroups of $E[N]$ of order N. Consider $\mathscr{h}_{(E,G_i)}(E', G')$ for $i = 0, 1, ..., N$. By construction, $\bigcup_{i=0}^{N} \mathscr{h}_{(E,G_i)}(E', G') = \mathrm{Hom}(E', E)$ because every isogeny from E' to E must send G' to either one of the G_i or the identity of E. Consider the intersection of these homomorphism rings:

$$\bigcap_{i=0}^{N} \left(\mathscr{h}_{(E,G_i)}(E', G')\right) = \{\phi \in \mathrm{Hom}(E', E) : G' \subseteq \ker \phi\}.$$

By Corollary III.4.11 of [Sil09], the set on the right is equivalently characterized:

$$\{\phi \in \mathrm{Hom}(E', E) : G' \subseteq \ker \phi\} = \{\phi \circ \varphi_{G'} : \phi \in \mathrm{Hom}(E'/G', E)\} = \mathrm{Hom}(E'/G', E)\varphi_{G'},$$

where $\varphi_{G'} : E' \to E'/G'$ is the unique separable isogeny with $\ker(\varphi_{G'}) = G'$. This is an ideal of $\mathrm{Hom}(E'/G', E)$, which is rank 4. It follows that each $\mathscr{h}_{(E,G_i)}(E', G')$ is rank-4 as well.

To prove the invertibility of $\mathscr{h}_{(E,G)}(E', G')$ as a left $\mathcal{O}(E, G)$-module, we use the fact that $\mathcal{O}(E, G)$ is isomorphic to an Eichler order of prime level in the quaternion algebra $B_{p,\infty}$, see Theorem 3.5. This strategy is similar to the maximal order case, detailed in [Voi21, Lemma 41.1.11]. Take a nonzero isogeny $\psi \in \mathscr{h}_{(E,G)}(E', G')$ and let $\widehat{\psi}$ denote the dual of ψ. Then, $I := \mathscr{h}_{(E,G)}(E', G')\widehat{\psi} \subset \mathcal{O}(E, G)$ is an integral left $\mathcal{O}(E, G)$ ideal, and is thus invertible by the hereditary property of $\mathcal{O}(E, G)$ (all lattices of hereditary orders are invertible by [Voi21, Section 23.1.2]). The same holds for $\mathscr{h}_{(E,G)}(E', G')$ as a left $\mathcal{O}(E, G)$-module. □

Lemma 6.7. Fix an integral left $\mathcal{O}(E, G)$-ideal I of norm prime to N. There exists an isogeny $\varphi_I : E \to E_I$ and a subgroup $G_I \subseteq E_I[N]$ of order N such that $\varphi(G) \subseteq G_I$, and $I = \mathscr{h}_{(E,G)}(E_I, G_I)\varphi_I$, and $\mathrm{Nrd}(I) = \deg(\varphi_I)$. This association defines a bijection between integral left $\mathcal{O}(E, G)$-ideals of norm prime to N and isogenies of $\mathcal{S}_N$.

Proof. By Theorem 3.5, $\mathcal{O}(E, G)$ is isomorphic to an Eichler order. It is contained in the maximal order M isomorphic to $\mathrm{End}(E)$. By [FKL+20, Lemma 5], the integral left ideals of the Eichler order $\mathcal{O}(E, G)$ of norm prime to N are in bijection with the integral left ideals of the maximal order $\mathrm{End}(E) \supset \mathcal{O}(E, G)$ of norm prime to N. This bijection sends the integral left ideal I of $\mathcal{O}(E, G)$ to $\mathrm{End}(E)I$. To avoid confusion, we will write $\mathrm{End}(E)I$ when we mean the left ideal of $\mathrm{End}(E)$, but use I when we are referring to I as a left $\mathcal{O}(E, G)$-ideal. As a left integral ideal of $\mathrm{End}(E)$, $\mathrm{End}(E)I$ can be used to define an isogeny in the following way (see [Voi21, 42.2]). Let

$$E[\mathrm{End}(E)I] := \bigcap_{\alpha \in \mathrm{End}(E)I} \ker(\alpha) \tag{7}$$

be the scheme theoretic intersection, and define $\varphi_I : E \to E_I =: E/E[\mathrm{End}(E)I]$ via $\ker \varphi_I = E[\mathrm{End}(E)I]$. By [Voi21, Proposition 42.2.16], $\deg \varphi_I = \mathrm{Nrd}(\mathrm{End}(E)I)$. Since $\mathrm{End}(E)I$ is of norm prime to N, φ_I maps $G \subset E[N]$ to some $G_I \subset E_I[N]$. □

Lemma 6.8. With the notation of the previous lemma, every object (E', G') of $\mathcal{S}_N$ is of the form (E_I, G_I) for some integral left $\mathcal{O}(E, G)$-ideal I.

Proof. By the connectedness of $\mathcal{E}^N_{p,\ell}$ (Theorem 7.2), there exists a chain of ℓ-isogenies connecting the vertices (E, G), (E', G'). Let $\varphi : E \to E'$ denote this isogeny composition, where $\varphi(G) = G'$. By the theory described in Section 2.2, the kernel of φ corresponds to an integral left-$\mathrm{End}(E)$ ideal I_φ of norm equal to the degree of φ, which is a power of ℓ by construction. Since the codomain of φ is E', we have $E' = E_{I_\varphi}$. Since $\varphi_I(G) = G'$, we have $G' = G_{I_\varphi}$. By the bijection in Lemma 3.7, $I \cap \mathcal{O}(E, G)$ is an integral left ideal of the Eichler order $\mathcal{O}(E, G)$. □

Lemma 6.9 (Fully Faithful)**.** The functor $h_{(E,G)}$ is fully faithful. In particular, every object (E', G') of $\mathcal{S}_N$ is of the form (E_I, G_I) for some integral left $\mathcal{O}(E, G)$-ideal I, and the map

$$\mathrm{Hom}_{\mathcal{S}_N}((E_{I'}, G_{I'}), (E_I, G_I)) \to \mathrm{Hom}_{\mathcal{LM}}(h_{(E,G)}(E_I, G_I), h_{(E,G)}(E_{I'}, G_{I'}))$$

from morphisms in $\mathcal{S}_N$ to morphisms in $\mathcal{LM}$ is bijective.

Proof. The statement that every object (E', G') of $\mathcal{S}_N$ is of the form (E_I, G_I) for some integral left $\mathcal{O}(E, G)$-ideal I is precisely the content of Lemma 6.8.

By Lemma 6.10, the left-hand side $\mathrm{Hom}_{\mathcal{S}_N}((E_{I'}, G_{I'}), (E_I, G_I))$ is in bijection with $I^{-1}I'$. If we can show that the right-hand side is in bijection with $I^{-1}I'$ as well, this completes the proof.

By Lemma 6.7, we obtain the identifications:

$$h_{(E,G)}(E_I, G_I) = \mathrm{Hom}((E_I, G_I), (E, G)) \cong I(\frac{1}{\deg \varphi_I}\widehat{\varphi}_I),$$

$$h_{(E,G)}(E_{I'}, G_{I'}) = \mathrm{Hom}((E_{I'}, G_{I'}), (E, G)) \cong I'(\frac{1}{\deg \varphi_{I'}}\widehat{\varphi}_{I'}),$$

which yield

$$\mathrm{Hom}_{\mathcal{LM}}(h_{(E,G)}(E_I, G_I), h_{(E,G)}(E_{I'}, G_{I'})) \cong \mathrm{Hom}_{\mathcal{LM}}(I(\frac{1}{\deg \varphi_I}\widehat{\varphi}_I), I'(\frac{1}{\deg \varphi_{I'}}\widehat{\varphi}_{I'})) \cong \mathrm{Hom}_{\mathcal{LM}}(I, I').$$

It remains to show that $\mathrm{Hom}_{\mathcal{LM}}(I, I') \cong I^{-1}I'$, which follows from Theorem 11.6(c) [Eis95]. □

Lemma 6.10. Let $I, I' \subset \mathcal{O}(E, G)$ be nonzero integral left $\mathcal{O}(E, G)$-ideals of norm prime to N. Define $\mathrm{Hom}((E_I, G_I), (E, G))\mathrm{Hom}((E_{I'}, G_{I'}), (E_I, G_I))$ to be the collection of isogenies

$$\{\varphi : (E_{I'}, G_{I'}) \to (E, G) : \varphi = \sum_i \alpha_i\beta_i, \alpha_i \in \mathrm{Hom}((E_I, G_I), (E, G)), \beta_i \in \mathrm{Hom}((E_{I'}, G_{I'}), (E_I, G_I))\}.$$

We will show that the natural map

$$\mathrm{Hom}((E_I, G_I), (E, G))\mathrm{Hom}((E_{I'}, G_{I'}), (E_I, G_I)) \to \mathrm{Hom}((E_{I'}, G_{I'}), (E, G))$$

is bijective, giving a further bijection

$$\mathrm{Hom}((E_{I'}, G_{I'}), (E_I, G_I)) \leftrightarrow I^{-1}I',$$

where $I^{-1} := \overline{I}\mathrm{Nrd}(I)^{-1}$ and $\overline{I} := \{\overline{\alpha} : \alpha \in I\} = \{\widehat{\alpha} : \alpha \in I\}$.

Proof. By construction $\mathrm{Hom}((E_I,G_I),(E,G))\mathrm{Hom}((E_{I'},G_{I'}),(E_I,G_I))$, the map above is injective.

By Lemma 6.7, we have:

$$I = \mathrm{Hom}((E_I,G_I),(E,G))\phi_I$$

where $\phi_I : E \to E_I$ with $\phi_I(G) =: G_I$, and $N = \deg(\phi_I) = \mathrm{Nrd}(I)$. Since $\mathcal{O}(E,G)$ is a hereditary order, I is invertible, and by Proposition 16.6.15 [Voi21], $(m) := (\mathrm{Nrd}(I)) = I\overline{I}$. The quaternion element $[m]$ has an expression as an element of

$$I\overline{I} = (\mathrm{Hom}((E_I,G_I),(E,G))\varphi_I)\overline{(\mathrm{Hom}((E_I,G_I),(E,G))\varphi_I)}.$$

There exist finitely many $\alpha_i, \beta_i \in \mathrm{Hom}((E_I,G_I),(E,G))$ to give this expression:

$$[m] = \sum_i (\alpha_i\phi_I)\widehat{(\beta_i\phi_I)} = \sum_i \alpha_i\phi_I\widehat{\phi}_I\widehat{\beta}_i = [m]\sum_i \alpha_i\widehat{\beta}_i$$

Since each $\alpha_i\widehat{\beta}_i : (E,G) \to (E,G)$, the sum $\sum_i \alpha_i\widehat{\beta}_i \in \mathcal{O}(E,G)$, and $[1] = \sum_i \alpha_i\widehat{\beta}_i$.

Take any $\psi \in \mathrm{Hom}((E_{I'},G_{I'}),(E,G))$. We need to show that it has a pre-image in $\mathrm{Hom}((E_I,G_I),(E,G))\mathrm{Hom}((E_{I'}$ under the natural map (composition and sum). To see this, post-compose ψ by $\sum_i \alpha_i\widehat{\beta}_i$:

$$\psi = \sum_i \alpha_i\widehat{\beta}_i\psi = \sum_i \alpha_i(\widehat{\beta}_i\psi)$$

By construction, $\alpha_i \in \mathrm{Hom}((E_I,G_I),(E,G))$ and $\widehat{\beta}_i\psi \in \mathrm{Hom}((E_{I'},G_{I'}),(E_I,G_I))$, so the map

$$\mathrm{Hom}((E_I,G_I),(E,G))\mathrm{Hom}((E_{I'},G_{I'}),(E_I,G_I)) \to \mathrm{Hom}((E_{I'},G_{I'}),(E,G))$$

is indeed surjective.

The second bijection follows immediately from the first. To see this, follow the definitions of I and I' as ideals of $\mathcal{O}(E,G)$:

$$\begin{aligned}
\mathrm{Hom}((E_I,G_I),(E,G))\mathrm{Hom}((E_{I'},G_{I'}),(E,G)) &\leftrightarrow \mathrm{Hom}((E_{I'},G_{I'}),(E,G))\\
(I(\frac{1}{\deg\phi_I}\widehat{\phi_I}))\mathrm{Hom}((E_{I'},G_{I'}),(E,G)) &\leftrightarrow (I'(\frac{1}{\deg\phi_{I'}}\widehat{\phi}_{I'}))\\
\mathrm{Hom}((E_{I'},G_{I'}),(E,G)) &\leftrightarrow (I(\frac{1}{\deg\phi_I}\widehat{\phi_I}))^{-1}(I'(\frac{1}{\deg\phi_{I'}}\widehat{\phi}_{I'}))\\
\mathrm{Hom}((E_{I'},G_{I'}),(E,G)) &\leftrightarrow \phi_I I^{-1}I'(\frac{1}{\deg\phi_{I'}}\widehat{\phi}_{I'})\\
\mathrm{Hom}((E_{I'},G_{I'}),(E,G)) &\leftrightarrow I^{-1}I'
\end{aligned}$$

□

7. The Level Structure Graph

Definition 1.2 defines the supersingular ℓ-isogeny graph with level-N structure. The objects of $\mathcal{S}_N$ form the nodes of the graph $\mathcal{E}^N_{p,\ell}$. If we restrict the morphisms of $\mathcal{S}_N$ to isogenies of degree ℓ, we have the set of edges of $\mathcal{E}^N_{p,\ell}$. For each supersingular elliptic curve $E/\overline{\mathbb{F}}_p$ with $j(E) \neq 0, 1728$, there are $N+1$ vertices of $\mathcal{E}^N_{p,\ell}$. For $E/\overline{\mathbb{F}}_p$ with $j(E) = 0$ or 1728, there are at most $N+1$ vertices of $\mathcal{E}^N_{p,\ell}$: the extra automorphisms of these j-invariants may map order-N subgroups to each other. There is a map of graphs from $\mathcal{E}^N_{p,\ell}$ to $\mathcal{G}^\ell_{\overline{\mathbb{F}}_p}$ which is $(N+1)$-to-1 on vertices away from $j = 0, 1728$. For any prime ℓ coprime to pN, a supersingular elliptic curve over $\overline{\mathbb{F}}_p$ has precisely $\ell+1$ degree-ℓ isogenies. Isogenies define edges *up to post-composition with a curve automorphism.* If $j(E) \neq 0, 1728$, the automorphism group $\mathrm{Aut}(E) = [\pm 1]$. Both automorphisms $[\pm 1]$ act as the identity on the groups

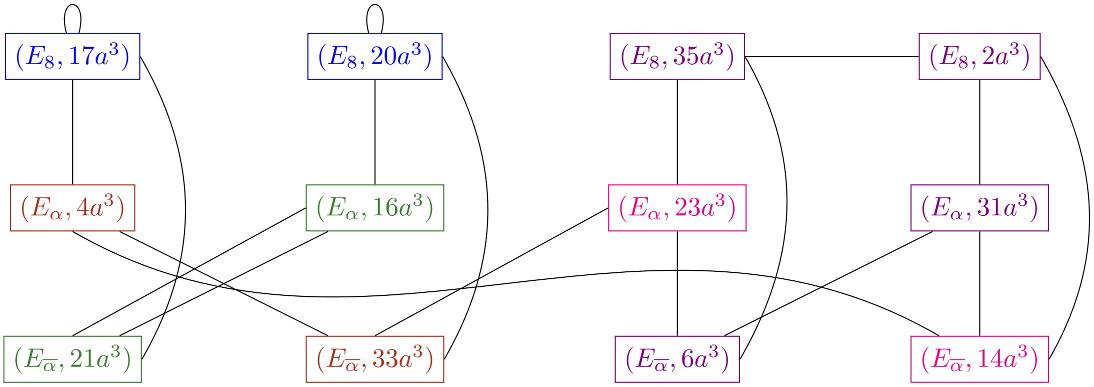


Figure 7.1. Graph of $\mathcal{E}^3_{37,2}$, with groups labeled by the first term in the x-coordinate of a generating point.

defining kernels. As a result, the duals of distinct isogenies must give distinct arrows in the graph. The graph can be taken to be undirected by identifying isogenies with their duals. See Figure 7.1.

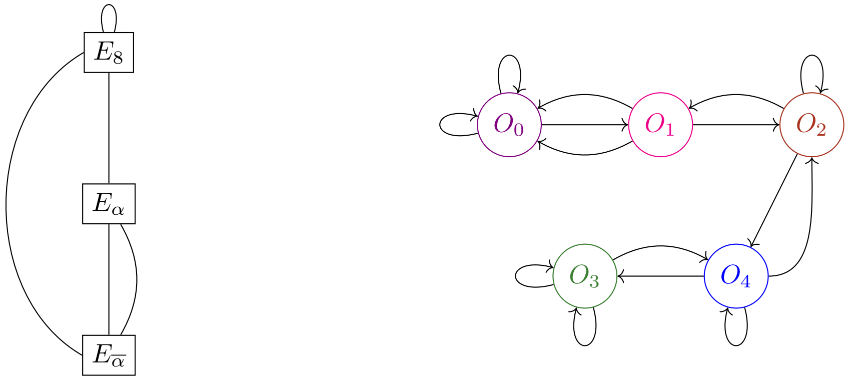
If $j(E) = 0$ or 1728, the automorphism groups expand to $\text{Aut}(E_0) = \{[\pm 1], [\pm\zeta_3], [\pm\zeta_3^2]\}$ and $\text{Aut}(E_{1728}) = \{[\pm 1], [\pm i]\}$. The 'extra' automorphisms potentially swap kernels, meaning that the duals of distinct isogenies need not give distinct arrows in the graph. In this case, we do not draw the edges of the graph as undirected.

Example 7.1 ($p = 37$, $N = 3$, $\ell = 2$)**.** We provide a reference example of the graph $\mathcal{E}^N_{p,\ell}$ in Figure 7.1. As $p = 37 \equiv 1 \pmod{12}$, this graph is drawn undirected by associating isogenies with their duals. Let $\mathbb{F}_{37}[s]/(s^2 + 33s + 2)$. The vertices are labeled with ordered pairs, the first element denoting the isomorphism class of elliptic curves with j-invariant j by E_j. Let $\alpha := 10s + 20$, $\overline{\alpha} = 27s + 23$ denote the j-invariants defined over $\mathbb{F}_{37^2} \setminus \mathbb{F}_{37}$. The supersingular elliptic curves over $\overline{\mathbb{F}}_{37}$ have 3-torsion defined over $\mathbb{F}_{37^4} := \mathbb{F}_{37}[a]/(a^4 + 6a^2 + 24a + 2)$. For compactness, we denote the 3-torsion subgroups using the a^3 term of the x-coordinate of a generating point. The vertex color aligns with the corresponding quaternion vertex, seen in Figure 7.2b. The corresponding supersingular 2-isogeny graph is shown in Figure 7.2a.

Theorem 7.2 (Connectedness of $\mathcal{E}^N_{p,\ell}$)**.** *The graph $\mathcal{E}^N_{p,\ell}$ consists of one connected component, for any pairwise coprime choices of p, N, ℓ.*

Proof. The connectedness of the graph follows from the work of Goren–Kassaei. In [GK17], the authors consider the ℓ-isogeny graph with level-N structure given by a choice of N-torsion point. The connectedness of $\mathcal{E}^N_{p,\ell}$ follows, as the Goren–Kassaei graph maps into $\mathcal{E}^N_{p,\ell}$. □

Additionally, the result of Theorem 7.2 can be seen as a corollary of a result provided by Roda [Rod19]. Roda studies a supersingular ℓ-isogeny level-N structure graph whose vertices are pairs (E, α), where $\alpha : (\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\sim} E[N]$. In Section 3.3, Roda describes a means of counting the number of connected components of this graph. Choosing particular lifts of pairs (E, G_1), (E, G_2) for $G_1 \neq G_2$, and showing that those lifts are connected using the conditions of [Rod19, Section 3.3], we can prove that all of the points corresponding to a particular supersingular elliptic curve



(A) Supersingular 2-isogeny graph over $\overline{\mathbb{F}}_{37}$

(B) Graph of level-3 Eichler orders in $B_{37,\infty}$ with connecting ideals of norm 2.

with level structure are connected in $\mathcal{E}_{p,\ell}^N$. Together with the fact that the supersingular ℓ-isogeny graph is connected, this proves that $\mathcal{E}_{p,\ell}^N$ is connected as well.

References

[ACNL$^+$21] Sarah Arpin, Catalina Camacho-Navarro, Kristin Lauter, Joelle Lim, Kristina Nelson, Travis Scholl, and Jana Sotáková. Adventures in supersingularland. *Experimental Mathematics*, 0(0):1–28, 2021.

[CGL09] Denis X. Charles, Eyal Z. Goren, and Kristin E. Lauter. Cryptographic hash functions from expander graphs. *J. Cryptology*, 22(1):93–113, 2009.

[CK20] Leonardo Colò and David Kohel. Orienting supersingular isogeny graphs. *Journal of Mathematical Cryptology*, 14(1):414–437, Oct 2020.

[CLM$^+$18] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: an efficient post-quantum commutative group action. In *Advances in cryptology—ASIACRYPT 2018. Part III*, volume 11274 of *Lecture Notes in Comput. Sci.*, pages 395–427. Springer, Cham, 2018.

[CS21] Mathilde Chenu and Benjamin Smith. Higher-degree supersingular group actions. *Math. Cryptology*, 1(1):1–15, 2021.

[DFJP14] Luca De Feo, David Jao, and Jérôme Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *J. Math. Cryptol.*, 8(3):209–247, 2014.

[DG16] Christina Delfs and Steven D. Galbraith. Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$. *Des. Codes Cryptogr.*, 78(2):425–440, 2016.

[EHL$^+$20] Kirsten Eisentraeger, Sean Hallgren, Chris Leonardi, Travis Morrison, and Jennifer Park. Computing endomorphism rngs of supersingular elliptic curves and connections to pathfinding in isogeny graphs. *Fourteenth Algorithmic Number Theory (ANTS XIV) Proceedings*, 2020.

[Eic55] Martin Eichler. Zur Zahlentheorie der Quaternionen-Algebren. *J. Reine Angew. Math.*, 195:127–151 (1956), 1955.

[Eic73] M. Eichler. The basis problem for modular forms and the traces of the Hecke operators. In *Modular functions of one variable, I (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 75–151. Lecture Notes in Math., Vol. 320, 1973.

[Eis95] David Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*. Springer, New York, N.Y., 1995.

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

[GK17] Eyal Z. Goren and Payman L Kassaei. p-adic dynamics of hecke operators on modular curves, 2017.

[KLPT14] David Kohel, Kristin Lauter, Christophe Petit, and Jean-Pierre Tignol. On the quaternion ℓ-isogeny path problem. Cryptology ePrint Archive, Report 2014/505, 2014. https://eprint.iacr.org/2014/505.

[Koh96] David Kohel. *Endomorphism rings of elliptic curves over finite fields*. PhD thesis, University of California, Berkely, 1996.

[LB20] Jonathan Love and Dan Boneh. Supersingular curves with small noninteger endomorphisms. In *ANTS XIV—Proceedings of the Fourteenth Algorithmic Number Theory Symposium*, volume 4 of *Open Book Ser.*, pages 7–22. Math. Sci. Publ., Berkeley, CA, 2020.

[Onu21] Hiroshi Onuki. On oriented supersingular elliptic curves. *Finite Fields and their Applications*, 69, 2021.

[Piz73] Arnold Pizer. Type numbers of eichler orders. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 1973, November 1973.

[Rib89] Kenneth A. Ribet. Bimodules and abelian surfaces. *Algebraic Number Theory — in honor of K. Iwasawa*, pages 359–407, 1989.

[Rod19] Megan Roda. Supersingular isogeny graphs with level n structure and path problems on ordinary isogeny graphs. Master's thesis, McGill University, Montreal, 2019.

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves, 2nd Edition*. Springer-Verlag, New York, N.Y., 2009.

[Voi21] John Voight. Quaternion algebras. https://math.dartmouth.edu/~jvoight/quat-book.pdf, 2021. Online. Last accessed 3/28/2021.