JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Sarah ARPIN

Adding Level Structure to Supersingular Elliptic Curve Isogeny Graphs

Tome 36, n° 2 (2024), p. 405-443.

https://doi.org/10.5802/jtnb.1283

e-ISSN : 2118-8572

Journal de Théorie des Nombres de Bordeaux **36** (2024), 405–443

Adding Level Structure to Supersingular Elliptic Curve Isogeny Graphs

par Sarah ARPIN

Résumé. Dans cet article, motivés par la cryptographie à base d'isogénies, nous étudions les courbes elliptiques supersingulières munies d'une structure de niveau. De la même manière que la correspondance classique de Deuring associe à une courbe elliptique supersingulière un ordre maximal dans une algèbre de quaternions, on associe à une courbe elliptique supersingulière avec une structure de niveau un ordre d'Eichler. Nous étudions cette correspondance et les ordres d'Eichler eux-mêmes. Nous examinons également les graphes d'isogénies des courbes elliptiques supersingulières avec structure de niveau et leur lien avec les graphes des ordres d'Eichler.

Abstract. 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 via the classical Deuring correspondence. 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 graphs of Eichler orders.

1. Introduction

Supersingular elliptic curve isogeny graphs have a rich underlying mathematical structure, and yet they appear to be difficult to navigate in a computational sense. The recent appearance of these graphs in cryptographic protocols which aim to be safe against classical and quantum attacks has led to a resurgence of interest in the mathematical properties of supersingular elliptic curves. In this work, we study supersingular elliptic curves endowed with level-N structure:

Definition 1.1 (Supersingular elliptic curve with level-N structure, see Definition 3.1)**.** Let p be a prime and N an integer coprime to p. Let $|\mathcal{S}_N|$ denote the set of pairs (E, G), up to isomorphism, where E is a supersingular elliptic curve over $\overline{\mathbb{F}}_p$ and $G \subseteq E[N]$ is a cyclic subgroup of order N.

Manuscrit reçu le 6 septembre 2022, révisé le 16 février 2024, accepté le 24 mai 2024.
2020 *Mathematics Subject Classification.* 11G20, 11T71.
Mots-clefs. supersingular, level structure, elliptic curves, isogeny graphs.
The author was supported by NSF-CAREER CNS-1652238 (P.I. Katherine E. Stange).

To better understand supersingular elliptic curves with level-N structure, we study maps on these curves, in particular their endomorphisms:

Definition 1.2 (Endomorphisms of (E, G), see Definition 3.2)**.** As a subring of $\mathrm{End}(E)$, we define the ring of endomorphisms of the pair $(E, G) \in |\mathcal{S}_N|$ as follows:

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

The endomorphism rings of supersingular elliptic curves are maximal orders in a quaternion algebra. This correspondence is an explicit equivalence of categories called the Deuring correspondence [14]. Research into this correspondence has greatly expanded our understanding of supersingular elliptic curves, and in this work we extend these tools to supersingular elliptic curves with level-N structure. In Theorem 3.7, restated below, we prove that the endomorphism rings $\mathcal{O}(E, G)$ are Eichler orders of level-N in the quaternion algebra $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$.

Theorem 1.3 (See Theorem 3.7)**.** $\mathcal{O}(E, G)$ *is isomorphic to an Eichler order of level* $|G| = N$.

The correspondence between isomorphism classes of supersingular elliptic curve endomorphism rings and isomorphism classes of maximal orders in a quaternion algebra is not a priori an injective map. The failure of injectivity comes from curves which are related by the p-power Frobenius map, as these curves have isomorphic endomorphism rings. In the case of supersingular elliptic curves with level-N structure the failure of injectivity is more complicated, but also reveals more information about the structure of the supersingular elliptic curves. In this case, we restrict to N squarefree and we study the failure of injectivity via involutions which we define on the isomorphism classes in $|\mathcal{S}_N|$. This complete description can be found in Section 4, culminating in Theorem 4.13 which completely describes the failure of injectivity of the map from $|\mathcal{S}_N|$ to isomorphism classes of Eichler orders of level-N. In addition to understanding the fiber size of the map taking supersingular elliptic curves with level-N structure to their Eichler order endomorphism rings, we also understand the structure on the quaternion side which dictates this fiber size. We restate a version of Theorem 4.13 below:

Theorem 1.4. *Fix an Eichler order* $\mathcal{O}$ *of level* $N = q_1 \cdots q_r$ *squarefree and coprime to* p*. The number of isomorphism classes of supersingular elliptic curves with level-*N *structure* $(E, G) \in |\mathcal{S}_N|$ *with endomorphism ring isomorphic to* $\mathcal{O}$ *is equal to the size of the two-sided ideal class group of* $\mathcal{O}$*, which equals* 2^k *for some* $k \in \{0, 1, \ldots, r + 1\}$.

With all of this structure understood, we prove a formal equivalence of categories for supersingular elliptic curves with level-N structure, in the style of the classical Deuring correspondence:

Theorem 1.5 (Equivalence of Categories, see Theorem 6.5)**.** Fix a supersingular elliptic curve E defined over $\overline{\mathbb{F}}_p$ and a cyclic subgroup $G \subset E[N]$ of squarefree order N, coprime to p. There is a contravariant functor $\hbar_{(E,G)}$ from the category $\mathcal{S}_N$ of supersingular elliptic curves with level-N structure to the category $\mathcal{LM}$ of invertible left $\mathcal{O}(E, G)$-modules. This functor defines an equivalence of categories.

Finally, we consider maps between supersingular elliptic curves with level-N structure in the form of ℓ-isogeny graphs, which are defined and explored in Section 7. We briefly recap some highlights of isogeny-based cryptography as motivation for studying this isogeny graph variant. Supersingular elliptic curve ℓ-isogeny graphs were first proposed for use in post-quantum cryptography in 2006 by Charles, Goren, and Lauter [8] with a hash function based on walks in the ℓ-isogeny graph. This was swiftly followed by papers of Rostovtsev–Stolbunov and Couveignes whose work (which was actually from 1997, but not made public at that time) took the perspective of using a class group action to walk the ℓ-isogeny graph. These works formed the basis for CSIDH [7], a key exchange protocol based on isogenies of supersingular elliptic curves over $\mathbb{F}_p$. Perhaps the most well-known isogeny-based cryptographic protocol was SIKE [12] (a variant of SIDH), a key exchange protocol which made public the images of certain torsion subgroup generators under certain isogenies. In 2022, Castryck–Decru [6], Maino–Martindale [22, 23], and Robert [28] were able to use this information to break the protocol and SIDH in general. This break has shaken trust in isogeny-based cryptography, but the reliance on the extra torsion point information was key to the break; this highlights the importance of understanding isogeny graphs which are enhanced by additional structure. Another protocol of mathematical interest is OSIDH [11], in which the supersingular elliptic curves are endowed with the information of an endomorphism in the form of an "orientation". These graphs have been studied extensively [3, 4, 33], and in future work we hope to explore the connection between orientations and level structure.

1.1. 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" [18, Section 4]: Papers have been written about related concepts in the context of modular forms (Ribet), or about different choices of level structure (Goren–Kassaei [1], with a choice of torsion point, Roda's thesis [29] 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 [32, Remark 42.3.10] notes that a generalization of the Deuring correspondence is possible through mild adjustments. Ribet, in [27], 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 [15, 16] and Pizer [26] provide the foundational theory of Eichler orders.

More recently, work of Goren and Kassaei [1] 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 [18] 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 squarefree 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.

Since the first appearance of this paper, Codogni and Lido [10] have continued to understand the spectral properties of isogeny graphs with level structure. Page and Wesolowski [25] introduced a framework to study a generalized notion of level structure.

1.2. Conventions. In this paper, p is a (cryptographic size) prime, ℓ is a small prime, and N is an integer which is coprime to $p\ell$. In Sections 4 and 6, we restrict N to be squarefree. In Section 5, we require N to be prime.

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. Many thanks to David Grant and Christelle Vincent for their feedback on the thesis-version of this work. Additional thanks to Leo Herr, Soumya Sankar, and Jaap Top for helpful discussions. Many thanks to the reviewer for their encouraging feedback and helpful suggestions, especially in Sections 4 and 6.

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 mapping the supersingular elliptic curves over $\overline{\mathbb{F}}_p$ to the maximal orders of $B_{p,\infty}$. The fibers of this map have either one or two elements, 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 [27] 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 [19]:

Theorem 2.2 ([19, Theorem 44])**.** 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 [19, 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 [32, Section 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 [32, 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 $B_{p,\infty}^E := \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q} \cong B_{p,\infty}$. 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 $B_{p,\infty}^E$, 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 $B_{p,\infty}^E$ via

$$\begin{aligned} \mathrm{End}(E') &\hookrightarrow B_{p,\infty}^E \\ \beta &\longmapsto \frac{1}{\deg \varphi}(\widehat{\varphi}\beta\varphi). \end{aligned} \tag{2.1}$$

The image of $\mathrm{End}(E')$ is the maximal order of $B_{p,\infty}^E$ 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 $B_{p,\infty}^E$ as defined above. Note that this map depends on a choice of φ. If instead we had chosen an isogeny $\varphi' := \eta \circ \varphi : E \to E'$, where $\eta \in \mathrm{Aut}(E')$, the image of $\mathrm{End}(E')$ in $B_{p,\infty}^E$ 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 [13] 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 ([13, Section 2])**.** 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 $\operatorname{End}(E) \cong \mathbb{Z}[\sqrt{-p}]$. If $p \equiv 3 \pmod 4$, then there are two possibilities for $\operatorname{End}_{\mathbb{F}_p}(E)$: if $\pi_p(P) = P$ for all $P \in E[2]$, then $\operatorname{End}_{\mathbb{F}_p}(E) \cong \mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$. Otherwise, $\operatorname{End}_{\mathbb{F}_p}(E) \cong \mathbb{Z}[\sqrt{-p}]$.

3. Elliptic Curves with Level Structure and Their Endomorphism Rings

Definition 3.1. Let p be a prime and N an integer coprime to p. 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 cyclic 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 $\operatorname{End}(E)$, we define the ring of endomorphisms of the pair $(E, G) \in |\mathcal{S}_N|$ as follows:

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

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. Let $(E, G), (F, H) \in |\mathcal{S}_N|$ and suppose 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 $\operatorname{End}(F) \to \operatorname{End}(E)$ 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:

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

□

In Theorem 3.7, 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 3.8, 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, $\mathcal{O}(E,G) = \operatorname{End}(E) \cap (\frac{1}{\deg\varphi}\widehat{\varphi}\operatorname{End}(E/G)\varphi)$ where the intersection is taken in $B^E_{p,\infty}$ via the embedding described in equation (2.1) and is independent of choice of φ.

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

To see $\mathcal{O}(E,G) \subseteq \operatorname{End}(E) \cap (\frac{1}{\deg\varphi}\widehat{\varphi}\operatorname{End}(E/G)\varphi)$, take $\alpha \in \mathcal{O}(E,G)$. To show $\alpha \in \frac{1}{\deg\varphi}\widehat{\varphi}\operatorname{End}(E/G)\varphi$, we will show that there exists a $\beta \in \operatorname{End}(E/G)$ 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 [31] 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 $\eta \in \operatorname{Aut}(E/G)$, we obtain the object:

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

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

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

3.1.1. *The effect of extra automorphisms on $|\mathcal{S}_N|$.* Counting the number of elements of $|\mathcal{S}_N|$ with $j(E) = 0, 1728$ is not as straightforward as counting subgroups of $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ of order N, due to the presence of extra automorphisms. The automorphisms $[\pm 1]$ of any E necessarily map G to itself. In the case where $\operatorname{Aut}(E) = \{[\pm 1]\}$, this means a fixed Weierstrass equation for a curve E will have $(E,G_0) \sim (E,G_1)$ if and only if $G_0 = G_1$. In particular, every supersingular j-invariant not equal to 0 or 1728 will have the same number of equivalence classes in $|\mathcal{S}_N|$: we refer to this as the generic case.

This is not necessarily the case for the extra automorphisms of E with $j(E) = 0, 1728$. The automorphisms of these curves can provide equivalences $(E, G_0) \sim (E, G_1)$ for $G_0 \neq G_1$. In these cases, the j-invariants 0 and 1728 may have fewer equivalence class representatives in $|\mathcal{S}_N|$ than the generic case.

Example 3.5. Let $p \equiv 3 \pmod 4$, $\mathbb{F}_{p^2} := \mathbb{F}_p[s]/(s^2+1)$, and $E_{1728} : y^2 = x^3 + x$. The order-two subgroups of $E(\overline{\mathbb{F}}_p)$ are:

$$G_0 := \{(0,0), O_{E_{1728}}\}, \quad G_1 := \{(s,0), O_{E_{1728}}\}, \quad G_2 := \{(-s,0), O_{E_{1728}}\}.$$

The curve E_{1728} has automorphism group isomorphic to $\mathbb{Z}/4\mathbb{Z}$ and is generated by $[s] : (x,y) \mapsto (-x, sy)$. The automorphism $[s]$ in particular sends G_1 to G_2 and vice versa, meaning $(E, G_1) \sim (E, G_2)$. Here, the j-invariant 1728 only has two distinct equivalence classes in $|\mathcal{S}_2|$ instead of three, which is the generic case.

In order to better understand the number of elements $(E, G) \in |\mathcal{S}_N|$ with $j(E) = 1728$, we write down a matrix representation for the action of $[i]$ on $E[N] \cong \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ for any N. A similar procedure works for $j(E) = 0$ as well. For simplicity of enumerating the subgroups, we restrict to the case N prime, but we hope that even with these simplifications the general principle will be clear to the reader.

Proposition 3.6. Let $E/\overline{\mathbb{F}}_p$ be an elliptic curve with $j(E) = 1728$, and let $N \neq p$ be prime. The action of $[i]$ on the set of order N subgroups of $E[N]$ is as follows:

(1) If N is odd and $\left(\frac{-1}{N}\right) = -1$, then $[i]$ permutes the order N subgroups in 2-cycles.
(2) If N is odd and $\left(\frac{-1}{N}\right) = 1$, then $[i]$ fixes two order N subgroups, and permutes the remaining $N-1$ order N subgroups in 2-cycles.
(3) If N is even, then $[i]$ fixes one order N subgroup and permutes the remaining two.

Proof. We begin by choosing a basis of $E[N]$ in order to write down a matrix representation of the action of $[i]$ on $E[N]$, for any integer $N > 1$. Begin by noting that the action of $[i]$ on $E[N]$ cannot be the same as the action of $[m]$, the multiplication-by-m map for any integer m. Assume $m < N$, as the action on the N-torsion is not changed by reducing m modulo N. If it were, then $E[N] \subseteq \ker([m] - [i])$, which implies $N^2 \mid \deg([m] - [i]) = m^2 + 1$. This contradicts the assumption that $m < N$. Thus there exists some $P \in E[N]$ such that $[i](P)$ is not a scalar multiple of P. We choose $P, Q := [i](P)$ as our basis for $E[N]$. The matrix representation of $[i]$ with respect to this basis is then:

$$M_{[i]} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Enumerate the subgroups of order N with respect to this basis as follows:

$$G_0 = \langle P\rangle,\ G_1 = \langle P+Q\rangle,\ \dots,G_{N-1} = \langle P+(N-1)Q\rangle,G_N = \langle Q\rangle.$$

By construction, $M_{[i]}(G_0) = G_N$ and $M_{[i]}(G_N) = G_0$.

Suppose N is odd. Take $k \in \{1, 2, \dots, N-1\}$. The group G_k is generated by $\binom{1}{k}$, which $[i]$ maps to:

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ k \end{pmatrix} = \begin{pmatrix} -k \\ 1 \end{pmatrix}.$$

The map $[i]$ fixes G_k precisely when $\binom{-k}{1} = \binom{s}{sk}$, for some integer s, modulo N. This gives the system of congruences:

$$s \equiv -k \pmod N$$

$$1 \equiv sk \pmod N$$

which leads to the equation $-1 \equiv k^2 \pmod N$. There are either 0 or 2 solutions to this equation, depending on the value of the Legendre symbol $\left(\frac{-1}{N}\right)$. Note that $1^2 = 1$ and $(-1)^2 = 1$, so k cannot be 1 or $N-1$ for this to be true, so these subgroups are never fixed.

For $N = 2$, direct computation shows that $[i]$ will fix precisely one subgroup of order 2 and permute the remaining two. □

3.2. Eichler Orders. The classical origins of Eichler orders can be traced to papers of Eichler himself [15, 16]. The theory of Eichler orders was further developed by Pizer [26]. Eichler orders of squarefree level are called *hereditary.* For relevant properties and background on Eichler and hereditary orders, see [32].

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 [20, 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 3.7. *$\mathcal{O}(E, G)$ 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 $B^E_{p,\infty} := \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$. 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 $\mathcal{O}_L(I)$, is $\mathrm{End}(E)$. Analogously, let $\mathcal{O}_R(I)$ denote the right order of I. The image of $\mathrm{End}(E/G)$ in $B_{p,\infty}^E$ under the embedding (2.1) is the right order of I. Together with Proposition 3.4, this shows that $\mathcal{O}(E,G) \cong \mathcal{O}_L(I) \cap \mathcal{O}_R(I)$. By [20, 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 3.8. 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 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 $\mathcal{O}_2$ [32, Proposition 23.4.3]. Eichler orders of prime level are only non-maximal at primes which divide level, so all three orders $\mathcal{O}, \mathcal{O}_1, \mathcal{O}_2$ lift uniquely to the global setting [32, 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 [20, 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 (2.1) 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,

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

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 Section 4.

3.3. ℓ-isogenies on the Quaternion Side.

Fix a small prime ℓ coprime to pN. 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 E be a supersingular elliptic curve over $\overline{\mathbb{F}}_p$ with level-N structure G. Let $\varphi : E \to E'$ be a degree-ℓ isogeny. Then $G \subset E[N], \varphi(G) \subset (E')[N]$ 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 $\varphi : E \to E'$ is also a morphism between elements of $|\mathcal{S}_N|$, as $\varphi : (E, G) \to (E', \varphi(G))$. In this section, we describe isogenies between elements of $|\mathcal{S}_N|$ as quaternion objects.

Proposition 3.9. Let $\mathcal{O}$ be an Eichler order of level-N specified by the intersection $M \cap M'$ of two maximal orders M and M'. The integral left ideals I of M of norm coprime to N 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 $\mathrm{Nrd}(I)$ is coprime to N, then $\mathrm{Nrd}(I) = \mathrm{Nrd}(\mathcal{O} \cap I)$.

Proof. Let $\mathcal{O} \subset M$ be as above. At $q \nmid N$, $\mathcal{O}_q = M_q$, so the ideals of $\mathcal{O}_q$ are precisely the ideals of M_q intersected with $\mathcal{O}_q$. At $q|N$, M_q and $\mathcal{O}_q$ each have a unique ideal of norm coprime to N, namely M_q and $\mathcal{O}_q$ respectively. The intersection $\mathcal{O}_q = M_q \cap \mathcal{O}_q$ thus realizes the bijection.

By [32, Theorem 9.1.1], the local bijection realized by intersection with $\mathcal{O}$ is in fact global. □

We have a way of associating the ideals I of maximal orders to isogenies $E \to E'$. To extend this picture to the level structure context, we need to show that a left ideal of $\mathcal{O}(E, G)$ has right order $\mathcal{O}(E', G')$, for some isogeny $\varphi : E \to E'$ such that $\varphi(G) = G'$.

By Proposition 3.9, every left-ideal of $\mathcal{O}(E, G)$ of norm prime to N is of the form $I \cap \mathcal{O}(E, G)$, where I is a left ideal of the maximal order $\mathrm{End}(E) \supseteq \mathcal{O}(E, G)$. Let $\varphi_I : E \to E'$ be the isogeny determined by I as in Section 2.3, and let $G' := \varphi_I(G)$.

Proposition 3.10. Let $I \cap \mathcal{O}(E, G)$ be a left ideal of $\mathcal{O}(E, G)$ of norm prime to N. Then,

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

Proof. We proceed by showing containment in both directions. By Proposition 3.9 $I \cap \mathcal{O}(E, G)$ 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 [32, 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:

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

The element $\beta \circ \alpha \circ \varphi_I$ satisfies condition (i). To check condition (ii):

$$\beta \circ \alpha \circ \varphi_I(G) = \beta \circ \alpha(G') \subseteq \beta(G') \subseteq G.$$

To see $\mathcal{O}_R(I \cap \mathcal{O}(E, G)) \subseteq \frac{1}{\deg \varphi_I} \widehat{\varphi}_I \mathcal{O}(E', G') \varphi_I$, 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 [32, Lemma 17.4.11]). Since $\mathcal{O}_R(I \cap \mathcal{O}(E, G))$ 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. □

For an explicit example illustrating the correspondence between supersingular elliptic curves with level-N structure and Eichler orders, we refer the reader to Example 7.2.

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 this section, we restrict to the case where N is squarefree, in addition to being coprime to p. Eichler orders of level N are in fact hereditary. 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 4.13 of Section 4.2.

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.

We begin by defining a dualizing involution on the equivalence classes $(E, G) \in |\mathcal{S}_N|$. For $N = q_1 q_2 \cdots q_r$, we will have r dualizing involutions. The initiated reader will recognize these dualizing involutions as Atkin–Lehner involutions, and the author would like to thank Jaap Top in particular for this helpful perspective. First, we will define and illustrate this involution when N is prime:

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

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

where $\varphi_G : E \to E/G$ is an isogeny with kernel G, and $\widehat{G}$ denotes the kernel of the dual isogeny $\widehat{\varphi}_G : E/G \to E$. In particular, $\widehat{G} = \varphi_G(E[N])$.

The data of (E, G) is equivalent to that of an isogeny, and that isogeny has a unique dual. In this way, the data of (E, G) is equivalent to the data of $(E/G, \widehat{G})$. When N factors as $N = q_1 q_2 \cdots q_r$, the kernel G factors as $G = G_1 \oplus G_2 \oplus \cdots \oplus G_r$. There is a D_i dualizing involution for each $i = 1, 2, \ldots, r$, defined as follows:

Definition 4.2 (Dualizing Involution on $|\mathcal{S}_N|$)**.** Let $N = q_1 \cdots q_r$, so $G = G_1 \oplus G_2 \oplus \cdots \oplus G_r$. Take $i \in \{1, \ldots, r\}$ and without loss of generality let $i = 1$. The isogeny with kernel G can be factored as $\varphi_G = \varphi_r \circ \varphi_{r-1} \circ \cdots \circ \varphi_2 \circ \varphi_1$ with $\ker \varphi_1 = G_1$, $\ker \varphi_2 = \varphi_1(G_2)$,. . . , $\ker \varphi_r = \varphi_{r-1}(\varphi_{r-2}(\cdots(\varphi_1(G_r))))$. Define $\widehat{G}_1 := \varphi_1(E[q_1])$, which is the kernel of $\widehat{\varphi}_1$. Define $\widehat{G} := \widehat{G}_1 \oplus \varphi_1(G_2) \oplus \varphi_1(G_3) \oplus \cdots \oplus \varphi_1(G_r)$, which is a subgroup of $\varphi_1(E)[N]$ of order N. Finally, we define:

$$D_1(E, G) := (\varphi_1(E), \widehat{G}).$$

For $N = q_1 \cdots q_r$, there are r distinct dualizing involutions. First, we show that they are compatible with the equivalence relation on $|\mathcal{S}_N|$ and then we show that they are commutative.

Lemma 4.3. *If $(E, G) \sim (E', G')$ as in Definition 3.1, then $D_i(E, G) \sim D_i(E', G')$.*

Proof. Without loss of generality, we take $i = 1$. We can factor $N = q_1 \cdots q_r$, $G = G_1 \oplus \cdots \oplus G_r$, and $G' = G'_1 \oplus \cdots \oplus G'_r$ with $|G_i| = |G'_i| = q_i$.

Suppose $\eta : E \to E'$ is the isomorphism sending G to G'. This gives the following commutative diagram:

$$\begin{tikzcd}
O_E \arrow[r] & G \arrow[r, hook] \arrow[d, "\eta"] & E \arrow[r, "\varphi_{G_1}"] \arrow[d, "\eta"] & E/G_1 \arrow[r] \arrow[d, dashed, "\omega"] & O_{E/G_1} \arrow[d, "\eta"] \\
O_{E'} \arrow[r] & G'_1 \arrow[r, hook] & E' \arrow[r, "\varphi_{G'_1}"] & E'/G'_1 \arrow[r] & O_{E'/G'_1}
\end{tikzcd}$$

Since $\omega \circ \varphi_{G_1} = \varphi_{G'_1} \circ \eta$ and $\deg \varphi_{G_1} = \deg \varphi_{G'_1}$ and η is an isomorphism, the map $\omega : E/G_1 \to E'/G'_1$ is an isomorphism. Moreover, $\widehat{\varphi_{G_1}} = \varphi_{\widehat{G}_1} = \widehat{\eta} \circ \varphi_{\widehat{G'_1}} \circ \omega$. Comparing the kernels on the left and right, we see $\omega(\widehat{G}_1) \subseteq \ker \varphi_{\widehat{G'_1}}$, and so $\omega(\widehat{G}_1) = \widehat{G}'_1$.

We also have $\eta(G_i) = G'_i$ for all $i \neq 1$, so we can construct:

$$\widehat{G} = \widehat{G}_1 \oplus \varphi_{G_1}(G_2) \oplus \varphi_{G_1}(G_3) \oplus \cdots \oplus \varphi_{G_1}(G_r)$$

and

$$\widehat{G}' = \widehat{G}'_1 \oplus \varphi_{G'_1}(G'_2) \oplus \varphi_{G'_1}(G'_3) \oplus \cdots \oplus \varphi_{G'_1}(G'_r)$$

where $\widehat{G} \cong \widehat{G}'$ via ω, and so we have $D_1(E, G) \sim D_1(E', G')$. □

Lemma 4.4. Let $(E, G) \in |\mathcal{S}_N|$ for $N = q_1 \cdots q_r$ and factor $G = G_1 \oplus \cdots \oplus G_r$ with $|G_i| = q_i$. Let D_i, D_j be any two dualizing involutions with $i \neq j$. Then, $D_j(D_i(E, G)) \sim D_i(D_j(E, G))$.

Proof. Without loss of generality, we may reorder the factors of $N = q_1 \cdots q_r$ in such a way that $i = 1$ and $j = 2$. Let φ_1 denote the isogeny from E with kernel G_1 and let φ_2 denote the isogeny from E with kernel G_2. Let φ_2' denote the isogeny from E/G_1 with kernel $\varphi_1(G_2)$ and let φ_1' denote the isogeny from E/G_2 with kernel $\varphi_2(G_1)$.

By definition, we have:

$$\begin{aligned}
&D_2(D_1(E, G))\\
&\quad = \Big((E/G_1)/\varphi_1(G_2), \varphi_2'(\widehat{G}_1) \oplus \ker \widehat{\varphi_2'} \oplus \varphi_2'(\varphi_1(G_3)) \oplus \cdots \oplus \varphi_2'(\varphi_1(G_r)\Big),\\
&D_1(D_2(E, G))\\
&\quad = \Big((E/G_2)/\varphi_2(G_1), \ker \widehat{\varphi_1'} \oplus \varphi_1'(\widehat{G}_2) \oplus \varphi_1'(\varphi_2(G_3)) \oplus \cdots \oplus \varphi_1'(\varphi_2(G_r))\Big).
\end{aligned}$$

There exist isomorphisms

$$\begin{aligned}
\eta_1 &: (E/G_1)/\varphi_1(G_2) \longrightarrow E/(G_1 \oplus G_2),\\
\eta_2 &: (E/G_2)/\varphi_2(G_1) \longrightarrow E/(G_1 \oplus G_2),
\end{aligned}$$

since $G_1 \oplus G_2$ is the kernel of the composition of the two quotients, in both cases. So $\eta := \eta_1^{-1} \circ \eta_2$ is an isomorphism $(E/G_2)/\varphi_2(G_1) \cong (E/G_1)/\varphi_1(G_2)$. This is summarized in the following commutative diagram where we see $\eta \circ \varphi_1' \circ \varphi_2 = \varphi_2' \circ \varphi_1$:

$$\begin{tikzcd}
E \arrow[r, "\varphi_1"] \arrow[d, equal] & E/G_1 \arrow[r, "\varphi_2'"] & E/(G_1 \oplus \varphi_1(G_2)) \\
E \arrow[r, "\varphi_2"] & E/G_2 \arrow[r, "\varphi_1'"] & E/(\varphi_2(G_1) \oplus G_2) \arrow[u, "\eta"]
\end{tikzcd}$$

We will show that the isomorphism η satisfies the following three properties:

(1) $\eta(\ker \widehat{\varphi_1'}) = \varphi_2'(\widehat{G}_1)$,
(2) $\eta(\varphi_1'(\widehat{G}_2)) = \ker \widehat{\varphi_2'}$,
(3) $\eta(\varphi_1'(\varphi_2(G_i))) = \varphi_2'(\varphi_1(G_i))$ for all $i = 3, 4, \ldots, r$.

For the first property, plug the q_1-torsion of E into both sides of the equation $\eta \circ \varphi_1' \circ \varphi_2 = \varphi_2' \circ \varphi_1$:

$$\begin{aligned}
\eta \circ \varphi_1' \circ \varphi_2(E[q_1]) &= \varphi_2' \circ \varphi_1(E[q_1])\\
\eta \circ \varphi_1'((E/G_2)[q_1]) &= \varphi_2'(\widehat{G}_1)\\
\eta(\ker \widehat{\varphi_1'}) &= \varphi_2'(\widehat{G}_1)
\end{aligned}$$

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

(A) Given an isomorphism $\alpha : E' \to E$ and the p-power Frobenius $\pi_p : E' \to (E')^p$, there exists a unique isogeny $\lambda : E \to (E')^p$ such that $\lambda \circ \alpha = \pi_p^{E'}$.

$$\begin{tikzcd}
E' \arrow[rr, "\alpha"] \arrow[dd, "\pi_p^{E'}"'] & & E \arrow[dl, dashed, "\pi_p^E"] \\
& E^p \arrow[dl, "\beta"] & \\
(E')^p & &
\end{tikzcd}$$

(B) By inseparable degrees of the right and left sides of $\lambda \circ \alpha = \pi_p^{E'}$, we decompose $\lambda = \beta \circ \pi_p^E$ where $\beta : E^p \to (E')^p$ is an isomorphism.

Figure 4.1. Diagram to support Lemma 4.6 in proving F_p is well-defined on equivalence classes of $|\mathcal{S}_N|$.

The second property follows symmetrically after applying η^{-1} to both sides. The third property is immediate by plugging G_i into both sides of the equation $\eta \circ \varphi_1' \circ \varphi_2 = \varphi_2' \circ \varphi_1$, for $i \in \{3, \ldots, r\}$.

We have established $D_1(D_2(E, G)) \sim D_2(D_1(E, G))$ via the isomorphism

$$\eta(D_1(D_2(E, G))) = D_2(D_1(E, G)). \qquad \square$$

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:

Definition 4.5 (Frobenius Involution on $|\mathcal{S}_N|$)**.**

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

where E^p is the codomain of $\pi_p^E : E \to E^p$ and $G^p = \pi_p^E(G)$.

Lemma 4.6 shows that this Frobenius involution gives an involution F_p on the set of equivalence classes $|\mathcal{S}_N|$.

Lemma 4.6. If $(E, G) \sim (E', G')$ as in Definition 3.1, then $F_p(E, G) \sim F_p(E', G')$.

Proof. Suppose $\alpha : E' \to E$ is the isomorphism such that $\alpha(G') = G$. Let $\pi_p^{E'} : E' \to (E')^p$ denote the p-power Frobenius map of E'. Since α is separable and $\ker \alpha = O_{E'} \subseteq \ker \pi_p^{E'}$, there exists a unique isogeny $\lambda : E \to (E')^p$ such that $\pi_p^{E'} = \lambda \circ \alpha$ [31, Corollary III.4.11]. See Figure 4.1a.

By comparing the total and inseparable degrees of the left and right sides of $\pi_p^{E'} = \lambda \circ \alpha$, we see that λ decomposes as $\lambda = \beta \circ \pi_p^E$, where β is separable and of degree 1. See Figure 4.1b.

Thus, $\beta : E^p \to (E')^p$ is an isomorphism. Moreover, $\beta \circ \pi_p^E \circ \alpha = \pi_p^{E'}$, and plugging in G' we have:

$$\begin{aligned}\pi_p^{E'}(G') &= \beta \circ \pi_p^E \circ \alpha(G') \\ (G')^p &= \beta \circ \pi_p^E(G) \\ (G')^p &= \beta(G^p)\end{aligned}$$

so β realizes $(E^p, G^p) \sim ((E')^p, (G')^p)$. □

Lemma 4.7. For all $i = 1, \dots, r$,

$$D_i(F_p(E,G)) \sim F_p(D_i(E,G)).$$

Proof. Without loss of generality, we assume $D_i = D_1$ corresponding to the factorizations $N = q_1 \cdots q_r$ with q_i distinct primes and $G = G_1 \oplus \cdots \oplus G_r$ with $|G_i| = q_i$.

With the notation established, we wish to show that

$$\begin{aligned}&((E/G_1)^p, (\widehat{G}_1)^p \oplus \varphi_1(G_2)^p \oplus \cdots \oplus \varphi_1(G_r)^p) \\ &\qquad\qquad \sim (E^p/G_1^p, \widehat{G_1^p} \oplus \varphi_{G_1^p}(G_2^p) \oplus \cdots \varphi_{G_1^p}(G_r^p)).\end{aligned}$$

Since $\varphi_1 : E \to E/G_1$ is separable and $\varphi_{G_1^p} \circ \pi_p^E(G_1) = O_{E^p/G_1^p}$, there exists a unique isogeny $\lambda : E/G_1 \to E^p/G_1^p$ such that $\lambda \circ \varphi_1 = \varphi_{G_1^p} \circ \pi_p^E$. See Figure 4.2a. By comparing the total and inseparable degrees of the left and right sides of $\lambda \circ \varphi_1 = \varphi_{G_1^p} \circ \pi_p^E$, we see that λ decomposes as $\alpha \circ \pi_p^{E/G_1}$, where π_p^{E/G_1} is the p-power Frobenius map on E/G_1 and α is an isomorphism. See Figure 4.2b.

Finally, to establish that $D_1(F_p(E,G)) \sim F_p(D_1(E,G))$, we must show

$$\alpha((\widehat{G}_1)^p \oplus \varphi_1(G_2)^p \oplus \cdots \oplus \varphi_1(G_r)^p) = \widehat{G_1^p} \oplus \varphi_{G_1^p}(G_2^p) \oplus \cdots \varphi_{G_1^p}(G_r^p),$$

which can be accomplished by showing the following two properties:

(1) $\alpha((\widehat{G}_1)^p) = \widehat{G_1^p}$ and
(2) $\alpha(\varphi_1(G_i)^p) = \varphi_{G_1^p}(G_i^p)$ for all $i = 2, \dots, r$.

For the first property, plug the q_1-torsion of E into both sides of the equation $\alpha \circ \pi_p^{E/G_1} \circ \varphi_1 = \varphi_{G_1^p} \circ \pi_p^E$:

$$\begin{aligned}\alpha \circ \pi_p^{E/G_1} \circ \varphi_1(E[q_1]) &= \varphi_{G_1^p} \circ \pi_p^E(E[q_1]) \\ \alpha \circ \pi_p^{E/G_1}(\widehat{G}_1) &= \varphi_{G_1^p}(E^p[q_1]) \\ \alpha((\widehat{G}_1)^p) &= \widehat{G_1^p}.\end{aligned}$$

$$\begin{tikzcd}
E \arrow[r, "\pi_p^E"] \arrow[d, "\varphi_1"'] & E^p \arrow[r, "\varphi_{G_1^p}"] & E^p/G_1^p \\
E/G_1 \arrow[rru, dashed, "\lambda"'] & &
\end{tikzcd}$$

(A) Given the separable isogeny $\varphi_1 : E \to E/G_1$ and the isogeny $\varphi_{G_1^p} \circ \pi_p^E$, there exists a unique isogeny $\lambda : E/G_1 \to E^p/G_1^p$ such that $\lambda \circ \varphi_1 = \varphi_{G_1^p} \circ \pi_p^E$.

$$\begin{tikzcd}
E \arrow[r, "\pi_p^E"] \arrow[dd, "\varphi_1"'] & E^p \arrow[r, "\varphi_{G_1^p}"] & E^p/G_1^p \\
 & (E/G_1)^p \arrow[ru, "\alpha"'] & \\
E/G_1 \arrow[ru, "\pi_p^{E/G_1}"'] & &
\end{tikzcd}$$

(B) By inseparable degrees of the right and left sides of $\lambda \circ \varphi_1 = \varphi_{G_1^p} \circ \pi_p^E$, we decompose $\lambda = \alpha \circ \pi_p^{E/G_1}$, where $\alpha : (E/G_1)^p \to E^p/G_1^p$ is an isomorphism.

Figure 4.2. Diagram to support Lemma 4.7 in proving that F_p and D_1 commute on equivalence classes of $|\mathcal{S}_N|$.

For the second property, we proceed in the same way by plugging G_i into both sides of the equation $\alpha \circ \pi_p^{E/G_1} \circ \varphi_1 = \varphi_{G_1^p} \circ \pi_p^E$:

$$\begin{aligned} \alpha \circ \pi_p^{E/G_1} \circ \varphi_1(G_i) &= \varphi_{G_1^p} \circ \pi_p^E(G_i) \\ \alpha(\varphi_1(G_i)^p) &= \varphi_{G_1^p}(G_i^p). \end{aligned}$$

□

4.2. Fibers of $\mathcal{O}(\,\cdot\,,\cdot\,)$. The involutions D_i and F_p descend to well-defined involutions on isomorphism classes of Eichler orders via the map $\mathcal{O}(\,\cdot\,,\cdot\,)$ as defined in Definition 3.2. In this section, we show that these descended involutions are all trivial on isomorphism classes of Eichler orders. As in the previous section, we factor N into distinct prime factors $N = q_1 \cdots q_r$, we decompose $G = G_1 \oplus \cdots \oplus G_r$ with $|G_i| = q_i$, and we let D_i denote the dualizing involutions for $i \in \{1, \ldots, r\}$.

Lemma 4.8. For any $(E, G) \in |\mathcal{S}_N|$ and any $i \in \{1, \ldots, r\}$, $\mathcal{O}(D_i(E, G)) \cong \mathcal{O}(E, G)$. Moreover, the isomorphism is given by an isomorphism of the quaternion algebras $B_{p,\infty}^{E/G_i} \to B_{p,\infty}^E$.

Proof. Without loss of generality, reorder the factors of N, G such that $D_i = D_1$. By definition of the dualizing involution, we have:

$$D_1(E, G) = (E/G_1, \widehat{G}_1 \oplus \varphi_1(G_2) \oplus \cdots \oplus \varphi_1(G_r)),$$

where $\varphi_1 : E \to E/G_1$ is the isogeny with $\ker \varphi_1 = G_1$ and where $\widehat{G}_1 = \ker \widehat{\varphi}_1$. To ease notation,

$$D_1(G) := \widehat{G}_1 \oplus \varphi_1(G_2) \oplus \cdots \oplus \varphi_1(G_r).$$

By Proposition 3.4,

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

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

$$\begin{aligned}
&[\mathcal{O}(D_1(E,G)) \\
&\quad = \operatorname{End}(E/G_1) \cap \left(\frac{1}{\deg \varphi_{D_1(G)}} \widehat{\varphi}_{D_1(G)} \operatorname{End}((E/G_1)/D_1(G))\varphi_{D_1(G)}\right) \\
&\quad \subseteq B_{p,\infty}^{E/G_1},
\end{aligned}$$

where $\varphi_{D_1(G)} : E/G_1 \to (E/G_1)/D_1(G)$ is the isogeny with kernel $D_1(G)$.

The map from $B_{p,\infty}^{E/G_1} \to B_{p,\infty}^{E}$ is given by conjugation by $\frac{1}{q_1}\widehat{\varphi}_1(-)\varphi_1$. Mapping $\mathcal{O}(D_1(E,G))$ into $B_{p,\infty}^{E}$ by this map, we wish to show

$$\frac{1}{q_1}\widehat{\varphi}_1 \mathcal{O}(D_1(E,G)))\varphi_1 = \mathcal{O}(E,G).$$

We will achieve this by showing containment in one direction. As these are Eichler orders of the same level, this suffices to show equality.

Take $\alpha \in \mathcal{O}(D_1(E,G))$. By definition, α satisfies the following two properties:

(1) $\alpha(\widehat{G}_1) \subseteq \widehat{G}_1$, and
(2) $\alpha(\varphi_1(G_i)) \subseteq \varphi_1(G_i)$ for $i = 2, \ldots, r$.

We need to show that $\frac{1}{q_1}\widehat{\varphi}_1 \circ \alpha \circ \varphi_1$ satisfies the following two properties:

(1) $\frac{1}{q_1}\widehat{\varphi}_1 \circ \alpha \circ \varphi_1(G_1) \subseteq G_1$, and
(2) $\frac{1}{q_1}\widehat{\varphi}_1 \circ \alpha \circ \varphi_1(G_i) \subseteq G_i$ for $i = 2, \ldots, r$.

For the first property, we plug G_1 into the equation and use the fact that $G_1 = \widehat{\varphi}_1((E/G_1)[q_1])$ and $\alpha((E/G_1)[q_1]) \subseteq (E/G_1)[q_1]$:

$$\begin{aligned}
\frac{1}{q_1}\widehat{\varphi}_1 \circ \alpha \circ \varphi_1(G_1) &= \frac{1}{q_1}\widehat{\varphi}_1 \circ \alpha \circ \varphi_1(\widehat{\varphi}_1((E/G_1)[q_1])) \\
&= \widehat{\varphi}_1 \circ \alpha((E/G_1)[q_1]) \subseteq \widehat{\varphi}_1((E/G_1)[q_1]) = G_1.
\end{aligned}$$

For the second property, take G_i with $i \in \{2, \ldots, r\}$ and plug into the equation and use the fact that $\alpha(\varphi_1(G_i)) \subseteq \varphi(G_i)$:

$$\frac{1}{q_1}\widehat{\varphi}_1 \circ \alpha \circ \varphi_1(G_i) \subseteq \frac{1}{q_1}\widehat{\varphi}_1(\varphi_1(G_i)) = G_i.$$

This establishes that $\frac{1}{q_1}\widehat{\varphi}_1 \mathcal{O}(D_1(E,G)))\varphi_1 = \mathcal{O}(E,G)$, and thus $\mathcal{O}(D_1(E,G))) \cong \mathcal{O}(E,G)$, where the isomorphism is the map $B_{p,\infty}^{E/G_1} \to B_{p,\infty}^{E}$ given by conjugation by φ_1. □

Denote an arbitrary composition of D_i involutions as $D_J(E,G) = (\varphi_J(E), G_J)$, where $J \subseteq \{1,\dots,r\}$ (including the possibility $J = \varnothing$), to ease notation. There are 2^r possible compositions of dualizing involutions: $(E,G), D_1(E,G), D_2(E,G), \dots, D_2 \circ D_1(E,G), \dots$, etc. For every arbitrary composition $D_J(E,G)$, we have $\mathcal{O}(E,G) = \mathcal{O}(D_J(E,G))$.

Lemma 4.9. For any $(E,G) \in |\mathcal{S}_N|$, $\mathcal{O}(F_p(E,G)) \cong \mathcal{O}(E,G)$. Moreover, the isomorphism is given by an isomorphism of the quaternion algebras $B_{p,\infty}^{E^p} \to B_{p,\infty}^{E}$.

Proof. By Proposition 3.4,

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

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

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

where $\varphi_{G^p} : E^p \to E^p/G^p$ 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 4.7, 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 an isomorphism $\alpha : (E/G)^p \to E^p/G^p$.

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

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

Table 4.1. j-invariants and Weierstrass equations for the computations of Example 4.10.

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

Recall that $\lambda : E/G \to E^p/G^p$ factors as $\lambda = \alpha \circ \pi_p^{E/G}$, where $\alpha : (E/G)^p \to E^p/G^p$ is an isomorphism. Substituting this in above gives:

$$\begin{aligned}
\frac{1}{p}\widehat{\pi_p}\mathcal{O}(E^p, G^p)\pi_p &= \operatorname{End}(E) \cap \left(\frac{1}{p \deg \varphi_G}\widehat{\varphi_G}\widehat{\pi_p^{E/G}}\hat{\alpha} \operatorname{End}(E^p/G^p)\alpha\pi_p^{E/G}\varphi_G\right) \\
&= \operatorname{End}(E) \cap \left(\frac{1}{p \deg \varphi_G}\widehat{\pi_p^{E/G}\varphi_G} \operatorname{End}((E/G)^p)\pi_p^{E/G}\varphi_G\right) \\
&\overset{(*)}{=} \operatorname{End}(E) \cap \left(\frac{1}{\deg \varphi_G}\widehat{\varphi_G} \operatorname{End}(E/G)\varphi_G\right) \\
&= \mathcal{O}(E, G),
\end{aligned}$$

where the equality $(*)$ follows from

$$\frac{1}{p}\widehat{\pi_p^{E/G}} \operatorname{End}((E/G)^p)\pi_p^{E/G} = \operatorname{End}(E/G).$$

We have recovered $\mathcal{O}(E^p, G^p) \cong \mathcal{O}(E, G)$, where the isomorphism is the map $B_{p,\infty}^{E^p} \to B_{p,\infty}^{E}$ given by conjugation by π_p. □

The fiber along $\mathcal{O}(\,\cdot\,,\cdot\,)$ above $\mathcal{O}(E, G)$ contains $D_J(E, G), D_J(E^p, G^p) \in |\mathcal{S}_N|$. We will see that these are the only possible elements of the fiber along $\mathcal{O}(\,\cdot\,,\cdot\,)$ in Theorem 4.13. However, this does not mean that the fiber along $\mathcal{O}(\,\cdot\,,\cdot\,)$ is always of the same size: it can happen that two or more of the equivalence classes listed above coincide.

Example 4.10 ($p = 61$, $N = 2$)**.** Let $\mathbb{F}_{61^2} = \mathbb{F}_{61}[s]/(s^2 + 60s + 2)$. Table 4.1 lists supersingular j-invariants and Weierstrass equations.

Table 4.2 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 $\mathcal{O}(\,\cdot\,,\cdot\,)$.

Lemma 4.11. If $(E, G), (F, H) \in |\mathcal{S}_N|$ and $\mathcal{O}(E, G) \cong \mathcal{O}(F, H)$, then $(F, H) = D_J(E, G)$ or $D_J(E^p, G^p)$ for some $J \subseteq \{1, \ldots, r\}$.

Table 4.2. 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 $p=61$, $N=2$

(E,G)	$(E/G,\widehat{G})$	(E^p,G^p)	$((E/G)^p,\widehat{G}^p)$	$\lvert$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

Proof. By definition,

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

$$\mathcal{O}(F,H)=\operatorname{End}(F)\cap\left(\frac{1}{\deg\varphi_H}\widehat{\varphi}_H\operatorname{End}(F/H)\varphi_H\right)\subseteq B^F_{p,\infty}.$$

Fix an isomorphism $B^F_{p,\infty}\cong B^E_{p,\infty}$ and work solely in $B^E_{p,\infty}$. Our assumption gives an isomorphism

$$\begin{aligned}\operatorname{End}(E)\cap\left(\frac{1}{\deg\varphi_G}\widehat{\varphi}_G\operatorname{End}(E/G)\varphi_G\right)&\\ \cong\operatorname{End}(F)\cap\left(\frac{1}{\deg\varphi_H}\widehat{\varphi}_H\operatorname{End}(F/H)\varphi_H\right)&.\end{aligned}$$

If we localize at any prime $q\nmid N$, this isomorphism is an equality of maximal orders. At any prime $q\mid N$, $\mathcal{O}(E,G)_q$ is a local Eichler order, which is the intersection of two uniquely determined maximal orders. This gives one of two possibilities:

$$\operatorname{End}(F)_q=\operatorname{End}(E)_q\ \text{ or }\ \operatorname{End}(F)_q=\left(\frac{1}{\deg\varphi_G}\widehat{\varphi}_G\operatorname{End}(E/G)\varphi_G\right)_q,$$

where '$\cdot_q$' denotes '$\cdot\otimes_{\mathbb{Z}}\mathbb{Z}_q$'. Let $J=\{i\in\{1,\dots,r\}:\operatorname{End}(F)_{q_i}\neq\operatorname{End}(E)_{q_i}\}$ and define $(E_J,G_J):=D_J(E,G)$. Let $\varphi_J:E\to E_J$ denote the isogeny in the definition of $D_J(E,G)$. Then, $\operatorname{End}(F)_q=\left(\frac{1}{\deg\varphi_J}\widehat{\varphi}_J\operatorname{End}(\varphi_J(E))\varphi_J\right)_q$ locally at every prime q, so this equality holds globally as well. By the Deuring correspondence, either $F\cong\varphi_J(E)$ or $F\cong\pi_p\circ\varphi_J(E)$.

The proof of Lemma 4.8 gives

$$\mathcal{O}(E,G)=\frac{1}{\deg\varphi_J}\widehat{\varphi}_J\mathcal{O}(E_J,G_J)\varphi_J.$$

Applying this above:

$$\begin{aligned}
\operatorname{End}(F) \cap \left(\frac{1}{\deg \varphi_H} \widehat{\varphi}_H \operatorname{End}(F/H)\varphi_H\right) \\
&= \mathcal{O}(E,G) \\
&= \frac{1}{\deg \varphi_J} \widehat{\varphi}_J \mathcal{O}(E_J, G_J)\varphi_J \\
&= \left(\frac{1}{\deg \varphi_J} \widehat{\varphi}_J \operatorname{End}(E_J)\varphi_J\right) \\
&\qquad \cap \left(\frac{1}{\deg \varphi_J} \widehat{\varphi}_J \left(\frac{1}{\deg \varphi_{G_J}} \widehat{\varphi}_{G_J} \operatorname{End}(E_J/G_J)\varphi_{G_J}\right)\varphi_J\right),
\end{aligned}$$

where $\varphi_{G_J} : E_J \to E_J/G_J$ denotes the isogeny with kernel G_J.

Since $\operatorname{End}(F) = \frac{1}{\deg \varphi_J} \widehat{\varphi}_J \operatorname{End}(E_J)\varphi_J$, the left ideal linking $\operatorname{End}(F)$ to $\operatorname{End}(F/H)$ is the same left ideal linking $\operatorname{End}(E_J)$ to $\operatorname{End}(E_J/G_J)$, up to conjugation by φ_J. The connecting ideal determines the kernel of a separable isogeny, giving either $(F,H) = (E_J, G_J)$ or $(F,H) = F_p(E_J, G_J)$. □

By [32, Section 23.3.19], above each of the primes dividing the reduced discriminant $pN = pq_1 \cdots q_r$ of $\mathcal{O}(E,G)$, there is a unique two-sided maximal ideal of order two in the two-sided ideal class group of $\mathcal{O}(E,G)$, and the collection of these ideals generates the two-sided ideal class group of $\mathcal{O}(E,G)$. Let $\mathfrak{p}$ denote the two-sided ideal of $\mathcal{O}(E,G)$ above p and let $\mathfrak{q}_i$ denote the two-sided ideal of $\mathcal{O}(E,G)$ above q_i.

Lemma 4.12. Let $J \subseteq \{1,\dots,r\}$. Then, $(E,G) \sim F_p^e(D_J(E,G))$ if and only if $\mathfrak{p}^e \prod_{i\in J} \mathfrak{q}_i$ is a principal two-sided ideal of $\mathcal{O}(E,G)$.

Proof. For simplicity, we begin with the case $J = \{1\}$ and $e = 0$. First suppose $\mathfrak{q}_1$ is principal with generator $\psi \in \mathcal{O}(E,G)$. Then, $\psi(G) \subseteq G$ and $\deg \psi = Nrd(\mathfrak{q}_1) = q_1$. Since q_1 is prime, either $\psi(G_1) = G_1$ or $\psi(G_1) = O_E$. By theory of hereditary orders, $\mathfrak{q}_1^2 = (q_1)$, so $[q_1] = \mu \circ \psi^2$ for some $\mu \in \operatorname{Aut}(E)$, and we must have $\psi(G_1) = O_E$. Since $\ker \varphi_1 \subseteq \ker \psi$ and $\deg \varphi_1 = \deg \psi$, there exists an isomorphism $\tau : E/G_1 \to E$ such that $\tau \circ \varphi_1 = \psi$. Since $\psi(G_i) = G_i$ for all $i = 2,\dots,r$, it follows that $\tau(\varphi_1(G_i)) = G_i$ for all $i = 2,\dots,r$. By separable degree considerations and the facts that $\psi(G_1) = O_E$ and $[q_1] = \mu \circ \psi^2$, we conclude that $\psi(E[q_1]) = G_1$. By construction, $\varphi_1(E[q_1]) = \widehat{G}_1$, so $\tau(\widehat{G}_1) = G_1$. Thus, τ gives an isomorphism from $D_1(E,G) = (\varphi_1(E), \widehat{G})$ to (E,G).

For the reverse implication, assume $(E,G) \sim D_1(E,G)$, so there exists an isomorphism $\eta : E/G_1 \to E$ such that $\eta(\widehat{G}) = G$. Additionally, $\eta \circ \varphi_1$ is an endomorphism of E and $\eta \circ \varphi_1(G) = G_2 \oplus \cdots \oplus G_r \subseteq G$, so $\eta \circ \varphi_1 \in \mathcal{O}(E,G)$. Thus, $\eta \circ \varphi_1$ generates a two-sided ideal of $\mathcal{O}(E,G)$ of norm q_1. To see that this is the unique two-sided ideal $\mathfrak{q}_1$ of $\mathcal{O}(E,G)$ above q_1, we show that

$[q_1] \in (\eta \circ \varphi_1)^2$:

$$\begin{aligned}(\eta \circ \varphi_1 \circ \eta \circ \varphi_1)(E[q_1]) &= (\eta \circ \varphi_1 \circ \eta)(\widehat{G}_1)\\ &= (\eta \circ \varphi_1)(G_1)\\ &= O_E.\end{aligned}$$

The above argument establishes that $(E,G) \sim D_1(E,G)$ if and only if $\mathfrak{q}_1$ is a principal two-sided ideal of $\mathcal{O}(E,G)$.

Now, suppose $e = 1$. For simplicity, assume $J = \varnothing$. If $\mathfrak{p}$ is a principal two-sided ideal of $\mathcal{O}(E,G)$, then by [32, 23.3.19], $\mathfrak{p}$ is the unique prime two-sided ideal of $\mathcal{O}(E,G)$ above p and $\mathfrak{p}^2 = (p)$. Let $\pi \in \mathcal{O}(E,G)$ denote the generator of $\mathfrak{p}$, which must be of degree p. Recall that E is supersingular, and so $[p]$ is purely inseparable. By definition, $\pi(E) = E$ and $\pi(G) \subseteq G$. It follows by degree argument that $\pi = \alpha \circ \pi_p^E$ for an isomorphism $\alpha : E^p \to E$ sending $G^p \to G$, so we have $(E,G) \sim F_p(E,G)$. Conversely, suppose $(E,G) \sim F_p(E,G)$. Let $\omega : E^p \to E$ be the isomorphism such that $\omega(G^p) = G$. Then $\omega \circ \pi_p^E$ generates a principal two-sided ideal of $\mathcal{O}(E,G)$ of norm p, which is necessarily the unique principal two-sided ideal of $\mathcal{O}(E,G)$ above p.

For general J, e, both directions of the proof require us to establish the existence of an element $\psi \in \mathcal{O}(E,G)$ of norm $p^e \prod_{i\in J} q_i$ with inseparable degree p^e and $\psi(G_i) = O_E$ and $\psi(E[q_i]) = G_i$ for $i \in J$, and $\psi(G_i) = G_i$ for $i \notin J$. Such properties are necessary and sufficient to prove the existence of a unique isomorphism η such that $\eta \circ \varphi_J \circ (\pi_p^E)^e) = \psi$, and η establishes the isomorphism required to show $(E,G) \sim D_J(F_p^e(E,G))$. □

Theorem 4.13. Let $\mathcal{O}$ be an Eichler order of $B_{p,\infty}$ of squarefree 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 $\mathcal{O}(E,G) \cong \mathcal{O}$. Moreover, the fiber above $\mathcal{O}(E,G)$ along the map $\mathcal{O}(\,\cdot\,,\cdot\,)$ contains precisely the equivalence classes (E,G), $D_J(E,G)$, $F_p(E,G)$, and $D_J(F_p(E,G))$, where D_J denotes the composition of dualizing involutions for some $J \subseteq \{1,\dots,r\}$. This fiber is of size 2^k for some $k \in \{0,1,\dots,r+1\}$.

Proof. By Proposition 3.8, $\mathcal{O} \cong \mathcal{O}(E,G)$ for some $(E,G) \in |\mathcal{S}_N|$. By Lemma 4.8 and Lemma 4.9, the fiber above $\mathcal{O}$ along $\mathcal{O}(\,\cdot\,,\cdot\,)$ contains $D_J(E,G)$ and $D_J(E^p,G^p)$ for all $J \subseteq \{1,\dots,r\}$: $\mathcal{O} \cong \mathcal{O}(D_J(E,G)) \cong \mathcal{O}(D_J(E^p,G^p))$. Lemma 4.11 shows these are the only possible elements of the fiber above $\mathcal{O}$ along $\mathcal{O}(\,\cdot\,,\cdot\,)$. Lemma 4.12 shows that the two-sided ideal class group of $\mathcal{O}(E,G)$ dictates when $F_p^{e_1}(D_{J_1}(E,G)) \sim F_p^{e_2}(D_{J_2}(E,G))$. Since $\mathcal{O}$ is a hereditary order of level N, the only possible non-principal two-sided ideals of $\mathcal{O}$ are the 2^{r+1} products of the ideals above primes dividing pN, and the information of Lemma 4.12 completely determines the number of distinct pairs of $|\mathcal{S}_N|$ with isomorphic images under the map

$\mathcal{O}(\,\cdot\,,\cdot\,)$. Since $D_i(D_i(E,G)) \sim (E,G)$ and $F_p(F_p(E,G)) \sim (E,G)$, any relation among the elements of the fiber above $\mathcal{O}(E,G)$ along $\mathcal{O}(\,\cdot\,,\cdot\,)$ can be phrased as $(E,G) \sim \cdot$, and the fiber size is equal to size of the two-sided ideal class group of $\mathcal{O}(E,G)$. □

For example, if $\mathfrak{q}_1$ is the only principal two-sided ideal of $\mathcal{O}(E,G)$, then $(E,G) \sim D_1(E,G)$ and the fiber above $\mathcal{O}$ along $\mathcal{O}(\,\cdot\,,\cdot\,)$ is of size 2^r containing the inequivalent elements $F_p^e(D_J(E,G))$ for all $(e,J) \subseteq \{0,1\} \times \mathcal{P}(\{2,\dots,r\})$, where $\mathcal{P}$ denotes the power set.

Example 4.14. We fix $p = 1123$ and $N = 2 \cdot 3 \cdot 5$ and use Magma [5] to enumerate the isomorphism classes of Eichler orders of level N in the definite quaternion algebra ramified at p and ∞. There are 456 such classes. Then, we can use built-in functions of Magma to determine the sizes of the two-sided ideal class groups of these orders:

- No isomorphism classes have two-sided ideal class groups of sizes 1 or 2.
- Three isomorphism classes have two-sided ideal class groups of size 4.
- Sixty-six isomorphism classes have two-sided ideal class groups of size 8.
- The remaining three hundred and eighty-seven isomorphism classes have two-sided ideal class groups of 16.

This indicates the expected "generic" behavior when p is large relative to N: the fiber size is in general as large as possible, as collisions via the involutions we have defined do not often occur.

5. Counting N-isogenies $E \to E^p$

In this section, we require N to be a prime $N \neq p$, and we will note where we use the fact that $N << p$. 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 [8, Lemma 6] and [17, Theorem 3.9] in Section 5.2.

Let α_N denote the number of pairs $(E,\psi) \in |\mathcal{S}_N|$ 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.

For this section, we assume $p \equiv 1 \pmod{12}$ unless otherwise stated. This is to avoid the case where there are fewer than $(N+1)$ level-N structures on a supersingular elliptic curve E (see Section 3.1.1). In this case, we have $\#|\mathcal{S}_N| = (N+1)(\#\mathbf{S}_p)$, where $\#(\mathbf{S}_p)$ denotes the number of supersingular j-invariants over $\overline{\mathbb{F}}_p$.

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 $B_{p,\infty}$.

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

$$\mathcal{F}_1 + \mathcal{F}_2 + \mathcal{F}_4 = T \tag{5.1}$$

$$\mathcal{F}_1 + 2\mathcal{F}_2 + 4\mathcal{F}_4 = \#|\mathcal{S}_N| = (N+1)(\#\mathbf{S}_p). \tag{5.2}$$

Proof. For (5.1): every Eichler order of level N has fiber size 1, 2, or 4 along $\mathcal{O}(\,\cdot\,,\cdot\,)$ by Theorem 4.13. For (5.2): 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 $\mathcal{F}_2$:

$$\mathcal{F}_2 = 2T - \frac{N+1}{2}(\#\mathbf{S}_p) - \frac{3}{2}\mathcal{F}_1. \tag{5.3}$$

When the fiber above $\mathcal{O}(E,G)$ is size one, all of the involutions described in Section 4 act as the identity: In particular, the isogeny φ_G is an endomorphism with kernel stable under the p-power Frobenius. For N much smaller than p, curves with degree-N endomorphisms are rare: The number of curves with a non-scalar endomorphism of degree less than or equal to N is $O(N^{3/2})$ (see for example [21]). Example 4.14 provides some empirical evidence to this claim. Assuming $\mathcal{F}_1 = 0$, we obtain an approximate upper bound for $\mathcal{F}_2$ from Equation (5.3):

$$2T - \frac{N+1}{2}(\#\mathbf{S}_p). \tag{5.4}$$

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 [2]). Therefore, Equation (5.4) 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:

$$4T - (N+1)(\#\mathbf{S}_p). \tag{5.5}$$

This approximate upper-bound for α'_N can be compared with the data computed in [2], 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 [2]. 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 [2], we computed α'_N for a wide range of values p.

Subsequently, [17] 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 [8, Lemma 6], which provides an approximation for this value. The authors also provided a lower-bound [17, 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, we plot this rational function for $N = 3$ against the data for 3-isogenous conjugates provided in [2] and the upper-bound for α'_3 in Equation (5.5) is plotted.

The big-O notation approximation provided in [8, Lemma 6] can be adjusted to give an exact count of N-isogenous conjugate curves. To begin this analysis, we provide the statement of [8, Lemma 6]:

Lemma 5.2 (Lemma 6 [8])**.** 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

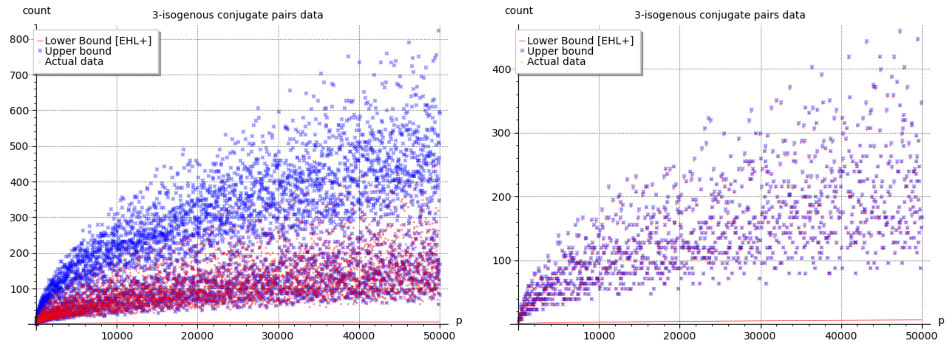
$$\alpha(i) = \ell^{i/2}\widetilde{O}(\sqrt{p}).$$

Inspired by Lemma 5.2, we prove the precise value of α_N. Chenu and Smith [9, Theorem 2] provide an alternative proof of this proposition.

Proposition 5.3. Let N be a prime such that $N < p/4$. 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 $\mathrm{End}(E)$.

Furthermore,

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



(A) All primes $5 \leq p < 50000$. A total of 5131 data points.

(B) Primes $5 \leq p < 50000$ with $p \equiv 1 \pmod{12}$. A total of 1264 data points.

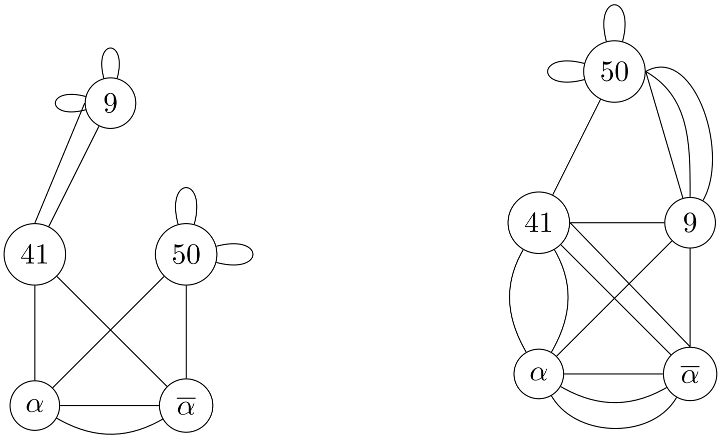
Figure 5.1. The counts of 3-isogenies between distinct p-power Frobenius conjugate supersingular elliptic curves over $\overline{\mathbb{F}}_p$. For $p \equiv 1 \pmod{12}$, the estimated upper bound described in this section was never off by more than four: exactly accurate for 23.33% of the data, over by two for 51.34% of the data, and over by four for 25.32% of the data. The lower bound from [17] is plotted in red.

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 $h \circ \pi_p$, where π_p is the p-power 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 $\mathrm{End}(E)$ [8, Lemma 6]. 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 [24]. By [9, 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



(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.

contained in the maximal order of $\mathbb{Q}(\sqrt{-pN})$, then this is not the full picture. If the ring of integers $\mathcal{O}_{\mathbb{Q}(\sqrt{-pN})} = \mathbb{Z}[\frac{1+\sqrt{-pN}}{2}] \supsetneq \mathbb{Z}[\sqrt{-pN}]$, then we will also want to count primitive embeddings of $\mathcal{O}_{\mathbb{Q}(\sqrt{-pN})}$.

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

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

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 [19]. In this categorical version, the supersingular elliptic curve objects are enhanced by the data of a Frobenius isogeny, as are the quaternion objects. Voight [32] presents a variation of this equivalence of categories, without this additional enhancement:

Theorem 6.1 ([32, Theorem 42.3.2])**.** Fix a supersingular elliptic curve E_0 with endomorphism ring $\mathcal{O}_0$. The functor $\operatorname{Hom}(\,\cdot\,, E_0)$ 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-$\mathcal{O}_0$-modules, under nonzero left $\mathcal{O}_0$-module homomorphisms.

We present an equivalence of categories for supersingular elliptic curves with level-N structure. We return to the case where N is any squarefree integer coprime to p.

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 an 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 left $\mathcal{O}(E, G)$-module homomorphism.

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

Definition 6.4. We let $\hbar_{(E,G)}$ denote the functor $\operatorname{Hom}_{\mathcal{S}_N}(-,(E,G))$, so

$$\hbar_{(E,G)}(E',G') = \operatorname{Hom}_{\mathcal{S}_N}((E',G'),(E,G)).$$

On morphisms, $\hbar_{(E,G)}$ maps $f:(E_0,G_0)\to(E_1,G_1)$ to the morphism

$$\operatorname{Hom}((E_1,G_1),(E,G)) \longrightarrow \operatorname{Hom}((E_0,G_0),(E,G))$$

given by $g\mapsto g\circ f$.

Theorem 6.5 (Equivalence of Categories)**.** Fix a supersingular elliptic curve E defined over $\overline{\mathbb{F}}_p$ and a cyclic subgroup $G\subset E[N]$ of order N. The functor $\hbar_{(E,G)}$ 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 $\hbar_{(E,G)}$ is well-defined as a functor. To see that $\hbar_{(E,G)}$ defines an equivalence of categories, it remains to show that $\hbar_{(E,G)}$ is essentially surjective and fully faithful.

First, we show that $\hbar_{(E,G)}$ 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 it is locally isomorphic to $\mathcal{O}(E,G)$. 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 [32, 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 $\operatorname{Nrd}(I)$. The norm $\operatorname{Nrd}(I)$ must be prime to N, otherwise it would violate the invertibility of the original left $\mathcal{O}(E,G)$-module. By Lemma 6.7, $I=\hbar_{(E,G)}(E_I,G_I)\varphi_I$ such that $\varphi_I:E\to E_I$ is a degree $\operatorname{Nrd}(I)$ isogeny and $\varphi_I(G)\subseteq G_I$. This identification shows $\hbar_{(E,G)}$ is essentially surjective.

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

$$\operatorname{Hom}_{\mathcal{S}_N}((E_{I'},G_{I'}),(E_I,G_I)) \longrightarrow \operatorname{Hom}_{\mathcal{LM}}(\hbar_{(E,G)}(E_I,G_I),\hbar_{(E,G)}(E_{I'},G_{I'}))$$

from morphisms in $\mathcal{S}_N$ to morphisms in $\mathcal{LM}$ is bijective. This is done in Lemma 6.10. □

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

Proof. By [32, Lemma 42.1.11], $\operatorname{Hom}(E',E)$ is a $\mathbb{Z}$-module of rank 4. By definition, $\hbar_{(E,G)}(E',G')$ contains the set $\{\phi\in\operatorname{Hom}(E',E):G'\subseteq\ker\phi\}$. By Corollary III.4.11 of [31], this set is equivalently characterized:

$$\begin{aligned}\{\phi\in\operatorname{Hom}(E',E):G'\subseteq\ker\phi\} &= \{\phi\circ\varphi_{G'}:\phi\in\operatorname{Hom}(E'/G',E)\}\\ &= \operatorname{Hom}(E'/G',E)\varphi_{G'},\end{aligned}$$

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 $\hbar_{(E,G)}(E', G')$ is rank 4 as well.

To prove the invertibility of $\hbar_{(E,G)}(E', G')$ as a left $\mathcal{O}(E, G)$-module, we use the fact that $\mathcal{O}(E, G)$ is isomorphic to a hereditary order of squarefree level coprime to p in the quaternion algebra $B_{p,\infty}$, see Theorem 3.7. This strategy is similar to the maximal order case, detailed in [32, Lemma 42.1.11]. Take a nonzero isogeny $\psi \in \hbar_{(E,G)}(E', G')$ and let $\widehat{\psi}$ denote the dual of ψ. Then, $I := \hbar_{(E,G)}(E', G')\widehat{\psi} \subset \mathcal{O}(E, G)$ 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 [32, Section 23.1.2]). The same holds for $\hbar_{(E,G)}(E', G')$ 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 $\varphi_I(G) \subseteq G_I$, and $I = \hbar_{(E,G)}(E_I, G_I)\varphi_I$, and $\mathrm{Nrd}(I) = \deg(\varphi_I)$.

Proof. By Theorem 3.7, $\mathcal{O}(E, G)$ is isomorphic to an Eichler order. It is contained in the maximal order M isomorphic to $\mathrm{End}(E)$. By Proposition 3.9 (and [18, Lemma 3]), 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 [32, Section 42.2]). Let

$$E[\mathrm{End}(E)I] := \bigcap_{\alpha \in \mathrm{End}(E)I} \ker(\alpha) \tag{6.1}$$

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 [32, 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. 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, where I can be chosen to have norm prime to N.

Proof. Let ℓ be a prime such that $\ell \nmid pN$. By the connectedness of the ℓ-isogeny graph $\mathcal{E}_{p,\ell}^N$ of supersingular elliptic curves with level-N structure (Theorem 7.3), 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 and thus is coprime to N. Since the codomain of φ is E', we have $E' = E_{I_\varphi}$. Since $\varphi_I(G) \subseteq G'$ and the degree of φ_I is coprime to N, we have $\varphi_I(G) = G'$ and furthermore $G' = G_{I_\varphi}$. By the bijection in Lemma 3.9, $I \cap \mathcal{O}(E,G)$ is an integral left ideal of the Eichler order $\mathcal{O}(E,G)$. □

Lemma 6.9. 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

$$\left\{ \varphi : (E_{I'},G_{I'}) \to (E,G) \;\middle|\; \begin{aligned} \varphi = \sum_i \alpha_i\beta_i,\ \ \alpha_i &\in \mathrm{Hom}((E_I,G_I),(E,G)),\\ \beta_i &\in \mathrm{Hom}((E_{I'},G_{I'}),(E_I,G_I)) \end{aligned} \right\}.$$

Then, the natural map

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

is a left $\mathcal{O}(E,G)$-module isomorphism.

Proof. By construction of $\mathrm{Hom}((E_I,G_I),(E,G))\,\mathrm{Hom}((E_{I'},G_{I'}),(E_I,G_I))$, 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[32], $(m) := (\mathrm{Nrd}(I)) = I\overline{I}$. The quaternion element $[m]$ has an expression as an element of

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

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

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

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

$$\begin{aligned}\mathrm{Hom}((E_I, G_I), (E, G))\,\mathrm{Hom}((E_{I'}, G_{I'}), (E_I, G_I))& \\ \longrightarrow \mathrm{Hom}((E_{I'}, G_{I'}), (E, G))&\end{aligned}$$

is indeed surjective. □

Lemma 6.10 (Fully Faithful)**.** The functor $\hbar_{(E,G)}$ is fully faithful. In particular, the map

$$\begin{aligned}\mathrm{Hom}_{\mathcal{S}_N}((E_1, G_1), (E_2, G_2)) &\longrightarrow \mathrm{Hom}_{\mathcal{LM}}(\hbar_{(E,G)}(E_2, G_2), \hbar_{(E,G)}(E_1, G_1)) \\ \phi &\longmapsto - \circ \phi\end{aligned}$$

from morphisms in $\mathcal{S}_N$ to morphisms in $\mathcal{LM}$ furnished by $\hbar_{(E,G)}$ is bijective.

Proof. First, we check that the functor is faithful. Suppose $f, f' : (E_1, G_1) \to (E_2, G_2)$ and $\hbar_{(E,G)}(f) = \hbar_{(E,G)}(f')$, that is $g \circ f = g \circ f'$ for every $g \in \mathrm{Hom}((E_2, G_2), (E, G))$. Take any such nonzero separable isogeny g of degree coprime to $\deg f$. Notice that $\deg f = \deg f'$ by comparing degrees on the left and righthand sides of $g \circ f = g \circ f'$. Postcomposing with $\widehat{g}$, we have $[\deg g] \circ f = [\deg g] \circ f'$. Since $\mathrm{Hom}((E_1, G_1), (E, G))$ is torsion-free, we have $f = f'$.

To see that it is also full, let $\psi : \mathrm{Hom}((E_2, G_2), (E, G)) \to \mathrm{Hom}((E_1, G_1), (E, G))$ be a nonzero left $\mathcal{O}(E, G)$-module homomorphism. We need to show that there exists $f \in \mathrm{Hom}((E_1, G_1), (E_2, G_2))$ such that $\psi(x) = x \circ f$ for all $x \in \mathrm{Hom}((E_2, G_2), (E, G))$. Begin by applying Lemma 6.8 to find integral left $\mathcal{O}(E, G)$-ideals I_1, I_2 of norm prime to N such that $(E_i, G_i) = (E_{I_i}, G_{I_i})$ and corresponding isogenies $\varphi_{I_i} : E \to E_{I_i}$ for $i = 1, 2$. By Lemma 6.7:

$$\begin{aligned}\mathrm{Hom}((E_1, G_1), (E, G))\varphi_{I_1} &= I_1, \\ \mathrm{Hom}((E_2, G_2), (E, G))\varphi_{I_2} &= I_2.\end{aligned} \tag{6.2}$$

The map ψ induces a map map of ideals $\psi' : I_2 \to I_1$ given by $x \circ \varphi_{I_2} \mapsto \psi(x) \circ \varphi_{I_1}$. Since ψ is injective, ψ' is as well giving an isomorphism of left $\mathcal{O}(E, G)$-ideals (namely $I_2 \cong \psi'(I_2) \subseteq I_1$). Any such isomorphism is given by precomposition by an invertible element of the quaternion algebra, so there exists some $\beta \in \mathcal{O}(E, G) \otimes_{\mathbb{Z}} \mathbb{Q}$ such that $\psi'(x \circ \varphi_{I_2}) = x \circ \varphi_{I_2}\beta$, for all $x \circ \varphi_{I_2} \in I_2$. This shows $I_2\beta \subseteq I_1$ and $\beta \in I_2^{-1}I_1$. Together with the definition of ψ' this gives

$$x \circ \varphi_{I_2}\beta = \psi(x) \circ \varphi_{I_1} \tag{6.3}$$

for all $x \in \mathrm{Hom}((E_2, G_2), (E, G))$. The result follows when we rewrite the left side of (6.3) in order to see that $\psi(x)$ is of the form $x \circ f$ for some $f \in \mathrm{Hom}((E_1, G_1), (E_2, G_2))$. Define the lattice

$$J := \frac{1}{\deg \varphi_{I_2}} \widehat{\varphi}_{I_2} \,\mathrm{Hom}((E_1, G_1), (E_2, G_2))\varphi_{I_1}$$

in $B_{p,\infty}^E$. By Lemma 6.9,

$$\mathrm{Hom}((E_2, G_2), (E, G)) \,\mathrm{Hom}((E_1, G_1), (E_2, G_2)) = \mathrm{Hom}((E_1, G_1), (E, G))$$

and so $I_2 J = I_1$, as lattices in $B_{p,\infty}^E$. The right order of I_2 and the left order of J are both the ring of endomorphisms of (E_2, G_2) (namely the order $\frac{1}{\varphi_{I_2}} \widehat{\varphi}_{I_2} \mathcal{O}(E_2, G_2) \varphi_{I_2}$ in $B_{p,\infty}^E$). Thus, $J = I_2^{-1} I_1$. Since $\beta \in I_2^{-1} I_2 = J$, β must be of the form

$$\beta = \frac{1}{\deg \varphi_{I_2}} \widehat{\varphi}_{I_2} \circ f \circ \varphi_{I_1},$$

for some $f \in \mathrm{Hom}((E_1, G_1), (E_2, G_2))$. Plugging this into Equation (6.3) above:

$$\begin{aligned} \psi(x) \circ \varphi_{I_1} &= x \circ \varphi_{I_2} \circ \beta \\ \psi(x) \circ \varphi_{I_1} &= x \circ f \circ \varphi_{I_1} \\ \psi(x) &= x \circ f. \end{aligned}$$ □

7. The Level Structure Graph

For distinct fixed primes p and ℓ, and a fixed positive integer N coprime to $p\ell$, we define the supersingular elliptic curves with level-N structure ℓ-isogeny graph.

Definition 7.1 (Supersingular elliptic curves with level-N structure ℓ-isogeny graph, $\mathcal{E}_{p,\ell}^N$)**.** In the graph $\mathcal{E}_{p,\ell}^N$, vertices are $\overline{\mathbb{F}}_p$-isomorphism classes of pairs (E, G), where E is a supersingular elliptic curve and G is a cyclic 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 objects of $\mathcal{S}_N$ form the nodes of the graph $\mathcal{E}_{p,\ell}^N$. If we restrict the morphisms of $\mathcal{S}_N$ to isogenies of degree ℓ, we have the set of edges of $\mathcal{E}_{p,\ell}^N$.

The graph structure is easily described in the special case where N is prime: For each supersingular elliptic curve $E/\overline{\mathbb{F}}_p$ with $j(E) \neq 0, 1728$, there are $N + 1$ vertices of $\mathcal{E}_{p,\ell}^N$. For $E/\overline{\mathbb{F}}_p$ with $j(E) = 0$ or 1728, there are at most $N + 1$ vertices of $\mathcal{E}_{p,\ell}^N$: the extra automorphisms of these j-invariants may map order-N subgroups to each other (see Section 3.1.1). There is a map of graphs from $\mathcal{E}_{p,\ell}^N$ to $\mathcal{G}_{\overline{\mathbb{F}}_p}^{\ell}$ 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. Each edge corresponds to an isogeny *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 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 $\mathrm{Aut}(E_0) = \{[\pm 1], [\pm\zeta_3], [\pm\zeta_3^2]\}$ and $\mathrm{Aut}(E_{1728}) = \{[\pm 1], [\pm i]\}$. 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 7.2 ($p = 37$, $N = 3$, $\ell = 2$)**.** We provide a reference example of the graph $\mathcal{E}_{p,\ell}^N$ 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 $\mathbb{F}_{37^4} := \mathbb{F}_{37}[a]/(a^4 + 6a^2 + 24a + 2)$. We denote the 3-torsion subgroups using the a^3 term of the x-coordinate of a generating point, as computed in Sage [30]. The vertex appearance (shading and line style) aligns with the corresponding quaternion vertex, seen in Figure 7.2b. The corresponding supersingular 2-isogeny graph is shown in Figure 7.2a.

Theorem 7.3 (Connectedness of $\mathcal{E}_{p,\ell}^N$)**.** The graph $\mathcal{E}_{p,\ell}^N$ 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 [1], the authors consider the ℓ-isogeny graph with level-N structure given by a choice of N-torsion point. The connectedness of $\mathcal{E}_{p,\ell}^N$ follows, as there is a map from the Goren–Kassaei graph to $\mathcal{E}_{p,\ell}^N$ that acts surjectively on the vertex sets. □

Additionally, the result of Theorem 7.3 can be seen as a corollary of a result provided by Roda [29]. 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 [29, Section 3.3], we can prove that all of the points corresponding to a particular supersingular elliptic curve 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.

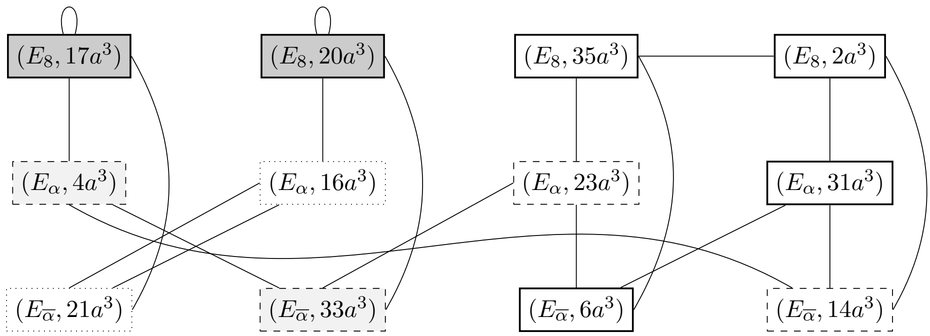
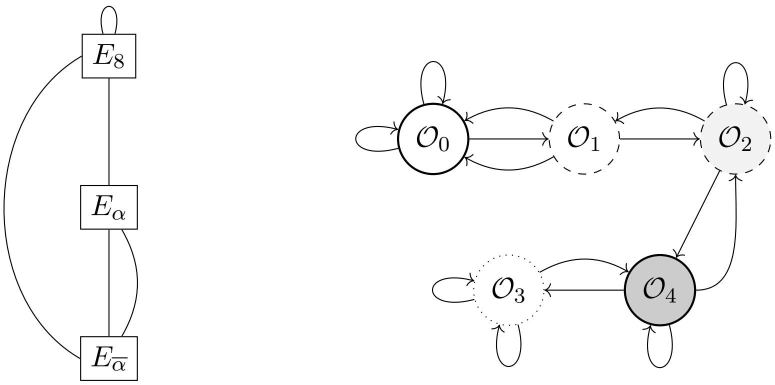


Figure 7.1. Graph of $\mathcal{E}^3_{37,2}$, with groups labeled by the first term in the x-coordinate of a generating point.



(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.

Figure 7.2

References

[1] "p-adic dynamics of Hecke operators on modular curves", *J. Théor. Nombres Bordeaux* **33** (2021), no. 2, p. 387-431.

[2] S. Arpin, C. Camacho-Navarro, K. Lauter, J. Lim, K. Nelson, T. Scholl & J. Sotáková, "Adventures in Supersingularland", *Exp. Math.* **32** (2021), no. 2, p. 1-28.

[3] S. Arpin, M. Chen, K. Lauter, R. Scheidler, K. E. Stange & H. T. N. Tran, "Orientations and cycles in supersingular isogeny graphs", 2022, `https://arxiv.org/abs/2205.03976`.

[4] ———, "Orienteering with one endomorphism", *Matematica* **2** (2023), no. 3, p. 523-582.

[5] W. Bosma, J. Cannon & C. Playoust, "The Magma algebra system. I. The user language", *J. Symb. Comput.* **24** (1997), no. 3-4, p. 235-265, Computational algebra and number theory (London, 1993).

[6] W. Castryck & T. Decru, “An efficient key recovery attack on SIDH”, in *Advances in Cryptology—EUROCRYPT 2023. Part V*, Lecture Notes in Computer Science, vol. 14008, Springer, 2023, p. 423-447.

[7] W. Castryck, T. Lange, C. Martindale, L. Panny & J. Renes, “CSIDH: an efficient post-quantum commutative group action”, in *Advances in Cryptology—ASIACRYPT 2018. Part III*, Lecture Notes in Computer Science, vol. 11274, Springer, 2018, p. 395-427.

[8] D. X. Charles, E. Z. Goren & K. Lauter, “Cryptographic hash functions from expander graphs”, *J. Cryptology* **22** (2009), no. 1, p. 93-113.

[9] M. Chenu & B. Smith, “Higher-degree supersingular group actions”, *Math. Cryptol.* **1** (2022), no. 2, p. 85-101.

[10] G. Codogni & G. Lido, “Spectral Theory of Isogeny Graphs”, 2023, `https://arxiv.org/abs/2308.13913`.

[11] L. Colò & D. Kohel, “Orienting supersingular isogeny graphs”, *J. Math. Cryptol.* **14** (2020), no. 1, p. 414-437.

[12] L. De Feo, D. Jao & J. Plût, “Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies”, *J. Math. Cryptol.* **8** (2014), no. 3, p. 209-247.

[13] C. Delfs & S. D. Galbraith, “Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$”, *Des. Codes Cryptography* **78** (2016), no. 2, p. 425-440.

[14] M. Deuring, “Die Typen der Multiplikatorenringe elliptischer Funktionenkörper”, *Abh. Math. Semin. Hansische Univ.* **14** (1941), p. 197-272.

[15] M. Eichler, “Zur Zahlentheorie der Quaternionen-Algebren”, *J. Reine Angew. Math.* **195** (1955), p. 127-151.

[16] ———, “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)*, Lecture Notes in Mathematics, vol. 320, Springer, 1973, p. 75-151.

[17] K. Eisentraeger, S. Hallgren, C. Leonardi, T. Morrison & J. Park, “Computing endomorphism rings of supersingular elliptic curves and connections to pathfinding in isogeny graphs”, in *ANTS XIV. Proceedings of the fourteenth algorithmic number theory symposium*, The Open Book Series, vol. 4, Mathematical Sciences Publishers, 2020, p. 215-232.

[18] L. D. Feo, D. Kohel, A. Leroux, C. Petit & B. Wesolowski, “SQISign: compact post-quantum signatures from quaternions and isogenies”, in *Advances in Cryptology—ASIACRYPT 2020. Part I*, Lecture Notes in Computer Science, vol. 12491, Springer, 2020, p. 64-93.

[19] D. Kohel, “Endomorphism rings of elliptic curves over finite fields”, PhD Thesis, University of California, Berkely, 1996.

[20] D. Kohel, K. Lauter, C. Petit & J.-P. Tignol, “On the quaternion ℓ-isogeny path problem”, Cryptology ePrint Archive, Report 2014/505, 2014, `https://eprint.iacr.org/2014/505`.

[21] J. Love & D. Boneh, “Supersingular curves with small noninteger endomorphisms”, in *ANTS XIV—Proceedings of the Fourteenth Algorithmic Number Theory Symposium*, The Open Book Series, vol. 4, Mathematical Sciences Publishers, 2020, p. 7-22.

[22] L. Maino & C. Martindale, “An attack on SIDH with arbitrary starting curve”, Cryptology ePrint Archive, Paper 2022/1026, 2022, `https://eprint.iacr.org/2022/1026`.

[23] L. Maino, C. Martindale, L. Panny, G. Pope & B. Wesolowski, “A direct key recovery attack on SIDH”, in *Advances in Cryptology—EUROCRYPT 2023. Part V*, Lecture Notes in Computer Science, vol. 14008, Springer, 2023, p. 448-471.

[24] H. Onuki, “On oriented supersingular elliptic curves”, *Finite Fields Appl.* **69** (2021), article no. 101777 (19 pages).

[25] A. Page & B. Wesolowski, “The supersingular Endomorphism Ring and One Endomorphism problems are equivalent”, Cryptology ePrint Archive, Paper 2023/1399, 2023, `https://eprint.iacr.org/2023/1399`.

[26] A. Pizer, “Type Numbers of Eichler Orders”, *J. Reine Angew. Math.* **264** (1973), p. 76-102.

[27] K. A. Ribet, “Bimodules and Abelian Surfaces”, in *Algebraic Number Theory — in honor of K. Iwasawa*, Advanced Studies in Pure Mathematics, vol. 17, Academic Press Inc.; Kinokuniya Company Ltd., 1989, p. 359-407.

[28] D. Robert, "Breaking SIDH in polynomial time", Cryptology ePrint Archive, Paper 2022/1038, 2022, `https://eprint.iacr.org/2022/1038`.

[29] M. Roda, "Supersingular isogeny graphs with level N structure and path problems on ordinary isogeny graphs", 2019, Master's thesis, McGill University.

[30] The Sage Developers, *SageMath, the Sage Mathematics Software System (Version 8.7)*, 2019, `https://www.sagemath.org`.

[31] J. H. Silverman, *The Arithmetic of Elliptic Curves, 2nd Edition*, Springer, 2009.

[32] J. Voight, *Quaternion algebras*, Graduate Texts in Mathematics, vol. 288, Springer, 2021, xxiii+885 pages.

[33] B. Wesolowski, "Orientations and the Supersingular Endomorphism Ring Problem", in *Advances in Cryptology—EUROCRYPT 2022* (O. Dunkelman & S. Dziembowski, eds.), Springer, 2022, p. 345-371.

Sarah Arpin
Mathematics Institute
Universiteit Leiden
Leiden, The Netherlands
Current address: The Department of Mathematics of
Virginia Polytechnic Institute and State University
E-mail: `sarpinmath@gmail.com`