DISTRIBUTION OF CYCLES IN SUPERSINGULAR ℓ-ISOGENY GRAPHS

ELI ORVIS

ABSTRACT. Recent work by Arpin, Chen, Lauter, Scheidler, Stange, and Tran [2] counted the number of cycles of length r in supersingular ℓ-isogeny graphs. In this paper, we extend this work to count the number of cycles that occur along the spine. We provide formulas for both the number of such cycles, and the average number as $p \to \infty$, with ℓ and r fixed. In particular, we show that when r is not a power of 2, cycles of length r are disproportionately likely to occur along the spine. We provide experimental evidence that this result holds in the case that r is a power of 2 as well.

1. INTRODUCTION

Supersingular isogeny graphs have enjoyed great interest in the past decade, primarily due to their applications to the study of modular forms [5] and their use in constructing post-quantum cryptographic primitives. For distinct primes p, ℓ, we denote the directed graph whose vertices are $\overline{\mathbb{F}_p}$-isomorphism classes of supersingular elliptic curves, and whose edges are isogenies of degree ℓ up to post-composition by an automorphism by $\mathcal{G}_{p,\ell}$. We will use simply $\mathcal{G}_\ell$ when there is no risk of confusion. These graphs have $(\ell + 1)$-regular out-degree, $\lfloor (p-1)/12 \rfloor + \epsilon$ vertices where $\epsilon \in \{0, 1, 2\}$, and Pizer has proven that they are Ramanujan [16].

Avoiding the existence of small cycles in $\mathcal{G}_{p,\ell}$ is advantageous in many isogeny-based cryptographic protocols. Charles, Goren, and Lauter described a method for guaranteeing that there are no small cycles in $\mathcal{G}_{p,\ell}$ when they introduced the CGL hash function, which was the first isogeny-based protocol [3]. In order to assess the soundness of SIDH-based identification protocols, Ghantous, Katsumata, Pintore, and Veroni obtained upper bounds on the expected number of cycles of a given length at a random vertex of $\mathcal{G}_{p,\ell}$ [7]. More recently, Arpin, Chen, Lauter, Scheidler, Stange, and Tran obtained a formula for the exact number of cycles of a given length in $\mathcal{G}_{p,\ell}$ in terms of class numbers of imaginary quadratic fields [2].

The *spine* of the graph, introduced by Arpin, Camacho-Navarro, Lauter, Lim, Newlso, Scholl, and Sotáková in [1], is another graph-theoretic feature of interest to isogenists. The spine is the subgraph induced by the vertices whose j-invariants are defined over $\mathbb{F}_p$, or alternatively, the subgraph induced by the set of vertices fixed by the Frobenius automorphism. It is known that for a density 1 set of primes ℓ, Frobenius is the only automorphism of the graph [14]. In most cases therefore, the set of vertices of the spine is the set of fixed points of the only non-trivial symmetry of $\mathcal{G}_{p,\ell}$. We denote the spine by $\mathcal{S}_{p,\ell}$.

In this paper we consider the distribution of cycles within the graph, in particular with respect to the spine. We study the ratio of cycles of length r that intersect the spine, for odd r, and show that as $p \to \infty$, the proportion of cycles of length r that intersect the spine eventually depends only on the residue class of p modulo a large, but computable integer. In particular, we introduce the notation n_t and n_s for the total number of r-cycles in $\mathcal{G}_{p,\ell}$, and the total number of r-cycles in $\mathcal{G}_{p,\ell}$ that intersect the spine, respectively, and we prove the following theorem:

Theorem (Theorem 4.1). *Let ℓ and r be fixed, with r odd. Then there exists a modulus M depending on ℓ and r such that for $p \gg 0$, n_t and n_s depend only on p modulo M.*

The idea behind the proof of Theorem 4.1 is to count the number of cycles along the spine in terms of imaginary quadratic class numbers. By Theorem 2.9 (Theorem 3.2 in [2]), every cycle of length r in $\mathcal{G}_\ell$ is obtained

by forgetting orientations on a subset of the oriented supersingular curves, where the orientations are from a finite set of imaginary quadratic discriminants. We then use a result of Chen and Xue [4], which says that the 2-torsion subgroup of the class group of $\mathcal{O}$ acts freely and transitively on the primitively $\mathcal{O}$-oriented supersingular curves to find that, for large enough p, the number of cycles of length r intersecting the spine depends only on p modulo M.

As a corollary to Theorem 4.1, we show that for sufficiently large p, the r-cycles in $\mathcal{G}_\ell$ either disproportionately intersect the spine, or never intersect the spine:

Corollary (Corollary 4.2). *Let ℓ and r be fixed, with r odd, and M be the modulus obtained in the previous Theorem. Then for any $[m] \in \mathbb{Z}/M\mathbb{Z}$, one of the following holds for all sufficiently large $p \in [m]$:*

(1) $n_t/\#V(\mathcal{G}_{p,\ell}) < n_s/\#V(\mathcal{S}_{p,\ell})$;
(2) $n_s = 0$,

where $\#V(G)$ denotes the number of vertices of G.

Our final result is a formula for the average value of n_s when we vary p and fix ℓ and r. Specifically, Theorem 6.10 provides a formula for the average of the sequence $n_{s,p_i}(r)$, where $n_{s,p_i}(r)$ is the number of cycles of length r in $\mathcal{G}_{p_i,\ell}$ that intersect the spine, and (p_i) is a sequence of consecutive primes:

Theorem (Theorem 6.10). *Let $(p_i)_{i=1}^\infty$ be an increasing sequence of consecutive primes. Then*

$$\lim_{n \to \infty} \frac{1}{n} \sum_{i=1}^n n_{s,p_i}(r) = \sum_{d|r} \mu(d) \#d(\mathcal{I}_{\ell,n|\frac{r}{d}}),$$

where $d(\mathcal{I}_{\ell,n|\frac{r}{d}})$ is defined in Proposition 6.1.

These results become particularly interesting in two contexts. First, interpreting cycles in $\mathcal{G}_{p,\ell}$ as cyclic endomorphisms, our results say that for large p, ℓ-power endomorphisms of a fixed degree are disproportionately likely to occur for supersingular elliptic curves defined over $\mathbb{F}_p$, as opposed to supersingular curves defined over $\mathbb{F}_{p^2}$. The methods in this paper rely primarily on the structure of the supersingular isogeny graphs and the arithmetic of quaternion algebras. An independent proof from the viewpoint of arithmetic geometry would be of interest.

Second, we can compare these results for supersingular isogeny graphs with the behavior of random $(\ell+1)$-regular graphs. A common heuristic is that, with the exception of the existence of an automorphism of order 2, the supersingular isogeny graphs "behave like random $(\ell+1)$-regular graphs." Our analysis provides another potential comparison between supersingular isogeny graphs and random graphs, by showing that odd length r-cycles in supersingular isogeny graphs do not distribute randomly throughout the graph. Instead, they are disproportionately likely to occur along the fixed vertices of the involution. It is therefore of interest to compare these results with the case of random graphs with an involution. Unfortunately, we were not able to find a construction of random graphs with an involution in the random-graph literature.

1.1. **Roadmap.** The paper is structured as follows: In Section 2 we provide preliminaries on supersingular elliptic curves and orientations. We also fix notation, and we recall results from the literature that will be used later on. In Section 3 we give results on the location of $\mathbb{F}_p$-vertices in oriented supersingular isogeny graphs. Section 4 gives the proofs of Theorem 4.1 and Corollary 4.2. We then give explicit examples of these results in Section 5. We address the expected number of cycles along the spine in Section 6. Finally, we give partial results in the case of even length cycles in Section 7.

1.2. **Acknowledgments.** The author would like to thank Joseph Macula, James Rickards, and Katherine E. Stange for helpful conversations, and Katherine E. Stange for helpful comments on an earlier draft of this paper.

2. Preliminaries

Throughout, we will use $\mathcal{O}_D$ for the imaginary quadratic order of discriminant D, and simply $\mathcal{O}$ when the discriminant is not relevant or is clear from context. We will use $cl(\mathcal{O})$ for the ideal class group of an order $\mathcal{O}$, and $h(\mathcal{O})$ for the class number of $\mathcal{O}$. The Hilbert class polynomial of an order $\mathcal{O}$ will be denoted by

$\mathcal{H}_{\mathcal{O}}(x)$. It is well known that $\mathcal{H}_{\mathcal{O}}(x) \in \mathbb{Z}[x]$, and so for any prime p we can consider the reduction modulo p. We denote this reduction by $\widetilde{\mathcal{H}_{\mathcal{O}}}(x)$ when there is no risk of confusion regarding the prime of reduction.

2.1. Background on Supersingular Elliptic Curves.
In this section, we present some general background material on elliptic curves. Our primary reference on elliptic curves is [17].

An *isogeny* $\phi : E_1 \to E_2$, between two elliptic curves E_1, E_2, is a rational map taking 0_{E_1} to 0_{E_2}. The *degree* of ϕ is the degree of the corresponding extension of function fields $[K(E_1) : \phi^*(K(E_2))]$. If the degree of ϕ is ℓ then we call ϕ an *ℓ-isogeny.*

An elliptic curve defined over $\overline{\mathbb{F}_p}$ is said to be *supersingular* if its endomorphism ring is non-commutative. By [17, p. III.9.4], this implies that $\mathrm{End}(E) := \{$isogenies $E \to E$ defined over $\overline{\mathbb{F}_p}\}$ is a maximal order in the unique (up to isomorphism) quaternion algebra over $\mathbb{Q}$ ramified at only p and ∞. We denote this quaternion algebra by $B_{p,\infty}$.

We are primarily interested in counting cycles in the ℓ-isogeny graph, so we record here the definition of an *isogeny cycle* from [2]. When we use the word "cycle" in reference to $\mathcal{G}_\ell$ we will always mean an isogeny cycle.

Definition 2.1. An *isogeny cycle* is a closed walk, forgetting basepoint, in $\mathcal{G}_\ell$ containing no backtracking (no consecutive edges compose to multiplication-by-ℓ) which is not a power of another closed walk (i.e. not equal to another closed walk repeated more than once).

Remark 2.2. Note that in Definition 2.1, we consider the two cycles obtained from a sequence $\{j_0, j_1, \ldots, j_{r-1}\}$ of j-invariants traversed in opposite directions as different cycles. We are therefore counting *directed* cycles, which agrees with what was done in previous literature [2].

We will also use a refinement of supersingular elliptic curves, known as *oriented supersingular curves*. For additional background on oriented supersingular curves and the oriented isogeny graph, see [2].

Let K be an imaginary quadratic field, $\mathcal{O}$ an order of K, and E be a supersingular elliptic curve. Recall the following definitions from [2]:

Definition 2.3. A *K-orientation* of E is an embedding $\iota : K \to \mathrm{End}(E) \otimes \mathbb{Q}$.

Definition 2.4. A *K-oriented elliptic curve* is a pair (E, ι), where E is an elliptic curve and ι is a K-orientation of E.

Definition 2.5. A K-orientation $\iota : K \to \mathrm{End}(E)$ is an *$\mathcal{O}$-orientation* if $\iota(\mathcal{O}) \subset \mathrm{End}(E)$. We say that an $\mathcal{O}$-orientation is *$\mathcal{O}$-primitive* if $\iota(\mathcal{O}) = \mathrm{End}(E) \cap \iota(K)$.

Definition 2.6. Let $\mathcal{O}$ be an imaginary quadratic order. Then $\mathcal{O}$ is *ℓ-fundamental* if ℓ does not divide the conductor of $\mathcal{O}$.

Given an isogeny $\phi : E_1 \to E_2$, we define the K-orientation induced on E_2 from a K-orientation ι on E_1 as follows:

$$(\phi_* \iota)(\alpha) := \frac{1}{[\deg \phi]} \phi \circ \iota(\alpha) \circ \hat{\phi}.$$

A *K-oriented isogeny* is an isogeny $\phi : (E_1, \iota_1) \to (E_2, \iota_2)$ such that $\phi_* \iota_1 = \iota_2$. Two K-oriented elliptic curves are *K-isomorphic* if there exists an isomorphism $\eta : E_1 \to E_2$ such that $\eta_* \iota_1 = \iota_2$.

We can now introduce the oriented isogeny graph for a fixed prime p:

Definition 2.7. We denote the *K-oriented supersingular ℓ-isogeny graph* by $\mathcal{G}_{K,\ell}$. This is the graph whose vertices are K-isomorphism classes of K-oriented supersingular elliptic curves over $\overline{\mathbb{F}_p}$, and whose edges are K-oriented ℓ-isogenies. We further denote by $\mathcal{G}_{\mathcal{O},\ell}$ the subgraph of $\mathcal{G}_{K,\ell}$ induced by restricting vertices to the primitively $\mathcal{O}$-oriented supersingular curves.

In Arpin, Chen, Lauter, Scheidler, Stange, and Tran [2], the authors describe the structure of the oriented isogeny graph, as well as how cycles in $\mathcal{G}_\ell$ are obtained from cycles in $\mathcal{G}_{K,\ell}$ by forgetting orientations. In particular, we have the following results:

Proposition 2.8 ([2], Proposition 2.16). *A connected component of $\mathcal{G}_{K,\ell}$, when identifying ℓ-isogenies with their duals, has at most one cycle, passing through the the vertices that are primitively $\mathcal{O}$-oriented for some ℓ-fundamental order $\mathcal{O}$.*

Theorem 2.9 ([2], Theorem 3.2). *Let $r > 2$. There is a bijection between cycles of length r in $\mathcal{G}_\ell$ and directed rims of size r in $\coprod_K \mathcal{G}_{K,\ell}$, identified up to conjugation of the orientation. We use $\coprod_K \mathcal{G}_{K,\ell}$ to denote the disjoint union of the K-oriented isogeny graphs, where K ranges over all imaginary quadratic fields.*

We also recall a tool used in proving the theorems cited above: the class group action on oriented curves. To define the action, we begin with the following definition from [2]:

Definition 2.10. Let (E, ι) be a primitively $\mathcal{O}$-oriented supersingular elliptic curve. Let $\mathfrak{a}$ be an integral ideal of $\mathcal{O}$ coprime to p. Define the intersection:

$$E[\iota(\mathfrak{a})] := \bigcap_{\alpha \in \mathfrak{a}} \ker((\iota(\alpha)).$$

This group defines an isogeny $\phi_{\mathfrak{a}}^{(E,\iota)} : E \to E/E[\iota(\mathfrak{a})]$. The action of $\mathfrak{a}$ on (E, ι) is defined as $\mathfrak{a} * (E, \iota) := (\phi_{\mathfrak{a}}^{(E,\iota)}(E), (\phi_{\mathfrak{a}}^{(E,\iota)})_* \iota)$.

We also define an action of the two-element group $\{1, \pi_p\}$ generated by the Frobenius automorphism π_p of $\mathbb{F}_{p^2}$ by

$$\pi_p * (E, \iota) := (E^{(p)}, \iota^{(p)}), \ \pi_p * \varphi = \varphi^{(p)}$$

where $\iota^{(p)} := (\pi_p)_* (\iota)$.

We can now give the primary result concerning the class group action on oriented curves:

Proposition 2.11 ([2], Proposition 2.26). *The actions of Definition 2.10 and Frobenius commute and hence give an action of $cl(\mathcal{O}) \times \langle \pi_p \rangle$ on the primitively $\mathcal{O}$-oriented supersingular elliptic curves over $\overline{\mathbb{F}_p}$. This action is transitive and its point stabilizers are either all trivial or all $\langle \pi_p \rangle$.*

2.2. **Background on Quadratic Orders in $B_{p,\infty}$.** In this section, we recall several results from the literature about quadratic orders in the quaternion algebra $B_{p,\infty}$.

First, we have the following result of Kaneko, which says roughly that a maximal order in $B_{p,\infty}$ can only contain two quadratic discriminants D_1, D_2 if $D_1 D_2$ is sufficiently large:

Theorem 2.12 ([10], Theorem 2). *Let D_1 and D_2 be two imaginary quadratic discriminants, and p be a prime such that the reductions of elliptic curves with CM by D_1 and D_2 are supersingular. If $D_1 D_2 < 4p$, then $\widetilde{\mathcal{H}_{\mathcal{O}_{D_1}}}(x)$ and $\widetilde{\mathcal{H}_{\mathcal{O}_{D_2}}}(x)$ have no common roots in $\overline{\mathbb{F}_p}$.*

In another format this gives the following:

Theorem 2.13 ([10], Theorem 2'). *Suppose that two quadratic orders $\mathcal{O}_{D_1}$ and $\mathcal{O}_{D_2}$ are optimally embedded in a maximal order of $B_{p,\infty}$ with different images. Then the inequality $D_1 D_2 \geq 4p$ holds. If $\mathbb{Q}(\sqrt{D_1}) = \mathbb{Q}(\sqrt{D_2})$, this inequality can be replaced by $D_1 D_2 \geq p^2$.*

Chen and Xue note the following corollary, which will also be of use to us:

Corollary 2.14 ([4], Corollary 2.7). *Let $\mathcal{O}$ be an imaginary quadratic order, p be a prime that does not split in $\mathcal{O}$, and $\mathfrak{P}$ be a prime of the Hilbert class field of $\mathcal{O}$ lying over p. If $p > |\operatorname{disc}(\mathcal{O})|$, then the reduction map $r_{\mathfrak{P}}$ from isomorphism classes of elliptic curves over $\overline{\mathbb{Q}}$ with CM by $\mathcal{O}$ to the set of isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}_p}$ is injective.*

Finally, we will use the following result of Onuki, which determines when the reduction map from a CM elliptic curve E to a supersingular elliptic curve $\tilde{E}$ gives an optimal embedding of $\operatorname{End}(E)$ into $\operatorname{End}(\tilde{E})$:

Lemma 2.15 ([15], Lemma 3.1). *Let E be an elliptic curve over a number field L containing K with $\mathrm{End}(E) \cong \mathcal{O} \subset K$, and $\mathfrak{p}$ a prime ideal of L above p such that E has good reduction at $\mathfrak{p}$. Then the reduced curve $\tilde{E}$ modulo $\mathfrak{p}$ is supersingular if and only if p does not split in K. Furthermore, let c be the conductor of $\mathcal{O}$ and write $c = p^r c_0$, where $p \nmid c_0$. Then*

$$\mathrm{End}(\tilde{E}) \cap [K]_{\tilde{E}} = [\mathbb{Z} + c_0 \mathcal{O}_K]_{\tilde{E}},$$

where $[\cdot]_{\tilde{E}}$ reduction map between endomorphism algebras.

2.3. **Setup.** Throughout, we will use the following set of imaginary quadratic orders:

$$\mathcal{I}_{\ell,r} = \left\{ \text{imaginary quadratic orders } \mathcal{O} : \begin{array}{c} \mathcal{O} \text{ is an } \ell\text{-fundamental order,} \\ (\ell) = \bar{\mathfrak{l}}\mathfrak{l} \text{ splits in } \mathcal{O}, \\ \text{and } [\mathfrak{l}] \text{ has order } r \text{ in } cl(\mathcal{O}). \end{array} \right\}.$$

We note that $\mathcal{I}_{\ell,r}$ is a finite set, since the last two conditions require that ℓ^r is primitively represented by the norm form of $\mathcal{O}$. We are considering only orders with positive-definite norm forms, so there are only finitely many $\mathcal{O}$ where this condition holds.

We will also use the following related definitions:

$$\mathrm{SS}^p := \{\text{isomorphism classes of supersingular elliptic curves over } \overline{\mathbb{F}}_p\}$$
$$d(\mathcal{I}_{\ell,r}) := \{d : d \text{ is the discriminant of } \mathcal{O} \text{ for some } \mathcal{O} \in \mathcal{I}_{\ell,r}\},$$
$$\mathcal{E}\ell\ell_{\mathcal{I}_{\ell,r}} := \{\text{elliptic curves } E \text{ over } \mathbb{C} \text{ such that } \mathcal{O} \cong \mathrm{End}(E) \text{ for some } \mathcal{O} \in \mathcal{I}_{\ell,r}\},$$
$$\mathcal{E}\ell\ell^p_{\mathcal{I}_{\ell,r}} := \{E \in \mathrm{SS}^p \text{ such that } \exists \mathcal{O} \in \mathcal{I}_{\ell,r} \text{ embedding optimally in } \mathrm{End}(E)\},$$
$$M_{\ell,r} := \max\{4, \max\{d_1 d_2/4 : d_1, d_2 \in d(\mathcal{I}_{\ell,r})\}\}.$$

In the second set, we take curves up to isomorphism over $\mathbb{C}$, and in the third up to isomorphism over $\overline{\mathbb{F}}_p$.

It is well-known that the j-invariants of elliptic curves with CM by an imaginary quadratic order $\mathcal{O}$ are the roots of $\mathcal{H}_{\mathcal{O}}(x)$. The j-invariants of the supersingular elliptic curves E over $\overline{\mathbb{F}}_p$ with $\mathcal{O}$ optimally embedded in $\mathrm{End}(E)$ are the roots of the reduction of $\mathcal{H}_{\mathcal{O}}(x)$ modulo p. Since we are interested in curves that lie on the spine of $\mathcal{G}_\ell$, we will be interested in the $\mathbb{F}_p$-roots of $\widetilde{\mathcal{H}_{\mathcal{O}}}$. The following result, which is Theorem 1.1 in [4], will be helpful in describing these roots:

Theorem 2.16 ([4], Theorem 1.1). *Let K be an imaginary quadratic field and $\mathcal{O}$ be an order in K. Let p be a prime inert in K and strictly greater than $|\mathrm{disc}(\mathcal{O})|$, and H_p be the set of $\mathbb{F}_p$-roots of $\widetilde{\mathcal{H}_{\mathcal{O}}}(x)$. If H_p is nonempty, then it admits a regular action by the 2-torsion subgroup $cl(\mathcal{O})[2] \subset cl(\mathcal{O})$. In particular, the number of $\mathbb{F}_p$-roots of $\widetilde{\mathcal{H}_{\mathcal{O}}}(x)$ is either zero or $|cl(\mathcal{O})[2]|$.*
Moreover, $H_p \neq \emptyset$ if and only if for every prime factor q of $\mathrm{disc}(\mathcal{O})$, one of the two conditions below holds, depending on the parity of q:

(1) $q \neq 2$ and the Legendre symbol $\left(\frac{-p}{q}\right) = 1$;
(2) $q = 2$ and one of the following conditions holds:
    (a) $p \equiv 7 \pmod 8$;
    (b) $-p + \frac{\mathrm{disc}(\mathcal{O})}{4} \equiv 0, 1, \text{ or } 4 \pmod 8$;
    (c) $-p + \mathrm{disc}(\mathcal{O}) \equiv 1 \pmod 8$.

We note the following corollary, which has been noted elsewhere in the literature, for example in [8]:

Corollary 2.17. *Let $\mathcal{O}_D$ be the maximal order in an imaginary quadratic field K, and p be a prime that does not split in $\mathcal{O}_D$. Suppose that the class number of $\mathcal{O}_D$ is odd. Then $\mathcal{H}_{\mathcal{O}_D}(x)$ has exactly one root in $\mathbb{F}_p$.*

We will omit the proof of Corollary 2.17, which can be done via a case-by-case analysis from Theorem 2.16. Neither the proof nor the result will be needed in the rest of the paper. For future reference, however, we include Theorem 2.18 below. This theorem is the other key ingredient in the proof of Corollary 2.17.

Theorem 2.18 ([6], Proposition 3.11). *Let $D \equiv 0, 1 \pmod 4$ be negative, and let r be the number of odd primes dividing D. Define the number μ as follows: if $D \equiv 1 \pmod 4$, then $\mu = r$, and if $D \equiv 0 \pmod 4$ then $D = -4n$, where $n > 0$, and μ is determined by the following table:*

n	μ
$n \equiv 3 \pmod 4$	r
$n \equiv 1, 2 \pmod 4$	$r + 1$
$n \equiv 4 \pmod 8$	$r + 1$
$n \equiv 0 \pmod 8$	$r + 2$

Then the class group $C(D)$ has exactly $2^{\mu-1}$ elements of order ≤ 2.

Remark 2.19. Corollary 2.17 inspired us to investigate the proportion of cycles of length r in $\mathcal{G}_{p,\ell}$ that intersect the spine. To illustrate why, suppose that we have $\mathcal{O} \in \mathcal{I}_{\ell,r}$ of discriminant d, such that p does not split in $\mathcal{O}$, and p does not divide the conductor of $\mathcal{O}$. We have a class group action by $[\mathfrak{l}]$ on $\mathcal{E}ll_{\mathcal{O}} := \{\text{elliptic curves over } \mathbb{C} \text{ that have } \mathrm{End}(E) = \mathcal{O}\}$. This action partitions $\mathcal{E}ll_{\mathcal{O}}$ into $cl(\mathcal{O})/r$ orbits each of size r. Since p does not split in $\mathcal{O}$, each curve $E \in \mathcal{E}ll_{\mathcal{O}}$ reduces to a supersingular curve modulo p. If we further assume that $p > d$, then the reduction map from elliptic curves with CM by $\mathcal{O}$ to supersingular curves is injective by Corollary 2.14. The $cl(\mathcal{O})/r$ orbits therefore reduce to distinct r-cycles in $\mathcal{G}_\ell$. Thus, if ℓ generates $cl(\mathcal{O})$, and $\# \, cl(\mathcal{O})$ is odd, Corollary 2.17 shows us that the reduced curves form a cycle of odd length that is guaranteed to intersect the spine. This provides a way of constructing cycles along the spine.

Finally, in order to give precise counts of the number of cycles through the spine, we will need the following lemma:

Lemma 2.20. *Let $p > M_{\ell,r}$. Then for any prime $\mathfrak{p}$ and number field L such that all curves in $\mathcal{E}ll_{\mathcal{I}_{\ell,r}}$ are defined over L and have good reduction at $\mathfrak{p}$, the reduction map $\rho_{\mathfrak{p}} : \mathcal{E}ll_{\mathcal{I}_{\ell,r}} \to \mathcal{E}ll^p_{\mathcal{I}_{\ell,r}}$ is injective.*

Proof. Our assumption on the size of p is chosen to guarantee that for any $\tilde{E} \in \mathcal{E}ll^p_{\mathcal{I}_{\ell,r}}$, there is only one $\mathcal{O} \in \mathcal{I}_{\ell,r}$ that is optimally embedded in $\mathrm{End}(\tilde{E})$, and that there is only one such embedding of $\mathcal{O}$. The assumption will further guarantee that for any $E \in \mathcal{E}ll_{\mathcal{I}_{\ell,r}}$, $\rho_{\mathfrak{p}}(\mathrm{End}(E))$ is optimally embedded in $\mathrm{End}(\rho_{\mathfrak{p}}(E))$. Together, these will prove that $\rho_{\mathfrak{p}}$ is injective into $\mathcal{E}ll^p_{\mathcal{I}_{\ell,r}}$.

By Lemma 2.15, in order to show that $\rho_{\mathfrak{p}}$ optimally embeds endomorphism rings, it suffices to show that our assumption guarantees that $p > |d|$ for all $d \in d(\mathcal{I}_{\ell,r})$. This is elementary, since for $|d| > 4$, we have that $d^2/4 > |d|$. Thus $p > 4$ and $p > d_1 d_2/4$ for all $d_1, d_2 \in \mathcal{I}_{\ell,r}$ guarantee that $p > |d|$ for all $d \in d(\mathcal{I}_{\ell,r})$. These conditions hold by the assumption that $p > M_{\ell,r}$.

To show that there is only one $\mathcal{O} \in \mathcal{I}_{\ell,r}$ that optimally embeds in $\mathrm{End}(\tilde{E})$ for any $\tilde{E} \in \mathcal{E}ll^p_{\mathcal{I}_{\ell,r}}$, we use Theorem 2.13. This says that if there is a maximal order in $B_{p,\infty}$ containing optimally embedded copies of both $\mathcal{O}_{d_1}$ and $\mathcal{O}_{d_2}$, then $p < \frac{d_1 d_2}{4}$. Thus our assumption guarantees that $B_{p,\infty}$ contains no such order for $d_1, d_2 \in d(\mathcal{I}_{\ell,r})$. Since $\mathrm{End}(\tilde{E})$ is a maximal order in $B_{p,\infty}$, it follows that there is only one $\mathcal{O} \in \mathcal{I}_{\ell,r}$ that optimally embeds in $\mathrm{End}(\tilde{E})$.

We now show that the reduction map $\rho_{\mathfrak{p}}$ is injective. Let $E_1, E_2 \in \mathcal{E}ll_{\mathcal{I}_{\ell,r}}$ be elliptic curves with CM by $\mathcal{O}_{d_1}$, $\mathcal{O}_{d_2}$, respectively. First, consider the case that $d_1 = d_2$. In this case, both $j(E_1)$ and $j(E_2)$ satisfy $\mathcal{H}_{\mathcal{O}_{d_1}}$. We have shown that our assumption guarantees $p > |d_1|$, and by Corollary 2.14, this guarantees that $\mathcal{H}_{\mathcal{O}_{d_1}}$ has no repeated roots modulo p. Thus we see that E_1 and E_2 cannot reduce to supersingular curves with the same j-invariant, and so $\rho_{\mathfrak{p}}(E_1) \neq \rho_{\mathfrak{p}}(E_2)$.

For the second case, suppose that $d_1 \neq d_2$, and suppose $\rho_{\mathfrak{p}}(E_1) = \rho_{\mathfrak{p}}(E_2) = E$. Then since $\rho_{\mathfrak{p}}$ optimally embeds the endomorphism rings of E_1, E_2 into $\mathrm{End}(E)$, we have that $\mathrm{End}(E)$ is a maximal order of $B_{p,\infty}$ with optimally embedded copies of $\mathcal{O}_{d_1}$ and $\mathcal{O}_{d_2}$. This contradicts Theorem 2.13, and so the result is proven. $\square$

Remark 2.21. We remark that the results and proof of Lemma 2.20 continue to hold for a finite set $\{r_1, \ldots, r_n\}$ of r-values, provided that $M_{\ell,r}$ is replaced by the maximum of the M_{ℓ,r_i}. This will be used in Section 7 when considering the case of even cycles.

3. $\mathbb{F}_p$-VERTICES ON ORIENTED ISOGENY CYCLES AND THE EVEN CLASS NUMBER CASE

In this section we will count the number $\mathbb{F}_p$ vertices on oriented isogeny cycles. This will allow us to extend the ideas from Remark 2.19 to the case of even class number. Our strategy is to apply results of Chen and Xue [4] about the class group action on $\mathbb{F}_p$-roots of the Hilbert class polynomial to oriented supersingular curves. We will conclude that for $p > d$, the number of r-cycles obtained from primitive $\mathcal{O}$-orientations that intersect the spine is either 0 or 2^μ, where μ defined as in Theorem 2.18.

Our first theorem in this section describes the action of the class group on $\mathbb{F}_p$-vertices of oriented isogeny cycles:

Theorem 3.1. *Let $p > |\operatorname{disc}(\mathcal{O})|$. Then the restriction of the action of $cl(\mathcal{O}) \times \langle \pi_p \rangle$ to $cl(\mathcal{O})[2] \times \langle \pi_p \rangle$ acts transitively on the $\mathbb{F}_p$-vertices.*

Proof. By Proposition 2.11, the action of $cl(\mathcal{O}) \times \langle \pi_p \rangle$ is transitive on the vertices of $\mathcal{G}_{\mathcal{O},\ell}$, so we need only show that for $k \in \{1, 2\}$ and (E, ι) with $j(E) \in \mathbb{F}_p$, $(E^{(\mathfrak{a}, \pi_p^k)}, \iota^{(\mathfrak{a}, \pi_p^k)})$ has $j(E^{(\mathfrak{a}, \pi_p^k)}) \in \mathbb{F}_p$ if and only if $[\mathfrak{a}] \in cl(\mathcal{O})[2]$.

Suppose that $j(E) \in \mathbb{F}_p$. Then $j(E^{(p)}) = j(E)$. Since $E^{(\mathfrak{a}, \pi_p)} = (E^{(p)})^{\mathfrak{a}}$, we are reduced to showing that $j(E^{\mathfrak{a}}) \in \mathbb{F}_p$ if and only if $[\mathfrak{a}] \in cl(\mathcal{O})[2]$. This follows from Theorem 2.16 under the assumption that $p > |\operatorname{disc}(\mathcal{O})|$. $\qquad\square$

As a corollary, we see that any two cycles in $\mathcal{G}_{\mathcal{O},\ell}$ containing at least one $\mathbb{F}_p$-vertex must contain the same number of $\mathbb{F}_p$-vertices:

Corollary 3.2. *Let C_1, C_2 be cycles in $\mathcal{G}_{\mathcal{O},\ell}$ such that both contain an $\mathbb{F}_p$-vertex. If $p > |\operatorname{disc}(\mathcal{O})|$, then C_1 and C_2 have the same number of $\mathbb{F}_p$-vertices.*

Proof. By Proposition 2.8, we know that each connected component of $\mathcal{G}_{K,\ell}$ has at most one cycle. By definition 2.7, $\mathcal{G}_{\mathcal{O},\ell}$ is the subgraph of $\mathcal{O}$-rims, so we see that $\mathcal{G}_{\mathcal{O},\ell}$ is a collection of disjoint cycles, possibly containing isolated vertices. Since the action of $cl(\mathcal{O}) \times \langle \pi_p \rangle$ preserves adjacency, we get that $cl(\mathcal{O}) \times \langle \pi_p \rangle$ takes cycles of $\mathcal{G}_{\mathcal{O},\ell}$ to cycles.

Let C_1, C_2 be cycles in $\mathcal{G}_{\mathcal{O},\ell}$, and let $C_i^p = \{$vertices $(E, \iota) \in C_i$ such that $j(E) \in \mathbb{F}_p\}$. Let v_1, v_2 be elements of C_1^p, C_2^p, respectively. We will show that $\#C_1^p = \#C_2^p$. By Theorem 3.1, there exists an element $g \in cl(\mathcal{O})[2] \times \langle \pi_p \rangle$ taking v_1 to v_2, and therefore necessarily taking C_1 to C_2. Further, g acts injectively, and takes C_1^p to C_2^p. We see therefore that $\#C_2^p \geq \#C_1^p$. Replacing g by g^{-1} gives the opposite inequality, which proves that $\#C_1^p = \#C_2^p$. $\qquad\square$

Finally, we will show that for sufficiently large p and odd r, the number of $\mathbb{F}_p$-vertices on a cycle in $\mathcal{G}_{\mathcal{O},\ell}$ is either 0 or 1, for any $\mathcal{O} \in \mathcal{I}_{\ell,r}$.

We begin by making explicit a result from Arpin, Chen, Lauter, Scheidler, Stange, and Tran [2]:

Lemma 3.3. *Let r be odd, and $\mathcal{O} \in \mathcal{I}_{\ell,r}$. Then every cycle in $\mathcal{G}_{\mathcal{O},\ell}$ has length r.*

Proof. We will show that every edge in $\mathcal{G}_{\mathcal{O},\ell}$ comes from the action of $[\mathfrak{l}]$ or $[\bar{\mathfrak{l}}]$ via a counting argument.

Since ℓ splits in $\mathcal{O}$ and does not divide the conductor of $\mathcal{O}$, we have by [2, Proposition 2.15] that there are 2 horizontal ℓ-isogenies out of each $(E, \iota) \in \mathcal{G}_{\mathcal{O},\ell}$. We now consider the isogeny $\phi_{\mathfrak{l}} : (E, \iota) \to [\mathfrak{l}] \star (E, \iota)$ whose kernel is $E[\iota(\mathfrak{l})]$. Since $N(\mathfrak{l}) = \ell$, $\phi_{\mathfrak{l}}$ is an ℓ-isogeny, and by definition of the orientation on $[\ell] \star (E, \iota)$, $\phi_{\mathfrak{l}}$ is a K-oriented ℓ-isogeny. Thus $\phi_{\mathfrak{l}}$ is one of the horizontal edges out of (E, ι), and by the same argument we get an isogeny $\phi_{\bar{\mathfrak{l}}}$ that gives the other horizontal edge.

The previous paragraph allows us to explicitly describe the action of $[\mathfrak{l}]$ on $\mathcal{G}_{\mathcal{O},\ell}$. Since each vertex in $\mathcal{G}_{\mathcal{O},\ell}$ has two horizontal ℓ-isogenies out of it, we see that there are no isolated vertices in $\mathcal{G}_{\mathcal{O},\ell}$, and so $\mathcal{G}_{\mathcal{O},\ell}$ is a disjoint union of cyclic subgraphs. Further, $[\mathfrak{l}]$ acts on $\mathcal{G}_{\mathcal{O},\ell}$ by cyclicly permuting the vertices in each cycle. The length of each cycle is therefore the minimum s such that $[\mathfrak{l}^s]$ acts as the identity on each vertex. By

Proposition 2.11, the point stabilizers of the vertices in $\mathcal{G}_{\mathcal{O},\ell}$ are all either trivial or $\langle \pi_p \rangle$, so we see that we must have $[\mathfrak{l}^s]$ is the identity in $c\ell(\mathcal{O})$. Thus the length of each cycle is equal to the order of $[\mathfrak{l}]$ in the class group, namely r.

$\square$

We aim to prove that for sufficiently large primes p, every odd cycle intersecting the spine contains at most one $\mathbb{F}_p$-vertex. Our first step is to prove Lemma 3.6 below, which says that for large enough p, a cycle C of length r through the spine is either fixed by action of Frobenius, or its orientation is reversed. To make this precise, we recall the following definition from [2]:

Definition 3.4. Given a cycle $C := \phi_1, \phi_2, \ldots, \phi_n$ in $\mathcal{G}_\ell$, we define the *opposite cycle* to be the cycle $\hat{C}$ given by the dual isogenies in the reverse order. Graph theoretically, the opposite cycle is a cycle that traverses the same vertices in the opposite order.

Remark 3.5. We remark that Definition 3.4 requires special care at the vertices $j = 0$ and $j = 1728$. The extra automorphisms at these vertices make it possible for more than one outgoing edge to correspond to the same incoming edge when taking the dual. This subtlety is handled in [2] by defining a *safe arbitrary assignment* (see Definition 3.13 in [2]). For our purposes, it is sufficient to know that we can make suitable choices so that every cycle has a unique corresponding opposite cycle. Further, if θ is the endomorphism corresponding to the composition of the isogenies in C, then $\pm\hat{\theta}$ is the endomorphism corresponding to the composition of the isogenies in $\hat{C}$. The interested reader can consult section 3 of [2] for details.

Lemma 3.6. *Let $p > M_{\ell,r}$, π_p be Frobenius, and C be a cycle of length r in $\mathcal{G}_\ell$. Suppose that C contains an $\mathbb{F}_p$-vertex v. Then we have that $\pi_p(C) \in \{C, \hat{C}\}$.*

Proof. Since v is defined over $\mathbb{F}_p$, we have that $\pi_p(v) = v$. Further, we know that π_p is a graph isomorphism, and so π_p takes C to a cycle of length r through v. By Theorem 2.9, every such cycle corresponds to an optimal embedding of some $\mathcal{O} \in \mathcal{I}_{\ell,r}$ into $\text{End}(v)$. Lemma 2.20 tells us that, up to conjugation, there is only one such optimal embedding. Thus there are only two cycles of length r through C, and they correspond to dual endomorphisms. The two cycles must therefore be opposite, which proves the $\pi_p(C) \in \{C, \hat{C}\}$. $\square$

We can now prove that each r-cycle has at most one $\mathbb{F}_p$-vertex.

Proposition 3.7. *Let r be odd, and $p > M_{\ell,r}$. Then the number of $\mathbb{F}_p$-vertices on each r-cycle in $\mathcal{G}_{\mathcal{O},\ell}$ is either 0 or 1. The same result also holds for r-cycles in $\mathcal{G}_\ell$.*

Proof. Let C be a cycle containing at least one $\mathbb{F}_p$-vertex in $\mathcal{G}_{\mathcal{O},\ell}$, $\tilde{C}$ be the cycle in $\mathcal{G}_\ell$ obtained by forgetting orientations, and $\tilde{C}^p$ be the set of $\mathbb{F}_p$-j-invariants appearing as vertices in $\tilde{C}$. We define C^p similarly. By Lemma 3.3 we know that the length of C is r. We will show that $\#C^p$ is odd.

By Lemma 3.6, we have that Frobenius fixes the vertex set of $\tilde{C}$, and therefore also fixes the set of j-invariants that appear in vertices of C. There is therefore an even number of $\mathbb{F}_{p^2}$-vertices in C and in $\tilde{C}$. Since there is an odd number of total vertices in C, we see that there is an odd number of $\mathbb{F}_p$-vertices in C.

We now show that our assumption on p guarantees there are a 2-power number of $\mathbb{F}_p$-vertices in $\mathcal{G}_{\mathcal{O},\ell}$. By Theorem 2.16, the number of $\mathbb{F}_p$-j-invariants obtained by forgetting orientations from $\mathcal{G}_{\mathcal{O},\ell}$ is $2^{\mu-1}$. We can therefore count $\mathbb{F}_p$-vertices in $\mathcal{G}_{\mathcal{O},\ell}$ by counting how many distinct orientations we obtain on each j-invariant. By the argument in Lemma 2.20, our assumption that $p > M_{\ell,r}$ implies that $p > |d|$. Thus p cannot ramify in $\mathcal{O}$, and so we must have that p is inert in $\mathcal{O}$. By [2, Proposition 4.2], this implies that for any orientation ι of E, (E, ι) and $(E, \bar{\iota})$ are non-isomorphic as oriented supersingular curves. As argued in Lemma 2.20, the assumption that $p > M_{\ell,r}$ also guarantees that there is only one embedding of $\mathcal{O}$ into $\text{End}(E)$, so we see that $j(E)$ appears exactly twice in $\mathcal{G}_{\mathcal{O},\ell}$. Thus the number of $\mathbb{F}_p$-vertices in $\mathcal{G}_{\mathcal{O},\ell}$ is $2(2^{\mu-1}) = 2^\mu$.

By Corollary 3.2, each cycle with at least one $\mathbb{F}_p$-vertex in $\mathcal{G}_{\mathcal{O},\ell}$ has the same number of $\mathbb{F}_p$-vertices. This number is odd by the argument in the second paragraph. The total number of $\mathbb{F}_p$-vertices in $\mathcal{G}_{\mathcal{O},\ell}$ is 2^μ by the arguments above. Letting $2k + 1$ be the number $\mathbb{F}_p$-vertices on any cycle in $\mathcal{G}_{\mathcal{O},\ell}$ with at least one such vertex, we see that $\#\{$cycles in $\mathcal{G}_{\mathcal{O},\ell}$ with an $\mathbb{F}_p$-vertex$\}(2k + 1) = 2^\mu$. It follows that $k = 0$, and so there is

either 0 or 1 such vertices on each cycle. Thus $\#C^p \in \{0, 1\}$.

Finally, we note that this implies $\#\tilde{C} \in \{0, 1\}$ as well, since the sets of j-invariants appearing as vertices in C and $\tilde{C}$ are the same. □

4. LIMITING DISTRIBUTION OF CYCLES ON AND OFF THE SPINE

By the results of the previous sections, we know that for sufficiently large primes p, all of the following hold:
  (1) $\mathcal{I}_{\ell,r}$ is a finite list of imaginary quadratic orders $\mathcal{O}$ such that every cycle of length r in $\mathcal{G}_\ell$ consists of vertices whose j-invariants satisfy the reduction modulo p of the Hilbert class polynomial for some $\mathcal{O} \in \mathcal{I}_{\ell,r}$.
  (2) For each order $\mathcal{O} \in \mathcal{I}_{\ell,r}$, the number of cycles obtained from the reductions of curves with CM by $\mathcal{O}$ is either 0 if p splits in $\mathcal{O}$, or $2h(\mathcal{O})/r$ otherwise.
  (3) The number of cycles obtained from the reduction of curves with CM by $\mathcal{O}$ that lie along the spine is either 0, or 2^μ. By Theorem 2.16, whether there are 0 or 2^μ cycles along the spine depends only on the discriminant, and the value of p modulo 8.

Together, these allow us to prove the first Theorem of the introduction:

Theorem 4.1. *Let ℓ and r be fixed, with r odd. Then there exists a modulus M depending on ℓ and r such that for $p \gg 0$, n_t and n_s depend only on p modulo M.*

Proof. We will see that for sufficiently large p, the number of r-cycles contributed by each order $\mathcal{O} \in \mathcal{I}_{\ell,r}$, both in total, and along the spine, depends only on congruence conditions on p.

Specifically, $\mathcal{O}$ contributes no r-cycles if p splits in $\mathcal{O}$, which is equivalent to d being a quadratic residue modulo p. By quadratic reciprocity this is equivalent to certain congruence conditions on p modulo d or $4d$. On the other hand, if p does not split in $\mathcal{O}$, then $\mathcal{O}$ gives 2^μ or 0 cycles along the spine according to p modulo 8 and congruence conditions on p modulo q for $q \mid d$, as in Theorem 2.16, and gives $2h(\mathcal{O})/r$ cycles in total.

For each discriminant $d \in d(\mathcal{I}_{\ell,r})$, we therefore have three sets of congruences $S_{d,1}, S_{d,2}, S_{d,3} \subseteq \mathbb{Z}/8d\mathbb{Z}$ with the following properties: if $[p] \in S_{d,1}$ then there are no cycles in $\mathcal{G}_\ell$ obtained from reduction of $\mathcal{O}$; if $[p] \in S_{d,2}$ then there are $2h(\mathcal{O})/r$ cycles in $\mathcal{G}_\ell$ obtained from reduction of $\mathcal{O}$, none of which lie along the spine; and if $[p] \in S_{d,3}$, then there are $2h(\mathcal{O})/r$ cycles in $\mathcal{G}_\ell$ obtained from reduction of $\mathcal{O}$, with 2^μ of them lying along the spine. For $p > M_{\ell,r}$, we have that the cycles obtained by $\mathcal{O}_1$ and $\mathcal{O}_2 \neq \mathcal{O}_1$ are distinct by Lemma 2.20, so we can obtain the exact count of cycles both in total, and along the spine from the value of p modulo $\mathrm{lcm}(8, d_1, \ldots, d_k)$, where the $\{d_1, \ldots, d_k\} = d(\mathcal{I}_{\ell,r})$. □

We are now in a position to prove the following Corollary as well:

Corollary 4.2. *Let ℓ and r be fixed, with r odd, and M be the modulus obtained in the previous Theorem. Then for any $[m] \in \mathbb{Z}/M\mathbb{Z}$, one of the following holds for all sufficiently large $p \in [m]$:*
  (1) $n_t/\#V(\mathcal{G}_{p,\ell}) < n_s/\#V(\mathcal{S}_{p,\ell})$;
  (2) $n_s = 0$.

Proof. In [1], the authors give the number of spine vertices as a constant multiple of either $h(\mathcal{O}_{-4p})$ or $h(\mathcal{O}_{-p})$, depending on p modulo 8. It is a standard bound in analytic number theory that $h(\mathcal{O}_d) \leq C\sqrt{|d|}\log(|d|)$ for imaginary quadratic discriminants d, and a constant C [9, Equation 8.11]. Letting s be the number of spine vertices we therefore have that $s = O(\sqrt{p}\log p)$. On the other hand, the number of vertices in $\mathcal{G}_{p,\ell}$ is $O(p)$.

Let n_t and n_s be as in the Corollary statement. Using the notation from the proof of Theorem 4.1, we see that if $[m] \in S_{d,1}$ or $[m] \in S_{d,2}$ for all $d \in d(\mathcal{I}_{\ell,r})$, then $n_s = 0$ for all sufficiently large $p \in [m]$. Otherwise, we have that $n_s, n_t > 0$.

Proposition 3.7 says that each cycle along the spine contains 1 spine vertex. Further, for $p > M_{\ell,r}$, all of the r-cycles in $\mathcal{G}_{p,\ell}$ are disjoint, unless the two cycles are the same up to direction of traversal. We therefore see that, for p sufficiently large, each spine vertex contained in an r-cycle is contained in exactly two r-cycles. Thus there are $n_s/2$ spine vertices that are part of an r-cycle. Each r-cycle contains r-total vertices, and as

discriminant	class number	$\left(\frac{d}{4643}\right)$	$\mathbb{F}_{4643^2}$ j-invariants
-23	3	-1	$173, 1283z_2 + 3319, 3360z_2 + 937$
-44	3	1	
-59	3	1	$1896, 1161, 851$
-83	3	1	$3690, 2630, 1486$
-92	3	-1	$4537, 732z_2 + 4024, 3911z_2 + 1326$
-104	6	-1	$2549z_2 + 3241, 3268z_2 + 3162, 3037z_2 + 3085, 2094z_2 + 2967, 1606z_2 + 2560, 1375z_2 + 73$
-107	3	1	$3870, 1520, 637$

TABLE 1. Discriminants in $\mathcal{I}_{3,3}$, and corresponding data for the prime $p = 4643$. The variable z_2 is a root of the polynomial $x^2 - 9x - 4638 \in \mathbb{F}_{4643}[x]$.

argued above, for sufficiently large p, the r-cycles are all disjoint, except for a cycle and its opposite. Thus there are $rn_t/2$ vertices contained in r-cycles. We therefore have that for $p \equiv m \pmod{M}$, the proportion of spine vertices contained in an r-cycle is $n_s/O(\sqrt{p}\log(p))$, while the proportion of all vertices contained in an r-cycles is $n_t/O(p)$. Since $O(p)$ is asymptotically greater than $O(\sqrt{p}\log(p))$, we see that the proportion of spine vertices with an r-cycle is eventually greater than the proportion of all vertices. $\square$

5. EXPLICIT EXAMPLES

In this section, we present explicit examples illustrating the key ideas in Theorem 4.1 and Corollary 4.2. We consider the distribution of 3 cycles in the 3-isogeny graph.

Referring to Table 1, we see that $\mathcal{I}_{3,3} = \{-23, -44, -59, -83, -92, -104, -107\}$. For $p > \frac{(-104)(-107)}{4}$, we have that the reductions of the curves with CM by these orders are all distinct. In these cases we can count the number of cycles in $\mathcal{G}_\ell$ that intersect $\mathcal{S}_\ell$ by counting the number resulting from each order separately. We will assume that p is sufficiently large for the rest of this example.

Consider the order $\mathcal{O}$ of discriminant -23. Reductions of curves with CM by $\mathcal{O}$ are supersingular if and only if $\left(\frac{-23}{p}\right) = -1$. By quadratic reciprocity, this occurs if and only if

$$p \equiv 3, 5, 17, 21, 23, 27, 31, 33, 35, 37, 39, 45, 47, 53, 55, 57, 59, 61, 65, 71, 75, 87, 89 \pmod{92}.$$

If p is in one of these residue classes, then the reductions of the curves with CM by $\mathcal{O}$ form two directed 3-cycles in the 3-isogeny graph. Further, $\left(\frac{-p}{23}\right) = 1$ in each of these cases, so Theorem 2.16 tells us that these 3-cycles intersects the spine.

Next, we analyze the case of $d = -104$, where more complicated scenarios can occur. We find again by quadratic reciprocity, that the curves with CM by $\mathcal{O}_{-104}$ reduce to supersingular curves if and only if

(1) $\qquad p \equiv 11, 19, 23, 29, 33, 41, 53, 55, 57, 59, 61, 67, 69, 73, 77, 79, 83, 87, 89, 95, 97, 99, 101, 103 \pmod{104}.$

The class group of $\mathcal{O}_{-104}$ is isomorphic to $\mathbb{Z}/6\mathbb{Z}$, so that for $p > 104$, there are either 0 or 2 $\mathbb{F}_p$-roots of the Hilbert Class Polynomial. By Theorem 2.16, there are 2 $\mathbb{F}_p$-roots as long as

(1) $\left(\frac{-p}{13}\right) = 1$, and
(2) at least one of the following holds:
    (a) $p \equiv 7 \pmod 8$,
    (b) $-p - 26 \equiv 0, 1,$ or $4 \pmod 8$, or,
    (c) $-p - 104 \equiv 1 \pmod 8$.

Simplifying these conditions shows that p must be in the following residue classes:

(2) $\qquad\qquad p \equiv 23, 29, 53, 55, 61, 69, 77, 79, 87, 95, 101, 103 \pmod{104}.$

Thus the discriminant $\mathcal{O}_{-104}$ produces 4 directed 3-cycles in $\mathcal{G}_{p,3}$ if and only if p is in one of the residues listed in (1), and these four 3-cycles lie along the spine if and only if p is in one of the residues listed in (2).

The analyses of the remaining discriminants are similar. For our purposes, it suffices to note that in each case, we can give an explicit list of residues modulo some m_i where the order produces supersingular curves, and further, when the class number is even we can give an explicit subset of these residues where there are 2^μ reduced curves along the spine. Considering each residue class in $(\mathbb{Z}/\operatorname{lcm}(m_i)\mathbb{Z})^\times$, we can then count the number of 3-cycles in the graph $\mathcal{G}_{p,3}$, as well as the number of 3-cycles along the spine. By explicit computation, we see that in this case, $\operatorname{lcm}(m_i) = 13,786,935,448$, so that for sufficiently large primes p, the number of 3-cycles in total and along the spine in the 3-isogeny graph depends only on p modulo $13,786,935,448$.

For example, consider $p = 4643$. Table 1 shows that in this case only the orders $\mathcal{O}_{-23}$, $\mathcal{O}_{-92}$, and $\mathcal{O}_{-104}$ produce supersingular j-invariants, and further we have that none of the 3-cycles coming from $\mathcal{O}_{-104}$ lie along the spine. We therefore have that $1/2$ of the 3-cycles lie along the spine and $1/2$ lie off of the spine. Since this ratio depends only on p modulo $13,786,935,448$, we see that for large enough p equivalent to 4643 modulo $13,786,935,448$, $1/2$ of the three cycles in $\mathcal{G}_{p,3}$ lie along spine, while the proportion of vertices that are on the spine approaches 0.

6. EXPECTED VALUES FOR n_s

In this section, we give an explicit formula for n_s, as well as for the expected value of n_s as $p \to \infty$. These formulae are given in terms of imaginary quadratic class numbers and discriminants, but without conditions on the order or splitting behavior of ℓ in the class group.

We first recall a convenient description for the set $\cup_{n|r} d(\mathcal{I}_{\ell,n})$ given in the proof of Theorem 7.4 in [2]:

Proposition 6.1. *The set of imaginary quadratic discriminants Δ where $\ell\mathcal{O}_\Delta$ splits, the primes above ℓ have order dividing r, and the conductor is not divisible by ℓ, is given by*

$$\left\{ \frac{x^2 - 4\ell^r}{f^2} : 0 < x < 2\ell^{r/2},\ x \not\equiv 0 \pmod{\ell},\ f^2 \mid x^2 - 4\ell^r,\ and\ \frac{x^2 - 4\ell^r}{f^2} \equiv 0,1 \pmod 4 \right\}.$$

We will denote this by $d(\mathcal{I}_{\ell,n|r})$.

Proof. Let p, ℓ, and r be fixed. Theorem 7.4 of [2] shows that the set of discriminants corresponding to cycles whose length divides r in $\mathcal{G}_{p,\ell}$ is given by the set of $\frac{x^2-4\ell^r}{f^2}$ such that all of the conditions above hold, but also $x^2 - 4\ell^r$ is not a quadratic residue modulo p and has valuation at most 1 at p. The set above simply removes the conditions on p. □

We now aim to compute the average number of spine cycles for large p. We first use Möbius inversion to find a formula for this count for a specific p. Let $n_{s,p}(r)$ be the number of spine cycles of length r in $\mathcal{G}_\ell$.

Theorem 6.2. *Let p, ℓ, and r be fixed, with $p > M_{\ell,r}$. Then*

$$n_{s,p}(r) = 2 \sum_{d|r} \mu(d) \sum_{\Delta \in d\left(\mathcal{I}_{\ell,n|\frac{r}{d}}\right)} \delta_p(\Delta) h_2(\Delta),$$

where $h_2(\Delta) = |\,cl(\mathcal{O}_\Delta)[2]|$, and $\delta_p(\Delta) = \begin{cases} 1 & \begin{array}{l} p \text{ is inert in } \mathcal{O} \text{ and} \\ H_\mathcal{O}(x) \text{ has a solution in } \mathbb{F}_p, \end{array} \\ 0 & \text{otherwise.} \end{cases}$

Remark 6.3. Note that using Theorem 2.16 and Theorem 2.18, $\delta_p(\Delta)$ and $h_2(\Delta)$ can both be calculated using only the factorization of Δ, legendre symbol computations, and modular arithmetic. Thus the formula in Theorem 6.2 depends entirely on "elementary" techniques, and does not require knowledge of the relevant class groups.

Proof. By Theorem 2.9, we have a map from isogeny cycles of length r in $\mathcal{G}_\ell$ to orders in $\mathcal{I}_{\ell,r}$, given by finding the unique order $\mathcal{O}$ such that the cycle appears as a rim in $\mathcal{G}_{\mathcal{O},\ell}$. Restricting to cycles along the spine, Corollary 3.2 shows that if $\mathcal{O}$ produces spine cycles, then it produces $2h_2(\Delta)$ of them, with the factor of 2 coming from considering directions of traversal. We therefore have that $\sum_{d|r} n_{s,p}(d) = 2\sum_{\Delta \in d(\mathcal{I}_{\ell,n|d})} \delta_p(\Delta)h_2(\Delta)$, and Möbius inversion finishes the proof. □

Turning to the average number of spine cycles as p varies, we have the following corollary:

Corollary 6.4. *Let $\{p_1, \ldots, p_n\}$ be a set of primes, all of which are greater than or equal to $M_{\ell,r}$. Then we have that*

$$(3) \qquad \frac{1}{n} \sum_{i=1}^{n} n_{s,p_i}(r) = 2 \sum_{d|r} \mu(d) \sum_{\Delta \in d(\mathcal{I}_{\ell,n|\frac{r}{d}})} \left(\frac{1}{n} \sum_{i=1}^{n} \delta_{p_i}(\Delta) \right) h_2(\Delta).$$

Proof. This follows from Theorem 4.1 by collecting all terms with the same d, Δ. $\qquad\square$

In order to compute the product on the right hand side of (3), we turn our attention to computing the average of the $\delta_{p_i}(\Delta)$.

Computing this average from Theorem 2.16 is possible via a case-by-case analysis, but we will give a more conceptual proof based on the work of Li, Li, and Ouyang. We begin with the following theorem:

Theorem 6.5 ([12], Theorem 4.1). *Let $\mathcal{O}$ be an order in an imaginary quadratic field K, and $\mathcal{H}_{\mathcal{O}}(x)$ be its Hilbert class polynomial. Let F be the genus field of $\mathcal{O}$, $F^+ = F \cap \mathbb{R}$, and p be a prime that does not split in K. Further, assume that $p \nmid \operatorname{disc} \mathcal{H}_{\mathcal{O}}(x)$ and $p \nmid \operatorname{disc}(\mathcal{O})$. Then $\mathcal{H}_{\mathcal{O}}(x)$ has a root in $\mathbb{F}_p$ if and only if p splits completely in F^+,*

In the cases of interest to us, the requirements that $p \nmid \operatorname{disc} \mathcal{H}_{\mathcal{O}}(x)$ and $p \nmid \operatorname{disc}(\mathcal{O})$ will always be satisfied, as the following lemma shows:

Lemma 6.6. *If $p > M_{\ell,r}$, then $p \nmid \operatorname{disc} \mathcal{H}_{\mathcal{O}}(x)$ and $p \nmid \operatorname{disc}(\mathcal{O})$ for all $\mathcal{O} \in \mathcal{I}_{\ell,r}$.*

Proof. By definition of $M_{\ell,r}$, we have that $p > M_{\ell,r}$ implies that $p > \operatorname{disc}(\mathcal{O})$ for all $\mathcal{O} \in \mathcal{I}_{\ell,r}$. Thus $p \nmid \operatorname{disc}(\mathcal{O})$ for any $\mathcal{O} \in \mathcal{I}_{\ell,r}$. Further, Corollary 2.14 implies that $\mathcal{H}_{\mathcal{O}}(x)$ has no repeated roots modulo p, and so we see that $p \nmid \operatorname{disc} \mathcal{H}_D(x)$ as well. $\qquad\square$

We now use Theorem 6.5 to reinterpret $\delta_{p_i}(\Delta)$ in terms of the Artin symbol $\left(\frac{F/\mathbb{Q}}{p} \right)$:

Lemma 6.7. *Let $\Delta \in d(\mathcal{I}_{\ell,r})$, and p be a prime such that $p > M_{\ell,r}$. Let $\sigma \in \operatorname{Gal}(F/\mathbb{Q})$ be the unique Galois element such that $\sigma|_{F^+}$ is the identity, and $\sigma|_K$ is conjugation. Then $\delta_p(\Delta) = 1$ if and only if $\left(\frac{F/\mathbb{Q}}{p} \right) = \sigma$.*

Proof. Since $p > M_{\ell,r}$ we have that $p > \Delta$, and so p is unramified in $K = \operatorname{Frac}(\mathcal{O}_\Delta)$. Since F is contained in the Hilbert class field of K, which is an unramified extension of K, we have that p is unramified in F as well. Thus $\left(\frac{F/\mathbb{Q}}{p} \right)$ is well-defined.

Next, we note that σ is well-defined, since $F^+ \subset \mathbb{R}$, and K is imaginary quadratic, so we have that $F^+ \cap K = \mathbb{Q}$. Thus $[F^+ K : \mathbb{Q}] = [K : \mathbb{Q}][F^+ : \mathbb{Q}] = 2(2^{\mu-1})$. This is equal to the degree of F over $\mathbb{Q}$, and since $F^+ K \subset F$, we have that $F = F^+ K$. It follows that $\operatorname{Gal}(F/\mathbb{Q}) \cong \operatorname{Gal}(F^+/\mathbb{Q}) \times \operatorname{Gal}(K/\mathbb{Q})$, which shows that σ is well-defined.

Finally, we come to the proof that $\delta_p(\Delta) = 1$ if and only if $\left(\frac{F/\mathbb{Q}}{p} \right) = \sigma$. By Theorem 6.5 and Lemma 6.6, $\delta_p(\Delta) = 1$ if and only if p is inert in K and splits completely in F^+. Since p is unramified in F^+, the second requirement is equivalent to requiring that the inertia degree of p is 1, which is in turn equivalent to the assertion that $\left(\frac{F^+/\mathbb{Q}}{p} \right) = 1$ by [6, Corollary 5.21]. Similarly, the first condition is equivalent to the inertia degree of p in K being 2, which is equivalent to $\left(\frac{K/\mathbb{Q}}{p} \right)$ being conjugation since this is the only element of order 2 in $\operatorname{Gal}(K/\mathbb{Q})$.

Finally, by [6, Exercise 5.16], we have that $\left(\frac{F^+/\mathbb{Q}}{p} \right)$ is the restriction of $\left(\frac{F/\mathbb{Q}}{p} \right)$ to F^+, and similarly for K. $\qquad\square$

We now use Chebotarev density to determine $\frac{1}{n} \sum_{i=1}^{n} \delta_{p_i}(\Delta)$. Recall the following version of Chebotarev density:

Theorem 6.8 ([11], pg. 167). *Let $K/\mathbb{Q}$ be an abelian extension, and let $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Then*

$$\lim_{x \to \infty} \frac{\#\{p : p \leq x, p \ unramified, \ \left(\frac{K/\mathbb{Q}}{p}\right) = \sigma\}}{\#\{p : p \leq x\}} = \frac{1}{[K : \mathbb{Q}]},$$

where $\left(\frac{K/\mathbb{Q}}{p}\right)$ is the Artin symbol.

We have the following lemma:

Lemma 6.9. *Let $(p_i)_{i=1}^{\infty}$ be an increasing sequence of consecutive primes, with $p_1 > M_{\ell,r}$, and $\Delta \in d(\mathcal{I}_{\ell,r})$. Then*

$$\lim_{n \to \infty} \frac{1}{n} \sum_{i=1}^{n} \delta_{p_i}(\Delta) = \frac{1}{2^{\mu}}.$$

Proof. Let $\pi_{\sigma}(x) = \#\{p : p \leq x, p \text{ unramified, and } \delta_p(\Delta) = 1\}$ and $\pi(x) = \#\{p : p \leq x\}$. By Lemma 6.7 and Theorem 6.8, we have

$$\lim_{x \to \infty} \frac{\pi_{\sigma}(x)}{\pi(x)} = \frac{1}{[F : \mathbb{Q}]} = \frac{1}{2^{\mu}}.$$

We now show that

$$\lim_{n \to \infty} \frac{\pi_{\sigma}(p_n)}{\pi(p_n)} = \frac{1}{n} \sum_{i=1}^{n} \delta_{p_i}(\Delta).$$

Extend $\delta_p(\Delta)$ to all primes p by setting $\delta_p(\Delta) = \begin{cases} 1 & \text{if } \left(\frac{K/\mathbb{Q}}{p}\right) = \sigma \\ 0 & \text{otherwise} \end{cases}$. Then we can compute directly that

$$\frac{\pi_{\sigma}(p_n)}{\pi(p_n)} = \frac{\sum_{i=1}^{n} \delta_{p_i}(\Delta) + \sum_{p < p_1} \delta_p(\Delta)}{n + \pi(p_1)}$$

$$= \left(1 + \frac{\pi(p_1)}{n}\right)^{-1} \left(\frac{1}{n} \sum_{i=1}^{n} \delta_{p_i}(\Delta)\right) + \left(1 + \frac{\pi(p_1)}{n}\right)^{-1} \left(\frac{1}{n} \sum_{p < p_1} \delta_p(\Delta)\right),$$

and the result follows by taking $n \to \infty$. $\square$

Combining Lemma 6.9 and Corollary 6.4, we can prove the final result from the introduction:

Theorem 6.10. *Let $(p_i)_{i=1}^{\infty}$ be an increasing sequence of consecutive primes. Then*

$$\lim_{n \to \infty} \frac{1}{n} \sum_{i=1}^{n} n_{s,p_i}(r) = \sum_{d | r} \mu(d) \# d(\mathcal{I}_{\ell, n | \frac{r}{d}}).$$

Proof. We first note that since the sequence (p_i) is increasing, only finitely many of the terms are less than $M_{\ell,r}$. Thus Corollary 6.4 applies unchanged.

Next, note that the first two sums in Corollary 6.4 are finite, we can interchange the limit and the sums to get that

$$\lim_{n \to \infty} \frac{1}{n} \sum_{i=1}^{n} n_{s,p_i}(r) = \sum_{d | r} \mu(d) \sum_{\Delta \in d\left(\mathcal{I}_{\ell, n | \frac{r}{d}}\right)} 2h_2(\Delta) \lim_{n \to \infty} \left(\frac{1}{n} \sum_{i=1}^{n} \delta_{p_i}(\Delta)\right).$$

The theorem follows from the fact that $h_2(\Delta) = 2^{\mu-1}$, and the remaining limit is $\frac{1}{2^{\mu}}$ by Lemma 6.9. $\square$

As an example, we compute the expected number of 3-cycles along the spine in $\mathcal{G}_3$.

Example 6.11. Using Proposition 6.1, we see that

$$d(\mathcal{I}_{3,n|3}) = \{-107, -104, -92, -83, -59, -44, -23, -11, -8\},$$

and $d(\mathcal{I}_{3,n|1}) = \{-11, -8\}$. Thus the expected number of 3-cycles along the spine in $\mathcal{G}_3$ is given by

$$\mu(1)\#d(\mathcal{I}_{3,n|3}) + \mu(3)\#d(\mathcal{I}_{3,n|1}) = 9 - 2 = 7.$$

(A) 3-cycles in the 3-isogeny graph
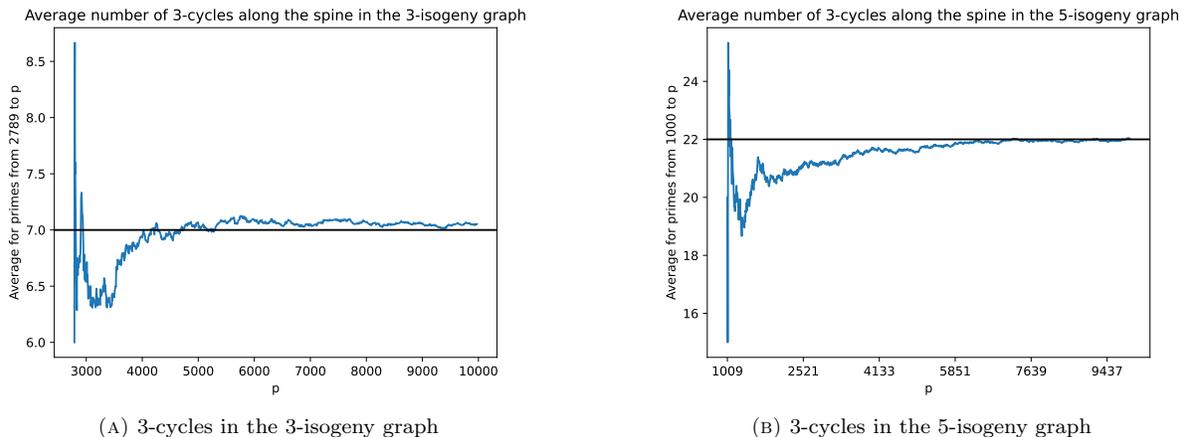
(B) 3-cycles in the 5-isogeny graph

FIGURE 1. Average numbers of 3-cycles along the spine in the 3-isogeny and 5-isogeny graphs

Example 6.11 demonstrates the following corollary:

Corollary 6.12. *With the notation and assumptions from Theorem 6.10, suppose further that r is prime. Then*

$$\lim_{n \to \infty} \frac{1}{n} \sum_{i=1}^{n} n_{s,p_i}(r) = \#d(\mathcal{I}_{\ell,r}).$$

Proof. Since r is prime, the only divisors of r are 1 and r. By Theorem 6.10, we have that

$$\lim_{n \to \infty} \frac{1}{n} \sum_{i=1}^{n} n_{s,r}(p_i) = \mu(1)\#d(\mathcal{I}_{\ell,n|r}) + \mu(r)\#d(\mathcal{I}_{\ell,n|1})$$

$$= \mu(1)(\#d(\mathcal{I}_{\ell,r}) + \#d(\mathcal{I}_{\ell,1})) + \mu(r)\#d(\mathcal{I}_{\ell,1})$$
$$= \#d(\mathcal{I}_{\ell,r}) + \#d(\mathcal{I}_{\ell,1}) - \#d(\mathcal{I}_{\ell,1})$$
$$= \#d(\mathcal{I}_{\ell,r}).$$

□

6.1. **Remarks on computational verification.** To verify the results of Theorem 6.10 and Corollary 6.4, we collected data on 3-cycles in the 3-isogeny and 5-isogeny graphs for all primes up to $10,000$.

Figures 1a and 1b show the results, with the black lines indicating the predicted limit in Theorem 6.4. In the case of Figure 1a, $2,789$ was chosen because it is the first prime larger than $M_{3,3}$. Since $M_{5,3} = 61,876$, considering only primes larger than $M_{5,3}$ was impractical, so $1,000$ was chosen arbitrarily. In particular, we see that even at primes less than $M_{\ell,r}$, the average converges quickly toward the final limit.

In Figure 1a, we see that the average remains slightly above the predicted limit even at the largest primes. We hypothesize that this happens due to inequalities in prime races. The number of 3-cycles along the spine produced by each determinant in $\mathcal{I}_{\ell,r}$ is determined by congruence conditions on p modulo d or $4d$, so it is likely that certain congruences are more common for small values of p. If these congruences produce more or less than the average number of 3-cycles along the spine, then this would cause the average number of 3-cycles along the spine for primes up to large bounds to remain slightly above or below the limit.

7. CYCLES OF EVEN LENGTH

We now consider the case of even cycles, where we are able to obtain partial results. The only place where our assumption that r has odd length was used in an essential fashion is in Proposition 3.7, when we proved

that each cycle of length r contains either 0 or 1 $\mathbb{F}_p$-vertices.

In this argument we showed that for large enough p, the number of $\mathbb{F}_p$-vertices on each cycle in $\mathcal{G}_{\mathcal{O},\ell}$ of length r is either 0 or odd. Further, this number has to divide a power of 2. This allowed us to conclude that any cycle of odd length r in $\mathcal{G}_\ell$ with one $\mathbb{F}_p$-vertex has exactly one $\mathbb{F}_p$-vertex. In the case where r is even, however, the number of $\mathbb{F}_p$-vertices on each cycle in $\mathcal{G}_{\mathcal{O},\ell}$ can be a non-trivial power of 2. In this section, we alter the graph theoretic arguments to show that under some additional assumptions, the number of such vertices is exactly 2. We begin by defining a modified version of our bound $M_{\ell,r}$:

Definition 7.1. Let r be even. We set $M_{\ell,r}^{\text{strong}} := \max\{M_{\ell,r_i} : r_i < r\}$.

Remark 7.2. We expect that $M_{\ell,r}^{\text{strong}}$ is always equal to $M_{\ell,r}$, since the discriminants where primes above ℓ have order r in the class group will generally be larger than discriminants where they have order r_i for $r_i < r$. For the purposes of this paper, however, it is most important to have a finite bound.

We can now state partial results for Theorem 4.1 in the case where r is even:

Theorem 7.3. *Let r be an even number that is not a power of 2, and $p > M_{\ell,r}^{strong}$. Then the results of Theorem 4.1 and Corollary 4.2 hold unchanged.*

The proof strategy will be the same, except that we will replace the result of Proposition 3.7 with Proposition 7.5 below. This proposition says that instead of 0 or 1 $\mathbb{F}_p$-vertex, each cycle will contain 0 or 2 $\mathbb{F}_p$-vertices. Thus, we will get the following modified version of Theorem 6.10:

Theorem 7.4. *Let $(p_i)_{i=1}^\infty$ be an increasing sequence of consecutive primes, and r be even. Then if r is not a power of 2 we have*

$$\lim_{n\to\infty} \frac{1}{n}\sum_{i=1}^n n_{s,p_i}(r) = \frac{1}{2}\sum_{d|r}\mu(d)\#d(\mathcal{I}_{\ell,n|\frac{r}{d}}).$$

The only modification of the proofs of Theorem 4.1 and Theorem 6.10 needed to prove Theorem 7.3 and Theorem 7.4 is replacing Proposition 3.7 with the following proposition:

Proposition 7.5. *Let r be even and $p > M_{\ell,r}^{\text{strong}}$. If r is not a power of 2, and C is an r-cycle in $\mathcal{G}_\ell$, then the number of $\mathbb{F}_p$-vertices on C is either 0 or 2.*

Before proving Proposition 7.5, we prove the following Lemma:

Lemma 7.6. *Let $p > M_{\ell,r}^{\text{strong}}$, and C be an isogeny cycle in $\mathcal{G}_\ell$ of length r. Let v be a vertex in C. Then there is only one incoming and one outgoing edge connected to v in C. Further, if C' is the cycle in $\mathcal{G}_{\mathcal{O},\ell}$ corresponding to C via Theorem 2.9, then the map from C' to C obtained by forgetting orientations is injective on vertices.*

Proof. Under the bijection of Theorem 2.9, there is an order $\mathcal{O} \in \mathcal{I}_{\ell,r}$, and a cycle C' in $\mathcal{G}_{\mathcal{O},\ell}$ that corresponds to C after forgetting orientations. The conclusion of the Lemma holds for C' by Proposition 2.8, and forgetting orientations preserves sources and targets of edges, so we need only show that forgetting orientations is injective on vertices.

Suppose instead that there are two vertices in C' with the same j-invariant. Let j be this j-invariant. We then obtain two cycles in $\mathcal{G}_\ell$ through j upon forgetting orientations. Both of these cycles have length at most r. By composing the isogenies in these cycles, we obtain two cyclic endomorphisms in $\text{End}(E(j))$, of degree ℓ^{r_i}, ℓ^{r_j} for $r_i, r_j < r$. These endomorphisms then give embeddings of imaginary quadratic orders in $\mathcal{I}_{\ell,r_i}$ and $\mathcal{I}_{\ell,r_j}$ into $\text{End}(E(j))$. This contradicts Remark 2.21, because we have chosen $p > M_{\ell,r}^{\text{strong}}$. Thus we see that forgetting orientations is injective on vertices. $\square$

We now return to the proof of Proposition 7.5.

Proof (Proposition 7.5). By Corollary 3.2, there is a constant K such that each r-cycle in $\mathcal{G}_{\mathcal{O},\ell}$ containing an $\mathbb{F}_p$-vertex contains K $\mathbb{F}_p$-vertices. Since the total number of such vertices is a power of 2, the number of vertices on each cycle cannot be r, since r is not a power of 2. By Lemma 7.6, each r-cycle in $\mathcal{G}_\ell$ also contains r vertices, and the number of $\mathbb{F}_p$-vertices is again a power of 2. Thus each r-cycle in $\mathcal{G}_\ell$ contains
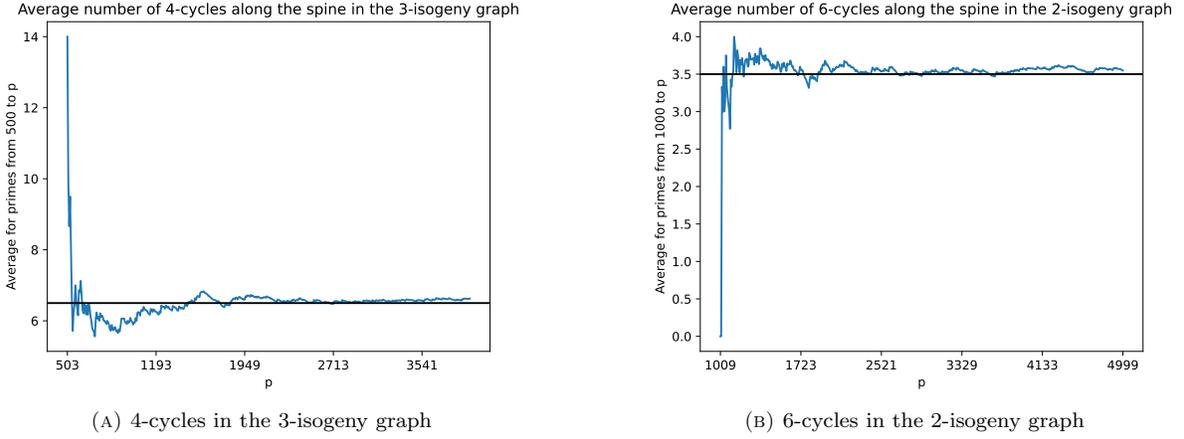
(A) 4-cycles in the 3-isogeny graph

(B) 6-cycles in the 2-isogeny graph

FIGURE 2. Average numbers of 4-cycles (resp. 6-cycles) along the spine in the 3-isogeny (resp. 2-isogeny) graph

$\mathbb{F}_{p^2}$-vertices. Let C be such a cycle containing at least one $\mathbb{F}_p$-vertex. We will show that C contains exactly 2 $\mathbb{F}_p$-vertices.

Let C be given by a sequence of isogenies $\phi_1, \phi_2, \ldots, \phi_r$. Since we are forgetting basepoint in Definition 2.1, we may assume that the domain of ϕ_1 is an $\mathbb{F}_p$-vertex, and the codomain is an $\mathbb{F}_{p^2}$-vertex. Let i be the first index such that the codomain of ϕ_i is an $\mathbb{F}_p$-vertex, and let v be this vertex. We will show that $i = \frac{r}{2}$, from which it will follow that there are exactly two $\mathbb{F}_p$-vertices in C.

By changing basepoint to v if necessary, we may assume that $i \leq \frac{r}{2}$. Applying Frobenius to the sequence of isogenies $\phi_1, \phi_2, \ldots, \phi_i$, we obtain a sequence $\phi_1^{(p)}, \phi_2^{(p)}, \ldots, \phi_i^{(p)}$, which begins at the domain of ϕ_1, and ends at v. The vertices in between in this sequence are distinct from the vertices traversed in the sequence $\phi_1, \phi_2, \ldots, \phi_i$ by the assumption that i is the first index where the codomain of ϕ_i is defined over $\mathbb{F}_p$. Taking duals therefore gives a closed walk $\phi_1, \ldots, \phi_i, \hat{\phi}_i^{(p)}, \ldots, \hat{\phi}_1^{(p)}$ with no-backtracking through v. This is an isogeny cycle of length $2i \leq r$, which we denote by C'. By Remark 2.21, our assumption that $p > M_{\ell,r}^{\text{strong}}$ guarantees that this cycle is either C or $\hat{C}$. Since C and $\hat{C}$ have the same vertices, and there are exactly 2 $\mathbb{F}_p$-vertices in C', we see that C has exactly 2 $\mathbb{F}_p$-vertices. This finishes the proof.

$\square$

See Figures 2a and 2b for experimental data verifying the results of Theorem 7.4. We note that Figure 2a provides computational evidence that the results of Theorem 7.3 and Theorem 7.4 both hold even in the case where r is a power of 2. In this case however, the possibility of cycles through the spine that are completely fixed by Frobenius makes the graph theoretic arguments in Propostion 7.5 fail to provide a proof.

We end with a remark on an interesting consequence of Proposition 7.5:

Remark 7.7. By taking $r = 2n$, Proposition 7.5 says that there are infinitely many primes p where $\mathcal{G}_\ell$ contains spine vertices of distance at most n from each other. The vertices on the spine are exactly the vertices whose endomorphism rings contain an embedded copy of $\mathbb{Z}[\sqrt{-p}]$. Boneh and Love studied the distribution of vertices with small endomorphisms in [13], and found that small endomorphisms have a repelling effect. In this context, our result says that vertices with endomorphisms of degree roughly $\sqrt{p}$ can remain close together in $\mathcal{G}_\ell$.

References

[1] Sarah Arpin, Catalina Camacho-Navarro, Kristin Lauter, Joelle Lim, Kristina Nelson, Travis Scholl, and Jana Sotáková. "Adventures in supersingularland". In: *Exp. Math.* 32.2 (2023), pp. 241–268. ISSN: 1058-6458,1944-950X. DOI: 10.1080/10586458.2021.1926009. URL: https://doi.org/10.1080/10586458.2021.1926009.

[2] Sarah Arpin, Mingjie Chen, Kristin E. Lauter, Renate Scheidler, Katherine E. Stange, and Ha T. N. Tran. *Orientations and cycles in supersingular isogeny graphs*. 2022. arXiv: 2205.03976 [math.NT].

[3] Denis X. Charles, Kristin E. Lauter, and Eyal Z. Goren. "Cryptographic hash functions from expander graphs". In: *J. Cryptology* 22.1 (2009), pp. 93–113. ISSN: 0933-2790,1432-1378. DOI: 10.1007/s00145-007-9002-x. URL: https://doi.org/10.1007/s00145-007-9002-x.

[4] Mingjie Chen and Jiangwei Xue. *On $\mathbb{F}_p$-roots of the Hilbert class polynomial modulo p*. 2022. arXiv: 2202.04317 [math.NT].

[5] Alex Cowan. "Computing newforms using supersingular isogeny graphs". In: *Res. Number Theory* 8.4 (2022), Paper No. 96, 23. ISSN: 2522-0160,2363-9555. DOI: 10.1007/s40993-022-00392-z. URL: https://doi.org/10.1007/s40993-022-00392-z.

[6] David A. Cox. *Primes of the form $x^2 + ny^2$—Fermat, class field theory, and complex multiplication*. Third. With contributions by Roger Lipsett. AMS Chelsea Publishing, Providence, RI, [2022] ©2022, pp. xv+533. ISBN: [9781470470289]; [9781470471835].

[7] Wissam Ghantous, Shuichi Katsumata, Federico Pintore, and Mattia Veroni. *Collisions in Supersingular Isogeny Graphs and the SIDH-based Identification Protocol*. Cryptology ePrint Archive, Paper 2021/1051. https://eprint.iacr.org/2021/1051. 2021. URL: https://eprint.iacr.org/2021/1051.

[8] Benedict H. Gross and Don B. Zagier. "On singular moduli". In: *J. Reine Angew. Math.* 355 (1985), pp. 191–220. ISSN: 0075-4102,1435-5345.

[9] Michael J. Jacobson Jr. and Hugh C. Williams. *Solving the Pell equation*. CMS Books in Mathematics/Ouvrages de Mathématiques de la SMC. Springer, New York, 2009, pp. xx+495. ISBN: 978-0-387-84922-5.

[10] Masanobu Kaneko. "Supersingular j-invariants as singular moduli mod p". In: *Osaka J. Math.* 26.4 (1989), pp. 849–855. ISSN: 0030-6126. URL: http://projecteuclid.org/euclid.ojm/1200781857.

[11] Serge Lang. *Algebraic number theory*. Second. Vol. 110. Graduate Texts in Mathematics. Springer-Verlag, New York, 1994, pp. xiv+357. ISBN: 0-387-94225-4. DOI: 10.1007/978-1-4612-0853-2. URL: https://doi.org/10.1007/978-1-4612-0853-2.

[12] Jianing Li, Songsong Li, and Yi Ouyang. *Factorization of Hilbert class polynomials over prime fields*. 2021. arXiv: 2108.00168 [math.NT].

[13] Jonathan Love and Dan Boneh. *Supersingular Curves With Small Non-integer Endomorphisms*. 2020. arXiv: 1910.03180 [math.NT].

[14] Sam Mayo. *Automorphisms of the Supersingular Isogeny Graph*. 2023. arXiv: 2305.08158 [math.NT].

[15] Hiroshi Onuki. "On oriented supersingular elliptic curves". In: *Finite Fields Appl.* 69 (2021), Paper No. 101777, 18. ISSN: 1071-5797,1090-2465. DOI: 10.1016/j.ffa.2020.101777. URL: https://doi.org/10.1016/j.ffa.2020.101777.

[16] Arnold K. Pizer. "Ramanujan graphs and Hecke operators". In: *Bull. Amer. Math. Soc. (N.S.)* 23.1 (1990), pp. 127–137. ISSN: 0273-0979,1088-9485. DOI: 10.1090/S0273-0979-1990-15918-X. URL: https://doi.org/10.1090/S0273-0979-1990-15918-X.

[17] Joseph H. Silverman. *The arithmetic of elliptic curves*. Vol. 106. Graduate Texts in Mathematics. Springer-Verlag, New York, 1986, pp. xii+400. ISBN: 0-387-96203-4. DOI: 10.1007/978-1-4757-1920-8. URL: https://doi.org/10.1007/978-1-4757-1920-8.

University of Colorado Boulder, Boulder, Colorado, USA
Email address: eli.orvis@colorado.edu
URL: https://euclid.colorado.edu/~wior7645/HTML/home.html