IHARA ZETA FUNCTIONS OF ABSTRACT ISOGENY GRAPHS AND MODULAR CURVES

JUN BO LAU, TRAVIS MORRISON, ELI ORVIS, GABRIELLE SCULLARD, AND LUKAS ZOBERNIG

Abstract. We introduce abstract isogeny graphs; these graphs encompass supersingular isogeny graphs with level structure and higher dimensional isogeny graphs. Our definition can be thought of as a "non-orientable" variation of Serre's definition of a graph. We prove an analogue of Ihara's determinant formula and use this formula, along with the Jacquet-Langlands correspondence, to relate the ℓ-isogeny graph of supersingular elliptic curves with level n structure to the zeta functions of the modular curves of $X_0(p)_{\mathbb{F}_\ell}$ and $X_0(pn)_{\mathbb{F}_\ell}$, generalizing previous results of Sugiyama and Lei-Mueller from $p = 1 \pmod{12}$ to arbitrary p.

1. Introduction

Let G be a finite graph. In the same spirit as Selberg's definition of the zeta function of a hyperbolic surface, following [Ser03, Sun86, Bas92, Iha66], one can associate a zeta function $\zeta_G(u)$ to G, defined as an Euler product

$$\zeta_G(u) \coloneqq \prod_{[C]} (1 - u^{\nu(C)})^{-1}, \tag{1}$$

where the product runs over the primes of G. A prime of G is an equivalence class of cyclic rotations of a non-backtracking, closed walk that is not a repeat of another, shorter cycle some number of times. This is a discrete analogue of a simple closed geodesic. The degree $\nu(C)$ of a prime $[C]$ is the number of edges in the cycle C.

Ihara showed ζ_G is a rational function. In particular, suppose G is undirected, connected, and $\ell + 1$-regular and let A denote the adjacency matrix of G. Then Ihara shows in [Iha66, Theorem 2][1] that

$$\zeta_G(u) = \frac{(1 - u^2)^{\chi(G)}}{\det(1 - uA + \ell u^2)},$$

where $\chi(G) = \#\operatorname{vert}(G) - \#\operatorname{edge}(G)$ is the Euler characteristic of G. Various properties of G can be read off from ζ_G. For example, the order of the pole of ζ_G at 1 is $B_1(G) = 1 - \chi(E)$, the rank of the fundamental group of the CW complex associated to G. The poles of ζ_G other than those at ± 1 and $1/\ell$ are related to the nontrivial eigenvalues of the adjacency operator of G and hence control expansion properties of G. For example, Sunada [Sun86] showed G is Ramanujan if and only if all other poles of ζ_G have magnitude $\sqrt{\ell}$.

Isogeny graphs of supersingular elliptic curves are interesting for both theoretical and practical reasons, from the fast computation of modular forms [Mes86] to isogeny-based cryptography [CLG09]. Fix distinct primes p and ℓ and let $G = G(p, \ell)$ denote the ℓ-isogeny graph of supersingular elliptic curves in characteristic p: vertices are isomorphism classes

Date: June 5, 2025.

[1] See [Sun86, Proposition F] where Sunada credits this result to Ihara, who proved the analogous statement for the zeta function associated to a subgroup of $\mathrm{PSL}_2(\mathbb{Q}_p)$.

of supersingular elliptic curves over $\overline{\mathbb{F}}_p$, and (directed) edges are isomorphism classes of isogenies of degree ℓ. Thus $G(p,\ell)$ is a directed multigraph with constant out-degree $\ell+1$. The adjacency matrix of G determines the action of T_ℓ, the ℓth Hecke operator acting on weight 2 cusp forms for $\Gamma_0(p)$. Thus by the Ramanujan-Petersson conjecture, proved by Deligne, the nontrivial eigenvalues of A have absolute value at most $2\sqrt{\ell}$. Thus G is (a directed variant of) a Ramanujan graph.

To define the zeta function of $G(p,\ell)$, we need a notion of a non-backtracking walk in an isogeny graph. Before addressing this, let us now be more precise about the definition of a graph, according to Serre [Ser03] and Bass [Bas92], that one uses to define the Ihara zeta function.

1.1. Graphs and their zeta functions.

A **graph** Γ consists of the data of a set of **vertices** X, **edges** Y, a function $(s,t)\colon Y\to X\times X$ giving the **source** and **target** of an edge, and a fixed-point free involution $J\colon Y\to Y$, the **orientation reversal map**, which satisfies $s(Jy)=t(y)$. A walk in Γ consists of a sequence of edges $(y_1,\dots,y_n)$ where $s(y_{i+1})=t(y_i)$; the walk is **reduced** or **non-backtracking** if $Jy_i\neq y_{i+1}$. One then defines cycles, primitive cycles, and primes as above. The dual map on isogenies induces a map on the edges of G that swaps source and target, but this map need not be an involution, and it can have fixed points! There is a natural notion of a non-backtracking walk, though: a sequence of edges, represented by isogenies $\phi_1,\dots,\phi_t$ where the target of ϕ_i is the source of ϕ_{i+1}, and $\phi_{i+1}\neq u\widehat{\phi_i}$ for any automorphism u. Non-backtracking walks in isogeny graphs are used in many isogeny-based cryptosystems [CLG09, DFJP14, BCC$^+$23], so this notion of non-backtracking has practical importance as well.

Since the dual map need not be a fixed-point free involution on edges, $G(p,\ell)$ is not a graph according to Serre's definition [Ser03]. This complicates the definition of the Ihara zeta function since there is more than one natural way to make G into an undirected graph. We describe the possibilities in Section 3.

There has been previous work on the Ihara zeta function of supersingular isogeny graphs. Sugiyama proves a relationship between the zeta function of $G(p,\ell)$ and of $X_0(p)_{\mathbb{F}_\ell}$ for $p\equiv 1 \pmod{12}$, where $X_0(N)$ denotes the modular curve whose non-cuspidal points parametrize isomorphism classes of elliptic curves with a marked cyclic subgroup of order N. One reason to restrict to $p\equiv 1 \pmod{12}$ is that for such p, the automorphism group of any supersingular elliptic curve E is equal to $\{\pm 1\}$. This is because the j-invariants 0 and 1728 are not supersingular if $p\equiv 1 \pmod{12}$. But this is not enough to make $G(p,\ell)$ into a graph in the sense of Serre [Ser03]; while the dual map induces an involution on $G(p,\ell)$, Serre requires that the involution on the graph is fixed-point free. This is important for the study of primes of $G(p,\ell)$, since a loop y can be a fixed point of the involution. Such a loop produces a cycle (y) of length one that will not induce a prime, since then the cycle has a "tail" and the cycle $C^2=(y,y)$ has backtracking. Such cycles exist in $G(p,\ell)$ whenever the prime p is inert in the order $\mathbb{Z}[\sqrt{-\ell}]$, which will happen for infinitely many p for any given ℓ. Sugiyama claims that

$$\zeta_{G(p,\ell)}=\frac{(1-s^2)^{n(1-\ell)/2}}{\det(1-As+\ell s^2)},$$

where A is the adjacency matrix of $G(p,\ell)$ and $n=(p-1)/12$ is the number of isomorphism classes of supersingular elliptic curves when $p=1 \pmod{12}$. As we shall see, this formula is incorrect. This is because the Ihara determinant formula does not hold in general, even for

$p \equiv 1 \pmod{12}$. In particular, the claim in [Sug17, Proposition 3.1(b)] is incorrect, and this means the result of Hashimoto [Has89] cannot be applied to give the determinant formula of the zeta function of $G(p, \ell)$. Instead, one requires a relaxed definition of a graph in order to obtain a meaningful definition of a prime of $G(p, \ell)$ and then a correct variation of Ihara's determinant formula for the zeta function of $G(p, \ell)$.

Lei and Müller [LM24] study a similar formula relating the zeta functions of $G(p, \ell, N)$, the "supersingular isogeny graph with level N structure" for $p \equiv 1 \pmod{12}$. This graph was used for cryptographic purposes in [BCC⁺23]. The results of [LM24] are not incorrect, since they take the determinant expression of the zeta function as the *definition* of the zeta function, but this means that their formula loses the connection to many of the graph theoretic properties that the Ihara zeta function is intended to capture. For example, their Ihara zeta function does not count primes in the sense described above.

1.2. **Abstract isogeny graphs.** In this paper, we introduce the notion of an *(abstract) isogeny graph* that extends Serre's definition of a graph Γ by relaxing the requirement that the map J on the edges of the graph is a fixed-point free involution. The only restriction we put on $J \colon Y \to Y$ is that for all $y \in Y$, we have $s(Jy) = t(y)$. When J is a fixed-point free involution, we may partition Y into subsets $S \sqcup JS$ [Ser03, §2.1]; such a partition is called an **orientation** of Γ. Abstract isogeny graphs can be viewed as graphs that may be "non-orientable", so we call a graph Γ orientable when J is a fixed-point free involution, or equivalently, when it is a graph in the sense of Serre and Bass. We show there are two natural orientable graphs Γ^{+1} and Γ^{-1} associated to Γ, and we study the topology of abstract isogeny graphs, assuming they are finite. We define primes of Γ in the natural way, and prove that the zeta function of an isogeny graph is a rational function. In Theorem 4.11, we prove a generalization of Ihara's determinant formula for our abstract isogeny graphs that recovers Ihara's formula when the isogeny graph is orientable (i.e., is a graph in the sense of Serre and Bass). We state it in a special case below. Suppose that $\Gamma = (X, Y, s, t, J)$ is an abstract isogeny graph such that J is an involution but with r fixed points. Since J is an involution, we can make Γ into an undirected multigraph with loops by defining the undirected edges to be subsets of Y of the form $\{y, Jy\}$; denote the resulting graph by Γ^u. Then Theorem 4.11 specializes to the following:

Theorem 1.1. *Let $\Gamma = (X, Y, s, t, J)$ be an abstract isogeny graph of degree $\ell + 1$ and assume J is an involution with r fixed points. Let A be the adjacency operator for Γ. Let $\chi(\Gamma^u) = \#\operatorname{edge}\Gamma^u - \#\operatorname{vert}\Gamma^u$ be the Euler characteristic of the undirected graph Γ^u. Then*

$$\zeta_\Gamma(u) = \frac{(1-u)^{\chi(\Gamma^u)}(1+u)^{\chi(\Gamma^u)+r}}{\det(1 - uA + u^2\ell)}$$

where A is the adjacency matrix of $G(p, \ell)$.

This theorem can be used to give a formula for the zeta function of the supersingular ℓ-isogeny graph in characteristic p when $p \equiv 1 \pmod{12}$; see **??**, which specializes to the following

Corollary 1.2. *Let p and ℓ be primes and assume $p \equiv 1 \pmod{12}$. Let $r = (1 - \left(\frac{-\ell}{p}\right)(h(-\ell) + h(-4\ell))/2$, where $h(D)$ denotes the class number of the quadratic order of discriminant D. Then*

$$\zeta_{G(p,\ell)} = \frac{(1-u)^{(1-\ell)(p-1)/24 - r/2}(1+u)^{(1-\ell)(p-1)/24 + r/2}}{\det(1 - uA + u^2\ell)}.$$

Our definition of an abstract isogeny graph captures many examples of supersingular isogeny graphs that appear in the literature, including the graphs that so far have been studied for cryptographic applications. We are thus able to correct [Sug17], improve on the results of [LM24], while also extending their results to arbitrary prime p.

2. Prior work on zeta functions of isogeny graphs

2.1. **Prior results.** Two authors have previously addressed the relationship between Ihara zeta functions of supersingular isogeny graphs and Hasse-Weil zeta functions of modular curves: Sugiyama in 2017 [Sug17] and Antonio Lei and Katharina Müller in 2024 [LM24]. In this subsection, we recall their results, paying special attention to the issues posed by the failure of the dual map to be fixed-point free. We identify a mistake in the formula of Sugiyama, and point out how the meaning of the Ihara zeta function is subtly altered in the work of Lei-Müller, causing it to no longer count non-backtracking paths.

Sugiyama defines $\zeta_{G(p,\ell)}(u)$ as the Euler product (1), where a path is considered to have backtracking if consecutive edges compose to the multiplication-by-ℓ map. He then claims that

$$\zeta_{G(p,\ell)}(u) = \frac{(1-u^2)^{n(1-\ell)/2}}{\det(1-uA+\ell u^2)},$$

where $n = \frac{p-1}{12}$. Example 2.2 below shows that this formula is incorrect in the case where $G(p,\ell)$ contains loops that are fixed by the action of the dual map. Ultimately, the error appears to stem from Proposition 3.1(b) in Sugiyama's paper, which claims that the diagonal entries of the Brandt matrix are all even. This is false in the presence of edges fixed by the dual map, and a counterexample is given in Example 2.2.

In [LM24], Antonio Lei and Katharina Müller extended the results of Sugiyama relating zeta functions of supersingular isogeny graphs and zeta functions of modular curves to the case of isogeny graphs with level structure. Let $W(C,S)$ denote the Hasse-Weil zeta function of an algebraic curve C, $Z(X_p^q(N),S)$ be the Ihara zeta function of the supersingular isogeny graph with Borel N-level structure, and $\chi(X_p^q(N))$ be the Euler characteristic of the graph $X_p^q(N)$. Theorem A in [LM24] states:

Theorem 2.1. *The following equality holds (for $q \equiv 1 \pmod{12}$):*

$$W(X_0(qN)_{\mathbb{F}_p},S)W(X_0(N)_{\mathbb{F}_p},S)^{-2}Z(X_p^q(N),S) = (1-S^2)^{\chi(X_p^q(N))}.$$

The formula in Theorem 2.1 is correct given the definition of the Ihara zeta function used by Lei and Müller, but this definition does not agree with the Euler product in (1). In particular, in Definition 2.9 of their paper, Lei and Müller *define* the Ihara zeta function of a graph X to be

$$Z(X,S) := \frac{(1-S^2)^{\chi(X)}}{\det(I-AS+(D-I)S^2)},$$

where A and D are the adjacency matrix and the degree matrix of X, respectively. This formula agrees with the Euler product in (1) in the case where J, is a fixed-point free involution, but not when J has fixed-points. Example 2.3 shows that even in the case where $p \equiv 1 \pmod{12}$, this definition may not give the exponential generating function for the number of primes in supersingular isogeny graphs, and so Lei-Müller's formula does not directly relate the count of primes in supersingular isogeny graphs to point counts on modular curves. In Section 7 we give a version of Theorem 2.1 with the zeta function defined by Lei-Müller replaced with one that is equal to the Euler product (1), and in Section 8 we use this to give a formula relating point counts on modular curves to prime counts in supersingular isogeny graphs, and ultimately, imaginary quadratic class numbers.

Example 2.2. *To give a concrete example of the mistake in Sugiyama's Proposition 3.1(b), we find a prime p that is equivalent to* 1 *modulo* 12*, and a prime ℓ such that $G(p, \ell)$ contains a self-dual loop. It turns out that the smallest example, $p = 13$, $\ell = 2$ suffices. When $p = 13$ there is only one supersingular j-invariant, so all three isogenies of degree two are endomorphisms of this curve, and the Brandt matrix $B(2)$ is the 1×1 matrix* [3].

The mistake in Sugiyama's argument is the claim that $\ker \phi$ and $\ker \hat{\phi}$ generate the ℓ-torsion, which is given without justification, and used to conclude that $\ker \phi \neq \ker \hat{\phi}$. This claim is simply false, and it is possible for $\ker \phi = \ker \hat{\phi}$. In Lemma 6.4 we count the number of endomorphisms of degree ℓ satisfying this condition on supersingular elliptic curves over $\overline{\mathbb{F}}_p$.

Example 2.3. *The mistake in Example 2.2 carries over into the results of Lei and Muller. For example, Lei and Müller claim, following Sugiyama, that the exponent of $(1 - u^2)$ in the Ihara zeta function of $G(p, \ell)$ is given by $n(1 - \ell)/2$. In the case $p = 13$ and $\ell = 2$, this exponent is not even integral.*

Even in the case where $p \equiv 1 \pmod{12}$ and the Euler characteristic is integral, however, the definition of the Ihara zeta function used by Lei and Müller does not capture the isogenists' notion of "non-backtrackracking path." For example, in the isogeny graph $G(13, 2)$ considered in the previous example, there is only one self-dual isogeny, by Lemma 6.4. Thus the number of length one non-backtracking tailless cycles is two, and we can easily count that the number of length two non-backtracking tailless cycles is six. The Euler characteristic, however, is two, so the definition of Ihara zeta function in Lei and Müller's paper (using the Euler characteristic, rather than the formula $n(1 - \ell)/2$ that is claimed to be equal to the Euler characteristic but is not integral) gives

$$\zeta_G(u) = \frac{(1 - u^2)^2}{1 - 3u + 2u^2},$$

which has

$$u\frac{d}{du}\log(\zeta_G(u)) = 3u + u^2 + 9u^3 + \cdots ,$$

whereas our zeta function has logarithmic derivative series expansion $2u + 6u^2 + 8u^3 + \cdots$.

3. Abstract isogeny graphs

In this section, we propose a definition of a graph that extends the definition of Serre [Ser03] and Bass [Bas92] that is general enough to accommodate various types of isogeny graphs. In particular, Serre defines a graph to consist of the data $\Gamma = (X, Y, s, t, J)$ where $X = \operatorname{vert} \Gamma$ and $Y = \operatorname{edge} \Gamma$ are sets, $s, t \colon Y \to X$ are functions (the source and target) and $J \colon Y \to Y$ is a fixed-point free involution such that $s(Jy) = t(y)$ (the orientation reversal map). As discussed in the previous section, the dual map on isogeny graphs is not necessarily an involution and it may have fixed-points even in cases that it is an involution. And worse, the dual map may not even preserve incidence of edges; see Section **??**.

Definition 3.1. *An* **(abstract) isogeny graph** Γ *consists of two sets,* $X = \operatorname{vert}\Gamma$ *and* $Y = \operatorname{edge}\Gamma$*, a function* $Y \to X \times X$ *sending an edge* y *to* $(s(y), t(y))$ *(the* **source** *and* **target** *of the directed edge* y*), a function* $J\colon Y \to Y$*, the* **dual** *map, and a function* $L\colon X \to X$*, such that*

(1) $s(Jy) = t(y)$ *for all* $y \in Y$*, and*
(2) $t(Jy) = Ls(y)$ *for all* $y \in Y$*.*

Definition 3.2. *Suppose* Γ *is an abstract isogeny graph. If* $\#\{y : s(y) = x\}$ *is finite and constant, independent of* $x \in X = \operatorname{vert}\Gamma$*, call* Γ **regular***; if this constant is* d*, call* Γ d**-regular***. If* J *is a fixed-point free involution, we will say* Γ *is an* **orientable isogeny graph***. Otherwise, we say that* Γ *is* **non-orientable***. Suppose* Γ *is an orientable graph. An* **orientation** *on* Γ *is a subset* $Y_+ \subset Y$ *such that* Y *is the disjoint union of* Y_+ *and* $J(Y_+)$*. An* **oriented graph** *is an orientable graph* Γ *equipped with a choice of orientation.*

If Γ is an orientable graph, an orientation always exists. When Γ is orientable, we have

$$t(Jy) = s(J^2y) = s(y)$$

for all $y \in Y$, so L is the identity. An orientable isogeny graph is simply a graph according to Serre and Bass.

We now extend the usual definitions of (reduced) paths in graphs to isogeny graphs.

Definition 3.3. *A* **path** *in a graph* Γ *is a sequence* $(y_1, \ldots, y_n)$ *of edges* $y_i \in \operatorname{edge}\Gamma = Y$ *where the edges* y_i *satisfy* $s(y_{i+1}) = t(y_i)$ *for* $1 \leq i \leq n-1$*. We will often denote the path by* $y_1 \cdots y_n$*. Call* $s(y_1)$ *and* $t(y_n)$ *the* **terminal vertices** *of the path. A* **cycle** *in* Γ *is a path* $\{y_1, \ldots, y_n\}$ *such that* $t(y_n) = s(y_1)$*. A graph is* **connected** *if every ordered pair of vertices are the terminal vertices of a path. A* **tree** *is a connected orientable graph with no cycles. A* **subtree** *of a graph is any subgraph isomorphic to a tree. A* **spanning tree** *in a graph* Γ *is a subtree containing all the vertices of* Γ*.*

4. The Ihara determinant formula for a non-orientable graph

In this section, we define the Ihara zeta function of an abstract isogeny graph and prove an analogue of Ihara's determinant formula in Theorem 4.11.

4.1. The zeta function of a regular abstract isogeny graph.

Definition 4.1. *Let* Γ *be an abstract isogeny graph. If* $P = y_1 \cdots y_n$ *is a path in* Γ*, define the* **length** *of* P *to be* $\nu(P) := n$*. The path* P *is* **reduced** *if* $Jy_i \neq y_{i+1}$ *for* $1 \leq i < n$*. A cycle* ***has a tail*** *if* $y_1 = Jy_s$*. A cycle* C *in* Γ *is* ***primitive*** *if it is reduced, has no tail, and* $C \neq D^f$ *for any* $f > 1$ *and any cycle* D*. A* ***prime*** *of* G *is an equivalence class of a primitive cycle under cyclic permutation:*

$$[C] = \{y_1 \cdots y_s, \quad y_2 \cdots y_s y_1, \quad \ldots, \quad y_s y_1 \cdots y_{s-1}\}.$$

Remark 4.2. *Let* Γ *be an isogeny graph and let* $y \in \operatorname{edge}\Gamma$ *satisfy* $Jy = y$*. Then* y *is a path beginning and ending at* $s(y) = t(y)$ *and is therefore a cycle. The cycle* y *has a tail, so it does not yield a prime of length* 1*.*

We now define the Ihara zeta function and edge zeta functions for an abstract isogeny graph.

Definition 4.3. *The* **Ihara zeta function** *of* Γ *is given by the Euler product*

$$\zeta_\Gamma(u) \coloneqq \prod_{[P]} (1 - u^{\nu(P)})^{-1}$$

where the product is taken over primes in Γ.

4.2. **Operators on vector spaces defined by abstract isogeny graphs.** In this section, we define operators that will be used in our proofs on certain vector spaces associated to an abstract isogeny graph. The presentation closely follows Bass' proof of the Ihara determinant formula [Bas92] and the presentation of that proof in [Ter11, Chapter 7]. Both proofs rely on having a regular, undirected graph. We remove these assumptions and make the necessary modifications to apply the results to our abstract isogeny graphs.

Let $\Gamma = (X, Y, s, t, J, L)$ be an isogeny graph. We assume Γ is finite. Let $\mathbb{C}^X$ and $\mathbb{C}^Y$ be the finite-dimensional vector spaces with bases given by $X = \operatorname{vert}\Gamma$ and $Y = \operatorname{edge}\Gamma$, respectively. Define the following operators via their action on the bases X and Y of $\mathbb{C}^X$ and $\mathbb{C}^Y$, respectively:

$$\begin{aligned} J\colon \mathbb{C}^Y &\to \mathbb{C}^Y \\ y &\mapsto J(y) \end{aligned} \qquad \begin{aligned} S\colon \mathbb{C}^Y &\to \mathbb{C}^X \\ y &\mapsto s(y) \end{aligned} \qquad \begin{aligned} T\colon \mathbb{C}^Y &\to \mathbb{C}^X \\ y &\mapsto t(y) \end{aligned}$$

$$\begin{aligned} W_1\colon \mathbb{C}^Y &\to \mathbb{C}^Y \\ y &\mapsto \sum_{\substack{s(y')=t(y) \\ y' \neq J(y)}} y' \end{aligned} \qquad \begin{aligned} S^*\colon \mathbb{C}^X &\to \mathbb{C}^Y \\ x &\mapsto \sum_{s(y)=x} y \end{aligned} \qquad \begin{aligned} L\colon \mathbb{C}^X &\to \mathbb{C}^X \\ x &\mapsto Lx. \end{aligned}$$

Also define

$$a_{xx'} \coloneqq \#\{e \in s^{-1}(x) : t(e) = x'\}$$

and let A be the adjacency operator of Γ, i.e. the operator

$$\begin{aligned} A\colon \mathbb{C}^X &\to \mathbb{C}^X \\ x &\mapsto \sum_{y\colon s(y)=x} t(y) = \sum_{x'} a_{xx'} x'. \end{aligned}$$

Finally, define $d(x) \coloneqq \#\{y : s(y) = x\}$ and define $D\colon \mathbb{C}^X \to \mathbb{C}^X$ via $D(x) = d(x)x$. Note that, following Bass and Serre, our degree $d(x)$ is the **out-degree** of a vertex x.

Proposition 4.4. *Let* $\Gamma = (X, Y, s, t, J, L)$ *be an isogeny graph. With the above notation, we have*

(a) $SJ = T$,
(b) $TJ = LS$,
(c) $TS^* = A$,
(d) $SS^* = D$, *and*
(e) $W_1 + J = S^*T$.

Proof. For any edge $y \in Y$ we have $SJy = s(Jy) = t(y) = Ty$, so SJ and T agree on the basis Y for $\mathbb{C}^Y$ and therefore are equal. Similarly, we have $TJy = t(Jy) = Ly$ for all $y \in Y$.

For a vertex x we have

$$TS^*x = T\left(\sum_{y\colon s(y)=x} y\right) = \sum_{x'} a_{xx'}x'$$

so TS^* and A agree on the basis X. Therefore they are equal as operators.

We also have

$$SS^*x = S\left(\sum_{y\colon s(y)=x} y\right) = d(x)x = Dx.$$

Now let $y \in Y$ and calculate

$$(W_1 + J)y = \left(\sum_{\substack{s(y')=t(y)\\ y'\neq Jy}} y'\right) + Jy = \sum_{y'\colon s(y')=t(y)} y' = S^*t(y) = S^*Ty.$$

□

Definition 4.5. *For $y, y' \in Y$, let $w_{yy'} \in \mathbb{C}$ satisfy $w_{yy'} = 0$ if $y' = Jy$ or $s(y') \neq t(y)$. Define the operator $W\colon \mathbb{C}^Y \to \mathbb{C}^Y$ by defining*

$$Wy = \sum_{y'} w_{yy'}y'.$$

Define the **norm** *of a cycle $C = y_1 \cdots y_s$ of length at least 2 to be*

$$N(C) = N_W(C) \coloneqq w_{y_1y_2} \cdots w_{y_{s-1}y_s}w_{y_sy_1}.$$

When $C = \{y\}$ is a loop, define $N(C) \coloneqq w_{yy}$. Then the **edge zeta function for** Γ *(with respect to W) is given by the Euler product*

$$\zeta_E(\Gamma, W) \coloneqq \prod_{[P]}(1 - N_W(P))^{-1}$$

where again the product is taken over primes of Γ.

Proposition 4.6. *If $W = W_1u$ with $u \in \mathbb{C}$ (i.e. each nonzero entry of W is defined to be u) then*

$$\zeta_E(\Gamma, W_1u) = \zeta_\Gamma(u).$$

Proof. For a prime $[P]$ with $P = y_1 \cdots y_s$ and $W = W_1u$ we have

$$N(P) = w_{y_1y_2} \cdots w_{y_{s-1}y_s}w_{y_sy_1} = u \cdots u = u^{\nu(P)}.$$

Thus

$$\zeta_E(\Gamma, W_1u) = \prod_{[P]}(1 - N(P))^{-1} = \prod_{[P]}(1 - u^{\nu(P)})^{-1} = \zeta_\Gamma(u).$$

□

Proposition 4.7. *The edge zeta function of Γ is related to the operator W_1, as follows:*

$$\zeta_E(\Gamma, W_1u) = \det(\mathrm{id}_{\mathbb{C}^Y} - W_1u)^{-1}.$$

Proof. The argument given by Bass in [Bas92, Theorem 3.3] works just as well for abstract isogeny graphs. Set $W = W_1 u$. One shows that

$$W^k y = \sum_{(yy_1 \dots y_k)} u^k y_k,$$

where the sum is over *reduced* paths from y to y_k, so

$$\log \zeta_E(\Gamma, W) = \sum_{\substack{C \text{ cycle} \\ \text{no backtracking or tail}}} \frac{u^{\nu(C)}}{\nu(C)} = \sum_{k \geq 1} \frac{\operatorname{Tr} W^k}{k}.$$

Next, compute

$$\operatorname{Tr} \log(\mathrm{id}_{\mathbb{C}^Y} - W)^{-1} = -\operatorname{Tr} \sum_{k \geq 1} \frac{-W^k}{k} = \operatorname{Tr} \sum_{k \geq 1} \frac{W^k}{k} = \sum_{k \geq 1} \frac{\operatorname{Tr} W^k}{k}.$$

Finally use the fact that $\operatorname{Tr} \log M = \log \det M$ for a matrix M to get

$$\log \det(\mathrm{id}_{\mathbb{C}^Y} - W)^{-1} = \operatorname{Tr} \log(\mathrm{id}_{\mathbb{C}^Y} - W)^{-1} = \sum_{C} \frac{N(C)}{\nu(C)} = \log \zeta_E(\Gamma, W).$$

□

We are almost ready to state the Ihara determinant formula for non-orientable graphs. We need some new notation and technical lemmas.

Lemma 4.8. *Let B be a finite, nomepty set and let $F \colon B \to B$ be a function. Then there exists a unique nonempty maximal subset Z of B such that $F\big|_Z$ is a permutation.*

Proof. If Z and Z' are two subsets of B such that $F\big|_Z$ and $F\big|_{Z'}$ are permutations, then $F\big|_{Z \cup Z'}$ is too. Thus there exists a unique maximal subset Z such that $F\big|_Z$ is a permutation if there exists any nonempty such subset. We prove such a subset exists by induction on $\#B$. If B is a singleton then F is already a permutation. Suppose the claim holds for $n > 1$ and let $\#B = n + 1$. If F is surjective, then it is bijective, since B is finite. So suppose $b \in B$ is not in the image of F and apply the inductive hypothesis to $B' = B - \{b\}$ and $F' = F\big|_{B'}$. □

Definition 4.9. *Let B be a finite, nonempty set and let $F \colon B \to B$ be a function. Let Z be the largest subset of B such that $F\big|_Z$ is a permutation. Define $F\big|_Z$ to be the* **permutation associated to** *F and define the* **cycle lengths associated to** *F to be $C_k(F)$, the number of cycles of length k in the cycle decomposition of $F\big|_Z$.*

Lemma 4.10. *Let B be a finite, nonempty set and let $F \colon B \to B$ be a function. Denote by F the operator on $V = \mathbb{C}^B$ determined by F. Let $s \in \mathbb{C}$. Then*

$$\det(\mathrm{id}_{\mathbb{C}^B} + sF) = (1+s)^{C_1(F)} \prod_{k>1} (1 - s^k)^{C_k(F)}.$$

Proof. Let $I := \mathrm{id}_{\mathbb{C}^B}$. We must compute $\det(I + sF)$. First, we claim that if b is not in the image of F then the determinant of $I + sF$ is equal to the determinant of $I + sF$ restricted to $\mathbb{C}^{B - \{b\}}$. Indeed, on $\mathbb{C}^B = \mathbb{C}^{\{b\}} \oplus \mathbb{C}^{B - \{b\}}$, $I + sF$ is block upper triangular with blocks given by the identity on $\mathbb{C}^{\{b\}}$ and $I + sF$ on $\mathbb{C}^{B - \{b\}}$. Thus we may restrict to the largest subset $Z \subseteq B$ such that every $b \in Z$ has a pre-image under F in Z. Then Z is also the largest subset of B such that F acts as a permutation σ_F on Z: the claim fails for any larger subset because there is an element without a preimage, and it holds on Z because Z is finite. The resulting permutation is unique, and if we order the elements of Z corresponding to the cycle decomposition of the permutation σ_J, we see we are left with computing the determinant of matrices of the form

$$\begin{pmatrix} 1 & 0 & 0 & \dots & 0 & s \\ s & 1 & 0 & \dots & 0 & 0 \\ 0 & s & 1 & \dots & 0 & 0 \\ 0 & 0 & s & \ddots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & 1 & 0 \\ 0 & 0 & 0 & \dots & s & 1 \end{pmatrix}.$$

This is the $k \times k$ matrix $I + sP_{(123\cdots k)}$ where P_τ denotes the permutation matrix for the permutation τ. Considering the Leibniz formula for the determinant, we see the only nonzero terms correspond to the identity permutation and the permutation $(123\dots k)$, giving us a factor of $1 - s^k$. We also get a factor of $(1+s)$ for each fixed point of F, i.e. each cycle of length 1. The resulting determinant is

$$\det(I + sF) = (1+s)^{C_1(F)} \prod_{k>1} (1 - s^k)^{C_k(F)}$$

as desired. □

Theorem 4.11 (The Ihara determinant formula for regular abstract isogeny graphs)**.** *Let* Γ *be a finite abstract isogeny graph such that* D *and* L *commute. Let* $Q = D - \mathrm{id}_{\mathbb{C}^X}$. *Then*

$$\zeta_\Gamma(u) = \frac{(1-u^2)^{C_1(L)}(1+u)^{-C_1(J)} \prod_{k>1}(1-(-1)^k u^{2k})^{C_k(L)}(1-u^k)^{-C_k(J)}}{\det(\mathrm{id}_{\mathbb{C}^X} - Au + u^2 QL)}.$$

Proof. Let $n = \#X$. A calculation shows

$$\begin{pmatrix} \mathrm{id}_{\mathbb{C}^X} - u^2 L & 0 \\ S^* u & \mathrm{id}_{\mathbb{C}^Y} - uW_1 \end{pmatrix} \begin{pmatrix} \mathrm{id}_{\mathbb{C}^X} & T \\ 0 & \mathrm{id}_{\mathbb{C}^Y} \end{pmatrix} = \begin{pmatrix} \mathrm{id}_{\mathbb{C}^X} - u^2 L & T - u^2 LT \\ uS^* & uS^*T + \mathrm{id}_{\mathbb{C}^Y} - uW_1 \end{pmatrix} \tag{2}$$

and that

$$\begin{pmatrix} \mathrm{id}_{\mathbb{C}^X} & T - uTJ \\ 0 & \mathrm{id}_{\mathbb{C}^Y} \end{pmatrix} \begin{pmatrix} \mathrm{id}_{\mathbb{C}^X} - uA + u^2 QL & 0 \\ uS^* & \mathrm{id}_{\mathbb{C}^Y} + uJ \end{pmatrix}$$

is equal to

$$\begin{pmatrix} 1 - uA + u^2 QL + uTS^* - u^2 TJS^* & T - u^2 TJ^2 \\ uS^* & 1 + uJ \end{pmatrix}. \tag{3}$$

We claim that the two matrix products in Equations 2 and 3 agree. To prove this, we make several uses of Proposition 4.4; note that our assumption that Γ is regular implies that D is scalar and hence commutes with any operator on $\mathbb{C}^X$, and in particular, with L. The upper-left entries in Equations 2 and 3 are equal since

$$\begin{aligned} \mathrm{id}_{\mathbb{C}^X} - uA + u^2 QL + uTS^* - u^2 TJS^* &= \mathrm{id}_{\mathbb{C}^X} + u^2 QL - u^2 TJS^* && \text{Proposition 4.4(c)} \\ &= \mathrm{id}_{\mathbb{C}^X} + u^2 (D - \mathrm{id}_{\mathbb{C}^X}) L - u^2 LSS^* && \text{Proposition 4.4(b)} \\ &= \mathrm{id}_{\mathbb{C}^X} - u^2 L + u^2 DL - u^2 LD && \text{Proposition 4.4(d)} \\ &= \mathrm{id}_{\mathbb{C}^X} - u^2 L && LD = DL. \end{aligned}$$

The upper-right entries are equal using Proposition 4.4 parts (a) and (b):

$$T - u^2TJ^2 = T - u^2LSJ = T - u^2LT.$$

We now show the bottom-right entries are equal; this follows from Proposition 4.4(e):

$$uS^*T + \mathrm{id}_{\mathbb{C}^Y} - uW_1 = u(J + W_1) + \mathrm{id}_{\mathbb{C}^Y} - uW_1 = + \mathrm{id}_{\mathbb{C}^Y} + uJ.$$

Thus

$$\det\bigl(\mathrm{id}_{\mathbb{C}^X} - u^2L\bigr)\det(\mathrm{id}_{\mathbb{C}^Y} - uW_1) = \det\bigl(\mathrm{id}_{\mathbb{C}^X} - uA + u^2QL\bigr)\det(\mathrm{id}_{\mathbb{C}^Y} + uJ).$$

The claimed formula for $\zeta_\Gamma(u)$ now follows by applying Lemma 4.10 to $\det(1 - u^2L)$ and $\det(1 + uJ)$ and using Propositions 4.6 and 4.7.

□

5. The orientable graphs associated to an abstract isogeny graph

Given a non-orientable graph Γ with vertex set X and edge set Y, we define two orientable graphs Γ^{+1} and Γ^{-1} as follows. Let $\sim_X$ be the smallest equivalence relation on X so that $x \sim Lx$ for all $x \in X$. Let $\sim_Y$ be the smallest equivalence relation on Y such that $y \sim_Y J^2y$ for all $y \in Y$. Let $X' = X/{\sim_X}$ and let $Y' = Y/{\sim_Y}$ denote the equivalence classes of $\sim_X$ and $\sim_Y$. Abusing notation, we define the source and target functions $s, t : Y' \to X'$ by $s([y]) = [s(y)]$ and $t([y]) = [t(y)]$; these maps are well-defined.

The map $J\colon Y \to Y$ induces a well-defined map

$$\begin{aligned} Y' &\to Y' \\ [y] &\mapsto [Jy] \end{aligned}$$

that we will also denote by J. In particular, we have

$$s(J[y]_{\sim_Y}) = [s(Jy)]_{\sim_X} = [t(y)]_{\sim_X} = t([y]_{\sim_Y})$$

and

$$t(J[y]_{\sim_Y}) = t([Jy]_{\sim_Y}) = [t(Jy)]_{\sim_X} = [L(t(y))]_{\sim_X} = [t(y)]_{\sim_X} = t([y]_{\sim_Y}).$$

From the definition of $\sim_Y$, the map J is an involution on $Y/{\sim_Y}$:

$$J^2[y] = [J^2y] = [y].$$

The vertex set of $\Gamma^{\pm 1}$ is $X/{\sim_X}$. We now define edge sets $Y^{+1} := Y' - \{[y] : J[y] = [y]\}$ and $Y^{-1} := Y' \sqcup \{[y] : J[y] = [y]\}$. Let J_{+1} denote the restriction of J to Y^{+1}. To define an involution on Y^{-1}, we define J_1 so -that $J_{-1}[y] = J[y]$ if $J[y] \neq [y]$ and J_{-1} swaps $[y] \in \{J[y] = [y]\}$ with its copy in Y^{-1}. Finally define Γ^{+1} to be the graph with vertex set X and edge set Y^{+1} and fixed-point free involution J_{+1}, and similarly Γ^{-1}. We call Γ^{+1} and Γ^{-1} the **orientable graphs associated to** Γ.

Remark 5.1. *Thereom 4.11 specializes to Ihara's determinant formula when Γ is orientable and has degree $\ell+1$: if Γ is orientable then J is a fixed-point free involution: we have $r = 0$, $C_k = 0$ for $k > 2$, and $C_2 = \frac{1}{2}\#\,\mathrm{edge}\,\Gamma$, so*

$$\zeta_\Gamma(u) = \frac{(1-u^2)^{\chi(\Gamma)}}{\det(\mathrm{id}_{\mathbb{C}^X} - uA + u^2Q)}.$$

More generally, suppose that J is an involution with r fixed points. Then every cycle in σ_J has length 1 or 2 and $t(Jy) = s(y)$ for all edges y, so L is the identity. This is the case *for the isogeny graph $G(p, B_0(N), \ell)$ for $p \equiv 1 \pmod{12}$. Then the only fixed points of J on $Y/{\sim_Y}$ come from fixed points of J on Y. We have*

$$\zeta_\Gamma(u) = \frac{(1+u)^r(1-u^2)^{\chi(\Gamma^{+1})}}{\det(\mathrm{id}_{\mathbb{C}^X} - uA + u^2Q)} = \frac{(1+u)^{\chi(\Gamma^{-1})}(1-u)^{\chi(\Gamma^{+1})}}{\det(\mathrm{id}_{\mathbb{C}^X} - uA + u^2Q)},$$

where $\Gamma^{\pm 1}$ are the orientable graphs obtained from Γ.

5.1. **The realization of an isogeny graph.** We now extend to abstract isogeny graphs the construction of Serre [Ser03, §2.1, pg. 14] of a CW complex associated to a graph Γ. Let $\Gamma = (X, Y, J)$ be an isogeny graph with vertex set X and edge set Y. Let $\operatorname{real}\Gamma$ be the quotient of $X \sqcup (Y \times [0,1])$ by the equivalence relation generated by the relations, for all $y \in Y$ and $r \in [0,1]$,

- $(y, r) \sim (Jy, 1-r)$,
- $(y, 0) \sim s(y)$, and
- $(y, 1) \sim t(y)$

and where the topology on $\operatorname{real}\Gamma$ is the quotient topology (we give the usual topology on $[0,1]$ and the discrete topologies to X and Y).

Observe that

$$s(y) \sim (y,0) \sim (Jy,1) \sim t(Jy),$$

so in $\operatorname{real}\Gamma$, two vertices $x, x' \in X$ are identified if there is an edge y with $x = s(y)$ and $t(Jy) = x'$, just as in the construction of $\Gamma^{\pm 1}$. Similarly we have

$$(y, r) \sim (Jy, 1-r) \sim (J^2y, r)$$

so edges in the same equivalence class under $\sim_Y$ will have the same image in $\operatorname{real}\Gamma$.

The realization $\operatorname{real}\Gamma$ can be given the structure of a CW-complex of dimension ≤ 1. The 0-cells are the image in $\operatorname{real}\Gamma$ of the vertices X, together with a 0-cell at the class of $(y, 1/2)$ for each $y \in Y$ with $J[y] = [y]$. The 1-cells correspond to images of subsets of Y of the form $\{y, Jy\}$.

Proposition 5.2. *The realization $\operatorname{real}\Gamma^{+1}$ of Γ^{+1} is a deformation retract of $\operatorname{real}\Gamma$.*

Proof. First, we define a map $f \colon \operatorname{real}\Gamma^{+1} \to \operatorname{real}\Gamma$. Given $[([y], r)] \in \operatorname{real}\Gamma^{+1}$, define $f([([y], r)]) = [(y, r)]$. This map is well-defined: if $y' = J^2y$ then

$$(y, r) \sim (Jy, 1-r) \sim (J^2y, r).$$

This implies f does not depend on the choice of representative $y \in [y]$. It is an injection, since if

$$[(y, r)] = [(y', r')]$$

then either $r = r'$ and $y \sim_Y y'$ so $[([y], r)] = [([y'], r')]$ or $r' = 1 - r$ and $Jy \sim_Y y'$. From now on, identify $\operatorname{real}\Gamma^{+1}$ with its image in $\operatorname{real}\Gamma$, i.e. the elements $[(y, r)]$ with $J[y] \neq [y]$. Consider a 1-cell corresponding to $y \in Y$ with $J[y] = [y]$. We claim that this 1-cell is homeomorphic to a segment $[0,1]$, where the boundary point of the 1-cell corresponding to 0 is in $\operatorname{real}\Gamma^{+1}$ and the boundary point corresponding to 1 is in the boundary of $\operatorname{real}\Gamma$. The subspace is $\{[(y, r)] : r \in [0,1]\}$. Define the map $(y, r) \mapsto -|2r-1| + 1$; this map is constant on equivalence classes, since

$$1 - |2(1-r) - 1| = 1 - |1 - 2r| = 1 - |2r - 1|,$$

and is a bijection, since

$$1 - |2r - 1| = 1 - |2r' - 1| \implies 2r - 1 = \pm(2r' - 1) \implies r = r' \text{ or } r = 1 - r'.$$

The closure of $\operatorname{real}\Gamma - \operatorname{real}\Gamma^{+1}$ consists of 1-cells corresponding to $y \in Y$ with $[Jy] = [y]$. Each such 1-cell y can be contracted to $s(y) \in \operatorname{real}\Gamma^{+1}$, so $\operatorname{real}\Gamma^{+1}$ is a deformation retract of $\operatorname{real}\Gamma$. More precisely, we have a homotopy

$$\begin{aligned} H\colon\ & \operatorname{real}\Gamma \times [0,1] \to \operatorname{real}\Gamma^{+1} \\ & ([(y,r)],t) \mapsto \begin{cases} [(y, t(1-|2r-1|))] & : J[y] = [y] \\ [(y,r)] & : J[y] \neq [y]. \end{cases} \end{aligned}$$

□

Let $\Gamma = (X, Y, J)$ be a graph, possibly non-orientable. We now assume Γ is **finite**, i.e. $\operatorname{vert}\Gamma$ and $\operatorname{edge}\Gamma$ are finite sets. For a finite, connected, orientable graph Γ, define

$$B_1(\Gamma) := \frac{1}{2}(\#\operatorname{edge}\Gamma) - \#\operatorname{vert}\Gamma + 1.$$

Corollary 5.3. *The realization* $\operatorname{real}\Gamma$ *of a finite (possibly non-orientable) graph* Γ *has the homotopy type of a* bouquet of circles*, where the number of circles is* $B_1(\Gamma^{+1})$*.*

Proof. This follows from [Ser03, Corollary 1] and the previous proposition: $\operatorname{real}\Gamma$ and $\operatorname{real}\Gamma^{+1}$ are homotopy equivalent, and $\operatorname{real}\Gamma^{+1}$, being the realization of an orientable graph, has the homotopy type of a bouquet of circles where the number of circles is $B_1(\Gamma^{+1})$.

□

Remark 5.4. *We can combine the arguments in* [Ser03, Corollary 1] *and in the proof of Proposition 5.2 above to see that* $\operatorname{real}\Gamma$ *has the homotopy type of a bouquet of* $B_1(\Gamma^{+1})$ *circles. Let* T *be any spanning tree in* Γ^{+1}*. Then its image in* $\operatorname{real}\Gamma^{+1} \subseteq \operatorname{real}\Gamma$ *is contractible. After we contract the subspace corresponding to* T *in* $\operatorname{real}\Gamma$ *to a point, we are left with a "bouquet of circles with thorns", that is, a wedge sum of circles and line segments. The circles correspond to edges in* $\operatorname{edge}\Gamma^{+1} - \operatorname{edge}T$*, i.e.* $\{[y], J[y]\} \subseteq Y^{+1} - T$ *and the segments correspond to* $[y] \in Y/{\sim_Y} - T$ *such that* $J[y] = [y]$*. Thus there are* $s = \#\{[y] : [Jy] = [y]\}$ *thorns and*

$$\frac{1}{2}(\#\operatorname{edge}\Gamma^{+1} - \#\operatorname{edge}T)$$

circles. By [Ser03, Proposition 12]*, we have* $\#\operatorname{edge}T = 2(\#\operatorname{vert}T - 1)$*, and* $\#\operatorname{vert}T = \#\operatorname{vert}\Gamma^{+1}$*. We may further contract each "thorn" to the point where the circles and thorns meet, so we're left with a bouquet of* $B_1(\Gamma^{+1})$ *circles, as in the statement of the proposition.*

6. Examples of abstract isogeny graphs

We now consider certain concrete examples of the theory given above, beginning with the classic supersingular isogeny graphs. We show that these graphs, as well as isogeny graphs of supersingular elliptic curves with level structure, and the $(\ell, \dots, \ell)$-isogeny graph of superspecial principally polarized abelian varieties are examples of abstract isogeny graphs.

6.1. **The supersingular ℓ-isogeny graph in characteristic p.** Let p and ℓ be distinct primes. Let $X = \{E_1, \dots, E_n\}$ denote a complete set of representatives for the isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$. Let

$$L_{ij} = \{\alpha \colon E_i \to E_j : \deg \alpha = \ell\}$$

denote the set of isogenies of degree ℓ from E_i to E_j. Then $\operatorname{Aut}(E_j)$ acts on the left on L_{ij} via $u \cdot \alpha := u \circ \alpha$ for $\alpha \in L_{ij}, u \in \operatorname{Aut}(E_j)$. We define $G(p, \ell)$, the supersingular ℓ-isogeny graph in characteristic p, to be the graph whose vertex set is X and edge set Y are the the orbits $\{\operatorname{Aut}(E_j)\backslash L_{ij} : 1 \leq i, j \leq n\}$. The *source* and *target* functions of $G(p, \ell)$ are the functions $s, t \colon X \to Y$ that map a directed edge to its source and target vertices:

$$s(\alpha \colon E_i \to E_j) = E_i, \quad t(\alpha \colon E_i \to E_j) = E_j.$$

Define $L \colon X \to X$ to be the identity function. We now define $J \colon Y \to Y$ on the edges of $G(p, \ell)$. We will show that this particular construction agrees with a natural construction of *orientable* graphs associated to $G(p, \ell)$.

We now define $J \colon Y \to Y$. For each i, j, $\operatorname{Aut}(E_i)$ acts on the right on L_{ij} via precomposition, and this action is compatible with the left action of $\operatorname{Aut}(E_j)$. Moreover, there is a well-defined involution on $\bigcup_{i,j} \operatorname{Aut}(E_j)\backslash L_{ij}/\operatorname{Aut}(E_i)$ via the dual map: define $\widehat{[\alpha]} := [\widehat{\alpha}]$. For each i, j and each orbit $O \in \operatorname{Aut}(E_j)\backslash L_{ij}/\operatorname{Aut}(E_i)$, choose $\phi_O \in O$. For each edge $y = \operatorname{Aut}(E_j)\phi_O u$ with $u \in \operatorname{Aut}(E_i)$, define $Jy = \operatorname{Aut}(E_i)\phi_{\widehat{O}}$.

Proposition 6.1. *$G(p, \ell) := (X, Y, s, t, L, J)$ defined as above is an $\ell + 1$-regular abstract isogeny graph.*

Proof. Let $y = \operatorname{Aut}(E_j)\alpha$ be an edge and let $E_i = s(y)$. Let $\phi_O \colon E_i \to E_j$ be the chosen representative of $O = \operatorname{Aut}(E_j)\alpha \operatorname{Aut}(E_i)$. Then $\operatorname{Aut}(E_j)\alpha = \operatorname{Aut}(E_j)\phi_O u$ for some $u \in \operatorname{Aut}(E_i)$, and

$$s(Jy) = s(J(\operatorname{Aut}(E_j)\alpha)) = s(J(\operatorname{Aut}(E_j)\phi_O u)) = s(\operatorname{Aut}(E_i)\widehat{\phi_O}) = E_j = t(y),$$

and

$$t(Jy) = t(\operatorname{Aut}(E_j)\phi_{\widehat{O}}) = E_i = L(s(y)).$$

Thus $G(p, \ell)$ is an abstract isogeny graph. It is $\ell + 1$-regular since for each i, there are $\ell + 1$ cyclic subgroups of order ℓ in $E_i[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^2$, thus $\ell + 1$ distinct ℓ-isogenies up to post-composition by automorphisms. □

We give an alternative construction of the orientable graphs $G(p, \ell)^{+1}$ and $G(p, \ell)^{-1}$ that justifies the choice that defines J. The right and left actions of $\operatorname{Aut}(E_i)$ and $\operatorname{Aut}(E_j)$ are compatible, so the action of $\operatorname{Aut}(E_i)$ on L_{ij} induces an action of $\operatorname{Aut}(E_i)$ on the orbits under the action of $\operatorname{Aut}(E_j)$ on L_{ij}, i.e. the edges from E_i to E_j. Let $y \operatorname{Aut}(E_i)$ denote the orbit of the edge y. If we write $y = \operatorname{Aut}(E_j)\alpha$, then $y \operatorname{Aut}(E_i)$ is the orbit of α under the action of $\operatorname{Aut}(E_i) \times \operatorname{Aut}(E_j)$, i.e. $\operatorname{Aut}(E_j)\alpha \operatorname{Aut}(E_i)$.

Proposition 6.2. *Let $G(p, \ell) = (X, Y, s, t, L, J)$ as above. The equivalence relation on Y generated by $y \sim_Y J^2 y$ is the relation*

$$y \sim y' \iff y \operatorname{Aut}(E_i) = y' \operatorname{Aut}(E_i).$$

Proof. We show that $\sim$ is a relation contained in $\sim_Y$ that satisfies $y \sim J^2 y$; recall $\sim_Y$ is the smallest such relation. First we show that $y \sim J^2 y$. Let $O = y \operatorname{Aut}(E_i)$ and let ϕ_O be the representative of O chosen in the definition of J. Then there is some automorphism u of E_i such that $y = \operatorname{Aut}(E_j)\phi_O u$ and $Jy = \operatorname{Aut}(E_i)\phi_{\widehat{O}}$ so

$$J^2 y = J(\operatorname{Aut}(E_i)\phi_{\widehat{O}}) = \operatorname{Aut}(E_j)\phi_O,$$

so

$$(J^2 y)\operatorname{Aut}(E_i) = \operatorname{Aut}(E_j)\phi_O \operatorname{Aut}(E_i) = O = y\operatorname{Aut}(E_i).$$

Thus the relation $\sim$ implies $\sim_Y$. On the other hand, suppose $y \sim_Y y'$, so $J^{2m}y = J^{2n}y'$ for some $m, n \geq 0$. Since L is the identity on X, we have $s(J^2 y) = s(y)$ for all y, so $y \sim_Y y'$ implies $s(y) = s(y') = E_i$ for some i. Let $O = y\operatorname{Aut}(E_i)$ and $O' = y'\operatorname{Aut}(E_i)$ be the orbits of y and y' under the right action of $\operatorname{Aut}(E_i)$. Then

$$J^{2m}y = J^{2m-1}(\operatorname{Aut}(E_j)\phi_{\widehat{O}}) = J^{2(m-1)}(\operatorname{Aut}(E_j)\phi_O) = \cdots = \operatorname{Aut}(E_j)\phi_O,$$

and similarly $J^{2n}y' = \operatorname{Aut}(E_j)\phi_{O'}$. Thus $\operatorname{Aut}(E_j)\phi_O = \operatorname{Aut}(E_j)\phi_{O'}$, so

$$y\operatorname{Aut}(E_i) = O = \operatorname{Aut}(E_j)\phi_O\operatorname{Aut}(E_i) = \operatorname{Aut}(E_j)\phi_{O'}\operatorname{Aut}(E_i) = O' = y'\operatorname{Aut}(E_i).$$

Thus $\sim_Y$ implies $\sim$, so the two relations are equal. □

We see that $Y/{\sim_Y} = \operatorname{Aut}(E_j)\backslash L_{ij}/\operatorname{Aut}(E_i)$, so $G(p,\ell)^{+1}$ has vertex set X and edge set

$$Y^{+1} = \bigcup_{i,j}\{[\alpha] \in \operatorname{Aut}(E_j)\backslash L_{ij}/\operatorname{Aut}(E_i) : \widehat{[\alpha]} \neq [\alpha]\}.$$

The edge set Y^{-1} of $G(p,\ell)^{-1}$ is

$$\left(\bigcup_{i,j}\operatorname{Aut}(E_j)\backslash L_{ij}/\operatorname{Aut}(E_i)\right)\bigsqcup\left\{[\alpha] \in \operatorname{Aut}(E_j)\backslash L_{ij}/\operatorname{Aut}(E_i) : \widehat{[\alpha]} = [\alpha]\right\}.$$

We have chosen J in a way that yields natural constructions of the orientable graphs associated to $G(p,\ell)$. We now show how to compute $\chi(G(p,\ell)^{\pm 1})$ for this choice of J. To compute $\chi(G(p,\ell)^{\pm 1})$, we need to compute the number of orbits of the involution acting on $\bigcup_{i,j}\operatorname{Aut}(E_j)\backslash L_{i,j}/\operatorname{Aut}(E_i)$. Letting $\mathcal{L} = \bigcup_{i,j}\operatorname{Aut}(E_j)\backslash L_{ij}\operatorname{Aut}(E_i)$, we first compute $\#\mathcal{L}$ in Lemma 6.3 below. Each orbit of the dual map on $\mathcal{L}$ has size either 1 or 2, so to count the number of orbits, we compute the number of fixed points in Lemma **??**.

Lemma 6.3. *Suppose $p > 3$ and for an integer j, let $\epsilon_p(j) = 1$ if an elliptic curve with j-invariant j is supersingular modulo p and 0 otherwise. If ℓ is odd then*

$$\begin{aligned}\#\bigcup_{i,j}\operatorname{Aut}(E_i)\backslash L_{ij}/\operatorname{Aut}(E_j) = (\ell+1)\left\lfloor\frac{p-1}{12}\right\rfloor & \\ + \epsilon_p(0)\left(\frac{\ell+3-2\left(\frac{-3}{\ell}\right)}{3}\right) & \\ + \epsilon_p(1728)\left(\frac{\ell+2-\left(\frac{-1}{\ell}\right)}{2}\right). &\end{aligned}$$

If $\ell = 2$ then

$$\#\bigcup_{i,j}\operatorname{Aut}(E_i)\backslash L_{ij}/\operatorname{Aut}(E_j) = 3\left\lfloor\frac{p-1}{12}\right\rfloor + \epsilon_p(0) + 2\epsilon_p(1728).$$

Proof. The group $\operatorname{Aut}(E_i)$ acts on the set of cyclic subgroups of order ℓ in $E_i[\ell]$, and for a fixed j, this restricts to an action on those subgroups C such that $E_i/C \simeq E_j$. To count $\bigcup_{i,j} \operatorname{Aut}(E_j)\backslash L_{ij}/\operatorname{Aut}(E_i)$, we count $\bigcup_j \operatorname{Aut}(E_j)\backslash L_{ij}/\operatorname{Aut}(E_i)$ for fixed i, and to count this, we count the number of orbits of the action of $\operatorname{Aut}(E_i)$ on cyclic subgroups of order ℓ. Suppose $\operatorname{Aut}(E_i) = \{\pm 1\}$. Then $\operatorname{Aut}(E_j)\backslash L_{ij}/\operatorname{Aut}(E_i)$ is in bijection with the set of cyclic subgroups C of order ℓ in $E_i[\ell]$ such that $E_i/C \simeq E_j$. There are $\lfloor \frac{p-1}{12} \rfloor$ isomorphism classes of supersingular elliptic curves with automorphism group equal to $\{[\pm 1]\}$. These account for the term $(\ell+1)\lfloor \frac{p-1}{12} \rfloor$.

We now count $\bigcup_j \operatorname{Aut}(E_j)\backslash L_{ij}/\operatorname{Aut}(E_i)$ when $\operatorname{Aut}(E_i) \supsetneq \{\pm 1\}$, that is, when $j(E_i)$ is 0 or 1728. First assume $E = E_i$ has j-invariant 0. Let ω denote a primitive third root of unity and let $[\omega]$ denote the corresponding automorphism of E (mapping $(x,y) \mapsto (\omega x, y)$). Then $\operatorname{Aut}(E)$ is generated by $[-1]$ and $[\omega]$ and is cyclic of order 6. There are $\ell+1$ cyclic subgroups of order ℓ in $E[\ell]$ on which $\operatorname{Aut}(E)$ acts. Each orbit will either have order 3 or consist of a single fixed point of the action. We count the number of fixed points of this action. The characteristic polynomial of $[\omega]$ is x^2+x+1, so the characteristic polynomial of the $\mathbb{F}_\ell$-linear map $[\omega]_{|E[\ell]}$ given by restricting $[\omega]$ to $E[\ell]$ is $x^2+x+1 \in \mathbb{F}_\ell[x]$. The number of cyclic subgroups of order ℓ fixed by $\operatorname{Aut}(E)$ is the number of one-dimensional eigenspaces of $[\omega]_{|E[\ell]}$, which is 0, 1, 2, or $\ell+1$ according to whether x^2+x+1 has no roots modulo ℓ, x^2+x+1 has one root modulo ℓ and is the minimal polynomial of $[\omega]_{|E[\ell]}$, two distinct roots modulo ℓ, or x^2+x+1 has one root modulo ℓ and is not the minimal polynomial of $[\omega]|_{E[\ell]}$. Suppose first $\ell > 3$. Then there are exactly two fixed ℓ-isogenies if and only if x^2+x+1 has two distinct roots modulo ℓ if and only if ℓ splits in $\mathbb{Z}[\omega]$ if and only if $\left(\frac{-3}{\ell}\right) = 1$. There are no fixed ℓ-isogenies if and only if x^2+x+1 has no roots modulo ℓ if and only if ℓ is inert in $\mathbb{Z}[\omega]$ if and only if $\left(\frac{-3}{\ell}\right) = -1$. In both cases we see there are $1 - \left(\frac{-3}{\ell}\right)$ many fixed points of the action. Now consider the case $\ell = 3$ (so x^2+x+1 has 1 as a double root modulo 3, and 3 is ramified in $\mathbb{Z}[\omega]$). Then $[\omega]$ either fixes exactly one edge or restricts to the identity on $E[3]$. The latter is impossible, since otherwise $E[3] \subseteq \ker(1-[\omega])$ implying $1-[\omega]$ would factor through $[3]$ and thus have degree at least 9, but $\deg(1-[\omega]) = 3$. We see that the formula $1 - \left(\frac{-3}{\ell}\right)$ for the number of ℓ-isogenies fixed by $\operatorname{Aut}(E)$ holds for all odd ℓ. Finally, for $\ell = 2$, we observe that if E is given by $y^2 = x^3 + B$ then the affine points in $E[2]$ are $(\omega^i B^{1/3}, 0)$ for $i = 0,1,2$, and $[\omega]$ cyclicly permutes these three points. Thus the three subgroups of order 2 in $E[2]$ make up a single $\operatorname{Aut}(E)$-orbit.

Now consider E with $j(E) = 1728$. Then $\operatorname{Aut}(E)$ is cyclic of order 4 generated by $[i] : (x,y) \mapsto (-x, iy)$ whose characteristic polynomial is x^2+1. For odd ℓ, we have $(1 - \left(\frac{-1}{\ell}\right))$ fixed edges, again by considering the action of $[i]$ on $E[\ell]$. For $\ell = 2$ the 2-torsion of $E : y^2 = x^3 + Ax$ is $(0,0)$ and $(\pm i\sqrt{A}, 0)$. The endomorphism $[i]$ fixes $(0,0)$ and swaps $(\pm i\sqrt{A}, 0)$. Thus there is exactly one fixed edge in the 2-isogeny graph at E. □

Lemma 6.4. *Suppose $p > 3$ and $\ell \neq p$ are primes. The the number of orbits that satisfy $\operatorname{Aut}(E_i)\widehat{\alpha}\operatorname{Aut}(E_i) = \operatorname{Aut}(E_i)\alpha\operatorname{Aut}(E_i)$ is*

$$r = \begin{cases} (h(-4\ell)+h(-\ell))\frac{(1-\left(\frac{-\ell}{p}\right))}{2} & \text{if } \ell \equiv 3 \pmod 4 \\ h(-4\ell)\frac{(1-\left(\frac{-\ell}{p}\right))}{2} & \text{otherwise} \end{cases} + \begin{cases} 1 & \text{if } \ell = 2 \text{ and } p \equiv 3 \pmod 4 \\ 0 & \text{otherwise.} \end{cases}$$

Proof. For a fixed supersingular elliptic curve E, orbits $[\alpha] = \operatorname{Aut}(E)\alpha\operatorname{Aut}(E)$ that satisfy $[\widehat{\alpha}] = [\alpha]$ are in bijection with $\operatorname{Aut}(E)$-conjugacy classes of conjugate pairs of optimal embeddings of certain imaginary quadratic orders into $\operatorname{End}(E)$, in particular $\mathbb{Z}[\sqrt{-\ell}]$,

$\mathbb{Z}[(1+\sqrt{-\ell})/2]$, and, if $\ell = 2$ and $p \equiv 3 \pmod 4$, $\mathbb{Z}[i]$. This correspondence arises from the function

$$\left(f, \widehat{f}\colon \mathbb{Z}[\sqrt{-\ell}] \hookrightarrow \operatorname{End}(E)\right) \mapsto \operatorname{Aut}(E) f\left(\sqrt{-\ell}\right) \operatorname{Aut}(E).$$

and, if $\ell = 2$ and $p \equiv 3 \pmod 4$, the embedding $g, \widehat{g}\colon \mathbb{Z}[i] \hookrightarrow \operatorname{End}(E)$ maps to $\operatorname{Aut}(E)(1 + g(i))\operatorname{Aut}(E)$. This map is well-defined on $\operatorname{Aut}(E)$-conjugacy classes of pairs of conjugate embeddings.

Suppose $[\widehat{\alpha}] = [\alpha]$. Then $\widehat{\alpha} = u\alpha v$ for $u, v \in \operatorname{Aut}(E)$ and

$$\widehat{v\alpha} = \widehat{\alpha} v^{-1} = u\alpha = uv^{-1}v\alpha,$$

we may assume $\widehat{\alpha} = u\alpha$ for some automorphism $u \in \operatorname{Aut}(E)$. Since u is an automorphism we have $u^{-1} = \widehat{u}$, so u and α commute:

$$\widehat{\alpha} = u\alpha \implies \alpha = \widehat{\alpha}u^{-1} = u\alpha u^{-1}.$$

Thus either $u = -1$ or $u \notin \mathbb{Z}$ and $\alpha \in \mathbb{Z}[u]$. If $u = [-1]$, then α satisfies $x^2 + \ell$ and thus is the image of $\sqrt{-\ell}$ under an embedding $f\colon \mathbb{Z}[\sqrt{-\ell}] \hookrightarrow \operatorname{End}(E)$.

If $u \neq [-1]$ then $j(E)$ is either 1728 or 0 and $\alpha \in \mathbb{Z}[u]$. Suppose $j(E) = 1728$. Then $\widehat{u} = -u$ since $u^4 = 1$ but $u \neq \pm 1$. Write $\alpha = a + bu$. Then $\widehat{\alpha} = u\alpha$ implies $a - bu = -b + au$ so $a = -b$. Thus $2a^2 = \ell$, so $a = 1$, $\ell = 2$, and $\alpha = \pm(1-u)$. Thus $\operatorname{Aut}(E)\alpha\operatorname{Aut}(E) = \{\pm(1 \pm g(i))\}$ where $g\colon \mathbb{Z}[i] \hookrightarrow \operatorname{End}(E)$ maps i to u. In particular, $\operatorname{Aut}(E)\alpha\operatorname{Aut}(E)$ contains elements corresponding to the unique pair of conjugate embeddings of $\mathbb{Z}[i]$ in $\operatorname{End}(E)$ and no elements corresponding to an embedding of $\mathbb{Z}[\sqrt{-\ell}]$. The case where u is a primitive third or sixth root of one can be checked similarly to the previous case, and there are no self-dual endomorphisms other than those represented by $\sqrt{-\ell}$.

Thus, we see that the number of self-dual loops is equal to the the number of conjugate-pairs of embeddings of $\sqrt{-\ell}$ into a set of representatives for the class set of $B_{p,\infty}$, plus one if $\ell = 2$ and $p \equiv 3 \pmod 4$. Using [Voi21], Theorems 30.4.7, 30.5.3, and 30.7.3 to count the embeddings of $\sqrt{-\ell}$ gives the claimed formula.

□

Corollary 6.5. *Let $p > 3$ be a prime and let $\ell \neq p$ be prime. Let r be as in Lemma 6.4. Let $G(p,\ell)^{+1}$ and $G(p,\ell)^{-1}$ be the orientable graphs associated to the abstract isogeny graph $G(p,\ell)$. If $\ell > 2$, then*

$$\chi(G(p,\ell)^{+1}) = \frac{-\ell}{2}\left\lfloor \frac{p-1}{12} \right\rfloor - \epsilon_p(0)\left(\frac{\ell - 3 + 2\left(\frac{-3}{\ell}\right)}{6}\right) - \epsilon_p(1728)\left(\frac{\ell - 2 + \left(\frac{-1}{\ell}\right)}{4}\right) - r/2,$$

$$\chi(G(p,\ell)^{-1}) = \frac{-\ell}{2}\left\lfloor \frac{p-1}{12} \right\rfloor - \epsilon_p(0)\left(\frac{\ell - 3 + 2\left(\frac{-3}{\ell}\right)}{6}\right) - \epsilon_p(1728)\left(\frac{\ell - 2 + \left(\frac{-1}{\ell}\right)}{4}\right) + r/2.$$

For $\ell = 2$ we have

$$\chi(G(p,2)^{+1}) = -\frac{1}{2}\left\lfloor \frac{p-1}{12} \right\rfloor - \frac{\epsilon_p(0)}{2} - r/2$$

and

$$\chi(G(p,2)^{-1}) = -\frac{1}{2}\left\lfloor \frac{p-1}{12} \right\rfloor - \frac{\epsilon_p(0)}{2} + r/2.$$

Proof. Let $X = \operatorname{vert} G(p,\ell) = \{E_1, \ldots, E_n\}$, $Y = \operatorname{edge} G(p,\ell)$, and $\mathcal{L} = \bigcup_{i,j} \operatorname{Aut}(E_j)\backslash L_{ij}/\operatorname{Aut}(E_i)$. Then the vertex set of $G(p,\ell)^{\pm 1}$ is X and has cardinality $n = \lfloor (p-1)/12 \rfloor + \epsilon_p(0) + \epsilon_p(1728)$. The number of edges of $G(p,\ell)^{+1}$ is $\#\mathcal{L} - \#\{O \in \mathcal{L} : \widehat{O} = O\}$ and the number of edges of $G(p,\ell)^{-1}$ is $\#\mathcal{L} + \#\{O \in \mathcal{L} : \widehat{O} = O\}$. The values of $\#\mathcal{L}$ and $\#\{O \in \mathcal{L} : \widehat{O} = O\}$ are given in Lemmas 6.3 and 6.4, respectively. The euler characteristic is $\#\operatorname{vert} - \frac{1}{2}\#\operatorname{edge}$. □

We now give an example to illustrate how these counts together give an elementary formula for the Ihara zeta function in terms of $\det(1 - uA - \ell u^2)$.

Example 6.6. *Let $p = 137$ and $\ell = 3$. By Lemma 6.4, we have that the number of self-dual orbits is given by*

$$\begin{aligned} r &= \frac{1}{2}(h(-12) + h(-3))\left(1 - \left(\frac{-3}{137}\right)\right) \\ &= \frac{1}{2}(1+1)(1-(-1)) \\ &= 2. \end{aligned}$$

Further, Lemma 6.3 tells us that $\#\mathcal{L}$ is given by

$$\#\mathcal{L} = 4 \cdot \left\lfloor \frac{136}{12} \right\rfloor + \frac{3 + 3 - 2\left(\frac{-3}{3}\right)}{3} = 46.$$

The number of vertices in $G(p,\ell)$ is 12, so we have:

$$\zeta_{G(p,\ell)}(u) = \frac{(1-u)^{-10}(1+u)^{-12}}{\det(1 - Au - 3u^2)}.$$

By a computer computation using SAGE,

$$u\frac{d}{du}\log \zeta_{G(p,\ell)}(u) = 4u^2 + 6u^3 + 12u^4 + 20u^5 + 82u^6 + 96u^7 + O(u^8).$$

6.2. **Isogeny graphs with level structure.** We now introduce the notion of an isogeny graph with level structure as defined by Codogni–Lido [CL24]. These graphs include the supersingular isogeny graphs in [Mes86] (the isogeny graph of supersingular elliptic curves and the isogeny graph of supersingular elliptic curves with $\Gamma_0(N)$-level structure).

Definition 6.7. *Let N be a positive integer and let H be a subgroup of $\mathrm{GL}(\mathbb{Z}/N\mathbb{Z})$. Let k be a field of characteristic not dividing N. Given an elliptic curve E over k, a* **level-N structure** *on E is an isomorphism $\phi\colon (\mathbb{Z}/N\mathbb{Z})^2 \to E[N]$ and a* **level-H structure** *on E is an equivalence class of isomorphisms $\phi\colon (\mathbb{Z}/N\mathbb{Z})^2 \to E[N]$, where two isomorphisms are equivalent if they differ by precomposition by an element of H. Denote the equivalence class of ϕ by $[\phi]_H$ (or just by $[\phi]$, if H is clear from context).*

Let $(E_1, [\phi_1])$ and $(E_2, [\phi_2])$ be two elliptic curves with level-H structures. A **morphism of level-H structures** *$(E_1, [\phi_1]) \to (E_2, [\phi_2])$ is an isogeny $\alpha\colon E_1 \to E_2$ such that $[\alpha \circ \phi_1] = [\phi_2]$.*

An isomorphism $\alpha\colon E_1 \to E_2$ induces a morphism $(E_1, [\phi_1]) \to (E_2, [\phi_2])$ if and only if $\phi_2^{-1} \circ \alpha \circ \phi_1 \in H$, and then the inverse of α is also a morphism:

$$\phi_2^{-1} \circ \alpha \circ \phi_1 \in H \implies (\phi_2^{-1} \circ \alpha \circ \phi_1)^{-1} = \phi_1^{-1} \circ \alpha^{-1} \circ \phi_2 \in H.$$

An automorphism u of E induces an automorphism of $(E, [\phi])$ if it is a morphism $(E, [\phi]) \to (E, [\phi])$, i.e. $u \circ \phi = \phi \circ h$ for some $h \in H$, which holds if and only if $\phi^{-1} \circ u \circ \phi \in H$.

Let d be an integer coprime to N and let $\phi\colon (\mathbb{Z}/N\mathbb{Z})^2$ be a level-N structure on E. Since d is prime to N, the function $d\phi := [d] \circ \phi\colon (\mathbb{Z}/N)^2 \to E[N]$ is also a level-N structure. Let X denote a complete set of representatives for the isomorphism classes of supersingular elliptic curves with level H structure. We have the **diamond operator** $\langle d\rangle\colon X \to X$ that maps $x = (E, [\phi])$ to $\langle d\rangle x := x' \simeq (E, [d\phi])$ where $x' \in X$.

Let $\alpha\colon (E, [\phi]) \to (E', [\phi'])$ be a morphism of elliptic curves with level-H structure. The dual map on isogenies induces a dual map on morphisms: if $[\alpha\phi] = [\phi']$ then there is $h \in H$ such that $\alpha \circ \phi = \phi' \circ h$, so

$$[\ell] \circ \phi = \widehat{\alpha} \circ \phi' \circ h$$

so $[\ell\phi] = [\widehat{\alpha} \circ \phi']$. Let $u\colon (E, [\ell\phi]) \to (E'', [\phi''])$ be an isomorphism. The dual map on morphisms induces a well-defined function on orbits

$$\begin{aligned}\operatorname{Aut}((E', [\phi']))\backslash L/\operatorname{Aut}((E, [\phi])) &\to \operatorname{Aut}((E, [\ell\phi])\backslash L'/\operatorname{Aut}((E'', [\phi''])) \\ \operatorname{Aut}((E', [\phi']))\alpha \operatorname{Aut}((E, [\phi])) &\mapsto \operatorname{Aut}((E'', [\phi'']))u \circ \widehat{\alpha} \operatorname{Aut}((E', [\phi']))\end{aligned}$$

that does not depend on the choice of isomorphism u.

Definition 6.8 (The ℓ-isogeny graph of elliptic curves with level H structure)**.** *Let N be a positive integer, let p and ℓ be distinct primes coprime to N, and let H be a subgroup of* $\mathrm{GL}(\mathbb{Z}/N\mathbb{Z})$*. The* **$\ell$-isogeny graph of supersingular elliptic curves with level-H structure***, denoted $G(p, \ell, H)$, is the graph with*

- **Vertices:** *A complete set of representatives $x_1 = (E_1, [\phi_1]), \dots, x_n = (E_n, [\phi_n])$ for isomorphism class of supersingular elliptic curves with level-H structure;*
- **Edges:** *Given vertices $x_i = (E_i, [\phi_i])$ and $x_j = (E_j, [\phi_j])$, let L_{ij} denote the degree ℓ morphisms $x_i \to x_j$. Then* $\operatorname{Aut}(x_j)$ *and* $\operatorname{Aut}(x_i)$ *have compatible left and right actions on L_{ij} defined via post- and pre-composition. Edges are orbits in L_{ij} of the left action of* $\operatorname{Aut}(x_j)$*. In particular, an edge is of the form* $\operatorname{Aut}(E_j, [\phi_j])\alpha$ *where $\alpha\colon (E_i, [\phi_i]) \to (E_j, [\phi_j])$ is a degree ℓ morphism.*
- **Source and target:** *The source and target of $y = \operatorname{Aut}(x_j)\alpha$ are x_i and x_j, respectively, where $\alpha \in L_{ij}$.*
- **L:** *Define $L((E_i, [\phi_i])) := \langle\ell\rangle x_i = x_k$, the isomorphism class representative $x_k = (E_k, [\phi_k])$ that is isomorphic to $(E_i, [\ell\phi_i])$.*
- **Dual map:** *For each orbit $O = \operatorname{Aut}(x_j)\alpha \operatorname{Aut}(x_i)$, define $JO := \operatorname{Aut}(x_k)u\widehat{\alpha} \operatorname{Aut}(x_j)$, where $x_k = Lx_i$ and $u\colon x_i \to x_k$ is an isomorphism. Pick a representative morphism α_O for each orbit O. For each edge of the form $y = \operatorname{Aut}(x_j)\alpha_O u$ with $u \in \operatorname{Aut}(x_i)$, define $Jy = \operatorname{Aut}(Lx_i)\alpha_{J(O)}$.*

Proposition 6.9. *$G(p, H, \ell)$ (with the above definition of s, t, J, L) is an abstract isogeny graph.*

Proof. We have to show that $s(Jy) = t(y)$ and $t(Jy) = Ls(y)$ for all edges y. Let y be an edge with $s(y) = x_i$ and $t(y) = x_j$ and write $y = \operatorname{Aut}(x_j)\alpha = \operatorname{Aut}(x_j)\phi_O u$ for some $u \in \operatorname{Aut}(E_i)$ where $O = \operatorname{Aut}(x_i)\alpha \operatorname{Aut}(x_j)$. Then $Jy = \operatorname{Aut}(x_k)\phi_{\widehat{O}}$, and $s(Jy)$ is the domain of $\alpha_{\widehat{O}}\colon x_j \to x_k$, i.e. $x_j = t(y)$. And $t(Jy)$ is $x_k = (E_i, [\ell\phi_i]) = Lx_i = Ls(y)$. The graph is $\ell + 1$-regular since each curve has $\ell + 1$ distinct cyclic subgroups of its ℓ-torsion. □

Let $\Gamma = G(p, \ell, H)$ and suppose $\ell \in H$. Then $L\colon X \to X$ is the identity, and we have $s(Jy) = t(y)$ and $t(Jy) = s(y)$ for all edges y of Γ. As in the previous section, we can construct $\Gamma^{\pm 1}$ directly. Let the vertex set be X, a complete set of representatives of isomorphism classes of supersingular elliptic curves with level H structure. Define

$$\mathcal{L} := \bigsqcup_{i,j} \operatorname{Aut}(x_j)\backslash L_{ij}/\operatorname{Aut}(x_i).$$

The edges of Γ^{+1} are

$$\mathcal{L} - \{O \in \mathcal{L} : \widehat{O} = O\}$$

and the edges of Γ^{-1} are

$$\mathcal{L} \sqcup \{O \in \mathcal{L} : \widehat{O} = O\}.$$

Corollary 6.10. *Let $H \leq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be a subgroup such that $\ell \in H$ and let $\Gamma = G(p, H, \ell)$ be the ℓ-isogeny graph of supersingular elliptic curves with level-H structure. Then*

$$\zeta_\Gamma(u) = \frac{(1-u)^{\chi(\Gamma^{+1})}(1+u)^{\chi(\Gamma^{-1})}}{\det(1 - uA + \ell u^2)}.$$

Proof. Let $G(p, \ell, H) = (X, Y, s, t, L, J)$. Since $\ell \in H$, the function $L\colon X \to X$ is the identity. Thus $C_1(L) = \#X$ and $C_k(L) = 0$ for $k > 1$. Given an orbit $O = \operatorname{Aut}(x_j)\alpha\operatorname{Aut}(x_i)$ we have

$$J(O) = \operatorname{Aut}(x_i)\widehat{\alpha}\operatorname{Aut}(x_j) = \widehat{O},$$

so $J^2(O) = O$. Let y be an edge from x_i to x_j and write $y = \operatorname{Aut}(x_j)\alpha_O u$ for some $u \in \operatorname{Aut}(x_i)$. If $y = Jy'$ we have $y = \operatorname{Aut}(x_j)\alpha_{JO'}$, so $O = JO'$ and $\alpha_O = \alpha_{JO'}$. Thus $Jy = J^2y' = \operatorname{Aut}(x_j)\alpha_{O'} = y'$. This implies that every cycle in J has length either 1 or 2, so $C_k(J) = 0$ if $k > 2$. By Theorem 4.11, we have

$$\zeta_\Gamma(u) = \frac{(1-u^2)^{\#X}(1+u)^{-C_1(J)}(1-u^2)^{-C_2(k)}}{\det(1 - uA + \ell u^2)} = \frac{(1-u)^{\#X - C_1(J) - C_2(J)}(1+u)^{\#X - C_2(J)}}{\det(1 - uA + \ell u^2)}.$$

We have that $C_1(J) = \#\{O \in \mathcal{L} : \widehat{O} = O\}$ and that

$$C_2(J) = \frac{1}{2}\#\{O \in \mathcal{L} : \widehat{O} \neq O\} = \frac{1}{2}\#\operatorname{edge}\Gamma^{+1}.$$

We also have $C_1(J) + 2C_2(J) = \#\operatorname{edge}\Gamma^{-1}$. Thus the corollary follows. □

6.3. **$(\ell, \ldots, \ell)$-isogeny graphs.** The $(\ell, \ldots, \ell)$-isogeny graph of superspecial principally polarized abelian varieties of dimension g can also be seen as an abstract isogeny graph. For more details, we refer the reader to the work of Jordan–Zaytman [JZ23] and Florit–Smith [FS22]. Define a graph $\Gamma = \Gamma(g, p, \ell)$ whose vertex set X is a complete set of representatives of the isomorphism classes of principally polarized superspecial abelian varieties $A_1, \ldots, A_h$. The edge set Y consist of equivalence classes of $(\ell, \ldots, \ell)$-isogenies $A_i \to A_j$; these equivalence classes correspond to Lagrangian subgroups $C \subseteq A_i[\ell]$ such that $A_i/C \simeq A_j$, where C is Lagrangian if it is maximally isotropic with respect to the Weil pairing. As before, we call two isogenies equivalent if they differ by post-composition by automorphism. This is the "big isogeny graph" in the language of Jordan and Zaytman [JZ23]. The source and target of an edge are the representative isogeny's domain and codomain. And we can define $J\colon Y \to Y$ as before, by choosing a representative α_O for each orbit $O = \operatorname{Aut}(A_j)\alpha\operatorname{Aut}(A_i)$ and then defining $J(\operatorname{Aut}(A_j)\alpha) = \operatorname{Aut}(A_i)\alpha_{\widehat{O}}$ where $O = \operatorname{Aut}(A_j)\alpha\operatorname{Aut}(A_i)$. The map $L\colon X \to X$ is the identity.

7. Relation to zeta functions of modular curves

We fix two distinct primes p and ℓ, an integer $N > 0$ with $\gcd(p\ell, N) = 1$, and a subgroup H of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. The goal of this section is to relate the Ihara zeta function of $G = G(p, \ell, H)$ (see Definition 4.1) to the Hasse-Weil zeta function associated to the modular curves $X_H(N)_{\mathbb{F}_\ell}$ and $X_{H_p}(N)_{\mathbb{F}_\ell}$, where $H_p = H \times B_0(p) \subset GL_2(\mathbb{Z}/pN\mathbb{Z})$, and the Euler characteristics of the orientable graphs associated to G.

7.1. **Preliminaries on isogeny graphs with level structure.**

We briefly summarize the definitions and results of [CL24] that we will use in our proof.

Definition 7.1. *We define* $\Gamma_H := \{M \in \mathrm{SL}_2(\mathbb{Z}) : M^T \in H \pmod{N}\}$*. The modular curve of level H is defined to be the Riemann surface obtained from the quotient of* $\mathcal{H}^* := \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$ *by the action of* Γ_H*. It is denoted by* $X_H(N) := \mathcal{H}^*/\Gamma_H$*.*

We also define $H_p = H \times B_0(p) \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) \cong \mathrm{GL}_2(\mathbb{Z}/pN\mathbb{Z})$*,* $\Gamma_{H_p} := \{M \in \mathrm{SL}_2(\mathbb{Z}) : M^T \in H_p \pmod{pN}\}$*, and* $X_{H_p}(N) := \mathcal{H}^*/\Gamma_{H_p}$*.*

The curve $X_H(N)$ parameterizes elliptic curves with level H structure, and the curve $X_{H_p}(N)$ parameterizes elliptic curves with level H structure and a cyclic subgroup of level p. The reduction mod p, $X_{H_p}(N)_{\overline{\mathbb{F}}_p}$, is isomorphic to two copies of $X_H(N)_{\overline{\mathbb{F}}_p}$ attached at the points $(E, [\phi])$ such that E is supersingular, which are exactly the vertices of G.

The action of the adjacency matrix A on $\mathbb{C}^{V(G)}$ coincides with the action of the ℓ-th Hecke operator T_ℓ on the maximal torus of $\mathrm{Pic}^0(X_{H_p}(N)_{\mathbb{F}_p})$ (see [CL24, Theorem 4.6] for the precise statement). This action induces an action of double coset operators on weight 2 cuspforms (see [CL24, Section 3,6] for more precise definitions and results).

The connected components of the graph G, as well as the components of the torus, can be described using the Weil invariant, which we now define.

Let $\mu_N^\times(\overline{\mathbb{F}}_p)$ denote the set of primitive N-th roots of unity in $\overline{\mathbb{F}}_p$. There is a right action of $(\mathbb{Z}/N\mathbb{Z})^\times$ on $\mu_N^\times(\overline{\mathbb{F}}_p)$ via $\zeta \cdot a = \zeta^a$, thus inducing an action of $\det(H)$ on $\mu_N^\times(\overline{\mathbb{F}}_p)$. Denote the orbits of this action by $R_H := \mu_N^\times(\overline{\mathbb{F}}_p)/\det(H)$. Since $\phi((1,0)), \phi((0,1))$ form a basis for $E[N]$ and since the Weil pairing is bilinear and alternating we have for any $h \in H$ that

$$w((\phi \circ h)(1,0), (\phi \circ h)(0,1)) = w(\phi(1,0), \phi(0,1))^{\det h}.$$

By surjectivity, we have $w(\phi(1,0), \phi(0,1)) \in \mu_N^\times$, so combining this with the previous comment, $w(E, [\phi]) \in R_H$ is well-defined. We make the following definition of the Weil invariant of the level structure.

Definition 7.2 (Weil invariant of the level structure)**.** *Let* $(E, [\phi])$ *be an elliptic curve with level structure. Let* ω *be the Weil pairing on* $E[N]$*. We define* $w(E, [\phi]) \in R_H$ *to be the Weil invariant of the level structure.*

The Weil invariant gives a surjective map of graphs from G to the oriented Cayley graph $C = C(N, \det(H), \ell)$. C is the graph whose vertices ζ_i are elements of R_H, and there is an edge from ζ_i to ζ_j if $\zeta_j = \zeta_i^\ell$. The mapping $w : V(G) \to R_H$ induces a surjective map $w_* : \mathbb{C}^{V(G)} \to \mathbb{C}^{R_H}$.

For each connected component C_i of C, let $G_i = w^{-1}(C_i)$. Then $w_i : G_i \to C_i$ is a surjective map of graphs, and there is a corresponding linear map $w_{i,*} : \mathbb{C}^{V(G_i)} \to \mathbb{C}^{V(C_i)}$. Write V_ξ as the set of vertices with Weil invariant $\xi \in R_H$. Then we have

$$\ker(w_*) = \bigoplus_{\xi \in R_H} \{(x_v) \in \mathbb{C}^{V_\xi} : \sum x_v = 0\} \quad , \quad \ker(w_{i,*}) = \bigoplus_{\xi \in V(C_i)} \{(x_v) \in \mathbb{C}^{V_\xi} : \sum x_v = 0\}..$$

Definition 7.3. *Let $e_i = \#\operatorname{Aut}(E_i, \phi_i)$ and define an inner product on $\mathbb{C}^{V(G)}$ by*

$$\langle (E_i, \phi_i), (E_j, \phi_j) \rangle = \begin{cases} e_i & : i = j \\ 0 & : i \neq j. \end{cases}$$

It is shown in [CL24, Proposition 2.2] that A is self-adjoint with respect to this inner product when $\ell \in H$.

7.2. Zeta functions of isogeny graphs and modular curves.

Now, we will show how to relate the Ihara zeta function of G to the Hasse-Weil zeta functions of X_H and X_{H_p}. First, we will reduce the computation of $\det(\mathrm{id}_{\mathbb{C}^{V(G)}} - uA + QLu^2)$ on $\mathbb{C}^{V(G)}$ to computing the determinant on $\ker(w_*)$.

Proposition 7.4. *Let k be the order of ℓ in $(\mathbb{Z}/N\mathbb{Z})^\times / \det(H)$, and let $n = \frac{\phi(N)}{k|\det(H)|}$. Let A be the adjacency matrix of G and $Q = D - I$ as in Section 4.*

Then

$$\det\big(\mathrm{id}_{\mathbb{C}^{V(G)}} - uA + QLu^2 | \mathbb{C}^V\big) = (1 - \ell^k u^k)^n (1 - u^k)^n \prod_{i=1}^{n} (\det\big(\mathrm{id}_{\mathbb{C}^{V(G)}} - uA + \ell L u^2 | \ker(\omega_{i,*})\big).$$

Proof. Because all vertices of G have out-degree $\ell + 1$, we have $Q = \ell\, \mathrm{id}_{\mathbb{C}^{V(G)}}$. Since n is the number of connected components of $C = C(N, \det(H), \ell)$, it suffices to fix a connected component C_i and compute $\det\big(1 - Au + QLu^2 | \mathbb{C}^{V(G_i)}\big)$ component by component.

Note that $\ker(\omega_{i,*})$ is invariant under A and L: Elements of $\ker(\omega_{i,*})$ are of the form $\sum a_{(E,[\phi])}(E, [\phi])$ such that for each $\zeta \in C_i$, $\sum_{\omega(E,\phi) = \zeta} a_{(E,\phi)} = 0$. Since $A(E, [\phi])$ is a sum of $(\ell + 1)$ vertices $(E', [\phi'])$ with Weil invariant $\omega(E, [\phi])^\ell$, this property is preserved under A. Similarly, $\omega(L(E, [\phi])) = \omega(E, [\ell]\phi) = \omega(E, \phi)^{\ell^2}$, so this property is preserved under L as well.

Let $\zeta_1, \zeta_2, \ldots, \zeta_k$ denote the vertices of C_i. For each ζ_j, let

$$\delta_j = \sum_{\omega(E,[\phi]) = \zeta_j} \frac{1}{\#\operatorname{Aut}(E, [\phi])} (E, [\phi]).$$

Each δ_j is orthogonal to $\ker(\omega_{i,*})$ under the inner product defined in Definition 7.3, and $\{\delta_j\}_{j=1}^k$ are linearly independent. Let U_i be the span of the $\{\delta_j\}_{j=1}^k$. Then U_i is the orthogonal complement of $\ker(\omega_{i,*})$ in $\mathbb{C}^{V(G_i)}$.

Fix δ_j. We will compute $A\delta_j$ and $L\delta_j$.

First, $A\delta_j = (\ell + 1)\delta_{j'}$, where $\zeta_{j'} = \zeta_j^\ell$. To see this, we compute:

$$\begin{aligned} A\delta_j &= \sum_{\omega(E,[\phi]) = \zeta_j} \sum \frac{\#\{\text{edges: } (E, [\phi]) \to (E', [\phi'])\}}{\#\operatorname{Aut}(E, [\phi])} (E', [\phi']) \\ &= \sum_{\omega(E',[\phi']) = \zeta_j^\ell} (E', [\phi']) \sum \frac{\#\{\text{edges: } (E, [\phi]) \to (E', [\phi'])\}}{\#\operatorname{Aut}(E, [\phi])} \end{aligned}$$

As $\frac{\#\{\text{edges: } (E,\phi)\to(E',\phi')\}}{\#\operatorname{Aut}(E,\phi)} = \frac{\#\{\text{edges: } (E',\phi')\to(E,[\ell]\phi)\}}{\#\operatorname{Aut}(E',\phi')}$ (see the proof of [CL24, Proposition 2.2]), the terms can be rewritten as,

$$A\delta_j = \sum_{\omega(E',[\phi'])=\zeta_j^{\ell}} \frac{(E',[\phi'])}{\#\operatorname{Aut}(E',[\phi'])} \sum \#\{\text{edges: } (E',[\phi'])\to(E,[\ell\phi])\}.$$

Note that the inner sum is over all $(E,[\phi])$ with an isogeny to $(E',[\phi'])$, as all such $(E,[\phi])$ must have the same Weil invariant ζ_j. Therefore, the edges $(E',[\phi'])\to(E,[\ell\phi])$ are all outgoing edges from $(E',[\phi'])$, and we obtain

$$A\delta_j = (\ell+1)\sum_{\omega(E',[\phi'])=\zeta_j^{\ell}} \frac{(E',[\phi'])}{\#\operatorname{Aut}(E',[\phi'])} = (\ell+1)\delta_{j'}.$$

Next, we show $L\delta_j = \delta_{j''}$, where $\zeta_{j''} = \zeta_j^{\ell^2}$. To see this, note that $L\delta_j = \sum_{\omega(E,\phi)=\zeta_j} \frac{(E,[\ell]\phi)}{\#\operatorname{Aut}(E,\phi)}$. Since $\operatorname{Aut}(E,\phi) = \operatorname{Aut}(E,[\ell]\phi)$, this is $L\delta_j = \sum_{\omega(E,\phi)=\zeta_j} \frac{(E,[\ell]\phi)}{\#\operatorname{Aut}(E,[\ell]\phi)}$. Now it suffices to show that the vertices $(E,[\ell]\phi)$ range over all vertices with $\omega((E',\phi')) = \zeta_j^{\ell^2}$. Choose m such that $\ell^m \in H$, and note that $k \mid 2m$. Then for any (E',ϕ') with $\omega(E',\phi') = \zeta_j^{\ell^2}$, we have $\omega((E',[\ell]^{m-1}\phi')) = \zeta_j^{\ell^{2m}}$. Since $k \mid 2m$, $\zeta_j^{\ell^{2m}} = \zeta_j$. Since $\ell^m \in H$, it follows that $(E',\phi') = (E',[\ell]^m\phi') = (E',[\ell][\ell]^{m-1}\phi')$, which shows that $(E',\phi') = (E,[\ell]\phi)$ for some (E,ϕ) with $\omega(E,\phi) = \zeta_j$.

Case 1. $k=1$.
In this case, $\zeta_j = \zeta_j^{\ell} = \zeta_j^{\ell^2}$, so the restriction of $1 - Au + QLu^2$ to the single vertex of U_i is $(1-(\ell+1)u+\ell u^2) = (1-\ell u)(1-u)$.

Case 2. $k=2$.
If $k=2$, then U_i has two distinct vertices ζ_j and ζ_j^{ℓ}, and $\zeta_j^{\ell^2} = \zeta_j$.
In this case, the restriction of $1 - uA + QLu^2$ to U_i has the form

$$\begin{pmatrix} (1+\ell u^2) & -(\ell+1)u \\ -(\ell+1)u & (1+\ell u^2) \end{pmatrix},$$

whose determinant is $(1+\ell u^2)^2 - (-(\ell+1)u)^2 = (1-\ell^2u^2)(1-u^2)$.

Case 3. $k \geq 3$.
In this case, ζ_j, ζ_j^{ℓ}, and $\zeta_j^{\ell^2}$ are all distinct. Therefore, the restriction of $(1 - Au + QLu^2)$ to U_i has the form of the circulant matrix whose first row is $1, -(\ell+1)u, \ell u^2$ followed by $k-3$ zeroes:

$$\begin{pmatrix} 1 & -(\ell+1)u & \ell u^2 & \dots & \\ 0 & 1 & -(\ell+1)u & \ell u^2 & \dots \\ \vdots & \vdots & \ddots & \ddots & \ddots \\ -(\ell+1)u & \ell u^2 & \dots & 0 & 1 \end{pmatrix},$$

whose determinant is $\prod_{j=1}^{k}(1-(\ell+1)u\omega^j + \ell u^2\omega^{2j})$, where ω is a primitive k-th root of unity. Factoring this expression as $\prod_{j=1}^{k}(1-\ell u\omega^j)(1-u\omega^j)$ and noting ω^j ranges over all k-th roots of 1, we obtain $\det(1 - Au + QLu^2|U_i) = (1-\ell^k u^k)(1-u^k)$. □

Corollary 7.5. *Suppose H contains $\begin{pmatrix} \ell & 0 \\ 0 & \ell \end{pmatrix}$ and has surjective determinant. Then*

$$\zeta_G(u) = \frac{(1-u)^{\chi(G^{+1})}(1+u)^{\chi(G^{-1})}}{(1-u)(1-\ell u)\det(\mathrm{id}_{\mathbb{C}^{V(G)}} - uA + \ell u^2)}$$

Proof. The condition $\ell \in H$ implies that L and J has no . This implies $C_1(L)$ is the number of vertices of G, $C_k(L) = 0$ for all $k > 1$, and $C_k(J) = 0$ for all $k > 2$. Since H has surjective determinant, $|R_H| = 1$.

Therefore, combining Theorem 4.11 and Proposition 7.4, we have

$$\begin{aligned} \zeta_G(u) &= \frac{(1-u^2)^{\#V(G)}(1+u)^{-\#\{[y]\in Y' : J[y]=[y]\}}(1-u^2)^{-\#Y'}}{(1-u)(1-\ell u)(\det(1-uA+\ell u^2|\ker(\omega_{1,*}))} \\ &= \frac{(1+u)^{\chi(\Gamma^{-1})}(1-u)^{\chi(\Gamma^{+1})}}{(1-u)(1-\ell u)(\det(1-uA+\ell u^2|\ker(\omega_{1,*}))}. \end{aligned}$$

□

Definition 7.6. *Let X be a smooth, irreducible, projective variety defined over $\mathbb{F}_\ell$. The **Hasse-Weil zeta function** for X is defined as:*

$$Z(X,u) = \exp\left(\sum_{n=1}^{\infty} \frac{\#X(\mathbb{F}_{\ell^n})}{n} u^n\right) = \prod_{x\in[C]} \frac{1}{1-u^{\deg(x)}},$$

where the product is defined over the closed points of C.

For a prime $\ell \nmid N$ and $H' \leq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, from the Eichler-Shimura relation and Weil Conjectures [CL24, Theorem 3.7], the Hasse-Weil zeta function of the modular curve $X_H(N)$ is given by

$$Z(X_{H'}(N)_{\mathbb{F}_\ell}, u) = ((1-u)(1-\ell u))^{-1} \det\Big(1 - \widetilde{T}_\ell u + \ell\langle\widetilde{\ell}\rangle u^2 | S_2(\Gamma_{H'}(N))\Big)$$

where $\langle\widetilde{\ell}\rangle$ sends $f \in S_2(\Gamma_{H'}(N))$ to $f[m_\ell]_2$, with $m_\ell \equiv \left(\begin{smallmatrix} \ell^{-1} & 0 \\ 0 & \ell \end{smallmatrix}\right) \pmod{N}$.

By the same argument,

$$Z(X_{H_p}(N)_{\mathbb{F}_\ell}, u) = (1-u)^{-1}(1-\ell u)^{-1} \det\Big(1 - \widetilde{T}_\ell u + \ell\langle\widetilde{\ell}\rangle u^2 | S_2(\Gamma_{H_p}(N))\Big)$$

Theorem 7.7. *Let G be the ℓ-isogeny graph with Borel level structure (i.e. $H = \{\begin{pmatrix} * & 0 \\ * & * \end{pmatrix}\}$). Let $X_0(pN)_{\mathbb{F}_\ell}$ and $X_0(N)_{\mathbb{F}_\ell}$ denote the modular curves over $\mathbb{F}_\ell$. Then we have that*

$$Z(X_0(pN)_{\mathbb{F}_\ell}, u) Z(X_0(N)_{\mathbb{F}_\ell}, u)^{-2} \zeta_G(u) = (1+u)^{\chi(G^{-1})}(1-u)^{\chi(G^{+1})},$$

where G^{+1} and G^{-1} are the orientable graphs associated to $\Gamma = G$ as constructed in Section 3.1.

Proof. For a prime ℓ and a positive integer M coprime to ℓ, let $\sigma_\ell \in \Gamma_0(M)$ satisfy $\ell\sigma_\ell \equiv \begin{pmatrix} 1 & 0 \\ 0 & \ell^2 \end{pmatrix} \pmod{M}$. By [Shi94, Theorem 7.11], for $\ell \nmid M$,

$$Z(X_0(M)_{\mathbb{F}_\ell}, u) = \frac{\det\Big(1 - \widetilde{T}_\ell u + \ell\langle\widetilde{\ell}\rangle u^2\Big)}{(1-u)(1-\ell u)},$$

where $\widetilde{T_\ell}$ and $\langle\widetilde{\ell}\rangle$ are the double coset operators on $S_2(\Gamma_0(M))$ defined by $\tilde{T}_\ell = [\Gamma_0(M)\begin{pmatrix}1 & 0\\ 0 & \ell\end{pmatrix}\Gamma_0(M)]$ and $\langle\tilde{\ell}\rangle = [\Gamma_0(M)\sigma_\ell\Gamma_0(M)]$. Since $\sigma_\ell \in \Gamma_0(M)$, we have that $\langle\tilde{\ell}\rangle$ acts as the identity on $S_2(\Gamma_0(M))$.

Decomposing $S_2(\Gamma_0(pN)) = S_2(\Gamma_0(pN))^{\text{p-old}} \oplus S_2(\Gamma_0(pN))^{p-new}$, and noting that the p-old and p-new spaces are stable under $\widetilde{T_\ell}$, we can write:

$$Z(X_0(pN)_{\mathbb{F}_\ell}, u) = \frac{\det\Big(1 - \tilde{T}_\ell u + \ell u^2 | S_2(\Gamma_0(pN))^{\text{p-old}}\Big)\det\Big(1 - \tilde{T}_\ell u + \ell u^2 | S_2(\Gamma_0(pN))^{p-new}\Big)}{(1-u)(1-\ell u)}.$$

Since $S_2(\Gamma_0(pN))^{\text{p-old}}$ is isomorphic to $S_2(\Gamma_0(N)) \oplus S_2(\Gamma_0(N))$ as $\tilde{T}_\ell$-modules (see the proof of [DS05, Proposition 5.6.2], and note that by [DS05, Proposition 5.2.1] the action of $[\Gamma_1(M)\begin{pmatrix}1 & 0\\ 0 & \ell\end{pmatrix}\Gamma_1(M)]$ on $S_2(\Gamma_0(M)) \subset S_2(\Gamma_1(M))$ agrees with the action of $\tilde{T}_\ell$ on $S_2(\Gamma_0(M))$), we have

$$Z(X_0(N)_{\mathbb{F}_\ell}, u)^2 = \frac{\det\Big(1 - \tilde{T}_\ell u + \ell u^2 | S_2(\Gamma_0(pN))^{\text{p-old}}\Big)}{(1-u)^2(1-\ell u)^2},$$

and therefore

$$Z(X_0(pN), u) Z(X_0(N), u)^{-2} = (1-u)(1-\ell u)\det\Big(1 - \tilde{T}_\ell u + \ell u^2 | S_2(\Gamma_0(pN))^{p-new}\Big).$$

Now we relate this expression to the Ihara zeta function of the graph G. In the Borel case, G is connected (so $n = 1$) and the order of ℓ in R_H is 1. The dual map J corresponds to taking the dual of an isogeny, and in particular, there are no cycles of length greater than 2 in the decomposition of σ_J. Combining Theorem 4.11 and Proposition 7.4, we have

$$\zeta_G(u) = (1-u)^{-1}(1-\ell u)^{-1}\det\big(1 - Au + Qu^2 | \ker(\omega_{1,*})\big)^{-1}(1+u)^{\chi(G^{-1})}(1-u)^{\chi(G^{+1})}.$$

It was shown by [CL24, Theorem 6.5.5] that there is an isomorphism of $S_2^{p-new}(\Gamma_0(pN))$ with $\ker(\omega_{1,*})$, which intertwines the action of $\widetilde{T_\ell}$ on $S_2^{p-new}(\Gamma_0(pN))$ with A on $\ker(\omega_{1,*})$. Therefore,

$$Z(X_0(pN), u) Z(X_0(N), u)^{-2} = (1-u)(1-\ell u)\det\big(1 - Au + Qu^2 | \ker(\omega_{1,*})\big),$$

and combining the two equations, we obtain

$$\zeta_G(u) Z(X_0(pN)_{\mathbb{F}_\ell}, u) Z(X_0(N)_{\mathbb{F}_\ell}, u)^{-2} = (1+u)^{\chi(G^{-1})}(1-u)^{\chi(G^{+1})}.$$

□

Following [CL24, Rib90], we define p-old and p-new spaces of $S_2(\Gamma(N) \cap \Gamma_0(p))$ using the following inclusions of $S_2(\Gamma(N))$ into $S_2(\Gamma(N) \cap \Gamma_0(p))$:

$$\begin{aligned} i_1 &: S_2(\Gamma(N)) \to S_2(\Gamma(N) \cap \Gamma_0(p)) & f(z) &\mapsto f(z)\\ i_2 &: S_2(\Gamma(N)) \to S_2(\Gamma(N) \cap \Gamma_0(p)) & f(z) &\mapsto f(pz)\end{aligned}$$

By considering H-invariant subspaces , this induces the following inclusion maps [CL24, Zyw21]:

$$\begin{aligned} i_3 : S_2(\Gamma_H(N)) &\to S_2(\Gamma_{H_p}(N)) & f(z) &\mapsto f(z) \\ i_4 : S_2(\Gamma_H(N)) &\to S_2(\Gamma_{H_p}(N)) & f(z) &\mapsto f(pz) \end{aligned}$$

Definition 7.8. *Define the p-**old subspaces** as*

$$\begin{aligned} S_2^{p-old}(\Gamma(N) \cap \Gamma_0(p)) &:= i_1(S_2(\Gamma(N))) \oplus i_2(S_2(\Gamma(N))) \\ S_2^{p-old}(\Gamma_{H_p}(N)) &:= i_3(S_2(\Gamma_H(N))) \oplus i_4(S_2(\Gamma_H(N))). \end{aligned}$$

*The p-**new subspaces** are the orthogonal complements with respect to the Petersson inner product, i.e.*

$$S_2^{p-new}(\Gamma(N) \cap \Gamma_0(p)) := \left(S_2^{p-old}(\Gamma(N) \cap \Gamma_0(p))\right)^{\perp}, \quad S_2^{p-new}(\Gamma_{H_p}(N)) := \left(S_2^{p-old}(\Gamma_{H_p}(N)\right)^{\perp}$$

The result of [CL24, Theorem 5.5.2] gives an isomorphism between the subspace of H-invariant cuspforms in $S_2^{p-new}(\Gamma_0(p) \cap \Gamma(N))$ and $\ker(w_*)$. For our setup, it is more convenient to rephrase in terms of $S_2(\Gamma_{H_p}(N))$.

Lemma 7.9. *Suppose* $\det(H) = (\mathbb{Z}/N\mathbb{Z})^\times$, *and consider the action of* $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ *on* $S_2(\Gamma_0(p) \cap \Gamma(N)) \otimes \mathbb{C}^{(\mathbb{Z}/N\mathbb{Z})^\times}$ *defined in* [CL24, Section 5 (5.5.1), Remark 5.5.3], *i.e.*

$$\begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix} \cdot (f_a)_a = (f_{ad})_a \qquad\qquad h \cdot (f_a)_a = (f_a[\tilde{h}_a]_2)_a, \det(h) = 1$$

where $\tilde{h}_a \in B_0(p)$ *such that* $\tilde{h}_a \equiv \left(\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} h \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}^{-1} \right)^T \pmod N$. *Let S^H denote the H-invariant subspace of cusp forms in S.*

Then $S_2(\Gamma(N))^H = S_2(\Gamma_H(N))$, $S_2(\Gamma_0(p) \cap \Gamma(N))^H = S_2(\Gamma_{H_p}(N))$, *and* $S_2^{p-new}(\Gamma_{H_p}(N)) = \left(S_2^{p-new}(\Gamma_0(p) \cap \Gamma(N)) \otimes \mathbb{C}^{(\mathbb{Z}/N\mathbb{Z})^\times}\right)^H$.

Proof. The first two equalities follow from [Zyw21, Lemma 6.5].

Now, we show that $S_2^{p-new}(\Gamma_{H_p}) = \left(S_2^{p-new}(\Gamma_0(p) \cap \Gamma(N)) \otimes \mathbb{C}^{(\mathbb{Z}/N\mathbb{Z})^\times}\right)^H$, i.e. that taking the p-new subspace commutes with taking the H-invariant subspace. By the action defined above, the non-determinant 1 matrices act by shifting the indices and surjective determinant implies that the H-invariant subspaces consists of tuples of the form $(f_a)_a = (f)_a$ for some chosen representative f. So we only have to show $(S_2^{p-new}(\Gamma_{H_p})) = \left(S_2^{p-new}(\Gamma_0(p) \cap \Gamma(N))\right)^H$, i.e., the action of $h \in H$ respects the Petersson inner product on $S_2(\Gamma_0(p) \cap \Gamma(N))$, i.e. $\langle h \cdot f, h \cdot g \rangle = \langle f, g \rangle$.

It suffices to consider $\det(h) = 1$ and to show that for each $a \in (\mathbb{Z}/N\mathbb{Z})^\times$, $\langle f[\tilde{h}_a]_2, g[\tilde{h}_a]_2 \rangle = \langle f, g \rangle$. Note that $\tilde{h}_a^{-1}(\Gamma_0(p) \cap \Gamma(N))\tilde{h}_a \subset \Gamma_0(p) \cap \Gamma(N) \subset \mathrm{SL}_2(\mathbb{Z})$, so by [DS05, Proposition 5.5.2(a), Exercise 5.4.3],

$$\langle f[\tilde{h}_a]_2, g[\tilde{h}_a]_2 \rangle_{\Gamma_0(p) \cap \Gamma(N)} = \langle f[\tilde{h}_a]_2, g[\tilde{h}_a]_2 \rangle_{\tilde{h}_a^{-1}(\Gamma_0(p) \cap \Gamma(N))\tilde{h}_a} = \langle f, g \rangle_{\Gamma_0(p) \cap \Gamma(N)}.$$

It follows that an orthogonal decomposition of H-invariant $f \in S_2(\Gamma_0(p) \cap \Gamma(N))$ into p-old and p-new components, is an orthogonal decomposition into H-invariant p-old and p-new components.

□

Theorem 7.10. *Let G be the ℓ-isogeny graph with level structure H, where $H \leq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ is a subgroup with surjective determinant, and $H_p := H \times B_0(p) \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, where $B_0(p)$ is the Borel subgroup. Suppose that $\left(\begin{smallmatrix} \ell^{-1} & 0 \\ 0 & \ell \end{smallmatrix}\right), \left(\begin{smallmatrix} \ell & 0 \\ 0 & \ell \end{smallmatrix}\right) \in H$. Denote $X_H(N)_{\mathbb{F}_\ell}$ and $X_{H_p}(N)_{\mathbb{F}_\ell}$ to be the associated modular curves. Then we have that*

$$Z(X_{H_p}(N)_{\mathbb{F}_\ell}, u) Z(X_H(N)_{\mathbb{F}_\ell}, u)^{-2} \zeta_G(u) = (1+u)^{\chi(G^{-1})}(1-u)^{\chi(G^{+1})},$$

where G^{+1} and G^{-1} are the orientable graphs associated to $\Gamma = G$ as constructed in Section 3.1.

Proof. Let ℓ be a prime not dividing a positive integer M. The Hasse-Weil zeta function of $X_H(M)$ is given by

$$Z(X_H(M)_{\mathbb{F}_\ell}, u) = \frac{\det\Big(1 - \widetilde{T}_\ell u + \ell \langle \widetilde{\ell} \rangle u^2 | S_2(\Gamma_H(M))\Big)}{(1-u)(1-\ell u)},$$

where $\widetilde{T}_\ell$ and $\langle \widetilde{\ell} \rangle$ are the double coset operators on $S_2(\Gamma_H(M))$ defined by $\tilde{T}_\ell = [\Gamma_H(M) \left(\begin{smallmatrix} 1 & 0 \\ 0 & \ell \end{smallmatrix}\right) \Gamma_H(M)]$ and $\langle \widetilde{\ell} \rangle = [\Gamma_H(M) \left(\begin{smallmatrix} \ell^{-1} & 0 \\ 0 & \ell \end{smallmatrix}\right) \Gamma_H(M)]$. Since $\left(\begin{smallmatrix} \ell^{-1} & 0 \\ 0 & \ell \end{smallmatrix}\right) \in \Gamma_H(M) \subset \Gamma_{H_p}(M)$, the diamond operator $\langle \tilde{\ell} \rangle$ acts as the identity on $S_2(\Gamma_H(M))$ and on $S_2(\Gamma_{H_p}(M))$.

Following Definition 7.8 and Lemma 7.9, we decompose the space of cusp forms of H_p into p-old and p-new subspaces:

$$S_2(\Gamma_{H_p}(N)) = S_2^{p-old}(\Gamma_{H_p}(N)) \oplus S_2^{p-new}(\Gamma_{H_p}(N)).$$

The p-old and p-new spaces are stable under $\tilde{T}_\ell$ following the arguments in [DS05, Propositions 5.5.2 and 5.6.2]. we can write:

$$Z(X_{H_p}(N)_{\mathbb{F}_\ell}, u) = \frac{\det\Big(1 - \tilde{T}_\ell u + \ell u^2 | S_2^{p-old}(\Gamma_{H_p}(N))\Big) \det\Big(1 - \tilde{T}_\ell u + \ell u^2 | S_2^{p-new}(\Gamma_{H_p}(N))\Big)}{(1-u)(1-\ell u)}.$$

The p-old subspace contains two copies of $S_2(\Gamma_H(N))$ as $\tilde{T}_\ell$-module. We have

$$Z(X_H(N)_{\mathbb{F}_\ell}, u)^2 = \frac{\det\Big(1 - \tilde{T}_\ell u + \ell u^2 | S_2^{p-old}(\Gamma_{H_p}(N))\Big)}{(1-u)^2(1-\ell u)^2},$$

and therefore

$$Z(X_{H_p}(N), u) Z(X_H(N), u)^{-2} = (1-u)(1-\ell u) \det\Big(1 - \tilde{T}_\ell u + \ell u^2 | S_2^{p-new}(\Gamma_{H_p}(N))\Big).$$

Now we relate this expression to the Ihara zeta function of the graph G. Since H has surjective determinant, we have $R_H = \{1\}$, G is connected and the order of ℓ in R_H is 1. The dual map J corresponds to taking the dual of an isogeny, and in particular, there are no cycles of length greater than 2 in the decomposition of σ_J. Combining Theorem 4.11, Remark 4.10, and Proposition 7.4, we have

$$\zeta_G(u) = (1-u)^{-1}(1-\ell u)^{-1} \det\big(1 - Au + Qu^2 | \ker(\omega_{1,*})\big)^{-1} (1+u)^{\chi(G^{-1})}(1-u)^{\chi(G^{+1})}.$$

It was shown by [CL24, Theorem 5.5.2] that there is an isomorphism of $S_2^{p-new}(\Gamma_{H_p}(N))$ with $\ker(\omega_{1,*})$, which intertwines the action of $\tilde{T}_\ell$ on $S_2^{p-new}(\Gamma_{H_p}(N))$ with A on $\ker(\omega_{1,*})$. Therefore,

$$Z(X_{H_p}(N), u) Z(X_H(N), u)^{-2} = (1-u)(1-\ell u) \det\big(1 - Au + Qu^2 | \ker(\omega_{1,*})\big),$$

and combining the two equations, we obtain

$$\zeta_G(u) Z(X_{H_p}(N)_{\mathbb{F}_\ell}, u) Z(X_H(N)_{\mathbb{F}_\ell}, u)^{-2} = (1+u)^{\chi(G^{-1})}(1-u)^{\chi(G^{+1})}.$$

□

We end with an explicit example of Theorem 7.7 in the case $N = 1$ and $H = \mathrm{GL}_2(\mathbb{Z})$.

Example 7.11. *Let $p = 11$ and $\ell = 3$. We consider the Ihara zeta function of $G(p, \ell)$. Since we are working with the isogeny graph with no additional level structure, Theorem 7.7 relates the Ihara zeta function to the zeta functions $Z(X_0(11)_{\mathbb{F}_3}, u)$ and $Z(X_0(1)_{\mathbb{F}_3}, u)$. The modular curve $X_0(p)$ is elliptic, given by the model*

$$y^2 + y = x^3 - x^2 - 10x - 20.$$

The trace of Frobenius at $\ell = 3$ is -1, so we get that

$$Z(X_0(11)_{\mathbb{F}_3}, u) = \frac{1 + u + 3u^2}{(1-u)(1-3u)}.$$

The modular curve $X_0(1)$ has genus zero, so the Hasse-Weil zeta function is

$$Z(X_0(1)_{\mathbb{F}_3}, u) = \frac{1}{(1-u)(1-3u)}.$$

The adjacency matrix for the graph $G(11, 3)$ is given by

$$A = \begin{pmatrix} 1 & 3 \\ 2 & 2 \end{pmatrix}.$$

Using Lemma 6.3 and Lemma 6.4 we can compute that the number of undirected edges is $\#E^u = 3$ and the number of self-dual loops is $r = 2$. Thus we have that

$$\begin{aligned}
\zeta_G(u) &= \frac{(1-u^2)^{-\#E^u + \#V + r}}{\det(1 - uA + 3u^2)(1+u)^r} \\
&= \frac{(1-u^2)^{-3+2+2}}{(1-u)(1-3u)(1+u+3u^2)(1+u)^2} \\
&= \frac{(1-u)(1+u)}{(1-u)(1-3u)(1+u+3u^2)(1+u)^2} \\
&= \frac{1}{(1-3u)(1+u+3u^2)(1+u)}.
\end{aligned}$$

The product is therefore given by

$$\left(\frac{1+u+3u^2}{(1-u)(1-3u)}\right)((1-u)(1-3u))^2\left(\frac{1}{(1-3u)(1+u+3u^2)(1+u)}\right) = \frac{1}{1+u}.$$

This is the result predicted by Theorem 7.7 because $B_1(G) = 1$ and $r = 1$.

8. Applications and examples

In this section, we present two applications of the results in Sections 4 and 7, as well as a number of explicit examples. First, we derive an explicit point count formula for the number of points on the modular curve $X_0(p)$ over the finite field $\mathbb{F}_{\ell^r}$ in terms of cycle counts in supersingular isogeny graphs. The resulting formula can be compared with explicit counting methods using group theory in [**?**]. Then, we relate our cycles to counts of "isogeny cycles" that were obtained in [ACL$^+$24]. We are able to expand and improve on an asymptotic given in the second paper, while also using their results to rephrase our point counts on $X_0(p)$ in terms of imaginary quadratic class numbers.

8.1. **Point-counting on modular curves.**

Since the Hasse-Weil zeta functions in Theorem 7.7 count points over extensions of $\mathbb{F}_\ell$ on $X_0(pN)$ and $X_0(N)$, and the Ihara zeta function counts non-backtracking cycles, we can use the product formula of Theorem 7.7 to obtain relationships between these counts. We make this explicit in the following proposition.

Proposition 8.1. *Let $r, B_1(G)$ be as in Theorem 7.7, and N_r be the number of non-backtracking tailless cycles of length r in $G(p,\ell,N)$. Then we have that*

$$\#X_0(pN)(\mathbb{F}_{\ell^r}) - 2\#X_0(N)(\mathbb{F}_{\ell^r}) + N_r = (B_1(G)-1) + (-1)^{r-1}(1-B_1(G)-r).$$

Proof. From the definitions of the relevant zeta functions, we have that $\#X_0(pN)(\mathbb{F}_{\ell^r})$ is the coefficient on u^r in $u\frac{d}{du}Z(X_0(pN)_{\mathbb{F}_{\ell^r}},u)$, and similar for $\#X_0(N)$ and N_r. We let $Z_1 = Z(X_0(pN)_{\mathbb{F}_{\ell^r}},u)$, $Z_2 = Z(X_0(N)_{\mathbb{F}_{\ell^r}},u)$, and $\zeta = \zeta_G(u)$. By Theorem 7.7 we have

$$\begin{aligned} u\frac{d}{du}\log(Z_1Z_2\zeta) &= u\frac{d}{du}\log\big((1-u)^{1-B_1(G)}(1+u)^{1-B_1(G)-r}\big) \\ u\frac{d}{du}\log(Z_1) + u\frac{d}{du}\log(Z_2) + u\frac{d}{du}\log(\zeta) &= (1-B_1(G))u\frac{d}{du}\log(1-u) \\ &\quad + (1-B_1(G)-r)u\frac{d}{du}\log(1+u) \\ &= (1-B_1(G))\frac{-u}{1-u} \\ &\quad + (1-B_1(G)-r)\frac{u}{1+u} \\ &= (B_1(G)-1)\sum_{n=0}^{\infty}u^{n+1} + (1-B_1(G)-r)\sum_{n=0}^{\infty}(-1)^nu^{n+1}. \end{aligned}$$

The result now follows by equating the coefficient on u^r on both sides. □

As a corollary, we obtain a formula for the number of points on $X_0(p)$ over $\mathbb{F}_{\ell^r}$ in terms of cycles in $G(p,\ell,1)$. These cycle counts have been studied previously in [ACL$^+$24] and we also note that there are explicit counting methods from group theory [**?**].

Proposition 8.2. *Let r be the number of self-dual loops in $G(p,\ell)$, which is given by Lemma 6.4, $\chi = -\#E^u + \#V + r$, and N_n be the coefficient on u in $u\frac{d}{du}\log\zeta_G(u)$. Then we have*

$$\#X_0(p)(\mathbb{F}_{\ell^n}) = ((-1)^{n-1}-1)\chi + (-1)^nr + 2(1+\ell^n) - N_n.$$

Proof. Take $N=1$ in Proposition 8.1, and use the fact that $X_0(1)$ has genus zero, and so $\#X_0(1)(\mathbb{F}_{\ell^r}) = 1+\ell^r$. □

8.2. **Relation to previous cycle counts.** To make this formula more explicit, and draw connections with other parts of the literature, we recall the results of [ACL$^+$24].

Definition 8.3. *An* isogeny cycle *is a closed walk, forgetting basepoint, in $\mathcal{G}_\ell$ containing no backtracking, which is not a power of another closed walk.*

The authors of [ACL$^+$24] prove the following:

Theorem 8.4. *Let $p \equiv 1 \pmod{12}$. Let $\mathcal{G}_\ell$ be the supersingular ℓ-isogeny graph over $\overline{\mathbb{F}}_p$ and let $\#\mathcal{G}_\ell$ denote its number of vertices. The number of non-backtracking closed walks of length r in $\mathcal{G}_\ell$, taken up to order of traversal and starting point, asymptotically approaches $\ell^r/2r$ as $r \to \infty$. Thus, the number of isogeny cycles in $\mathcal{G}_\ell$ is also asymptotically $\ell^r/2r$ as $r \to \infty$.*

We give a generalization of Theorem 8.4 to isogeny graphs with level structure, while also removing the assumption that $p \equiv 1 \pmod{12}$.

Theorem 8.5. *Let $\mathcal{G}(p, \ell, N)$ be the supersingular ℓ-isogeny graph modulo p with N-level structure. Let N_r be the number of non-backtracking cycles of length r in $\mathcal{G}(p, \ell, N)$. Then N_r asymptotically approaches ℓ^r as $r \to \infty$.*

Proof. By Proposition 8.1 we have that $N_r = O(r) + 2\#X_0(N)(\mathbb{F}_{\ell^r}) - \#X_0(pN)(\mathbb{F}_{\ell^r})$. We now note that by the Hasse-Weil bound, $|\#X - (1 + \ell^r)| \leq K\sqrt{\ell^r}$, where X can be either $X_0(N)$ or $X_0(pN)$, and K is a contant that depends on the curve, but not on r. Thus, as $r \to \infty$, $\#X/\ell^r \to 1$, for either $X = X_0(N)$ or $X = X_0(pN)$. Using the formula for N_r above, we get that $N_r/\ell^r \to 1$ as $r \to \infty$. □

Remark 8.6. *To recover Theorem 8.4 from Theorem 8.5, take $N = 1$, and note that N_r counts all non-backtracking cycles of length r, so the number of non-backtracking cycles up to basepoint and direction of traversal is asymptotically $\ell^r/2r$.*

We now turn our attention to making the point count in Corollary 8.2 more explicit. From definition 8.3, we have that if c_r is the number of isogeny cycles of length r, then $N_n = \sum_{r|n} rc_r$. The authors of [ACL$^+$24] have given an explicit formula for rc_r in terms of imaginary quadratic class numbers. We begin with following definition:

$$\mathcal{I}_r := \left\{ \text{imaginary quadratic orders } \mathcal{O} : \begin{array}{l} p \text{ does not split in the field containing } \mathcal{O} \\ p \text{ does not divide the conductor of } \mathcal{O} \\ \mathcal{O} \text{ is an } \ell\text{-fundamental order,} \\ (\ell) = \mathfrak{l}\bar{\mathfrak{l}} \text{ splits in } \mathcal{O}, \\ \text{and } [\mathfrak{l}] \text{ has order } r \text{ in } \mathrm{Cl}(\mathcal{O}). \end{array} \right\}$$

Then we have

Theorem 8.7. *Let $r > 2$ such that $\ell^r < p$. Then we have that*

$$rc_r = 2 \sum_{\mathcal{O} \in \mathcal{I}_r} h(\mathcal{O}).$$

We give an example of using Theorem 8.7 and Theorem 8.1 to compute the number of points on a modular curve.

Example 8.8. *Let $p = 11$ and $\ell = 2$. We will use Proposition 8.1 to compute the number of points on $X_0(p)$ over $GF(8)$. Using Lemma 6.4, we see that the number of self-dual loops in $G(p, \ell)$ is*

$$r = \frac{1}{2}h(-8)\left(1 - \left(\frac{-2}{11}\right)\right) + 1 = 1.$$

We can also compute that this is the only loop in $G(p, \ell)$, so the number of isogeny cycles of length 1 is $c_1 = 0$. We then compute find that $\mathcal{I}_r = \{-31, -23\}$, and both of these orders have class number 3. Thus we see that $N_3 = c_1 + 3c_3 = 0 + 2(3 + 3) = 12$. We can therefore compute

$$\begin{aligned}\#X_0(11)(GF(8)) &= ((-1)^{3-1} - 1)\chi + (-1)^3 r + 2(1 + 2^3) - 12 \\ &= 0 - 1(1) + 2(9) - 12 \\ &= 5.\end{aligned}$$

To confirm the result, we note that we have a model for $X_0(p)$ given in the previous example, and the result can be confirmed directly in Sage.

References

[ACL$^+$24] Sarah Arpin, Mingjie Chen, Kristin E. Lauter, Renate Scheidler, Katherine E. Stange, and Ha T. N. Tran. Orientations and cycles in supersingular isogeny graphs. In *Research directions in number theory*, volume 33 of *Assoc. Women Math. Ser.*, pages 25–86. Springer, Cham, [2024] ©2024.

[Bas92] Hyman Bass. The Ihara-Selberg zeta function of a tree lattice. *Internat. J. Math.*, 3(6):717–797, 1992.

[BCC$^+$23] Andrea Basso, Giulio Codogni, Deirdre Connolly, Luca De Feo, Tako Boris Fouotsa, Guido Maria Lido, Travis Morrison, Lorenz Panny, Sikhar Patranabis, and Benjamin Wesolowski. Supersingular curves you can trust. In *Advances in Cryptology – EUROCRYPT 2023: 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23–27, 2023, Proceedings, Part II*, page 405–437, Berlin, Heidelberg, 2023. Springer-Verlag.

[CL24] Giulio Codogni and Guido Lido. Spectral theory of isogeny graphs, 2024.

[CLG09] Denis X. Charles, Kristin E. Lauter, and Eyal Z. Goren. Cryptographic hash functions from expander graphs. *J. Cryptology*, 22(1):93–113, 2009.

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

[DS05] Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[FS22] Enric Florit and Benjamin Smith. Automorphisms and isogeny graphs of abelian varieties, with applications to the superspecial Richelot isogeny graph. In *Arithmetic, geometry, cryptography, and coding theory 2021*, volume 779 of *Contemp. Math.*, pages 103–132. Amer. Math. Soc., [Providence], RI, [2022] ©2022.

[Has89] Ki-ichiro Hashimoto. Zeta functions of finite graphs and representations of p-adic groups. In *Automorphic forms and geometry of arithmetic varieties*, volume 15 of *Adv. Stud. Pure Math.*, pages 211–280. Academic Press, Boston, MA, 1989.

[Iha66] Yasutaka Ihara. On discrete subgroups of the two by two projective linear group over $\mathfrak{p}$-adic fields. *J. Math. Soc. Japan*, 18:219–235, 1966.

[JZ23] Bruce W. Jordan and Yevgeny Zaytman. Isogeny graphs of superspecial abelian varieties and brandt matrices, 2023.

[LM24] Antonio Lei and Katharina Müller. On the zeta functions of supersingular isogeny graphs and modular curves. *Arch. Math. (Basel)*, 122(3):285–294, 2024.

[Mes86] J.-F. Mestre. La méthode des graphes. Exemples et applications. In *Proceedings of the international conference on class numbers and fundamental units of algebraic number fields (Katata, 1986)*, pages 217–242. Nagoya Univ., Nagoya, 1986.

[Rib90] K.A. Ribet. On modular representations of Gal($\bar{Q}/Q$) arising from modular forms. *Inventiones mathematicae*, 100(2):431–476, 1990.

[Ser03] Jean-Pierre Serre. *Trees*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2003. Translated from the French original by John Stillwell, Corrected 2nd printing of the 1980 English translation.

[Shi94] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume 11 of *Publications of the Mathematical Society of Japan*. Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original, Kanô Memorial Lectures, 1.

[Sug17] Kennichi Sugiyama. Zeta functions of Ramanujan graphs and modular forms. *Comment. Math. Univ. St. Pauli*, 66(1-2):29–43, 2017.

[Sun86] Toshikazu Sunada. L-functions in geometry and some applications. In *Curvature and topology of Riemannian manifolds (Katata, 1985)*, volume 1201 of *Lecture Notes in Math.*, pages 266–284. Springer, Berlin, 1986.

[Ter11] Audrey Terras. *Zeta functions of graphs*, volume 128 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2011. A stroll through the garden.

[Voi21] John Voight. *Quaternion algebras*, volume 288 of *Graduate Texts in Mathematics*. Springer, Cham, [2021] ©2021.

[Zyw21] David Zywina. Computing actions on cusp forms, 2021.

KU Leuven, Leuven, Belgium
Email address: junbo.lau@kuleuven.be

Virginia Tech, Blacksburg, Virginia, USA
Email address: tmo@vt.edu
URL: travismo.github.io

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

University of Georgia, Athens, Georgia
Email address: gabrielle.scullard@uga.edu

Google
Email address: lukas.zobernig@gmail.com