Ordinary isogeny graphs with level structure

Derek Perrin and José Felipe Voloch

Abstract. We study ℓ-isogeny graphs of ordinary elliptic curves defined over $\mathbb{F}_q$ with an added level structure. Given an integer N coprime to p and ℓ, we look at the graphs obtained by adding $\Gamma_0(N)$, $\Gamma_1(N)$, and $\Gamma(N)$-level structures to volcanoes. Given an order $\mathcal{O}$ in an imaginary quadratic field K, we look at the action of generalized ideal class groups of $\mathcal{O}$ on the set of elliptic curves whose endomorphism rings are $\mathcal{O}$ along with a given level structure. We show how the structure of the craters of these graphs is determined by the choice of parameters.

1 Introduction

The set of isomorphism classes of elliptic curves over a finite field $\mathbb{F}_q$ can be viewed as vertices of a graph known as the isogeny graph. Vertices E and E' are connected by a directed edge (E, E') if and only if there exists an isogeny $\varphi : E \to E'$. Advancements in quantum computing have motivated the search for new cryptographic primitives which are resistant to quantum-style attacks. The search for problems which are computationally difficult for quantum adversaries gave birth to what is known as *isogeny-based cryptography* [3]. Given two vertices E and E', the underlying hard problem of isogeny-based cryptography is that of finding a path from E to E' in the isogeny graph.

Cryptographic applications of isogenies has attracted more attention to studying them. One such development in the field of isogenies has been to look at adding a level N structure to the isogeny graph. This graph consists of vertices of the form (E, γ) where γ is some level N structure on E, and there is an edge between two vertices $(E, \gamma), (E', \gamma')$ if and only if there exists an isogeny $\varphi : E \to E'$ with the added condition that $\varphi(\gamma) = \gamma'$. Isogeny graphs with level N structure were first studied by Roda in [14] in which they looked at adding a full level N structure to the supersingular component of the ℓ-isogeny graph. Following Roda, further works have also studied adding level structure to the supersingular component; see [1, 12]. Additionally, during the writing of this article, Arpin, Castryck, Eriksen, Lorenzon, and Vercauteren [2] published results involving generalized class group actions on oriented elliptic curves with level structure. Prior to that, Colò [4] pointed out that the action of the ideals on elliptic curves with level structure factors through a ray class group.

Parallel to these developments, the isogeny graphs for ordinary elliptic curves was studied, motivated by problems in computational number theory. Kohel [10] showed that the ordinary components have a nice "volcano" structure, where the term volcano was later coined by Fouquet and Morain [8] to describe the components due to their similarities to geological volcanoes. Sutherland [16] provides a summary of various algorithms, including computing the endomorphism ring of ordinary elliptic curves, which make use of volcanoes.

Due to their applications in cryptography, the supersingular setting has received more attention and the ordinary setting is not as well-studied. However, recent work by Lei and Müller [11] studies ordinary isogeny graphs with a $\Gamma_1(Np^m)$-level structure. Our work differs as we will consider ordinary isogeny graphs with $\Gamma_0(N)$, $\Gamma_1(N)$, and $\Gamma(N)$-level structures.

The viewpoint of our work is more mathematical in nature, and we will not discuss cryptographic applications here. For use of level structures in cryptography, the interested reader is recommended to look at [6, 9]. This article aims to answer a question first raised by Levin [12], namely that of determining the crater size and number of components of the graphs constructed by adding various level structures to an ordinary component of the ℓ-isogeny graph.

The theory of complex multiplication (CM) tells us that for an order $\mathcal{O}$ in an imaginary quadratic field K, the ideal class group $Cl(\mathcal{O})$ acts simply transitively on the set

$$\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q) = \left\{ E/\mathbb{F}_q \mid \mathrm{End}(E) \simeq \mathcal{O} \right\} / \overline{\mathbb{F}_q}\text{-isomorphism}$$

of ordinary elliptic curves whose endomorphism rings are isomorphic to $\mathcal{O}$ modulo $\overline{\mathbb{F}_q}$-isomorphism. The main contribution of this work can be thought of as a generalization of this group action. We address Levin's question by considering generalized ideal class groups acting on $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$ endowed with various level structures. For $\mathfrak{l}$ a prime $\mathcal{O}$-ideal above ℓ, we show that the crater size of components with a level structure is related to the order of the subgroup $\langle \mathfrak{l}, \bar{\mathfrak{l}} \rangle$ when viewed as a subgroup of a generalized class group. In Section 5, we give descriptions of these class groups for $\Gamma_0(N)$, $\Gamma_1(N)$, and $\Gamma(N)$-level structures. We also show the role the prime factorization of N as an $\mathcal{O}$-ideal plays in both the number and size of the components of these graphs with level structure. In Section 6, we conclude by showing several examples of adding $\Gamma_0(N)$ and $\Gamma_1(N)$-level structures to an isogeny volcano.

2 Background

Definition 2.1   Let $\mathbb{F}_q$ be a finite field of characteristic $p \neq 2, 3$ and ℓ a prime different from p. Recall that the set of $\overline{\mathbb{F}_q}$-isomorphism classes of elliptic curves over $\mathbb{F}_q$ can be identified with $\mathbb{F}_q$ via the j-invariant. We let $X_\ell(\mathbb{F}_q)$ denote the ℓ-*isogeny graph of* $\mathbb{F}_q$ where $X_\ell(\mathbb{F}_q)$ has vertex set $\mathbb{F}_q$. Each vertex represents an isomorphism class of elliptic curves defined over $\mathbb{F}_q$. The edge set of $X_\ell(\mathbb{F}_q)$ consists of pairs (j_1, j_2) where j_1, j_2 are j-invariants of elliptic curves which are $\overline{\mathbb{F}_q}$-isogeneous via an isogeny of degree ℓ.

The field we work with will generally be understood to be $\mathbb{F}_q$, so we will write X_ℓ instead of $X_\ell(\mathbb{F}_q)$. Unless otherwise stated, we will treat X_ℓ as an undirected graph since given an isogeny $\varphi : E \to E'$ of degree ℓ, there exists a dual isogeny $\hat{\varphi} : E' \to E$ of degree ℓ such that $\varphi \circ \hat{\varphi} = \hat{\varphi} \circ \varphi = [\ell]$.

For the purposes of this article, we will focus our attention on the ordinary components, volcanoes, of X_ℓ.

Definition 2.2 An *ℓ-volcano* is a connected, undirected graph whose vertices may be partitioned into one or more levels $V_0, \dots, V_d$ such that:

(i)   The subgraph on V_0 is a regular connected graph of degree at most 2.

(ii) For each $i > 0$, the vertices in V_i have exactly one neighbour in V_{i-1} and the subgraph on V_i is totally disconnected.

(iii) For each $i < d$, the vertices in V_i have degree $\ell + 1$.

Definition 2.3 Let G_ℓ be an ℓ-isogeny volcano of X_ℓ. The subgraph of level zero on G_ℓ is called the *crater of G_ℓ* and is denoted C_ℓ and the subgraph of X_ℓ consisting of the craters of all ordinary components will be denoted $\mathcal{C}_\ell$ and is called the *crater of X_ℓ*.

The term *crater* was introduced in [8] and strictly refers to the level zero subgraph of a single volcano. Some definitions of a volcano [7] require the crater to consist of a cycle, but we do not require this in our work and use a definition as in [16]. Many of the graphs we work with contain multiple components with a volcanic structure, so it makes sense to discuss the craters of all of X_ℓ. This terminology is consistent with what the authors of [11] use.

We can now add an additional structure to the ordinary components of X_ℓ. The structure we impose is called a *level structure* and it is related to the N-torsion subgroup $E[N]$ of an elliptic curve E.

Definition 2.4 Let $E/\mathbb{F}_q$ be an elliptic curve, N an integer, and $E[N]$ the group of N-torsion points of E. Then we call

(1) a *$\Gamma_0(N)$-level structure* a cyclic subgroup $\langle P \rangle \subseteq E[N]$ of order N;

(2) a *$\Gamma_1(N)$-level structure* a point $P \in E[N]$ of order N;

(3) and a *$\Gamma(N)$-level structure*, or *full level structure*, an ordered pair of points P, $Q \in E[N]$ which are a basis for $E[N]$.

In this article, we will always assume N is an integer coprime to p and ℓ.

Definition 2.5 Consider the set of pairs (E, γ) where E is an ordinary elliptic curve and γ is a level structure on E. Then we may define an equivalence relation $\sim$ on pairs (E, γ), where $(E, \gamma) \sim (E', \gamma')$ if and only if there exists an isomorphism $\varphi : E \to E'$ such that $\varphi(\gamma) = \gamma'$.

Note that if $\varphi \in \mathrm{Aut}(E)$, then (E, γ) is equivalent to $(E, \varphi(\gamma))$. In particular this applies to $[-1]$.

We add a level structure to X_ℓ by adding the level structure to each vertex in X_ℓ up to the equivalence relation $\sim$ in Definition 2.5.

Definition 2.6   Let G_ℓ be an isogeny volcano with vertex set $\mathbb{V} = E_i$. Up to the equivalence relation in Definition 2.5, consider the set of tuples

$$\mathbb{V}' = \left\{ (E_i, \gamma_i) \mid \forall E_i \in \mathbb{V} \text{ where } \gamma_i \text{ is a level structure on } E_i \right\} / \sim$$

and the set of tuples

$$\mathbb{E}' = \big\{ ((E_i, \gamma_i), (E_j, \gamma_j)) \text{ if } \exists \varphi : E_i \to E_j \text{ such that } \deg \varphi = \ell$$
$$\text{and } \varphi(\gamma_i) = \varphi(\gamma_j) \big\} / \sim .$$

Then

(i)   if the γ_i are all $\Gamma_0(N)$ level structures on the E_i's, we let $G_{\ell,0}(N)$ denote the graph whose vertex set is $\mathbb{V}'$ and edge set is $\mathbb{E}'$;

(ii)   if the γ_i are all $\Gamma_1(N)$ level structures on the E_i's, we let $G_{\ell,1}(N)$ denote the graph whose vertex set is $\mathbb{V}'$ and edge set is $\mathbb{E}'$;

(iii)   if the γ_i are all $\Gamma(N)$ level structures on the E_i's, we let $G_\ell(N)$ denote the graph whose vertex set is $\mathbb{V}'$ and edge set is $\mathbb{E}'$.

We will say we *add a γ level structure to G_ℓ* when we construct one of the graphs in Definition 2.6. We also remark that while $G_{\ell,0}(N)$ remains undirected, the graphs $G_{\ell,1}(N)$ and $G_\ell(N)$ in Definition 2.6 are no longer undirected graphs.

3   Stabilizers of level structures

In this section, we will discuss the stabilizers of the $\Gamma_0(N)$, $\Gamma_1(N)$, and $\Gamma(N)$-level structures.

     We will let K be an imaginary quadratic field with ring of integers given by $\mathcal{O}_K$. We are interested in ordinary elliptic curves with CM by an order $\mathcal{O} \subseteq \mathcal{O}_K$ where $\mathcal{O} = \mathbb{Z}[\Phi]$ for some $\Phi \in \mathcal{O}_K$; in other words, their endomorphism ring is equal to $\mathcal{O}$. We will restrict ourselves to the case of $(f, N) = 1$ where f is the conductor of $\mathcal{O}$ (i.e., $f = [\mathcal{O}_K : \mathcal{O}]$). Finally, we will assume that all elliptic curves we work with have j-invariant not equal to $0, 1728$.

Definition 3.1   Let γ be a $\Gamma_0(N)$, $\Gamma_1(N)$, or $\Gamma(N)$-level structure on an ordinary elliptic curve E. A *stabilizer of γ* is an element α of $\mathcal{O}/N\mathcal{O}$ where $(E, \gamma) \sim (E, \alpha(\gamma))$ where $\sim$ is the equivalence relation defined in Definition 2.5. The set $\mathrm{Stab}(\gamma)$ of stabilizers of γ form a subgroup of $(\mathcal{O}/N\mathcal{O})^\times$.

Lemma 3.1   *The N-torsion subgroup $E[N]$ and $\mathcal{O}/N\mathcal{O}$ are isomorphic as $\mathcal{O}/N\mathcal{O}$-modules.*

Proof   A proof when $\mathcal{O} = \mathcal{O}_K$ is given in [15, Proposition II.1.4]. For $\mathcal{O}$ a non-maximal order, a proof is given in [2, Section 3.1 Lemma 1 pg 7]   ∎

     The importance of Theorem 3.1 is that it allows us to work with a somewhat simpler structure as we will shortly see. For the three level structures $\Gamma(N)$, $\Gamma_1(N)$, and $\Gamma_0(N)$, we are interested in stabilizers of all of $E[N]$, points $P \in E[N]$ of order N,

and cyclic subgroups $\langle P \rangle \subseteq E[N]$ of order N respectively. The authors of [9] find the stabilizers of a $\Gamma(N)$-level structure by considering subgroups of the kernel of an isogeny which fixes all of $E[N]$; this method can be adapted for $\Gamma_1(N)$ and $\Gamma_0(N)$-level structures, but one needs to take into consideration eigenvectors of Φ. We instead look at the equivalent problem of finding stabilizers for all of $\mathcal{O}/N\mathcal{O}$, elements $\alpha \in \mathcal{O}/N\mathcal{O}$ of order N, and cyclic subgroups $\langle \alpha \rangle \subseteq \mathcal{O}/N\mathcal{O}$ of order N respectively.

Proposition 3.2 *The stabilizers of a $\Gamma(N)$-level structure are given by*

$$\text{Stab}(\mathcal{O}/N\mathcal{O}) = \{\alpha \in (\mathcal{O}/N\mathcal{O})^\times \mid \alpha \equiv \pm 1 \mod N\mathcal{O}\}.$$

Proof Due to the equivalence relation in Definition 2.5, we trivially have $\alpha \equiv \pm 1$ mod $N\mathcal{O}$. ∎

Let $\tilde{P} \in E[N]$ be a $\Gamma_1(N)$-level structure. After choosing a generator of $E[N]$ as an $\mathcal{O}/N\mathcal{O}$-module, then by Theorem 3.1 we may identify $\tilde{P}$ with an element $P \in \mathcal{O}/N\mathcal{O}$. In what follows, we will work with P instead of $\tilde{P}$.

Proposition 3.3 *Given $P \in \mathcal{O}/N\mathcal{O}$ of order N and the ideal $\mathfrak{a} = \langle P, N\mathcal{O} \rangle$, then*

$$\text{Stab}(P) = \left\{\alpha \in (\mathcal{O}/N\mathcal{O})^\times \mid \alpha \equiv \pm 1 \mod \mathfrak{a}^{-1}N\mathcal{O}\right\}.$$

Proof Let $\alpha \in \text{Stab}(P)$. Then

$$\alpha P \equiv \pm P \mod N\mathcal{O}$$
$$(\alpha \pm 1)P \equiv 0 \mod N\mathcal{O}.$$

Then $(\alpha \pm 1)P \in N\mathcal{O}$. For any element $\beta = aP + bN \in \mathfrak{a}$ for $a, b \in \mathcal{O}$, consider the product

$$(\alpha \pm 1)\beta = (\alpha \pm 1)(aP + bN)$$
$$= a(\alpha \pm 1)P + b(\alpha \pm 1)N.$$

We have shown the first term is in $N\mathcal{O}$, and the second term is certainly in $N\mathcal{O}$, so their sum is in $N\mathcal{O}$. Then $(\alpha \pm 1)\mathfrak{a} \subseteq N\mathcal{O}$, and so $(\alpha \pm 1) \in \mathfrak{a}^{-1}N\mathcal{O}$, and $\text{Stab}(P) \subseteq \left\{\alpha \in \mathcal{O}/N\mathcal{O} \mid \alpha \equiv \pm 1 \mod \mathfrak{a}^{-1}N\mathcal{O}\right\}$. The reverse containment is clear. ∎

Proposition 3.4 *Let $G = \langle P \rangle$ be a $\Gamma_0(N)$-level structure and $\mathfrak{a} = \langle P, N\mathcal{O} \rangle$ the smallest ideal containing P and N. Then*

$$\text{Stab}(G) = \left\{\alpha \in (\mathcal{O}/N\mathcal{O})^\times \mid \alpha \equiv c \mod \mathfrak{a}^{-1}(N) \text{ for } c \in \mathbb{Z}, (c, N) = 1\right\}.$$

Proof Let $\alpha G = G$. Then $\alpha P = P'$ where $G = \langle P' \rangle$. Since G is cyclic of order N, we must have $P' = cP$ for some c coprime to N. The rest of the proof follows as Theorem 3.3 but by replacing the requirement of $\alpha \equiv \pm 1$ mod $\mathfrak{a}^{-1}N\mathcal{O}$ with $\alpha \equiv c$ mod $\mathfrak{a}^{-1}N\mathcal{O}$ where c is an integer coprime to N. ∎

Remark 3.5 The above propositions can be modified to work for j-invariants 0 and 1728 by considering congruences modulo a 6th or 4th root of unity respectively.

4 Adding level structure to isogeny graphs

This section will be organized into three subsections where we will look at ordinary ℓ-isogeny graphs with the three types of level structures. We are particularly interested in how the choice of N affects the size and number of components when adding level structure. In what follows, we will let $\mathcal{O}$ be an order in an imaginary quadratic field K. Rather than look at the entire isogeny graph, we will focus our attention on the connected components (i.e., volcanoes), and in particular, their craters. We will let G_ℓ be such a component whose crater C_ℓ consists of isomorphism classes of elliptic curves whose endomorphism rings are equal to $\mathcal{O}$. Further, we will restrict ourselves to only working with elliptic curves whose j-invariants are not 0 or 1728 to avoid automorphism groups different from $\{\pm 1\}$. As usual, we will let N be a positive integer coprime to p, ℓ, and the conductor of $\mathcal{O}$.

Lemma 4.1   *Let G_ℓ be an isogeny volcano with n vertices.*

(i)   *The graph $G_{\ell,0}(N)$ has*

$$nN \prod_{p|N} \left(1 + \frac{1}{p}\right)$$

vertices.

(ii)   *If $N > 2$, the graph $G_{\ell,1}(N)$ has*

$$\frac{nN\phi(N)}{2} \prod_{p|N} \left(1 + \frac{1}{p}\right)$$

vertices and $3n$ if $N = 2$.

(iii)   *If $N > 2$, the graph $G_\ell(N)$ has*

$$\frac{nN^2\phi(N)^2}{2} \prod_{p|N} \left(1 + \frac{1}{p}\right)$$

vertices and $6n$ if $N = 2$.

where ϕ is Euler's totient function.

Proof   For each case, we proceed by counting the number of level structures which can be added to each vertex in G_ℓ.

We begin by proving (ii). Since $E[N] \simeq \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ and $N = \prod p_i^{e_i}$, then by the Chinese remainder theorem we may write

(4.1) $E[N] \simeq \left(\mathbb{Z}/p_1^{e_1}\mathbb{Z}\right)^2 \times \left(\mathbb{Z}/p_2^{e_2}\mathbb{Z}\right)^2 \times \cdots \times \left(\mathbb{Z}/p_r^{e_r}\mathbb{Z}\right)^2.$

An element P of $E[N]$ has maximal order N if and only if it has maximal order in each of factors on the right-hand side of (4.1), and so it is sufficient to find the number of elements of maximal order of each factor of $E[N]$. An element (a, b) of $(\mathbb{Z}/p_i^{e_i})^2$ is of maximal order if either $(a, p_i^{e_i}) = 1$ or $(b, p_i^{e_i}) = 1$. There are $\phi(p_i^{e_i})p_i^{e_i}$ pairs where a is coprime to $p_i^{e_i}$ and $\phi(p_i^{e_i})(p_i^{e_i} - \phi(p_i^{e_i}))$ pairs where b is coprime to $p_i^{e_i}$ and a is not. Some algebraic manipulation shows there are a total of $p_i^{2e_i} - p_i^{2(e_i - 1)}$ such elements

of maximal order in $(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^2$. We repeat this for each prime power factor of N and by the Chinese remainder theorem we may take their product to get

$$(4.2) \qquad N\phi(N)\prod_{p|N}\left(1+\frac{1}{p}\right)$$

total points of order N. If $N = 2$, then $P = -P$ for any point P and so we may substitute $N = 2$ into (4.2) to get a scaling factor of 3. Otherwise, if $N > 2$, then we must divide the result of (4.2) by 2 due to identifying P with $-P$.

To prove (i), we use the fact that any cyclic subgroup $\langle P \rangle \subseteq E[N]$ of order N has $\phi(N)$ elements with order N. We may therefore partition the elements P of order N into equivalence classes where $P \sim P'$ if there exists an integer k such that $P' = kP$. From (ii), we have that there are

$$N\phi(N)\prod_{p|N}\left(1+\frac{1}{p}\right)$$

elements of order N in $E[N]$. Dividing by $\phi(N)$ the size of each partition, we see there are

$$N\prod_{p|N}\left(1+\frac{1}{p}\right)$$

such equivalence classes, and therefore subgroups, of order N.

To prove (iii), we first work with a factor $(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^2$ of (4.1). The result of (ii) gives us the number of ways to choose a first basis point P. The restrictions on choosing a second basis point Q is that it must be of order $p_i^{e_i}$ and it cannot be congruent to a scalar multiple of P modulo p_i. The congruence requirement arises from the fact that $\mathbb{Z}/p_i^{e_i}\mathbb{Z}$ is local at p_i. From (ii), we know there are $\phi(p_i^{e_i})$ elements of order $p_i^{e_i}$ in $\langle P \rangle$ and that each of those elements is congruent to $p_i^{e_i-1}$ distinct elements of order $p_i^{e_i}$. This gives a total of $\phi(p_i^{e_i})(p_i^{e_i}+p_i^{e_i-1})-\phi(p_i^{e_i})p_i^{e_i-1}=p_i^{e_i}\phi(p_i^{e_i})$ choices for Q. Taking the product over all p_i by the Chinese remainder theorem gives

$$(4.3) \qquad N^2\phi(N)^2\prod_{p|N}\left(1+\frac{1}{p}\right)$$

choices of bases. If $N = 2$, then $P = -P$ and $Q = -Q$ for any choice of P, Q, and so substituting $N = 2$ into (4.3) gives a scaling factor of 6. If $N > 2$, we divide (4.3) by 2 due to identifying the pair (P, Q) with $(-P, -Q)$. ∎

The graphs of Definition 2.6 consist of components which are each a covering graph of G_ℓ. The crater C_ℓ is the defining characteristic of G_ℓ, so the following work will only discuss craters unless otherwise stated.

Definition 4.1 Let G_ℓ be an isogeny volcano and $G_{\ell,0}(N)$, $G_{\ell,1}(N)$, and $G_\ell(N)$ the graphs obtained as described in Definition 2.6. Then

(i) $C_{\ell,0}(N)$ denotes the subgraph of $G_{\ell,0}(N)$ whose components are obtained by adding a $\Gamma_0(N)$-level structure to C_ℓ;

(ii) $C_{\ell,1}(N)$ denotes the subgraph of $G_{\ell,1}(N)$ whose components are obtained by adding a $\Gamma_1(N)$-level structure to C_ℓ; and,

(iii) $C_\ell(N)$ denotes the subgraph of $G_\ell(N)$ whose are obtained by adding a $\Gamma(N)$-level structure to C_ℓ.

For lack of a better term, we will refer to the graphs $C_{\ell,0}(N)$, $C_{\ell,1}(N)$, and $C_\ell(N)$ as the *craters* of $G_{\ell,0}(N)$, $G_{\ell,1}(N)$, and $G_\ell(N)$ respectively. The reader should note that since the graphs $G_{\ell,1}(N)$ and $G_\ell(N)$ are directed, their craters do not look like craters of standard isogeny volcanoes.

Let $\mathfrak{l}$ be a prime $\mathcal{O}$-ideal above ℓ. If ℓ is an inert prime, then $\mathfrak{l}$ does not induce a degree ℓ isogeny and C_ℓ is totally disconnected. Adding a level structure does not change these craters. As such, for the remainder of this article we will only concern ourselves with primes ℓ which either split or ramify. From [10], we know the size of C_ℓ is equal to the order n of $[\mathfrak{l}]$ in the class group $Cl(\mathcal{O})$. In particular, we have $\mathfrak{l}^n = \lambda\mathcal{O}$ and $\bar{\mathfrak{l}}^n = \bar{\lambda}\mathcal{O}$ for some $\lambda, \bar{\lambda} \in \mathcal{O}^\times$ where $\mathfrak{l} = \bar{\mathfrak{l}}$ if ℓ is ramified.

4.1   Crater graphs $C_{\ell,0}(N)$

We will begin by looking at the components with a $\Gamma_0(N)$-level structure. Let E be an elliptic curve on a crater C_ℓ.

Definition 4.2   Let G be a $\Gamma_0(N)$-level structure of E. Then $v = (E, G)$ is a vertex on some component $\mathcal{C}_{\ell,0}(N) \subseteq C_{\ell,0}(N)$. We say a vertex $v' \in \mathcal{C}_{\ell,0}(N)$ is a Γ_0-*principal vertex of v* if v' is of the form (E, G') for some $G' \subseteq E[N]$ of order N.

A crater C_ℓ can be described by the behavior of ℓ in its class group. If ℓ splits as a product of non-principal ideals, the crater is a cycle of length equal to the order of a prime $\mathfrak{l}$ above ℓ in its class group. If ℓ splits as a product of principal ideals, the crater consists of a single vertex with two loops. If ℓ ramifies as a non-principal ideal, then the crater consists of an edge, and if ℓ ramifies as a principal ideal, then the crater is a single vertex with a loop. The following lemma and theorem are independent of the behavior of ℓ in its class group.

Lemma 4.2   *Let $v = (E, G)$ be a vertex on $\mathcal{C}_{\ell,0}(N) \subseteq C_{\ell,0}(N)$. If $v' = (E, G')$ is a Γ_0-principal vertex of v, then there exists an endomorphism $\alpha \in \mathrm{End}(E)$ such that $\alpha(G) = G'$. Furthermore, there exists some positive integer d such that $\mathfrak{l}^d = \alpha\mathcal{O}$.*

Proof   Any edge of $\mathcal{C}_{\ell,0}(N)$ represents an isogeny induced by $\mathfrak{l}$ which has finite order n in $Cl(\mathcal{O})$. Since v, v' are on the same component, the path connecting them is the isogeny $\varphi_{\mathfrak{l}^d}$ induced by $\mathfrak{l}^d$ for some d. This isogeny must be induced by a principal ideal $\alpha\mathcal{O}$ since $\varphi_{\mathfrak{l}^d} : E \to E$, and so $\mathfrak{l}^d = \alpha\mathcal{O}$ where $n \mid d$.   ∎

It is now clear why we use the term *principal vertex* in Definition 4.2: paths from a vertex v to a principal vertex arise from principal ideals. Theorem 4.2 tells us the size of a component $\mathcal{C}_{\ell,0}(N) \subseteq C_{\ell,0}(N)$ is equal to the order n of $[\mathfrak{l}]$ in the class group scaled by the number of principal vertices for some fixed vertex v.

Given $\mathfrak{a}$ an $\mathcal{O}$-ideal, we will let $\phi_{\mathcal{O}}(\mathfrak{a})$ denote the size of the residue ring $(\mathcal{O}/\mathfrak{a})^{\times}$. This can be thought of as a generalized version of Euler's totient function. A standard result [13, Theorem 1.19] gives

$$(4.4) \qquad \phi_{\mathcal{O}}(\mathfrak{a}) = \mathcal{N}(\mathfrak{a}) \prod_{\mathfrak{p}|\mathfrak{a}} \left(1 - \frac{1}{\mathcal{N}(\mathfrak{p})}\right),$$

where $\mathcal{N}(\mathfrak{a})$ denotes the norm of $\mathfrak{a}$. We will let $\phi_{\mathcal{O}}$ denote the totient function on $\mathcal{O}$-ideals and ϕ denote the usual Euler totient function. We remark that $\phi(N) \neq \phi_{\mathcal{O}}(N\mathcal{O})$ as the right-hand side depends on how the (rational) prime factors of N behave in $\mathcal{O}$ while the left-hand side only depends on the (rational) prime factorization of N.

Theorem 4.3 *Let $v = (E, G)$ be a vertex on a component $\mathcal{C}_{\ell,0}(N) \subseteq C_{\ell,0}(N)$ where $G = \langle P \rangle$ and let $\mathfrak{a} = (P, N)$ be the $\mathcal{O}$-ideal generated by P and N. Recall that λ was defined by $\mathfrak{l}^n = \lambda \mathcal{O}$. Then $\#\mathcal{C}_{\ell,0}(N) = nm_{\mathfrak{a}}$ where $m_{\mathfrak{a}}$ is the order of the natural projection of λ in $(\mathcal{O}/N\mathcal{O})^{\times}/\mathrm{Stab}(G)$. Further, $C_{\ell,0}(N)$ contains $\frac{\phi_{\mathcal{O}}(\mathfrak{a}^{-1}N\mathcal{O})}{\phi(N)m_{\mathfrak{a}}}$ components isomorphic to $\mathcal{C}_{\ell,0}(N)$.*

Proof We first note that any component $\mathcal{C}_{\ell,0}(N)$ of $C_{\ell,0}(N)$ will have a crater whose size is divisible by the order n of $\mathfrak{l}$ in $Cl(\mathcal{O})$. Using this fact combined with Theorem 4.2, it suffices to know how many principal vertices exist for some fixed vertex v. Since paths between principal vertices correspond to principal ideals of the form $\lambda^k \mathcal{O}$ for some $k \in \mathbb{Z}$, we need to find the smallest k such that $\lambda^k G = G$ to determine the component sizes. Theorem 3.4 tells us the stabilizers of G, and so the number of principal vertices of v is simply the order of the natural projection of λ in $(\mathcal{O}/N\mathcal{O})^{\times}/\mathrm{Stab}(G)$.

To prove the second claim, observe that $\mathfrak{a}$ is the smallest ideal containing P and N, so by the isomorphism in Theorem 3.1, the image of P under the natural projection is in $(\mathcal{O}/\mathfrak{a}^{-1}N\mathcal{O})^{\times}$. By (4.4), the ring $(\mathcal{O}/\mathfrak{a}^{-1}N\mathcal{O})$ contains $\phi_{\mathcal{O}}(\mathfrak{a}^{-1}N\mathcal{O})$ such elements, one of which is the image of P. For a cyclic group G of order N, there are $\phi(N)$ elements of order N, and so we may partition these $\phi_{\mathcal{O}}(\mathfrak{a}^{-1}N\mathcal{O})$ elements whereby two points are equivalent if and only if they generate the same cyclic group. The result follows since any component contains $m_{\mathfrak{a}}$ such cyclic subgroups belonging to $E[N]$. ∎

A consequence of Theorems 4.2 and 4.3 is that if ℓ decomposes as a product of principal ideals, then the crater may consist of a cycle rather than loops when adding a $\Gamma_0(N)$ level structure.

By Theorem 4.3, we can determine the components (and thus all) of $G_{\ell,0}(N)$ by considering all ideals (including all of $\mathcal{O}$) $\mathfrak{a}$ dividing $N\mathcal{O}$ along with the condition that $N \mid \mathcal{N}(\mathfrak{a}^{-1}N)$, and looking at the order $m_{\mathfrak{a}}$ of the projection of λ in $(\mathcal{O}/\mathfrak{a}^{-1}N\mathcal{O})^{\times}$ divided by the index $[(\mathcal{O}/\mathfrak{a}^{-1}N\mathcal{O})^{\times} : (\mathbb{Z}/N\mathbb{Z})^{\times}]$. The divisibility condition on $\mathcal{N}(\mathfrak{a}^{-1}N)$ arises from the fact that P must generate a cyclic group of order N. Equivalently, we can determine $G_{\ell,0}(N)$ by considering each $\Gamma_0(N)$-level structure and applying Theorem 4.3 directly.

If we only consider the case where N is a rational prime, the situation is simpler and we can describe component sizes of $C_{\ell,0}(N)$.

Corollary 4.4 *Let N be a prime different from ℓ and p and let m denote the order of the natural projection of λ in $(\mathcal{O}/N\mathcal{O})^{\times}/(\mathbb{Z}/N\mathbb{Z})^{\times}$. Then $C_{\ell,0}(N)$ consists of one of the following:*

(i)   *If N is inert, then $C_{\ell,0}(N)$ contains $\frac{N+1}{m}$ components each of size nm.*

(ii)   *If $N\mathcal{O} = \mathfrak{N}_1\mathfrak{N}_2$, then $C_{\ell,0}(N)$ contains $\frac{N-1}{m}$ components each of size nm and two components of size n.*

(iii)   *If $N\mathcal{O} = \mathfrak{N}^2$, then $C_{\ell,0}(N)$ contains $\frac{N}{m}$ components each of size nm and one component of size n.*

Proof   These are all special cases of Theorem 4.3.

To prove (i), observe that $\mathcal{O}/N\mathcal{O}$ is isomorphic to a finite field of order N^2, and so for any P of order N, we have $\mathfrak{a} = (P, N) = \mathcal{O}$. Then $\#(\mathcal{O}/N)^{\times} = N^2 - 1$ and $\mathrm{Stab}(G) = (\mathbb{Z}/N\mathbb{Z})^{\times}$ for any G. By Theorem 4.3, $\mathcal{C}_{\ell,0}(N)$, contains $\frac{N^2-1}{m(N-1)}$ components each of size nm. To prove (ii), we first observe that $|(\mathcal{O}/N\mathcal{O})^{\times}| = (N-1)^2$ and that $\mathfrak{a} \in \{\mathfrak{N}_1, \mathfrak{N}_2, \mathcal{O}\}$. If $\mathfrak{a} = \mathfrak{N}_1$ or $\mathfrak{N}_2$, then by Theorem 4.3 we can determine the corresponding components by computing the order of the projection of λ in $(\mathcal{O}/\mathfrak{a}^{-1}N\mathcal{O})^{\times}/(\mathbb{Z}/N\mathbb{Z})^{\times}$, but this is the trivial group, and so we obtain two components each of size n. If $\mathfrak{a} = \mathcal{O}$, then G has a generator corresponding to an element of $(\mathcal{O}/N\mathcal{O})^{\times}$, and so there are $\frac{(N-1)^2}{m(N-1)}$ components each of size nm. To prove (iii), we proceed as in the split case but set $\mathfrak{N}_1 = \mathfrak{N}_2 = \mathfrak{N}$ and observe that $|(\mathcal{O}/N\mathcal{O})^{\times}| = N^2 - N$. If $\mathfrak{a} = \mathfrak{N}$, then $(\mathcal{O}/\mathfrak{a}^{-1}N\mathcal{O})^{\times} = (\mathcal{O}/\mathfrak{N})^{\times} \simeq (\mathbb{Z}/N\mathbb{Z})^{\times}$ and so we obtain one component of size n. If $\mathfrak{a} = \mathcal{O}$, then we obtain $\frac{N^2-N}{m(N-1)} = \frac{N}{m}$ components of size nm.   ∎

4.2   Crater graphs $C_{\ell,1}(N)$

Definition 4.3   *Let P be a $\Gamma_1(N)$-level structure of E. Then $v = (E, P)$ is a vertex on some component $\mathcal{C}_{\ell,1}(N) \subseteq C_{\ell,1}(N)$. We say a vertex $v' \in \mathcal{C}_{\ell,1}(N)$ is a Γ_1-principal vertex of v if it is of the form (E, P') for some $P' \in E[N]$ of order N.*

Lemma 4.5   *Let $v = (E, P)$ be a vertex on $\mathcal{C}_{\ell,1}(N) \subseteq C_{\ell,1}(N)$. If $v' = (E, P')$ is a Γ_1-principal vertex of v, then there exists an endomorphism $\alpha \in \mathrm{End}(E)$ such that $\alpha(P) = \pm P'$. Furthermore, there exists some ideal $\mathfrak{b}$ in the group $\langle \mathfrak{l}, \bar{\mathfrak{l}} \rangle$ such that $\mathfrak{b} = \alpha\mathcal{O}$.*

Proof   Any edge of $\mathcal{C}_{\ell,1}(N)$ arises from an isogeny induced by $\mathfrak{l}$ or $\bar{\mathfrak{l}}$. Since $C_{\ell,1}(N)$ is a directed graph, then an isogeny induced by $\bar{\mathfrak{l}}$ does not necessarily represent a reverse edge to that arising from $\mathfrak{l}$ as in the case of G_ℓ or $G_{\ell,0}(N)$. Any isogeny mapping v to v' must be an endomorphism since it maps a point P on E to a point P' which also lies on E and thus proves the first claim. α be such an endomorphism.

Any path between principal vertices is the result of an isogeny induced by some ideal $\mathfrak{b}$ belonging to the group $\langle \mathfrak{l}, \bar{\mathfrak{l}} \rangle$. Since v and v' are on the same component, they are connected by a path arising from $\mathfrak{b}$ where $\mathfrak{b} = \alpha\mathcal{O}$.   ∎

Theorem 4.6 *Let $v = (E, P)$ be a vertex on a component $\mathcal{C}_{\ell,1}(N) \subseteq C_{\ell,1}(N)$ where $P \in E[N]$ is of order N, and let $\mathfrak{a} = (P, N)$ be the $\mathcal{O}$-ideal generated by P and N. Then $\#\mathcal{C}_{\ell,1}(N) = nm_{\mathfrak{a}}$ where $m_{\mathfrak{a}}$ is the order of the group generated by the natural projections of λ, $\overline{\lambda}$ in $(\mathcal{O}/N\mathcal{O})^{\times}/\operatorname{Stab}(P)$. Further, $C_{\ell,1}(N)$ contains $\frac{\phi_{\mathcal{O}}(\mathfrak{a}^{-1}N\mathcal{O})}{2m_{\mathfrak{a}}}$ components isomorphic to $\mathcal{C}_{\ell,1}(N)$.*

Proof The proof follows that of Theorem 4.3, but with making the necessary change in stabilizer subgroup and utilizing Theorem 4.5. As observed in Theorem 4.5, we must look at the group generated by the natural projections of λ, $\overline{\lambda}$ since $C_{\ell,1}(N)$ is a directed graph. The difference in the second claim is that we instead partition $\frac{\phi_{\mathcal{O}}(\mathfrak{a}^{-1}N\mathcal{O})}{2}$ elements where the denominator of 2 comes from the fact that elements are equivalent if and only if they differ by a factor of -1. ∎

As in Theorem 4.4, if we restrict ourselves to the case where N is prime, then we can describe the component sizes of $C_{\ell,1}(N)$.

Corollary 4.7 *Let N be a prime different from ℓ and p, and let m denote the order of the group generated by the natural projections of λ, $\overline{\lambda}$ in $(\mathcal{O}/N\mathcal{O})^{\times}/\{\pm 1\}$. Then the graph $G_{\ell,1}(N)$ consists of one of the following:*

(i)   *If N is inert, then there are $\frac{N^2-1}{2m}$ components each of size nm.*

(ii) *If $N\mathcal{O} = \mathfrak{N}_1\mathfrak{N}_2$, then there are $\frac{(N-1)^2}{2m}$ components each of size nm, $\frac{(N-1)}{2m_1}$ components each of size nm_1 and $\frac{N-1}{2m_2}$ components each of size nm_2 where m_1, m_2 are the orders of the groups generated by the natural projections of λ, $\overline{\lambda}$ in $(\mathcal{O}/\mathfrak{N}_1)^{\times}$ and $(\mathcal{O}/\mathfrak{N}_2)^{\times}$ respectively.*

(iii) *If $N\mathcal{O} = \mathfrak{N}^2$, then there are $\frac{N^2-N}{2m}$ components each of size nm and $(N-1)/2m$ components each of size nm_1 where m_1 is the order of the group generated by the natural projections of λ, $\overline{\lambda}$ in $(\mathcal{O}/\mathfrak{N})^{\times}/\{\pm 1\}$.*

Proof The proof of (i) is similar to that of Theorem 4.4 (i), and so we will focus on (ii) and (iii).

As in Theorem 4.4, we fix a vertex $v = (E, P)$ where E is on C_{ℓ} and P is an element of $\mathcal{O}/N\mathcal{O}$ corresponding to a $\Gamma_1(N)$-level structure of E. In the case where $N\mathcal{O} = \mathfrak{N}_1\mathfrak{N}_2$, if $P \in (\mathcal{O}/N\mathcal{O})^{\times}$, then by Theorem 3.3 we have $\operatorname{Stab}(P) = \{\alpha \in \mathcal{O}/N\mathcal{O} \mid \alpha \equiv \pm 1 \bmod N\}$. The component containing v will then be of size nm. As $\phi_{\mathcal{O}}(N\mathcal{O}) = (N-1)^2$, and we identify P with $-P$, we will have $\frac{(N-1)^2}{2m}$ components of size nm. If instead $P \in \mathfrak{N}_1$ (resp. $\mathfrak{N}_2$), then by Theorem 3.3, we instead have $\operatorname{Stab}(P) = \{\alpha \in \mathcal{O}/N\mathcal{O} \mid \alpha \equiv \pm 1 \bmod \mathfrak{N}_2\}$ (resp. $\{\alpha \in \mathcal{O}/N\mathcal{O} \mid \alpha \equiv \pm 1 \bmod \mathfrak{N}_1\}$). By the CRT, $(\mathcal{O}/N\mathcal{O})^{\times} \simeq (\mathcal{O}/\mathfrak{N}_1)^{\times} \times \mathcal{O}/(\mathfrak{N}_2)^{\times}$ and under this isomorphism P may be written as $(0 \bmod \mathfrak{N}_1, P \bmod \mathfrak{N}_2)$ (resp. $(P \bmod \mathfrak{N}_1, 0 \bmod \mathfrak{N}_2)$). It follows that the component containing v will be of size nm_2 (resp. nm_1). Since $\#(\mathcal{O}/\mathfrak{N}_1)^{\times}/\{\pm 1\} = \#(\mathcal{O}/\mathfrak{N}_2)^{\times}/\{\pm 1\} = \frac{N-1}{2}$, it follows that there are $\frac{N-1}{2m_2}$ (resp. $\frac{N-1}{2m_1}$) components of size nm_2 (resp. nm_1).

The proof of (iii) is the same, but with the change that $\phi_{\mathcal{O}}(N\mathcal{O}) = N^2 - N$. ∎

4.3 Crater graphs $C_\ell(N)$

Definition 4.4 Let (P, Q) be $\Gamma(N)$-level structure of E. Then the vertex $v = (E, P, Q)$ is on some component $\mathcal{C}_\ell(N) \subseteq C_\ell(N)$. We say a vertex $v' \in \mathcal{C}_\ell(N)$ is a Γ-*principal vertex of v* if it is of the form (E, P', Q') for some $P', Q' \in E[N]$ which are a basis for $E[N]$.

Lemma 4.8 Let $v = (E, P, Q)$ be a vertex on $\mathcal{C}_\ell(N) \subseteq C_\ell(N)$. If $v' = (E, P', Q')$ is a Γ-principal vertex of v, then there exists an endomorphism $\alpha \in \mathrm{End}(E)$ such that $\alpha(P) = \pm P'$ and $\alpha(Q) = \pm Q'$. Furthermore, there exists some ideal $\mathfrak{b}$ in the group $\langle \mathfrak{l}, \bar{\mathfrak{l}} \rangle$ such that $\mathfrak{b} = \alpha \mathcal{O}$.

Proof   The proof is similar to that of Theorem 4.5.   ∎

As we will see shortly, the full level N structure case turns out to be the simplest of the three cases to describe.

Theorem 4.9 Let $v = (E, P, Q)$ be a vertex on a component $\mathcal{C}_\ell(N) \subseteq C_\ell(N)$ where P, Q are a $\mathbb{Z}$-basis for $E[N]$. Then $\#\mathcal{C}_\ell(N) = nm$ where m is the order of the group generated by the natural projections of $\lambda, \bar{\lambda}$ in $(\mathcal{O}/N\mathcal{O})^\times/\pm 1$. Further, $C_\ell(N)$ contains

$$\frac{N^2 \phi(N)^2}{2m} \prod_{p | N} \left(1 + \frac{1}{p} \right)$$

components isomorphic to $\mathcal{C}_\ell(N)$.

Proof   We first fix a vertex $v = (E, P, Q)$ where E is on C_ℓ and P, Q are a $\mathbb{Z}$-basis for $E[N]$. From Theorem 3.2, we have that $\mathrm{Stab}((P, Q)) = \{\alpha \in \mathcal{O}/N\mathcal{O} \mid \alpha \equiv \pm 1 \bmod N\mathcal{O}\}$. The number of principal vertices of v is given by the order m of the group generated by the projections of $\lambda, \bar{\lambda}$ in $(\mathcal{O}/N\mathcal{O})^\times/\{\pm 1\}$ and so the component containing v is of size nm. Theorem 4.1 (iii) gives us the number of vertices containing E, and division by m gives the desired result.   ∎

We immediately see a difference between Theorem 4.9 and the theorems describing $G_{\ell,0}(N)$ and $G_{\ell,1}(N)$ graphs: the structure is independent of the prime ideal factorization of $N\mathcal{O}$. However, given a vertex $v = (E, P, Q)$, the factorization of $N\mathcal{O}$ can place restrictions on the possible principal vertices of v. For example, if $N = \mathfrak{N}_1 \mathfrak{N}_2$ and $P \in \mathfrak{N}_1, Q \in (\mathcal{O}/N\mathcal{O})^\times$, then any principal vertex $v' = (E, P', Q')$ of v must have the same structure (i.e., $P' \in \mathfrak{N}_1, Q' \in (\mathcal{O}/N\mathcal{O})^\times$).

5 Class field theory

We now extend these results and use the language of class field theory to describe a group action on the various level structures. We will begin by briefly discussing congruence subgroups. Much of the content we discuss here is covered in more detail in [5].

5.1 Generalized ideal class groups

Let K be an imaginary quadratic field and $\mathcal{O}$ an order in K. We will let $\mathcal{I}_\mathcal{O}$ denote the group of proper fractional $\mathcal{O}$-ideals and $\mathcal{P}_\mathcal{O} \subseteq \mathcal{I}_\mathcal{O}$ the subgroup of fractional principal $\mathcal{O}$-ideals. In the imaginary quadratic setting[1], a modulus $\mathfrak{m} \subseteq \mathcal{O}$ is simply an $\mathcal{O}$-ideal. For a modulus $\mathfrak{m}$, we let $\mathcal{I}_\mathcal{O}(\mathfrak{m})$ denote the group of proper fractional $\mathcal{O}$-ideals which are coprime to $\mathfrak{m}$, $\mathcal{P}_\mathcal{O}(\mathfrak{m}) \subseteq \mathcal{I}_\mathcal{O}(\mathfrak{m})$ denote the subgroup of principal ideals which are coprime to $\mathfrak{m}$, and $\mathcal{P}_{\mathcal{O},1}(\mathfrak{m}) \subseteq \mathcal{P}_\mathcal{O}$ denote the subgroup of principal ideals generated by $\alpha \in K^\times$ such that $\alpha \equiv 1 \bmod \mathfrak{m}$. A subgroup $H \subseteq \mathcal{I}_\mathcal{O}(\mathfrak{m})$ satisfying $\mathcal{P}_{\mathcal{O},1}(\mathfrak{m}) \subseteq H \subseteq \mathcal{I}_\mathcal{O}(\mathfrak{m})$ is called a *congruence subgroup* for $\mathfrak{m}$. Given a congruence subgroup H, we may form the quotient group

$$Cl_\mathcal{O}(\mathfrak{m}) = \mathcal{I}_\mathcal{O}(\mathfrak{m})/H$$

which we call a *generalized ideal class group* for $\mathfrak{m}$.

A trivial example of a congruence subgroup we are familiar with is obtained by setting $\mathfrak{m} = 1$. In this setting, any principal ideal (α) satisfies $\alpha \equiv 1 \bmod \mathfrak{m}$ and so $\mathcal{P}_{\mathcal{O},1} = \mathcal{P}_\mathcal{O}$. Then the generalized ideal class group is the usual ideal class group $Cl_\mathcal{O} = \mathcal{I}_\mathcal{O}/\mathcal{P}_\mathcal{O}$ we are familiar with.

In this article, we focus on the setting $\mathfrak{m} = N\mathcal{O}$ where N is defined as in the previous sections. The two congruence subgroups we are interested in are $\mathcal{P}_{\mathcal{O},1}(N)$, and

$$\mathcal{P}_{\mathcal{O},\mathbb{Z}}(N) = \{(\alpha) \mid \alpha \equiv c \mod N\mathcal{O} \text{ for } c \in \mathbb{Z} \text{ with } (c,N) = 1\}.$$

The first of these congruence subgroups is generated by the elements which fix all of a $\Gamma_1(N)$ and $\Gamma(N)$-level structure, while the second fixes all of a $\Gamma_0(N)$-level structure.

Proposition 5.1 *Let $\mathcal{O}, \mathcal{O}'$ be orders such that $\mathcal{O}' \subseteq \mathcal{O}$ and $[\mathcal{O} : \mathcal{O}'] = f$. Then*

$$Cl_{\mathcal{O}'} \simeq \mathcal{I}_\mathcal{O}(f)/\mathcal{P}_{\mathcal{O},\mathbb{Z}}(f).$$

Proof   As stated in [2, Theorem 2.3.1], the proof is the relative version of [5, Proposition 7.22]. ∎

We are now ready to discuss the group action on level structures. Given an ordinary elliptic curve E with $\mathrm{End}(E) \simeq \mathcal{O}$ and a level structure $\gamma(N)$ on E of type $\Gamma_0(N)$, $\Gamma_1(N)$, or $\Gamma(N)$, we may define a group action

$$\mathfrak{a} \cdot \gamma(N) = \varphi_\mathfrak{a}(\gamma(N)),$$

where $\mathfrak{a} \in \mathcal{I}_\mathcal{O}(N)$ and $\varphi_\mathfrak{a}$ is the isogeny induced by $\mathfrak{a}$ whose kernel is given by $E[\mathfrak{a}]$. Up to the equivalence relation defined in Definition 2.5, if $\gamma(N)$ is a $\Gamma_0(N)$-level structure, then the common stabilizers among all $\Gamma_0(N)$-level structures is the set $\mathcal{P}_{\mathcal{O},\mathbb{Z}}(N)$ of principal ideals which act as scalar multiplication on $\gamma(N)$; if it is a $\Gamma_1(N)$-level structure, then common stabilizers is the set $\mathcal{P}_{\mathcal{O},1}(N)$ of principal ideals which act as multiplication by ± 1 on $\gamma(N)$; and if it is a $\Gamma(N)$-level structure, its stabilizers is the set $\mathcal{P}_{\mathcal{O},1}(N)$. We can then form quotient groups

---

[1]For general number fields, one needs to consider the real infinite primes dividing $\mathfrak{m}$. Our focus is only on the imaginary quadratic setting where K has no real infinite primes.

$$(5.1) \qquad Cl_{N\mathcal{O}}(N) = \mathcal{I}_{N\mathcal{O}}(N)/\mathcal{P}_{NO}(N) \text{ and}$$

$$(5.2) \qquad Cl_{\mathcal{O},1}(N) = \mathcal{I}_{\mathcal{O}}(N)/\mathcal{P}_{\mathcal{O},1}(N),$$

where (5.1) acts on isomorphism classes of $\Gamma_0(N)$-level structures and (5.2) acts on isomorphism classes of $\Gamma_1(N)$ and $\Gamma(N)$-level structures. The first of these two generalized ideal class groups is simply the ideal class group for the order of index N in $\mathcal{O}$, while the second is known as the *ray class group* for modulus $\mathfrak{m} = N$.

6 Examples

We will now look at several examples. We will add various level structures to craters. The examples covered are computed using Sagemath [17]. The craters with level structure are constructed by explicitly computing ℓ-isogenies and applying them to the various level structures we are interested in. The examples we look at will all consider the case where ℓ splits in $\mathcal{O}$ as $\ell\mathcal{O} = \mathfrak{l} \cdot \bar{\mathfrak{l}}$. We will lift $\mathfrak{l}$ to the various groups discussed in Section 5 and compute its order to show consistency with the craters we construct.

Example 6.1   Let $p = 107$, $\ell = 5$, $N = 6$, and $E/\mathbb{F}_p$ defined by $y^2 = x^3 + 43x + 86$ where $j(E) = 19$. We have the discriminant of Frobenius $\Delta_\pi = -284 = 2^2(-71)$ and so E has CM by an order $\mathcal{O}$ in $K = \mathbb{Q}(\sqrt{-71})$. One can check that $\text{End}(E) = \mathcal{O}_K = \mathbb{Z}[\Phi] = \mathbb{Z}\left[\frac{1+\sqrt{-71}}{2}\right]$. Figure 1 shows the crater of the component of the ℓ-isogeny graph containing E with the blue vertex highlighting the isomorphism class E belongs to while Figure 2 shows the crater graph $C_{5,0}(6)$ obtained by adding a $\Gamma_0(5)$-level structure to the graph in Figure 1.

The factorization of ℓ and N into products of prime ideals is given by

$$\ell\mathcal{O} = (5) = \mathfrak{l} \cdot \bar{\mathfrak{l}} = (5, \Phi+1)(5, \Phi+3)$$
$$N\mathcal{O} = (6) = \mathfrak{p} \cdot \bar{\mathfrak{p}} \cdot \mathfrak{q} \cdot \bar{\mathfrak{q}} = (2, \Phi)(2, \Phi+1)(3, \Phi)(3, \Phi+2).$$

The ideal class $[\mathfrak{l}]$ has order 7 in Cl_K which is consistent with the crater size seen in Figure 1. For the ideal $\mathfrak{l}$, we have $\mathfrak{l}^7 = \lambda\mathcal{O} = (-4\Phi + 281)$. If $\langle P \rangle$ is a $\Gamma_0(N)$-level structure on E, we have three cases to consider:

(i) P is identified with an element of $(\mathcal{O}/N\mathcal{O})^\times$;
(ii) P is identified with an element of exactly one of $\mathfrak{p}, \bar{\mathfrak{p}}, \mathfrak{q},$ or $\bar{\mathfrak{q}}$ or;
(iii) P is identified with an element of exactly one of $\mathfrak{p}, \bar{\mathfrak{p}}$ and exactly one of $\mathfrak{q}, \bar{\mathfrak{q}}$.

For the first case, we can determine the size of the component containing $\langle P \rangle$ by considering the order of the projection of λ in $(\mathcal{O}/N\mathcal{O})^\times/(\mathbb{Z}/N\mathbb{Z})^\times$. We have $\#(O/N\mathcal{O})^\times/(\mathbb{Z}/N\mathbb{Z})^\times = 4/2 = 2$ and $\lambda = -4\Phi + 281 \equiv 2\Phi + 5$ modulo 6. This is clearly not congruent to an integer modulo 6, so $|\lambda| = 2$ and so by Theorem 4.3 we have one component which is twice the size of our original volcano. For the second
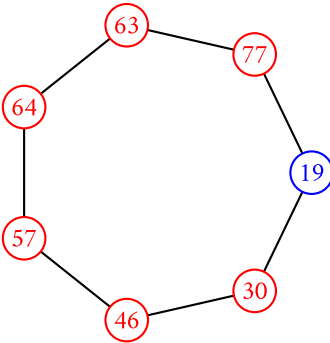
Figure 1: Crater of 5-volcano containing $j(E) = 19$ over $\mathbb{F}_{107}$.
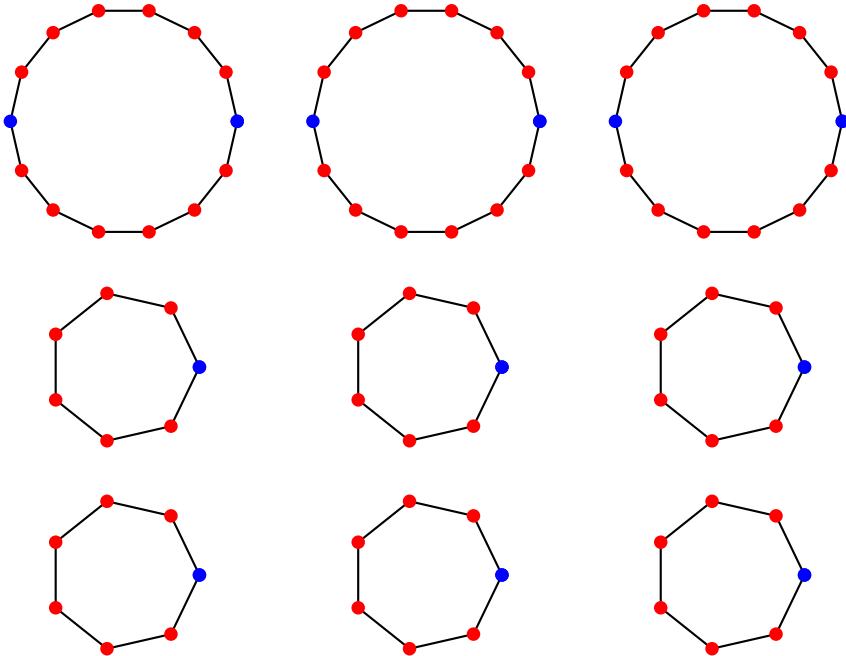

Figure 2: Crater $C_{5,0}(6)$ corresponding to adding a $\Gamma_0(6)$-level structure to the 5-isogeny graph containing $j(E) = 19$. Blue vertices correspond to principal vertices of E.

case, we need to consider the order of the projection of λ in each of

$$(\mathcal{O}/\mathfrak{p}^{-1}N\mathcal{O})^{\times}/(\mathbb{Z}/N\mathbb{Z})^{\times},$$
$$(\mathcal{O}/\overline{\mathfrak{p}}^{-1}N\mathcal{O})^{\times}/(\mathbb{Z}/N\mathbb{Z})^{\times},$$
$$(\mathcal{O}/\mathfrak{q}^{-1}N\mathcal{O})^{\times}/(\mathbb{Z}/N\mathbb{Z})^{\times}; \text{ and}$$
$$(\mathcal{O}/\overline{\mathfrak{q}}^{-1}N\mathcal{O})^{\times}/(\mathbb{Z}/N\mathbb{Z})^{\times}.$$
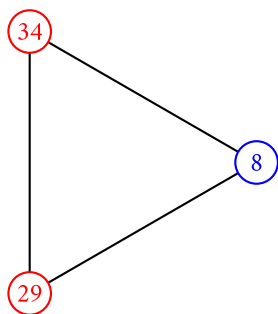
Figure 3: Crater of 5-volcano containing $j(E) = 8$ over $\mathbb{F}_{47}$.

The last two of these rings has trivial order and so each corresponds to a component isomorphic to our original volcano. The first two rings are of size 2, and so it suffices to check the projection of λ in $(\mathcal{O}/\mathfrak{p}^{-1}N\mathcal{O})^\times$ and $(\mathcal{O}/\overline{\mathfrak{p}}^{-1}N\mathcal{O})^\times$. We compute these projections to be $2\Phi - 1$ and $-\Phi - 1$ respectively which both square to the identity element in their respective rings. Therefore, we have an additional two components which are twice of our original volcano, giving a total of three components of this size. Finally, consider when $P \in \mathfrak{pq}$. Then

$$(\mathcal{O}/\mathfrak{p}^{-1}\mathfrak{q}^{-1}N\mathcal{O})^\times \simeq (\mathcal{O}/\overline{\mathfrak{pq}})^\times \simeq (\mathbb{Z}/N\mathbb{Z})^\times,$$

and so λ always acts as an integer on $\langle P \rangle$. The result holds for all possibilities in the third case, and so we have four additional components isomorphic to the original volcano for a total of six copies of the original volcano.

Example 6.2 Let $p = 47$, $\ell = 5$, $N = 3$ and $E/\mathbb{F}_p$ defined by $y^2 = x^3 + 14x + 5$ where $j(E) = 8$. The discriminant of Frobenius is given by $\Delta_\pi = 2^2(-31)$. We compute the endomorphism ring of E to be $\text{End}(E) = \mathcal{O} = \mathbb{Z}[\pi]$. Seen in Figure 3 is the crater containing the isomorphism class of E and Figure 4 shows the crater graph $C_{5,0}(3)$. A notable difference between the graph seen in Figure 4 and the one seen in Figure 2 of the previous example is the number of components. In this example,

$$\ell\mathcal{O} = (5) = \mathfrak{l} \cdot \overline{\mathfrak{l}} = (5, \pi + 3)(5, \pi + 4)$$

and N is an inert prime, so any $\Gamma_0(N)$-level structure is generated by an element P which can be identified with an element of $(\mathcal{O}/N\mathcal{O})^\times$. Consequently, the crater graph $C_{5,0}(3)$ will consist of components all isomorphic to each other and by Theorem 5.1, they will have size equal to the order of $[\mathfrak{l}]$ in $Cl(\mathcal{O}')$ where $\mathcal{O}' = \mathbb{Z} + 3\mathcal{O} = \mathbb{Z} + 6\mathcal{O}_K$. We compute $h(O') = 12$, and so we simply need to check whether which of $\mathfrak{l}^3$, $\mathfrak{l}^6$, and $\mathfrak{l}^{12}$ is principal when $\mathfrak{l}$ is viewed as an $\mathcal{O}'$-ideal. We compute

$$\mathfrak{l} = (5, 3\pi + 2)$$
$$\mathfrak{l}^3 = (125, 3\pi + 52)$$
$$\mathfrak{l}^6 = (15625, 3\pi + 3802)$$

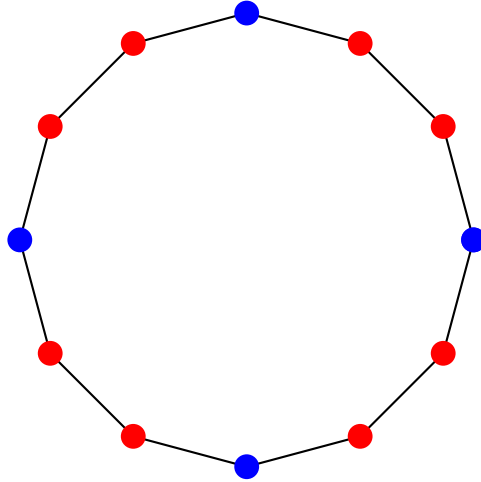none of which is principal, and so $[\mathfrak{l}]$ has order 12 in $Cl(\mathcal{O})$.

Figure 4: Crater $C_{5,0}(3)$ corresponding to adding a $\Gamma_0(3)$-level structure to the 5-isogeny graph containing $j(E) = 8$. Blue vertices correspond to principal vertices of E.
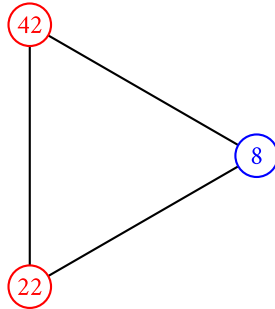

Figure 5: Crater of 3-volcano containing $j(E) = 8$ over $\mathbb{F}_{53}$.

We now look at our final example which is a graph obtained by adding a $\Gamma_1(N)$-level structure.

Example 6.3 Let $p = 53$, $\ell = 3$, $N = 5$, and $E/\mathbb{F}_p$ be defined by $y^2 = x^3 + 46x + 6$ where $j(E) = 8$. The endomorphism ring of E is given by $\mathrm{End}(E) = \mathcal{O} = \mathbb{Z} + 2\mathbb{Z}[\Phi]$ where $\Phi = \left[\frac{1+\sqrt{-11}}{2}\right]$.

Figure 5 shows the crater containing the isomorphism class of E, and Figure 6 shows the crater graph $C_{3,1}(5)$.

We factor ℓ, N into prime $\mathcal{O}$-ideals as

$$\ell\mathcal{O} = \mathfrak{l} \cdot \bar{\mathfrak{l}} = (3, 2\Phi + 1)(3, 2\Phi),$$

$$N\mathcal{O} = \mathfrak{N} \cdot \overline{\mathfrak{N}} = (5, 2\Phi + 1)(5, 2\Phi + 2).$$

In $Cl(K)$, $[\mathfrak{l}]$ has order 3 and $\mathfrak{l}^3 = \lambda\mathcal{O} = (-2\Phi + 5)$. For a $\Gamma_1(N)$-level structure P, we have three cases to consider:
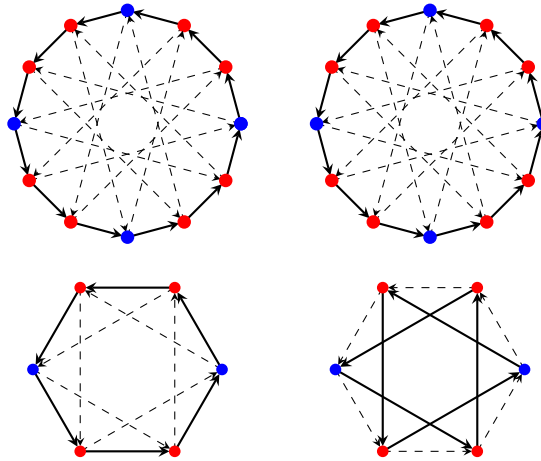
Figure 6: Crater $C_{3,1}(5)$ corresponding to adding a $\Gamma_1(5)$-level structure to the 3-isogeny graph containing $j(E) = 8$. Blue vertices correspond to principal vertices of E. Solid arrows represent isogenies induced by $\mathfrak{l}$, and dashed lines represent isogenies induced by $\bar{\mathfrak{l}}$.

(i) P is identified with an element of $(\mathcal{O}/N\mathcal{O})^\times$;
(ii) P is identified with an element of $\mathfrak{N}$ or;
(iii) P is identified with an element of $\overline{\mathfrak{N}}$.

For the first case, we have $\#(\mathcal{O}/N\mathcal{O})^\times/2 = 8$. We let $\tilde{\lambda}$ denote the equivalence class of $(\mathcal{O}/N\mathcal{O})^\times$ containing λ and compute

$$\tilde{\lambda} = -2\Phi + 5 \equiv -2\Phi \quad \mathrm{mod}\ N$$
$$\tilde{\lambda}^2 = -16\Phi + 13 \equiv -\Phi + 3 \quad \mathrm{mod}\ N$$
$$\tilde{\lambda}^4 = -160\Phi - 599 \equiv 1 \quad \mathrm{mod}\ N,$$

and so $\tilde{\lambda}$ has order 4 and we get two components of size 12. Performing the same computations with $\bar{\mathfrak{l}}$ we find that the projection of $\bar{\lambda}$ in $(\mathcal{O}/N\mathcal{O})^\times$ also has order 4. One may also show that $\bar{\mathfrak{l}} \equiv \mathfrak{l}^5$ mod N to construct the other half of the edges in Figure 6.

The other two cases we need to consider are when P corresponds to an element of either $\mathfrak{N}$ or $\overline{\mathfrak{N}}$. If P corresponds to an element of $\mathfrak{N}$, then we need to consider the order of $\tilde{\lambda}$ in $(\mathcal{O}/\overline{\mathfrak{N}})^\times$. In the quotient ring $(\mathcal{O}/\overline{\mathfrak{N}})^\times$, $-2\Phi \equiv 3$ and so $\tilde{\lambda} \equiv 3$ which squares to -1 and stabilizes P. This gives us one component of size six. In the quotient ring $(\mathcal{O}/\mathfrak{N})^\times$, $-2\Phi \equiv 4$ and so $\tilde{\lambda} \equiv -1$ which gives two components of size 3. To obtain the other half of the edges, we perform the same computations with $\bar{\mathfrak{l}}$ and find that the projection of $\bar{\lambda}$ has order 3 and 6 in $(\mathcal{O}/\mathfrak{N})^\times$ and $(\mathcal{O}/\overline{\mathfrak{N}})^\times$ respectively and compute that $\mathfrak{l}^2 \equiv \bar{\mathfrak{l}}$ mod $\mathfrak{N}$ and $\bar{\mathfrak{l}}^2 \equiv \mathfrak{l}$ mod $\overline{\mathfrak{N}}$.

References

[1] S. Arpin, *Adding level structure to supersingular elliptic curve isogeny graphs*. Journal de théorie des nombres de Bordeaux **36**(2024) no. 2, pp. 405–443.

[2] S. Arpin, W. Castryck, J. K. Eriksen, G. Lorenzon, and F. Vercauteren, *Generalized class group actions on oriented elliptic curves with level structure*. To appear at the International Workshop for the Arithmetic of Finite Fields. 2024.

[3] D. X Charles, K. E Lauter, and E. Z Goren, *Cryptographic hash functions from expander graphs*. J. Cryptol. **22**(2009), no. 1, 93–113.

[4] L. Colò, *Oriented supersingular elliptic curves and class group actions*. Ph.D. thesis, Aix-Marseille Université, Nov. 2022. Available at https://www.leonardocolo.com/documents/thesis/PhD_Thesis.pdf.

[5] D. A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*, Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts, Wiley, Hoboken, NJ, 2013.

[6] L. De Feo, T. B. Fouotsa, and L. Panny, *Isogeny problems with level structure*. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, Zurich, Switzerland, 2024, pp. 181–204.

[7] M. Fouquet, J. M Miret, and J. Valera, *Distorting the volcano*. Finite Fields Appl. **49**(2018), 108–125.

[8] M. Fouquet and F. Morain, *Isogeny volcanoes and the sea algorithm*. In: Algorithmic Number Theory: 5th International Symposium, ANTS-V Sydney, Australia, July 7–12, 2002 Proceedings 5, Springer, Berlin, 2002, pp. 276–291.

[9] S. D Galbraith, D. Perrin, and J. F. Voloch, *CSIDH with level structure*. Cryptology ePrint Archive, 2023.

[10] D. R. Kohel, *Endomorphism rings of elliptic curves over finite fields*. University of California, Berkeley, CA, 1996.

[11] A. Lei and K. Müller, *On ordinary isogeny graphs with level structure*. Expositiones Mathematicae, **42**(2024), no. 5, 125589.

[12] S. Levin, *Lifted elliptic curve isogeny graphs*. University of Canterbury, Christchurch, New Zealand, 2021.

[13] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*. 3rd ed., Springer, Berlin, 2011.

[14] M. Roda, *Supersingular isogeny graphs with level N structure and path problems on ordinary isogeny graphs*. McGill University, Montreal, Canada, 2019.

[15] J. H Silverman, *Advanced topics in the arithmetic of elliptic curves*, Vol. 151. Springer Science & Business Media, New York, NY, 1994.

[16] A. Sutherland, *Isogeny volcanoes*. Open Book Series **1**(2013), no. 1, 507–530.

[17] The Sage Developers, SageMath, the sage mathematics software system (Version 10.4). 2024. https://www.sagemath.org.

School of Mathematics and Statistics, University of Canterbury, Private Bag 4800, Christchurch 8140, New Zealand

e-mail: derek.perrin@pg.canterbury.ac.nz   felipe.voloch@canterbury.ac.nz