Available online at www.sciencedirect.com

ScienceDirect

Expositiones Mathematicae 42 (2024) 125589

EXPOSITIONES MATHEMATICAE

www.elsevier.com/locate/exmath

On ordinary isogeny graphs with level structures

Antonio Lei[a,*], Katharina Müller[b]

[a] *Department of Mathematics and Statistics University of Ottawa, 150 Louis-Pasteur Pvt Ottawa, ON, Canada K1N 6N5*

[b] *Institut für Theoretische Informatik, Mathematik und Operations Research Universität der Bundeswehr München, Werner-Heisenberg-Weg 39 85577 Neubiberg, Germany*

Received 29 June 2023; received in revised form 18 June 2024; accepted 18 June 2024

Abstract

Let ℓ and p be two distinct prime numbers. We study ℓ-isogeny graphs of ordinary elliptic curves defined over a finite field of characteristic p, together with a level structure. Firstly, we show that as the level varies over all p-powers, the graphs form an Iwasawa-theoretic abelian p-tower, which can be regarded as a graph-theoretical analogue of the Igusa tower of modular curves. Secondly, we study the structure of the crater of these graphs, generalizing previous results on volcano graphs. Finally, we solve an inverse problem of graphs arising from the crater of ℓ-isogeny graphs with level structures, partially generalizing a recent result of Bambury, Campagna and Pazuki.

MSC: primary 05C25; 11G20; secondary 11R23; 14G17; 14K02

Keywords: Isogeny graphs; Iwasawa theory for graphs; Inverse problem for graphs

1. Introduction

Let p be a fixed prime number. Let X be a finite connected graph (in this article, we allow multiple edges and loops in a graph). In a series of articles, [20,21,27] Vallières and McGown–Vallières studied Iwasawa theory of the so-called abelian p-towers of graphs above X (see Definition 3.1; note that we have replaced the prime ℓ in the aforementioned

[*] Corresponding author.
E-mail addresses: antonio.lei@uottawa.ca (A. Lei), katharina.mueller@unibw.de (K. Müller).

https://doi.org/10.1016/j.exmath.2024.125589

works by p in this article). Let $(X_n)_{n\geq 0}$ be such a tower and write κ_n for the number of spanning trees of X_n. Then there exist integers μ, λ and ν such that

$$\mathrm{ord}_p(\kappa_n) = \mu p^n + \lambda n + \nu$$

for $n \gg 0$. This can be regraded as the graph-theoretic analogue of the seminal formula of Iwasawa on class groups of sub-extensions inside a $\mathbb{Z}_p$-extension of a number field proved in [13].

As discussed in [12,19], Iwasawa theory of number fields draws strong analogies with its function field counterpart in which one studies towers of Galois coverings of curves. One important example of such towers is the Igusa tower of modular curves initially studied in [11]; see also [10,14,19]. Roughly speaking, an Igusa tower consists of

$$X_0 \leftarrow X_1 \leftarrow \cdots \leftarrow X_n \leftarrow X_{n+1} \leftarrow \cdots$$

where X_n is the modular curve classifying isomorphism classes of (E, P), where E is an elliptic curve over a finite field of characteristic p and P is a point on E of order p^n.

The first goal of this article is to construct an explicit $\mathbb{Z}_p$-tower of graph coverings arising from isogeny graphs of ordinary elliptic curves defined over a finite field k, whose characteristic is p. This gives a graph theoretical analogue of Igusa towers. Let ℓ be a prime number distinct from p and let $m \geq 0$, $N \geq 1$ be integers. We define in Section 2.1 the ℓ-isogeny graph G_N^m whose vertices consist of $\overline{k}$-isomorphism classes of pairs (E, P), where E is an ordinary elliptic curve defined over k and P is a point of $E(\overline{k})$ of order Np^m, and edges between two vertices are defined by ℓ-isogenies. When $N = 1$ and $m = 0$, this recovers the volcano graphs studied in [2,15,26]. The graphs G_N^m can be regarded as an enhancement of the volcano graphs via the addition of a $\Gamma_1(Np^m)$-level structure. Similar (but slightly different) graphs have been studied in [9]. See in particular Sections 2 and 3 in op. cit.

A priori, G_N^m is a directed graph. We shall write $\tilde{G}_N^m$ for the undirected graph obtained from G_N^m by ignoring the directions of the edges. The first main result of the present article is the following:

Theorem A (Corollary 3.7)**.** *Let E be an elliptic curve representing a non-isolated vertex of $\tilde{G}_1^0$ (i.e., a vertex whose degree is strictly positive). Let $\tilde{\mathcal{G}}_N^m$ denote the connected component of $\tilde{G}_N^m$ containing a vertex arising from E. Then there exists an integer m_0 such that the graphs $\left(\tilde{\mathcal{G}}_N^{m_0+r}\right)_{r\geq 0}$ form an abelian p-tower in the sense of Vallières and McGown–Vallières.*

In Appendix, we explain how to realize such a tower of graph coverings as voltage graphs when $N = 1$. This may be of independent interest since voltage assignments are used to define Iwasawa invariants of abelian p-towers in [20,21,27].

The integer m_0 featured in Theorem A depends on the variation of the number of connected components in G_N^m as m increases. We show in Proposition 3.3 that when m is sufficiently large, the number of components in $\tilde{G}_N^m$ stabilizes. Such stabilization is necessary to ensure that the coverings $\tilde{\mathcal{G}}_N^{m+r}/\tilde{\mathcal{G}}_N^m$ are Galois.

In the case of volcano graphs, each vertex is assigned a "level", depending on the endomorphism ring of the elliptic curve attached to the vertex. The level zero vertices form the "crater" of a volcano graph. In [2, Proposition 3.14], Bambury–Campagna–Pazuki gave a complete description of all possible craters. One may extend the concept of "levels" and "craters" to G_N^m in a natural manner (see Definition 2.9). In Section 4, we give a detailed description of the crater of G_N^m; see in particular Remark 4.21 and Proposition 4.24. Several explicit examples are given throughout the section. The introduction of $\Gamma_1(Np^m)$-level structure has the advantage that we may avoid working with loops if we assume either N or m is sufficiently large (see Lemma 2.11). While many of our results are direct analogues of those given in [2], the absence of loops allows us to simplify some of the proofs.

In Section 5, we define the so-called "abstract tectonic craters", which are graphs that have the same geometry as a connected component of the crater that we describe in Section 4 (see Definition 5.1). We prove a result on the inverse problem for such graphs.

Theorem B (*Theorem* 5.2)**.** *Let G be an abstract tectonic crater. There exist infinitely many pairs of distinct primes p and ℓ, and nonnegative integers N such that one of the connected components of the crater of the ℓ-isogeny graph G_N^1 is isomorphic to G.*

This can be regarded as a partial generalization of results in [2], where the inverse problem for volcano graphs over $\mathbb{F}_p$ without level structure has been studied. The inverse problem without level structure is false when $k \neq \mathbb{F}_p$ because of connectedness issue (see §5.1 of op. cit. for a detailed discussion). In the present paper, we consider connected components separately allowing us to avoid this issue. Furthermore, we have the liberty to increase the level N to simplify the structure of the graphs being studied. In particular, we do not recover results of [2] since the level is fixed to be 1 in the aforementioned work.

Outlook

In the setting of number fields, questions on distributions of Iwasawa invariants attached to cyclotomic $\mathbb{Z}_p$-extensions of imaginary quadratic fields have initially been studied in [8]. More recently, similar questions on abelian number fields have been studied in [6]. In [7], questions on distributions of Iwasawa invariants attached to abelian p-towers of graphs were studied. Unlike the setting of number fields, the notion of cyclotomic extensions does not exist in the context of graphs. The towers given by Theorem A could potentially be a candidate of substitution for cyclotomic extensions. We plan to study how the Iwasawa invariants vary as ℓ and/or p vary. Techniques developed in [22] could potentially be adopted in this setting.

It may also be interesting to seek arithmetic interpretation of the p-adic zeta functions attached the towers given by Theorem A. One might naively hope that they could be related to p-adic zeta functions of modular curves over k originating from the Iwasawa theory of function fields. Results in [18,25] tell us that the latter are closely related to supersingular isogeny graphs. However, we would not be able to construct abelian p-towers for supersingular isogeny graphs in the manner presented in this article because of the lack of p-power torsions on supersingular elliptic curves over finite fields of characteristic p. This suggests that fundamentally new ideas are required to establish links between abelian p-towers of ordinary isogeny graphs with objects from function field Iwasawa theory.

In a different direction, we plan to study the following inverse problem further generalizing Theorem B: Given a volcano graph G with a tectonic crater (see Definition 5.1), can we find primes p and ℓ, a finite field k of characteristic p and an integer N such that G is a connected component of G_N^m for some non-negative integer m? The additional difficulty in solving this question compared to Theorem B is that a volcano of depth $d > 0$ (i.e a volcano not only consisting of a crater) does not leave any room for choosing the prime ℓ, whereas our proof of Theorem B depends crucially on using Tchebotarev's Theorem to choose ℓ. One could hope to resolve this problem by choosing the imaginary quadratic field K appropriately — similar to the techniques employed to solve the inverse volcano problem for $N = 1$ and $m = 0$ in [2].

Finally, we mention that several works on isogeny graphs with level structures have been released in recent years; see [1,3,9,17,24,28]. In a different vein, Pengo–Vallières [23] developed a general theory of graph coverings indexed by natural numbers of a given finite graph using Mahler measures. More specifically, given a finite graph X, they study a collection of graph coverings $\{X_n\}_{n\geq 1}$ of X, where X_n/X is a Galois covering whose Galois group is isomorphic to $\mathbb{Z}/n\mathbb{Z}$. It seems natural to study how isogeny graphs with level structures might fit in this framework.

2. The definition of isogeny graphs and basic properties

Throughout this article, a graph X may be directed or undirected. We write $V(X)$ for the set of vertices of X and $\mathbb{E}(X)$ for the set of edges of X. We shall say that $v \in V(X)$ admits an edge in X if there exists $e \in \mathbb{E}(X)$ such that v is one of the end-points of e.

2.1. Defining ordinary isogeny graphs

Let p be an odd prime. We fix a second prime number $\ell \neq p$ and $N \geq 1$ an integer coprime to $p\ell$. Further, we fix a finite field k of characteristic p. We fix once and for all a set of representatives of $\overline{k}$-isomorphism classes of elliptic curves defined over k, which we denote by $\mathcal{E}$. Note that a $\overline{k}$-isomorphism of two curves over k can be realized over the unique quadratic extension k' of k as long as the j-invariant is different from 0 and 1728.

We introduce the main object of interest of the present article:

Definition 2.1.

(i) Let E and E' be elliptic curves defined over k. Let $P \in E(\overline{k})$ and $P' \in E'(\overline{k})$ be points of order Np^m. We say that (E, P) and (E', P') are equivalent if there is a $\overline{k}$-isomorphism of elliptic curves $\phi : E \to E'$ with $\phi(P) = P'$.

(ii) Let E and E' be elliptic curves defined over k. Let ϕ and ϕ' be isogenies from E to E' defined over $\overline{k}$. We say that ϕ and ϕ' are equivalent if $\ker(\phi) = \ker(\phi')$.

(iii) For an integer $m \geq 1$, we define a directed graph G_N^m whose vertices are the equivalence classes of tuples (E, P) given by (i). There is a directed edge from

(E, P) to (E', P') if and only if there is an ℓ-isogeny $\phi : E \to E'$ such that $\phi(P) = P'$, with each equivalence class of such isogenies gives rise to exactly one edge.

By an abuse of notation, if $v \in V(G_N^m)$, we shall take any one representative of the equivalence class and simply write (E, P). If ϕ gives rise to an edge from (E, P) to (E', P'), we shall write $\phi(E, P)$, (E', P') and $(\phi(E), \phi(P))$ interchangeably.

Remark 2.2. Let $E \in \mathcal{E}$ and $\alpha \in \mathrm{Aut}(E)$. By definition, $(E, \alpha P)$ and (E, P) give rise to the same vertex in G_N^m.

In the cases where $j(E) = 0$ or $j(E) = 1728$, the group $\mathrm{Aut}(E)$ is strictly larger than $\{\pm 1\}$. Assume that this is the case and let E' be an elliptic curve with $\mathrm{Aut}(E') = \{\pm 1\}$ such that there is an ℓ-isogeny $\phi : E \to E'$. Let $\alpha \in \mathrm{Aut}(E) \setminus \{\pm 1\}$. Then (E, P) and $(E, \alpha P)$ define the same vertex in G_N^m, whereas $(E', \phi(P))$ and $(E', \phi(\alpha P))$ give rise to two distinct vertices. The isogenies ϕ and $\phi \circ \alpha$ are not equivalent, resulting in two edges from $(E, P) = (E, \alpha P)$ to $(E', \phi(P))$ and $(E', \phi(\alpha P))$, respectively. ♢

Remark 2.3. If E is an ordinary elliptic curve over $\overline{\mathbb{F}_p}$, there exists an imaginary quadratic field K and an order $\mathcal{O}$ in K such that $\mathrm{End}(E) = \mathcal{O}$. Note that p is split in K. Thus, if E is defined over k, then all of its endomorphisms are defined over k. ♢

Remark 2.4. Let $(E, P) \in V(G_N^m)$. If $\phi : E \to E'$ is an ℓ-isogeny that maps P to P', then the dual isogeny maps P' to the point ℓP on ℓE, where ℓE denotes the image of the multiplication-by-ℓ map on E. The curve ℓE is isomorphic to E. Let α be such an isomorphism. Then $(\ell E, \ell P)$ is equivalent to $(E, \alpha(\ell P))$, which we explain below.

Let $\mathrm{End}(E) = \mathcal{O}$ and $K = \mathrm{End}(E) \otimes \mathbb{Q}$. By Deuring's lifting theorem (see [16, Chapter 13, Theorem 14]), there exists a lift $\mathbf{E}$ of E over a finite extension L of K and a prime ideal $\mathfrak{p}$ above p such that $\mathbf{E} \pmod{\mathfrak{p}'} = E$ for some ideal $\mathfrak{p}'$ above p in the ring of integers of L and that $\mathrm{End}(\mathbf{E}) = \mathrm{End}(E) = \mathcal{O}$. Then P admits a unique lift $\mathbf{P} \in \mathbf{E}[N\overline{\mathfrak{p}}^m] \cong E[Np^m]$, where $\overline{\mathfrak{p}}$ is an ideal above p in $\mathcal{O}$ that is coprime to $\mathfrak{p}'$. (The isomorphism follows from the theory of formal groups when $\mathcal{O} = \mathcal{O}_K$; see for example [5, Chapters I and II]. As every CM elliptic curve is isogenous to one with complex multiplication by $\mathcal{O}_K$, this result easily carries over to general CM elliptic curves.)

To determine $\alpha(\ell P)$, it suffices to consider $\tilde{\alpha}(\ell \mathbf{P})$, where $\tilde{\alpha} : \ell\mathbf{E} \to \mathbf{E}$ is a lift of α. Furthermore, we may even base change to $\mathbb{C}$. We have $\mathbf{E}(\mathbb{C}) = \mathbb{C}/\Lambda$ for some lattice Λ in $\mathbb{C}$. Then, we may realize $\ell\mathbf{E}(\mathbb{C})$ as $\mathbb{C}/\frac{1}{\ell}\Lambda$ and

$$\begin{aligned} \tilde{\alpha} : \ell\mathbf{E}(\mathbb{C}) &\to \mathbf{E}(\mathbb{C}) \\ x + \frac{1}{\ell}\Lambda &\mapsto \ell x + \Lambda. \end{aligned}$$

Furthermore, we have

$$\begin{aligned} [\ell] : \mathbf{E}(\mathbb{C}) &\to \ell\mathbf{E}(\mathbb{C}) \\ x + \Lambda &\mapsto x + \frac{1}{\ell}\Lambda. \end{aligned}$$

If we write $\mathbf{P} = x + \Lambda$, then $\tilde{\alpha}(\ell\mathbf{P}) = \ell\mathbf{P}$. Thus $\alpha((\ell E, \ell P)) = (E, \ell P)$ as claimed. ♢

It follows from Remark 2.4 that if ϕ is an isogeny that induces an edge from (E, P) to (E', P') in G_N^m, then the dual isogeny $\hat{\phi}$ gives an edge from (E', P') to $(E, \ell P)$.

Remark 2.5. Each curve $E_{/\overline{\mathbb{F}_p}}$ admits $\ell + 1$ isogenies that are of degree ℓ. Let $\phi_1, \ldots, \phi_{\ell+1}$ denote these isogenies. Note that $\phi_i(E)$ may not be defined over k. As the vertices in G_N^m are defined by elliptic curves over k, not all ϕ_i will necessarily result in an edge in G_N^m. In general, the number of edges between E and E' is exactly the multiplicity of $j(E')$ as a root of the modular polynomial $\Phi_\ell(j(E), Y)$. ♢

If there is an ℓ-isogeny between two elliptic curves E and E', then $\mathrm{End}(E) \otimes \mathbb{Q} = \mathrm{End}(E') \otimes \mathbb{Q}$. Thus, $\mathrm{End}(E)$ and $\mathrm{End}(E')$ are orders in the same imaginary quadratic field. In particular, to each connected component of G_N^m, we may attach a unique imaginary quadratic field. This allows us to give the following definition:

Definition 2.6. Let $\mathcal{G}_N^m$ be a connected component of G_N^m. Let (E, P) be any vertex in $\mathcal{G}_N^m$. We call $\mathrm{End}(E) \otimes \mathbb{Q}$ the **CM field** of $\mathcal{G}_N^m$.

2.2. Coverings of ordinary isogeny graphs

The goal of this section is to show that as N and m vary, the graphs introduced in the previous section give rise to coverings of graphs. Let r, m, N, N' be nonnegative integers such that $N'|N$. There is a natural projection

$$\pi_{Np^{m+r}/N'p^m} : V(G_N^{m+r}) \to V(G_{N'}^m)$$

given by $(E, P) \mapsto (E, \frac{Np^r}{N'} P)$. Further, if ϕ is an ℓ-isogeny such that $\phi(E, P) = (E', P')$, we have $\phi \circ \pi_{Np^{m+r}/N'p^m}(E, P) = \pi_{Np^{m+r}/N'p^m}(E', P')$. Therefore, $\pi_{Np^{m+r}/N'p^m}$ extends to a map on the whole graph. By an abuse of notation, we shall write

$$\pi_{Np^{m+r}/N'p^m} : G_N^{m+r} \to G_{N'}^m$$

for this map.

Let $\mathcal{G}_N^{m+r}$ be a fixed connected component of G_N^{m+r} and let $\mathcal{G}_{N'}^m$ be the unique connected component of $G_{N'}^m$ that contains $\pi_{Np^{m+r}/N'p^m}(\mathcal{G}_N^{m+r})$.

Lemma 2.7. *The map $\pi_{Np^{m+r}/N'p^m}$ induces a covering of connected graphs $\mathcal{G}_N^{m+r}/\mathcal{G}_{N'}^m$.*

Proof. To simplify notation, we write $\mathcal{G}$ for $\mathcal{G}_N^{m+r}$ and $\mathcal{H}$ for $\mathcal{G}_{N'}^m$. Further, we write π for $\pi_{Np^{m+r}/N'p^m}$. We first show that $\pi(V(\mathcal{G})) = V(\mathcal{H})$.

Let $u = (E, P) \in V(\mathcal{G})$ and let $v = (E', Q) \in V(\mathcal{H})$. Our goal is to find a preimage of v in $V(\mathcal{G})$ under π. Let $w = (E, P_0) = \pi((E, P))$. As $\mathcal{H}$ is connected, there exists a path C from w to v. Let n be the length of C and write $\phi_1, \phi_2, \ldots \phi_n$ for the isogenies corresponding the edges of C. The composition $\Phi = \phi_n \circ \cdots \circ \phi_1$ is an isogeny from E to E' with $\Phi(\frac{Np^r}{N'} P) = Q$.

Let $v' = (E', \Phi(P)) \in G_N^{m+r}$. The isogenies $\phi_i' s$ induce a path from u to v'. Therefore, v' belongs to $V(\mathcal{G})$. Furthermore, it is clear from definition that $\pi(v') = v$. This proves our claim above.

As for edges, there is a one-one correspondence between the edges for which $(E, P) \in V(\mathcal{G})$ is the target (resp. source) and the ℓ-isogenies for which E is the codomain (resp. domain). The same can be said for $\pi(E, P) = (E, \frac{Np^r}{N'}P)$. Thus, it follows that π is locally an isomorphism of graphs, which concludes the proof of the lemma. □

Suppose that $N = N'$ and $r = 1$. Since E is defined over $\overline{\mathbb{F}_p}$ and E is ordinary, the cover $\mathcal{G}_N^{m+1} \to \mathcal{G}_N^m$ is of degree p. We will be interested in the tower of covers of the form

$$\mathcal{G}_N^m \leftarrow \mathcal{G}_N^{m+1} \leftarrow \mathcal{G}_N^{m+2} \leftarrow \cdots .$$

2.3. Horizontal and vertical edges

In this section, we are interested in counting edges in and out of a vertex in G_N^m. A large part of our discussion therein has been inspired by the work of Bambury–Campagna–Pazuki [2].

Definition 2.8. Suppose that $\phi : E \to E'$ is an ℓ-isogeny, and write $\mathcal{O} = \mathrm{End}(E)$ and $\mathcal{O}' = \mathrm{End}(E')$. Recall that $\mathcal{O}$ and $\mathcal{O}'$ are rings in the same imaginary quadratic field. There are three cases that may arise:

(1) $[\mathcal{O} : \mathcal{O}'] = 1$. In this case, we say that ϕ is ***horizontal***.
(2) $[\mathcal{O} : \mathcal{O}'] = \ell$. In this case, we say that ϕ is ***descending***.
(3) $[\mathcal{O}' : \mathcal{O}] = \ell$. In this case, we say that ϕ is ***ascending***. We say that ϕ is **vertical** if it is either descending or ascending.

If ϕ gives rise to $e \in \mathbb{E}(G_N^m)$, we shall use the same terminology introduced above to describe e.

Definition 2.9. Let (E, P) be a vertex in G_N^m and write $\mathrm{End}(E) = \mathbb{Z} + f\mathcal{O}_K$, where $f \in \mathbb{Z}$.

(i) We call $v_\ell(f)$ the **level** of E. Note that this is well-defined (i.e., $v_\ell(f)$ is independent of the choice of f) and it only depends on the curve E, not on the point P.
(ii) The subgraph of G_N^m generated by the set of vertices of level zero is called the **crater** (i.e., the maximal subgraph of G_N^m containing all the level zero vertices). We write $\mathcal{C}(G_N^m)$ for the crater of G_N^m.
(iii) Let $\mathcal{G}_N^m$ be a connected component of G_N^m. We define the **depth** of $\mathcal{G}_N^m$ to be the maximal integer d such that there is a vertex of level d in $\mathcal{G}_N^m$.
(iv) If $\mathcal{G}_N^m$ is as above, the crater of $\mathcal{G}_N^m$ is defined to be the intersection of $\mathcal{C}(G_N^m)$ and $\mathcal{G}_N^m$. It will be denoted by $\mathcal{C}(\mathcal{G}_N^m)$.

Suppose that $N = 1$ and $m = 0$. The vertices of G_1^0 consist of isomorphism classes of elliptic curves (with P taken as the identity element). Furthermore, if ϕ induces an edge e from E to E', then the dual isogeny $\hat{\phi}$ of ϕ induces an edge $\hat{e}$ from E' to E. Let $\mathfrak{G}$ denote the *undirected* graph whose set of vertices is given by $V(G_1^0)$ and the set of edges is given by those in $\mathbb{E}(G_1^0)/\sim$, where $\sim$ is the equivalence relation identifying e with $\hat{e}$. The concepts introduced in Definitions 2.8 and 2.9 carry over to $\mathfrak{G}$ naturally. The structure of $\mathfrak{G}$ can be described explicitly as follows.

Lemma 2.10. *Let $\mathcal{G}$ be a connected component of $\mathfrak{G}$. Suppose that it is of depth d with CM field K and that it contains no vertex E with $j(E) \in \{0, 1728\}$. Then the following statements hold.*

(i) Let v be a vertex of $\mathcal{C}(\mathcal{G})$. It admits $1 + \left(\frac{D_K}{\ell}\right)$ horizontal edges and no ascending edges. If $d > 0$, it admits $\ell - \left(\frac{D_K}{\ell}\right)$ descending edges. If $d = 0$, it admits no descending edge.

(ii) Let $1 \leq n \leq d$ and let v be a vertex in $\mathcal{G}$ of level n. Then v admits one ascending edge. If $n < d$, then v admits $\ell - 1$ descending edges. If $d = n$, then v admits no descending edges.

Proof. This follows directly from [2, Proposition 3.17]. □

This in turn allows us to describe the structure of G_N^m when Np^m is sufficiently large.

Lemma 2.11. *Let $\mathcal{G}_N^m$ be a connected component of G_N^m. Let d be the depth of $\mathcal{G}_N^m$. Assume that $\mathcal{G}_N^m$ does not contain a vertex of the form (E, P) with $j(E) \in \{0, 1728\}$. Let K be the CM field of $\mathcal{G}_N^m$.*

(i) If ℓ splits in K and $d = 0$, each vertex in $\mathcal{G}_N^m$ admits 4 edges for N or m sufficiently large.

(ii) Suppose that $d > 0$ and that ℓ splits in K. If N or m is sufficiently large, each vertex in $\mathcal{C}(\mathcal{G}_N^m)$ admits $\ell + 3$ edges in $\mathcal{G}_N^m$. For $1 \leq n \leq d - 1$, each vertex of level n admits $\ell + 1$ edges. Each vertex of level d admits 1 edge.

(iii) Suppose that ℓ ramifies in K. If $d = 0$, each vertex in $\mathcal{G}_N^m$ admits 2 edges for N or m sufficiently large.

(iv) Suppose that ℓ ramifies in K and that $d > 0$. Each vertex in $\mathcal{C}(\mathcal{G}_N^m)$ admits $\ell + 2$ edges in $\mathcal{G}_N^m$ for N or m large enough.

(v) Suppose that ℓ is inert in K. If $d = 0$, then each vertex in $\mathcal{C}(\mathcal{G}_N^m)$ is isolated. If $d > 0$, then each vertex in $\mathcal{C}(\mathcal{G}_N^m)$ admits $\ell + 1$ edges in $\mathcal{G}_N^m$.

Proof. Assume that $v = (E, P)$ is a vertex in $\mathcal{C}(\mathcal{G}_N^m)$. Let us first assume that ℓ splits in K, Lemma 2.10(i) tells us that v admits two horizontal isogenies ϕ_1 and ϕ_2 connecting (E, P) to (E', P') and (E'', P''), respectively. The dual isogenies $\hat{\phi}_1$ and $\hat{\phi}_2$ give rise to edges going from $(E', \frac{1}{\ell}P')$ and $(E'', \frac{1}{\ell}P'')$ to (E, P) (note that $\ell \nmid Np$ implies that $\frac{1}{\ell}P'$ and $\frac{1}{\ell}P''$ are well-defined). For m or N large enough, the four vertices (E', P'), (E'', P''), $(E', \frac{1}{\ell}P')$ and $(E'', \frac{1}{\ell}P'')$ are pairwise distinct. This proves part (i) of the lemma.

Now suppose that $d > 0$. By Lemma 2.10(ii) v admits $\ell - 1$ descending edges and no ascending edges. Together with the 4 edges arising from the 4 horizontal isogenies, we deduce that v admits $(\ell - 1) + 4 = \ell - 3$ edges.

The other cases can be proved similarly. □

We consider the cases where $j(E) \in \{0, 1728\}$ separately.

Lemma 2.12. *Let E be an elliptic curve with $j(E) = 0$. Let $\mathcal{G}_N^m$ be a connected component of G_N^m containing a vertex of the form $v = (E, P)$.*

(i) If $\ell = 3$*, then each vertex in* $\mathcal{C}(\mathcal{G}_N^m)$ *admits* 5 *edges in* $\mathcal{G}_N^m$ *for* N *or* m *sufficiently large.*
(ii) If $\ell \equiv 1 \pmod 3$ *and* $d = 0$*, then each vertex in* $\mathcal{C}(\mathcal{G}_N^m)$ *admits* 4 *edges in* $\mathcal{G}_N^m$ *for* N *or* m *sufficiently large.*
(iii) If $\ell \equiv 1 \pmod 3$ *and* $d > 0$*, then each vertex in* $\mathcal{C}(\mathcal{G}_N^m)$ *admits* $\ell + 3$ *edges in* $\mathcal{G}_N^m$*.*
(iv) If $\ell \equiv 2 \pmod 3$ *and* $d = 0$*, then each vertex in* $\mathcal{C}(\mathcal{G}_N^m)$ *is isolated.*
(v) If $\ell \equiv 2 \pmod 3$ *and* $d > 0$*, then each vertex in* $\mathcal{C}(\mathcal{G}_N^m)$ *admits* $\ell + 1$ *edges in* $\mathcal{G}_N^m$*.*

Proof. The proof is essentially the same proof as that Lemma 2.11 upon replacing Lemma 2.10 by [2, Proposition 3.19]. □

Lemma 2.13. *Let* E *be an elliptic curve with* $j(E) = 1728$*. Let* $\mathcal{G}_N^m$ *be a connected component of* G_N^m *containing a vertex of the form* $v = (E, P)$*.*

(i) If $\ell = 2$*, then each vertex in* $\mathcal{C}(\mathcal{G}_N^m)$ *admits* 4 *edges in* $\mathcal{G}_N^m$ *for* N *or* m *sufficiently large.*
(ii) If $\ell \equiv 1 \pmod 4$ *and* $d = 0$*, then each vertex in* $\mathcal{C}(\mathcal{G}_N^m)$ *admits* 4 *edges in* $\mathcal{G}_N^m$ *for* N *or* m *sufficiently large.*
(iii) If $\ell \equiv 1 \pmod 4$ *and* $d > 0$*, then each vertex in* $\mathcal{C}(\mathcal{G}_N^m)$ *admits* $\ell + 3$ *edges in* $\mathcal{G}_N^m$*.*
(iv) If $\ell \equiv 2 \pmod 4$ *and* $d = 0$*, then each vertex in* $\mathcal{C}(\mathcal{G}_N^m)$ *is isolated.*
(v) If $\ell \equiv 2 \pmod 4$ *and* $d > 0$*, then each vertex in* $\mathcal{C}(\mathcal{G}_N^m)$ *admits* $\ell + 1$ *edges in* $\mathcal{G}_N^m$*.*

Proof. This follows again from the same proof as that of Lemma 2.11 upon employing [2, Proposition 3.20]. □

3. Abelian *p*-towers

The main goal of this section is to prove Theorem A. Throughout, the notation introduced in Section 2 continues to be in force. We begin by recalling the definition of an abelian p-tower from [27, Definition 4.1]:

Definition 3.1. An abelian p-tower of undirected graphs above a graph X is a sequence of covers

$$X = X_0 \leftarrow X_1 \leftarrow X_2 \leftarrow \cdots \leftarrow X_n \leftarrow \cdots$$

such that for each $n \geq 0$, the cover X_n/X is abelian with Galois group isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$.

We are interested in the case where X_n are connected for all n. If X_0 admits more than one connected component, the Galois group of X_n/X may potentially be a direct product of two or more groups, which we would like to avoid.

Definition 3.2. The undirected graph obtained by ignoring directions of the edges in G_N^m is denoted by $\tilde{G}_N^m$. Similarly if $\mathcal{G}_N^m$ is a connected component of G_N^m, we define $\tilde{\mathcal{G}}_N^m$ similarly.

We shall take X to be a single connected component $\tilde{\mathcal{G}}_N^{m_0}$, where m_0 is a sufficiently large integer that will be given in Section 3.1.

3.1. Connected components

The goal of this section is to study the number of connected components of G_N^m as m varies.

Proposition 3.3. *Assume that none of the connected components of G_1^0 is a single vertex without any edges. There exists an integer m_0 such that the number of connected components in G_N^m is the same as $G_N^{m_0}$ for all $m \geq m_0$.*

Proof. Let s_N^m be the number of connected components in G_N^m. It follows from Lemma 2.7 that $\pi_{Np^{m+1}/Np^m} : G_N^{m+1} \to G_N^m$ is a graph covering. Thus, $s_N^{m+1} \geq s_N^m$. It remains to show that this sequence stabilizes when m is sufficiently large.

Suppose that $m \geq 1$. Since E is ordinary at p and $p \nmid N$, we have the group isomorphisms

$$\mathrm{Aut}(E[p^m N]) \cong (\mathcal{O}/N\mathcal{O})^\times \times (\mathbb{Z}/p^m\mathbb{Z})^\times,$$

where $\mathcal{O}$ is an order in an imaginary quadratic field. Therefore, the order of $[\ell]$ (the multiplication by ℓ map) in $\mathrm{Aut}(E[p^m N])$ is equal to the multiplicative order of ℓ in the group $(\mathbb{Z}/Np^m\mathbb{Z})^\times$. Thus, there exist integers m_0 and c such that this order is given by cp^{m-m_0} for all $m \geq m_0$. For all such m, we have

$$\ell^{cp^{m-m_0}} \equiv 1 \pmod{Np^m}.$$

In particular, $\ell^c \equiv 1 \pmod{Np^{m_0}}$. It follows that

$$\ell^c p^{m-m_0} \equiv p^{m-m_0} \pmod{Np^m}. \tag{3.1}$$

Let $v_0 = (E, P_0) \in V(G_N^{m_0})$ and let $v = (E, P) \in V(G_N^m)$ be a pre-image of v_0 under $\pi_{Np^m/Np^{m_0}}$, where $m \geq m_0$. Consider the set

$$C := \left\{(E, \ell^{cn} P) : n \in \mathbb{Z}_{\geq 0}\right\}.$$

By (3.1), all elements of C are sent to v_0 under $\pi_{Np^m/Np^{m_0}}$. Furthermore, the fact that the order of $[\ell]$ in $\mathrm{Aut}(E[p^m N])$ equals cp^{m-m_0} implies that C contains exactly the p^{m-m_0} elements. In particular, C is precisely the pre-image of v_0 in G_N^m. By our assumption on G_1^0, E admits an ℓ-isogeny. Thus, as we have seen in Remark 2.4, all vertices in C lie in the same connected component of G_N^m as v. This implies that the number of connected components stabilizes and concludes the proof. □

Remark 3.4. Assume that there is an isolated vertex E in G_N^1. Then for all $m \geq 1$ and all $P \in E[Np^m]$, the vertex $(E, P) \in G_N^m$ is also isolated. In particular, as we pass from G_N^m to G_N^{m+1}, the number of connected components arising from E is multiplied by p. Therefore, the number of connected components in G_N^m is unbounded as $m \to \infty$.

Let $\mathcal{E}'$ be the set of $\overline{k}$ equivalence classes of ordinary elliptic curves over k that are not isolated in G_1^0, i.e. $\mathcal{E}'$ only contains isomorphism classes of curves admitting a degree ℓ isogeny to a curve defined over k. Let $H_N^m \subset G_N^m$ be the subgraph on the vertices of the form (E, P) with $E \in \mathcal{E}'$. Then the proof of Proposition 3.3 shows that the number of connected components of H_N^m is constant for $m \geq m_0$.

In particular, if $m \geq m_0$ and $\mathcal{G}_N^m$ is a connected component of H_N^m, then H_N^{m+r} admits a unique connected component whose image under π_{Np^{m+r}/Np^m} is $\mathcal{G}_N^m$. ◊

Definition 3.5. Given an integer $N \geq 1$, we write m_0 to be the integer given by Remark 3.4.

3.2. Galois covers and abelian p-towers

We now prove a proposition regarding the cover G_N^{m+r}/G_N^m, which will imply Theorem A stated in the introduction. We shall work with undirected graphs, following works on Iwasawa theory of graphs in the literature, in particular [7,20,21,27].

Proposition 3.6. *Let H_N^m and m_0 be defined as in Remark 3.4. Let $\mathcal{G}_N^m$ be a connected component of H_N^m and fix $m \geq \max(m_0, 1)$. Let $\mathcal{G}_N^{m+r}$ be the connected component of H_N^{m+r} that maps onto $\mathcal{G}_N^m$ via π_{Np^{m+r}/Np^m}. Then $\tilde{\mathcal{G}}_N^{m+r}/\tilde{\mathcal{G}}_N^m$ is a Galois graph covering whose Galois group is isomorphic to $\mathbb{Z}/p^r\mathbb{Z}$.*

Proof. Let $U \subset (\mathbb{Z}/Np^{m+r}\mathbb{Z})^\times$ be the subgroup consisting of elements that are congruent to 1 modulo Np^m. Note that $U \cong \mathbb{Z}/p^r\mathbb{Z}$ as abelian groups.

Let $\pi = \pi_{Np^{m+r}/Np^m}$. We define an action of U on $V(G_N^{m+r})$ by

$$a \cdot (E, P) = (E, aP).$$

As $\pi(E, P) = \pi(E, aP)$. It follows from the proof of Proposition 3.3 that (E, aP) and (E, P) lie in the same connected component of G_N^{m+r}. In particular, the action defined above restricts to an action of U on $V(\mathcal{G}_N^{m+r})$.

This action extends to a graph homomorphism of $\tilde{\mathcal{G}}_N^{m+r}$. Indeed, let (E, P) and (E', P') be adjacent vertices in $\tilde{\mathcal{G}}_N^{m+r}$, connected by an edge e. Without loss of generality, we can assume that e is induced by an ℓ-isogeny $\phi : E \to E'$ such that $\phi(P) = P'$. Then the same isogeny induces an edge between (E, aP) and (E', aP') since $\phi(aP) = a\phi(P) = aP'$.

Let $\mathrm{Deck}(\tilde{\mathcal{G}}_N^{m+r}/\tilde{\mathcal{G}}_N^m)$ denote the group of deck transformations of the graph covering $\pi : \tilde{\mathcal{G}}_N^{m+r} \to \tilde{\mathcal{G}}_N^m$, whose degree equals p^r. Recall that $\mathrm{Aut}(E) \in \{\{\pm 1\}, \mu_6, \mu_4\}$. Let K be the CM field of $\mathcal{G}_N^m$. Let $\mathfrak{p}$ be a prime above p in K. Then $\alpha \not\equiv 1 \pmod{\mathfrak{p}^2}$ for every $\alpha \in \mathrm{Aut}(E)$ that is not the identity. In particular, (E, P) and (E, aP) are two distinct vertices. Thus, the action of U on $\tilde{\mathcal{G}}_N^{m+r}$ induces an injective group homomorphism

$$U \hookrightarrow \mathrm{Deck}(\tilde{\mathcal{G}}_N^{m+r}/\tilde{\mathcal{G}}_N^m).$$

To show that π is a Galois cover whose Galois group is isomorphic to $\mathbb{Z}/p^r\mathbb{Z}$, it remains to show that this injective group homomorphism is surjective.

Let ψ be a deck transformation and let $(E, P) \in V(\tilde{\mathcal{G}}_N^{m+r})$. We write $\psi(P)$ for the point of order $p^{m+r}N$ such that $\psi(E, P) = (E, \psi(P))$. As $\pi(E, P) = \pi(\psi((E, P)))$, we have

$$P - \psi(P) \in E[p^r].$$

In particular, $\psi(P) = aP$ for some $a \in U$. Therefore, $\psi((E, P)) = a \cdot (E, P)$.

It remains to show that

$$\psi(E', P') = a \cdot (E', P') \tag{3.2}$$

for all $(E', P') \in V(\tilde{\mathcal{G}}_N^{m+r})$. Let us first consider the case (E', P') is a vertex that is adjacent to (E, P). Suppose that there is a degree ℓ isogeny $\phi\colon E \to E'$ with $\phi(P) = P'$. As ψ is a deck transformation, we have the following commutative diagram

$$\begin{tikzcd}
(E, P) \arrow[r, "\phi"] \arrow[d, "\psi"] & (E', P') \arrow[d, "\psi"] \\
(E, \psi(P)) \arrow[r, "\phi"] & (E', \psi(P')).
\end{tikzcd}$$

Therefore,

$$\psi(E', P') = (E', \phi(\psi(P))) = (E', \phi(aP)) = (E', a\phi(P)) = (E', aP') = a(E', P').$$

Assume now that there is an isogeny $\phi\colon E' \to E$ of degree ℓ. Then

$$\phi(aP') = aP = \psi(P) = \phi(\psi(P')).$$

As ϕ is injective on $E'[Np^{m+r}]$ it follows that $aP' = \psi(P')$. So in both cases we have shown that $\psi((E', P')) = a(E', P')$.

As $\tilde{\mathcal{G}}_N^{m+r}$ is connected, we deduce that (3.2) holds for all (E', P') as required. □

Proposition 3.6 implies immediately Theorem A stated in the introduction:

Corollary 3.7. *The graph coverings*

$$\tilde{\mathcal{G}}_N^{m_0} \leftarrow \tilde{\mathcal{G}}_N^{m_0+1} \leftarrow \cdots$$

is an abelian p-tower in the sense of Definition 3.1.

4. The structure of the crater

The goal of this section is to study the connected components of the crater $\mathcal{C}(G_N^m)$ for any given N and m. The CM field of this chosen connected component will be denoted by K throughout.

We consider two separate cases. Namely, when ℓ is non-split in K and when ℓ is split in K. The split case turns out to be more delicate than the non-split case.

4.1. The non-split case

We first study the case where ℓ is non-split in K. This can be divided further into two sub-cases, namely either ℓ is inert or ramified in K.

Lemma 4.1. *Let $\mathcal{C}_0$ be a connected component of $\mathcal{C}(G_N^m)$.*

(i) If ℓ is inert in K, then $\mathcal{C}_0$ consists of a single vertex, without any edges.

(ii) If ℓ is ramified in K, then $\mathcal{C}_0$ is either a single vertex with a loop or it is a directed cycle, i.e., there exists an integer $s \geq 1$ such that $\mathcal{C}_0$ consists of s vertices $\{v_1, \ldots v_s\}$ with edges going from v_i to v_{i+1} for $1 \leq i \leq s-1$ and an edge from v_s to v_1.

Proof. If there is an edge between two vertices of level zero, it has to be induced by a horizontal isogeny. Part (i) follows immediately from [2, Corollary 3.13].

We now prove part (ii). Let $(E, P) \in V(\mathcal{C}_0)$. We set $\mathcal{O} = \mathrm{End}(E)$. Let $\mathfrak{L}$ be the ideal of $\mathcal{O}$ above ℓ (i.e. $\ell\mathcal{O} = \mathfrak{L}^2$). Note that $\mathfrak{L}^2$ is a principal ideal.

If $\mathfrak{L}$ itself is principal, then there exists an element $x \in \mathcal{O}$ such that $E/E[\mathfrak{L}] = xE \cong E$. Let h be the order of x in $(\mathcal{O}/N\mathfrak{p}^m)^\times/\mathcal{O}^\times$, where we have written $\mathcal{O}^\times$ for its natural image in $(\mathcal{O}/N\mathfrak{p}^m)^\times$ and $\mathfrak{p}$ is an ideal of $\mathcal{O}$ lying above p.[1] If $h = 1$, then $\mathcal{C}_0$ consists of a single vertex (E, P) together with a loop. If $h > 1$, then $\mathcal{C}_0$ is a directed cycle of length h, with vertices given by $(E, x^i P)$, $i = 0, 2, \dots, h-1$, and edges given by $(E, P) \to (E, xP) \to \cdots \to (E, x^{h-1}P) \to (E, P)$.

If $\mathfrak{L}$ is not principal, the curve $E' := E/E[\mathfrak{L}]$ is not isomorphic to E. There is an ℓ-isogeny $\phi : E \to E'$ and a dual isogeny $\hat{\phi} : E' \to E'/E'[\mathfrak{L}] \cong E$. Let h be the order of ℓ in $(\mathcal{O}/N\mathfrak{p}^m)^\times/\mathcal{O}^\times$. Then $\mathcal{C}_0$ is a directed cycle of length $2h$, with vertices given by $(E, \ell^i P)$ and $(E', \phi(\ell^i P))$, $i = 1, \dots, h$; the edges are given by $(E, \ell^i P) \to (E', \phi(\ell^i P))$ and $(E', \phi(\ell^i P)) \to (E, \ell^{i+1} P)$. □

Remark 4.2. In the inert case, while $\mathcal{C}_0$ consists of a single vertex, there may be edges in G_N^m connecting it to other vertices in $\mathcal{C}(G_N^m)$ via edges arising from vertical isogenies.

Let $v = (E, P) \in V(\mathcal{C}_0)$ and assume that v admits an edge in G_N^m. Let $\mathcal{G}_N^m \subset G_N^m$ be the connected component containing v. Then all the vertices of the form $(E, \ell^t P)$, $t \in \mathbb{Z}$, lie in $\mathcal{G}_N^m$, as we have seen in Remark 2.4. Suppose that $v' \neq v$ is any vertex in $\mathcal{C}(\mathcal{G}_N^m)$. We claim that v' is of the form $(E, \ell^t P)$.

Indeed, as E admits no horizontal isogeny, a level zero vertex of $\mathcal{G}_N^m$ is of the form (E, P') for some P'. Thus, there is an endomorphism of E of ℓ power degree that maps P to P'. As ℓ is inert, the only ℓ power degree endomorphisms are given by powers of $[\ell]$. Thus, $P' = \ell^t P$ for some t as claimed. ◊

Remark 4.3. If $v \in \mathcal{C}_0$ and $\mathfrak{L}$ is ramified or split in K, then all level zero vertices that lie in the same connected component of G_N^m as v are also elements of $V(\mathcal{C}_0)$. ◊

4.2. Classification of vertices and edges in the split case

From now on, we assume that ℓ splits in K. Let $v_1 = (E, P)$ be a fixed level zero vertex in G_N^m and let $\mathcal{O} = \mathrm{End}(E)$. The ideal $\ell\mathcal{O}$ splits into two distinct ideals $\mathfrak{L}$ and $\overline{\mathfrak{L}}$. We continue to write $\mathcal{C}_0$ for the connected component of $\mathcal{C}(G_N^m)$ containing v_1.

Note that all level zero vertices connected to v_1 are connected through horizontal isogenies. Further, E admits exactly two horizontal isogenies, namely $E \to E/E[\mathfrak{L}]$ and $E \to E/E[\overline{\mathfrak{L}}]$. Thus, all elements of $V(\mathcal{C}_0)$ arise from the curves of the form $E/E[\mathfrak{L}^a\overline{\mathfrak{L}}^b]$. In particular, all these curves have complex multiplication by the same ring $\mathcal{O}$. An edge between two such vertices arises from either $\mathfrak{L}$ or $\overline{\mathfrak{L}}$.

It follows from Lemma 2.11 that when either m or N is sufficiently large, there are two edges $\mathbb{E}(\mathcal{C}_0)$ with v_1 as the source and two edges with v_1 as the target. We see that

[1] The choice of $\mathfrak{p}$ depends on the choice of a CM lift $\mathbf{E}$ of E over some finite abelian extension L/K together with a prime ideal $\mathfrak{p}'$ above p in $\mathcal{O}_L$ such that $\mathbf{E} \pmod{\mathfrak{p}'} = E$. As the integer h does not depend on the choice of $\mathfrak{p}$, we suppress this choice here.

$\mathfrak{L}$ induces precisely one of the former and one of the latter, whereas the other two edges are induced by $\overline{\mathfrak{L}}$.

The following lemma studies equalities in $V(\mathcal{C}_0)$.

Lemma 4.4. *Let $v_i = (E_i, P_i) \in V(\mathcal{C}_0)$, $i = 1, 2$. Suppose that*

$$(E_1/E_1[\mathfrak{L}^a\overline{\mathfrak{L}}^b], P_1 + E_1[\mathfrak{L}^a\overline{\mathfrak{L}}^b]) = (E_1/E_1[\mathfrak{L}^d\overline{\mathfrak{L}}^e], P_1 + E_1[\mathfrak{L}^d\overline{\mathfrak{L}}^e])$$

as elements of $V(\mathcal{C}_0)$ for some nonnegative integers a, b, d and e. Then

$$(E_2/E_2[\mathfrak{L}^a\overline{\mathfrak{L}}^b], P_2 + E_2[\mathfrak{L}^a\overline{\mathfrak{L}}^b]) = (E_2/E_2[\mathfrak{L}^d\overline{\mathfrak{L}}^e], P_2 + E_2[\mathfrak{L}^d\overline{\mathfrak{L}}^e])$$

as elements of $V(\mathcal{C}_0)$.

Proof. Let $i \in \{1, 2\}$ and α, β be nonnegative integers. We write $\phi_{\alpha,\beta,i} : E_i \to E_i/E_i[\mathcal{L}^\alpha\overline{\mathcal{L}}^\beta]$ for the isogeny given by the natural projection. Let us write $v_3 = \phi_{a,b,1}(v_1) = \phi_{d,e,1}(v_1)$. We define $\phi_{\alpha,\beta,3}$ similarly.

Since v_1 and v_2 are level zero vertices lying in the same connected component of $\mathcal{C}(G_N^m)$, there is a path in $\mathcal{C}_0$ connecting v_1 to v_2. Thus, upon propagating along this path, we may assume that there is an edge in $\mathbb{E}(\mathcal{C}_0)$ connecting v_1 to v_2. In this case, this edge is induced by $\phi_{1,0,1}$ or $\phi_{0,1,1}$. Thus it suffices to prove the lemma for these two cases.

Suppose that $\phi_{1,0,1}$ induces an edge from v_1 to v_2. Then one can check directly from definition that

$$\phi_{a,b,2}(v_2) = \phi_{a+1,b,1}(v_1) = \phi_{1,0,3} \circ \phi_{a,b,1}(v_1) = \phi_{1,0,3}(v_3).$$

Similarly,

$$\phi_{d,e,2}(v_2) = \phi_{d+1,e,1}(v_1) = \phi_{1,0,3} \circ \phi_{d,e,1}(v_1) = \phi_{1,0,3}(v_3).$$

This proves the desired equality. The other case can be treated in the same manner. □

Definition 4.5.

(i) We call an edge in $\mathcal{C}_0$ **blue** if it is induced by the isogeny given by $\mathfrak{L}$ and we call it **green** if it is induced by $\overline{\mathfrak{L}}$.

(ii) We call a path in $\mathcal{C}_0$ **blue** if it only consists of blue edges, we call it **green** if it only consists of green edges.

(iii) Let h_1 (resp. h_2) be the minimal length of a closed blue (resp. green) path starting at v_1 in $\mathcal{C}_0$ without backtracks.

Note that all edges in $\mathcal{C}_0$ are either blue or green (but not both). If we repeatedly apply $\mathfrak{L}$ to v_1, we will eventually obtain v_1. Indeed, there exists a nonnegative integer n such that $\mathfrak{L}^n$ is a principal ideal $\gamma\mathcal{O}$, say. As $\ell \nmid Np$, there exists an integer n' such that $\gamma^{n'}P = P$. By a similar argument to the one presented in Remark 2.4, there is a blue path of length nn' sending v_1 to itself. This tells us that h_1 is finite. The same holds for h_2.

If (E', P') lies on a blue (resp. green) path originating from v_1, then $E' = E/E[\mathfrak{F}^a]$, $P' = P + E[\mathfrak{F}^a]$ for some integer a and $\mathfrak{F} = \mathfrak{L}$ (resp. $\overline{\mathfrak{L}}$). It can happen that these two classes of vertices coincide. We study this phenomenon in the following proposition.

Proposition 4.6. *There are positive integers $s \mid h_1$ and $t \mid h_2$ and a positive integer c coprime to h_2/t such that*

$$(E/E[\mathfrak{L}^s], P + E[\mathfrak{L}^s]) = (E/E[\overline{\mathfrak{L}}^{ct}], P + E[\overline{\mathfrak{L}}^{ct}])$$

as elements of $V(\mathcal{C}_0)$. Suppose that (s, t, c) is such a tuple with s minimal. If (s', t', c') is another tuple such that

$$(E/E[\mathfrak{L}^{s'}], P + E[\mathfrak{L}^{s'}]) = (E/E[\overline{\mathfrak{L}}^{c't'}], P + E[\overline{\mathfrak{L}}^{c't'}]),$$

then there exists $d \in \mathbb{Z}$ such that $s' = ds$ and $t' = dt$. In particular, the minimality of s implies the minimality of t.

Proof. Let $\mathcal{S}$ be the set of all tuples (s_1, t_1, c_1) such that $s_1 \mid h_1$, $t_1 \mid h_2$ and

$$(E/E[\mathfrak{L}^{s_1}], P + E[\mathfrak{L}^{s_1}]) = (E/E[\overline{\mathfrak{L}}^{c_1 t_1}], P + E[\overline{\mathfrak{L}}^{c_1 t_1}]).$$

Note that $\mathcal{S}$ is non-empty since it contains $(h_1, h_2, 1)$.

Let $(s, t, c) \in \mathcal{S}$ such that s is minimal. It follows from Lemma 4.4 that $h_1/s = h_2/t$. It implies that t is also minimal. Let $(s', t', c') \in \mathcal{S}$ and write $s'' = \gcd(s', s)$. There are nonnegative integers a_1, a_2 such that $s'' \equiv a_1 s + a_2 s' \pmod{h_1}$. Lemma 4.4 implies that

$$\begin{aligned}(E/E[\mathfrak{L}^{s''}], P + E[\mathfrak{L}^{s''}]) &= (E/E[\mathfrak{L}^{a_1 s + a_2 s'}], P + E[\mathfrak{L}^{a_1 s + a_2 s'}]) \\ &= (E/E[\overline{\mathfrak{L}}^{a_1 ct + a_2 c' t'}], P + E[\overline{\mathfrak{L}}^{a_1 ct + a_2 c' t'}]).\end{aligned}$$

As s is minimal, we see that $s'' = s$ and $s' = ds$ for some integer d. It follows that $t' = h_2 s'/h_1 = dh_2 s/h_1 = dt$ as required. □

From now on, we shall always write s and t for the minimal integers given by Proposition 4.6.

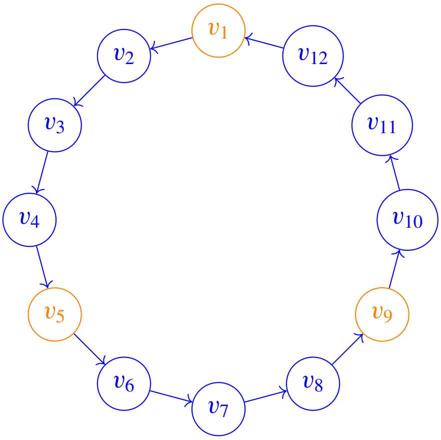
Definition 4.7. We call a vertex $v \in V(\mathcal{C}_0)$ **central** if there exists some positive integer α and a blue path of length αs connecting v_1 to v.

Remark 4.8. Suppose that v is a central vertex. Then Proposition 4.6 tells us that there is a nonnegative integer α' such that there is a green path of length $\alpha' t$ connecting v_1 to v. In other words, we may give an equivalent definition central vertices using green paths.

Definition 4.9. Let v and v' be any two central vertices connected through a blue path of length s. We call the $s - 1$ vertices on this path that are different from v and v' **blue primary vertices**. We define **green primary vertices** similarly for a green path of length t between two central vertices.

Remark 4.10. The blue primary vertices introduced in Definition 4.9 only exist if $s > 1$. Similarly, the green primary ones only exist if $t > 1$. ◊

To illustrate, suppose that $h_1 = 12$ and $s = 4$. Then we have a directed cycle $v_1 \to v_2 \to \cdots \to v_{12} \to v_1$ of length 12 passing through v_1, consisting of blue edges. The vertices v_1, v_5, v_9 are central, whereas the rest of the vertices on the cycle are blue primary.



We prove in the following lemma that central vertices and blue primary vertices are in fact mutually exclusive.

Lemma 4.11. *The blue primary vertices and green primary vertices are not central.*

Proof. We only consider blue primary vertices; the other case can be proved in a similar manner. Let v be a blue primary vertex. By definition, it lies on a blue path of length s from one central vertex to another, say w. In particular, there is a blue path of length a going from v to w, where $1 \leq a \leq s-1$.

Suppose that v is central. Since both w and v are central, it follows from Proposition 4.6 that there is a blue path of length $a's$ going from w to v for some nonnegative integer a'. Consequently, we obtain a closed blue path from v to itself of length $a+a's$.

By Lemma 4.4, there is a closed blue path of length $a+a's$ from v_1 to itself. Proposition 4.6 says that s divides $a+a's$. But this contradicts that $1 \leq a \leq s-1$. Thus, v is not central. □

Remark 4.12. Lemma 4.11 tells us that there are in total h_1/s central vertices, equally distributing along a closed blue path of length h_1 passing through v_1. Furthermore, Remark 4.8 tells us that we may equally count h_2/t central vertices on a closed green path of length h_2 passing through v_1. In particular, we have the equality

$$\frac{h_1}{s} = \frac{h_2}{t}.$$

◊

Lemma 4.13. *There are* $\frac{h_1}{s} \cdot (s-1)$ *blue primary vertices and* $\frac{h_2}{t} \cdot (t-1)$ *green primary vertices, respectively.*

Proof. We only prove the statement on blue primary vertices. The closed blue path of length h_1 gives rise to h_1/s blue paths of length s, each of which connecting two central vertices. Each of these paths in turn gives rise to $s-1$ blue primary vertices. Thus, $\frac{h_1}{s} \cdot (s-1)$ is an upper bound on the total number of blue primary vertices.

We deduce from the previous paragraph that the total number of blue and central vertices is bounded above by

$$\frac{h_1}{s} + \frac{h_1}{s} \cdot (s-1) = h_1.$$

All these vertices are connected through blue edges and lie on a closed blue path (without backtracks) through v_1. The minimal number of edges needed to draw a closed blue path is h_1. Therefore, this upper bound is in fact optimal. Thus, there are exactly $\frac{h_1}{s} \cdot (s-1)$ blue primary vertices. □

Lemma 4.14. *There is no vertex that is simultaneously blue primary and green primary.*

Proof. Suppose that v is a vertex that is both blue primary and green primary. There exist central vertices w and w' such that w is connected to v through a blue path of length $1 \le a \le s-1$ and w' is connected to v through a green path of length $1 \le a' \le t-1$.

Since both w and w' are central, they are connected through a green path of length $a''t$ for some nonnegative integer a''. It follows that the isogenies induced by $\mathfrak{L}^a$ and by $\overline{\mathfrak{L}}^{a'+ta''}$ coincide on v. But $0 < a < s$ and $0 < a' < t$, which contradicts Proposition 4.6. Thus, such v does not exist. □

Suppose that both s and t are strictly greater than 1. Let v be a blue primary vertex. It follows from Lemma 4.11 that v is not central. Consequently, there is a green path of length t from v to some blue primary vertex v'. We shall study the vertices appearing on such a path.

Definition 4.15. Excluding the end-points, we call the vertices lying on a green path linking two blue primary vertices **green secondary vertices**. We define **blue secondary** vertices in a similar manner.

By Lemma 4.13, there are $h_1 - h_1/s$ blue primary vertices. A green path connecting two blue primary vertices has length t (following from Lemma 4.4 and Proposition 4.6). Thus, the number of green secondary vertices is bounded above by

$$\left(h_1 - \frac{h_1}{s}\right)(t-1) = \frac{h_1}{s}(s-1)(t-1).$$

Similarly, the number of blue secondary vertices is bounded above by

$$\left(h_2 - \frac{h_2}{t}\right)(s-1) = \frac{h_2}{t}(s-1)(t-1).$$

These two upper bounds are equal to each other since $h_1/s = h_2/t$ by Remark 4.12.

Lemma 4.16. *There are exactly $\frac{h_1}{s}(s-1)(t-1) = \frac{h_2}{t}(s-1)(t-1)$ blue/green secondary vertices.*

Proof. Take any two central vertices linked by a blue path of length s. This gives $s-1$ blue primary vertices lying on a blue path of length $s-2$. Through each of these vertices, there exists a green cycle of minimal length, i.e., a cycle of length h_2 obtained by repeatedly applying $\overline{\mathfrak{L}}$. Let us call them $C_1, \dots, C_{s-1}$. These cycles are disjoint by construction.

Let $v = (E', P')$ be one of the chosen blue primary vertices. Then $E' \cong E/E[\mathfrak{L}^\alpha]$ for some nonnegative integer α. Proposition 4.6 tells us that after applying $\overline{\mathfrak{L}}^t$ to v, we obtain a primary blue vertex. Therefore, each cycle C_i contains h_2/t blue primary vertices. In particular, the rest of the vertices on C_i are green secondary since they lie on a green path linking two blue primary vertices. This results in $h_2 - h_2/t$ green secondary vertices on C_i. Thus, this gives in total at least $(s-1)(h_2 - h_2/t)$ green secondary vertices. But this is exactly the upper bound, hence the equality holds. □

Lemma 4.17. *A blue/green secondary vertex is not central.*

Proof. Let v be a blue secondary vertex. Let v' be a green primary vertex connected to v through a blue path of length $1 \le a \le s-1$. Let w be a central vertex connected to v' through a green path of length $1 \le a' \le t-1$. If v is also central, then v and w are connected through a blue path of length $a''s$. This implies that the isogenies induced by $\mathfrak{L}^a\overline{\mathfrak{L}}^{a'}$ and $\mathfrak{L}^{a''s}$ coincide on v, which is impossible by Proposition 4.6. □

By a similar argument, one can show:

Lemma 4.18. *A blue secondary vertex is not a green primary vertex. And a green secondary one is not blue primary.*

Proof. Let v be a blue secondary vertex and let v' be a green primary vertex connected to v through a blue path of length $1 \le a \le s-1$. Let w be a central vertex connected to v' via a green path of length $1 \le a' \le t-1$. If v is a green primary vertex, then v and w are connected through a green path of length $bt + a''$ with $1 \le a'' \le t-1$. Thus, the isogeny induced by $\mathfrak{L}^a\overline{\mathfrak{L}}^{a'}$ and the one induced by $\overline{\mathfrak{L}}^{bt+a''}$ coincide, which is impossible by Proposition 4.6. □

Lemma 4.19. *A blue secondary vertex is not blue primary.*

Proof. Let v be a blue secondary vertex. Let w and w' be green primary vertices connected through a green path of length s passing through v. If v is blue primary, then w and w' are central, which contradicts Lemma 4.11. □

Lemma 4.20. *Each blue secondary vertex is a green secondary vertex, and vice versa.*

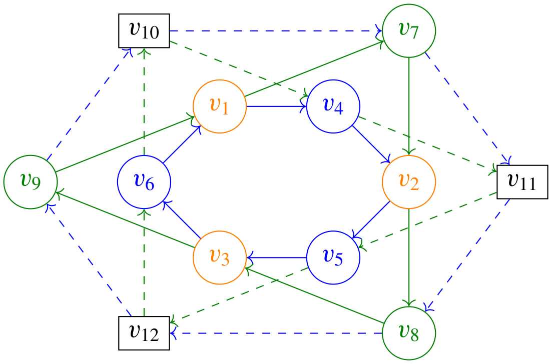
Proof. Let v be a blue secondary vertex. Let v' be a green primary vertex such that there is a blue path of length $1 \le a \le s-1$ from v to v'. Let w be a central vertex such that there is a green path of length $1 \le a' \le t-1$ form v' to w. Let w' be the blue vertex at the end of a blue path of length $s(h_1/s - 1) + (s - a)$ starting at w.

There is also a green path of length $t(h_2/t - 1) + (t - a')$. The end point v'' of this path is a green secondary vertex. Putting these together, we have a path starting at v with $a + s(h_1/s - 1) + s - a = h_1$ blue and h_2 green edges. Thus, $v'' = v'$. □

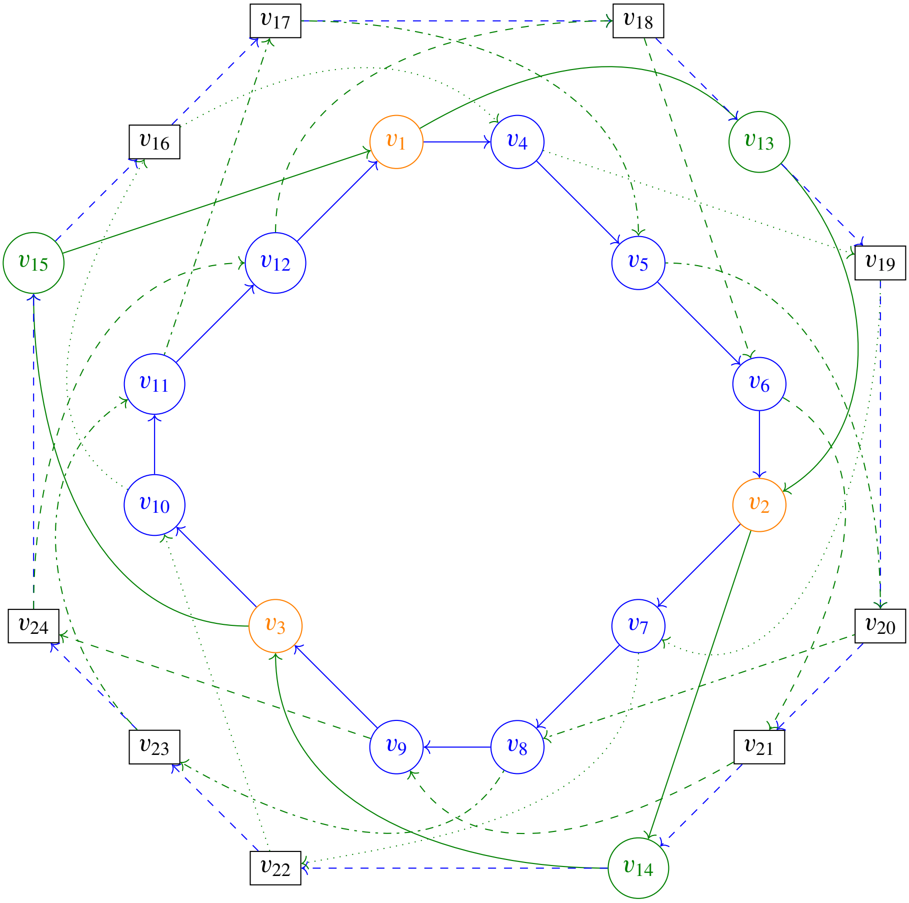
Remark 4.21. To conclude, we may classify the vertices in $\mathcal{C}_0$ as follows.

- We have $h_1/s = h_2/t$ central vertices, which include v_1;
- The central vertices can be equally distributed along a blue closed path of length h_1 containing v_1 (the distance between two consecutive central vertices is s). The non-central vertices on this path are blue primary. There are $\frac{h_1(s-1)}{s}$ such vertices;
- The central vertices can also be found along a green closed path of length h_1 containing v_1. The non-central vertices on this path are green primary. There are $\frac{h_2(t-1)}{t}$ such vertices;
- The rest of the vertices are blue secondary, which can be found on a blue path between two primary green vertices. There are
$$\frac{h_1(s-1)(t-1)}{s} = \frac{h_2(s-1)(t-1)}{t}$$
such vertices;
- We may reverse the roles of blue and green in the previous bullet point, resulting in the same vertices.
- In total, there are $st\Omega$ vertices, where $\Omega = \frac{h_1}{s} = \frac{h_2}{t}$ is the number of central vertices. ♢

Example 4.22. Suppose that $h_1 = h_2 = 6$, $s = t = 2$ and $c = 1$. We have the following graph. The "solid" cycles are obtained from repeatedly applying $\mathcal{L}$ and $\overline{\mathcal{L}}$ to v_1, respectively. This gives us the central vertices v_1, v_2 and v_3 (coloured in orange), the blue primary vertices are v_4, v_5 and v_6, and the green primary vertices are v_7, v_8 and v_9. The "dotted" cycles are the ones obtained from applying $\mathcal{L}$ and $\overline{\mathcal{L}}$ to the primary vertices. The secondary vertices are v_{10}, v_{11} and v_{12} (coloured in black).



Example 4.23. Suppose $h_1 = 12$, $h_2 = 6$, $s = 4$, $t = 2$ and $c = 1$.



The central vertices are v_1, v_2 and v_3, which are once again coloured orange. There are 9 blue primary vertices (v_4 to v_{12}), 3 green primary ones (v_{13} to v_{15}) and 9 secondary vertices (v_{16} to v_{24}).

4.3. A special case

In this section, still assuming ℓ is a split prime, we specialize to the case where $N = 1$ and the ideals of $\mathcal{O}$ above ℓ are principal. In this case, we can describe the structure of $\mathcal{C}_0$ more precisely and give a less combinatorial proof.

Proposition 4.24. *Let E be an elliptic curve of level zero and P a point on E of order p^m. Let $\mathcal{O}$ be the endomorphism ring of E. Assume that the two ideals above ℓ in $\mathcal{O}$ are principal ideals $\mathfrak{L} = (x)$ and $\overline{\mathfrak{L}} = (\overline{x})$. Let $\mathcal{C}_0$ be the connected component of $\mathcal{C}(G_1^m)$ containing (E, P). Let $V(\mathcal{C}_0) = \{v_1, \ldots, v_u\}$. Assume that $\mathcal{C}_0$ does not contain any loops. Then $\mathcal{C}_0$ satisfies one of the following conditions.*

(1) For every $1 \leq i \leq u$, there is an edge from v_i to v_{i+1} (here we consider the indices modulo u). Furthermore, there exists $r \in \{1, 2, \ldots, u\}$ such that there is an edge from v_i to v_{i+r} for $1 \leq i \leq u$.

(2) We have $\operatorname{lcm}(h_1, h_2) = u$, where h_1 and h_2 are given as in Definition 4.5. Let $t_i = u/h_i$. Then there is an integer r that is coprime to u such that for $1 \leq i \leq u$ the targets of the edges whose source is v_i are given by v_{i+t_1} and v_{i+rt_2}, respectively.

Remark 4.25. The order of x (resp. $\overline{x}$) in $(\mathcal{O}/\overline{\mathfrak{p}}^m)^\times/\mathcal{O}^\times$ is equal to h_1 (resp. h_2). Here, we have denoted the image of $\mathcal{O}^\times$ in $(\mathcal{O}/\overline{\mathfrak{p}}^m)^\times$ by the same symbol as before. Suppose that $h_1 \geq h_2$.

We will see in the proof that case (1) occurs when $h_2|h_1$. In this case, $u = h_1$ and the blue edges form the directed cycle $v_1 \to v_2 \to \cdots \to v_u \to v_1$. The edges from v_i to v_{i+r} are green. Furthermore, the central vertices are of the form $v_{1+\alpha r}$, $\alpha \in \mathbb{Z}$. There are no secondary vertices.

Still assuming $h_1 \geq h_2$, if $h_2 \nmid h_1$, then case (2) occurs. The edges of the form $v_i \to v_{i+t_1}$ are blue, whereas those of the form $v_i \to v_{i+rt_2}$ are green. The central vertices are of the form $v_{1+\alpha r t_1 t_2}$, $\alpha \in \mathbb{Z}$. ♢

Remark 4.26. We have seen in the proof of Lemma 2.11 that when m is sufficiently large, the hypothesis that $\mathcal{C}_0$ does not admit any loops holds. ♢

Proof. Let $K = \mathcal{O} \otimes \mathbb{Q}$. Note that $\operatorname{Aut}(E[p^m]) \cong (\mathbb{Z}/p^m\mathbb{Z})^\times$. In particular, the group of automorphisms is cyclic. Let $\mathbf{E}$ be a CM lift of E over $K(j(\mathcal{O}))$ and let $\overline{\mathfrak{p}}$ be a prime ideal above p in $\mathcal{O}$ such that $\mathbf{E}[\overline{\mathfrak{p}}^m]$ reduces to $E[p^m]$ modulo some fixed ideal above p in the ring of integers of $K(j(\mathcal{O}))$. There is a natural isomorphism

$$\operatorname{Aut}(E[p^m]) \cong (\mathcal{O}/\overline{\mathfrak{p}}^m)^\times.$$

The two horizontal degree ℓ isogenies of E act on the p^m-torsion points by $[x]$ and $[\overline{x}]$, respectively. As we have discussed in Remark 4.25, h_1 (resp. h_2) is the order of x (resp. $\overline{x}$) as an element in $(\mathcal{O}/\overline{\mathfrak{p}}^m)^\times/\mathcal{O}^\times$. Without loss of generality, we assume that $h_1 \geq h_2$.

We first consider the case $h_2 \mid h_1$. As $(\mathcal{O}/\overline{\mathfrak{p}}^m)^\times$ is a cyclic group, there exists an integer r such that the cosets $\mathcal{O}^\times\overline{x}$ and $\mathcal{O}^\times x^r$ in $\mathcal{O}/\overline{\mathfrak{p}}^m$ coincide. Note that $\gcd(h_1, r) = h_1/h_2$.

Consider the closed blue path

$$C : v_1 \to \cdots \to v_{h_1} \to v_1$$

obtained by repeatedly applying $[x]$ to (E, P). If we apply $[\overline{x}]$ to v_i, we obtain a closed green path of the form $v_i \to v_{i+r} \to v_{i+2r} \to \cdots \to v_i$. In particular, we see that C contains all vertices of $\mathcal{C}_0$ and so $u = h_1$ and $\mathcal{C}_0$ is described as in (1).

We now consider the case where h_2 does not divide h_1. Then there exist integers $t_1, t_2 > 1$ such that $h_1 t_1 = h_2 t_2 = \operatorname{lcm}(h_1, h_2)$. Let

$$z = \gcd(h_1, h_2) = h_1/t_2 = h_2/t_1.$$

We see that both x^{t_2} and $\overline{x}^{t_1}$ have order z as elements in the cyclic group $(\mathcal{O}/\overline{\mathfrak{p}}^m)^\times/\mathcal{O}^\times$. Thus, there exists an integer r coprime to z such that the cosets $\mathcal{O}^\times\overline{x}^{t_1}$ and $\mathcal{O}^\times x^{rt_2}$ coincide in $(\mathcal{O}/\overline{\mathfrak{p}}^m)^\times$.

As $[x]$ and $[\overline{x}]$ commute, each path in $\mathcal{C}_0$ is given by $[x^a\overline{x}^b]$ for some integers a and b. Thus, the number of vertices in $\mathcal{C}_0$ is given by the cardinality of the subgroup U generated by x and $\overline{x}$ in $(\mathcal{O}/\overline{\mathfrak{p}}^m)^\times/\mathcal{O}^\times$. Let

$$\Phi: \mathbb{Z}/h_1\mathbb{Z} \times \mathbb{Z}/h_2\mathbb{Z} \to U,$$

be the surjective group homomorphism given by $(a, b) \mapsto x^a\overline{x}^b$. By the definition of r, the kernel of Φ is generated by $(rt_2, -t_1)$, which generates a cyclic subgroup of $\mathbb{Z}/h_1\mathbb{Z} \times \mathbb{Z}/h_2\mathbb{Z}$ of order z. It follows that there are in total $u = h_1h_2/z = \operatorname{lcm}(h_1, h_2)$ vertices in $\mathcal{C}_0$.

By adding a multiple of z to r if necessary, we may assume that r is coprime to u. Consider the group homomorphism

$$\Theta: \mathbb{Z}/h_1\mathbb{Z} \times \mathbb{Z}/h_2\mathbb{Z} \to \mathbb{Z}/u\mathbb{Z}, \quad (a, b) \mapsto at_1 + brt_2.$$

Since t_1 and rt_2 are coprime integers, Θ is surjective and the kernel is generated by $(rt_2, -t_1)$. Let $(E, P) = v_1$. We enumerate the vertices of $\mathcal{C}_0$ so that $v_{\Theta((a,b))} = [x^a\overline{x}^b]v_1$. It then follows that $[x]$ (resp. $[\overline{x}]$) induces a blue (resp. green) edge from v_i to v_{i+t_1} (resp. v_{i+rt_2}) as described in (2). □

Remark 4.27.

- If x and $\overline{x}$ act trivially on $E[p]$, then the order of x and $\overline{x}$ in $\operatorname{Aut}(E[p^m])$ will always be a p-power. In this case $\mathcal{C}_0$ is described by (1).
- If $m = 1$ and $\mathcal{C}_0$ is described by (2), then $\mathcal{C}_0$ is described by (2) for all $m \geq 1$.
- If $m = 2$ and the structure of $\mathcal{C}_0$ is described by (1), then $\mathcal{C}_0$ is described by (1) for all $m \geq 2$. ♢

Example 4.28. Let $K = \mathbb{Q}(\sqrt{-5})$ and $p = 3$. We consider an elliptic curve $\mathbf{E}$ with complex multiplication by $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. The two prime ideals above 3 are $(3, 1 + \sqrt{-5})$ and $(3, 1 - \sqrt{-5})$. We take $\overline{\mathfrak{p}} = (3, 1 + \sqrt{5})$. Let $\ell = 409$. Then the two ideals above (409) in $\mathcal{O}_K$ are $(2 + 9\sqrt{-5})$ and $(2 - 9\sqrt{-5})$. Let $x = 2 + 9\sqrt{-5}$. Then

$$x \equiv \overline{x} \equiv 2 \pmod{(3, 1 + \sqrt{-5})^2}.$$

It can be checked that 2 is indeed a generator of $(\mathcal{O}_K/(3, 1+\sqrt{-5})^2)^\times$. It follows that the orders of x and $\overline{x}$ in $(\mathcal{O}_K/(3, 1 + \sqrt{-5})^m)^\times/\{\pm 1\}$ are 3^{m-1}. Thus, the graph $\mathcal{C}_0$ obtained from $\mathbf{E} \pmod{\mathfrak{p}}$ is described by case (1) of Proposition 4.24 with $u = 3^{m-1}$. ♢

Example 4.29. Let $K = \mathbb{Q}(\sqrt{-10})$ and $p = 13$. We consider again an elliptic curve $\mathbf{E}$ with complex multiplication by $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{-10}$. The two ideals over 13 are $(13, 4 + \sqrt{-10})$ and $(13, 4 - \sqrt{-10})$. Let $\overline{\mathfrak{p}} = (13, 4 + \sqrt{-10})$. Let $\ell = 11$. The two ideals over (11) are given by $(1 + \sqrt{-10})$ and $(1 - \sqrt{-10})$. Let $x = 1 + \sqrt{-10}$. Then

$$x \equiv -3 \pmod{(13, 4 + \sqrt{-10})}$$

and

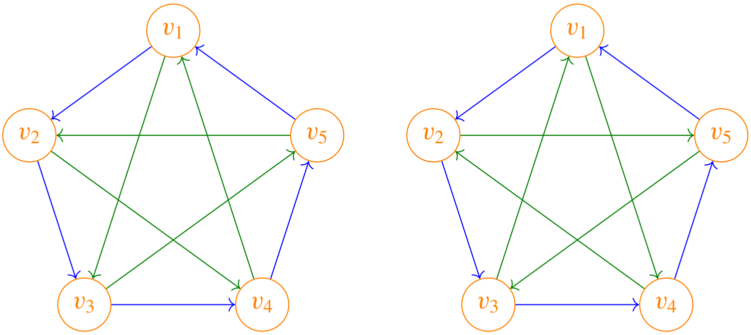
$$\overline{x} \equiv 5 \pmod{(13, 4 + \sqrt{-10})}.$$

The order of -3 in $(\mathcal{O}_K/(13, 4+\sqrt{-10}))^\times/\{\pm 1\}$ is 3, while the order of 5 is 2. It follows that for $m = 1$, the graph $\mathcal{C}_0$ obtained from $\mathbf{E} \pmod{\overline{\mathfrak{p}}}$ is described by case (2) of Proposition 4.24 with $u = 6$, $h_1 = 3$ and $h_2 = 2$. ◊

We conclude this section with a number of illustrations of several graphs given by Proposition 4.24.

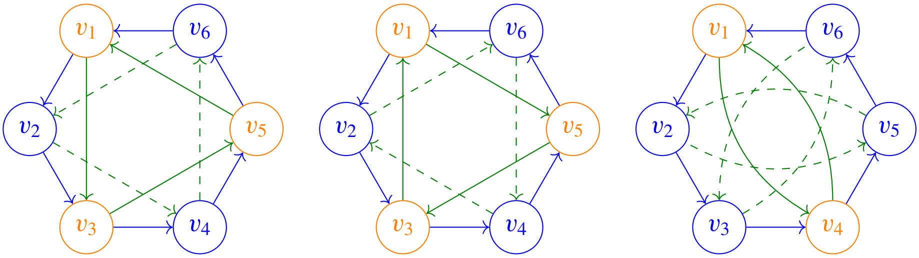
Case (1) with $u = 5$

Since we have assumed that there is no loop, we have $h_1, h_2 > 1$. Thus, in order for case (1) to occur, we must have $h_1 = h_2 = 5$. Every vertex is central and we have the complete graph K_5 (after ignoring the directions). Depending on the value of r, we have one of the following two graphs.



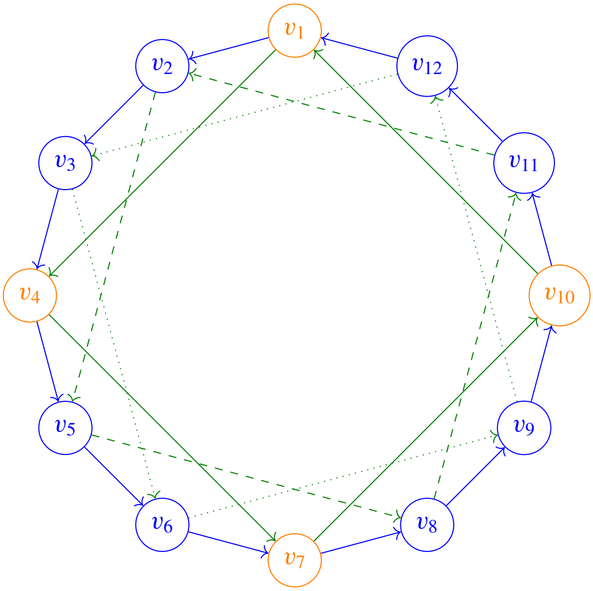
Case (1) with $u = 6$

We have $h_1 = 6$. We illustrate the cases where $h_2 = 3$ and $h_2 = 2$ below. When $h_2 = 3$, r can be either 2 or 4.



Case (1) with $u = 12$

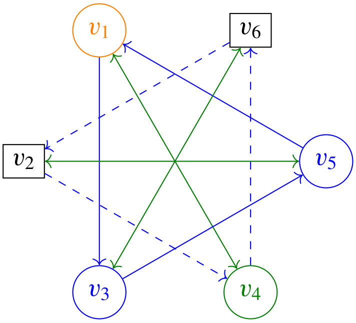
Suppose that $h_1 = 12$, $h_2 = 4$ with $r = 3$. We have the following graph.



If $r = 9$, then the directions of the green edges are reversed.

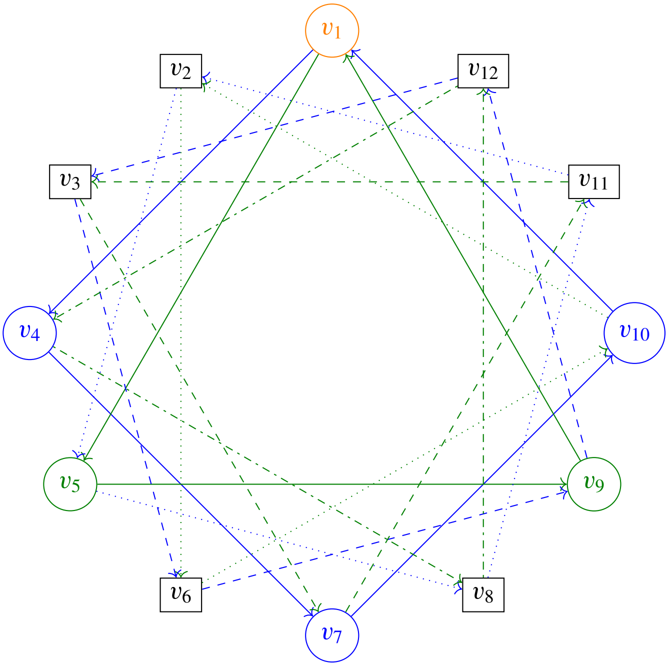
Case (2) with $u = 6$

Suppose that $h_1 = 3$, $h_2 = 2$ and $r = 1$. Then $t_1 = 2$ and $t_2 = 3$. We have the following graph:



Case (2) with $u = 12$

Suppose that $h_1 = 4$, $h_2 = 3$ and $r = 1$. Then $t_1 = 3$, $t_2 = 4$, resulting in the following graph:



5. An inverse problem for craters

The goal of this section is to prove Theorem B stated in the introduction. In particular, we study an inverse problem for the graphs arising in Section 4.2. We first introduce the following definition of graphs, which can be regarded as a partial generalization of abstract volcano graphs introduced in [2, Definition 4.1].

Definition 5.1. Let $\mathfrak{r}$, $\mathfrak{s}$, $\mathfrak{t}$, $\mathfrak{c}$ be nonnegative integers. We say that a directed graph is an **abstract tectonic crater** of parameters $(\mathfrak{r}, \mathfrak{s}, \mathfrak{t}, \mathfrak{c})$ if it satisfies

(a) There are $\mathfrak{r}\mathfrak{s}\mathfrak{t}$ vertices;
(b) Each edge is assigned a colour — blue or green;
(c) At each vertex v, there is exactly one blue edge with v as the source, and exactly one blue edge with v as the target, and similarly for green edges;
(d) Starting at each vertex, there is exactly one closed blue (resp. green) path without backtracks of length $\mathfrak{r}\mathfrak{s}$ (resp. $\mathfrak{r}\mathfrak{t}$);
(e) After every $\mathfrak{s}$ (resp. $\mathfrak{c}\mathfrak{t}$) steps in the closed blue (resp. green) paths given in (d), the two paths meet at a common vertex.

We now prove Theorem B.

Theorem 5.2. *Let G be an abstract tectonic crater. There exist infinitely many pairs of distinct primes p and ℓ, and nonnegative integers N such that one of the connected components of the crater of the ℓ-isogeny graph G_N^1 (over $\mathbb{F}_p$) is isomorphic to G.*

Remark 5.3. We emphasize that an abstract tectonic crater can never describe a connected component of G_1^0. Indeed, each vertex v in an abstract tectonic admits 4 edges, two with source v and to with target v. In G_1^0 each vertex admits at most two vertices. Thus, the level structure is crucial for the above result.

Proof. Let (Ω, s, t, c) be the parameters of G. We shall construct a $\mathcal{C}_0$ that is isomorphic to G where the symbols Ω, s, t, c have the same significations as those assigned in Remark 4.21.

Let K be an imaginary quadratic field different from $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$. Let $\mathfrak{f}$ be an ideal coprime to 10 and let $F = K(\mathfrak{f})$ be the ray class field of conductor $\mathfrak{f}$. Then there exists an elliptic curve $\mathbf{E}/F$ that has complex multiplication by $\mathcal{O}_K$ and such that $K(\mathbf{E}_{\mathrm{tors}})/K$ is abelian (see [4, Lemma 2] or [5, Chapter II, 1.4]). Let $L' = F(\mathbf{E}[5])$. Then, the theory of complex multiplication tells us that $\mathrm{Gal}(L'/K) \cong (\mathcal{O}_K/(5))^\times/\{\pm 1\}$.

Let p be a prime number such that

- $p \neq 5$;
- $p \equiv 1 \pmod{\Omega}$;
- p is totally split in F.

Then $\mathbf{E}$ has good ordinary reduction at all the primes of F lying above p. We fix once and for all a prime $\mathfrak{p}'|p$ of F. Let $\mathfrak{p}$ be the unique prime of K lying below $\mathfrak{p}'$.

Choose two different prime numbers N' and M' that are coprime to $5p\mathfrak{f}$ and are split in K, with $N' \equiv 1 \pmod{s}$ and $M' \equiv 1 \pmod{t}$. Let $\mathfrak{N}$ (resp. $\mathfrak{M}$) be a prime ideal of $\mathcal{O}_K$ lying above N' (resp. M'). Let $L = F(\mathbf{E}[5N'M'])$. Define furthermore $L_1 = F(\mathbf{E}[5N'M'\overline{\mathfrak{p}}])$ and $L_2 = F(\mathbf{E}[5N'M'\mathfrak{p}])$. We have the following group isomorphisms

$$\mathrm{Gal}(L_1/L') \cong (\mathcal{O}_K/\mathfrak{N})^\times \times (\mathcal{O}_K/\overline{\mathfrak{N}})^\times \times (\mathcal{O}_K/\mathfrak{M})^\times \times (\mathcal{O}_K/\overline{\mathfrak{M}})^\times \times (\mathcal{O}_K/\overline{\mathfrak{p}})^\times, \quad (5.1)$$

and

$$\mathrm{Gal}(L_2/L') \cong (\mathcal{O}_K/\mathfrak{N})^\times \times (\mathcal{O}_K/\overline{\mathfrak{N}})^\times \times (\mathcal{O}_K/\mathfrak{M})^\times \times (\mathcal{O}_K/\overline{\mathfrak{M}})^\times \times (\mathcal{O}_K/\mathfrak{p})^\times. \quad (5.2)$$

Furthermore $L_1 \bigcap L_2 = L$.

By Tchebotarev's theorem, there exists a prime ideal $\mathfrak{L}$ in $\mathcal{O}_K$ such that

(i) $\mathfrak{L}$ splits in L'/K;
(ii) $\mathfrak{L} \neq \overline{\mathfrak{L}}$;
(iii) The Frobenius of $\mathfrak{L}$ in $\mathrm{Gal}(L_1/L')$ gives rise to an element of the form $(a, 1, 1, b, d)$ on the right-hand side of (5.1), where $\mathrm{ord}(a) = s$, $\mathrm{ord}(b) = t$ and $\mathrm{ord}(d^s) = \Omega$;
(iv) The Frobenius of $\mathfrak{L}$ in $\mathrm{Gal}(L_2/L')$ gives rise to an element of the form $(a, 1, 1, b, d')$ on the right-hand side of (5.2), with $\mathrm{ord}(d')^t = \Omega$ and $d'^{ct} = d^s$ (after identifying $\mathcal{O}/\overline{\mathfrak{p}}$ with $\mathcal{O}/\mathfrak{p}$ via complex conjugation).

Let σ (resp. τ) be the Frobenius of $\mathfrak{L}$ (resp. $\overline{\mathfrak{L}}$) in $\mathrm{Gal}(L_1/L)$. Note that τ gives an element of the form $(1, a, b, 1, d')$ on the right-hand side of (5.1).

Let H_1 (resp. H_2) be the cyclic subgroup of $\mathrm{Gal}(L_1/L')$ generated by σ (resp. τ). Let Q be a primitive $5\mathfrak{N}\mathfrak{M}$-torsion point on $\mathbf{E}$. Then σ (resp. τ) acts on Q via $(a, 1, 1, 1, 1)$ (resp. $(1, 1, b, 1, 1)$). The orbit of Q under the action of H_1 (resp. H_2) contains s (resp. t) elements. As σ and τ fix $\mathbf{E}[5]$ by construction, $-Q$ is not contained in either of these orbits and the only point contained in both orbits is Q.

Now, let P be a primitive $5\mathfrak{N}\mathfrak{M}\bar{\mathfrak{p}}$-torsion point in $\mathbf{E}$ such that $pP = Q$. By the conditions (iii) and (iv), the orbit of P under the action of H_1 contains $s\Omega$ elements, whereas that under H_2 contains $t\Omega$ elements. Again neither of these orbits contains $-P$. Note that σ^s is of the form $(a^s, 1, 1, b^s, d^s)$, while τ^{ct} is of the form $(1, a^{ct}, b^{ct}, 1, d'^{ct})$ by construction, and both elements act on P via $(1, 1, 1, d^s)$. Therefore, $\sigma^s(P) = \tau^{ct}(P)$ and the orbits of P under H_1 and H_2 intersect precisely in the set $\{P, \sigma^s P, \sigma^{2s} P, \dots, \sigma^{(\Omega-1)s} P\}$.

We have $\sigma(P) = \phi(P)$, where ϕ is the isogeny $\mathbf{E} \to \mathbf{E}/\mathbf{E}[\mathfrak{L}] \cong \mathbf{E}$ and likewise for τ (see [5, Chapter II, 1.3 and 1.4]). Let $E = \mathbf{E} \pmod{\mathfrak{p}'}$, ℓ be the rational prime below $\mathfrak{L}$ and $N = 5N'M'$. Then the connected component $\mathcal{C}_0$ containing $(E, P \pmod{\mathfrak{p}'})$ is precisely the tectonic crater G. □

Remark 5.4. Let $u = \mathrm{lcm}(h_1, h_2)$ and suppose that there are u vertices in $\mathcal{C}_0$. Let $V = \{v_1, \dots, v_u\}$ be the set of vertices. After relabelling if necessary, we have blue edges going from v_i to v_{i+u/h_1} and green edges from v_i to $v_{i+c\cdot u/h_2}$ for some c that is coprime to u.

We have seen in Remark 4.21 that the total number of vertices is given by $h_2 s = h_1 t$. Thus, we have

$$u = \mathrm{lcm}(h_1, h_2) = h_2 s = h_1 t.$$

This happens if the smallest subgroup of $\mathrm{Aut}(V)$ containing H_1 and H_2 is cyclic (where H_1 and H_2 are the subgroups defined in the proof of Theorem 5.2). If H has rank two, the graph contains two blue directed cycles, as in Examples 4.22 and 4.23. ♢

CRediT authorship contribution statement

Antonio Lei: Writing – review & editing, Writing – original draft, Supervision, Investigation, Funding acquisition, Conceptualization. **Katharina Müller:** Writing – review & editing, Writing – original draft, Investigation, Conceptualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgements

We thank Pete Clark, Daniel Larsson, Fabien Pazuki and Daniel Vallières for interesting discussions during the preparation of this article. We are also indebted to the anonymous referees for helpful comments and suggestions which led to many improvements in the article. The authors' research is supported by the NSERC Discovery

Grants Program RGPIN-2020-04259 and RGPAS-2020-00096. Parts of this paper is based upon work supported by the National Science Foundation, United States under Grant No. DMS-1928930 while A. L. was in residence at the MSRI/Simons Laufer Mathematical Sciences Institute (SLMath) in Berkeley, California, during the Spring 2023 semester.

Appendix. Voltage assignment

The goal of this appendix is to describe the voltage assignment associated with the tower $(G_1^m)_{m\geq 0}$. Let us recall the definition of a voltage assignment on a directed graph.

Definition A.1. Let X be a directed graph, $(G, \cdot)$ an abelian group and $n \geq 1$ an integer. A G-valued **voltage assignment** on X is a function $\alpha : \mathbb{E}(X) \to G$.

To each voltage assignment, we define the derived graph $X(G, \alpha)$ whose vertices and edges are given by $V(X) \times G$ and $\mathbb{E}(X) \times G$ respectively. If $(e, \sigma) \in \mathbb{E}(X) \times G$, it links (s, σ) to $(t, \sigma \cdot \alpha(e))$, where e is an edge in X from s to t.

Note that $X(G, \alpha) \to X$ given by $(x, \sigma) \mapsto x$ is a graph covering.

Let $X = G_1^0$. For each $E \in \mathcal{E}$, we fix a group isomorphism

$$\Phi_E : E[p^\infty] \to \mathbb{Q}_p/\mathbb{Z}_p.$$

This is equivalent to fixing a $\mathbb{Z}_p$-basis of the p-adic Tate module $T_p(E)$. More explicitly, let t_E be such a basis. Given $P \in E[p^m]$, we have $\Phi_E(P) = a/p^m + \mathbb{Z}_p$ for a unique integer $a \in \{0, 1, \dots, p^m - 1\}$.

$$\Phi_E(P) = a\overline{t_E}, \tag{A.1}$$

where $\overline{t_E}$ denotes the image of t_E in $E[p^m]$.

Let us write $Z_m = \frac{1}{p^m}\mathbb{Z}_p/\mathbb{Z}_p$ and $Z_m^* = Z_m \setminus Z_{m-1}$, which we may identify with $(\mathbb{Z}/p^m\mathbb{Z})^\times$. Then, we may identify the vertices of G_1^m with $G_1^0 \times Z_m^*$, given by $(E, P) \mapsto (E, \Phi_E(P))$. Under (A.1), $\Phi_E(P)$ is given by the image of a in $(\mathbb{Z}/p^m\mathbb{Z})^\times$.

Definition A.2. Let $E_1, E_2 \in \mathcal{E}$. Suppose that there exists an ℓ-isogeny $\phi : E_1 \to E_2$. For each equivalence class of degree ℓ-isogenies we fix one representative ϕ. We write $t_\phi \in \mathbb{Z}_p^\times$ to be the unique element such that

$$\phi^*(t_{E_1}) = t_\phi \cdot t_{E_2}, \tag{A.2}$$

where $\phi^* : T_p(E_1) \to T_p(E_2)$ is the $\mathbb{Z}_p$-isomorphism induced by ϕ.

Let $\phi : E \to E'$ be an ℓ-isogeny. This induces an edge e in G_1^0. Consider the corresponding edge from (E, P) to (E', P') in G_1^m. Then, one can check that

$$\Phi_E(P)t_\phi = \Phi_{E'}(P').$$

Therefore, we may identify G_1^m with the voltage graph $X((\mathbb{Z}/p^m\mathbb{Z})^\times, \alpha)$, where α is the voltage assignment α on G_1^m sending ϕ to $t_\phi \pmod{p^m}$.

Remark A.3. While our voltage assignment depends on a choice of basis for each $T_p(E)$ as E runs through $\mathcal{E}$. This can be regarded as the analogue of picking a spanning tree of G_1^0 (when it is connected) as in [7, Theorem 2.11]. Indeed, suppose that G_1^0 is connected and $\mathcal{T}$ is a spanning tree. Since $\ell \neq p$, an ℓ-isogeny $\phi : E_1 \to E_2$ induces an isomorphism $\phi^* : T_p(E_1) \to T_p(E_2)$. Thus, once a basis is picked for one $E \in \mathcal{E}$, this basis can be propagated to all other curves in $\mathcal{E}$ along $\mathcal{T}$. ◊

Remark A.4. Since we have realized G_1^m as a voltage graph arising from a voltage assignment on G_1^0, this gives an alternative proof of Lemma 2.7 in the special case where $N = 1$. ◊

References

[1] Sarah Arpin, Adding level structure to supersingular elliptic curve isogeny graphs, 2022, to appear in J. Théor. Nombres Bordeaux, arXiv:2203.03531.

[2] Henry Bambury, Francesco Campagna, Fabien Pazuki, Ordinary isogeny graphs over $\mathbb{F}_p$: The inverse volcano problem, 2022, preprint, arxiv: 2210.01086.

[3] Giulio Codogni, Guido Lido, Spectral theory of isogeny graphs, 2023, preprint, arXiv:2308.13913.

[4] Vlad Crişan, Katharina Müller, The vanishing of the μ-invariant for split prime $\mathbb{Z}_p$-extensions over imaginary quadratic fields, Asian J. Math. 24 (2) (2020) 267–302.

[5] Ehud de Shalit, Iwasawa theory of elliptic curves with complex multiplication, in: Perspectives in Mathematics, vol. 3, Academic Press, Inc., Boston, MA, 1987, p. x+154, p-adic L functions.

[6] Daniel Delbourgo, Heiko Knospe, On Iwasawa λ-invariants for abelian number fields and random matrix heuristics, Math. Comp. 92 (342) (2023) 1817–1836.

[7] Cédric Dion, Antonio Lei, Anwesh Ray, Daniel Vallières, On the distribution of Iwasawa invariants associated to multigraphs, Nagoya Math. J. 253 (2024) 48–90.

[8] Jordan S. Ellenberg, Sonal Jain, Akshay Venkatesh, Modeling λ-invariants by p-adic random matrices, Comm. Pure Appl. Math. 64 (9) (2011) 1243–1262.

[9] Eyal Z. Goren, Payman L. Kassaei, p-adic dynamics of Hecke operators on modular curves, J. Théor. Nombres Bordeaux 33 (2) (2021) 387–431.

[10] Haruzo Hida, Irreducibility of the Igusa tower, Acta Math. Sin. (Engl. Ser.) 25 (1) (2009) 1–20.

[11] Jun-ichi Igusa, Kroneckerian model of fields of elliptic modular functions, Amer. J. Math. 81 (1959) 561–577.

[12] Kenkichi Iwasawa, Analogies between number fields and function fields, in: Some Recent Advances in the Basic Sciences, Vol. 2 (Proc. Annual Sci. Conf., Belfer Grad. School Sci., Yeshiva Univ., New York, 1965-1966), Yeshiva Univ., Belfer Graduate School of Science, New York, 1969, pp. 203–208.

[13] Kenkichi Iwasawa, On $\mathbf{Z}_\ell$-extensions of algebraic number fields, Ann. of Math. (2) 98 (1973) 246–326.

[14] Nicholas M. Katz, Barry Mazur, Arithmetic moduli of elliptic curves, in: Annals of Mathematics Studies, vol. 108, Princeton University Press, Princeton, NJ, 1985, p. xiv+514.

[15] David Russell Kohel, Endomorphism Rings of Elliptic Curves Over Finite Fields (Ph.D. thesis –University of California, Berkeley), ProQuest LLC, Ann Arbor, MI, 1996, p. 117.

[16] Serge Lang, Elliptic functions, second ed., in: Graduate Texts in Mathematics, vol. 112, Springer-Verlag, New York, 1987, p. xii+326, With an appendix by J. Tate.

[17] Antonio Lei, Katharina Müller, On towers of isogeny graphs with full level structure, 2023, preprint, arXiv:2309.00524.

[18] Antonio Lei, Katharina Müller, On the zeta functions of supersingular isogeny graphs andmodular curves, Arch. Math. 122 (3) (2024) 2851–294.

[19] B. Mazur, A. Wiles, Analogies between function fields and number fields, Amer. J. Math. 105 (2) (1983) 507–521.

[20] Kevin McGown, Daniel Vallières, On abelian ℓ-towers of multigraphs II, Ann. Math. Qué. 47 (2) (2023) 461–473.

[21] Kevin McGown, Daniel Vallières, On abelian ℓ-towers of multigraphs III, Ann. Math. Qué. 48 (1) (2024) 1–19.

[22] Nathanaël Munier, Ari Shnidman, Sandpile groups of supersingular isogeny graphs, J. Théor. Nombres Bordeaux 35 (3) (2023) 751–774.

[23] Riccardo Pengo, Daniel Vallières, Spanning trees in $\mathbb{Z}$-covers of a finite graph and Mahler measures, 2023, preprint, arXiv:2310.15619.

[24] Megan Roda, Supersingular Isogeny Graphs with Level N Structure and Path Problems on Ordinary Isogeny Graphs (Master thesis), McGill University, 2019, https://escholarship.mcgill.ca/concern/theses/c247dx821.

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

[26] Andrew V. Sutherland, Isogeny volcanoes, in: ANTS X—PRoceedings of the Tenth Algorithmic Number Theory Symposium, in: Open Book Ser., vol. 1, Math. Sci. Publ., Berkeley, CA, 2013, pp. 507–530.

[27] Daniel Vallières, On abelian ℓ-towers of multigraphs, Ann. Math. Qué. 45 (2) (2021) 433–452.

[28] Guanju Xiao, Zijian Zhou, Longjiang Qu, Oriented supersingular elliptic curves and eichler orders, 2023, preprint, arXiv 2312.08844.