

ORDINARY ISOGENY GRAPHS OVER \mathbb{F}_p : THE INVERSE VOLCANO PROBLEM

HENRY BAMBURY, FRANCESCO CAMPAGNA, FABIEN PAZUKI

ABSTRACT. We give a detailed presentation of ℓ -isogeny graphs associated with ordinary elliptic curves defined over \mathbb{F}_p . We then focus on the following inverse problem: given an abstract volcano V , do there always exist primes $\ell, p \in \mathbb{N}$ such that the ordinary ℓ -isogeny graph over \mathbb{F}_p contains V as a connected component? We provide an affirmative answer to this question.

Keywords: Isogenies, modular polynomials.

Mathematics Subject Classification: 11G18, 11G20, 14G17, 14K02.

1. INTRODUCTION

Given a finite field \mathbb{F} of characteristic p and a prime number $\ell \neq p$, one can consider the so-called ℓ -isogeny graph over \mathbb{F} . Roughly speaking, one can construct this graph \mathcal{G} by taking as vertices the elements of \mathbb{F} , which in this context are seen as the j -invariants of elliptic curves defined over \mathbb{F} , and by drawing an oriented edge from one vertex to another if there is a geometric isogeny of degree ℓ between the corresponding elliptic curves. The graph \mathcal{G} naturally decomposes into two subgraphs \mathcal{G}_{ord} and \mathcal{G}_{ss} , which are respectively induced by the elements of \mathbb{F} that are j -invariants of ordinary and supersingular elliptic curves. Pictorially, the structural difference between these two subgraphs is clear.

The supersingular isogeny graph \mathcal{G}_{ss} has been first studied in [10] as an example of large Ramanujan graph. Due to their complicated structure, supersingular isogeny graphs have found several cryptographic applications, see for instance [1] and [3]. On the other hand, the ordinary isogeny graph \mathcal{G}_{ord} has a much more regular structure which has first been studied in the seminal work of Kohel [5] and subsequently by Fouquet and Morain [4]. In particular, in [4] the authors coined the term *isogeny volcano* to denote connected components of \mathcal{G}_{ord} . This terminology is justified by the fact that the connected components of ordinary isogeny graphs often appear as a cycle, the *crater*, whose vertices are roots of isomorphic trees, the *lava flows*. Because of this satisfyingly regular structure, ordinary isogeny graphs have attracted a lot of attention, finding applications both in computational number theory (see for instance [15, 14]) and in cryptography (see for instance [7]).

We focus here on ordinary isogeny graphs over \mathbb{F}_p and the text consists of two parts. The first part is essentially a review of known results on the structure of \mathcal{G}_{ord} . We gather in a unique place the terminology that appeared in different works and provide details when needed. Within what we call the *volcano park*, we thus identify the *cordilleras* in Section 3.1, the *belts* in Section 3.2, and finally the *volcanoes* in Section 3.3. We also treat in full detail the pathological cases corresponding to the j -invariants 0 and 1728 (see for instance Propositions 3.19 and 3.20). The geological lexicon we use is sometimes new and sometimes borrowed from previous works; for instance, the term “cordillera” first appeared in [7].

In the second part of this manuscript we solve the following inverse problem: suppose we are given an abstract volcano graph V , *i.e.* a graph that looks like a genuine volcano (see Definition 4.1); does there then exist a pair of distinct primes ℓ and p such that the ordinary ℓ -isogeny

graph over \mathbb{F}_p has V as a connected component? If the target abstract volcano is given only as a crater with no lava flows, the answer to this question is easier since we have a lot of freedom in the choice of ℓ and p . We prove the following result (see again Definition 4.1 for terminology):

Theorem 1.1. *Let V be an abstract volcano of depth 0. Then there exists infinitely many distinct primes $p, \ell \in \mathbb{Z}$ such that V is a connected component of the ℓ -isogeny graph over \mathbb{F}_p .*

On the other hand, if V has lava flows then the inverse volcano problem becomes more difficult, since the theory of isogeny volcanoes now fixes ℓ uniquely (we speak of ℓ -volcano in this case) and we thus only have freedom on the choice of p . We prove nonetheless:

Theorem 1.2. *Let $\ell \in \mathbb{N}$ be a prime number and let V be an abstract ℓ -volcano of depth $d > 0$. Then there exists infinitely many primes $p \in \mathbb{Z}$ such that V is a connected component of the ℓ -isogeny graph over \mathbb{F}_p .*

The proofs of Theorems 1.1 and 1.2 feature a study of elements in the class group of imaginary quadratic fields: in a nutshell, volcanoes with crater size n exist because one can find ideal classes in well-chosen imaginary quadratic fields with order n . To study these questions on orders of elements in class groups, we are lead to study and explicitly solve some diophantine equations. Using variations of arguments of Nagell, Mahler, Pell, one is able to prove the following key step:

Theorem 1.3. *The following properties hold.*

- (1) *Let $n \neq 4$ be a positive integer and let $K = \mathbb{Q}(\sqrt{1 - 2^{n+2}})$. Then in \mathcal{O}_K the prime 2 splits into two prime ideals whose corresponding classes in $\text{Cl}(\mathcal{O}_K)$ have order n .*
- (2) *Let $K = \mathbb{Q}(\sqrt{-39})$. Then in \mathcal{O}_K the prime 2 splits into two prime ideals whose corresponding classes in $\text{Cl}(\mathcal{O}_K)$ have order 4.*
- (3) *Let $\ell \in \mathbb{Z}$ be an odd prime and let $n \in \mathbb{Z}_{>0}$. Define $K_1 := \mathbb{Q}(\sqrt{1 - \ell^n})$ and $K_2 := \mathbb{Q}(\sqrt{1 - 4\ell^n})$. Then either in \mathcal{O}_{K_1} or in \mathcal{O}_{K_2} the prime ℓ splits into two prime ideals whose corresponding classes in $\text{Cl}(\mathcal{O}_{K_i})$ have order n .*

To obtain a proof of Theorem 1.3, we prove Propositions 4.6, 4.7, and 4.8. We are in fact more precise and are able to decide in the third item which of K_1 or K_2 is the correct field to consider, for a given pair (ℓ, n) .

In the final section, we discuss two follow-up projects: the first one concerns the inverse volcano problem over more general finite fields. We prove in Proposition 5.1 the existence of abstract 2-volcanoes such that for any prime $p \neq 2$, these are not connected components of ordinary isogeny graphs over \mathbb{F}_{p^2} . This triggers natural questions: how many exceptions can occur? Infinitely many or not? Do they come up with a specific shape? We plan to come back to these questions in future work.

The second project focuses on solving the inverse volcano problem with algorithmic efficiency: we provide an explicit solution to the inverse volcano problem over \mathbb{F}_p , but when working with concrete examples, it appears that one is often able to find number fields with smaller discriminants than the ones in our families. Is it possible to describe a solution with minimal discriminant? What is the smallest prime p that realises an abstract volcano as an isogeny volcano over \mathbb{F}_p ?

We also present a detailed study of the ordinary 3-isogeny graph over \mathbb{F}_{1009} in an appendix, including a complete picture of the corresponding volcano park ¹. We encourage the reader to take a look at this volcano park before starting, it is very beautiful!

¹All the heavy computations in this paper have been performed using the SageMath software [17]

ACKNOWLEDGEMENTS

The authors thank the IRN GandA (CNRS) and IRN MaDeF (CNRS) for support. HB thanks the University of Copenhagen for its hospitality. FP is supported by ANR-17-CE40-0012 Flair, FC and FP are both supported by ANR-20-CE40-0003 Jinvariant. FC is grateful to Max Planck Institute for Mathematics in Bonn for its hospitality and financial support. The three authors warmly thank Teresa Sorbera for helping in organising the workshop in Rømø, where the whole project started.

2. PRELIMINARIES

We gather general results on isogenies of elliptic curves and modular polynomials in this first section.

2.1. Isogenies of elliptic curves. Let k be either a finite field or a number field (which we suppose to be embedded in \mathbb{C}). By ℓ -isogeny between two elliptic curves over k we mean an isogeny of degree ℓ defined over \bar{k} . An elliptic curve E/k has complex multiplication by a ring R strictly containing \mathbb{Z} if $\text{End}_{\bar{k}}(E) \cong R$. An elliptic curve over a finite field is ordinary if R is an imaginary quadratic order. It is supersingular if R is an order in a quaternion algebra.

Proposition 2.1. *Let $\varphi : E_1 \rightarrow E_2$ be an ℓ -isogeny of ordinary elliptic curves over k with geometric endomorphism rings \mathcal{O}_1 and \mathcal{O}_2 . If $\text{char}(k) \neq \ell$ then $[\mathcal{O}_1 : \mathcal{O}_2] \in \{1/\ell, 1, \ell\}$.*

Proof. See [5, Proposition 21] or [14, §2.7]. □

Definition 2.2. Using the notations of Proposition 2.1, we say that φ is *horizontal* if $\mathcal{O}_1 = \mathcal{O}_2$. Otherwise φ is *vertical*; *descending* if $[\mathcal{O}_1 : \mathcal{O}_2] = \ell$, *ascending* if $[\mathcal{O}_2 : \mathcal{O}_1] = \ell$.

Remark 2.3. The dual of a horizontal isogeny is horizontal, and the dual of a vertical isogeny is vertical, ascending if the initial isogeny was descending, and vice versa.

Definition 2.4. Let \mathcal{O} be an imaginary quadratic order and let E/k be an elliptic curve with $\text{End}_{\bar{k}}(E) \cong \mathcal{O}$. For every \mathcal{O} -ideal \mathfrak{a} the \mathfrak{a} -torsion subgroup of E is defined as

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

The \mathfrak{a} -torsion subgroups correspond to isogenies $\varphi_{\mathfrak{a}} : E \rightarrow E/E[\mathfrak{a}]$ with kernel $E[\mathfrak{a}]$ and degree $\deg(\varphi_{\mathfrak{a}}) = N(\mathfrak{a})$. Here, $E/E[\mathfrak{a}]$ denotes the quotient elliptic curve of E by the subgroup $E[\mathfrak{a}]$. If \mathfrak{a} is an invertible ideal of $\text{End}_{\bar{k}}(E)$, then $\text{End}_{\bar{k}}(E/E[\mathfrak{a}]) \cong \text{End}_{\bar{k}}(E)$ (see [19, Proposition 3.9 and Theorem 4.5]).

We thus obtain an action of the group of invertible \mathcal{O} -ideals on the set of \bar{k} -isomorphism classes of elliptic curves with complex multiplication by \mathcal{O} , given by

$$\mathfrak{a} * E := E/E[\mathfrak{a}].$$

This action factors via a faithful and transitive action of the class group $\text{Cl}(\mathcal{O})$ of the order \mathcal{O} . If k is a number field, we can write $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ where $\Lambda \subseteq K := \text{Frac}(\mathcal{O})$ is an invertible ideal, and then one has

$$(E/E[\mathfrak{a}])(\mathbb{C}) \cong \mathbb{C}/\mathfrak{a}^{-1}\Lambda.$$

We then see that the above action corresponds to the classical one over complex numbers described for instance in [12, II, Proposition 1.2] for maximal orders. We summarise this discussion in the following theorem.

Theorem 2.5. *Let K be an imaginary quadratic field, and let \mathcal{O} be an order in K . Then, for every ideal class $[\mathfrak{a}] \in \text{Cl}(\mathcal{O})$ and every elliptic curve E/\bar{k} with $\text{End}_{\bar{k}}(E) \cong \mathcal{O}$ the association*

$$\mathfrak{a} * E := E/E[\mathfrak{a}]$$

defines a faithful and transitive action of the class group on the set of \bar{k} -isomorphism classes of elliptic curves with complex multiplication by \mathcal{O} .

Proof. If k is a number field the statement is proved in [6, Chapters 8 and 10]. If k is a finite field, the statement is proved in [19, Theorem 4.5]. \square

Definition 2.6. Let E and E' be elliptic curves over k . We say that two ℓ -isogenies $\varphi, \psi : E \rightarrow E'$ are equivalent if $\ker \varphi = \ker \psi$. This is the same as requiring that there exists $\alpha \in \text{Aut}_{\bar{k}}(E')$ such that $\alpha \circ \varphi = \psi$.

Lemma 2.7. *Let k be a finite field of characteristic p and let E/k be an elliptic curve with geometric endomorphism ring isomorphic to an order \mathcal{O} in an imaginary quadratic field K . Denote by f the conductor of \mathcal{O} . Then p does not divide f .*

Proof. By Deuring's lifting theorem [6, Chapter 13, Theorem 14] there exists an elliptic curve E' over $\overline{\mathbb{Q}}$ and a prime ideal $\mathfrak{p} \subseteq \overline{\mathbb{Q}}$ such that E' has complex multiplication by an order $\mathcal{O}' \supseteq \mathcal{O}$, it has good reduction at \mathfrak{p} and $E' \bmod \mathfrak{p}$ is isomorphic to E . By [12, II, Proposition 4.4] we must in fact have $\mathcal{O}' = \mathcal{O}$ and by [6, Chapter 13, Theorem 12] the prime p does not divide f . \square

Corollary 2.8. *Let k be a finite field of characteristic p and let $j(E) \in k$ be the j -invariant of an elliptic curve E/k with complex multiplication by an order \mathcal{O} in the imaginary quadratic field K . If $h(\mathcal{O})$ denotes the class number of \mathcal{O} , then there are exactly $h(\mathcal{O})$ distinct elements of k that are the j -invariants of elliptic curves with complex multiplication by \mathcal{O} .*

Proof. By Deuring's lifting theorem [6, Chapter 13, Theorem 14] and [12, II, Proposition 4.4] there exists a prime $\mathcal{P} \subseteq \overline{\mathbb{Q}}$ lying above p and an element $j' \in \overline{\mathbb{Q}}$ such that j' is the j -invariant of an elliptic curve with complex multiplication by \mathcal{O} and $j' \equiv j \pmod{\mathcal{P}}$. Denoting by D the discriminant of the order \mathcal{O} , we then have that the Hilbert class polynomial $H_D(X)$ (see [2, pag. 285]) has a root modulo p , namely the reduction of j' modulo \mathcal{P} . Let now $H_{\mathcal{O}}$ be the compositum over \mathbb{Q} of $\mathbb{Q}(j')$ and K . It is well-known (see for instance [2, Lemma 9.3]) that $H_{\mathcal{O}}$ is a Galois extension of \mathbb{Q} which can only be ramified at the rational primes dividing D . In particular, using Lemma 2.7 and the fact that the prime p is split in K by [6, Chapter 13, Theorem 12], we see that the prime p does not ramify in $\mathbb{Q} \subseteq H_{\mathcal{O}}$. Moreover, by assumption the prime $\mathfrak{p} := \mathcal{P} \cap \mathbb{Q}(j')$ has residue field $k_{\mathfrak{p}}$ contained in k . Let $\mathfrak{P} := \mathcal{P} \cap H_{\mathcal{O}}$ and denote by $D(\mathfrak{P}/\mathfrak{p}) \subseteq \text{Gal}(H_{\mathcal{O}}/\mathbb{Q}(j'))$ the decomposition group of \mathfrak{P} over \mathfrak{p} . For every $\sigma \in D(\mathfrak{P}/\mathfrak{p})$, the restriction $\sigma|_K$ belongs to the decomposition group of $\mathfrak{P} \cap K$ over p , which is trivial. Since $H_{\mathcal{O}}$ is the compositum of K and $\mathbb{Q}(j')$, we deduce that $D(\mathfrak{P}/\mathfrak{p})$ is also trivial, so that in particular the residue degree $f(\mathfrak{P}/\mathfrak{p}) = 1$. Because the extension $\mathbb{Q} \subseteq H_{\mathcal{O}}$ is Galois, we see that all the primes in $H_{\mathcal{O}}$ lying above p have the same residue field isomorphic to $k_{\mathfrak{p}}$.

Hence, all the roots $j \in H_{\mathcal{O}}$ of $H_D(X)$, which are all the possible singular invariants of elliptic curves over $\overline{\mathbb{Q}}$ with complex multiplication by \mathcal{O} , satisfy $j \bmod \mathcal{P} \in k_{\mathfrak{p}} \subseteq k$. By [6, Chapter 13, Theorems 12 and 13] and Lemma 2.7, this shows that there are at least $\deg(H_D(X)) = h(\mathcal{O})$ distinct elements of k that are the j -invariants of elliptic curves with complex multiplication by \mathcal{O} . By Deuring's lifting theorem there cannot be more, and this concludes the proof. \square

2.2. Modular polynomials. Let $\ell \in \mathbb{N}$ be a prime. The *modular polynomial of level ℓ* is the polynomial $\Phi_{\ell}(X, Y) \in \mathbb{Z}[X, Y]$ characterised by the following property: for every $j \in \overline{\mathbb{Q}}$ which is the j -invariant of an elliptic curve E , the polynomial $\Phi_{\ell}(j, Y)$ factors as

$$(1) \quad \Phi_{\ell}(j, Y) = \prod_C (Y - j(E/C))$$

where C varies among the $\ell + 1$ cyclic subgroups of order ℓ of $E(\overline{\mathbb{Q}})$, and E/C denotes the quotient of the curve E by the subgroup C . One can prove that $\Phi_\ell(j, Y)$ is symmetric in its variables and has degree $\ell + 1$. For more information concerning modular polynomials see [2, Chapter 11, paragraph C].

Since the polynomial $\Phi_\ell(X, Y)$ has integer coefficients, we can reduce it modulo a prime p , obtaining a polynomial $\tilde{\Phi}_\ell(X, Y) \in \mathbb{F}_p[X, Y]$. It is not difficult to show that, if $p \neq \ell$, then $\tilde{\Phi}_\ell$ satisfies the analogous property (1) with $\overline{\mathbb{Q}}$ replaced by $\overline{\mathbb{F}}_p$. Indeed, if $\tilde{j} \in \overline{\mathbb{F}}_p$ is the j -invariant of an elliptic curve $\tilde{E}/\overline{\mathbb{F}}_p$, choose a prime $\mathfrak{p} \subseteq \overline{\mathbb{Q}}$ lying above p and $j \in \overline{\mathbb{Q}}$ such that j is the singular invariant of an elliptic curve E reducing to \tilde{E} modulo \mathfrak{p} . Then, by reducing the factorization (1) modulo \mathfrak{p} , we see that the roots of $\tilde{\Phi}_\ell(\tilde{j}, Y)$ are precisely the reductions $j(\widetilde{E/C})$ for all subgroups C of order ℓ in $E(\overline{\mathbb{Q}})$. By Vélú's formulas [18] we have $j(\widetilde{E/C}) = j(\tilde{E}/\tilde{C})$, where $\tilde{C} = C \bmod \mathfrak{p}$, and, since $p \neq \ell$, [13, VII, Proposition 3.1] implies that the subgroups \tilde{C} range among all possible cyclic subgroups of order ℓ of $\tilde{E}(\overline{\mathbb{F}}_p)$.

From now on, we fix k to be either \mathbb{Q} or \mathbb{F}_p for some prime $p \neq \ell$, and we consider Φ_ℓ as a polynomial defined over k . The affine curve $\mathcal{C} \subseteq \mathbb{A}_k^2$ described by Φ_ℓ is a singular model for the modular curve $Y_0(\ell)/k$. This in particular means that every smooth point $Q \in \mathcal{C}(\bar{k})$ corresponds to an isomorphism class of pairs (E, C) , where E is an elliptic curve over \bar{k} and C is a cyclic subgroup of order ℓ of E . If $\Phi_\ell(j, j') = 0$, then the smooth point $(j, j') \in \mathcal{C}(\bar{k})$ represents the equivalence class of a pair (E, C) with $j(E) = j$ and $j(E/C) = j'$. More generally, the roots of $\Phi_\ell(j, Y)$, counted with multiplicities, are in bijection with the isomorphism classes of pairs (E, C) where $j(E) = j$ and the subgroup $C \subseteq E(\bar{k})$ is cyclic of order ℓ . The presence of multiple roots of $\Phi_\ell(j, Y)$ comes from the existence of distinct cyclic subgroups C, C' in E such that $j(E/C) = j(E/C')$. This certainly occurs if there exists an automorphism $\alpha \in \text{Aut}_{\bar{k}}(E)$ such that $\alpha(C) = C'$, which can be the case when $j = 0$ or $j = 1728$.

Example 2.9. This example is taken from [11, page 238]. Consider the elliptic curve $E : y^2 = x^3 - 1$ defined over \mathbb{F}_7 . This is an ordinary elliptic curve with $j(E) = 0$, whose CM order is generated over the integers by the automorphism $[\zeta_3] : (x, y) \mapsto (2x, y)$. The four cyclic subgroups of order 3 in $E(\overline{\mathbb{F}}_7)$ are given by

$$C_0 = \langle (0, i) \rangle, \quad C_1 = \langle (\sqrt[3]{4}, 2i) \rangle, \quad C_2 = \langle (2\sqrt[3]{4}, 2i) \rangle, \quad C_3 = \langle (4\sqrt[3]{4}, 2i) \rangle$$

where $i, \sqrt[3]{4} \in \overline{\mathbb{F}}_7$ are respectively a fixed square root of -1 and cube root of 4 . Note that the automorphism $[\zeta_3]$ acts transitively on the subgroups C_i with $i = 1, 2, 3$. In accordance with what was mentioned above, the polynomial $\Phi_3(0, Y) = Y(Y-3)^3$ has a triple root, corresponding to the fact that $j(E/C_i) = 3$ for all $i = 1, 2, 3$.

3. ORDINARY ISOGENY GRAPHS OVER \mathbb{F}_p

Let $p \geq 5$ be a prime number and denote by \mathbb{F}_p the prime field of characteristic p , with algebraic closure $\overline{\mathbb{F}}_p$. The condition on p is not restrictive for our study of the inverse volcano problem and, besides, it allows us to simplify the exposition of the theory in this section (cfr. for instance the use of Waterhouse's [19, Theorem 4.1] in the proof of Lemma 3.4). We want to define and study ordinary isogeny graphs over \mathbb{F}_p . All the constructions appearing in this section can be performed, *mutatis mutandis*, over \mathbb{F}_{p^s} for any $s > 1$. We decided to focus only on prime fields, over which we will formulate and solve the inverse volcano problem.

Let \mathcal{V} be the subset of $j \in \mathbb{F}_p$ such that the elliptic curves $E/\overline{\mathbb{F}}_p$ with $j(E) = j$ are ordinary. For any $j \in \mathcal{V}$, let \mathcal{E}_j be the set of \mathbb{F}_{p^2} -isomorphism classes of elliptic curves E/\mathbb{F}_p with $j(E) = j$. In other words, two elliptic curves E, E' over \mathbb{F}_p represent the same class in \mathcal{E}_j if and only if $j(E) = j(E') = j$ and E is a quadratic twist of E' . If $j \neq 0, 1728$, the set \mathcal{E}_j has cardinality 1

(see [13, Proposition 5.4]), and we fix a representative E_j/\mathbb{F}_p . If $j = 0$ then $\#\mathcal{E}_0 = 3$ and we fix $\{E_0^{(1)}, E_0^{(2)}, E_0^{(3)}\}$ to be three representatives of the different isomorphism classes. Similarly, if $j = 1728$ then $\#\mathcal{E}_{1728} = 2$ and we fix $\{E_{1728}^{(1)}, E_{1728}^{(2)}\}$ to be two representatives of the different isomorphism classes. In these two special cases, we generically use E_0 (resp. E_{1728}) to denote any of the three elliptic curves $\{E_0^{(1)}, E_0^{(2)}, E_0^{(3)}\}$ (resp. $\{E_{1728}^{(1)}, E_{1728}^{(2)}\}$).

Definition 3.1. For a prime $\ell \neq p$, the ordinary ℓ -isogeny graph over \mathbb{F}_p is the directed graph $\mathcal{G}_\ell(\mathbb{F}_p)$ whose vertex set equals \mathcal{V} and such that, for every $j, j' \in \mathcal{V}$, there are m directed edges from j to j' if and only if j' is a root of $\Phi_\ell(j, Y)$ with multiplicity m .

Remark 3.2. The directed edges from one node j_1 to another node j_2 in $\mathcal{G}_\ell(\mathbb{F}_p)$ represent the non-equivalent classes of cyclic isogenies of degree ℓ between E_{j_1} and E_{j_2} . If there is a directed edge between j_1 and j_2 with $j_1 \neq j_2$, and if $j_1, j_2 \notin \{0, 1728\}$, then there is a unique edge from j_2 to j_1 corresponding to the dual isogeny. By convention, in this situation we only represent one undirected edge in our figures. The case $j_1 = j_2$ can be more subtle, as an elliptic curve may have a self ℓ -isogeny φ with dual $\widehat{\varphi}$ satisfying $\ker \varphi \neq \ker \widehat{\varphi}$. In this case, the graphic representations display both φ and $\widehat{\varphi}$.

We begin our systematic study of the structure of $\mathcal{G}_\ell(\mathbb{F}_p)$. Moving from general to specific, we divide the isogeny graph into progressively smaller subgraphs: cordilleras, belts and volcanoes. We follow the geological terminology from [4, 7].

Before leaving on a mountain hike, we fix some notations: for each $j \in \mathcal{V}$, the elliptic curve E_j has complex multiplication by an order $\mathcal{O}_j := \text{End}_{\mathbb{F}_p}(E_j)$ in an imaginary quadratic field K . We write $D(\mathcal{O})$ for the discriminant of a general order \mathcal{O} . For imaginary quadratic orders, it is a negative integer congruent to 0 or 1 mod 4.

3.1. Cordilleras. For every $j \in \mathcal{V}$ let us denote by $\text{Tr} : \text{End}_{\mathbb{F}_p}(E_j) \otimes_{\mathbb{Z}} \mathbb{Q} \rightarrow \mathbb{Q}$ the trace map and by $\pi_j \in \text{End}_{\mathbb{F}_p}(E_j)$ the Frobenius endomorphism of the elliptic curve E_j . One knows that $\text{Tr}(\pi_j) = p + 1 - \#E_j(\mathbb{F}_p)$ and that $\mathbb{Z}[\pi_j]$ is isomorphic to the imaginary quadratic order of discriminant $D(\mathbb{Z}[\pi_j]) = \text{Tr}(\pi_j)^2 - 4p$.

Definition 3.3. Let $t \in \mathbb{Z}$. The t -cordillera in $\mathcal{G}_\ell(\mathbb{F}_p)$ is the subgraph of $\mathcal{G}_\ell(\mathbb{F}_p)$ induced by the subset of vertices

$$\mathcal{V}_t := \{j \in \mathbb{F}_p : \text{Tr}(\pi_j) = \pm t\} \subseteq \mathcal{V}.$$

By definition, if $j, j' \in \mathcal{V}_t$ we have $D(\mathbb{Z}[\pi_j]) = D(\mathbb{Z}[\pi_{j'}])$, so that both $\text{End}_{\mathbb{F}_p}(E_j)$ and $\text{End}_{\mathbb{F}_p}(E_{j'})$ contain an order isomorphic to the imaginary quadratic order of discriminant $t^2 - 4p$. In particular, E_j and $E_{j'}$ have complex multiplication by an order inside the *same* imaginary quadratic field K . We call K the *field associated with the t -cordillera* and, if $D(\mathcal{O}_K) < -4$, we say that the cordillera is *regular*. Cordilleras span the whole isogeny graph. Note that their vertices are defined independently of the isogeny degree ℓ . See Appendix C for an example of how changing ℓ changes the edges in the same t -cordillera.

Lemma 3.4. For $t \in \mathbb{Z}_{\neq 0}$ the following holds:

- (1) The set \mathcal{V}_t is non-empty if and only if $-2\sqrt{p} \leq t \leq 2\sqrt{p}$;
- (2) If \mathcal{V}_t is non-empty then for every order \mathcal{O} containing the order of discriminant $t^2 - 4p$ there exists an elliptic curve E/\mathbb{F}_p such that $\text{End}_{\mathbb{F}_p}(E) \cong \mathcal{O}$ and $j(E)$ is in \mathcal{V}_t ;
- (3) If $j(E) \in \mathcal{V}_t$ and if $\text{End}_{\mathbb{F}_p}(E) \cong \mathcal{O}$, then all the $h(\mathcal{O})$ j -invariants corresponding to curves with CM by \mathcal{O} are also in \mathcal{V}_t .

Proof. The first part is given in [19, Theorem 4.1]. We now prove the second part: let $j(E)$ be an element in \mathcal{V}_t . Let \mathcal{O} be the endomorphism ring of E . It contains the order $\mathbb{Z}[\pi_E]$

generated by the Frobenius π_E , which has discriminant $t^2 - 4p$. Each order containing an order isomorphic to $\mathbb{Z}[\pi_E]$ can be realised as the endomorphism ring of an elliptic curve defined over \mathbb{F}_p and \mathbb{F}_p -isogenous to E , see [19, Theorem 4.2, point (2)]. In particular, as these curves are all \mathbb{F}_p -isogenous to E , they have the same trace t and this proves the second part. For the third part, by Corollary 2.8, all the j -invariants corresponding to curves with CM by \mathcal{O} are rational over \mathbb{F}_p . If $j(E) = 0$ or $j(E) = 1728$, the class number of \mathcal{O} is one and the result is immediate. If $j(E) \notin \{0, 1728\}$, consider a j -invariant $j(E') \in \mathbb{F}_p$ of an elliptic curve E' with complex multiplication by \mathcal{O} . Since E and E' have complex multiplication by the same order, they are geometrically isogenous. Let k/\mathbb{F}_p be a degree r field extension over which this isogeny is defined. The Frobenius endomorphisms π_E and $\pi_{E'}$ of the two elliptic curves, seen as elements of the same imaginary quadratic field $K = \text{Frac}(\mathcal{O})$, satisfy $\pi_E^r = \pi_{E'}^r$ or $\pi_E^r = \overline{\pi_{E'}^r}$ by Tate's isogeny theorem [16, Theorem 1 (c4)]. This means that there exists a root of unity $\zeta \in K$ such that

$$\pi_E = \zeta \pi_{E'} \quad \text{or} \quad \pi_E = \zeta \overline{\pi_{E'}}.$$

If $\zeta = \pm 1$, it follows immediately that $j(E') \in \mathcal{V}_t$. Otherwise, $\zeta \in \{\pm i, \pm \zeta_3, \pm \zeta_3^2\}$, where i is a primitive fourth root of unity and ζ_3 is a primitive third root of unity. In this case, one easily deduces that $j(E) = j(E') \in \{0, 1728\}$, a contradiction. There are $h(\mathcal{O})$ possibilities for $j(E')$, and that gives the claim. \square

Fix a nonzero integer $t \in (-2\sqrt{p}, 2\sqrt{p})$ and let K be the field associated with the t -cordillera. All the j -invariants of elliptic curves with complex multiplication by the maximal order in K belong to \mathcal{V}_t by Lemma 3.4 (3). Fix such a singular invariant j and let E_j be a corresponding elliptic curve over \mathbb{F}_p . If $D(\mathcal{O}_K) < -4$, then E_j is determined only up to quadratic twisting, and the Frobenius endomorphism of any of its quadratic twists has, up to sign, the same trace. This in particular implies, using Lemma 3.4 (2) that any imaginary quadratic number field K with discriminant $D(\mathcal{O}_K) < -4$ can be associated to *at most one cordillera* (with positive trace). One can formulate this statement in terms of norm equations as follows.

Lemma 3.5. *Let K be an imaginary quadratic field of discriminant $D(\mathcal{O}_K) < -4$. Then the equation*

$$(2) \quad 4p = t^2 - v^2 D(\mathcal{O}_K)$$

has at most one solution $(t, v) \in \mathbb{N}^2$ with $p \nmid t$.

If $\text{disc}(K) \in \{-3, -4\}$ the situation is more delicate because the vertices $j = 0$ and $j = 1728$ are represented by 3 and 2 curves respectively, and the squared traces of the Frobenius endomorphisms of these curves may be different. These vertices may thus belong to different cordilleras at the same time. This is indeed always the case, as the following lemma shows.

Lemma 3.6. *The following holds:*

(i) *The equation*

$$(3) \quad 4p = t^2 + 3v^2$$

has no integer solutions if $p \equiv 2 \pmod{3}$, and exactly three solutions (t, v) with $t > 0$ and $v > 0$ if $p \equiv 1 \pmod{3}$.

(ii) *The equation*

$$(4) \quad 4p = t^2 + 4v^2$$

has no solutions if $p \equiv 3 \pmod{4}$, and exactly two solutions (x, y) with $x > 0$ and $y > 0$ if $p \equiv 1 \pmod{4}$.

Proof. Both statements reduce to solving a norm equation in the ring $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ and $\mathbb{Z}[\sqrt{-1}]$ respectively. \square

In particular, Lemma 3.6 shows that if $j = 0$ is an ordinary invariant then $K = \mathbb{Q}(\sqrt{-3})$ is associated with three t -cordilleras, and if $j = 1728$ is an ordinary invariant then $K = \mathbb{Q}(\sqrt{-1})$ is associated with two t -cordilleras (t positive).

3.2. Belts. In this section, we work inside a fixed non-empty t -cordillera \mathcal{C}_t with vertex set \mathcal{V}_t . Let K be the imaginary quadratic number field associated with this cordillera and denote by \mathcal{O}_K its ring of integers. Choose $\pi \in K$ to be any element such that

$$\pi^2 - t\pi + p = 0$$

so that, if $v := [\mathcal{O}_K : \mathbb{Z}[\pi]]$ denotes the conductor of the order $\mathbb{Z}[\pi]$ in K , then

$$4p - t^2 = -v^2 D(\mathcal{O}_K)$$

where $D(\mathcal{O}_K)$ is the discriminant of K . Denoting by $v_\ell(\cdot)$ the usual ℓ -adic valuation on \mathbb{Q} , we let $d := v_\ell(v)$ and $v' := v \cdot \ell^{-d}$.

Definition 3.7. An order \mathcal{O} such that $\mathbb{Z}[\pi] \subset \mathcal{O} \subset \mathcal{O}_K$ is said to be ℓ -saturated if $v_\ell([\mathcal{O}_K : \mathcal{O}]) = d$. It is said to be ℓ -dry if $v_\ell([\mathcal{O}_K : \mathcal{O}]) = 0$.

For every order $\mathbb{Z}[\pi] \subset \mathcal{O} \subset \mathcal{O}_K$ we define its *saturation* $\tilde{\mathcal{O}}$ as the unique order in K such that

$$[\mathcal{O}_K : \tilde{\mathcal{O}}] = [\mathcal{O}_K : \mathcal{O}] \cdot \ell^{d - v_\ell([\mathcal{O}_K : \mathcal{O}])}.$$

Note that $\tilde{\mathcal{O}}$ still contains $\mathbb{Z}[\pi]$. We are now ready to state the main definition of this section.

Definition 3.8. For a positive integer $m \mid v'$, the t -belt of index m , denoted by $\mathcal{B}_{t,m}$, is the subgraph of $\mathcal{G}_\ell(\mathbb{F}_p)$ induced by the subset

$$\mathcal{V}_{t,m} = \{j \in \mathcal{V}_t : \widetilde{\text{End}}_{\mathbb{F}_p}(E_j) \cong \mathbb{Z} + m\ell^d \mathcal{O}_K\} \subseteq \mathcal{V}_t.$$

Lemma 3.9. *The following holds:*

- (1) *The cut-set determined by the vertex partition $(\mathcal{V}_{t,m}, \mathcal{V} \setminus \mathcal{V}_{t,m})$ is empty.*
- (2) *Different t -belts form disjoint subgraphs of $\mathcal{G}_\ell(\mathbb{F}_p)$.*

Proof. Both points follow immediately from Proposition 2.1 and the fact that the endomorphism ring of every elliptic E with $j(E) \in \mathcal{V}_t$ must contain a subring isomorphic to $\mathbb{Z}[\pi]$. \square

Note that two belts \mathcal{B}_{t,m_1} and \mathcal{B}_{t,m_2} for $m_1 \neq m_2$ cannot contain j -invariants of elliptic curves that have isomorphic endomorphism ring. Moreover, a belt does not have to be connected.

3.3. Isogeny volcanoes. Isogeny volcanoes are the connected components of $\mathcal{G}_\ell(\mathbb{F}_p)$. The vertices of these graphs come endowed with a natural ‘‘stratification’’ by level, in the sense of the following definition.

Definition 3.10. An ordinary elliptic curve E/\mathbb{F}_p , its j -invariant $j(E)$, and its associated order $\text{End}(E) = \mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ are said to lie at *level* n in the volcano containing $j(E)$ if $v_\ell(f) = n$.

The subgraph induced by the subset of level- n vertices in a volcano V is denoted by V_n . The graph V_0 is called the *crater* of V while we say that the vertices in $V \setminus V_0$ are on the *lava flows* of the volcano V . The *depth* of V is the maximal level on which vertices $j \in V$ lie.

Lemma 3.11. *Let k be a finite field of characteristic p and $\ell \neq p$ a prime number. Let E and E' be two elliptic curves over k with complex multiplication by an order \mathcal{O} of conductor f in an imaginary quadratic field K .*

- (1) *If $\mathfrak{L} \subseteq \mathcal{O}$ is an invertible ideal of norm ℓ , then $E/E[\mathfrak{L}]$ has complex multiplication by \mathcal{O} and the quotient map $E \rightarrow E/E[\mathfrak{L}]$ has degree ℓ ;*

- (2) If $\varphi : E \rightarrow E'$ is an isogeny of degree ℓ , then there exists an invertible ideal $\mathfrak{L} \subseteq \mathcal{O}$ of norm ℓ such that $E' \cong E/E[\mathfrak{L}]$;
- (3) If $\mathfrak{L} \subseteq \mathcal{O}$ is a non-invertible ideal of norm ℓ , then $\ell \mid f$ and $E/E[\mathfrak{L}]$ has complex multiplication by the unique quadratic order containing \mathcal{O} with index ℓ .

Proof. For an ideal $I \subseteq \mathcal{O}$ we denote by $\mathcal{O}(I) := \{x \in K : xI \subseteq I\}$ the order associated with I . We always have $\mathcal{O} \subseteq \mathcal{O}(I)$ and $\mathcal{O}(I)$ is by definition the smallest quadratic order $\mathcal{O}' \supseteq \mathcal{O}$ such that $I\mathcal{O}'$ is invertible in \mathcal{O}' .

Part (1) follows from [19, Proposition 3.9] and the fact that $\#E[\mathfrak{L}] = \#(\mathcal{O}/\mathfrak{L})$, since $\ell \neq p$. We now prove part (2). Consider the ideal

$$\mathfrak{L} := \{f \in \text{End}_{\overline{k}}(E) : f(\ker \varphi) = 0\} \subseteq \text{End}_{\overline{k}}(E) = \mathcal{O}.$$

We clearly have $\ker \varphi \subseteq E[\mathfrak{L}]$. On the other hand, it is not difficult to see, using a finite fields analogue of [12, II, Corollary 1.1.1] and the fact that E and E' have complex multiplication by the same order, that $\ker \varphi$ is a cyclic \mathcal{O} -module which is then isomorphic to $\mathcal{O}/\text{Ann}_{\mathcal{O}}(\ker \varphi) = \mathcal{O}/\mathfrak{L}$, where $\text{Ann}_{\mathcal{O}}(\ker \varphi)$ denotes the annihilator ideal of $\ker \varphi$. Since $\ell \neq p$ we have

$$\#E[\mathfrak{L}] = \#\mathcal{O}/\mathfrak{L} = \#\ker \varphi = \ell$$

and we then obtain $\ker \varphi = E[\mathfrak{L}]$. Hence $E' \cong E/\ker \varphi = E/E[\mathfrak{L}]$. Using [19, Proposition 3.9] (which can be applied thanks to [19, Theorem 4.5]) we see that $\mathcal{O}(\mathfrak{L}) = \mathcal{O}$ and so \mathfrak{L} is invertible in \mathcal{O} .

We finally prove part (3). Note that the existence of a non-invertible ideal of norm ℓ implies that the conductor of \mathcal{O} is divisible by ℓ . Using [19, Proposition 3.9] again, we need to prove that $\mathcal{O}(\mathfrak{L})$ is equal to the unique order \mathcal{O}' containing \mathcal{O} with index ℓ . Set $\mathcal{O}' = \mathbb{Z}[\omega]$. Then we have $\mathcal{O} = \mathbb{Z}[\ell\omega]$ and $\mathfrak{L} = (\ell, \ell\omega)$. Hence $\mathfrak{L}\mathcal{O}'$ is principal, generated by ℓ , and in particular invertible. We deduce that $\mathcal{O}(\mathfrak{L}) = \mathcal{O}'$ and the proof is concluded. \square

Remark 3.12. If \mathcal{O} is an imaginary quadratic order of discriminant $D_{\mathcal{O}}$ and ℓ is a prime, then there are exactly $1 + \left(\frac{D_{\mathcal{O}}}{\ell}\right)$ prime ideals in \mathcal{O} with norm ℓ . If $\ell \mid [D_{\mathcal{O}} : D_K]$, the unique prime ideal of norm ℓ is not invertible. In all other cases, the primes of norm ℓ are always invertible.

From a volcanic perspective, Lemma 3.11 and Remark 3.12 translate in the following way.

Corollary 3.13. *Horizontal isogenies in $\mathcal{G}_{\ell}(\mathbb{F}_p)$ can only occur between vertices at level 0 in the volcanoes belonging to the same belt. More precisely, for every non-zero $t \in \mathbb{Z}$, for every t -cordillera, if K is the field associated with the t -cordillera, then for every m , for every belt $\mathcal{B}_{t,m}$, for every volcano V in $\mathcal{B}_{t,m}$, there are exactly*

$$1 + \left(\frac{D(\mathcal{O}_K)}{\ell}\right) = \begin{cases} 0 & \text{if } \ell \text{ is inert in } K, \\ 1 & \text{if } \ell \text{ is ramified in } K, \\ 2 & \text{if } \ell \text{ splits in } K, \end{cases}$$

distinct edges of $\mathcal{G}_{\ell}(\mathbb{F}_p)$ from $j \in V_0$ to other vertices in V_0 .

We will now describe the structure of an isogeny volcano by analysing crater and lava flow separately. We start by analysing crater structure, then focus on a single belt (that is, looking at a fixed endomorphism structure), and finally we let the lava flow down, looking at class numbers at every level of the volcanoes. In other words, there is a simultaneous eruption in all volcanoes belonging to the same belt, and class number arithmetic constrains the shape to which lava solidifies!

3.3.1. *The crater.* The following proposition presents the possible craters that can occur.

Proposition 3.14. *Let $\mathcal{B}_{t,m}$ be a belt in the isogeny graph $\mathcal{G}_\ell(\mathbb{F}_p)$ and let $\mathcal{C}_{t,m}$ be the subgraph of $\mathcal{B}_{t,m}$ induced by the vertices at level 0. Let \mathcal{O} be the CM order associated with any vertex in $\mathcal{C}_{t,m}$ and let $\mathfrak{L} \subseteq \mathcal{O}$ be a prime ideal dividing ℓ . Then each connected component of $\mathcal{C}_{t,m}$ is a crater of a volcano in $\mathcal{B}_{t,m}$ and consists of:*

- (1) A single vertex if ℓ is inert in K ;
- (2) A single vertex with a self-loop if ℓ is ramified in K and \mathfrak{L} is principal;
- (3) A single vertex with two self-loops if ℓ splits in K and \mathfrak{L} is principal;
- (4) Two vertices connected with a single edge if ℓ ramifies in K and \mathfrak{L} is not principal;
- (5) Two vertices connected with a double edge if ℓ splits in K and \mathfrak{L} has order 2 in the class group $\text{Cl}(\mathcal{O})$;
- (6) More generally, a cycle of size the order of $[\mathfrak{L}]$ in the class group $\text{Cl}(\mathcal{O})$ if ℓ splits in K and we are not in any of the previous cases.

Proof. Fix $j(E) \in \mathcal{C}_{t,m}$. We want to analyse the connected component of $\mathcal{C}_{t,m}$ containing $j(E)$. Using Lemma 3.11, there is an edge from $j(E)$ to $j(E/E[\mathfrak{L}])$. As the action described in Theorem 2.5 is faithful and transitive, by iteration we obtain a cycle of length the order of the class of \mathfrak{L} in $\text{Cl}(\mathcal{O})$.

A case by case analysis concludes the proof, for instance: In the case where ℓ is ramified in K , and the unique ideal \mathfrak{L} lying above ℓ is principal, then $\mathfrak{L} = \overline{\mathfrak{L}}$, and $\mathfrak{L}, \overline{\mathfrak{L}}$ correspond to mutually dual isogenies with the same kernel. This situation is represented by a unique self-loop. In the case where ℓ splits into principal ideals $\mathfrak{L}, \overline{\mathfrak{L}}$ in K , and the ideal \mathfrak{L} lying above ℓ is principal, then $\mathfrak{L} \neq \overline{\mathfrak{L}}$. These ideals correspond to two self-isogenies with distinct kernels. This situation is represented by two self-loops in the graph (cfr. Remark 3.2). \square

Remark 3.15. Case (6) in the above proposition in fact includes also case (5). However, we decided to separate the two cases in order to underline the difference between case (4) and case (5).

See Figure 1 for a view of all possible subgraphs at level 0.

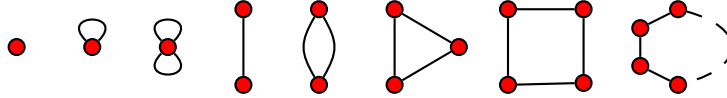


FIGURE 1. All possible craters.

3.3.2. *The lava flows.* We now explain what the other levels of a volcano look like.

Lemma 3.16. *Let E/k be an elliptic curve. The number of non-equivalent ℓ -isogenies from E to any other curve with k -rational j -invariant is 0, 1, 2 or $\ell + 1$.*

Proof. The kernel of an isogeny from E must be a subgroup of $E[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$. For it to be an ℓ -isogeny the subgroup must have order ℓ . In order for the target curve to be k -rational, the kernel of the isogeny must be invariant under the action of the Galois group $G = \text{Gal}(\overline{k}/k)$. There are $\ell + 1$ subgroups of order ℓ in $E[\ell]$, that can be seen as lines in an \mathbb{F}_ℓ -vector space. G acts linearly, and if it fixes three or more such lines, then it acts as an homothety and hence fixes every subgroup. \square

Proposition 3.17. *Let V be a volcano of depth d in the isogeny graph $\mathcal{G}_\ell(\mathbb{F}_p)$. Assume that the crater V_0 contains j -invariants corresponding to elliptic curves with complex multiplication by an order \mathcal{O} of discriminant $D(\mathcal{O})$ with $D(\mathcal{O}) \neq -3, -4$. Then:*

- For every $j \in V_0$, the elliptic curve E_j has, up to equivalence, 0 descending isogenies if $d = 0$ and $(\ell - (\frac{D}{\ell}))$ descending isogenies otherwise;
- For every $n > 0$ and every $j \in V_n$, the elliptic curve E_j has, up to equivalence, ℓ descending isogenies if $n < d$ and 0 descending isogenies otherwise;
- For every $n > 0$ and every $j \in V_n$, the elliptic curve E_j has, up to equivalence, exactly 1 ascending isogeny.

Proof. The proof of this proposition is essentially contained in the second part of the proof of [14, Lemma 6]. We sketch the argument here.

Let $\mathcal{B}_{t,m}$ be the belt containing the volcano V . We determine the vertical isogenies between the elliptic curves corresponding to the vertices in $\mathcal{B}_{t,m}$ by induction on the level n of the vertices themselves.

If $n = 0$, all the elliptic curves corresponding to the vertices at level 0 of $\mathcal{B}_{t,m}$ have, by Corollary 3.13, exactly $1 + (\frac{D(\mathcal{O}_K)}{\ell})$ horizontal isogenies. Note that, since the order of discriminant D must be ℓ -dry by the level-0 assumption, we have $(\frac{D(\mathcal{O}_K)}{\ell}) = (\frac{D(\mathcal{O})}{\ell})$. The maximal possible number of non-equivalent isogenies from every E_j is $\ell + 1$, so the maximal possible number of non-equivalent descending isogenies from every E_j is

$$(\ell + 1) - \left(1 + \left(\frac{D(\mathcal{O})}{\ell}\right)\right) = \ell - \left(\frac{D(\mathcal{O})}{\ell}\right).$$

If $d = 0$, there are none. If $d > 0$, then by Corollary 2.8 there are exactly $h(\mathcal{O}')$ vertices in $\mathcal{B}_{t,m}$ at level 1, where \mathcal{O}' is the unique order contained in \mathcal{O} with index ℓ . Using [2, Corollary 7.28] and the fact that $D \neq -3, -4$ we have

$$h(\mathcal{O}') = h(\mathcal{O}) \left(\ell - \left(\frac{D(\mathcal{O})}{\ell}\right)\right).$$

By Lemma 3.11, each of the $h(\mathcal{O}) \left(\ell - \left(\frac{D(\mathcal{O})}{\ell}\right)\right)$ elliptic curves with CM by \mathcal{O}' admit a vertical isogeny. Since, by duality and the fact that $D(\mathcal{O}) \neq -3, -4$, the number of ascending isogenies from level 1 to level 0 is the same as the number of descending isogenies from level 0 to level 1, a counting argument shows that every elliptic curve E_j at level 0 has, up to equivalence, $(\ell - (\frac{D(\mathcal{O})}{\ell}))$ descending isogenies and every elliptic curve E_j at level 1 has, up to equivalence, precisely 1 vertical isogeny.

If $n = 1$, there are no horizontal isogenies by Corollary 3.13. Hence, all elliptic curves corresponding to the vertices at level 1 of $\mathcal{B}_{t,m}$ have one ascending isogeny (by the previous discussion) and $(\ell + 1) - 1 = \ell$ descending isogenies if $d > 1$, no descending isogenies otherwise. Suppose then that $d > 1$. Then by Corollary 2.8 there are exactly $h(\mathcal{O}'')$ vertices in $\mathcal{B}_{t,m}$ at level 2, where \mathcal{O}'' is the unique order contained in \mathcal{O}' with index ℓ . Using [2, Corollary 7.28] we see that

$$h(\mathcal{O}'') = \ell h(\mathcal{O}').$$

By Lemma 3.11, each of the $\ell h(\mathcal{O}')$ elliptic curves with CM by \mathcal{O}'' admits a vertical isogeny. As above we conclude that every elliptic curve E_j at level 1 has, up to equivalence, ℓ descending isogenies and every elliptic curve E_j at level 2 has, up to equivalence, precisely 1 vertical isogeny. An easy induction now leads to the claim. \square

It is now time to deal with the pathological volcanoes containing 0 and 1728. We warm up with the following lemma.

Lemma 3.18. *Suppose that $0 \in \mathbb{F}_p$ or $1728 \in \mathbb{F}_p$ is the j -invariant of an ordinary elliptic curve E and let $\ell \neq p$ be a prime. Suppose that there exists a cyclic subgroup $H \subseteq E(\overline{\mathbb{F}}_p)$ of order ℓ*

which is fixed by all the automorphisms of E . Then there exists an ideal $\mathfrak{L} \subseteq \text{End}_{\overline{\mathbb{F}}_p}(E)$ of norm ℓ such that $H = E[\mathfrak{L}]$.

Proof. We give the details for 0, the proof is similar for 1728. There is an isomorphism $\mathcal{O} := \text{End}_{\overline{\mathbb{F}}_p}(E) \cong \mathbb{Z}[\zeta_6]$ where $\zeta_6 \in \overline{\mathbb{Q}}$ is a primitive 6-th root of unity. In particular, $\text{Aut}_{\overline{\mathbb{F}}_p}(E) \cong \langle \zeta_6 \rangle$. Hence, if H is fixed by all the automorphisms of E , then it is in fact fixed by all its endomorphisms. We deduce that H is a cyclic \mathcal{O} -module of order ℓ . We then have an \mathcal{O} -module isomorphism

$$\mathcal{O}/\text{Ann}_{\mathcal{O}}(H) \cong H$$

where $\text{Ann}_{\mathcal{O}}(H)$ is the annihilator of H in \mathcal{O} . The isomorphism above shows that $\mathfrak{L} := \text{Ann}_{\mathcal{O}}(H)$ is an ideal of \mathcal{O} of norm ℓ and $H \subseteq E[\mathfrak{L}]$. Since these two groups have the same cardinality, we deduce that $H = E[\mathfrak{L}]$, as wanted. \square

We now describe the directed neighbourhood of the vertex 0.

Proposition 3.19. *Suppose that $0 \in \mathbb{F}_p$ is the j -invariant of an ordinary elliptic curve E and let $\ell \neq p$ be a prime. In the volcano containing 0, the directed subgraph induced by the neighbours of 0 at level zero and level 1 can be described as:*

- If $\ell = 3$: the vertex 0 has one self-loop, three descending isogenies towards a unique vertex j at level 1, and there is one unique isogeny from j to 0;
- If $\ell \equiv 1 \pmod{3}$: the vertex 0 has two self-loops. Level 1 has either zero or $(\ell - 1)/3$ vertices. In the latter case, each of these vertices receives three descending isogenies from 0 and sends one ascending isogeny to 0;
- If $\ell \equiv 2 \pmod{3}$, the vertex 0 has no self-loop. Level 1 has either zero or $(\ell + 1)/3$ vertices. In the latter case, each of these vertices receives three descending isogenies from 0, and sends one ascending isogeny to 0.

Proof. The structure of the crater is already described in Proposition 3.14. If level 1 is empty we are done. We then assume that there is at least one j -invariant at level 1.

Let μ_6 be the group of $\overline{\mathbb{F}}_p$ -automorphisms of E . It acts on the set S of subgroups of order ℓ in E . The orbits of this action can be described by means of Lemma 3.18: if $H \in S$ is of the form $H = E[\mathfrak{L}]$ for some ideal $\mathfrak{L} \subseteq \mathbb{Z}[\zeta_3]$ of norm ℓ then its orbit is a singleton, otherwise the orbit of H contains three elements. Each singleton orbit gives rise to a self-loop around 0 thanks to Proposition 3.14, while each orbit of cardinality 3 gives rise to three directed edges (descending isogenies) from 0 towards the same j -invariant in level 1 by Lemma 3.11. Note also that there is a directed edge from each j -invariant at level 1 to 0 by Lemma 3.11. Dualising this isogeny, we see that there is at least one, hence three, directed edges from 0 to each j -invariant at level 1. Let \mathcal{O} be the order corresponding to the vertices at level 1. The number of vertices on this level is given by the class number $h(\mathcal{O})$ (see Corollary 2.8), which in turn is equal to

$$h(\mathcal{O}) = \frac{1}{3} \left(\ell - \left(\frac{-3}{\ell} \right) \right)$$

by [2, Corollary 7.28]. On the other hand, the total number of oriented edges from level 0 to level 1 is precisely $\ell - \left(\frac{-3}{\ell} \right)$. This, together with the discussion above, implies that for each vertex j at level 1 there are exactly three directed edges from 0 to j in the isogeny graph. By counting, one also easily sees that there is exactly one ascending isogeny from each vertex at level 1 to 0. \square

Proposition 3.20. *Suppose that $1728 \in \mathbb{F}_p$ is the j -invariant of an ordinary elliptic curve E and let $\ell \neq p$ be a prime. In the volcano containing 0, the directed subgraph induced by the neighbours of 0 at level zero and level 1 can be described as:*

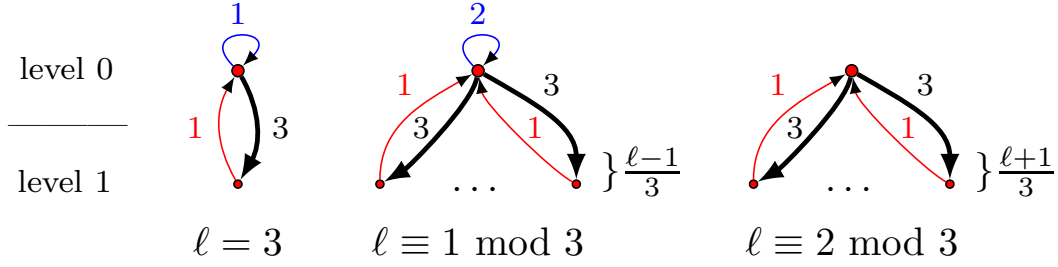


FIGURE 2. All possible neighbourhoods of depth 1 around 0. Numbers next to directed edges represent multiplicities.

- If $\ell = 2$: the vertex 1728 has one self-loop, two descending isogenies towards a unique vertex j at level 1, and there is one unique isogeny from j to 1728;
- If $\ell \equiv 1 \pmod{4}$: the vertex 1728 has two self-loops. Level 1 has either zero or $(\ell - 1)/2$ vertices. In the latter case, each of these vertices receives two descending isogenies from 1728 and sends one ascending isogeny to 1728;
- If $\ell \equiv 3 \pmod{4}$, the vertex 1728 has no self-loop. Level 1 has either zero or $(\ell + 1)/2$ vertices. In the latter case, each of these vertices receives two descending isogenies from 1728, and sends one ascending isogeny to 1728.

Proof. The proof goes along the same lines as the proof of Proposition 3.19. \square

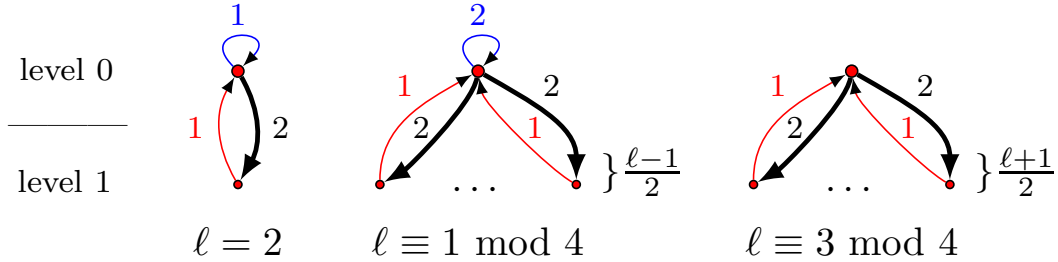


FIGURE 3. All possible neighbourhoods of depth 1 around 1728. Numbers next to directed edges represent multiplicities.

3.4. Mapping the territory. In this paragraph, we count the number of volcanic structures.

Lemma 3.21. For $t \in \mathbb{Z}_{>0}$, the number of non-empty t -cordilleras in $\mathcal{G}_\ell(\mathbb{F}_p)$ is $\lfloor 2\sqrt{p} \rfloor$.

Proof. The number of cordilleras is the number of possible traces up to sign. By Waterhouse [19, Theorem 4.1 page 536], each trace in the Hasse interval $[-2\sqrt{p}, 2\sqrt{p}]$ is attained over \mathbb{F}_p . This gives $\lfloor 2\sqrt{p} \rfloor$ possibilities for non-zero traces up to sign. It is independent of ℓ . \square

Lemma 3.22. Let $t \in [1, 2\sqrt{p}]$ be an integer. Let K be the associated field $\mathbb{Q}(\sqrt{t^2 - 4p})$. Let $D(\mathcal{O}_K)$ denote its discriminant. Let $v = \sqrt{(t^2 - 4p)/D(\mathcal{O}_K)}$. Let $d = v_\ell(v)$. The number of belts in the t -cordillera is $\omega(v\ell^{-d})$, where $\omega(k)$ is the number of positive divisors of the integer k .

Proof. For every positive divisor m of $v\ell^{-d}$, we have the belt $B_{t,m}$ induced by the following set of vertices:

$$\mathcal{V}_{t,m} = \{j \in \mathcal{V}_t \mid \widetilde{\text{End}(E_j)} \cong \mathbb{Z} + m\ell^d \mathcal{O}_K\}.$$

□

Lemma 3.23. *Let $\mathcal{B}_{t,m}$ be a belt associated with a trace $t \neq 0$ and integer m . Let K be the associated field. Let $\mathcal{O} = \mathbb{Z} + m\mathcal{O}_K$.*

- (i) *If ℓ is inert, the number of volcanoes in $\mathcal{B}_{t,m}$ is $h(\mathcal{O})$;*
- (r) *If ℓ is ramified, if $\ell\mathcal{O} = \mathcal{L}^2$ with \mathcal{L} principal, then the number of volcanoes in $\mathcal{B}_{t,m}$ is $h(\mathcal{O})$. If $\ell\mathcal{O} = \mathcal{L}^2$ with \mathcal{L} not principal, then the number of volcanoes in $\mathcal{B}_{t,m}$ is $h(\mathcal{O})/2$;*
- (s) *If ℓ is split and $\ell\mathcal{O} = \mathcal{L}\overline{\mathcal{L}}$, let r be the order of \mathcal{L} in $\text{Cl}(\mathcal{O})$, then the number of volcanoes in $\mathcal{B}_{t,m}$ is $h(\mathcal{O})/r$.*

Proof. The number of volcanoes is the number of craters, and the craters are isomorphic within a belt. The total number of vertices of depth 0 in $\mathcal{B}_{t,m}$ is $h(\mathcal{O})$. The size of each crater is given by Proposition 3.14. □

Remark 3.24. All volcanoes on the same cordillera have the same depth. All volcanoes on the same belt have the exact same shape. The total number of vertices at level 0 in a belt with endomorphism order \mathcal{O} is $h(\mathcal{O})$.

Lemma 3.25. *Let V be a volcano in the belt $\mathcal{B}_{t,m}$, where t corresponds to a cordillera of depth d . Let K be the associated field. Let $\mathcal{O} = \mathbb{Z} + m\mathcal{O}_K$. The number of vertices in the volcano V is*

$$c + \frac{2c}{\#\mathcal{O}^\times} \left(\left(\ell - \left(\frac{D(\mathcal{O})}{\ell} \right) \right) \frac{\ell^d - 1}{\ell - 1} \right).$$

Proof. Use Proposition 3.17 in the regular case and Propositions 3.19 and 3.20 in the non-regular case. A formula for c is given in Proposition 3.14. □

Remark 3.26. There are exactly p j -invariants in \mathbb{F}_p . Therefore, by taking into account supersingular curves, we can partition p and obtain a mass formula. A full study in the case $p = 1009$ and $\ell = 3$ is enclosed in the appendix A.

4. THE INVERSE VOLCANO PROBLEM

Inspired by the structure of the connected components of $\mathcal{G}_\ell(\mathbb{F}_p)$, we give the following definition.

Definition 4.1. An *abstract volcano* $V = (\mathcal{V}, \mathcal{E})$ of *depth* $d \geq 0$ is a connected undirected graph together with a distinguished subset $\mathcal{V}_0 \subseteq \mathcal{V}$ such that the subgraph V_0 induced by \mathcal{V}_0 is one of the graphs described in Proposition 3.14. Moreover, $d > 0$ if and only if $\mathcal{V} \setminus \mathcal{V}_0 \neq \emptyset$, in which case there exists a partition

$$\mathcal{V} \setminus \mathcal{V}_0 = \bigcup_{i=1}^d \mathcal{V}_i$$

and a prime number $\ell \in \mathbb{Z}$ such that, denoting by V_i the subgraph induced by \mathcal{V}_i , the following holds:

- (1) All vertices in $\mathcal{V}_0 \cup \dots \cup \mathcal{V}_{d-1}$ have degree $\ell + 1$ and all vertices in \mathcal{V}_d have degree 1;
- (2) If $v \in \mathcal{V}_r$ and $v' \in \mathcal{V}_k$ are connected by an edge, then $|r - k| \leq 1$;
- (3) For all $0 < r \leq d$, the graph V_r is totally disconnected;
- (4) For $0 < r \leq d$, each vertex in V_r has exactly one edge to a vertex in V_{r-1} ;

We call V_0 the *crater* of V and we say that the vertices in \mathcal{V}_r lie at *level* r .

If the depth d of an abstract volcano \mathcal{V} is strictly positive, then the prime ℓ appearing in Definition 4.1 is uniquely determined by condition (1) above. In this case, we will also speak of \mathcal{V} as of an (abstract) ℓ -volcano.

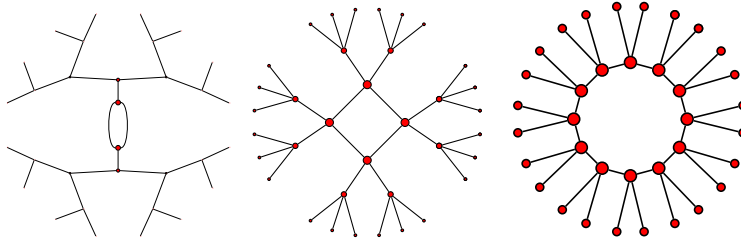


FIGURE 4. Three abstract volcanoes.

It follows from the discussion in Section 3 that a connected component of $\mathcal{G}_\ell(\mathbb{F}_p)$ not containing 0 or 1728 is an abstract volcano in the sense above. One may wonder whether the converse is also true. More precisely, we pose the following question.

Question 4.2 (Inverse Volcano Problem over \mathbb{F}_p). *Let V be an abstract volcano as in Definition 4.1. Can we find primes $p, \ell \in \mathbb{Z}$ with $p \neq \ell$ such that V is a connected component in the isogeny graph $\mathcal{G}_\ell(\mathbb{F}_p)$?*

Roughly speaking, one can study this question by dividing it into two subcases:

- (1) The volcano V has depth $d = 0$ i.e. $V = V_0$;
- (2) The volcano V has depth $d > 0$ i.e. $V \neq V_0$.

These two cases are fundamentally different in nature. Indeed, in the first case we can try to find (and we will find) the volcano V as connected component of $\mathcal{G}_\ell(\mathbb{F}_p)$ where both ℓ and p are allowed to vary. However, in the second case the prime ℓ is fixed, since it must be one less than the degree of any vertex in V_0 . Hence, in this second setting we have less freedom of choice and the inverse volcano problem becomes more difficult.

To study Question 4.2, it is useful to introduce a couple of definitions. First of all note that, letting V_0 be one of the graphs described in Proposition 3.14, ℓ a prime number and $d \in \mathbb{Z}_{>0}$, there exists a unique abstract ℓ -volcano $V = V(V_0, \ell, d)$ with crater V_0 and depth d . We call V the *volcano induced by the triple* (V_0, ℓ, d) . We also give the following definition of abstract crater associated with a prime ideal.

Definition 4.3. Let \mathcal{O} be an imaginary quadratic order and $\ell \in \mathbb{Z}_{>0}$ a prime number not dividing the conductor of \mathcal{O} . Choose a prime ideal $\mathfrak{L} \subseteq \mathcal{O}$ lying above ℓ . The *abstract crater* V_0 associated with \mathfrak{L} is the graph consisting of:

- A single vertex if ℓ is inert in \mathcal{O} ;
- A single vertex with a self-loop if ℓ is ramified in \mathcal{O} and \mathfrak{L} is principal;
- A single vertex with two self-loops if ℓ splits in \mathcal{O} and \mathfrak{L} is principal;
- Two vertices connected with a single edge if ℓ ramifies in \mathcal{O} and \mathfrak{L} is not principal;
- A cycle of size the order of $[\mathfrak{L}]$ in the class group $\text{Cl}(\mathcal{O})$ if ℓ splits in \mathcal{O} and we are not in any of the previous cases.

The relationship between Definition 4.3, Proposition 3.14 and Question 4.2 is clear: if we want to realise an ℓ -volcano V as the connected component of $\mathcal{G}_\ell(\mathbb{F}_p)$ for some prime p , it seems natural to begin by realising its crater V_0 . By Proposition 3.14, a good start would be to find an imaginary quadratic field K whose ring of integers contains an ideal $\mathfrak{L} \mid \ell$ such that V_0 is equal to the abstract crater associated with \mathfrak{L} (here we are evidently hoping to view the vertices of V_0 as j -invariants of CM elliptic curves with complex multiplication by the *maximal order* in K).

In fact, we will now prove that, in order to solve the inverse volcano problem, realising V_0 as a crater is the key step.

Proposition 4.4. *Let \mathcal{O} be an order of discriminant $D(\mathcal{O}) < -4$ in an imaginary quadratic field K and let $\ell \in \mathbb{Z}_{>0}$ be a prime not dividing the conductor of \mathcal{O} . Let $\mathfrak{L} \subseteq \mathcal{O}$ be a prime lying above ℓ and let V_0 be the abstract crater associated with \mathfrak{L} . Then for every $d > 0$ there exist infinitely many primes $p = p(d) \in \mathbb{Z}_{>0}$ such that $\mathcal{G}_\ell(\mathbb{F}_p)$ contains the volcano induced by (V_0, ℓ, d) as connected component. Moreover, if $\ell \neq 2$ the same is true with $d = 0$.*

Proof. Given a positive integer d , our goal is to find infinitely many primes $p \in \mathbb{Z}_{>0}$ and pairs $(t, v) \in \mathbb{Z}^2$ such that $t \neq 0$, the prime power ℓ^d divides exactly v and $4p = t^2 - v^2 D(\mathcal{O})$. Indeed, suppose this is the case. Then of course we must have $-2\sqrt{p} \leq t \leq 2\sqrt{p}$ so by Lemma 3.4 the t -cordillera in $\mathcal{G}_\ell(\mathbb{F}_p)$ is non-empty. Since the order \mathcal{O} certainly contains the order of discriminant $v^2 D(\mathcal{O})$ and ℓ does not divide the conductor of \mathcal{O} , by Proposition 3.17 combined again with Lemma 3.4 the t -cordillera possesses a connected component isomorphic to the volcano induced by (V_0, ℓ, d) .

To find primes p and corresponding couples (t, v) as above, we proceed as follows. For every $k \in \mathbb{N}$, denote by H_k the ring class field of the order $\mathbb{Z}[\ell^k \sqrt{D(\mathcal{O})}] \subseteq \mathcal{O}$. We have that $H_k \subsetneq H_{k+1}$ for all $k \in \mathbb{N}$. To see this, one can simply use [2, Corollary 7.28] to compute $[H_{k+1} : H_k]$: if $\ell \neq 2$ one has $[H_{k+1} : H_k] \in \{\ell - 1, \ell, \ell + 1\}$ for all $k \geq 0$, while in the case $\ell = 2$ one has $[H_{k+1} : H_k] = 2$ for all $k \geq 0$ since $\mathbb{Z}[2^k \sqrt{D(\mathcal{O})}]$ has always even discriminant.

In particular $H_d \subsetneq H_{d+1}$, so by the Chebotarëv density theorem there are infinitely many primes $p \nmid 2\ell D(\mathcal{O})$ that split completely in H_d but do not split completely in H_{d+1} . Using [2, Theorem 9.4], we see that there exist $x, y \in \mathbb{Z}$ such that $p = x^2 - D(\mathcal{O})\ell^{2d}y^2$. Moreover, we also have $\ell \nmid y$, since otherwise there would exist $\tilde{y} \in \mathbb{Z}$ such that $p = x^2 - D(\mathcal{O})\ell^{2d+2}\tilde{y}^2$ and then p would split completely (again by [2, Theorem 9.4]) in H_{d+1} , contradicting our assumptions. Now such a p satisfies the norm equation

$$4p = t^2 - v^2 D(\mathcal{O})$$

where $t = 2x$ and $v = 2\ell^d y$. We certainly have $t \neq 0$ since p is split in K by our choices. Moreover, if $\ell \neq 2$, the power ℓ^d divides exactly v so in this case the theorem is proved.

If $\ell = 2$ then the same arguments work by considering primes splitting completely in H_{d-1} but not in H_d (here we use the fact that $d > 0$). This concludes the proof. \square

Remark 4.5. In the above proof we have chosen a down-to-earth approach, proving the existence of the volcano induced by (V_0, ℓ, d) in $\mathcal{G}_\ell(\mathbb{F}_p)$ by solving an equation of the form $4p = t^2 - v^2 \ell^{2d} D(\mathcal{O})$ with $t, v \in \mathbb{Z}$. We could have been more sophisticated and argued as follows: if one manages to find a prime that splits completely in the ring class field of $\mathbb{Z} + \ell^d \mathcal{O}$ but not in the ring class field of $\mathbb{Z} + \ell^{d+1} \mathcal{O}$, then the residue field at p will certainly contain all j -invariants of elliptic curves with CM by $\mathbb{Z} + \ell^d \mathcal{O}$ but no j -invariant of elliptic curves with CM by $\mathbb{Z} + \ell^{d+1} \mathcal{O}$ (cfr. Corollary 2.8) and this would ensure the existence of the desired volcano. By the Chebotarëv density theorem, this can be achieved if and only if the two aforementioned ring class fields are distinct, which certainly happens if $\ell \neq 2$ or $\ell = 2$ and $d > 0$.

Ultimately, the difference in the two proofs lies in the following fact: in the first proof we have solved the equation

$$(5) \quad 4p = t^2 - v^2 \ell^{2d} D(\mathcal{O})$$

by first solving the auxiliary equation

$$(6) \quad p = x^2 - y^2 \ell^{2d} D(\mathcal{O})$$

and then multiplying by 2 the found x, y . However, (5) may have a solution even if (6) does not. For instance, the prime 3 is certainly not of the form $x^2 + 11y^2$, but we have $4 \cdot 3 = 1^2 + 11 \cdot 1^2$.

The proof appearing in this remark directly solves equation (5) without expressing p itself in the form $t^2 - v^2 \ell^{2d} D(\mathcal{O})$. This may be useful in view of explicit computations, since the smallest prime p solving (5) is smaller or equal than the smallest prime solving (6).

Depth $d = 0$. Let us now analyze more closely the first instance of the inverse volcano problem, that is, the case when our given volcano V coincides with its crater V_0 . We will now answer Question 4.2 in this case.

Proof of Theorem 1.1. We refer to the possible shapes of $V = V_0$ as described in Proposition 3.14. For each of the cases appearing in the proposition, we first want to find an imaginary quadratic field K and a prime $\mathfrak{L} \subseteq \mathcal{O}_K$ such that V is the abstract crater associated with \mathfrak{L} . In cases (1) – (5) it is easy to find such a field K of discriminant $D(\mathcal{O}_K) < -4$ and a prime ideal \mathfrak{L} with odd residue characteristic.

To deal with the case where V is a cycle of length $n \geq 3$ we appeal to [20, Theorem 2], which ensures the existence of an imaginary quadratic field K of discriminant < -4 whose class group contains an element of order n . Since by [2, Theorem 9.12] every ideal class contains infinitely many prime ideals, we deduce that there exists a prime $\ell > 2$ that splits in \mathcal{O}_K into two prime ideals of order n in the class group.

Applying Proposition 4.4 now allows us to conclude. \square

Depth $d > 0$. We now turn to the second, more difficult instance of the inverse volcano problem *i.e.* the case when V has depth $d > 0$. Given an ℓ -volcano V of depth $d > 0$, realising its crater V_0 as an abstract crater amounts to finding an imaginary quadratic order of conductor coprime to ℓ where there exists a prime ideal $\mathfrak{L} \supseteq \ell$ satisfying the condition in Proposition 3.14 corresponding to V_0 . In order to apply Proposition 4.4 we may also want the discriminant of the order to be smaller than -4 . So let us fix ℓ prime and see if we manage to find, for each of the six conditions expressed in Proposition 3.14, an imaginary quadratic order that realises that condition:

- (1) By Dirichlet's theorem on primes in arithmetic progression, there are infinitely many imaginary quadratic fields where ℓ is inert;
- (2) If $\ell \neq 3$, then ℓ ramifies in a principal ideal in the ring of integers of $\mathbb{Q}(\sqrt{-\ell})$ and the latter has discriminant < -4 . If $\ell = 3$ the same is true if we consider the order $\mathbb{Z}[\sqrt{-3}]$ of conductor 2 in $\mathbb{Q}(\sqrt{-3})$;
- (3) In the imaginary quadratic field $K = \mathbb{Q}(\sqrt{1-4\ell})$ the integral element $\alpha = \frac{1+\sqrt{1-4\ell}}{2}$ has norm ℓ . We deduce that ℓ splits in \mathcal{O}_K into the two principal prime ideals generated by α and $\bar{\alpha}$;
- (4) If q is a prime that is sufficiently large with respect to ℓ then in the ring of integers of $K = \mathbb{Q}(\sqrt{-\ell q})$ the prime ℓ is ramified into a non-principal ideal. This follows from the fact that every element $\alpha \in \mathcal{O}_K \setminus \mathbb{Z}$ has norm $N_{K/\mathbb{Q}}(\alpha) \geq (1 + \ell q)/4$.

Conditions (5) and (6) in Proposition 3.14 are more obscure, as they require to construct an imaginary quadratic field K where ℓ splits into two prime ideals whose class in the ideal class group of K has prescribed order n . We now prove that it is always possible to find such a field. Our construction is inspired by the techniques used by Nagell in [8] and very much depends on whether $\ell = 2$ or $\ell > 2$. We begin by treating the first case.

Proposition 4.6. *Let $n \neq 4$ be a positive integer and let $K = \mathbb{Q}(\sqrt{1-2^{n+2}})$. Then in \mathcal{O}_K the prime 2 splits into two prime ideals whose corresponding classes in $\text{Cl}(\mathcal{O}_K)$ have order n .*

Proof. Some preliminary remarks: write $\sqrt{1-2^{n+2}} = x \cdot \sqrt{-A}$ with $x, A \in \mathbb{Z}$ and $A > 0$ squarefree. In particular, we can write

$$(7) \quad Ax^2 + 1 = 2^{n+2}.$$

Moreover, since $n \geq 1$ we know that x is odd and we thus also have

$$(8) \quad 1 \equiv 1 - 2^{n+2} \equiv x^2 \cdot (-A) \equiv -A \pmod{8}$$

so that $D(\mathcal{O}_K) = -A$ and $2\mathcal{O}_K$ splits into two distinct conjugate prime ideals \mathfrak{p}_2 and $\bar{\mathfrak{p}}_2$.

Consider now the two conjugate principal ideals $\mathfrak{a} := \left(\frac{1+x\sqrt{-A}}{2}\right)$ and $\bar{\mathfrak{a}}$. We have

$$\mathfrak{a} \cdot \bar{\mathfrak{a}} = N_{K/\mathbb{Q}} \left(\frac{1+x\sqrt{-A}}{2} \right) = \frac{Ax^2+1}{4} = 2^n$$

hence these two ideals can be divisible only by \mathfrak{p}_2 and $\bar{\mathfrak{p}}_2$. Moreover, the ideals \mathfrak{a} and $\bar{\mathfrak{a}}$ are coprime, as one can see by adding their generators. Hence, we can assume without loss of generality that the prime ideal factorization of \mathfrak{a} is

$$\mathfrak{a} = \left(\frac{1+x\sqrt{-A}}{2} \right) = \mathfrak{p}_2^n$$

and in particular, the class of \mathfrak{p}_2 in $\text{Cl}(\mathcal{O}_K)$ has order dividing n . Our goal for the rest of this proof is to prove that this order is precisely n .

Assume by contradiction that this is not the case. Then there exists a prime q and $\tilde{u}, \tilde{v} \in \mathbb{Z}$ such that the following equality of ideals holds:

$$(9) \quad \left(\frac{\tilde{u} + \tilde{v}\sqrt{-A}}{2} \right)^q = \left(\frac{1+x\sqrt{-A}}{2} \right).$$

We now distinguish two cases.

First case: q odd. We begin by noting that $A \neq 3$ since by (8) we have $-A \equiv 1 \pmod{8}$. This implies, using that fact that q is odd, that all the units in \mathcal{O}_K are q -th powers. Hence, there exist $u, v \in \mathbb{Z}$ with $u \equiv v \pmod{2}$ such that the following equality of elements of K holds:

$$(10) \quad \left(\frac{u + v\sqrt{-A}}{2} \right)^q = \frac{1+x\sqrt{-A}}{2}.$$

Expanding the left-hand side and collecting the rational terms together, we reach the equality

$$(11) \quad u^q - \binom{q}{2} u^{q-2} v^2 A + \dots + \binom{q}{q-1} u v^{q-1} (-A)^{\frac{q-1}{2}} = 2^{q-1}.$$

Clearly, (11) implies that u divides 2^{q-1} . Suppose initially that u is even *i.e.* $u = 2c$ for some $c \in \mathbb{Z}$. Since $u \equiv v \pmod{2}$ we can also write $v = 2d$ for some $d \in \mathbb{Z}$. Plugging $2c$ and $2d$ in place of u and v in equation (11), one obtains that 2^q divides 2^{q-1} , a contradiction.

Hence, u must be odd, *i.e.* $u = \pm 1$. Reducing (11) modulo q we obtain

$$(\pm 1)^q \equiv 2^{q-1} \equiv 1 \pmod{q},$$

so, since q is odd, we in fact have $u = 1$. In particular, equality (10) now reads

$$\left(\frac{1 + v\sqrt{-A}}{2} \right)^q = \frac{1 + x\sqrt{-A}}{2}$$

and taking norms we obtain

$$\left(\frac{1 + v^2 A}{4} \right)^q = \frac{Ax^2 + 1}{4}.$$

After some manipulations, this can be rewritten as follows:

$$A^2 x^2 - (A + v^2 A^2) \left[\left(\frac{1 + v^2 A}{4} \right)^{\frac{q-1}{2}} \right]^2 = -A$$

so we reach an equation of the form

$$(12) \quad U^2 - DV^2 = -A$$

where $U = Ax$, $D = A + v^2A^2$ and $V = [(1 + v^2A)/4]^{(q-1)/2}$. We now wish to apply Mahler's theorem [8, Theorem 16], since all the prime factors of V divide D . Let us verify that the hypotheses of the theorem are satisfied:

- We certainly have $A \neq 1$ since $-A \equiv 1 \pmod{8}$. This also implies that $A \neq D$. Moreover A is squarefree by hypothesis;
- By the previous bullet point we have $D = A(1 + v^2A) > 1$. Moreover, D is not a perfect square since $v \neq 0$ (because it is odd), so all the primes dividing A cannot divide also $1 + v^2A$;

Hence, [8, Theorem 16] implies that the only positive solutions to (12) are given by the fundamental solution $U, V = U_1, V_1$ (that is, the solution with $U, V > 0$ such that $|U + \sqrt{D}V|$ is the smallest possible in absolute value) and by

$$U = \frac{U_1^3 + 3U_1V_1^2D}{A}, \quad V = \frac{3U_1^2V_1 + DV_1^3}{A}.$$

In our case, the fundamental solution is given by $U = vA$ and $V = 1$. This latter equality yields in particular $v^2A = 3$, hence $A = 3$, which is not possible.

By looking at the V of the non-fundamental solution, we find

$$\left(\frac{1 + v^2A}{4}\right)^{\frac{q-1}{2}} = V = \frac{3v^2A^2 + D}{A} = 1 + 4v^2A = 4(1 + v^2A) - 3.$$

In order to conclude, note that since v is odd, we have

$$1 + v^2A \equiv 1 + 1 \cdot 7 \equiv 0 \pmod{8}$$

so in particular the left-hand side of the above equality is even. However, the right-hand side of the equality is odd, contradiction. This concludes the proof in this case.

Second case: $q = 2$. By (8) we have $A \neq 1, 3$ and so $\mathcal{O}_K^\times = \{\pm 1\}$. Hence the equality of ideals (9) yields an equality of elements of K

$$\left(\frac{u + v\sqrt{-A}}{2}\right)^2 = \pm \frac{1 + x\sqrt{-A}}{2}$$

where $u, v \in \mathbb{Z}$ are such that $u \equiv v \pmod{2}$ (here we have simply set $u = \tilde{u}$ and $v = \tilde{v}$). Expanding and looking at rational/irrational parts gives

$$\begin{cases} u^2 - v^2A & = \pm 2 \\ 2uv & = \pm 2x. \end{cases}$$

By substituting $v = \pm x/u$ in the first equation and expanding we get

$$u^4 \mp 2u^2 - Ax^2 = 0,$$

and solving this quadratic equation gives, after using (7)

$$u^2 = 2^{n/2+1} \pm 1.$$

Looking modulo 4 one sees that $u^2 = 2^{n/2+1} - 1$ cannot hold, as $n \geq 2$. Hence we must have $u^2 = 2^{n/2+1} + 1$, or otherwise written $(u - 1)(u + 1) = 2^{n/2+1}$. This implies yields $u = \pm 3$ and $n = 4$. However, this case is excluded by our assumptions and the theorem is proved. \square

One can directly verify that in $\mathbb{Q}(\sqrt{-39})$ the prime 2 splits into two prime ideals having order 4 in the class group. This observation and the previous proposition imply that for every $n \in \mathbb{Z}_{>0}$ there exists an imaginary quadratic field K where 2 splits into two prime ideals having order n in $\text{Cl}(\mathcal{O}_K)$.

We now treat the case when ℓ is odd. We will prove that for every $n \in \mathbb{Z}_{>0}$ at least one among the imaginary quadratic fields $\mathbb{Q}(\sqrt{1-\ell^n})$ and $\mathbb{Q}(\sqrt{1-4\ell^n})$, call it K , has the property that the prime ℓ splits in \mathcal{O}_K into two prime ideals having order n in $\text{Cl}(\mathcal{O}_K)$. Let us begin by studying these fields separately.

Proposition 4.7. *Let $\ell \in \mathbb{N}$ be an odd prime and let $n \in \mathbb{Z}_{>0}$. Define $K := \mathbb{Q}(\sqrt{1-\ell^n})$. Suppose that:*

- (1) *Either $n \geq 3$ is odd and $(\ell, n) \neq (3, 5)$;*
- (2) *Or n is even and neither $\frac{\ell^{n/2}+1}{2}$ nor $\frac{\ell^{n/2}-1}{2}$ is a square;*

Then in \mathcal{O}_K the prime ℓ splits into two prime ideals whose corresponding classes in $\text{Cl}(\mathcal{O}_K)$ have order n .

Proof. We proceed as in the proof of Proposition 4.6. Write $\sqrt{1-\ell^n} = x \cdot \sqrt{-A}$ with $x, A \in \mathbb{Z}$ and $A > 0$ squarefree, so that we have

$$(13) \quad Ax^2 + 1 = \ell^n.$$

This equation implies in particular that $-A$ is a square modulo ℓ , so that $\ell\mathcal{O}_K = \mathfrak{p}_\ell \bar{\mathfrak{p}}_\ell$ with $\mathfrak{p}_\ell, \bar{\mathfrak{p}}_\ell \subseteq \mathcal{O}_K$ distinct prime ideals. Consider the two conjugate principal ideals $\mathfrak{a} := (1 + x\sqrt{-A})$ and $\bar{\mathfrak{a}}$. We have

$$\mathfrak{a} \cdot \bar{\mathfrak{a}} = N_{K/\mathbb{Q}}(1 + x\sqrt{-A}) = \ell^n.$$

Since ℓ is odd, the ideals \mathfrak{a} and $\bar{\mathfrak{a}}$ are coprime, so we have, without loss of generality, $\mathfrak{a} = \mathfrak{p}_\ell^n$. In particular, the class of \mathfrak{p}_ℓ in $\text{Cl}(\mathcal{O}_K)$ has order dividing n . If this order is not precisely n , then there exists a prime q and $u, v \in \mathbb{Z}$ with $u \equiv v \pmod{2}$ such that the following equality of ideals holds:

$$(14) \quad (1 + x\sqrt{-A}) = \left(\frac{u + v\sqrt{-A}}{2} \right)^q.$$

Suppose first that q is odd. Then, the proof of [8, Theorem 25] shows that we must have $x = 11$, $A = 2$, $\ell = 3$ and $q = 5$. From (13), we deduce that $q = n = 5$, which contradicts assumption (1).

Hence, we must have $q = 2$ and, in particular, n is even. Reducing equation (13) modulo 4 and using that A is squarefree, we see that x is even, say $x = 2y$ for $y \in \mathbb{Z}$. Now we can write

$$(15) \quad Ay^2 = \left(\frac{\ell^{n/2} - 1}{2} \right) \left(\frac{\ell^{n/2} + 1}{2} \right).$$

The factors on the right hand side are consecutive, hence coprime, integers. By assumption (2) neither of them can be a square, and we deduce that A must be divisible by at least two different primes. In particular, $A > 3$ and $\mathcal{O}_K^\times = \{\pm 1\}$.

Now from (14) we get the following equality of elements of K :

$$\left(\frac{u + v\sqrt{-A}}{2} \right)^2 = \pm(1 + x\sqrt{-A})$$

Expanding and looking at rational/irrational parts gives

$$\begin{cases} u^2 - v^2A & = \pm 4 \\ 2uv & = \pm 4x. \end{cases}$$

From the second equation we get $u \equiv v \equiv x \equiv 0 \pmod{2}$. So writing $(u', v', y) = (\frac{u}{2}, \frac{v}{2}, \frac{x}{2})$ and proceeding as in the second case of Proposition 4.6, we get

$$u^2 = \frac{\pm 1 + \sqrt{1 + 4y^2 A}}{2} = \frac{\pm 1 + \ell^{n/2}}{2},$$

which is excluded by our hypotheses. This concludes the proof. \square

Proposition 4.8. *Let $\ell \in \mathbb{N}$ be an odd prime, and n an even positive integer. Define $K := \mathbb{Q}(\sqrt{1 - 4\ell^n})$. If $\ell^{n/2}$ is not the sum two consecutive squares, then ℓ splits in \mathcal{O}_K into two prime ideals whose classes in $\text{Cl}(K)$ have order n .*

Proof. Write $\sqrt{1 - 4\ell^n} = x \cdot \sqrt{-A}$ with $x, A \in \mathbb{Z}$ and $A > 0$ squarefree. In particular,

$$(16) \quad Ax^2 + 1 = 4\ell^n.$$

We have that x is odd as it divides $4\ell^n - 1$. Thus $A \equiv 3 \pmod{8}$ and so $A \neq 1$. Suppose we have $A = 3$. Then (16) becomes

$$3x^2 = (2\ell^{n/2} - 1)(2\ell^{n/2} + 1).$$

Both factors on the right hand side are consecutive odd integers, so they are coprime. Hence one of them must be a perfect square and the other three times a perfect square. Suppose that $2\ell^{n/2} - 1$ is a square. Since it is odd, we would have $2\ell^{n/2} - 1 = (2j + 1)^2$ which is equivalent to $\ell^{n/2} = j^2 + (j + 1)^2$, contradicting our assumptions. This means that there exists $k \in \mathbb{Z}_{>0}$ such that $2\ell^{n/2} + 1 = k^2$. However, reducing this equality modulo 4 shows that this cannot happen either and we conclude that $A \neq 3$. In particular, $\mathcal{O}_K^\times = \{\pm 1\}$.

Equality (16) implies that ℓ splits in \mathcal{O}_K into distinct conjugate prime ideals \mathfrak{p}_ℓ and $\bar{\mathfrak{p}}_\ell$. Now consider the conjugate principal ideals $\mathfrak{a} = \left(\frac{1+x\sqrt{-A}}{2}\right)$ and $\bar{\mathfrak{a}}$. We have

$$\mathfrak{a}\bar{\mathfrak{a}} = N_{K/\mathbb{Q}}\left(\frac{1+x\sqrt{-A}}{2}\right) = \frac{1+Ax^2}{4} = \ell^n,$$

and $\mathfrak{a} + \bar{\mathfrak{a}} = \mathcal{O}_K$, so we can assume without loss of generality that $\mathfrak{a} = \mathfrak{p}_\ell^n$. Once again the class of \mathfrak{p}_ℓ in $\text{Cl}(K)$ has order dividing n and we want to prove this order is exactly n . Assume by contradiction it is not the case. Then there exists a prime divisor q of n and $u, v \in \mathbb{Z}$ with $u \equiv v \pmod{2}$ such that the following equality of ideals holds:

$$\left(\frac{u+v\sqrt{-A}}{2}\right)^q = \left(\frac{1+x\sqrt{-A}}{2}\right)^q.$$

If q is odd we use the same argument as in the first part of the proof of Proposition 4.6, using that $A \neq 1, 3$ to rule out this case. The argument goes through unchanged up until the final part, when we reach the equality

$$\left(\frac{1+v^2A}{4}\right)^{\frac{q-1}{2}} = 4(1+v^2A) - 3$$

with $v \in \mathbb{Z}$ odd. In Proposition 4.6 here we concluded by using the fact that $A \equiv 7 \pmod{8}$ in that setting. In the current setting however, the congruence $A \equiv 3 \pmod{8}$ does not yield any contradiction. Instead to conclude one can notice that after setting $z = \frac{1+v^2A}{4}$, the above equation becomes

$$z^{\frac{q-1}{2}} = 16z - 3$$

which does not have any integral solution.

Hence, we can assume that $q = 2$. Again using the fact that $\mathcal{O}_K^\times = \{\pm 1\}$, we have the following equality of elements of K :

$$\left(\frac{u + v\sqrt{-A}}{2}\right)^2 = \pm \frac{1 + x\sqrt{-A}}{2}$$

where $u, v \in \mathbb{Z}$ are such that $u \equiv v \pmod{2}$. With the usual arguments we arrive at

$$u^2 = \frac{\pm 2 + \sqrt{4 + 4x^2A}}{2} = \pm 1 + \sqrt{1 + x^2A} = \pm 1 + 2\ell^{n/2}.$$

As we showed above this is impossible and the proof is concluded. \square

One can directly verify that in $\mathbb{Q}(\sqrt{-971}) = \mathbb{Q}(\sqrt{1 - 4 \cdot 3^5})$ the prime 3 splits into two prime ideals of order 5 in the class group. This observation and the two previous propositions imply that for every $n \in \mathbb{Z}_{>0}$ and every odd prime ℓ there exists an imaginary quadratic field K where ℓ splits into two prime ideals having order n in $\text{Cl}(\mathcal{O}_K)$.

We are now ready to prove Theorem 1.3.

Proof of Theorem 1.3. By Propositions 4.6, 4.7 and 4.8 and the comments in between, it suffices to show that for every even $n \in \mathbb{N}$ the two sets

$$E_1(n) := \left\{ \ell > 2 \text{ prime} : \frac{\ell^{n/2} - 1}{2} = j^2 \text{ or } \frac{\ell^{n/2} + 1}{2} = j^2 \text{ for some } j \in \mathbb{N} \right\},$$

$$E_2(n) := \left\{ \ell > 2 \text{ prime} : \ell^{n/2} = j^2 + (j + 1)^2 \text{ for some } j \in \mathbb{N} \right\}$$

have empty intersection. Let $\ell \in E_1(n) \cap E_2(n)$. Then there exists $j \in \mathbb{N}$ such that $\ell^{n/2} = j^2 + (j + 1)^2$. We have

$$\frac{\ell^{n/2} - 1}{2} = j^2 + j,$$

and

$$\frac{\ell^{n/2} + 1}{2} = j^2 + j + 1.$$

Suppose there exists $k \in \mathbb{N}$ such that $k^2 = \frac{\ell^{n/2} - 1}{2}$. Then $(k - j)(k + j) = j$, so $k + j$ divides j , which is impossible as $j, k > 0$. Hence, since $\ell \in E_1(n)$, there exists $k \in \mathbb{N}$ such that $k^2 = \frac{\ell^{n/2} + 1}{2}$, that is, $(k - j)(k + j) = j + 1$. Now we must have $k + j$ divides $j + 1$ yielding $k = 1$ and $j = 0$. This is impossible, and the corollary follows. \square

Theorem 1.2 now follows by combining Proposition 4.4 and Theorem 1.3. The inverse volcano problem over \mathbb{F}_p is solved.

5. NEW QUESTIONS

In this final section, we discuss two follow-up projects: first, the inverse volcano problem over more general finite fields. Second, the question of solving the inverse volcano problem with algorithmic efficiency.

FIGURE 5. The abstract volcano induced by $(V_0, 2, 1)$.

5.1. The inverse volcano problem over \mathbb{F}_{p^s} with $s > 1$. The inverse volcano problem over \mathbb{F}_{p^s} with $s > 1$ does not always have a solution. An example where $s = 2$ is provided by the next proposition.

Proposition 5.1. *Let V_0 be a cycle of length 2 and let V be the abstract volcano induced by $(V_0, 2, 1)$, as in Figure 5. For every prime $p \neq 2$, the volcano V is not a connected component of $\mathcal{G}_2(\mathbb{F}_{p^2})$.*

Proof. Let us first notice that the ring of integers \mathcal{O}_K of $K := \mathbb{Q}(\sqrt{-15})$ is the only imaginary quadratic order where 2 splits into two ideals having order 2 in its class group (for example this can be seen using Lemma 5.2 proved below). Hence, if V were an isogeny volcano in characteristic p , the elliptic curves corresponding to the vertices on its crater would have necessarily complex multiplication by \mathcal{O}_K and p would be split in it. Let H be the ring class field relative to the order $\mathcal{O} := \mathbb{Z}[2\sqrt{-15}]$. The natural exact sequence (see [9, Chapter I, Proposition 12.9])

$$1 \rightarrow (\mathcal{O}_K/4\mathcal{O}_K)^\times / \{\pm 1\} \rightarrow \text{Cl}(\mathcal{O}) \rightarrow \text{Cl}(\mathcal{O}_K) \rightarrow 1$$

splits, so we have $\text{Gal}(H/K) \cong (\mathbb{Z}/2\mathbb{Z})^2$. In particular, by [2, Lemma 9.3]

$$\text{Gal}(H/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2 \rtimes \mathbb{Z}/2\mathbb{Z} \cong (\mathbb{Z}/2\mathbb{Z})^3$$

and this implies that every prime $\mathfrak{p} \subseteq \mathcal{O}_H$ has residue degree bounded by 2. Hence, for every prime $p \neq 2$ and split in \mathcal{O}_K the field \mathbb{F}_{p^2} contains the j -invariants of elliptic curves with complex multiplication by \mathcal{O} . The connected component of $\mathcal{G}_2(\mathbb{F}_{p^2})$ containing them must necessarily be a volcano of depth ≥ 2 whose crater vertices correspond to all the elliptic curves with complex multiplication by \mathcal{O}_K . This proves the proposition. \square

This fact triggers many questions: what are the obstructions to a possible solution? Are there infinitely many abstract volcanoes that are not connected components of ordinary isogeny graphs over \mathbb{F}_{p^s} , for fixed $s > 1$? If there are only finitely many counter-examples, how many of them? This will be the subject of further research.

5.2. Algorithmic corner. For any given abstract volcano V it is possible to explicitly find some ordinary isogeny graph that contains V as a connected component, as our proofs show. However, computationally speaking, our theorems are far from optimal. For instance, by Theorem 1.3 the prime 3 certainly splits into two prime ideals having order 5 in the ideal class group of $\mathbb{Q}(\sqrt{-971})$. However, the same is true for the field $\mathbb{Q}(\sqrt{-47})$, whose discriminant is more than 20 times smaller in absolute value. In this respect, the following easy lemma can be a useful tool for computational purposes.

Lemma 5.2. *Let ℓ be a prime and $n \in \mathbb{N}$ a fixed integer. Suppose that \mathcal{O} is an imaginary quadratic order of conductor coprime to ℓ where ℓ splits into two prime ideals having order n in $\text{Cl}(\mathcal{O})$. Then $|D(\mathcal{O})| \leq 4\ell^n - 1$.*

Proof. Set $K := \text{Frac}(\mathcal{O})$ and let \mathfrak{L} and $\overline{\mathfrak{L}}$ be the two distinct prime ideals lying above ℓ . Then by assumption there exists $\alpha \in \mathcal{O}$ such that $\mathfrak{L}^n = (\alpha)$. We have that $\alpha \notin \mathbb{Z}$ since otherwise n would be even and $\alpha = \pm\ell^{n/2}$, implying that $\mathfrak{L} = \overline{\mathfrak{L}}$. The lemma now follows from the fact that every element $\beta \in \mathcal{O} \setminus \mathbb{Z}$ satisfies $N_{K/\mathbb{Q}}(\beta) \geq \frac{1+|D(\mathcal{O})|}{4}$. \square

Applying the above lemma sometimes leads to easier (*i.e.* with associated imaginary quadratic field that has smaller discriminant) solutions than the ones provided by Theorem 1.3.

Example 5.3. Let V_0 be a cycle of length 6 and let V be the volcano induced by $(V_0, 2, 1)$, as in Figure 6.

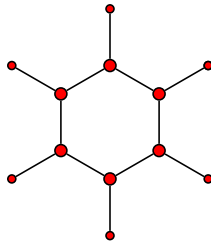


FIGURE 6. The abstract volcano V .

We claim that V is realisable as a connected component of $\mathcal{G}_2(\mathbb{F}_{103})$ (more precisely, as a connected component of the 8-cordillera in this graph). Indeed, using Lemma 5.2 one finds that $K = \mathbb{Q}(\sqrt{-87})$ is an imaginary quadratic field where $\ell = 2$ splits into two ideals having order 6 in $\text{Cl}(\mathcal{O}_K)$. The prime $p = 103$ splits completely in the ring class field of $\mathbb{Z}[\sqrt{-87}]$ but does not split completely in the ring class field of $\mathbb{Z}[2\sqrt{-87}]$. We have

$$4 \cdot 103 = 8^2 + 87 \cdot 2^2$$

and the results explained in this paper now imply the result.

We encourage the reader to work out that the three abstract volcanoes appearing in Figure 4 are connected components, respectively, of the isogeny graphs $\mathcal{G}_2(\mathbb{F}_{1009})$, $\mathcal{G}_3(\mathbb{F}_{1303})$ and $\mathcal{G}_3(\mathbb{F}_{997})$.

APPENDIX A. FULL STUDY FOR $p = 1009$ AND $\ell = 3$

In this section, we present the 3-isogeny graph $\mathcal{G}_3(\mathbb{F}_{1009})$, and count the number of vertices in each connected components. This count is essentially another take on the Hurwitz class number formula (see [2], formula (14.21))

$$p = \frac{1}{2} \sum_{0 < |a| < 2\sqrt{p}} H(a^2 - 4p).$$

From Lemma 3.4, we expect traces of maximal absolute value $\lfloor 2\sqrt{1009} \rfloor = 63$.

Note that $1009 \equiv 1 \pmod{12}$, therefore $j = 0$ and $j = 719$ are j -invariants of ordinary elliptic curves (where $1728 \equiv 719 \pmod{1009}$).

A.1. Supersingulars. We can check that the set of supersingular j -invariants is

$$\{149, 155, 157, 529, 602, 605, 838, 890, 897, 905\},$$

of cardinality 10.

A.2. More automorphisms than usual: $j = 0$. As $1009 \equiv 1 \pmod{3}$, 0 is ordinary, and we can compute the three traces in its cordillera: $(t_1, t_2, t_3) = (19, 43, 62)$. The orders $\mathbb{Z}[\pi_{t_i}]$ for $i \in \{t_1, t_2, t_3\}$ have pairwise coprime conductors f_1, f_2, f_3 . If two of the conductors had a common prime factor q , then there would exist a q -isogeny connecting curves with different traces, which is impossible if neither of the curves have j -invariant 0 or 1728. We obtain $f_1 = 5 \cdot 7$, $f_2 = 3^3$ and $f_3 = 2^3$. We deduce that 0 must connect to points corresponding to curves of trace $t_2 = 43$, as $\ell | f_2$. We expect volcanoes in the cordillera to have depth 0 if the trace of their curves is t_1 or t_3 , and depth 3 if it is t_2 or the curve has j -invariant 0. How 0 connects to the rest of the cordillera has been described in Proposition 3.19. This behaviour can be observed in Figure 7 with vertex $j = 0$ pictured in blue.

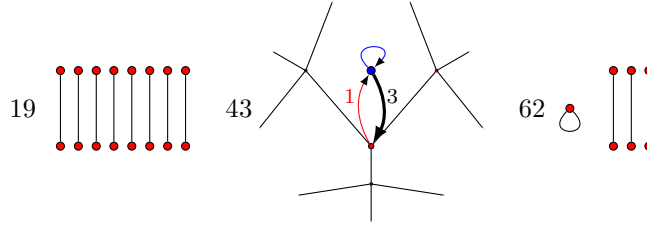


FIGURE 7. The 19/43/62-cordillera in $\mathcal{G}_3(\mathbb{F}_{1009})$.

Using Lemma 3.25, the number of vertices in the volcano containing 0 is given by

$$1 + \frac{2 \cdot 1}{6} \times \left(3 - \left(\frac{D(\mathcal{O}_K)}{3} \right) \right) \frac{3^3 - 1}{3 - 1} = 1 + \frac{27 - 1}{3 - 1} = 14$$

as $K = \mathbb{Q}(\sqrt{-3})$. We can compute the number of vertices in the cordilleras associated with K that are not connected to $j = 0$, belt by belt. The conductors of $\mathbb{Z}[\pi_{t_i}]$ stripped of multiples of 3 are $5 \cdot 7$ for $t_1 = 19$, 1 for $t_2 = 43$ and 2^3 for $t_3 = 62$, therefore the number of vertices for trace 19 is

$$h(5^2 \cdot (-3)) + h(7^2 \cdot (-3)) + h(35^2 \cdot (-3)) = 2 + 2 + 12 = 16$$

and

$$h(2^2 \cdot (-3)) + h(4^2 \cdot (-3)) + h(8^2 \cdot (-3)) = 1 + 2 + 4 = 7$$

for trace 62. There are no additional belts for trace 43 because the f_2 is a power of ℓ .

A.3. More automorphisms than usual: $j = 1728$. The same study can be done for 1728 (or rather 719 as we are in \mathbb{F}_{1009}), $1728 \equiv 1 \pmod{4}$ so we know that two traces are associated with 719 in this case: $(t_4, t_5) = (30, 56)$. The conductors are coprime $f_4 = 2^2 \cdot 7$ and $f_5 = 3 \cdot 5$, hence according to Proposition 3.20, 719 in blue connects to $\frac{3+1}{2}$ curves of trace t_5 . Figure 8 shows the non-regular subgraph for 1728.

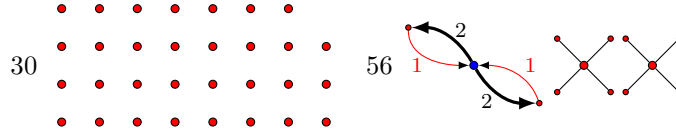


FIGURE 8. The 30- and 56-cordilleras in $\mathcal{G}_3(\mathbb{F}_{1009})$.

As $K = \mathbb{Q}(\sqrt{-4})$, we can compute the number of points in the belt where the vertex 1728 attaches:

$$1 + \frac{2 \cdot 1}{4} \left(3 - \left(\frac{D(\mathcal{O}_K)}{3} \right) \right) \frac{3^1 - 1}{3 - 1} = 1 + \frac{4}{2} = 3.$$

Counting the other vertices gives

$$\sum_{1 < m | 28} h(-4m^2) = 31$$

for trace 30 and

$$h(-4 \cdot 5^2) \left(1 + (3 - (-1)) \left(\frac{3^1 - 1}{3 - 1} \right) \right) = 10$$

for trace 56.

A.4. Regular case. In this section we present an extensive classification of all volcanoes appearing as regular connected components in $\mathcal{G}_3(\mathbb{F}_{1009})$, and we count their number of vertices. We go through the graph belt by belt and expose the results in four tables.

The first table, Figure 9 lists volcanoes that are single vertices. We can note that they arise in cordilleras whose traces are multiples of 3. Indeed if the trace is a multiple of 3, v in the equation $4p = t^2 - D(\mathcal{O}_K)v^2$ can not be divisible by three, and the Kronecker symbol $(D(\mathcal{O}_K)/3)$ is always -1 , meaning that 3 is inert in K . This is also the case for the 30-cordillera, already discussed in the non-regular case (see Figure 8).

Secondly in Figure 10 we look at cordilleras with volcanoes that are just two vertices connected by a single edge. These are frequent and can be listed in the same way. Another example is the 19-cordillera shown in Figure 7, with 16 vertices and 8 volcanoes.

Cordillera (Trace)	Associated field	Belt (Order)	Vertex count	Volcano shape
3	$\mathbb{Q}(\sqrt{-4027})$	$\mathbb{Z}[\sqrt{-4027}]$	$h(-4027) = 9$	$\bullet \times 9$
6	$\mathbb{Q}(\sqrt{-40})$	$\mathbb{Z}[\sqrt{-40}]$	$h(-40) = 2$	$\bullet \times 2$
		$\mathbb{Z}[2\sqrt{-40}]$	$h(-160) = 4$	$\bullet \times 4$
		$\mathbb{Z}[5\sqrt{-40}]$	$h(-1000) = 10$	$\bullet \times 10$
		$\mathbb{Z}[10\sqrt{-40}]$	$h(-4000) = 20$	$\bullet \times 20$
9	$\mathbb{Q}(\sqrt{-3955})$	$\mathbb{Z}[\sqrt{-3955}]$	$h(-3955) = 12$	$\bullet \times 12$
12	$\mathbb{Q}(\sqrt{-3892})$	$\mathbb{Z}[\sqrt{-3892}]$	$h(-3892) = 12$	$\bullet \times 12$
15	$\mathbb{Q}(\sqrt{-3811})$	$\mathbb{Z}[\sqrt{-3811}]$	$h(-3811) = 10$	$\bullet \times 10$
18	$\mathbb{Q}(\sqrt{-232})$	$\mathbb{Z}[\sqrt{-232}]$	$h(-232) = 2$	$\bullet \times 2$
		$\mathbb{Z}[2\sqrt{-232}]$	$h(-928) = 4$	$\bullet \times 4$
		$\mathbb{Z}[4\sqrt{-232}]$	$h(-3712) = 8$	$\bullet \times 8$
21	$\mathbb{Q}(\sqrt{-3595})$	$\mathbb{Z}[\sqrt{-3595}]$	$h(-3595) = 8$	$\bullet \times 8$
24	$\mathbb{Q}(\sqrt{-3460})$	$\mathbb{Z}[\sqrt{-3460}]$	$h(-3460) = 16$	$\bullet \times 16$
27	$\mathbb{Q}(\sqrt{-3307})$	$\mathbb{Z}[\sqrt{-3307}]$	$h(-3307) = 9$	$\bullet \times 9$
33	$\mathbb{Q}(\sqrt{-2947})$	$\mathbb{Z}[\sqrt{-2947}]$	$h(-2947) = 8$	$\bullet \times 8$
36	$\mathbb{Q}(\sqrt{-2740})$	$\mathbb{Z}[\sqrt{-2740}]$	$h(-2740) = 12$	$\bullet \times 12$
39	$\mathbb{Q}(\sqrt{-2515})$	$\mathbb{Z}[\sqrt{-2515}]$	$h(-2515) = 6$	$\bullet \times 6$
42	$\mathbb{Q}(\sqrt{-568})$	$\mathbb{Z}[\sqrt{-568}]$	$h(-568) = 4$	$\bullet \times 4$
		$\mathbb{Z}[2\sqrt{-568}]$	$h(-2272) = 8$	$\bullet \times 8$
45	$\mathbb{Q}(\sqrt{-2011})$	$\mathbb{Z}[\sqrt{-2011}]$	$h(-2011) = 7$	$\bullet \times 7$
48	$\mathbb{Q}(\sqrt{-1732})$	$\mathbb{Z}[\sqrt{-1732}]$	$h(-1732) = 12$	$\bullet \times 12$
51	$\mathbb{Q}(\sqrt{-1435})$	$\mathbb{Z}[\sqrt{-1435}]$	$h(-1435) = 4$	$\bullet \times 4$
54	$\mathbb{Q}(\sqrt{-280})$	$\mathbb{Z}[\sqrt{-280}]$	$h(-280) = 4$	$\bullet \times 4$
		$\mathbb{Z}[2\sqrt{-280}]$	$h(-1120) = 8$	$\bullet \times 8$
57	$\mathbb{Q}(\sqrt{-787})$	$\mathbb{Z}[\sqrt{-787}]$	$h(-787) = 5$	$\bullet \times 5$
60	$\mathbb{Q}(\sqrt{-436})$	$\mathbb{Z}[\sqrt{-436}]$	$h(-436) = 6$	$\bullet \times 6$
63	$\mathbb{Q}(\sqrt{-67})$	$\mathbb{Z}[\sqrt{-67}]$	$h(-67) = 1$	\bullet

FIGURE 9. Distribution of single-point volcanoes in $\mathcal{G}_3(\mathbb{F}_{1009})$.

Cordillera (Trace)	Associated field	Belt (Order)	Vertex count	Volcano shape
1	$\mathbb{Q}(\sqrt{-4035})$	$\mathbb{Z}[\sqrt{-4035}]$	$h(-4035) = 12$	$\bullet\text{---}\bullet \times 6$
4	$\mathbb{Q}(\sqrt{-4020})$	$\mathbb{Z}[\sqrt{-4020}]$	$h(-4020) = 16$	$\bullet\text{---}\bullet \times 8$
5	$\mathbb{Q}(\sqrt{-4011})$	$\mathbb{Z}[\sqrt{-4011}]$	$h(-4011) = 20$	$\bullet\text{---}\bullet \times 10$
8	$\mathbb{Q}(\sqrt{-3972})$	$\mathbb{Z}[\sqrt{-3972}]$	$h(-3972) = 12$	$\bullet\text{---}\bullet \times 6$
10	$\mathbb{Q}(\sqrt{-984})$	$\mathbb{Z}[\sqrt{-984}]$ $\mathbb{Z}[2\sqrt{-984}]$	$h(-984) = 12$ $h(-3936) = 24$	$\bullet\text{---}\bullet \times 6$ $\bullet\text{---}\bullet \times 12$
13	$\mathbb{Q}(\sqrt{-3867})$	$\mathbb{Z}[\sqrt{-3867}]$	$h(-3867) = 14$	$\bullet\text{---}\bullet \times 7$
14	$\mathbb{Q}(\sqrt{-15})$	$\mathbb{Z}[\sqrt{-15}]$ $\mathbb{Z}[2\sqrt{-15}]$ $\mathbb{Z}[4\sqrt{-15}]$ $\mathbb{Z}[8\sqrt{-15}]$ $\mathbb{Z}[16\sqrt{-15}]$	$h(-15) = 2$ $h(-60) = 2$ $h(-240) = 4$ $h(-960) = 8$ $h(-3840) = 16$	$\bullet\text{---}\bullet$ $\bullet\text{---}\bullet$ $\bullet\text{---}\bullet \times 2$ $\bullet\text{---}\bullet \times 4$ $\bullet\text{---}\bullet \times 8$
17	$\mathbb{Q}(\sqrt{-3747})$	$\mathbb{Z}[\sqrt{-3747}]$	$h(-3747) = 12$	$\bullet\text{---}\bullet \times 6$
22	$\mathbb{Q}(\sqrt{-888})$	$\mathbb{Z}[\sqrt{-888}]$ $\mathbb{Z}[2\sqrt{-888}]$	$h(-888) = 12$ $h(-3552) = 24$	$\bullet\text{---}\bullet \times 6$ $\bullet\text{---}\bullet \times 12$
23	$\mathbb{Q}(\sqrt{-3507})$	$\mathbb{Z}[\sqrt{-3507}]$	$h(-3507) = 8$	$\bullet\text{---}\bullet \times 4$
26	$\mathbb{Q}(\sqrt{-840})$	$\mathbb{Z}[\sqrt{-840}]$ $\mathbb{Z}[2\sqrt{-840}]$	$h(-840) = 8$ $h(-3360) = 16$	$\bullet\text{---}\bullet \times 4$ $\bullet\text{---}\bullet \times 8$
28	$\mathbb{Q}(\sqrt{-3252})$	$\mathbb{Z}[\sqrt{-3252}]$	$h(-3252) = 12$	$\bullet\text{---}\bullet \times 6$
31	$\mathbb{Q}(\sqrt{-123})$	$\mathbb{Z}[\sqrt{-123}]$ $\mathbb{Z}[5\sqrt{-123}]$	$h(-123) = 2$ $h(-3075) = 12$	$\bullet\text{---}\bullet$ $\bullet\text{---}\bullet \times 6$
32	$\mathbb{Q}(\sqrt{-3012})$	$\mathbb{Z}[\sqrt{-3012}]$	$h(-3012) = 12$	$\bullet\text{---}\bullet \times 6$
35	$\mathbb{Q}(\sqrt{-2811})$	$\mathbb{Z}[\sqrt{-2811}]$	$h(-2811) = 16$	$\bullet\text{---}\bullet \times 8$
37	$\mathbb{Q}(\sqrt{-2667})$	$\mathbb{Z}[\sqrt{-2667}]$	$h(-2667) = 8$	$\bullet\text{---}\bullet \times 4$
40	$\mathbb{Q}(\sqrt{-2436})$	$\mathbb{Z}[\sqrt{-2436}]$	$h(-2436) = 16$	$\bullet\text{---}\bullet \times 8$
41	$\mathbb{Q}(\sqrt{-2355})$	$\mathbb{Z}[\sqrt{-2355}]$	$h(-2355) = 12$	$\bullet\text{---}\bullet \times 6$
44	$\mathbb{Q}(\sqrt{-84})$	$\mathbb{Z}[\sqrt{-84}]$ $\mathbb{Z}[5\sqrt{-84}]$	$h(-84) = 4$ $h(-2100) = 16$	$\bullet\text{---}\bullet \times 2$ $\bullet\text{---}\bullet \times 8$
46	$\mathbb{Q}(\sqrt{-120})$	$\mathbb{Z}[\sqrt{-120}]$ $\mathbb{Z}[2\sqrt{-120}]$ $\mathbb{Z}[4\sqrt{-120}]$	$h(-120) = 4$ $h(-480) = 8$ $h(-1920) = 16$	$\bullet\text{---}\bullet \times 2$ $\bullet\text{---}\bullet \times 4$ $\bullet\text{---}\bullet \times 8$
49	$\mathbb{Q}(\sqrt{-1635})$	$\mathbb{Z}[\sqrt{-1635}]$	$h(-1635) = 8$	$\bullet\text{---}\bullet \times 4$
50	$\mathbb{Q}(\sqrt{-24})$	$\mathbb{Z}[\sqrt{-24}]$ $\mathbb{Z}[2\sqrt{-24}]$ $\mathbb{Z}[4\sqrt{-24}]$ $\mathbb{Z}[8\sqrt{-24}]$	$h(-24) = 2$ $h(-96) = 4$ $h(-384) = 8$ $h(-1536) = 16$	$\bullet\text{---}\bullet$ $\bullet\text{---}\bullet \times 2$ $\bullet\text{---}\bullet \times 4$ $\bullet\text{---}\bullet \times 8$
53	$\mathbb{Q}(\sqrt{-1227})$	$\mathbb{Z}[\sqrt{-1227}]$	$h(-1227) = 4$	$\bullet\text{---}\bullet \times 2$
55	$\mathbb{Q}(\sqrt{-1011})$	$\mathbb{Z}[\sqrt{-1011}]$	$h(-1011) = 12$	$\bullet\text{---}\bullet \times 6$
58	$\mathbb{Q}(\sqrt{-168})$	$\mathbb{Z}[\sqrt{-168}]$ $\mathbb{Z}[2\sqrt{-168}]$	$h(-168) = 4$ $h(-672) = 8$	$\bullet\text{---}\bullet \times 2$ $\bullet\text{---}\bullet \times 4$
59	$\mathbb{Q}(\sqrt{-555})$	$\mathbb{Z}[\sqrt{-555}]$	$h(-555) = 4$	$\bullet\text{---}\bullet \times 2$

FIGURE 10. Distribution of double-point volcanoes in $\mathcal{G}_3(\mathbb{F}_{1009})$.

The next cordilleras have volcanoes in an X-shape. They are pictured in Figure 11.








Cordillera (Trace)	Associated field	Belt (Order)	Vertex count	Volcano shape
2	$\mathbb{Q}(\sqrt{-7})$	$\mathbb{Z}[\sqrt{-7}]$	$\left(1 + (3 - (-7/3)) \left(\frac{3^1-1}{3-1}\right)\right) h(-7) = 5$	
		$\mathbb{Z}[2\sqrt{-7}]$	$\left(1 + (3 - (-28/3)) \left(\frac{3^1-1}{3-1}\right)\right) h(-28) = 5$	
		$\mathbb{Z}[4\sqrt{-7}]$	$\left(1 + (3 - (-112/3)) \left(\frac{3^1-1}{3-1}\right)\right) h(-112) = 10$	 $\times 2$
		$\mathbb{Z}[8\sqrt{-7}]$	$\left(1 + (3 - (-448/3)) \left(\frac{3^1-1}{3-1}\right)\right) h(-448) = 20$	 $\times 4$
25	$\mathbb{Q}(\sqrt{-379})$	$\mathbb{Z}[\sqrt{-379}]$	$\left(1 + (3 - (-379/3)) \left(\frac{3^1-1}{3-1}\right)\right) h(-379) = 15$	 $\times 3$
29	$\mathbb{Q}(\sqrt{-355})$	$\mathbb{Z}[\sqrt{-355}]$	$\left(1 + (3 - (-355/3)) \left(\frac{3^1-1}{3-1}\right)\right) h(-355) = 20$	 $\times 4$
52	$\mathbb{Q}(\sqrt{-148})$	$\mathbb{Z}[\sqrt{-148}]$	$\left(1 + (3 - (-148/3)) \left(\frac{3^1-1}{3-1}\right)\right) h(-148) = 10$	 $\times 2$

FIGURE 11. Distribution of X-shaped volcanoes in $\mathcal{G}_3(\mathbb{F}_{1009})$.

Finally, the remaining vertices form larger more diverse volcanoes that are described in Figure 12.












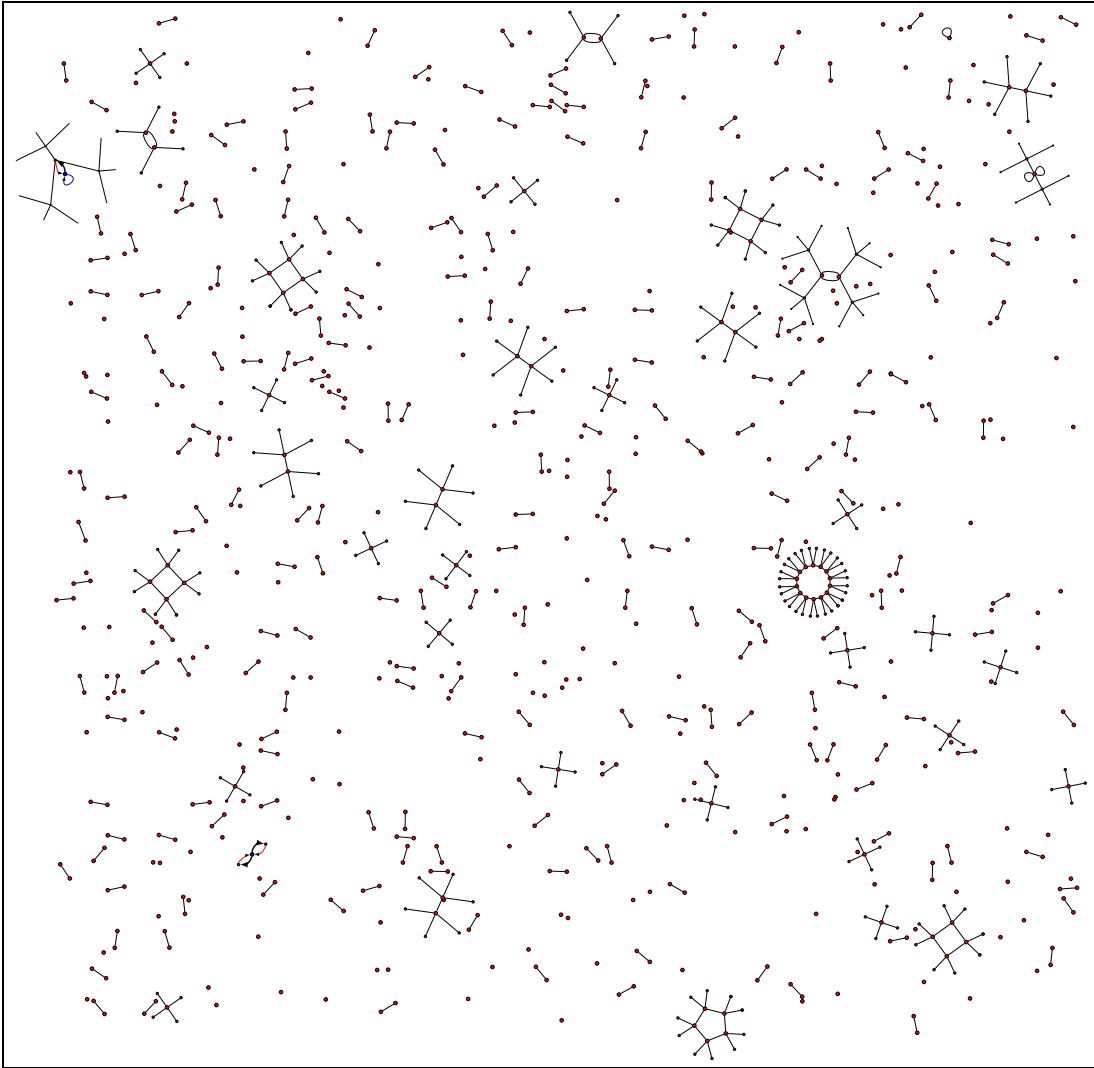
Cordillera (Trace)	Associated field	Belt (Order)	Vertex count	Volcano shape
7	$\mathbb{Q}(\sqrt{-443})$	$\mathbb{Z}[\sqrt{-443}]$	$3^1 \cdot h(-443) = 15$	
11	$\mathbb{Q}(\sqrt{-435})$	$\mathbb{Z}[\sqrt{-435}]$	$(1+3)h(-435) = 16$	 $\times 2$
16	$\mathbb{Q}(\sqrt{-420})$	$\mathbb{Z}[\sqrt{-420}]$	$(1+3)h(-420) = 32$	 $\times 4$
20	$\mathbb{Q}(\sqrt{-404})$	$\mathbb{Z}[\sqrt{-404}]$	$3^1 \cdot h(-404) = 42$	
34	$\mathbb{Q}(\sqrt{-20})$	$\mathbb{Z}[\sqrt{-20}]$	$3^1 \cdot h(-20) = 6$	
		$\mathbb{Z}[2\sqrt{-20}]$	$3^1 \cdot h(-80) = 12$	
		$\mathbb{Z}[4\sqrt{-20}]$	$3^1 \cdot h(-320) = 24$	 $\times 2$
38	$\mathbb{Q}(\sqrt{-8})$	$\mathbb{Z}[\sqrt{-8}]$	$3^2 \cdot h(-8) = 9$	
		$\mathbb{Z}[2\sqrt{-8}]$	$3^2 \cdot h(-32) = 18$	
47	$\mathbb{Q}(\sqrt{-203})$	$\mathbb{Z}[\sqrt{-203}]$	$3^1 \cdot h(-203) = 12$	
61	$\mathbb{Q}(\sqrt{-35})$	$\mathbb{Z}[\sqrt{-35}]$	$3^1 \cdot h(-35) = 6$	

FIGURE 12. Distribution of larger volcanoes in $\mathcal{G}_3(\mathbb{F}_{1009})$.

This completes our extensive description of $\mathcal{G}_3(\mathbb{F}_{1009})$. We may now check that all vertices are accounted for by adding all red numbers. We obtain a total of

- 10 supersingular j -invariants;
- $14 + 16 + 7 = 37$ non-regular vertices for 0;
- $3 + 31 + 10 = 44$ non-regular vertices for 1728;
- 211 solo regular vertices;
- 430 vertices in regular duos;
- 85 vertices in X-shaped volcanoes;
- and 192 vertices in larger volcanoes.

In total $10 + 37 + 44 + 211 + 430 + 85 + 192 = 1009 = p$ vertices!

APPENDIX B. THE FULL ISOGENY GRAPH FOR $p = 1009$ AND $\ell = 3$ FIGURE 13. The volcano park $\mathcal{G}_3(1009)$

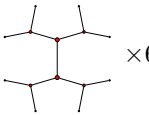
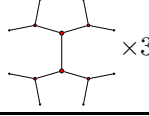
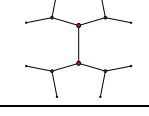
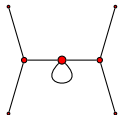
m	$h(\mathcal{O}_0)$	ord_m	$\mathcal{B}_{t,m}$
1	12	2	 $\times 6$
3	6	2	 $\times 3$
5	2	2	
$3 \cdot 5$	1	1	

FIGURE 14. The 22-cordillera in $\mathcal{G}_2(\mathbb{F}_{7321})$.

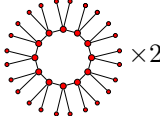
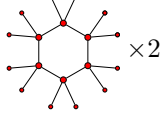
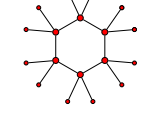
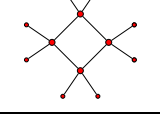
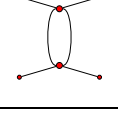
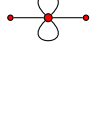
m	$h(\mathcal{O}_0)$	ord_m	$\mathcal{B}_{t,m}$
1	24	12	 $\times 2$
2	12	6	 $\times 2$
2^2	6	6	
5	4	4	
$2 \cdot 5$	2	2	
$2^2 \cdot 5$	1	1	

FIGURE 15. The 22-cordillera in $\mathcal{G}_3(\mathbb{F}_{7321})$.

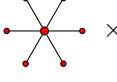
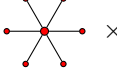
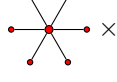
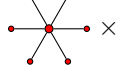
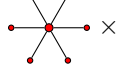

m	$h(\mathcal{O}_0)$	ord_m	$\mathcal{B}_{t,m}$
1	8	1	 $\times 8$
2	4	1	 $\times 4$
2^2	2	1	 $\times 2$
3	4	1	 $\times 4$
$2 \cdot 3$	2	1	 $\times 2$
$2^2 \cdot 3$	1	1	

FIGURE 16. The 22-cordillera in $\mathcal{G}_5(\mathbb{F}_{7321})$.

REFERENCES

- [1] D.X. Charles, K.E. Lauter, and E.Z. Goren. Cryptographic hash functions from expander graphs. *J. Cryptology*, 22(1):93–113, 2009.
- [2] D.A. Cox. *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*. John Wiley & Sons, Inc., Hoboken, NJ, USA, April 1997.
- [3] L. De Feo, D. Jao, and J. Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *J. Math. Cryptol.*, 8(3):209–247, 2014.
- [4] M. Fouquet and F. Morain. Isogeny volcanoes and the sea algorithm. In C. Fieker and D.R. Kohel, editors, *Algorithmic Number Theory*, pages 276–291, Berlin, Heidelberg, 2002. Springer Berlin Heidelberg.
- [5] D. Kohel. *Endomorphism rings of elliptic curves over finite fields*. PhD thesis, University of California at Berkeley, 1996.
- [6] S. Lang. *Elliptic Functions*, volume 112 of *Graduate Texts in Mathematics*. Springer New York, New York, NY, 1987.
- [7] J. Miret, D. Sadornil, J. Tena, R. Tomàs, and M. Valls. Isogeny cordillera algorithm to obtain cryptographically good elliptic curves. In *ACSW*, 2007.
- [8] T. Nagell. Contributions to the theory of a category of Diophantine equations of the second degree with two unknowns. *Nova Acta Soc. Sci. Upsaliensis (4)*, 16(2):38, 1955.
- [9] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.
- [10] A.K. Pizer. Ramanujan graphs and Hecke operators. *Bull. Amer. Math. Soc. (N.S.)*, 23(1):127–137, 1990.
- [11] R. Schoof. Counting points on elliptic curves over finite fields. *Journal de Théorie des Nombres de Bordeaux*, 7(1):219–254, 1995.
- [12] J.H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.
- [13] J.H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer New York, 2009.
- [14] A. Sutherland. Isogeny volcanoes. *The Open Book Series*, 1(1):507–530, November 2013.
- [15] A.V. Sutherland. Identifying supersingular elliptic curves. *LMS Journal of Computation and Mathematics*, 15:317–325, September 2012.
- [16] J. Tate. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*, 2:134–144, 1966.
- [17] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.2)*, 2022. <https://www.sagemath.org>.
- [18] J. Vêlu. Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris Sér. A-B*, 273:A238–A241, 1971.
- [19] W.C. Waterhouse. Abelian varieties over finite fields. *Annales scientifiques de l'École normale supérieure*, 2(4):521–560, 1969.
- [20] Y. Yamamoto. On unramified Galois extensions of quadratic number fields. *Osaka Math. J.*, 7:57–76, 1970.

HENRY BAMBURY. ECOLE POLYTECHNIQUE, INSTITUT POLYTECHNIQUE DE PARIS, PALAISEAU, FRANCE.
Email address: `henry.bambury@polytechnique.edu`

FRANCESCO CAMPAGNA. MAX-PLANCK-INSTITUT FÜR MATEMATIK, VIVATSGASSE 7, 53111 BONN, GERMANY.
Email address: `campagna@mpim-bonn.mpg.de`

FABIEN PAZUKI. UNIVERSITY OF COPENHAGEN, INSTITUTE OF MATHEMATICS, UNIVERSITETSPARKEN 5, 2100 COPENHAGEN, DENMARK, AND UNIVERSITÉ DE BORDEAUX, IMB, 351, COURS DE LA LIBÉRATION, 33400 TALENCE, FRANCE.

Email address: `fpazuki@math.ku.dk`