J. Cullinan, N. Kaplan *Res. Number Theory(2023)9:57*
https://doi.org/10.1007/s40993-023-00456-8

Research in Number Theory

RESEARCH

The probability of non-isomorphic group structures of isogenous elliptic curves in finite field extensions, I

John Cullinan[1*] and Nathan Kaplan[2]

*Correspondence:
cullinan@bard.edu
|http://faculty.bard.edu/cullinan/
[1]Department of Mathematics,
Bard College,
Annandale-On-Hudson, NY
12504, USA
Full list of author information is
available at the end of the article

Abstract

Let ℓ be a prime number and let E and E' be ℓ-isogenous elliptic curves defined over a finite field k of characteristic $p \neq \ell$. Suppose the groups $E(k)$ and $E'(k)$ are isomorphic, but $E(K) \not\simeq E'(K)$, where K is an ℓ-power extension of k. In a previous work we have shown that, under mild rationality hypotheses, the case of interest is when $\ell = 2$ and K is the unique quadratic extension of k. In this paper we study the likelihood of such an occurrence by fixing a pair of 2-isogenous elliptic curves E, E' over $\mathbf{Q}$ and asking for the proportion of primes p for which $E(\mathbf{F}_p) \simeq E'(\mathbf{F}_p)$ and $E(\mathbf{F}_{p^2}) \not\simeq E'(\mathbf{F}_{p^2})$.

1 Introduction

1.1 Overview

Let E and E' be elliptic curves defined over a finite field k. If E and E' are isogenous, then the groups $E(k)$ and $E'(k)$ have the same order, but might not be isomorphic. For example, if k is the field of 5 elements, and E and E' are defined by

$$E : y^2 = x^3 + x = x(x+2)(x+3)$$
$$E' : y^2 = x^3 + x + 2 = (x+1)(x^2 + 4x + 2),$$

then E and E' are isogenous with $E(k) \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ and $E'(k) \simeq \mathbf{Z}/4\mathbf{Z}$. Looking ahead to future calculations, we note that the kernel of the 2-isogeny $E \to E'$ is $\{\infty, (-2, 0)\}$ and by [20, III.4.12], a Galois-stable subgroup of an elliptic curve uniquely determines an isogenous curve.

Returning to our setup, we can ask if $E(k) \simeq E'(k)$ implies that $E(K) \simeq E'(K)$, as K ranges over finite extensions of k. It is similarly easy to see that the answer is no:

Example 1.1.1 Let k be the field of 17 elements and K the field of 17^2 elements. Let

$$E : y^2 = x(x+6)(x+12)$$
$$E' : y^2 = (x+1)(x+4)(x-4).$$

Observe that $E' = E/\langle(0,0)\rangle$, so E and E' are 2-isogenous. One can check that

$$E(k) \simeq E'(k) \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/10\mathbf{Z},$$

but $E(K) = \mathbf{Z}/8\mathbf{Z} \times \mathbf{Z}/40\mathbf{Z}$ and $E'(K) = \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/80\mathbf{Z}$.

It is even possible to come up with examples where $E(K) \simeq E'(K)$ for all finite extensions K/k, but E and E' are not isomorphic as curves. However, extreme examples such as these, and routine ones like 1.1.1, only happen under very specific circumstances. In fact, Example 1.1.1 can be viewed as a "worst case scenario" in the sense that, under mild rationality conditions, it is only in the context of rational 2-isogenies and quadratic extensions that we can have $E(k) \simeq E'(k)$ and $E(K) \not\simeq E'(K)$. We will explain these rationality assumptions in detail below. In this paper we aim to understand *how often* examples such as 1.1.1 occur.

1.2 Reduction to 2-isogenies

Throughout this paper we consider the simplest case where E and E' are related by an isogeny of prime degree ℓ, coprime to the characteristic of k. If we additionally assume that $E(k)$ and $E'(k)$ have order divisible by ℓ and the kernel of the isogeny $E \to E'$ is generated by a rational point of order ℓ, then we recall the main theorem of [6]:

Theorem 1.2.1 (Theorem 1 of [6])
Let k be a finite field of odd characteristic p, $\ell \neq p$ an odd prime, and E and E' ordinary elliptic curves over k. Suppose E and E'

- *each have a point of order ℓ defined over k, and*
- *are ℓ-isogenous with kernel generated by a point defined over k.*

Then $E(k) \simeq E'(k)$ if and only if $E(K) \simeq E'(K)$ for all finite extensions K/k.

Concretely, *when ℓ is odd*, if E and E' are ℓ-isogenous and each has a non-trivial point of order ℓ defined over k, then $E(k) \simeq E'(k)$ implies $E(K) \simeq E'(K)$ in all finite extensions K/k.

Because it is known how the ℓ-part of the groups of rational points grow in towers [9], we can take from this theorem that the group structure of $E(k)$ completely determines the group structure of all ℓ-isogenous curves to E, in all finite extensions K/k, under the hypothesis that the isogeny is generated by a k-rational point of order ℓ. (In case the isogeny has degree ℓ, but the groups $E(k)$ and $E'(k)$ have order coprime to ℓ, then one must perform an initial base-field extension to (say) L to obtain a point of order ℓ. Then we can apply Theorem 1.2.1 taking L as the base field.)

Example 1.1.1 shows that Theorem 1.2.1 cannot be true when $\ell = 2$. But it also exemplifies the only way for Theorem 1.2.1 to fail. More precisely, in [7] the first author proved the following theorem, showing exactly under which circumstances the groups of rational points of 2-isogenous curves fail to be isomorphic in towers:

Theorem 1.2.2 (Theorem 2 of [7]) *Let E and E' be ordinary, 2-isogenous elliptic curves defined over a finite field k. Suppose $E(k) \simeq E'(k)$. Let the endomorphism ring of each curve be an order in the quadratic imaginary ring $\mathbf{Z}[\omega]$ and write $\pi = a + b\omega \in \mathbf{Z}[\omega]$, where a is odd and b is even, for the Frobenius endomorphism. Then $E(K) \simeq E'(K)$ for all finite*

extensions K/k unless the following holds:

$$v_2(a-1) = 1 \text{ and } v_2(a+1) > v_2(b) - s_2.$$

In that case, $E(K) \simeq E'(K)$ for odd-degree extensions K/k only.

Remark 1.2.3 In the published version of [7, Theorem 2] there is a typographical error in the statement of the theorem. There is an extra "+1" in the inequality for $v_2(a+1)$. The corrected statement is listed above.

In the theorem, s_2 is a positive integer related to the conductors of the endomorphism rings of E and E'. The upshot of this result is that there are precisely two possibilities. Either

(1) $E(K) \simeq E'(K)$ for all finite extensions K/k, or
(2) we can detect that $E(K) \not\simeq E'(K)$ in the unique quadratic extension K/k. Moreover, we can detect this failure by performing computations *exclusively over* k.

We will review all of this background in detail in later sections of the paper.

1.3 Setup and statement of the main results

Granting this background, we now set our notation and aims for the paper. Let E and E' be 2-isogenous elliptic curves defined over a field k such that the isogeny is also defined over k. We call such a pair (E, E') **rationally 2-isogenous**. In this paper we focus exclusively on the cases $k = \mathbf{F}_p$ and $k = \mathbf{Q}$.

Fix an odd prime p. If E and E' are rationally 2-isogenous over $\mathbf{F}_p$, then $E(\mathbf{F}_p)$ has a point P of order 2 and

$$E' = E/\langle P \rangle.$$

We say that the pair (E, E') is an **anomalous pair** if E and E' are rationally 2-isogenous over $\mathbf{F}_p$, $E(\mathbf{F}_p) \simeq E'(\mathbf{F}_p)$, and $E(\mathbf{F}_{p^2}) \not\simeq E'(\mathbf{F}_{p^2})$. As explained above, this is precisely the obstruction for rationally 2-isogenous curves having isomorphic group structures in towers over $\mathbf{F}_p$.

Here is the point of view we take for the paper. Fix a pair of rationally 2-isogenous curves (E, E') over $\mathbf{Q}$. To streamline notation, we will also use E and E' to denote the reductions modulo p of the curves over $\mathbf{Q}$. We call a prime p of good reduction **anomalous** for (E, E') if $E(\mathbf{F}_p) \simeq E'(\mathbf{F}_p)$ and $E(\mathbf{F}_{p^2}) \not\simeq E'(\mathbf{F}_{p^2})$. Therefore, at an anomalous prime for the pair (E, E') defined over $\mathbf{Q}$, we have that (E, E') is an anomalous pair. Depending on whether p or E is fixed, the two usages of "anomalous" should not be in conflict.

Given this setup, we seek to understand the ratio

$$\mathcal{P}(X) = \frac{\#\{\text{anomalous } p \le X\}}{\pi(X)}, \tag{1.3.1}$$

where $\pi(X)$ is the prime counting function, and also the limit $\mathcal{P} = \lim_{X\to\infty} \mathcal{P}(X)$, if it exists. We note that $\mathcal{P}(X)$ and $\mathcal{P}$ depend on both E and E' (more specifically, they depend on the images of the 2-adic representations over $\mathbf{Q}$ for each curve). In this paper we only make one computation explicit: the case where the 2-adic images are isomorphic and as large as possible given the constraints of the setup. The following examples show that there exist pairs (E, E') for which anomalous primes exist, and there exist pairs for which

they do not. Throughout this paper when we refer to a proportion of primes with some property, or the probability that a prime has some property, we mean it in this sense of counting primes up to X and taking a limit.

Example 1.3.2 Let E be the elliptic curve `210.e5` and E' the curve `210.e4` of the `LMFDB` [22]. Then E and E' are 2-isogenous, with $\mathbf{Q}$-torsion subgroups $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z}$ and $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$, respectively. There are no anomalous primes for these curves, a consequence (as we will see below) of the sizes of $E(\mathbf{Q})_{\text{tors}}$ and $E'(\mathbf{Q})_{\text{tors}}$.

Example 1.3.3 The isogeny class `10608.y` consists of two elliptic curves, E and E', such that

$$E(\mathbf{Q}) \simeq E'(\mathbf{Q}) \simeq \mathbf{Z}/2\mathbf{Z};$$

these are the smallest Mordell-Weil groups possible given that E and E' are rationally 2-isogenous. Moreover, the mod 2 representation of each curve has order 2, and the 2-adic representation of each has index 3 in $\mathrm{GL}_2(\mathbf{Z}_2)$, i.e., is as large as possible given the hypotheses on each curve. We consider all primes up to some bound and count those that are anomalous:

total $\#p$	$\#p \mid E(\mathbf{F}_p) \not\simeq E'(\mathbf{F}_p)$	$\#p \mid E(\mathbf{F}_p) \simeq E'(\mathbf{F}_p)$	#anomalous
1000	539	457	30
10000	5324	4672	335

Converting the number of good primes to a value of X, we see that

$$\mathcal{P}(7919) = \frac{30}{1000} = 0.03, \text{ and}$$
$$\mathcal{P}(104741) = \frac{335}{10000} = 0.0335,$$

suggesting that the limit might exist.

The main result of this paper is that the limit does exist and can be computed using the image of the 2-adic representations attached to E and E'. In general, a pair of rationally 2-isogenous elliptic curves define adjacent vertices on an isogeny-torsion graph over $\mathbf{Q}$. In [4,5], the authors give a classification of all isogeny-torsion graphs over $\mathbf{Q}$. Moreover, the classification of Rouse and Zureick-Brown [19] of the possible images of the 2-adic representation of elliptic curves over $\mathbf{Q}$ presents us with a finite list of graphs and images to consider for E and E'.

In a forthcoming paper [8] we work out, among other things, the possible values that can occur for elliptic curves over $\mathbf{Q}$. In this paper, we consider only one case and prove the following theorem.

Theorem 1.3.4 *Let E and E' be rationally 2-isogenous elliptic curves over $\mathbf{Q}$ such that $[\mathrm{GL}_2(\mathbf{Z}_2) : \mathrm{im}\, \rho_{E,2}] = 3$, i.e., both curves have maximal 2-adic image given that each has a rational 2-torsion point. Then $\mathcal{P} = 1/30$.*

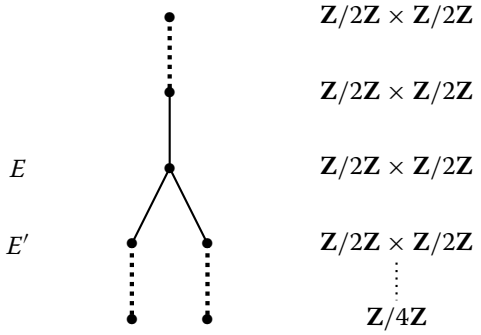
Remark 1.3.5 The elliptic curves of Theorem 1.3.4 are parameterized by the curve X_6 of the `RZB` database, and the group that generates X_6 has label `2.3.0.1` in the `LMFDB` database.

Remark 1.3.6 See Sect. 7 for a discussion of the non-maximal cases and setup to be addressed in [8].

In order to get the result that $\mathcal{P} = 1/30$, we make full use of the structure of the **2-isogeny volcano** V_p of E at p. The 2-isogeny volcano is a graph, the connected components of which consist of vertices (elliptic curves over $\mathbf{F}_p$) and edges ($\mathbf{F}_p$-rational 2-isogenies), that organizes the curves into levels (we reserve the term *height* for the entire volcano and review our conventions in later sections). All curves at the same level have isomorphic endomorphism rings, which implies that all curves at the same level have isomorphic group structures over $\mathbf{F}_p$.

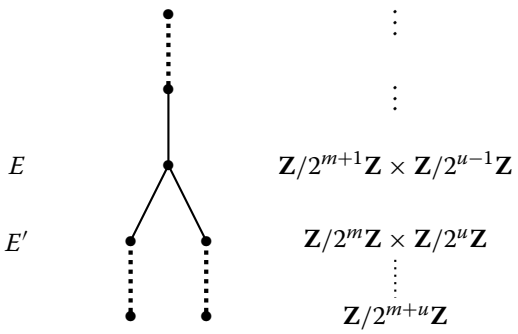
A 2-isogeny $E \to E'$ defined over $\mathbf{F}_p$ can be **vertical** ($[\mathrm{End}(E) : \mathrm{End}(E')] = 2$ or $1/2$) or **horizontal** ($\mathrm{End}(E) \simeq \mathrm{End}(E')$); horizontal isogenies necessarily preserve the group structure over $\mathbf{F}_p$, while vertical isogenies may or may not. At an anomalous prime p, we have the following confluence of events:

- the $\mathbf{Q}$-isogeny $E \to E'$ reduces to a vertical isogeny over $\mathbf{F}_p$, and
- $E(\mathbf{F}_p)[2^\infty] \simeq E'(\mathbf{F}_p)[2^\infty] \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ so that the volcano V_p has the rough structure



where either E or E' lies at least two levels above the floor, and

- $E(\mathbf{F}_{p^2})[2^\infty] \not\simeq E'(\mathbf{F}_{p^2})[2^\infty]$ and E and E' are situated on V_{p^2} as follows



We interpret the value $\mathcal{P} = 1/30$ as the sum of a geometric series, where the summands reflect the group theory of $\mathrm{im}\,\rho_{E,2}$ and $\mathrm{im}\,\rho_{E',2}$. In particular, we filter the anomalous primes by **defect** (which we explain in detail in the sections below). Briefly, an anomalous prime has defect (a, b) if $E(\mathbf{F}_{p^2})$ has full 2^a-torsion but not full 2^{a+1}-torsion and $E'(\mathbf{F}_{p^2})$ has full 2^b-torsion, but not full 2^{b+1}-torsion. It is a fact about adjacent vertices on an isogeny

volcano that a prime can only have defect $(m+1, m)$ or $(m, m+1)$. (This is exemplified in the figure above.) Filtering by defect, and weighting each defect by the size of the kernels of the homomorphisms $\operatorname{im} \overline{\rho}_{E,2^{m+1}} \to \operatorname{im} \overline{\rho}_{E,2^m}$ and $\operatorname{im} \overline{\rho}_{E',2^{m+1}} \to \operatorname{im} \overline{\rho}_{E',2^m}$, we obtain the summands in the geometric series.

To ease the cumbersome notation, we let $G = \operatorname{im} \rho_{E,2}$ and $G' = \operatorname{im} \rho_{E',2}$. Recall that if E and E' are isogenous elliptic curves without CM, then the indexes $[\mathrm{GL}_2(\mathbf{Z}) : G]$ and $[\mathrm{GL}_2(\mathbf{Z}_2) : G']$ are equal [11, Prop. 2.2.1]. If p is a good prime, let $F \in G$ and $F' \in G'$ denote representatives of the class of Frobenius. Note that even though as a quadratic irrational number, the Frobenius endomorphism $\pi = a + b\omega$ is represented in $\mathrm{End}(E)$ and $\mathrm{End}(E')$ by the same integral expression, the interpretation in each ring is different when those rings are not isomorphic. Given all of this, we prove the following finer version of Theorem 1.3.4.

Theorem 1.3.7 *Let E and E' be rationally 2-isogenous elliptic curves over $\mathbf{Q}$ such that $[\mathrm{GL}_2(\mathbf{Z}_2) : G] = 3$. Let p be a prime such that $F \equiv -I \pmod{2^m}$ but $F \not\equiv -I \pmod{2^{m+1}}$. Then with probability 1/2, $F' \equiv -I \pmod{2^m}$ and p is not anomalous, and with probability 1/2, $F' \equiv -I \pmod{2^{m-1}}$ and $F' \not\equiv -I \pmod{2^m}$ and p is anomalous of defect $(m+1, m)$. Furthermore, this characterizes all anomalous primes of defect $(m+1, m)$.*

Remark 1.3.8 A similar result holds for primes of defect $(m, m+1)$.

This brings us to the final portion of the paper where we re-interpret our results on anomalous primes and their defects in terms of a probabilistic model of the distribution of heights of volcanoes and the discriminants of the endomorphism rings at each level.

1.4 Organization of the paper

In the next section we review background on elliptic curves over finite fields, in particular the relationship between the endomorphism ring and rational points. We also recall the relevant history of this problem as well as the results in [6,7] that are applicable in this context.

As a rough guide to the results, the main point of Sect. 3 is to determine the structure of the 2-Sylow subgroup of $E(\mathbf{F}_p)$ and $E'(\mathbf{F}_p)$ at anomalous primes. This leads to the notion of the defect of an anomalous prime.

In Sect. 5 we prove Theorem 1.3.4 by filtering the anomalous primes by defect, determining the exact proportion of each defect, and then summing over all defects. We determine the exact proportion of each defect by re-interpreting the criteria of Sect. 3 for a prime to be anomalous in terms of matrix conditions in the 2-adic representations attached to E and E'. Following this, we interpret the defect of an anomalous prime as determining where on the isogeny volcano of the pair (E, E') lies and give numerical data suggesting a finer relationship between anomalous primes and endomorphism rings.

Section 7 is dedicated to future work. In particular, we contextualize the results of the present paper within the goals of a follow-up paper in which we explore the range of values of $\mathcal{P}$ that can occur for elliptic curves over $\mathbf{Q}$.

1.5 Databases

We use two online databases in this work: the L-Functions and Modular Forms Database (LMFDB), and the classification of 2-adic images of Galois representations attached to

elliptic curves over $\mathbf{Q}$, due to Rouse and Zureick-Brown (RZB), based on the paper [19]. Whenever we use an entry in the database, such as an isogeny class or elliptic curve in the LMFDB, or a modular curve in the RZB database, we link to that entry in the database.

1.6 Notation

We will explain any specialized notation in main body of the paper, but we remind the reader of some standard conventions. If k is a field and k^s a separable closure of k, then we write Gal_k for the Galois group of k^s/k. If E is an elliptic curve over k and ℓ is a prime number, then we write $T_\ell E$ for the ℓ-adic Tate module of E and

$$\rho_{E,\ell} : \mathrm{Gal}_k \to \mathrm{Aut}(T_\ell E), \text{ and}$$
$$\overline{\rho}_{E,\ell^n} : \mathrm{Gal}_k \to \mathrm{Aut}(T_\ell E \otimes \mathbf{Z}/\ell^n\mathbf{Z})$$

for the ℓ-adic and mod ℓ^n representations of E, respectively. If $G \subseteq \mathrm{GL}_2(\mathbf{Z}_2)$ is the image of the ℓ-adic representation, then we write $G(\ell^n) \subseteq \mathrm{GL}_2(\mathbf{Z}/\ell^n\mathbf{Z})$ for its reduction modulo ℓ^n.

If R is a ring, then we write $M_n(R)$ for the ring of $n \times n$ matrices with entries in R. Finally, if p is a prime number, then we write $v_p : \mathbf{Q}^\times \to \mathbf{Z}$ for the p-adic valuation.

2 Elliptic curves over finite fields

2.1 Endomorphism rings and rational points

Let q be a power of an odd prime p and let E be an ordinary elliptic curve defined over $\mathbf{F}_q$; we will address supersingular curves in Sect. 2.3. Since E is ordinary, its endomorphism ring $\mathrm{End}(E)$ is isomorphic to an order $\mathcal{O}$ in an imaginary quadratic field $K = \mathbf{Q}(\sqrt{D})$ for a squarefree negative integer D, and all endomorphisms of E are defined over $\mathbf{F}_q$.

Let $\mathcal{O}_K$ denote the ring of integers of K. Write d_K for the discriminant of $\mathcal{O}_K$, the maximal order of K. Then

$$d_K = \begin{cases} D & \text{if } D \equiv 1 \pmod 4 \\ 4D & \text{if } D \equiv 2, 3 \pmod 4. \end{cases}$$

Recall that if g is a positive integer, then we denote by $\mathcal{O}_g := \mathbf{Z} \oplus \mathbf{Z}g\omega$ the order of conductor g in $\mathcal{O}_K$, where

$$\omega = \begin{cases} (1+\sqrt{D})/2 & \text{if } D \equiv 1 \pmod 4 \\ \sqrt{D} & \text{if } D \equiv 2, 3 \pmod 4. \end{cases}$$

We may therefore write $\mathbf{Z}[\pi] = \mathcal{O}_f$ for some positive integer f, and $\mathcal{O}_K = \mathcal{O}_1$. Since $\mathrm{End}(E) = \mathcal{O}$ contains $\mathbf{Z}[\pi]$, we may write $\mathcal{O} = \mathcal{O}_g$ for some $g \mid f$ with

$$\mathcal{O}_f \subseteq \mathcal{O}_g \subseteq \mathcal{O}_1.$$

If Δ_g denotes the discriminant of $\mathcal{O}_g$, then $\Delta_g = g^2 d_K$.

Identifying $\mathrm{End}(E)$ with an order in $\mathcal{O}_K$, we may write the Frobenius endomorphism $\pi \in \mathrm{End}(E)$ explicitly as an element of $\mathcal{O}_K$. We now review how to do this. Recall the well-known formulas relating the cardinality of $E(\mathbf{F}_q)$, the fundamental discriminant of K, and the trace t of π:

$$\#E(\mathbf{F}_q) = 1 + q - t \tag{2.1.1}$$
$$4q = t^2 - \beta^2 \Delta_g, \tag{2.1.2}$$

where t is the trace of Frobenius, β is a positive integer, and $\Delta_g = g^2 d_K$, as above.

Then π has a unique integral representation $\pi = a + b\omega \in \mathbf{Z}[\omega]$ given by

$$a = \begin{cases} (t - \beta g)/2 & \text{if } D \equiv 1 \pmod 4 \\ t/2 & \text{if } D \equiv 2, 3 \pmod 4, \end{cases}$$
$$b = \beta g.$$

We also recall a fundamental result of Lenstra [15], which gives the structure of $E(\mathbf{F}_{q^m})$ for all positive integers m:

$$E(\mathbf{F}_{q^m}) \simeq \frac{\mathcal{O}}{(\pi^m - 1)}. \tag{2.1.3}$$

2.2 Isogenies

Keeping with the notation above, suppose that E and E' are isogenous (ordinary) elliptic curves defined over $\mathbf{F}_q$. Then the groups $E(\mathbf{F}_q)$ and $E'(\mathbf{F}_q)$ have the same cardinality, as do the groups $E(\mathbf{F}_{q^m})$ and $E'(\mathbf{F}_{q^m})$, for all positive integers m.

Let $\ell \neq p$ be a prime number. If E and E' have endomorphism rings $\mathcal{O}$ and $\mathcal{O}'$, respectively, and are ℓ-isogenous, then by a result of Kohel [14, Prop. 21] we have

$$[\mathcal{O} : \mathcal{O}'] = \ell, \ell^{-1}, \text{ or } 1.$$

In the first two cases, the isogeny is called *vertical* (ascending/descending, depending on the inclusion) and in the latter it is *horizontal*.

Isogenous elliptic curves have the same trace of Frobenius. In the case of a vertical isogeny, $\mathcal{O}$ and $\mathcal{O}'$ are orders in $\mathcal{O}_K$ of relative index ℓ. We explain what happens when $\mathcal{O}' \subseteq \mathcal{O}$. (There is a completely analogous setup when $\mathcal{O} \subseteq \mathcal{O}'$.) There exist divisors g and g' of f such that $g'/g = \ell$ and $\mathcal{O} = \mathcal{O}_g$, $\mathcal{O}' = \mathcal{O}_{g'}$ with

$$\mathbf{Z}[\pi] = \mathcal{O}_f \subseteq \mathcal{O}_{g'} \subseteq \mathcal{O}_g \subseteq \mathcal{O}_1 = \mathcal{O}_K.$$

Turning to the group structures of isogenous curves, we recall that the main results of [12,23] give criteria for any pair of isogenous elliptic curves to have isomorphic groups of $\mathbf{F}_{q^m}$-rational points in terms of the prime divisors of the integral components of π^m. We now recall some of the special notation introduced in [12] that we will adopt throughout the rest of this paper.

Define a finite set of prime numbers $\mathbf{P}$ as follows, incorporating the notation above:

$$\mathbf{P} = \{p \text{ prime} \mid v_p(g) \neq v_p(g')\}.$$

For each $p \in \mathbf{P}$ we set

$$s_p = \max\{v_p(g), v_p(g')\},$$

whence $s_p \geq 1$. With this notation in place, write

$$\pi^m = a_m + b_m\omega,$$

for integers a_m, b_m. Finally, we recall the criterion of [12, Thm. 2.4] for $E(\mathbf{F}_{q^m})$ and $E'(\mathbf{F}_{q^m})$ to be isomorphic:

$$E(\mathbf{F}_{q^m}) \simeq E'(\mathbf{F}_{q^m}) \iff v_p(a_m - 1) \leq v_p(b_m) - s_p, \tag{2.2.1}$$

for all $p \in \mathbf{P}$.

Now we specialize to the situation that is the primary focus of this paper. When the degree of the vertical isogeny $E \to E'$ is a prime number ℓ, then $g'/g = \ell^{\pm 1}$ and so $\mathbf{P} = \{\ell\}$. For descending isogenies we have $v_\ell(g') = 1 + v_\ell(g)$ and for ascending isogenies we have $v_\ell(g) = 1 + v_\ell(g')$. Specializing further, we set $\ell = 2$ for the remainder of the paper. In [7, Thm. 2] the first author proved that if $E(\mathbf{F}_q) \simeq E'(\mathbf{F}_q)$ and $E(\mathbf{F}_{q^2}) \simeq E'(\mathbf{F}_{q^2})$, then $E(\mathbf{F}_{q^m}) \simeq E(\mathbf{F}_{q^m})$ for all positive integers m. Theorem 1.2.2 gives the precise conditions under which the second isomorphism fails, given the first.

2.3 Supersingular curves

In the case where E and E' are supersingular curves over $\mathbf{F}_p$ the situation is (perhaps surprisingly) much simpler. We recall the following result of Wittmann.

Theorem 2.3.1 (Theorem 4.1 of [23]) *Let $E/\mathbf{F}_p$ be a supersingular elliptic curve. Then*

$$E(\mathbf{F}_{p^{2k}}) \simeq \mathbf{Z}/((-p)^k - 1)\mathbf{Z} \times \mathbf{Z}/((-p)^k - 1)\mathbf{Z}.$$

Further:

- *If $p \not\equiv 3 \pmod 4$ or $p \equiv 3 \pmod 4$ and $E[2] \not\subseteq E(\mathbf{F}_p)$ we have*

$$E(\mathbf{F}_{p^{2k+1}}) \simeq \mathbf{Z}/(p^{2k+1} + 1)\mathbf{Z} \text{ and } \mathrm{End}_{\mathbf{F}_p}(E) \simeq \mathbf{Z}[\sqrt{-p}].$$

- *If $p \equiv 3 \pmod 4$ and $E[2] \subseteq E(\mathbf{F}_p)$ we have*

$$E(\mathbf{F}_{p^{2k+1}}) \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/\left(\frac{p^{2k+1}+1}{2}\right)\mathbf{Z} \text{ and } \mathrm{End}_{\mathbf{F}_p}(E) \simeq \mathbf{Z}[(1+\sqrt{-p})/2].$$

In [7] we observed that this immediately implies that when E and E' are supersingular, then the group structure over $\mathbf{F}_p$ completely determines the group structure over any finite extension:

Corollary 2.3.2 (Corollary 1 of [7]) *Let p be a prime. Let E_1 and E_2 be supersingular, isogenous elliptic curves defined over $\mathbf{F}_p$. Suppose $E_1(\mathbf{F}_p) \simeq E_2(\mathbf{F}_p)$. Then $E_1(K) \simeq E_2(K)$ for every finite extension $K/\mathbf{F}_p$.*

3 General properties of anomalous primes and curves

We retain the notation and setup of the previous sections, in particular we assume E and E' are ordinary. We start with a general property of anomalous pairs.

Proposition 3.0.1 *Let (E, E') be an anomalous pair of elliptic curves defined over the finite field $\mathbf{F}_p$. Then $p \equiv 1 \pmod 4$.*

Proof Suppose $p \equiv 3 \pmod 4$. We distinguish between the cases where $|E(\mathbf{F}_p)| \equiv 2 \pmod 4$ versus $|E(\mathbf{F}_p)| \equiv 0 \pmod 4$. Recall that if (E, E') is an anomalous pair then in the representation $\pi = a + b\omega$ of Frobenius as an element of $\mathcal{O}_K$, we have that b is even; write $b = 2b'$.

If $|E(\mathbf{F}_p)| \equiv 0 \pmod 4$, then $t \equiv 0 \pmod 4$; write $t = 4t'$. By (2.1.2),

$$4p = t^2 - b^2 d_K = 16(t')^2 - 4(b')^2 d_K,$$

so we must have $p = 4(t')^2 - (b')^2 d_K$. Thus b' and d_K are odd. In particular, $v_2(b) = 1$. But since (E, E') is an anomalous pair, we have by Theorem 1.2.2

$$v_2(a-1) = 1 \leq v_2(b) - s_2 = 1 - s_2,$$

whence $s_2 = 0$. But this means $\mathrm{End}(E) \simeq \mathrm{End}(E')$, contradicting the fact that (E, E') are an anomalous pair.

If $|E(\mathbf{F}_p)| \equiv 2 \pmod 4$, then $t \equiv 2 \pmod 4$ by (2.1.1), so write $t = 2t'$ with t' odd. But then

$$p = (t')^2 - (b')^2 d_K.$$

Since $p \equiv 3 \pmod 4$ and $(t')^2 \equiv 1 \pmod 4$, we must have $(b')^2 d_K \equiv 2 \pmod 4$. But since b' is odd and $d_K \equiv 0$ or $1 \pmod 4$, this is impossible. We conclude that if $p \equiv 3 \pmod 4$ then p cannot be anomalous. □

Lemma 3.0.2 *If* $|E(\mathbf{F}_p)| \equiv 2 \pmod 4$ *then* $E(\mathbf{F}_p) \simeq E'(\mathbf{F}_p)$.

Proof Since E and E' are 2-isogenous, the prime-to-2 parts of $E(\mathbf{F}_p)$ and $E'(\mathbf{F}_p)$ are isomorphic [6, Cor. 3]. Since each has a single point of order 2, the result follows by the structure theorem for finite abelian groups. □

Theorem 3.0.3 *If* $|E(\mathbf{F}_p)| \equiv 2 \pmod 4$ *then* $E(\mathbf{F}_{p^2}) \simeq E'(\mathbf{F}_{p^2})$.

Proof If $|E(\mathbf{F}_p)| \equiv 2 \pmod 4$ then by Lemma 3.0.2 we have $E(\mathbf{F}_p) \simeq E'(\mathbf{F}_p)$. If, in addition, $E(\mathbf{F}_{p^2}) \not\simeq E'(\mathbf{F}_{p^2})$, then (E, E') is anomalous whence $p \equiv 1 \pmod 4$. Writing $\pi = a + b\omega$ in the notation of Section 2, we have

1. $v_2(a-1) = 1 \leq v_2(b) - s_2$, and
2. $v_2(a+1) > v_2(b) - s_2$.

Since $v_2(a-1) = 1$, we have $a \equiv 3 \pmod 4$. We also have

$$|E(\mathbf{F}_p)| = 1 + p - t \equiv 2 \pmod 4, \tag{3.0.4}$$

hence $t \equiv 0 \pmod 4$. Now we divide the argument into two cases based on $D \pmod 4$, where D is the squarefree integer for which $K = \mathbf{Q}(\sqrt{D})$ is the endomorphism algebra of E (and E').

If $D \equiv 2, 3 \pmod 4$, then $a = t/2$ and so $t \equiv 6 \pmod 8$, a contradiction. If $D \equiv 1 \pmod 4$, then we first recall the inequality (1). Since (E, E') is an anomalous pair, we must have $s_2 \geq 1$ (otherwise, $\mathrm{End}(E) \simeq \mathrm{End}(E')$), and so we conclude that $v_2(b) \geq 2$. But when $D \equiv 1 \pmod 4$, we have $a = (t-b)/2$. Since both t and b must be divisible by 4, we get that a is even. This contradicts $a \equiv 3 \pmod 4$, established above. □

Corollary 3.0.5 *If* $|E(\mathbf{F}_p)| \equiv 2 \pmod 4$ *then* $E(\mathbf{F}_{p^m}) \simeq E'(\mathbf{F}_{p^m})$ *for all positive integers* m.

Proof This follows from [7, Thm. 2]: if $E(\mathbf{F}_{p^m}) \simeq E'(\mathbf{F}_{p^m})$ for $m \in \{1, 2\}$, then $E(\mathbf{F}_{p^m}) \simeq E'(\mathbf{F}_{p^m})$ for all positive integers m. □

Remark 3.0.6 It follows that *every* pair of curves E, E' over $\mathbf{F}_p$ with $|E(\mathbf{F}_p)| \equiv 2 \pmod 4$ and that are rationally 2-isogenous have isomorphic Mordell-Weil groups in all finite extensions. Therefore, any anomalous pair must have $|E(\mathbf{F}_p)| \equiv 0 \pmod 4$ and $p \equiv 1 \pmod 4$.

Next, we define a finer notion of (E, E') being an anomalous pair. This will carry over to a refined notion of p being an anomalous prime, which will be an important topic in the following sections. Because the 2-Sylow subgroups of $E(\mathbf{F}_{p^2})$ and $E'(\mathbf{F}_{p^2})$ have the same size, but are not isomorphic, we can ask how they differ. We describe this difference using the notion of defect.

Definition 3.0.7 Let $E \to E'$ be rationally 2-isogenous elliptic curves over $\mathbf{Q}$ and let p be an anomalous prime. If

$$a = \max\{i \in \mathbf{N} \mid E(\mathbf{F}_{p^2})[2^\infty] \supseteq \mathbf{Z}/2^i\mathbf{Z} \times \mathbf{Z}/2^i\mathbf{Z}\}, \text{ and}$$
$$a' = \max\{i \in \mathbf{N} \mid E'(\mathbf{F}_{p^2})[2^\infty] \supseteq \mathbf{Z}/2^i\mathbf{Z} \times \mathbf{Z}/2^i\mathbf{Z}\},$$

then we say that p has **defect** (a, a').

Remark 3.0.8 It is a well-known property of the ℓ-**isogeny volcano** (which we will recall in Sect. 4) that if E and E' are ℓ-isogenous elliptic curves over a finite field k and the ℓ-Sylow subgroups of $E(k)$ and $E'(k)$ are not isomorphic, then $E(k)[\ell^\infty] \simeq \mathbf{Z}/\ell^u\mathbf{Z} \times \mathbf{Z}/\ell^v\mathbf{Z}$ and $E'(k)[\ell^\infty] \simeq \mathbf{Z}/\ell^{u-1}\mathbf{Z} \times \mathbf{Z}/\ell^{v+1}\mathbf{Z}$ or $E'(k)[\ell^\infty] \simeq \mathbf{Z}/\ell^{u+1}\mathbf{Z} \times \mathbf{Z}/\ell^{v-1}\mathbf{Z}$ for some positive integer u and nonnegative integer v. Theorem 3.0.12 establishes a similar result and relates the defect of an anomalous prime to the 2-valuation of the Frobenius endomorphism. For more details and an extensive background on the theory of isogeny volcanoes, see [21]. In the specific case $\ell = 2$, the authors of [18] show how the 2-adic valuation of the number of rational points grows in towers of finite fields.

Concerning the growth of the number of rational points in towers, we remind the reader of the growth in quadratic extensions.

Lemma 3.0.9 *Let E be an elliptic curve defined over a finite field $\mathbf{F}_q$ of odd cardinality and let t be the trace of Frobenius over $\mathbf{F}_q$. Then $|E(\mathbf{F}_{q^2})| = (1 - t + q)(1 + t + q)$.*

Proof If M is a matrix defined over a field of characteristic $\neq 2$, then the identity

$$\operatorname{tr}(M^2) = \operatorname{tr}(M)^2 - 2\det(M)$$

is directly applicable to our situation. If F represents the Frobenius endomorphism of E over $\mathbf{F}_q$, then F^2 represents the Frobenius over $\mathbf{F}_{q^2}$ and we have $\operatorname{tr}(F^2) = t^2 - 2q$, whence

$$|E(\mathbf{F}_{q^2})| = 1 - \operatorname{tr}(F^2) + q^2 = 1 - t^2 + 2q + q^2 = (1 - t + q)(1 + t + q),$$

as claimed. □

We will apply the following results in the proof of Theorem 3.0.12.

Lemma 3.0.10 *Let E be an ordinary elliptic curve defined over a finite field $\mathbf{F}_q$ of odd characteristic. Let $\pi \in \operatorname{End}(E)$ be the Frobenius endomorphism. If v is the largest integer such that $\pi^m - 1$ factors as $2^v\alpha$ in $\operatorname{End}(E)$, then $E(\mathbf{F}_{q^m})$ has full 2^v-torsion but not full 2^{v+1}-torsion.*

Proof By Lenstra's theorem (2.1.3) [15, Thm. 1(a)], we have $E(\mathbf{F}_{q^m}) \simeq \operatorname{End}(E)/(\pi^m - 1)$. If $\pi^m - 1$ factors as $2^v\alpha$, then clearly $E(\mathbf{F}_{q^m})$ has full 2^v-torsion. By factoring isogenies via [10, Thm. 25.1.2], any $\mathbf{F}_q$-rational endomorphism of E whose kernel contains the 2^{v+1}-torsion

points would have to factor as $2^{\nu+1}\beta$ in $\mathrm{End}(E)$. Thus $E(\mathbf{F}_{q^m})$ has full 2^ν-torsion but not full $2^{\nu+1}$-torsion. □

Lemma 3.0.11 *Suppose (E, E') is an anomalous pair. Then $E(\mathbf{F}_p)[2^\infty] \simeq E'(\mathbf{F}_p)[2^\infty] \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.*

Proof If (E, E') is an anomalous pair, then we must have $p \equiv 1 \pmod 4$ and $|E(\mathbf{F}_p)| \equiv 0 \pmod 4$, as previously established. If neither curve has full 2-torsion defined over $\mathbf{F}_p$, then the 2-Sylow subgroups of $E(\mathbf{F}_p)$ and $E'(\mathbf{F}_p)$ are cyclic and the curves are rationally 2-isogenous. By [1, Thm. 1.2], this is not possible. This establishes that $E(\mathbf{F}_p)[2] \simeq E'(\mathbf{F}_p)[2] \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

To see that $E(\mathbf{F}_p)[2^\infty] \simeq E'(\mathbf{F}_p)[2^\infty] \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ as well, by the paragraph following Corollary 1 in [17, p. 742] we have that if E and E' are 2-isogenous and have isomorphic group structures over $\mathbf{F}_p$, then it must be the case that $E(\mathbf{F}_p)[2^\infty] \simeq E'(\mathbf{F}_p)[2^\infty] \simeq \mathbf{Z}/2^k\mathbf{Z} \times \mathbf{Z}/2^k\mathbf{Z}$ for some k, hence $|E(\mathbf{F}_p)| = p + 1 - t \equiv 0 \pmod{2^{2k}}$. Suppose $k > 1$. Then both curves will have at least full 2^{k+1}-torsion over $\mathbf{F}_{p^2}$ (if $F \equiv I \pmod{2^k}$, then $F^2 \equiv I \pmod{2^{k+1}}$; now apply (2.1.3)), and at least one will have full 2^{k+2}-torsion (since $E(\mathbf{F}_{p^2}) \not\simeq E'(\mathbf{F}_{p^2})$). Applying Lemma 3.0.9 we have

$$|E(\mathbf{F}_{p^2})| = (p + 1 - t)(p + 1 + t) \equiv 0 \pmod{2^{2k+4}},$$

and so $p + 1 + t \equiv 0 \pmod{16}$. Since $k > 1$, we have $p + 1 - t \equiv 0 \pmod{16}$ as well, which implies that $t \equiv 0 \pmod 8$. But this contradicts the fact that for an anomalous pair we must have $t \equiv 2 \pmod 4$. This completes the proof. □

Theorem 3.0.12 *Let $E \to E'$ be 2-isogenous elliptic curves over $\mathbf{Q}$ and let p be an anomalous prime. Suppose $\mathrm{End}(E) = \mathcal{O}_g$ and $\mathrm{End}(E') = \mathcal{O}_{g'}$ are orders of conductor g and g', respectively, in the the imaginary number ring $\mathcal{O}_K = \mathbf{Z} + \mathbf{Z}\omega$; write $\pi = a + b\omega$ with $b = \beta g = \beta' g'$. Then p has defect $(m + 1, m)$ or $(m, m + 1)$ for some integer $m \geq 2$, where $m = \nu_2(\beta)$.*

Proof The isogeny $E \to E'$, initially defined over $\mathbf{Q}$, reduces modulo p to a vertical isogeny (if the reduction were horizontal then $\mathcal{O}_g = \mathcal{O}_{g'}$ and p would not be anomalous). For the remainder of the proof we assume the isogeny is descending and will conclude that p has defect $(m + 1, m)$; an identical argument for ascending isogenies would show that p has defect $(m, m + 1)$.

Write $\mathrm{End}(E) = \mathcal{O}_g = \mathbf{Z} + g\mathbf{Z}\omega$ and $\mathrm{End}(E') = \mathcal{O}_{g'} = \mathbf{Z} + g'\mathbf{Z}\omega$. We have $g' = 2g$ and also write $\pi = a + b\omega$ with $b = \beta g$ as established in Sect. 2.1. Since p is anomalous and since $\nu_2(g') = \nu_2(g) + 1$, we have

$$\nu_2(a - 1) = 1 \leq \nu_2(b) - s_2 = \nu_2(\beta) - 1 < \nu_2(a + 1).$$

Observe that $\nu_2(\beta) \geq 2$.

Now we compute

$$\pi^2 - 1 = \begin{cases} (a^2 - 1 + b^2 D) + 2ab\omega & \text{if } d_K = 4D \text{ and } D \equiv 2, 3 \pmod 4, \text{ and} \\ (a^2 - 1 + b^2\left(\frac{D-1}{4}\right)) + (2ab + b^2)\omega & \text{if } d_K = D \text{ with } D \equiv 1 \pmod 4. \end{cases}$$

In $\mathcal{O}_g$ we can factor,

$$\pi^2 - 1 = \begin{cases} (a^2 - 1 + \beta^2 g^2 D) + (2\beta)ag\omega, \text{ or} \\ (a^2 - 1 + \beta^2 g^2\left(\frac{D-1}{4}\right)) + 2\beta(a + (\beta/2))g\omega, \end{cases}$$

depending on $d_K \pmod 4$. In the first case (since a is odd) and in the second case (since a is odd and $\beta/2$ is even), $\pi^2 - 1$ is divisible in $\mathcal{O}_g$ by $2^{\nu_2(\beta)+1}$ and no higher power of 2.

Similarly, in $\mathcal{O}_{g'} = \mathcal{O}_{2g}$, $\pi^2 - 1$ is divisible by $2^{\nu_2(\beta)}$ and no higher power of 2. By Lemma 3.0.10, $E(\mathbf{F}_{p^2})$ has full $2^{\nu_2(\beta)+1}$-torsion (and no higher) and $E'(\mathbf{F}_{p^2})$ has full $2^{\nu_2(\beta)}$-torsion (and no higher). Thus p has defect $(m+1, m)$ for some integer $m = \nu_2(\beta) \geq 2$. □

In the next section we interpret anomalous primes and their defects in relation to isogeny volcanoes.

4 Isogeny volcanoes of elliptic curves

Following a brief recap of the theory of isogeny volcanoes of ordinary elliptic curves, our purpose in this section is to prove a key proposition in service of Theorems 1.3.4 and 1.3.7. We do not intend for this to be a complete treatment of the background material; we refer the reader to [21] for further details and proofs.

Let q be a power of a prime p and E an ordinary elliptic curve over $\mathbf{F}_q$. Let V_q be the connected component of the 2-isogeny graph (volcano) containing E. Then V_q is a graph whose vertices correspond to elliptic curves defined over $\mathbf{F}_q$ that are 2-power $\mathbf{F}_q$-rationally isogenous to E and edges are $\mathbf{F}_q$-rational 2-isogenies. Thus, in our setup, E and E' represent adjacent vertices on the graph V_p; note that V_p is a subgraph of V_{p^2}.

Let T be the trace of Frobenius over $\mathbf{F}_q$ and let $\mathsf{sqf}(m)$ denote the squarefee part of an integer m. Let $K = \mathbf{Q}\left(\sqrt{T^2 - 4q}\right) = \mathbf{Q}\left(\sqrt{D}\right)$ where $D = \mathsf{sqf}(T^2 - 4q)$. Then

$$\operatorname{disc} \mathcal{O}_K = \begin{cases} D & \text{if } D \equiv 1 \pmod 4, \text{ and} \\ 4D & \text{if } D \equiv 2, 3 \pmod 4. \end{cases}$$

Let $\mathcal{O}_0$ denote the endomorphism ring of an elliptic curve lying on the crater of the volcano. A theorem of Kohel [21, Theorem 7(5)] shows that for a 2-isogeny volcano $2 \nmid [\mathcal{O}_K : \mathcal{O}_0]$. The *height* of the volcano V_q is given by [21, Thm. 7]

$$h(V_q) = \frac{1}{2}\nu_2\left(\frac{T^2 - 4q}{\operatorname{disc} \mathcal{O}_0}\right) = \frac{1}{2}\nu_2\left(\frac{T^2 - 4q}{\operatorname{disc} \mathcal{O}_K}\right). \tag{4.0.1}$$

We choose the opposite labeling of the height as defined in [21] (there it is called the **depth**) and declare the floor of the volcano to have height 0. In the case that V_q consists of an isolated vertex, we set $h(V_q) = 0$. The subgraph of vertices at level $h(V_q)$ is called the **crater** of the volcano. This labeling is more convenient for interpreting the defect of an anomalous prime in terms of the location of E and E'.

The endomorphism rings of the elliptic curves at the same level of the volcano are isomorphic, hence the 2-Sylow subgroups at the same level are isomorphic. Elliptic curves on the floor of a volcano have cyclic 2-Sylow subgroups [21, §3], say of order 2^ν. Then, for each $0 < m \leq h_{\text{stab}}$, we have the 2-Sylow subgroup at height m is $\mathbf{Z}/2^m\mathbf{Z} \times \mathbf{Z}/2^{\nu-m}\mathbf{Z}$. If $h_{\text{stab}} < h(V_p)$ then the volcano is called **irregular** and h_{stab} is called the **stability level** [17, p. 742]. By [17, §4], all curves between the stability level and the crater have isomorphic 2-Sylow subgroups. We refer to the levels of the volcano between the stability level and the crater as the **stability zone**.

Lemma 4.0.2 *Let E and E' be 2-isogenous elliptic curves defined over $\mathbf{F}_p$. Let V_p be the isogeny volcano which contains E and E' as adjacent vertices; let V_{p^2} be the isogeny volcano over $\mathbf{F}_{p^2}$. Suppose $t \equiv 2 \pmod 4$. Then $h(V_{p^2}) = h(V_p) + 1$.*

Proof Let t be the trace of π_E and T the trace of π_E^2. By assumption $v_2(t) = 1$. We have $T = t^2 - 2p$ since $|E(\mathbf{F}_{p^2})| = (p + 1 - t)(p + 1 + t)$. Then

$$h(V_{p^2}) = \frac{1}{2} v_2\left(\frac{T^2 - 4p^2}{\operatorname{disc} \mathcal{O}_0}\right) = \frac{1}{2} v_2\left(\frac{(T - 2p)(T + 2p)}{\operatorname{disc} \mathcal{O}_0}\right) = \frac{1}{2} v_2\left(\frac{t^2 - 4p}{\operatorname{disc} \mathcal{O}_0}\, t^2\right) = h(V_p) + 1.$$

□

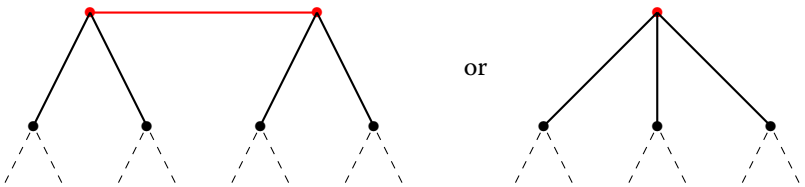
Remark 4.0.3 The hypothesis that $t \equiv 2 \pmod 4$ means that this lemma will be applicable to the case of anomalous pairs of elliptic curves.

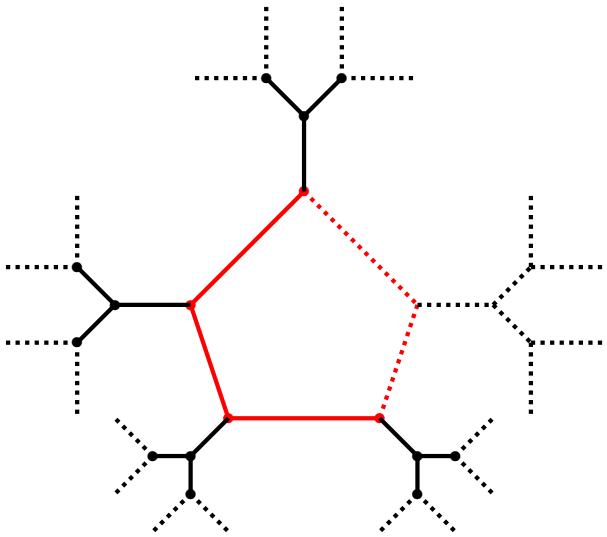
Proposition 4.0.4 *Let E and E' be 2-isogenous elliptic curves defined over a finite field $\mathbf{F}_p$ and suppose (E, E') is an anomalous pair. Then:*

- *V_p is irregular, and*
- *E and E' represent adjacent edges on V_p in the stability zone, and*
- *E and E' do not both lie in the stability zone on V_{p^2}.*

Proof This is just a matter of terminology. Since (E, E') is an anomalous pair, they are vertically isogenous. By Lemma 3.0.11, we have $E(\mathbf{F}_p)[2^\infty] \simeq E'(\mathbf{F}_p)[2^\infty] \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, hence neither curve lies on the floor of the volcano V_p. Since the 2-Sylow subgroups are isomorphic, V_p is an irregular volcano and the curves must lie in the stability zone. However, over $\mathbf{F}_{p^2}$ the 2-Sylow subgroups are not isomorphic, hence at least one curve lies outside the stability zone. □

Note that since $\operatorname{disc} \mathcal{O}_0 = \operatorname{disc} \mathcal{O}_K [\mathcal{O}_K : \mathcal{O}_0]^2$ and $[\mathcal{O}_K : \mathcal{O}_0]$ is odd, we have that $\operatorname{disc} \mathcal{O}_0 \equiv \operatorname{disc} \mathcal{O}_K \pmod 8$. Turning now to the endomorphism rings, we distinguish between the congruence classes $\operatorname{disc} \mathcal{O}_0 \equiv 0, 1, 4, 5 \pmod 8$. In these cases, the shape of the crater corresponds to the discriminant in the following way, as established by [21, Thm. 7]. When $\operatorname{disc} \mathcal{O}_0 \equiv 0 \pmod 4$ or $\operatorname{disc} \mathcal{O}_0 \equiv 5 \pmod 8$ then the volcanoes have shapes respectively (with the crater highlighted in red). If $\operatorname{disc} \mathcal{O}_0 \equiv 1 \pmod 8$ then the crater forms a cycle whose length is the order of a certain element in the class group of $\mathcal{O}_0$, as depicted in the following figure.





Remark 4.0.5 Observe that when $\operatorname{disc} \mathcal{O}_0 \equiv 5 \pmod 8$ and E is on the crater, then all 2-isogenies from E are descending.

We now discuss some aspects of the volcano V_q in terms of a matrix representation of Frobenius. We will use this material in the proof of Theorem 5.2.4. We continue with the notation from earlier in this section. If p is a prime number, then the Frobenius endomorphism at p has a representative conjugacy class in $\mathrm{GL}_2(\mathbf{Z}_2)$ via the 2-adic representation. Let $F \in \mathrm{GL}_2(\mathbf{Z}_2)$ be a matrix in this conjugacy class. For any positive integer k, we have $\det(F) \equiv q \pmod{2^k}$. We note that a unit in $\mathbf{Z}_2$ is a square in $\mathbf{Z}_2$ if and only if it is 1 modulo 8. Therefore, it still makes sense to take $\mathsf{sqf}(\alpha) \pmod 8$ for an $\alpha \in \mathbf{Z}_2$.

Suppose $F = -I + 2^m M$ where $m \geq 2$ and $M = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right) \in \mathrm{M}_2(\mathbf{Z}_2)$. This implies

$$q \equiv (-1 + 2^m x)(-1 + 2^m w) - 2^{2m} yz \equiv 1 - 2^m(x + w) - 2^{2m}(yz - xw) \pmod{2^k},$$

and

$$\begin{aligned} t^2 - 4q &\equiv (-2 + 2^m(x + w))^2 - 4\left((-1 + 2^m x)(-1 + 2^m w) - 2^{2m}(yz - xw)\right) \pmod{2^k} \\ &\equiv 2^{2m}\left((x - w)^2 + 4yz\right) \pmod{2^k}. \end{aligned}$$

Moreover,

$$\mathsf{sqf}(t^2 - 4q) \equiv \mathsf{sqf}\left((x - w)^2 + 4yz\right) \pmod 8.$$

Therefore, we have the following:

(1) $v_2(\operatorname{disc} \mathcal{O}_0)$ is determined by $\mathsf{sqf}\left((x - w)^2 + 4yz\right) \pmod 8$, and
(2) $h(V_q)$ is determined by

- $v_2\left((x - w)^2 + 4yz\right)$, and
- $\mathsf{sqf}\left((x - w)^2 + 4yz\right) \pmod 8$.

5 Elliptic curves over Q

We now turn to the proof of Theorem 1.3.4. Let E, E' be rationally 2-isogenous elliptic curves defined over $\mathbf{Q}$. Because the 2-isogeny is defined over $\mathbf{Q}$, each curve has at least a rational 2-torsion point. The exact proportion of anomalous primes is determined by the

images of the 2-adic representations of E and E', as we will see below. For the remainder of this section we will assume that both $G := \operatorname{im} \rho_{E,2}$ and $G' := \operatorname{im} \rho_{E',2}$ have index 3 in $\mathrm{GL}_2(\mathbf{Z}_2)$. Up to isomorphism, $\mathrm{GL}_2(\mathbf{Z}_2)$ has a unique subgroup of index 3.

5.1 Frobenius at anomalous primes

In this section we will describe the conjugacy class in $\mathrm{GL}_2(\mathbf{Z}_2)$ associated to Frobenius at an anomalous prime p.

If p is anomalous then both E and E' have $E(\mathbf{F}_p)[2^\infty] \simeq E'(\mathbf{F}_p)[2^\infty] \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ by Lemma 3.0.11. Write F and F' for matrix representatives of the Frobenius classes of E and E', respectively, as elements of $\mathrm{GL}_2(\mathbf{Z}_2)$. It follows that

$$F \equiv F' \equiv I \pmod 2$$

and that neither $F \pmod 4$ nor $F' \pmod 4$ fixes a cyclic subgroup of $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$ of order 4.

Since anomalous primes can be partitioned by defect as in Theorem 3.0.12, let us fix $m \geq 2$ and suppose that p has defect $(m+1, m)$. In particular, we assume that the isogeny $E \to E'$ is descending. Then we have

$$E(\mathbf{F}_{p^2})[2^\infty] \simeq \mathbf{Z}/2^a\mathbf{Z} \times \mathbf{Z}/2^{m+1}\mathbf{Z} \qquad \text{and} \qquad E'(\mathbf{F}_{p^2})[2^\infty] \simeq \mathbf{Z}/2^{a+1}\mathbf{Z} \times \mathbf{Z}/2^m\mathbf{Z},$$

where $a \geq m+1$. Therefore

$$\begin{aligned} F^2 &\equiv I \pmod{2^{m+1}} \text{ but } F^2 \not\equiv I \pmod{2^{m+2}}, \text{ and} \\ (F')^2 &\equiv I \pmod{2^m} \text{ but } (F')^2 \not\equiv I \pmod{2^{m+1}}. \end{aligned}$$

We are thus led to the problem of determining, for fixed $m \geq 2$, matrices $A \in \mathrm{GL}_2(\mathbf{Z}_2)$ such that the following are simultaneously satisfied

- $A \equiv I \pmod 2$,
- $A \pmod 4$ does not fix any cyclic subgroup of $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$ of order 4, and
- $A^2 \equiv I \pmod{2^{m+1}}$ but $A^2 \not\equiv I \pmod{2^{m+2}}$.

It is now an exercise in squaring matrices (which we omit) to conclude that there exist matrices $M, M' \in \mathrm{M}_2(\mathbf{Z}_2)$ such that neither M nor M' is $\equiv 0 \pmod 2$ and that F and F' are, up to conjugation, given by

$$\begin{aligned} F &= -I + 2^m M \\ F' &= -I + 2^{m-1} M'. \end{aligned}$$

We finish this subsection by collecting some known results on the Galois theory of torsion point fields and their consequences for anomalous primes. The important point is that if k is a number field and E/k is an elliptic curve for which $k(E[\ell^n])/k$ has Galois group $\mathrm{GL}_2(\mathbf{Z}/\ell^n\mathbf{Z})$, then the normal subgroup $\{\pm I\}$ of $\mathrm{GL}_2(\mathbf{Z}/\ell^n\mathbf{Z})$ is the Galois group of $k(E[\ell^n])/k(x(E[\ell^n]))$, with clear implications for the Frobenius at anomalous primes.

Proposition 5.1.1 *Let k be a number field and E/k an elliptic curve. Let ℓ be a prime number and $n \geq 1$ an integer. Let $k(E[\ell^n])$ be the ℓ^n-torsion field of E and $k(x(E[\ell^n]))$ the subfield generated by the x-coordinates of the points of $E[\ell^n]$. Let $G(\ell^n) = \operatorname{im} \overline{\rho}_{E,\ell^n} \subseteq \mathrm{GL}_2(\mathbf{Z}/\ell^n\mathbf{Z})$ be the image of the mod ℓ^n representation. Then $[k(E[\ell^n]) : k(x(E[\ell^n]))] \leq 2$ with $\mathrm{Gal}(k(E[\ell^n])/k(x(E[\ell^n]))) \simeq G(\ell^n) \cap \{\pm I\}$.*

Proof This is contained in [2, Chap. 5]; see especially Figs. 5.4, 5.5, 5.7. □

Lemma 5.1.2 *Let E be an elliptic curve over $\mathbf{Q}$ and suppose $p \neq 2$ is a good prime for E. Let $K_{2^n} = \mathbf{Q}(E[2^n])$ with Galois group $\mathrm{Gal}(K_{2^n}/\mathbf{Q}) \simeq G(2^n) \subseteq \mathrm{GL}_2(\mathbf{Z}/2^n\mathbf{Z})$. Suppose $\mathrm{Frob}_p \in \mathrm{Gal}(K_{2^n}/\mathbf{Q})$ is a lift of the Frobenius automorphism at p (so that the decomposition group of K_{2^n} is generated by Frob_p) and suppose that $\overline{\rho}_{E,2^n}(\mathrm{Frob}_p) = F = -I \in G(2^n)$. Then $\mathbf{F}_p(x(E[2^n])) = \mathbf{F}_p$ and $\mathbf{F}_p$ contains no y-coordinate of any 2^n-torsion point of E.*

Proof This is a matter of translating the arithmetic of elliptic curves into the Galois theory of torsion point fields and the behavior of Frobenius at unramified primes. In particular, it is the "reduction modulo p" of Proposition 5.1.1.

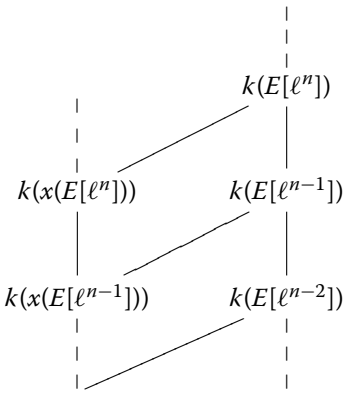
Since p is an odd prime of good reduction for E it is unramified in K_{2^n}, hence we can appeal to the explicit polynomial descriptions in [2, Table 5.1]. Let K_{2^n} be the splitting field of the polynomial $T_{2^n}(x)$ and $\mathbf{Q}(x(E[2^n]))$ the splitting field of $\Lambda_{2^n}(x)$.

In general, the field extension $K_{2^n}/\mathbf{Q}(x(E[2^n]))$ has degree 1 or 2, depending on whether $\mathbf{Q}(x(E[2^n]))$ contains any y-coordinates of any 2^n-torsion points (note that if $G(2^n) = \mathrm{GL}_2(\mathbf{Z}/2^n\mathbf{Z})$ then the extension has degree 2). We have $\mathrm{Gal}(K_{2^n}/\mathbf{Q}(x(E[2^n]))) \simeq \{\pm I\} \cap G(2^n)$ by Proposition 5.1.1, $\Lambda_{2^n}(x)$ splits completely in $\mathbf{Q}(x(E[2^n]))$, and that K_{2^n} is generated over $\mathbf{Q}(x(E[2^n]))$ by a single y-coordinate of a single 2^n-torsion point (see [2, p. 74]).

The Galois theory of number fields then says that either $T_{2^n}(x)$ splits completely over $\mathbf{Q}(x(E[2^n]))$ or factors as a product of irreducible quadratic polynomials, each of them Galois-conjugate. In either case, the Galois group $\mathrm{Gal}(K_{2^n}/\mathbf{Q}(x(E[2^n])))$ is the decomposition group at p, which is isomorphic to $\langle \mathrm{Frob}_p \rangle$. The hypothesis that $F \equiv -I \pmod{2^n}$ means that the polynomial $\Lambda_{2^n}(x)$ splits completely modulo p, hence $\mathbf{F}_p(x(E[2^n])) = \mathbf{F}_p$. The fact that Frobenius is non-trivial implies that $\mathbf{F}_p(E[2^n])$ is a quadratic extension of $\mathbf{F}_p$, hence contains no y-coordinate of any 2^n-torsion point of E. □

Next, we recall a basic fact about towers of torsion fields.

Theorem 5.1.3 *Let k be a field, ℓ a prime number, and E/k an elliptic curve. Then we have the following inclusions of fields for all $n \geq 1$:*



Corollary 5.1.4 *With all notation as above, suppose $E/\mathbf{F}_p$ is an elliptic curve such that $\mathbf{F}_p(x(E[2^n])) = \mathbf{F}_p$. Then $\mathbf{F}_p(x(E[2^k])) = \mathbf{F}_p$ for all $k \leq n$.*

Proof This follows immediately. □

Remark 5.1.5 One can see this from a representation theory point of view too: if $F \equiv -I \pmod{2^n}$, then $F \equiv -I \pmod{2^k}$ for all $k \leq n$ as well.

The next proposition shows that over a finite field $\mathbf{F}_p$, if $E \to E'$ is descending and $F \equiv -I \pmod{2^m}$ then we automatically get that $F' \equiv -I \pmod{2^{m-1}}$. This does not immediately imply that that p is anomalous because it could further be the case that $F' \equiv -I \pmod{2^m}$. This will be used in the proof of Theorem 5.2.1 below where we argue that $F' \equiv -I \pmod{2^m}$ for half of the primes for which $F \equiv -I \pmod{2^m}$ and $F' \equiv -I \pmod{2^{m-1}}$ for the other half.

Proposition 5.1.6 *Let E and E' be ordinary 2-isogenous elliptic curves defined over $\mathbf{F}_p$ and suppose that the isogeny $E \to E'$ is descending. Suppose $E(\mathbf{F}_p)[2^\infty] \simeq E'(\mathbf{F}_p)[2^\infty] \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ and that $F \equiv -I \pmod{2^m}$. Then $F' \equiv -I \pmod{2^{m-1}}$.*

Proof Fix $m \geq 2$ and suppose $F \equiv -I \pmod{2^m}$. Then it is also true that $F \equiv -I \pmod{2^{m-k}}$ for $k = 0, \ldots, m-1$; in particular $E(\mathbf{F}_p)[2] \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ since F is represented by the identity class modulo 2. However, no conjugate of F fixes a point modulo 2^{m-k} (since F is scalar modulo 2^{m-k}). Thus $E(\mathbf{F}_p)[2^\infty] \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. A calculation shows that $F^2 \equiv I \pmod{2^{m+1}}$, hence by (2.1.3) we must have $E(\mathbf{F}_{p^2})[2^{m+1}] \simeq \mathbf{Z}/2^{m+1}\mathbf{Z} \times \mathbf{Z}/2^{m+1}\mathbf{Z}$. Since E and E' are isogenous, the groups $E(\mathbf{F}_{p^2})$ and $E'(\mathbf{F}_{p^2})$ have the same size, hence their 2-Sylow subgroups have the same size.

If the 2-Sylow subgroups over $\mathbf{F}_{p^2}$ are isomorphic, then $(F')^2 \equiv I \pmod{2^{m+1}}$. It is also the case that $F' \equiv I \pmod{2}$ and F' does not fix a cyclic subgroup of $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$ of order 4. A calculation with matrices shows that $F' = -I \in \mathrm{GL}_2(\mathbf{Z}/2^m\mathbf{Z})$ is the unique matrix satisfying these conditions simultaneously. Thus, $F' \equiv -I \pmod{2^m}$. Hence it is also true that $F' \equiv -I \pmod{2^{m-1}}$.

If the 2-Sylow subgroups of E and E' defined over $\mathbf{F}_{p^2}$ are not isomorphic, then because the isogeny is descending we have $E(\mathbf{F}_{p^2})[2^m] \simeq \mathbf{Z}/2^m\mathbf{Z} \times \mathbf{Z}/2^m\mathbf{Z}$. Hence F' is a matrix such that $F' \equiv I \pmod{2}$, does not stabilize a cyclic subgroup of $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$ of order 4, and satisfies $(F')^2 \equiv I \pmod{2^m}$. Therefore $F' \equiv -I \pmod{2^{m-1}}$ by the same reasoning. □

Remark 5.1.7 This proposition tells us that if $\mathbf{F}_p(x(E[2^n])) = \mathbf{F}_p$ then $\mathbf{F}_p(x(E'[2^{n-1}])) = \mathbf{F}_p$.

To finish off this section we will record a technical lemma that we will need in the proof of Theorem 5.2.1 below.

Lemma 5.1.8 *Let E be an elliptic curve over a field k of characteristic $p > 3$ and write*

$$E : y^2 = x^3 + ax + b.$$

Suppose that k contains $x(E[2^n])$. Let $P = (\xi, \eta)$ be a point of order 2^{n+1} and let $\langle P \rangle$ denote the cyclic subgroup of $E[2^{n+1}]$ generated by P. Then the set of x-coordinates of the points in $\langle P \rangle$ are contained in k if and only if the the polynomial

$$x^4 - 4\xi x^3 - 2ax^2 + (-4\xi a - 8b)x + (a^2 - 4\xi b)$$

splits in k.

Proof The difference between any two generators in $\langle P\rangle$ is a point of order dividing 2^n. By Theorem 5.1.3, since k contains $x(E[2^n])$, it contains the x-coordinates of all points of order dividing 2^n. Thus, one point of $\langle P\rangle$ of exact order 2^{n+1} will have rational x-coordinate if and only if they all do. Therefore, all the points of $\langle P\rangle$ will have rational x-coordinates if and only if the points of exact order 2^{n+1} do. Such a point P is the preimage under the duplication map of a point of order 2^n in $\langle P\rangle$, hence by [20, III.2.3(d)] the x-coordinate of P is k-rational if and only if the quartic polynomial (whose roots are the x-coordinates of these points of order 2^{m+1})

$$x^4 - 4\xi x^3 - 2ax^2 + (-4\xi a - 8b)x + \left(a^2 - 4\xi b\right)$$

has all its roots defined over k. □

5.2 The proportion of anomalous primes

Fix $m \geq 2$. The key step in proving Theorem 1.3.4 is the following.

Theorem 5.2.1 *Suppose E and E' are rationally 2-isogenous elliptic curves defined over $\mathbf{Q}$ such that G and G' each have index 3 in $\mathrm{GL}_2(\mathbf{Z}_2)$. Let $m \geq 2$. Then the proportion of anomalous primes of defect $(m+1, m)$ is*

$$\frac{1}{2} \cdot \frac{1}{|G(2^m)|} = \frac{1}{2^{4m-2}}.$$

We break this proof into two steps, starting with a lemma.

Lemma 5.2.2 *Suppose p is a prime for which $F \equiv -I + 2^m M \pmod{2^{m+1}}$ with $M \not\equiv 0 \pmod 2$. Then p is anomalous of defect $(m+1, m)$ if and only if $\mathbf{F}_p(x(E'[2^m])) \neq \mathbf{F}_p$.*

Proof This follows from the results of the previous section. We have that p is anomalous of defect $(m+1, m)$ if and only if $E(\mathbf{F}_p)[2^\infty] \simeq E'(\mathbf{F}_p)[2^\infty] \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, $E(\mathbf{F}_{p^2})[2^\infty] \simeq \mathbf{Z}/2^a\mathbf{Z} \times \mathbf{Z}/2^{m+1}\mathbf{Z}$, and $E'(\mathbf{F}_{p^2}) \simeq \mathbf{Z}/2^{a+1}\mathbf{Z} \times \mathbf{Z}/2^m\mathbf{Z}$. By our matrix calculations, this is true if and only if $F \equiv -I + 2^m M \pmod{2^{m+1}}$ and $F' \equiv -I + 2^{m-1}M' \pmod{2^m}$ with neither M nor $M' \equiv 0 \pmod 2$. By Proposition 5.1.6, $F \equiv -I + 2^m M \pmod{2^{m+1}}$ implies $F' \equiv -I + 2^{m-1}M' \pmod{2^m}$. By the Galois theory of torsion point fields from Lemma 5.1.2, $M' \not\equiv 0 \pmod 2$ if and only if $\mathbf{F}_p(x(E'[2^m])) \neq \mathbf{F}_p$. □

We now make some global choices for E that we use in the next proof. Fix a basis P, Q for T_2E and write P_{2^k}, Q_{2^k} for the reductions modulo 2^k of P and Q, respectively. Since E and E' are rationally 2-isogenous, there exists a 2-isogeny $\varphi : E \to E'$ defined over $\mathbf{Q}$. Since φ is defined over $\mathbf{Q}$, we may write $E' = E/\langle S\rangle$ for some $\mathbf{Q}$-rational 2-torsion point S of E. We choose our basis so that $S = P_2$.

Let $P' = \varphi(P)$ and $Q' = \varphi(Q)$ with P'_{2^k} and Q'_{2^k} defined similarly. We have that $Q'_{2^k} = Q_{2^k} + \langle P_2\rangle$ is a 2^k-torsion point of E', but P'_{2^k} is not necessarily independent of Q'_{2^k}. We fix a basis Q', R' for T_2E' so that for all m, Q'_{2^m} and R'_{2^m} form a basis for $E'[2^m]$.

By applying Vélu's explicit formulas, we see that there exists a change of coordinates such that E and E' are given by the explicit Weierstrass equations

$$E:\ y^2 = (x + a_2)(x^2 - 4a_4)$$
$$E':\ y^2 = x(x^2 + a_2x + a_4),$$

where $P_2 = (-a_2, 0)$ and $P_2' = (0, 0)$. Write $R'_{2^{m-1}} = (\xi_{m-1}, \eta_{m-1})$ with $\xi_{m-1}, \eta_{m-1} \in \overline{\mathbf{Q}}$. Then the x-coordinate ξ_m of R'_{2^m} is given by one of the roots the quartic

$$x^4 - 4\xi_{m-1}x^3 + (-4\xi_{m-1}a_2 + 6a_4)x^2 + (4a_4a_2 - 8a_4)x + \left(-4a_4a_2 + \left(a_4^2 - 4\xi_{m-1}a_4\right)\right). \tag{5.2.3}$$

Next we show the existence of anomalous primes of defect $(m+1, m)$ for all $m \geq 2$.

Theorem 5.2.4 *Let E and E' be rationally 2-isogenous elliptic curves over $\mathbf{Q}$ and suppose that G and G' each have index 3 in $\mathrm{GL}_2(\mathbf{Z}_2)$. Then for all $m \geq 2$ there exist anomalous primes of defect $(m+1, m)$.*

Proof Fix $m \geq 2$. By the assumption on the size of G and G' and the Chebatorev Density Theorem, there exist infinitely many primes p for which $F \pmod{2^{m+1}}$ is in the conjugacy class of

$$-I + 2^m \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Let V_p be the isogeny volcano which contains E and E' as adjacent vertices and let V_{p^2} be the corresponding volcano over $\mathbf{F}_{p^2}$. By our work in Sect. 4 we know that E is on level at least m of V_p. The form of this matrix will allow us to conclude, in this instance, that E lies on the crater of V_p, from which we will be able to deduce the defect of p.

Claim: The height of V_p is m and $\operatorname{disc} \mathcal{O}_0 \equiv 5 \pmod 8$.

We now prove the claim. Write $F = -I + 2^m \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbf{Z}_2)$. As in the end of Sect. 4,

$$t^2 - 4p \equiv 2^{2m}((x-w)^2 + 4yz) \pmod{2^{2m+1}}.$$

Therefore $v_2(t^2 - 4p) = 2m + v_2((x-w)^2 + 4yz)$.

We have $\mathsf{sqf}(t^2 - 4p) \equiv \mathsf{sqf}((x-w)^2 + 4yz)) \pmod 8$. If $x - w$ is odd, then $v_2((x-w)^2 + 4yz) = 0$ and $v_2(t^2 - 4p) = 2m$. In this case it is also true that $\mathsf{sqf}((x-w)^2 + 4yz)) \equiv 5 \pmod 8$ if and only if yz is odd. If this holds, $\operatorname{disc} \mathcal{O}_0 \equiv 5 \pmod 8$. Consequently, since $\operatorname{disc} \mathcal{O}_0 \equiv 1 \pmod 4$, equation (4.0.1) shows that the height of V_p is $v_2((t^2 - 4p)/2) = m$.

Now set $\left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ as above. We saw in Sect. 4 that for a volcano V_p in which $\operatorname{disc} \mathcal{O}_0 \equiv 5 \pmod 8$, there is a unique vertex on the crater. Since E lies on level at least m of V_p and $h(V_p) = m$, we see that E is the unique vertex on the crater of V_p.

Returning to the proof of the theorem, we conclude from the Claim that V_{p^2} has height $m+1$ and the group structure on the crater is $\mathbf{Z}/2^a\mathbf{Z} \times \mathbf{Z}/2^{m+1}\mathbf{Z}$. Since a vertex on the floor of V_{p^2} has a cyclic group of rational points, it must be the case that the curves on each level of V_{p^2} have different group structures. So in particular, $E'(\mathbf{F}_{p^2})[2^\infty] = \mathbf{Z}/2^{a-1}\mathbf{Z} \times \mathbf{Z}/2^m\mathbf{Z}$. This means that p must have defect $(m+1, m)$. □

We now finish the proof of Theorem 5.2.1.

Proof of Theorem 5.2.1 By Lemma 5.2.2 a prime p is anomalous of defect $(m+1, m)$ if and only if $F = -I + 2^m M$ and $F' = -I + 2^{m-1}M'$, with neither M nor $M' \equiv 0 \pmod 2$. We will interpret our proportion $1/2^{4m-2}$ as a conditional probability. Suppose p is a prime such that $F = -I + 2^m M$. By the Chebotarev Density Theorem, the proportion of such primes is $1/|G(2^m)| = 1/2^{4m-3}$. By Proposition 5.1.6, we have that $F' \equiv -I \pmod{2^{m-1}}$

at these primes as well. We will show that for a proportion of 1/2 of these primes we have $F' \not\equiv -I \pmod{2^m}$ and so p is anomalous with defect $(m+1, m)$. Now we compute in the basis we have set above:

$$F(P_{2^m}) = -P_{2^m}$$
$$F(Q_{2^m}) = -Q_{2^m}$$

so that

$$F'(Q'_{2^m}) = F'(Q_{2^m} + \langle P_2 \rangle) = F(Q_{2^m}) + F(\langle P_2 \rangle) = -Q_{2^m} + \langle P_2 \rangle = -Q'_{2^m}$$

because P_2 is defined over $\mathbf{Q}$.

Therefore, we have determined that F' acts on $E'[2^m]$ via

$$F' \equiv \begin{pmatrix} -1 & * \\ 0 & * \end{pmatrix} \pmod{2^m}.$$

But since $p \equiv \det(F) \pmod{2^m}$ and $\det(F) \equiv 1 \pmod{2^m}$, we must additionally have $F' \equiv \left(\begin{smallmatrix} -1 & * \\ 0 & -1 \end{smallmatrix}\right) \pmod{2^m}$. Therefore, Proposition 5.1.1 shows that in this setting p is not anomalous of defect $(m+1, m)$ if and only all the x-coordinates of the 2^m-torsion points of E' are defined over $\mathbf{F}_p$. To determine when this happens, we examine the quartic (5.2.3).

By Propositions 5.1.1 and 5.1.6, we know that the the x-coordinates of the 2^{m-1}-torsion points on E' are $\mathbf{F}_p$-rational. Any two choices of R'_{2^m} differ by a 2^{m-1}-torsion point. Therefore, the x-coordinate of any choice of R'_{2^m} is defined over $\mathbf{F}_p$ if and only if the x-coordinate of one choice of of R'_{2^m} is defined over $\mathbf{F}_p$.

With notation as above, consider the quartic polynomial given in (5.2.3). The roots of this polynomial give the x-coordinates of the 2^m-torsion points of all preimages of $R_{2^{m-1}}$.

Since the x-coordinates of all of the 2^m-torsion points of E are defined over $\mathbf{F}_{p^2}$, the quartic polynomial in (5.2.3) must factor over $\mathbf{F}_p$ as a product of irreducible polynomials each of degree at most 2. In particular, it is reducible over $\mathbf{F}_p$.

We have shown that if the quartic (5.2.3) has one root defined over $\mathbf{F}_p$, then it splits completely into linear factors over $\mathbf{F}_p$. Therefore, since (5.2.3) is reducible over $\mathbf{F}_p$, it factors as a product of two conjugate quadratic polynomials over $\mathbf{F}_p$. If it were the case that these polynomials split into linear factors over $\mathbf{F}_p$ for every p, there would not exist any primes of defect $(m+1, m)$, contradicting Theorem 5.2.4. Thus they must be irreducible for 1/2 of the primes considered in this proof and and split for the complementary primes, and so the proportion of primes of defect $(m+1, m)$ is $(1/2) \cdot (1/2^{4m-3}) = 1/2^{4m-2}$, as claimed. □

We now complete the proof of Theorem 1.3.4 as a corollary.

Corollary 5.2.5 *With all notation as above, we have* $\mathcal{P} = 1/30$.

Proof For all $m \geq 2$, Theorem 5.2.1 shows that the proportion of anomalous primes of defect $(m+1, m)$ is 2^{-4m+2}. By symmetry via the dual isogeny, the proportion of anomalous primes of defect $(m, m+1)$ is 2^{-4m+2} as well. Therefore, the proportion of anomalous primes $\mathcal{P}$ is given by the geometric series

$$\mathcal{P} = 2 \sum_{m=2}^{\infty} \frac{1}{2^{4m-2}} = \frac{1}{32} \sum_{k=0}^{\infty} \frac{1}{16^k} = \frac{1}{30}.$$

□

5.3 Isogenies of composite degree

A natural question is whether these results can be immediately extended to the case where the 2-adic images G and G' are conjugate to the group that generates X_6 and the isogeny in question has composite degree $\equiv 2 \pmod 4$. In fact the answer is subtle, as the following examples show.

Example 5.3.1 Let E be the elliptic curve `336.b1` and E' the 6-isogenous elliptic curve `336.b4`. Of the first 100,000 good primes, we find that **7432** are anomalous, which does not agree experimentally with the proportion of 1/30 predicted by Theorem 1.3.4. Note that the image of the 3-adic representation of both E and E' has LMFDB label `3.4.0.1`.

Example 5.3.2 Let E be the elliptic curve `798.d3` and E' the 6-isogenous elliptic curve `798.d6`. Of the first 100,000 good primes, we find that **2199** are anomalous, which again does not agree experimentally with the proportion of 1/30 predicted by Theorem 1.3.4. Note that the image of the 3-adic representation of E has LMFDB label `3.24.0.1` and E' has `9.24.0.1`.

The difference between the two examples may be explained by the difference in their 3-adic representations. It would be interesting to extend Theorems 1.3.4 and 1.3.7 to the cases of isogenies of degree 6, 10, 14, 18 (the cyclic isogenies of composite degree $\equiv 2 \pmod 4$ allowed over $\mathbf{Q}$, by [13, Thm. 1]), filtering by ℓ-adic image. We thank one of the anonymous referees for bringing this question to our attention.

6 The distribution of anomalous primes by volcano height

In this section we take a different point of view and explore how the defect of an anomalous prime corresponds to the height and shape of the associated volcano. These results are motivated by experiments with the pair (E, E') of rationally 2-isogenous elliptic curves over $\mathbf{Q}$ where where E has LMFDB label `69.a2` and E' has label `69.a1`. We computed the anomalous primes p up to $2 \cdot 10^7$ and divided them up by defect, the height of the associated volcano $h(V_p)$, and disc $\mathcal{O}_0 \pmod 8$, which determines the shape of the crater of V_p. We include the data for anomalous primes of defect (3, 2) and for anomalous primes of defect (4, 3) in Appendix A.

Let S_m be the set of anomalous primes of defect $(m+1, m)$. For $i \in \{0, 1, 4, 5\}$ and a positive integer $H \geq m$, let $S_m(i, H)$ be the subset of $p \in S_m$ for which $\operatorname{disc} \mathcal{O}_0 \equiv i \pmod 8$ and $h(V_p) = H$. Let $S'_m(i, H)$ denote the proportion of primes in S_m that lie in $S_m(i, H)$. The data we have collected strongly suggest the following results.

Conjecture 6.0.1 *Let E and E' be rationally 2-isogenous elliptic curves over $\mathbf{Q}$ such that $[\mathrm{GL}_2(\mathbf{Z}_2) : \operatorname{im} \rho_{E,2}] = [\mathrm{GL}_2(\mathbf{Z}_2) : \operatorname{im} \rho_{E',2}] = 3$. For any $H \geq m$, we have*

$$S'_m(1, H) = S'_m(5, H) = 4^{-(H-(m-1))}$$

and

$$S'_m(0, H) = S'_m(4, H) = \frac{1}{2} \cdot 4^{-(H-(m-1))}.$$

We give one quick check that this conjecture is reasonable. Since every $p \in S_m$ lies in exactly one of the sets $S_m(i, H)$, it must be the case that

$$\sum_{i\in\{0,1,4,5\}} \sum_{H\geq m} S_m(i, H) = 1.$$

For $i \in \{1, 5\}$ we have

$$\sum_{H\geq m} S_m(i, H) = \sum_{H\geq m} 4^{-(H-(m-1))} = \frac{1}{4} \cdot \frac{1}{1-\frac{1}{4}} = \frac{1}{3}.$$

For $i \in \{0, 4\}$ we have

$$\sum_{H\geq m} S_m(i, H) = \sum_{H\geq m} \frac{1}{2} \cdot 4^{-(H-(m-1))} = \frac{1}{8} \cdot \frac{1}{1-\frac{1}{4}} = \frac{1}{6}.$$

There are three possibilities for the shape of the crater of the volcano V_p, depending on whether disc $\mathcal{O}_0$ is congruent to 1 modulo 8, 5 modulo 8, or 0 modulo 4. This calculation suggests that among the set of all anomalous primes, these three shapes are equally likely, and further that if we divide up the volcanoes of a fixed height $H \geq m$, all three crater shapes are equally likely. Another nice consequence of this conjecture is that for any fixed $i \in \{0, 1, 4, 5\}$ it is clear how $S_m(i, H)$ changes with H, as it predicts that

$$\frac{S_m(i, H+1)}{S_m(i, H)} = \frac{1}{4}.$$

In Sect. 5 we saw that if p is anomalous of defect $(m + 1, m)$ and $F \in \mathrm{GL}_2(\mathbf{Z}_2)$ is in the conjugacy class of Frobenius, then

$$F = -I + 2^m \begin{pmatrix} x & y \\ z & w \end{pmatrix}$$

where x, y, z, w are not all $0 \pmod 2$. At the end of Sect. 4 we saw that disc $\mathcal{O}_0 \pmod 8$ is determined by $\mathsf{sqf}((x-w)^2+4yz) \pmod 8$ and that $h(V_p)$ is determined by both disc $\mathcal{O}_0 \pmod 8$ and $v_2\left((x-w)^2+4yz\right)$.

The goal of this section is to show that if the matrix $\left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right)$ were distributed like a Haar random matrix in $\mathrm{M}_2(\mathbf{Z}_2)$ subject to the additional constraint that $v_2(y) = 0$, we would see the behavior predicted in Conjecture 6.0.1. We do not currently have a satisfactory explanation of why Frobenius at anomalous primes of defect $(m+1, m)$ should correspond to these 'random matrices with y odd'.

Fix a positive integer $m \geq 2$. We now explain our model for anomalous primes of defect $(m + 1, m)$. Let E be an elliptic curve over $\mathbf{F}_p$ with trace of Frobenius t and V_p be the associated 2-isogeny volcano over $\mathbf{F}_p$. Let $K = \mathbf{Q}\left(\sqrt{t^2-4p}\right) = \mathbf{Q}\left(\sqrt{D}\right)$ where $D = \mathsf{sqf}(t^2-4p)$. Recall from Sect. 4 that $h(V_p) = H$ if and only if

$$v_2(t^2-4p) = 2m + v_2((x-w)^2+4yz) = \begin{cases} 2H & \text{if } D \equiv 1 \pmod 4 \\ 2H+2 & \text{if } D \equiv 3 \pmod 4 \\ 2H+3 & \text{if } D \equiv 2 \pmod 4. \end{cases}$$

Also recall that disc $\mathcal{O}_0 \equiv$ disc $\mathcal{O}_K \pmod 8$.

Instead of starting from an elliptic curve over $\mathbf{F}_p$ we consider a Haar random matrix $M = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right)$ with entries in $\mathbf{Z}_2$ subject to the additional constraint that $v_2(y) = 0$. We use $\det(-I + 2^m M)$ in place of p and $\mathrm{trace}(-I + 2^m M) = -2 + 2^m(x + w)$ in place of t. Note that for any fixed x, the map taking w to $\alpha = x - w$ is a bijection on $\mathbf{Z}_2$. For the

rest of the proof we usually do not refer to x and w, but only to α. Let α and z be random elements of $\mathbf{Z}_2$ distributed with respect to Haar measure, and $y \in \mathbf{Z}_2^*$ be a random unit in $\mathbf{Z}_2$. We write Prob$(\cdot)$ to denote the proportion of α, y, z for which some property holds.

We define a kind of height associated to the matrix M. Let

$$H_M = \begin{cases} m + \frac{v_2((x-w)^2+4yz)}{2} & \text{if } \mathsf{sqf}((x-w)^2+4yz) \equiv 1 \pmod 4 \\ m - 1 + \frac{v_2((x-w)^2+4yz)}{2} & \text{if } \mathsf{sqf}((x-w)^2+4yz) \equiv 3 \pmod 4 \\ m - 1 + \frac{v_2((x-w)^2+4yz)-1}{2} & \text{if } \mathsf{sqf}((x-w)^2+4yz) \equiv 2 \pmod 4 \end{cases}.$$

Theorem 6.0.2 *Let $m \geq 2$ and $H \geq m$ be positive integers. Let $M = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right) \in \mathrm{M}_2(\mathbf{Z}_2)$ be a Haar random matrix subject to the additional constraint that $v_2(y) = 0$.*

(1) *For $i \in \{1, 5\}$, the probability that $\mathsf{sqf}((x-w)^2+4yz) \equiv i \pmod 8$ and $H_M = H$ is $4^{-(H-(m-1))}$.*

(2) *For $i \in \{2, 3\}$, the probability that $\mathsf{sqf}((x-w)^2+4yz) \equiv i \pmod 4$ and $H_M = H$ is $\frac{1}{2} \cdot 4^{-(H-(m-1))}$.*

Theorem 6.0.2 follows from the following stronger result.

Theorem 6.0.3

$$(1) \qquad \mathrm{Prob}\left(\begin{matrix} v_2(\alpha^2+4yz) = k \\ \mathsf{sqf}(\alpha^2+4yz) \equiv 1 \pmod 8 \end{matrix}\right) = \mathrm{Prob}\left(\begin{matrix} v_2(\alpha^2+4yz) = k \\ \mathsf{sqf}(\alpha^2+4yz) \equiv 5 \pmod 8 \end{matrix}\right) = \begin{cases} 0 & \text{if } k \text{ is odd,} \\ 2^{-(k+2)} & \text{if } k \text{ is even.} \end{cases}$$

$$(2) \qquad \mathrm{Prob}\left(\begin{matrix} v_2(\alpha^2+4yz) = k \\ \mathsf{sqf}(\alpha^2+4yz) \equiv 3 \pmod 4 \end{matrix}\right) = \begin{cases} 0 & \text{if } k \text{ is odd or } k = 0, \\ 2^{-(k+1)} & \text{if } k \geq 2 \text{ is even.} \end{cases}$$

$$(3) \qquad \mathrm{Prob}\left(\begin{matrix} v_2(\alpha^2+4yz) = k \\ \mathsf{sqf}(\alpha^2+4yz) \equiv 2 \pmod 4 \end{matrix}\right) = \begin{cases} 0 & \text{if } k \text{ is even or } k = 1, \\ 2^{-k} & \text{if } k \geq 3 \text{ is odd.} \end{cases}$$

It is straightforward to check that this result implies Theorem 6.0.2 by checking the base case $H = m$ and then thinking about what happens to these probabilities as we increase H, dividing things into cases based on $\mathsf{sqf}(\alpha^2+4yz) \pmod 8$ and using the definition of H_M.

We prove this result by dividing the set of all $\alpha, z \in \mathbf{Z}_2$ and $y \in \mathbf{Z}_2^*$ based on the relative sizes of $v_2(\alpha^2)$ and $v_2(4yz) = 2 + v_2(z)$. More precisely, we prove Theorem 6.0.3 in three parts, where each part is divided into cases based on $\mathsf{sqf}(\alpha^2+4yz) \pmod 8$.

Lemma 6.0.4

$$(1) \ \mathrm{Prob}\left(\begin{matrix} v_2(\alpha^2+4yz) = k \\ \mathsf{sqf}(\alpha^2+4yz) \equiv 1 \pmod 8 \\ v_2(\alpha^2) < v_2(4yz) \end{matrix}\right) = \begin{cases} 0 & \text{if } k \text{ is odd,} \\ 2^{-(3k/2+2)} & \text{otherwise.} \end{cases}$$

$$(2)\ \text{Prob}\left(\begin{array}{rcl} \nu_2(\alpha^2+4yz) & = & k \\ \mathsf{sqf}(\alpha^2+4yz) & \equiv 5 & \pmod 8 \\ \nu_2(\alpha^2) < \nu_2(4yz) & & \end{array}\right) = \begin{cases} 0 & \text{if } k \text{ is odd,} \\ 2^{-(3k/2+2)} & \text{otherwise.} \end{cases}$$

$$(3)\ \text{Prob}\left(\begin{array}{rcl} \nu_2(\alpha^2+4yz) & = & k \\ \mathsf{sqf}(\alpha^2+4yz) & \equiv 3 & \pmod 4 \\ \nu_2(\alpha^2) < \nu_2(4yz) & & \end{array}\right) = \begin{cases} 0 & \text{if } k \text{ is odd or } k=0, \\ 2^{-(3k/2+1)} & \text{otherwise.} \end{cases}$$

$$(4)\ \text{Prob}\left(\begin{array}{rcl} \nu_2(\alpha^2+4yz) & = & k \\ \mathsf{sqf}(\alpha^2+4yz) & \equiv 2 & \pmod 4 \\ \nu_2(\alpha^2) < \nu_2(4yz) & & \end{array}\right) = 0.$$

Lemma 6.0.5

$$(1)\ \text{Prob}\left(\begin{array}{rcl} \nu_2(\alpha^2+4yz) & = & k \\ \mathsf{sqf}(\alpha^2+4yz) & \equiv 1 & \pmod 8 \\ \nu_2(\alpha^2) > \nu_2(4yz) & & \end{array}\right) = \begin{cases} 0 & \text{if } k \text{ is odd,} \\ 2^{-(3k/2+2)} & \text{otherwise.} \end{cases}$$

$$(2)\ \text{Prob}\left(\begin{array}{rcl} \nu_2(\alpha^2+4yz) & = & k \\ \mathsf{sqf}(\alpha^2+4yz) & \equiv 5 & \pmod 8 \\ \nu_2(\alpha^2) > \nu_2(4yz) & & \end{array}\right) = \begin{cases} 0 & \text{if } k \text{ is odd,} \\ 2^{-(3k/2+2)} & \text{otherwise.} \end{cases}$$

$$(3)\ \text{Prob}\left(\begin{array}{rcl} \nu_2(\alpha^2+4yz) & = & k \\ \mathsf{sqf}(\alpha^2+4yz) & \equiv 3 & \pmod 4 \\ \nu_2(\alpha^2) > \nu_2(4yz) & & \end{array}\right) = \begin{cases} 0 & \text{if } k \text{ is odd or } k=0, \\ 2^{-(3k/2+1)} & \text{otherwise.} \end{cases}$$

$$(4)\ \text{Prob}\left(\begin{array}{rcl} \nu_2(\alpha^2+4yz) & = & k \\ \mathsf{sqf}(\alpha^2+4yz) & \equiv 2 & \pmod 4 \\ \nu_2(\alpha^2) > \nu_2(4yz) & & \end{array}\right) = \begin{cases} 0 & \text{if } k \text{ is even or } k=1, \\ 2^{-(3k/2-1/2)} & \text{otherwise.} \end{cases}$$

Lemma 6.0.6

$$(1)\ \text{Prob}\left(\begin{array}{rcl} \nu_2(\alpha^2+4yz) & = & k \\ \mathsf{sqf}(\alpha^2+4yz) & \equiv 1 & \pmod 8 \\ \nu_2(\alpha^2)=\nu_2(4yz)=2\beta & & \end{array}\right) = \begin{cases} 0 & \text{if } k \text{ is odd or } k \in \{0,2\}, \\ 2^{-(k+\beta+2)} & \text{if } k \text{ is even and } 2 \le 2\beta \le k-1. \end{cases}$$

$$(2)\ \text{Prob}\left(\begin{array}{rcl} \nu_2(\alpha^2+4yz) & = & k \\ \mathsf{sqf}(\alpha^2+4yz) & \equiv 5 & \pmod 8 \\ \nu_2(\alpha^2)=\nu_2(4yz)=2\beta & & \end{array}\right) = \begin{cases} 0 & \text{if } k \text{ is odd or } k \in \{0,2\}, \\ 2^{-(k+\beta+2)} & \text{if } k \text{ is even and } 2 \le 2\beta \le k-1. \end{cases}$$

$$(3)\ \text{Prob}\left(\begin{array}{rcl} \nu_2(\alpha^2+4yz) & = & k \\ \mathsf{sqf}(\alpha^2+4yz) & \equiv 3 & \pmod 4 \\ \nu_2(\alpha^2)=\nu_2(4yz)=2\beta & & \end{array}\right) = \begin{cases} 0 & \text{if } k \text{ is odd or } k \in \{0,2\}, \\ 2^{-(k+\beta+1)} & \text{if } k \text{ is even and } 2 \le 2\beta \le k-1. \end{cases}$$

$$(4)\ \text{Prob}\left(\begin{array}{rcl} \nu_2(\alpha^2+4yz) & = & k \\ \mathsf{sqf}(\alpha^2+4yz) & \equiv 2 & \pmod 4 \\ \nu_2(\alpha^2)=\nu_2(4yz)=2\beta & & \end{array}\right) = \begin{cases} 0 & \text{if } k \text{ is even or } k=1, \\ 2^{-(k+\beta)} & \text{if } k \text{ is odd and } 2 \le 2\beta \le k-1. \end{cases}$$

Before proving these individual results, we see how they imply Theorem 6.0.3. We divide this argument into cases. Combining these three lemmas, it is clear that

$$\text{Prob}\left(\begin{array}{rcl} \nu_2(\alpha^2+4yz) & = & k \\ \mathsf{sqf}(\alpha^2+4yz) & \equiv 1 & \pmod 8 \end{array}\right) = \text{Prob}\left(\begin{array}{rcl} \nu_2(\alpha^2+4yz) & = & k \\ \mathsf{sqf}(\alpha^2+4yz) & \equiv 5 & \pmod 8 \end{array}\right),$$

and that these probabilities are 0 when k is odd. When $k=0$ we have

$$\text{Prob}\left(\begin{array}{rcl} \nu_2(\alpha^2+4yz) & = & 0 \\ \mathsf{sqf}(\alpha^2+4yz) & \equiv 1 & \pmod 8 \end{array}\right) = 2^{-2}+0+0,$$

and when $k=2$ we have

$$\text{Prob}\left(\begin{array}{rcl} \nu_2(\alpha^2+4yz) & = & 2 \\ \mathsf{sqf}(\alpha^2+4yz) & \equiv 1 & \pmod 8 \end{array}\right) = 2^{-5}+2^{-5}+0 = 2^{-4}.$$

Now suppose $k \geq 4$ is even. Note that $\lfloor \frac{k-1}{2} \rfloor = k/2 - 1$. We have

$$\begin{aligned}\text{Prob}\begin{pmatrix} v_2(\alpha^2+4yz) = & k \\ \mathsf{sqf}(\alpha^2+4yz) \equiv 1 & \pmod 8 \end{pmatrix} &= 2^{-(3k/2+2)} + 2^{-(3k/2+2)} + \sum_{\beta=1}^{\lfloor \frac{k-1}{2} \rfloor} 2^{-(k+\beta+2)} \\ &= 2^{-(3k/2+1)} + 2^{-(k+2)} \sum_{\beta=1}^{k/2-1} 2^{-\beta}.\end{aligned}$$

We write

$$\sum_{\beta=1}^{k/2-1} 2^{-\beta} = 2^{-1} \sum_{\beta=0}^{k/2-2} 2^{-\beta} = 2^{-1}\left(2^{-(k/2-2)} + 2^{-(k/2-3)} + \cdots + 2^{-1} + 2^0\right).$$

We see that

$$\begin{aligned}\text{Prob}\begin{pmatrix} v_2(\alpha^2+4yz) = & k \\ \mathsf{sqf}(\alpha^2+4yz) \equiv 1 & \pmod 8 \end{pmatrix} &= 2^{-(3k/2+1)} + 2^{-(k+3)}(2^{-(k/2-2)} + 2^{-(k/2-3)} + \cdots + 2^{-1} + 2^0) \\ &= 2^{-(3k/2+1)} + 2^{-(3k/2+1)} + 2^{-(3k/2+2)} + \cdots + 2^{-(k+3)} \\ &= 2^{-(k+2)}.\end{aligned}$$

We next consider the analogous computation for the case where $\mathsf{sqf}(\alpha^2 + 4yz) \equiv 3 \pmod 4$. Combining the lemmas above, we see that

$$\text{Prob}\begin{pmatrix} v_2(\alpha^2+4yz) = & k \\ \mathsf{sqf}(\alpha^2+4yz) \equiv 3 & \pmod 4 \end{pmatrix} = 0$$

if k is odd or $k = 0$. Suppose that $k \geq 2$ is even. We have

$$\text{Prob}\begin{pmatrix} v_2(\alpha^2+4yz) = & k \\ \mathsf{sqf}(\alpha^2+4yz) \equiv 3 & \pmod 4 \end{pmatrix} = 2^{-(3k/2+1)} + 2^{-(3k/2+1)} + 2^{-(k+2)} \sum_{\beta=1}^{k/2-1} 2^{-\beta},$$

where for $k = 2$ the empty sum in the final term is 0. Arguing as above, it is now clear that this sum is 2 times the analogous one for $\mathsf{sqf}(\alpha^2 + 4yz) \equiv 1 \pmod 8$.

Finally, we consider the computation for the case where $\mathsf{sqf}(\alpha^2 + 4yz) \equiv 2 \pmod 4$. Combining the lemmas above, we see that

$$\text{Prob}\begin{pmatrix} v_2(\alpha^2+4yz) = & k \\ \mathsf{sqf}(\alpha^2+4yz) \equiv 2 & \pmod 4 \end{pmatrix} = 0$$

if k is even or $k = 1$. Suppose $k \geq 3$ is odd. We have

$$\text{Prob}\begin{pmatrix} v_2(\alpha^2+4yz) = & k \\ \mathsf{sqf}(\alpha^2+4yz) \equiv 2 & \pmod 4 \end{pmatrix} = 2^{-(3k/2-1/2)} + \sum_{\beta=1}^{\frac{k-1}{2}} 2^{-(k+\beta)}.$$

Note that

$$\sum_{\beta=1}^{\frac{k-1}{2}} 2^{-(k+\beta)} = 2^{-(k+1)} \sum_{\beta=0}^{\frac{k-3}{2}} 2^{-\beta} = 2^{-(k+1)}\left(2^{-(k/2-3/2)} + 2^{-(k/2-5/2)} + \cdots + 2^{-1} + 2^0\right).$$

This gives

$$\begin{aligned}\text{Prob}\begin{pmatrix} v_2(\alpha^2+4yz) = & k \\ \mathsf{sqf}(\alpha^2+4yz) \equiv 2 & \pmod 4 \end{pmatrix} &= 2^{-(3k/2-1/2)} + \left(2^{-(3k/2-1/2)} + 2^{-(3k/2-3/2)} + \cdots + 2^{-(k+1)}\right) \\ &= 2^{-k}.\end{aligned}$$

We now prove the three lemmas.

Proof of Lemma 6.0.4 Suppose $v_2(\alpha^2) = k < v_2(4yz)$. Therefore k is even and $v_2(\alpha^2 + 4yz) = k$. The probability that $v_2(\alpha) = k/2$ is $2^{-(k/2+1)}$. The probability that $v_2(4yz) = 2 + v_2(z) > k$ is the probability that $v_2(z) \geq k - 1$, which is 1 if $k = 0$ and is $2^{-(k-1)}$ if $k \geq 2$ is even.

Write $\alpha = 2^{k/2}u$ where $u \in \mathbf{Z}_2^*$ and $4yz = 2^{k+1}v$ where $v \in \mathbf{Z}_2$. If $k = 0$ we must have $v_2(v) \geq 1$. By varying z, we see that v is a Haar random element of $2\mathbf{Z}_2$ when $k = 0$ and is a Haar random element of $\mathbf{Z}_2$ otherwise.

We have

$$\mathsf{sqf}(\alpha^2 + 4yz) = \mathsf{sqf}(u^2 + 2v) \equiv u^2 + 2v \pmod 8.$$

Since $u^2 \equiv 1 \pmod 8$ we see that

$$u^2 + 2v \equiv \begin{cases} 1 \pmod 8 & \text{if } v_2(v) \geq 2, \\ 5 \pmod 8 & \text{if } v_2(v) = 1, \\ 3 \pmod 4 & \text{if } v_2(v) = 0. \end{cases}$$

We see that $\mathsf{sqf}(\alpha^2 + 4yz) \equiv 1 \pmod 8$ if and only if $v_2(z) \geq 2k + 1$, which happens with probability $2^{-(2k+1)}$, that $\mathsf{sqf}(\alpha^2 + 4yz) \equiv 5 \pmod 8$ if and only if $v_2(z) = 2k$, which happens with probability $2^{-(2k+1)}$, and that $\mathsf{sqf}(\alpha^2 + 4yz) \equiv 3 \pmod 4$ if and only if $v_2(z) = 2k - 1$, which happens with probability 2^{-2k} if $k \geq 2$ and probability 0 if $k = 0$.

□

Proof of Lemma 6.0.5 Suppose $v_2(4yz) = 2 + v_2(z) = k < v_2(\alpha^2)$. So $v_2(\alpha^2 + 4yz) = k$. The probability that $v_2(z) = k - 2$ is $2^{-(k-1)}$ if $k \geq 2$ and is 0 otherwise. If $k \geq 2$ is even,

$$\mathrm{Prob}(v_2(\alpha^2) > k) = \mathrm{Prob}(v_2(\alpha) \geq k/2 + 1) = 2^{-(k/2+1)},$$

and if k is odd,

$$\mathrm{Prob}(v_2(\alpha^2) > k) = \mathrm{Prob}(v_2(\alpha) \geq k/2 + 1/2) = 2^{-(k/2+1/2)}.$$

Suppose $v_2(z) = k - 2$ where $k \geq 2$. We write $z = 2^{k-2}u$ where $u \in \mathbf{Z}_2^*$, so $4yz = uy2^k$. Suppose $v_2(\alpha^2) > k$. If k is even, then $\alpha = \gamma 2^{k/2+1}$ where $\gamma \in \mathbf{Z}_2$ is not necessarily a unit. In this case, $\mathsf{sqf}(\alpha^2 + 4yz) = \mathsf{sqf}(4\gamma + yu)$. For a fixed value of z, by varying y we see that yu is a Haar random element of $\mathbf{Z}_2^*$. Therefore, the probability that $\mathsf{sqf}(\alpha^2 + 4yz) \equiv 3 \pmod 4$ is $1/2$, and the probability that $\mathsf{sqf}(\alpha^2 + 4yz) \equiv i \pmod 8$ is $1/4$ for $i \in \{1, 5\}$. This completes the proof in the case that k is even. If k is odd, then $\alpha = \gamma 2^{k/2+1/2}$ where $\gamma \in \mathbf{Z}_2$ is not necessarily a unit. In this case, $\mathsf{sqf}(\alpha^2 + 4yz) = \mathsf{sqf}(4\gamma + 2yu) \equiv 2 \pmod 4$. This completes the proof when $k \geq 3$ is odd.

□

Proof of Lemma 6.0.6 Suppose that $v_2(\alpha^2) = v_2(4yz) = 2 + v_2(z)$. Since $v_2(\alpha^2) = 2v_2(\alpha)$, we must have $v_2(\alpha^2) = v_2(4yz) = 2 + v_2(z) = 2\beta$ with $\beta \geq 1$.

Suppose $v_2(\alpha) = \beta$ and write $\alpha = 2^\beta u$ where $u \in \mathbf{Z}_2^*$. Suppose that $v_2(z) = 2\beta - 2$ and write $z = 2^{2\beta-2}v$ where $v \in \mathbf{Z}_2^*$. So $4yz = 2^{2\beta}yv$. For a fixed value of z, varying y shows that yv is a Haar random element of $\mathbf{Z}_2^*$.

We have $v_2(\alpha^2 + 4yz) = 2\beta + v_2(u^2 + yv)$. Since u^2 and yv are both units, $v_2(u^2 + yv) \geq 1$ and we can write $u^2 + yv = 2\delta$ where $\delta \in \mathbf{Z}_2$. Since yv is a Haar random element of $\mathbf{Z}_2^*$,

we see that δ is a Haar random element of $\mathbf{Z}_2$. Suppose that $k - 2\beta \geq 0$. Therefore,

$$\text{Prob}(v_2(u^2 + yv) = k - 2\beta) = \begin{cases} 0 & \text{if } k - 2\beta = 0 \\ 2^{-(k-2\beta)} & \text{otherwise.} \end{cases}$$

We have

$$\mathsf{sqf}(\alpha^2 + 4yz) = \mathsf{sqf}(u^2 + yv) = \mathsf{sqf}(2\delta).$$

If $v_2(\delta)$ is even, then $\mathsf{sqf}(2\delta) \equiv 2 \pmod 4$. If $v_2(\delta)$ is odd, then for some nonnegative integer r we have $2\delta = 2^{2r}\delta'$, where $\delta' \in \mathbf{Z}_2^*$, and $\mathsf{sqf}(2\delta) = \mathsf{sqf}(\delta')$. If we restrict to any particular value of r, since δ is a Haar random element of $\mathbf{Z}_2$, we see that δ' is a Haar random element of $\mathbf{Z}_2^*$. In particular, the probability that $\mathsf{sqf}(\alpha^2 + 4yz) \equiv 3 \pmod 4$ is $1/2$ and the probability that $\mathsf{sqf}(\alpha^2 + 4yz) \equiv i \pmod 8$ is $1/4$ for $i \in \{1, 5\}$.

The probability that $v_2(\alpha) = \beta$ is $2^{-(\beta+1)}$. The probability that $v_2(z) = 2\beta - 2$ is $2^{-(2\beta-1)}$ if $\beta \geq 1$ and is 0 if $\beta = 0$. We note that

$$2^{-(\beta+1)}2^{-(2\beta-1)}2^{-(k-2\beta)} = 2^{-(k+\beta)}.$$

Considering the different cases for $\mathsf{sqf}(\alpha^2 + 4yz)$ modulo 4 and 8 completes the proof. □

7 Future work

If the groups G and G' are not as large as possible (i.e., do not have index 3 in $\mathrm{GL}_2(\mathbf{Z}_2)$), or if $G \not\simeq G'$, then the proportion $\mathcal{P}$ of anomalous primes might be quite different than $1/30$, as the following example shows.

Example 5.2.1 Let E be the elliptic curve `1200.e5` and E' the curve `1200.e2`. Both mod 4 representations have order 4 and neither mod 8 representation contains $-I$. By inspecting the 2-adic representations, one can check that the only possible defects of anomalous primes are (3, 2) and (2, 3). In fact, more is true.

If we look explicitly at the images of the mod 4 representations, we see

$$G(4) = \left\{ \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix} \right\}$$
$$G'(4) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & \pm 1 \end{pmatrix}, \begin{pmatrix} -1 & 2 \\ 0 & \pm 1 \end{pmatrix} \right\}.$$

If p is anomalous, then using the fact that $p \equiv 1 \pmod 4$ and that the 2-Sylow subgroups of $E(\mathbf{F}_p)$ and $E'(\mathbf{F}_p)$ are both $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, we must have $F \equiv -I \pmod 4$ and $F' \equiv \left(\begin{smallmatrix} -1 & 2 \\ 0 & -1 \end{smallmatrix}\right) \pmod 4$. Therefore, every anomalous prime has defect (3, 2) and by the Chebotarev density theorem this is exactly 1/4 of all primes.

In a forthcoming paper [8], we take up the problem of determining all possible values of $\mathcal{P}$, for all pairs of rationally 2-isogenous elliptic curves over $\mathbf{Q}$, including the case where E and E' have CM over $\mathbf{Q}$ (which produces very different values of $\mathcal{P}$). What makes this a finite task is that

(1) all images of 2-adic representations have been classified ([19] for the non-CM case and [16] for the CM case), and
(2) all isogeny-torsion graphs over $\mathbf{Q}$ have been classified in [4] and [5].

There are additional consequences for the isogeny volcanoes attached to these curves that we explore as well, including how the torsion point fields $\mathbf{Q}(E[2^m])$ and $\mathbf{Q}(E'[2^m])$ are "entangled". For example, we are able to show the following two results.

- If $\mathbf{Q}(E[2]) = \mathbf{Q}(E'[2])$ then G and G' must each have index greater than 3 in $\mathrm{GL}_2(\mathbf{Z}_2)$.
- If there are no primes of defect $(m+1, m)$ then we must have $\mathbf{Q}(E[2^m]) = \mathbf{Q}(E'[2^m])$ and $\mathbf{Q}(x(E[2^m])) = \mathbf{Q}(x(E'[2^m]))$.

We explore the consequences of these and similar results for anomalous primes.

Acknowledgements
We would like to thank Andrew Sutherland for supplying us with the initial computations that suggested the correct value of $\mathcal{P}$. We would also like to thank the anonymous referees for their careful reading and suggestions which improved the clarity of the paper. The second author was supported by NSF Grants DMS 1802281 and DMS 2154223.

Data availibility Data sets generated during the current study are available from the corresponding author on reasonable request.

Author details
[1]Department of Mathematics, Bard College, Annandale-On-Hudson, NY 12504, USA, [2]Department of Mathematics, University of California, Irvine, CA 92697, USA.

Appendix A: Sample calculations

Here we present some corroborating evidence for Theorem 1.3.4 which served as the impetus for this project. In the table below we present 15 pairs of curves whose 2-adic images have index 3 in $\mathrm{GL}_2(\mathbf{Z}_2)$ and list the number of anomalous primes up to 2^{30}. The proportions listed are the number of anomalous primes divided by $\pi(2^{30}) = 54400028$. One can see the 1/30 proportion very clearly emerging in the data. These calculations were performed on Magma [3] by Andrew Sutherland and we thank him for allowing us to include these data in this paper.

E	E'	Anomalous	Proportion
69.a1	69.a2	1814517	0.033355075
77.c1	77.c2	1812315	0.033314597
84.b1	84.b2	1813293	0.033332575
99.a1	99.a2	1812977	0.033326766
99.c1	99.c2	1812977	0.033326766
132.a1	132.a2	1812966	0.033326564
132.b1	132.b2	1812959	0.033326435
138.a1	138.a2	1813813	0.033342134
141.b1	142.b2	1812863	0.033324670
154.a1	154.a2	1812080	0.033310277
154.c1	154.c2	1813344	0.033333512
155.b1	155.b2	1813606	0.033338328
156.a1	156.a2	1813340	0.033333439
10608.y1	10608.y2	1812615	0.033320112
10608.j1	10608.j2	1814206	0.033349358

We also include some data for the pair (E, E') of rationally 2-isogenous elliptic curves over $\mathbf{Q}$ where E has LMFDB label `69.a2` and E' has label `69.a1`. We computed that there were 42,298 anomalous primes less than $2 \cdot 10^7$, a proportion of approximately

0.0333 among all primes. They are distributed by defect as follows:

(3, 2) : 19821 (2, 3) : 19831	**Total:** 39652
(4, 3) : 1264 (3, 4) : 1205	**Total:** 2469
(5, 4) : 84 (4, 5) : 86	**Total:** 170
(6, 5) : 3 (5, 6) : 4	**Total:** 7

We now look more closely at the 19,821 of these anomalous primes with defect (3, 2) and divide them up into rows based on disc $\mathcal{O}_0 \pmod 8$ and columns based on the height of V_p, the isogeny volcano associated to (E, E'):

disc $\mathcal{O}_0 \pmod 8 \setminus h(V_p)$	2	3	4	5	6	≥ 7
1	4930	1279	322	76	22	7
5	5024	1225	308	82	31	4
0	2501	570	168	45	10	3
4	2363	628	172	38	8	5

We give an analogous table for the 1264 of these anomalous primes with defect (4, 3):

disc $\mathcal{O}_0 \pmod 8 \setminus h(V_p)$	3	4	5	6	≥ 7
1	305	73	20	5	2
5	318	85	18	5	1
0	155	40	13	5	0
4	158	28	9	2	2

In both cases observe that the values decrease roughly by a factor of 4 as we move along a row, as predicted by Conjecture 6.0.1.

Received: 30 January 2023 Accepted: 3 June 2023
Published online: 10 July 2023

References

1. Achter, J., Wong, S.: Quotients of elliptic curves over finite fields. Int. J. Number Theory **9**(6), 1395–1412 (2013)
2. Adelmann, C.: The Decomposition of Primes in Torsion Point Fields. Lecture Notes in Mathematics, vol. 1761. Springer, Berlin (2001)
3. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symb. Comput. **24**(3–4), 235–265 (1997)
4. Chiloyan, G.: Infinite families of isogeny-torsion graphs. J. Number Theory **244**, 369–417 (2023)
5. Chiloyan, G., Lozano-Robledo, A.A.: A classification of isogeny-torsion graphs of elliptic curves over Q (with Garen Chiloyan). Trans. Lond. Math. Soc. **8**(1), 1–34 (2021)
6. Cullinan, J.: A remark on the group structure of elliptic curves in towers of finite fields. N. Y. J. Math. **24**, 857–865 (2018)
7. Cullinan, J.: A remark on the group structure of 2-isogenous elliptic curves in towers of finite fields. N. Y. J. Math. **26**, 207–217 (2020)
8. Cullinan, J., et al.: The probability of non-isomorphic group structures of isogenous elliptic curves in finite field extensions, II. (2023)
9. Freeman, D., Lauter, K.: Computing endomorphism rings of Jacobians of genus 2 curves over finite fields
10. Galbraith, S.: Mathematics of Public Key Cryptography. Cambridge University Press, Cambridge (2012)
11. Greenberg, R.: The image of Galois representations attached to elliptic curves with an isogeny. Am. J. Math. **134**(5), 1167–1196 (2012)
12. Heuberger, C., Mazzoli, M.: Elliptic curves with isomorphic groups of points over finite field extensions. J. Number Theory **181**, 89–98 (2017). https://doi.org/10.1016/j.jnt.2017.05.028
13. Kenku, M.A.: On the number of $\mathbf{Q}$-isomorphism classes of elliptic curves in each $\mathbf{Q}$-isogeny class. J. Number Theory **15**(2), 199–202 (1982)
14. Kohel, D.R.: Endomorphism rings of elliptic curves over finite fields. Thesis (Ph.D.). University of California, Berkeley
15. Lenstra, H.W., Jr.: Complex multiplication structure of elliptic curves. J. Number Theory **56**(2), 227–241 (1996). https://doi.org/10.1006/jnth.1996.0015

16. Lozano-Robledo, Á.: Galois representations attached to elliptic curves with complex multiplication. Algebra Number Theory **16**, 4 (2022)
17. Miret, J., Moreno, R., Sadornil, D., Tena, J., Valls, M.: An algorithm to compute volcanoes of 2-isogenies of elliptic curves over finite fields. Appl. Math. Comput. **176**(2), 739–750 (2006)
18. Miret, J., Pujolàs, J., Valera, J.: On the 2-adic valuation of the cardinality of elliptic curves over finite extensions of $\mathbf{F}_q$. Arch. Math. (Basel) **111**(6), 611–620 (2018)
19. Rouse, J., Zureick-Brown, D.: Elliptic curves over $\mathbf{Q}$ and 2-adic images of Galois. Res. Number Theory **1**, 12 (2015)
20. Silverman, J.H.: The Arithmetic of Elliptic Curves. Graduate Texts in Mathematics, vol. 106. Springer, Cham (2009)
21. Sutherland, A.V.: Isogeny volcanoes. In: ANTS X—proceedings of the tenth algorithmic number theory symposium, pp. 507–530 (2013). https://doi.org/10.2140/obs.2013.1.507
22. The LMFDB Collaboration: The L-functions and modular forms database. (2021). http://www.lmfdb.org accessed 11 Aug 2021
23. Wittmann, C.: Group structure of elliptic curves over finite fields. J. Number Theory **88**(2), 335–344 (2001). https://doi.org/10.1006/jnth.2000.2622

Publisher's Note