New York Journal of Mathematics

New York J. Math. **26** (2020) 207–217.

A remark on the group structure of 2-isogenous elliptic curves in towers of finite fields

John Cullinan

Abstract. Let A and B be ordinary 2-isogenous elliptic curves defined over a finite field F of odd characteristic. Suppose the groups A(F) and B(F) are isomorphic. We determine necessary and sufficient conditions for the groups A(L) and B(L) to be isomorphic for all finite extensions L/F. This complements recent work in which we considered the similar question for l-isogenous curves, when l is odd.

Contents

1. Introduction

Let ℓ be a prime number and F a finite field of characteristic coprime to ℓ. Let E_1 and E_2 be ordinary, ℓ-isogenous, elliptic curves defined over F such that the isogeny is also defined over F. In [2], building on [3] and [8], we considered the following problem.

Question 1.1. *Suppose the groups $E_1(F)$ and $E_2(F)$ are isomorphic. Under what conditions are $E_1(L)$ and $E_2(L)$ isomorphic, as L ranges over all finite extensions of F?*

Put another way, does the fact that $E_1(F)$ and $E_2(F)$ are isomorphic imply that $E_1(L)$ and $E_2(L)$ are isomorphic over all finite extensions L of F? We answered this question when ℓ is an odd prime, and record here the main result of [2].

Received October 29, 2019.
2010 *Mathematics Subject Classification.* 11G25, 14G15.
Key words and phrases. elliptic curve, finite field, isogeny.

ISSN 1076-9803/2020

Theorem 1.2 ([2]). *Let ℓ be an odd prime, F a finite field of characteristic coprime to ℓ, and E_1 and E_2 ordinary, ℓ-isogenous, elliptic curves defined over F. Then*

1. *the prime-to-ℓ parts of the groups $E_1(L)$ and $E_2(L)$ are isomorphic for every finite extension L/F, and*
2. *$E_1(L) \simeq E_2(L)$ for all finite extensions L/F if and only if the ℓ-Sylow subgroups of $E_1(F)$ and $E_2(F)$ are isomorphic and non-trivial.*

The upshot of Theorem 1.4 is a certificate for checking whether the groups $E_1(L)$ and $E_2(L)$ are isomorphic: replace F with a (possibly trivial) extension K/F so that the E_i acquire an ℓ-torsion point over K. Then for any finite extension L/K, $E_1(L) \simeq E_2(L)$ if and only if $E_1(K) \simeq E_2(K)$.

A result of Lenstra [6] relates the group structure of an elliptic curve over a finite field to the endomorphism ring of the curve. Specifically, if E is an ordinary elliptic curve defined over F, $\pi \in \mathrm{End}(E)$ the Frobenius endomorphism, and $[L : F] = k$, then

$$E(L) \simeq \mathrm{End}(E)/(\pi^k - 1). \tag{1}$$

A result of Kohel [5] states that for ordinary, ℓ-isogenous, elliptic curves E_1, E_2 defined over a finite field F with endomorphism rings $\mathcal{O}_1$ and $\mathcal{O}_2$, respectively, the endomorphism rings satisfy

$$[\mathcal{O}_1 : \mathcal{O}_2] = \ell^{\pm 1}, \text{ or } 1,$$

via the inclusion of endomorphism rings induced by the isogeny. In the former cases the isogeny is called **vertical**, while in the latter it is called **horizontal**.

In light of (1), any horizontally-isogenous elliptic curves will trivially have isomorphic groups of rational points over all finite extensions L/F (here we are using the fact that for ordinary elliptic curves all endomorphisms are defined over F). Therefore, for the remainder of the paper we will consider only vertical isogenies. A byproduct of our results in [2] is a general construction of pairs of elliptic curves that are vertically ℓ-isogenous (so they are neither isomorphic as curves, nor have isomorphic endomorphism rings) and yet have isomorphic groups of rational points in towers over F.

When $\ell = 2$ the situation is more complicated, as the following example from [2] and [4] illustrates.

Example 1.3. *Let $q = 257$, $F = \mathbf{F}_q$, and $L = \mathbf{F}_{q^2}$. Set*

$$E_1 : y^2 = x^3 + 90x + 101$$
$$E_2 : y^2 = x^3 + 196x + 159$$

and observe $E_2 = E_1/\langle(-10, 0)\rangle$, so E_1 and E_2 are 2-isogenous. One can check that

$$E_1(F)[2^\infty] \simeq E_2(F)[2^\infty] \simeq \mathbf{Z}/2 \times \mathbf{Z}/2,$$

but

$$E_2(L)[2^\infty] = \mathbf{Z}/4 \times \mathbf{Z}/16 \quad \textit{and} \quad E_2(L)[2^\infty] = \mathbf{Z}/8 \times \mathbf{Z}/8.$$

Therefore, in contrast to the case of odd ℓ, it is not enough to have $E_1(F) \simeq E_2(F)$ with non-trivial 2-Sylow subgroups to conclude that $E_1(L) \simeq E_2(L)$ for all L/F. In this paper we answer Question 1.1 for vertical 2-isogenies.

The proof of Theorem 1.2, Part (1) applies when $\ell = 2$ also, so it suffices to determine necessary and sufficient conditions for the 2-Sylow subgroups of $E_1(L)$ and $E_2(L)$ to be isomorphic when E_1 and E_2 are vertically 2-isogenous. Similarly as in [2], our main result can be viewed as a certificate for checking whether or not the groups $E_1(L)$ and $E_2(L)$ are isomorphic, for any finite extension L/F, based only on computations performed over F.

To put this paper into the context of related works, we recall that in [3] the authors determine necessary and sufficient conditions for elliptic curves E_1 and E_2 defined over a finite field F to have isomorphic groups of rational points in extensions L/F of degree k, for $k \geq 1$, extending the results of Wittman for $k = 1$. Our approach is different and focuses only on the case $\ell = 2$, in light of Theorem 1.2. In particular, we start with the hypothesis that the ℓ-Sylow subgroups of $E_1(F)$ and $E_2(F)$ are isomorphic and then ask about isomorphic groups of rational points in towers over F. The examples of [3] where the elliptic curves have isomorphic groups of rational points for certain extensions and not others stems from the fact that the curves they consider are ℓ-isogenous but do not possess a point of order ℓ over the ground field; it is only when the curves acquire an ℓ-torsion point in a finite extension that the groups are revealed to be non-isomorphic.

To state our main result precisely we set some preliminary notation which we will expand in Section 2. The endomorphism rings $\mathcal{O}_1$ and $\mathcal{O}_2$ of the ordinary elliptic curves E_1 and E_2 are orders in an imaginary quadratic number ring $\mathbf{Z}[\delta]$, where $\delta = \sqrt{d}$ if $d \equiv 2, 3 \pmod 4$ and $(1+\sqrt{d})/2$ if $d \equiv 1 \pmod 4$, for some negative, square-free, integer d. Write π for the Frobenius endomorphism and set

$$\pi = a + b\delta \in \mathbf{Z}[\delta].$$

As we will recall in Section 2, we can assume that a is odd and b is even. If g_1 and g_2 are the conductors of $\mathcal{O}_1$ and $\mathcal{O}_2$, respectively, then write $s_2 = \max\{v_2(g_1), v_2(g_2)\}$, where v_2 is the 2-adic valuation. Our main theorem can then be stated as follows.

Theorem 1.4. *Let E_1 and E_2 be ordinary, 2-isogenous elliptic curves defined over a finite field F such that the isogeny is also defined over F. Suppose $E_1(F) \simeq E_2(F)$. Let the endomorphism ring of each curve be an order in the quadratic imaginary ring $\mathbf{Z}[\delta]$ and write $\pi = a + b\delta \in \mathbf{Z}[\delta]$, where a is odd and b is even, for the Frobenius endomorphism. Then:*

(1) *if $v_2(a-1) > 1$, or if $v_2(a-1) = 1$ and $v_2(a+1) + 1 \leq v_2(b) - s_2$, then $E_1(L) \simeq E_2(L)$ for all finite extensions L/F, otherwise*

(2) $E_1(L) \simeq E_2(L)$ *for all odd-degree extensions* L/F *only.*

Just like in [2], this result can be viewed as a certificate for checking whether or not $E_1(L) \simeq E_2(L)$ for any finite extension L/F by performing an F-computation only. In fact, one way in which this result is simpler than the one in [2] is that if the 2-isogeny is defined over F, then E_1 and E_2 necessarily have non-trivial 2-Sylow subgroups over F. Therefore, one does not need to perform an initial base-field extension to check whether the ℓ-Sylow subgroups are isomorphic, as in the case of odd ℓ.

In the next section we give a brief background on isogenous elliptic curves and set up the necessary notation to prove Theorem 1.4. Section 3 is dedicated to the proof of Theorem 1.4. In Section 4 we address Question 1.1 for supersingular curves. Finally, we conclude with a remark that contextualizes our result in terms of isogeny volcanoes.

Acknowledgments. We thank the anonymous referee for a careful reading of the draft and detailed comments which improved the exposition and content of the paper.

2. Background and setup

We import much of the notation from [3]. Let E_1 and E_2 be ordinary ℓ-isogenous elliptic curves defined over a finite field F of characteristic coprime to ℓ. Let $\mathcal{O}_1$ and $\mathcal{O}_2$ be the endomorphism rings of E_1 and E_2, which can be viewed as orders in the imaginary quadratic ring $\mathbf{Z}[\delta]$, such that $\delta = \sqrt{d}$ if $d \equiv 2, 3 \pmod 4$ or $\delta = (1 + \sqrt{d})/2$ if $d \equiv 1 \pmod 4$. Associated to each elliptic curve is the Frobenius endomorphism π, which has the same representative in $\mathbf{Z}[\delta]$ for both curves; we write

$$\pi = a_1 + b_1\delta$$

for some $a_1, b_1 \in \mathbf{Z}$. For k a positive integer we have

$$\pi^k = a_k + b_k\delta,$$

for $a_k, b_k \in \mathbf{Z}$. The main result [3, Thm. 2.4] can then be stated as follows. If $[L : F] = k$, then

$$E_1(L) \simeq E_2(L) \Leftrightarrow v_2(a_k - 1) \leq v_2(b_k) - s_2 \tag{2}$$

where s_2 is a non-negative integer supported on a finite set of primes $\mathcal{P}$. It remains to describe the set $\mathcal{P}$ explicitly.

The endomorphism rings $\mathcal{O}_1$ and $\mathcal{O}_2$ are orders of conductor g_1 and g_2 in $\mathbf{Z}[\delta]$, respectively, and both g_1 and g_2 divide b_1. The fact that there is a vertical 2-isogeny between E_1 and E_2 means either $g_2/g_1 = 2$ or $g_1/g_2 = 2$. In general, the set $\mathcal{P}$ of [3, Thm. 2.4] is the set of primes p for which $v_p(g_1) \neq v_p(g_2)$ and

$$s_p = \max\{v_p(g_1), v_p(g_2)\}. \tag{3}$$

Because we are restricting to 2-isogenies, we have $\mathcal{P} \subseteq \{2\}$. However, because we assume the isogeny is vertical, $\mathcal{P}$ is nonempty and so we have $\mathcal{P} = \{2\}$. Since both g_1 and g_2 divide b, we have that b is even. By [3, Rmk. 2], a is coprime to the elements of $\mathcal{P}$ or else E would be supersingular.

Altogether, we seek necessary and sufficient conditions for (2) to hold when $\mathcal{P} = \{2\}$, b_k is even for all k and a_k is odd for all k (which follow from b_1 and a_1 being even and odd, respectively). This is the topic of Section 3 below. We conclude this section by observing that it suffices to restrict to the case where k is a power of 2.

Lemma 2.1. *Let E be an elliptic curve defined over a field K of odd characteristic. Let L/K be an extension of odd degree. Suppose that $E(F)[2]$ is nontrivial. Then $E(F)[2^\infty] = E(L)[2^\infty]$.*

Proof. If $E(F)[2]$ is nontrivial, then $E(F)$ achieves full 2-torsion in an extension F_2 of degree 2 or 1, depending on whether $E(F)[2]$ is cyclic or not, respectively. In general, the kernel of the reduction map $\mathrm{GL}(2, \mathbf{Z}/\ell^{n+1}) \to \mathrm{GL}(2, \mathbf{Z}/\ell^n)$ is isomorphic to $(\mathbf{Z}/\ell)^4$, hence the 2^n-torsion of E is defined over a 2-power extension of F_2. Thus if L/F has odd degree then $E(L)[2^\infty] = E(F)[2^\infty]$, as desired. □

Lemma 2.1 applies to our setup since by hypothesis the elliptic curves E_1 and E_2 are 2-isogenous by an F-rational isogeny, which means each curve has an F-rational 2-torsion point.

3. Proof of Theorem 1.4

Recall that throughout the paper we fix a finite field F of odd characteristic. Define the tower $\mathcal{L} = \{L_i/F\}_{i=0}^\infty$ where L_i is the unique extension of F of degree 2^i. Recalling our notation from Section 2, write $\pi^k = a_k + b_k\delta$ for $k \geq 1$. Then the Frobenius in the field L_i is π^{2^i} with representative

$$a_{2^i} + b_{2^i}\delta \in \mathbf{Z}[\delta].$$

An easy calculation shows that for $i \geq 1$,

$$(a_{2^i} - 1, b_{2^i}) = \left(a_{2^{i-1}}^2 - 1 + b_{2^{i-1}}^2 d, 2a_{2^{i-1}}b_{2^{i-1}}\right)$$

when $d \equiv 2, 3 \pmod 4$, and

$$(a_{2^i} - 1, b_{2^i}) = \left(a_{2^{i-1}}^2 - 1 + b_{2^{i-1}}^2 \left(\frac{d-1}{4}\right), 2a_{2^{i-1}}b_{2^{i-1}} + b_{2^{i-1}}^2\right)$$

when $d \equiv 1 \pmod 4$. The initial setup and the hypothesis $E_1(F) \simeq E_2(F)$ constrains the 2-valuations as follows. Since a_k is odd and b_k is even for all $k \geq 1$, we can write

$$a_1 - 1 = 2^n\alpha_1, \quad b_1 = 2^m\beta_1,$$

for some odd integers α_1 and β_1. Moreover, since $v_2(a_1 - 1) \leq v_2(b_1) - s_2$, we have

$$1 \leq n \leq m - s_2, \tag{4}$$

from which it follows that $m = v_2(b_1) \geq 2$, since $s_2 \geq 1$.

We have

$$v_2(b_{2^i}) = v_2(b_1) + i, \tag{5}$$

which follows immediately the formulas above and the fact that a_{2^i} is odd for all $i \geq 0$, when $d \equiv 2, 3 \pmod 4$. When $d \equiv 1 \pmod 4$, (5) is true as well, but uses both the fact that a_{2^i} is odd and that $m = v_2(b_1) \geq 2$, as established in the previous paragraph. The valuation $v_2(a_{2^i} - 1)$ is slightly more complicated, though when $n > 1$ we easily prove the following lemma.

Lemma 3.1. *With all notation as above, suppose $n > 1$. Then $E_1(F) \simeq E_2(F)$ if and only if $E_1(L) \simeq E_2(L)$ for all finite extensions L/F.*

Proof. One direction is trivial, so we assume $E_1(F) \simeq E_2(F)$. It suffices to show $E_1(L) \simeq E_2(L)$ for all $L \in \mathcal{L}$ by Lemma 2.1. Let $d' = d$ when $d \equiv 2, 3 \pmod 4$ and $(d-1)/4$ when $d \equiv 1 \pmod 4$. Then

$$v_2\left(a_2 - 1\right) = v_2(2^n\alpha_1(2^n\alpha_1 + 2) + 2^{2m}\beta_1^2 d') = n + 1 = v_2(a - 1) + 1,$$

because $2^{n-1}\alpha_1 + 1$ is odd and $2m > n + 1$. An easy induction argument shows

$$v_2\left(a_{2^i} - 1\right) = v_2(a_1 - 1) + i$$

for all $i \geq 0$. Combined with (5) and applying (2), this shows $E_1(L_i) \simeq E_2(L_i)$ for all $i \geq 0$, and the lemma is proved. □

If $n = 1$ then $2^n\alpha_1 + 2$ is divisible by 4, and so $v_2(a_2 - 1)$ might be strictly greater than $v_2(a_1 - 1) + 1$. If this happens, then we may have $E_1(L_1)[2^\infty] \not\simeq E_2(L_1)[2^\infty]$ even though $E_1(F) \simeq E_2(F)$. And since $E_1(L_1)$ (resp. $E_2(L_1)$) is a subgroup of $E_1(L)$ (resp. $E_2(L)$) for all $L \in \mathcal{L}$, we consequently have $E_1(L) \not\simeq E_2(L)$ for all $L \in \mathcal{L}$.

To see this phenomenon explicitly, write

$$a_1 + 1 = 2\alpha_1 + 2 = 2^\rho\alpha_1',$$

with $\rho \geq 2$. Then

$$v_2(a_2 - 1) = v_2(2^{\rho+1}\alpha_1\alpha_1' + 2^{2m}\beta_1^2 d') \geq \min(1 + \rho, 2v_2(b_1)), \tag{6}$$

while $v_2(b_2) = v_2(b_1) + 1$. In the next lemma we show that this potential "quadratic obstruction" is the only one that affects whether or not $E_1(L) \simeq E_2(L)$ for $L \in \mathcal{L}$. See Example 3.3 following the lemma for an example in coordinates.

Lemma 3.2. *With all notation as above, suppose $v_2(a_1 - 1) = 1$ and suppose $E_1(F) \simeq E_2(F)$. Then $E_1(L) \simeq E_2(L)$ for all $L \in \mathcal{L}$ if and only if $v_2(a_1 + 1) \leq v_2(b_1) - s_2$.*

Proof. If L_1 is the quadratic extension of F, then $E_1(L_1) \simeq E_2(L_1)$ if and only if $v_2(a_2-1) \leq v_2(b_2)-s_2$. As above, set $\rho = v_2(a_1+1)$ and $m = v_2(b_1)$. If $\rho > m-s_2$, then by (6) $v_2(a_2-1) \geq \min(\rho+1, 2m) > m+1-s_2 = v_2(b_2)-s_2$, and so $E_1(L_1) \not\simeq E_2(L_1)$. Since $E_1(L_1)$ (resp. $E_2(L_1)$) is a subgroup of $E_1(L_i)$ (resp. $E_2(L_i)$) for all $i > 0$, we conclude that $E_1(L_i) \not\simeq E_2(L_i)$ for all $i > 0$.

Conversely, suppose $\rho \leq m - s_2$. We first check that $E_1(L_1) \simeq E_2(L_1)$:

$$v_2(a_2 - 1) = v_2(a_1^2 - 1 + b_1^2 d') = v_2(2^{\rho+1}\alpha_1\alpha_1' + 2^{2m}\beta_1^2 d').$$

Since $\rho \leq m - s_2$, we have $\rho + 1 < 2m$ and so

$$v_2(a_2 - 1) = 1 + \rho \leq 1 + v_2(b_1) - s_2 = v_2(b_2) - s_2,$$

whence $E_1(L_1) \simeq E_2(L_1)$.

If $i = 2$, then

$$a_4 - 1 = \underbrace{(a_2 - 1)}_{v_2=\rho+1}\underbrace{(a_2 + 1)}_{v_2=1} + \underbrace{b_2^2}_{v_2=2m+2} d',$$

and so $v_2(a_4 - 1) = \rho + 2 = v_2(a_1 + 1) + 2$. By induction, for all $i \geq 2$ we have

$$v_2\left(a_{2^i} - 1\right) = v_2(a_1 + 1) + i.$$

Combined with (5), and the fact that $E_1(L_1) \simeq E_2(L_1)$, we get that $E_1(L) \simeq E_2(L)$ for all $L \in \mathcal{L}$. □

We conclude this section with two examples. First, we revisit Example 1.3 from the introduction to see the failure of the group isomorphism in towers in light of our main result.

Example 3.3 (Example 1.3, Revisited)**.** *Recall from above that $q = 257$, $F = \mathbf{F}_q$, and E_1 and E_2 are the 2-isogenous curves with Weierstrass equations*

$$E_1 : y^2 = x^3 + 90x + 101$$
$$E_2 : y^2 = x^3 + 196x + 159.$$

We compute $\pi = -9 + 4\sqrt{-11}$ so that $a_1 = -9$ and $b_1 = 4$.

The endomorphism algebra of each curve is $\mathbf{Q}(\sqrt{-11})$ and the fundamental discriminant of the maximal order is -11. The discriminant of $\mathbf{Z}[\pi]$ is $-64 \cdot 11$, hence the conductors g_1 and g_2 belong to the set $\{1, 2, 4, 8\}$ with either $g_1/g_2 = 2$ or $g_2/g_1 = 2$. Applying the methods of [1], we compute $s_2 = \max\{v_2(g_1), v_2(g_2)\} = 1$. With this pre-computation in place, we are in a position to apply our main results.

Observe

$$v_2(a_1 - 1) = 1 \leq 2 - 1 = v_2(b_1) - s_2,$$

so that $E_1(F) \simeq E_2(F)$. But now we check

$$v_2(a_1 + 1) = 3 > 1 = v_2(b_1) - s_2,$$

so $E_1(L_1) \not\simeq E_2(L_1)$, where L_1 is the unique quadratic extension of F. Since $E_i(L_1)$ is a subgroup of $E_i(L)$ for every $L \in \mathcal{L}$, we have $E_1(L) \not\simeq E_2(L)$ for all $L \in \mathcal{L}$. It follows that $E_1(K) \simeq E_2(K)$ only when $[K : F]$ is odd.

We remark that although we did not need to perform an L_1-computation to conclude that $E_1(L_1) \not\simeq E_2(L_2)$ (some of the impetus behind this paper was to perform F-computations only), it is worth pointing out that $v_2(a_1 - 1) = 1$ and $v_2(a_2 - 1) = v_2(-1856) = 6$. This large increase is behind the failure of $E_1(L_1)$ and $E_2(L_1)$ to be isomorphic, according to the results of [3].

Next, we revisit the motivating example of Wittmann [8, Appendix] in which he exhibits two non-isomorphic elliptic curves over a finite field F such that the groups $E_1(L) \simeq E_2(L)$ are isomorphic for any finite extension L/F. We examine this example in the context of Lemma 3.2.

Example 3.4. *Let $q = 73$ and $F = \mathbf{F}_q$. Let E_1 and E_2 be the elliptic curves over F with Weierstrass equations*

$$E_1 : \ y^2 = x^3 + 25x$$
$$E_2 : \ y^2 = x^3 + 53x + 55.$$

Then $E_2 = E_1/\langle(-11, 0)\rangle$ and so E_1 and E_2 are 2-isogenous. Additionally, he shows $\mathrm{End}(E_1) \simeq \mathbf{Z}[i]$ and $\mathrm{End}(E_2) \simeq \mathbf{Z}[2i]$ (so the isogeny is vertical), and

$$\pi = 3 + 8i.$$

Observe that $v_2(a_1 - 1) = 1$ and $m = v_2(b_1) = 3 \geq 2$ and so we are in a position to apply Lemma 3.2. Because the associated conductors g_1 and g_2 are equal to 1 and 2, respectively, we see that $s_2 = 1$ by (3). We then check

$$v_2(a_1 + 1) = 2 \leq 3 - 1 = v_2(b_1) - s_2$$

and conclude from Lemma 3.2 that $E_1(L) \simeq E_2(L)$ for all $L \in \mathcal{L}$, the 2-tower over F. Because the prime-to-2 parts of the groups $E_1(K)$ and $E_2(K)$ are isomorphic in all finite extensions K/F, we conclude that $E_1(K) \simeq E_2(K)$ for every finite extension K/F.

4. Supersingular curves

If E_1 and E_2 are supersingular, then the situation is potentially much different. Neither we in [2] nor the authors in [3] considered Question 1.1 in the context of supersingular curves, though in [8] the author worked out the group structure of supersingular curves in towers. In this section we attempt to consolidate known results and answer Question 1.1 for supersingular curves. We start by recalling the group structure in towers of supersingular curves defined over prime finite fields, as determined in [8].

Theorem 4.1 (Theorem 4.1 of [8])**.** *Let $E/\mathbf{F}_p$ be a supersingular elliptic curve. Then*

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

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*
$$E(\mathbf{F}_{p^{2k+1}}) \simeq \mathbf{Z}/(p^{2k+1}+1) \text{ and } \operatorname{End}_{\mathbf{F}_p}(E) \simeq \mathbf{Z}[\sqrt{-p}].$$
- *If* $p \equiv 3 \pmod 4$ *and* $E[2] \subseteq E(\mathbf{F}_p)$ *we have*
$$E(\mathbf{F}_{p^{2k+1}}) \simeq \mathbf{Z}/2 \times \mathbf{Z}/\left(\frac{p^{2k+1}+1}{2}\right) \text{ and } \operatorname{End}_{\mathbf{F}_p}(E) \simeq \mathbf{Z}[(1+\sqrt{-p})/2].$$

Using this result, we present the following corollary on supersingular, isogenous elliptic curves, regardless of the degree of the isogeny.

Corollary 4.2. *Let* p *be a prime number and* $\mathbf{F}_p$ *the field of* p *elements. 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* $K/\mathbf{F}_p$*.*

Proof. This is immediate: Theorem 4.1 shows that the group structure of a supersingular elliptic curve over a prime finite field determines uniquely, and with only one possibility, the group structure in any finite extension $K/\mathbf{F}_p$. □

If q is a power of a prime p, then we have the following theorem from [8]:

Theorem 4.3 (Theorem 4.2 of [8])**.** *Let* $E/\mathbf{F}_q$ *be supersingular.*

(a) *If* $\pi \in \mathbf{Z}$*, then* $E(\mathbf{F}_{q^k}) \simeq \mathbf{Z}/(\pi^k-1) \times \mathbf{Z}/(\pi^k-1)$.

(b) *Otherwise the groups of* $\mathbf{F}_{q^k}$*-rational points that occur are precisely*
$$\mathcal{O}_g/(\pi^k-1),$$
where $d = (q+1-\#E(\mathbf{F}_q))^2 - 4q < 0$*,* $K = \mathbf{Q}(\sqrt{d})$*, and* $\mathcal{O}_g$ *is the order of* $\mathcal{O}_K$ *of conductor* g*. Moreover, all orders* $\mathcal{O}_g$ *with* $\mathbf{Z}[\pi] \subseteq \mathcal{O}_g \subseteq \mathcal{O}_K$ *and* g *coprime to* p *occur.*

Remark 4.4. *In Theorem 4.3(a) the endomorphism ring of* E *has* $\mathbf{Z}$*-rank 4, while in (b) the endomorphism ring is an order in an imaginary quadratic number field.*

Similar to Corollary 4.2 above, we see that if $E/\mathbf{F}_q$ is supersingular with $\pi \in \mathbf{Z}$, then the group structure in towers over $\mathbf{F}_q$ is uniquely determined by the group structure over $\mathbf{F}_q$. The only unresolved case of Question 1.1 in the context of supersingular elliptic curve is the case of Theorem 4.3(b).

However, in this case we may now apply [2, Thm. 1] or Theorem 1.4 of the present work, depending on whether ℓ is odd or even. Indeed, the group structure of each curve is given by a quotient of an order in an imaginary quadratic number ring, where one ring is of index ℓ in the other, and the fact that the curves are supersingular is irrelevant. By our standing hypothesis, ℓ is coprime to the characteristic of the field, and so the conductor g will not equal ℓ (the only extra requirement of Theorem 4.3(b)).

To recap, the answer to Question 1.1 for supersingular curves is exactly the same as for ordinary curves when the endomorphism ring is an order in an imaginary quadratic number field and, in every other case, if $E_1(F) \simeq E_2(F)$, then $E_1(L) \simeq E_2(L)$ for all finite extensions L/F trivially, since the group structure over L is determined uniquely, and with only one possibility, by the group structure over F.

5. Remarks on volcanoes

The ℓ-isogeny graph of an elliptic curve over a finite field has a rich structure known as an **ℓ-volcano**. In this paper we did not use the structure of the 2-volcano to prove our main theorem, but, because it may be of independent interest, we give a brief description of the 2-volcanoes associated to the elliptic curves that we are studying in this paper. Our treatment is intentionally brief and we refer to [7] for an extensive background.

The ℓ-Sylow subgroup of an elliptic curve on the floor of an ℓ-volcano is cyclic of order ℓ^v, where $v = v_\ell(\#E(F))$. All of the elliptic curves on the first level of the volcano (so in the image of a vertical ℓ-isogeny from a curve on the floor) has ℓ-Sylow subgroup $\mathbf{Z}/\ell^{v-1} \times \mathbf{Z}/\ell$. This pattern continues: at the jth level up from the floor the ℓ-Sylow subgroup is $\mathbf{Z}/\ell^{v-j} \times \mathbf{Z}/\ell^j$. If the ℓ-Sylow subgroups are distinct at all levels, then the ℓ-volcano is called **regular**. If not, it is called **irregular**.

On an irregular volcano, there will necessarily be a level where the ℓ-Sylow subgroup equals $\mathbf{Z}/\ell^{v/2} \times \mathbf{Z}/\ell^{v/2}$ and will remain unchanged for all levels up to, and including, the crater. The minimum level for which the ℓ-Sylow subgroup has this structure is called the **stability level** of the volcano. Proofs of these assertions can be found in [4, §2].

When E_1 and E_2 are vertically ℓ-isogenous with $E_1(F) \simeq E_2(F)$, it must be the case that the ℓ-volcano of E_1 is irregular, otherwise it would be impossible for the ℓ-Sylow subgroups of the $E_i(F)$ to be isomorphic. Altogether, we can contextualize our result in terms of 2-volcanoes as follows:

Either both curves lie on the crater of the 2-isogeny volcano and we trivially have $E_1(L) \simeq E_2(L)$ for all extensions L/F, or the curves are vertically isogenous on an irregular volcano above the stability level. In the latter case, we either have $E_1(L) \simeq E_2(L)$ for all finite extensions L/F, or only for odd-degree extensions, where the distinction is determined by a computation over F.

References

[1] Bisson, Gaetan, Sutherland, Andrew V. Computing the endomorphism ring of an ordinary elliptic curve over a finite field. *J. Number Theory* **131** (2011) no. 5, 815 – 831. MR2772473, Zbl 1225.11085, arXiv:0902.4670, doi: 10.1016/j.jnt.2009.11.003. 213

[2] Cullinan, John. A remark on the group structure of elliptic curves in towers of finite fields. *New York J. Math.* **24** (2018) 856–864. MR3861038, Zbl 06957218. 207, 208, 209, 210, 214, 215

[3] Heuberger, Clemens, Mazzoli, Michela. Elliptic curves with isomorphic groups of points over finite field extensions. *J. Number Theory* **181** (2017), 89–98. MR3689671, Zbl 06772969, arXiv:1605.03474, doi: 10.1016/j.jnt.2017.05.028. 207, 209, 210, 211, 214

[4] Ionica, Sorina, Joux, Antoine. Pairing the volcano. *Math. Comp.* **82** (2013), no. 281, 581–603. MR2983037, Zbl 1278.11067, doi: 10.1090/S0025-5718-2012-02622-6. 208, 216

[5] Kohel, David Russell. Endomorphism rings of elliptic curves over finite fields. Thesis (Ph.D.) – University of California, Berkeley. 1996. 117 pp. ISBN: 978-0591-32123-4. MR2695524. 208

[6] Lenstra, Hendrik W., Jr. Complex multiplication structure of elliptic curves. *J. Number Theory* **56** (1996), no. 2, 227–241. MR1373549, Zbl 1044.11590, doi: 10.1006/jnth.1996.0015. 208

[7] Sutherland, Andrew V. Isogeny volcanoes. *ANTS X – Proceedings of the Tenth Algorithmic Number Theory Symposium*, 507–530. Open Book Ser., 1. *Math. Sci. Publ., Berkeley, CA*, 2013. MR3207429, Zbl 1345.11044, arXiv:1208.5370, doi: 10.2140/obs.2013.1.507. 216

[8] Wittmann, Christian. Group structure of elliptic curves over finite fields. *J. Number Theory* **88**, (2001), no. 2, 335–344. MR1832010, Zbl 1047.11062, doi: 10.1006/jnth.2000.2622. 207, 214, 215

(John Cullinan) Department of Mathematics, Bard College, Annandale-On-Hudson, NY 12504, USA
cullinan@bard.edu

This paper is available via http://nyjm.albany.edu/j/2020/26-10.html.