New York Journal of Mathematics

New York J. Math. **24** (2018) 856–864.

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

John Cullinan

Abstract. Let l be an odd prime, let F be a finite field of characteristic different from l and let A and B be l-isogenous elliptic curves defined over F. We study how the group structures of A(L) and B(L) vary in finite extensions L/F and prove that if the cardinality of the groups A(F) and B(F) are divisible by l and if A(F) and B(F) are isomorphic, then so are A(L) and B(L) for all finite extensions L of F.

Contents

1. Introduction

Let F be a finite field and let E_1 and E_2 be ordinary, isogenous, elliptic curves defined over F such that the isogeny $E_1 \to E_2$ is also defined over F. Because the curves are F-isogenous, by [8, Thm. 1] they have the same number of L-rational points for every finite extension L/F. The basic question we seek to address here is the following. Suppose $E_1(F)$ and $E_2(F)$ are isomorphic as groups. Under what conditions are $E_1(L)$ and $E_2(L)$ isomorphic as groups in a non-trivial finite extension L/F? We show (roughly) the only obstruction to the groups being isomorphic over L comes from the F-rational points of order dividing the degree of the isogeny between E_1 and E_2. We explain all of this in detail below.

This problem has been addressed previously in [9] and (building on those results) in [2]. Our results can be viewed as generalizing these two. Their main results are algorithms for determining when the groups $E_1(L)$ and $E_2(L)$ are isomorphic for a given finite extension L/F and can be summarized as follows. The Frobenius endomorphism of each curve has the same

Received May 4, 2018.
2010 *Mathematics Subject Classification.* 11G25, 14G15.
Key words and phrases. elliptic curve, finite field, isogeny.

ISSN 1076-9803/2018

representation as an element in an imaginary quadratic field K, though the endomorphism rings need not be isomorphic; writing π for Frobenius, set

$$\pi = a + b\sqrt{D_K} \in K,$$

for $a, b \in \mathbf{Z}$. Then, given a degree $n = [L : F]$, write $(a + b\sqrt{D_K})^n = a_n + b_n\sqrt{D_K}$ for $a_n, b_n \in \mathbf{Z}$. Depending on the prime divisors of the a_n and b_n, they determine whether $E_1(L)$ and $E_2(L)$ are isomorphic. As an extreme example, in [9, Appendix] the author provides an explicit triple (E_1, E_2, F) such that $E_1(L) \simeq E_2(L)$ for every finite extension L/F yet E_1 and E_2 are not isomorphic as elliptic curves. Another such example is given in [2, §3]. We will show in Section 4 below how to easily generate such examples.

The crux of this general question lies in the endomorphism rings of the elliptic curves. Our main reference is the following theorem of Lenstra which relates the group structure of E to that of its endomorphism ring. We quote the theorem here:

Theorem [5, Thm. 1]**.** *Let k be a finite field, let E be an elliptic curve over k, and put $R = \mathrm{End}_k E$. Let $\pi \in R$ be the Frobenius endomorphism of E. Further, let l be a finite field extension of k, and denote by $n = [l : k]$ its degree.*

(a) *Suppose that $\pi \notin \mathbf{Z}$. Then R has rank 2 over $\mathbf{Z}$, and there is an isomorphsim $E(l) \simeq R/R(\pi^n - 1)$ of R-modules.*

(b) *Suppose that $\pi \in \mathbf{Z}$. Then R has rank 4 over $\mathbf{Z}$, we have $E(l) \simeq \mathbf{Z}/\mathbf{Z}(\pi^n - 1) \oplus \mathbf{Z}/\mathbf{Z}(\pi^n - 1)$ as abelian groups, and this group has, up to isomorphism, exactly one left R-module structure. Furthermore, one has $E(l) \oplus E(l) \simeq R/R(\pi^n - 1)$ as R-modules.*

Remark. We focus exclusively on the case of ordinary elliptic curves, so we will not use Part (b) of Lenstra's theorem. Moreover, we use the notation F for his k and L for his l. We thus write

$$E(L) = \frac{\mathrm{End}_k(E)}{(\pi^n - 1)}. \tag{1}$$

In the aforementioned examples of [9] and [2], the elliptic curves E_1 and E_2 are distinct orders in an imaginary quadratic field, yet the quotients $\mathrm{End}_k(E_1)/(\pi^n - 1)$ and $\mathrm{End}_k(E_2)/(\pi^n - 1)$ are isomorphic for all positive integers n. Our approach in this note is to relate the degree of the isogeny between E_1 and E_2 to the group structures in towers.

We now set and fix our notation for the remainder of the paper. Fix an odd prime ℓ and suppose that the characteristic of F is different from ℓ. Let E_1 and E_2 be ℓ-isogenous elliptic curves defined over F such that the isogeny is defined over F as well. We first show that in every finite extension L/F the prime-to-ℓ parts of the groups $E_1(L)$ and $E_2(L)$ are isomorphic, so it suffices to compare the ℓ-Sylow subgroups. Assuming the ℓ-Sylow subgroups of $E_1(F)$ and $E_2(F)$ are non-trivial, we show that if $\mathrm{Syl}_\ell(E_1(F)) \simeq \mathrm{Syl}_\ell(E_2(F))$ then $E_1(L) \simeq E_2(L)$ for all finite extensions

L/F. In other words, our result can be taken as a certificate for checking whether the groups $E_1(L)$ and $E_2(L)$ are isomorphic: perform a base-field extension (possibly trivial) so that $E_1(F)$ and $E_2(F)$ acquire an ℓ-torsion point. Then if $\mathrm{Syl}_\ell(E_1(F)) \simeq \mathrm{Syl}_\ell(E_2(F))$, we have $E_1(L) \simeq E_2(L)$ for all finite extensions L/F (the converse of this statement is trivial):

Theorem 1. *Let ℓ be an odd prime, F a finite field of characteristic different from 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 interesting examples raised by Theorem 1 are those curves which have distinct endomorphism rings but, in view of Lenstra's structure theorem, have isomorphic groups of rational points. We obtain our results by exploiting the structure of the ℓ-isogeny volcano V_E, viewing the curves E_1 and E_2 as adjacent vertices. In the next section we review the relevant background on elliptic curves. We then split the proof of Theorem 1 over the following two sections, focusing first on the prime-to-ℓ part of the groups and then on the ℓ-Sylow subgroups.

Acknowledgments. We would like to thank Andrew Sutherland for helpful email discussions and Keith Conrad for pointing us to the proof of Lemma 2. We would also like to thank the anonymous referee for a careful reading of the draft and detailed comments which improved the exposition and content of the paper.

2. Ordinary endomorphism rings

Here we recall some background information on endomorphism rings of elliptic curves; for more details see [1]. We also make use of the language of *isogeny volcanoes* and refer to [7] for the relevant background and definitions.

The endomorphism ring $\mathrm{End}(E)$ of an ordinary elliptic curve E over a finite field F of cardinality q is an order $\mathcal{O}$ in an imaginary quadratic number field K. Let u be the conductor of $\mathcal{O} \subset \mathcal{O}_K$. Writing π for the Frobenius endomorphism of E (viewed as an element of $\mathcal{O}$) we have the representation, following the notation of [1]:

$$\pi = \frac{t + v\sqrt{D_K}}{2},$$

where D_K is the discriminant of $\mathcal{O}_K$, v is the conductor of $\mathbf{Z}[\pi] \subset \mathcal{O}_K$, and t is the trace of π, all subject to the relation $4q = t^2 - v^2 D_K$. Let $D_\mathcal{O}$ denote the discriminant of $\mathcal{O}$ and D_π the discriminant of $\mathbf{Z}[\pi]$. Then the orders satisfy the containments

$$\mathbf{Z}[\pi] \subset \mathcal{O} \subset D_K,$$

and the discriminants are related by $D_{\mathcal{O}} = u^2 D_K$ and $D_\pi = v^2 D_K$, where $u \mid v$ and uniquely determines $\mathcal{O}$.

If E_1 and E_2 are ordinary, F-isogenous, elliptic curves defined over F with endomorphism rings $\mathcal{O}_1$ and $\mathcal{O}_2$, then they have the "same" π viewed as an element of $\mathcal{O}_K$. Moreover, because E_1 and E_2 are isogenous over F, the groups $E_1(L)$ and $E_2(L)$ have the same cardinality for all finite extensions L/F [8, Thm. 1]. However, it might not be the case that $\mathcal{O}_1 = \mathcal{O}_2$. In the special case where the degree of the isogeny is a prime number ℓ, we have the following theorem of Kohel which we will use extensively in the following sections (in the statement of the theorem $\mathcal{O}$ denotes the endomorphism ring of E):

Theorem [4, Prop. 21]**.** *Let E/k be an ordinary elliptic curve over the finite field k. Let $\varphi : E \to E'$ be an isogeny of prime degree ℓ different from the characteristic of k. Then $\mathcal{O}$ contains $\mathcal{O}' = \mathrm{End}(E')$ or $\mathcal{O}'$ contains $\mathcal{O}$ in K and the index of one in the other divides ℓ.*

Using the notation of our paper, if the isogeny $E_1 \to E_2$ has prime degree ℓ, then either $\mathcal{O}_1 = \mathcal{O}_2$, $[\mathcal{O}_1 : \mathcal{O}_2] = \ell$, or $[\mathcal{O}_2 : \mathcal{O}_1] = \ell$. In each case we say the isogeny $E_1 \to E_2$ is *horizontal*, *descending*, or *ascending*, respectively. In terms of the *ℓ-volcano* V_E, the vertices along the crater are joined by horizontal isogenies, while those on the *volcanoside* are related by ascending or descending isogenies; vertices on the floor of the volcano only admit ascending isogenies. With a view toward the group structures of ℓ-isogenous curves, we recall [6, Thm. 3] which determines the ℓ-Sylow subgroups of the vertices of V_E. Since we use their conventions in Section 4, we remind the reader that the authors in [6] label an ℓ-volcano as follows: the vertices are partitioned into levels $V_0, \ldots, V_h$ with the crater at level V_0 and the floor at level V_h; the vertices on the floor correspond to curves with cyclic ℓ-Sylow subgroup.

Theorem [6, Thm. 3]**.** *Let E be an elliptic curve over $\mathbf{F}_q$ of order m with $\nu = \nu_\ell(m) \geq 1$. Then the volcano V_E satisfies:*

1. *The ℓ-Sylow subgroup of the curves on the floor is $\mathbf{Z}/\ell^\nu\mathbf{Z}$.*
2. *If ν is odd, the ℓ-Sylow subgroup of the curves on the i-th level is $\mathbf{Z}/\ell^{\nu-i}\mathbf{Z} \times \mathbf{Z}/\ell^i\mathbf{Z}$.*
3. *If ν is even, the ℓ-Sylow subgroup of the curves on the i-th level is $\mathbf{Z}/\ell^{\nu-i}\mathbf{Z} \times \mathbf{Z}/\ell^i\mathbf{Z}$ for $1 \leq i \leq \nu/2$. Moreover, for the rest of levels (if any) until reaching the crater, the structure is $\mathbf{Z}/\ell^{\nu/2}\mathbf{Z} \times \mathbf{Z}/\ell^{\nu/2}\mathbf{Z}$.*

If ν is even and the height h is greater than ν, the authors in [6] refer to the level $\nu/2$ (as in Case (3)) as the *stability level*. We go further and call the levels between the crater and the stability level the *stability zone*. We split our study of the group structures of isogenous curves over the next two sections, beginning with the prime-to-ℓ part of the group. We will make use of [6, Thm. 3] in Section 4 when we consider the ℓ-Sylow subgroups.

3. A ring-theoretic lemma

The main result of this section is a lemma on the quotients of orders in an algebraic number field. We then apply the result to the case of endomorphism rings of elliptic curves over finite fields.

Lemma 2. *Let K be an algebraic number field and let $\mathcal{O}_1 \subset \mathcal{O}_2$ be orders in K with $[\mathcal{O}_2 : \mathcal{O}_1] = m \geq 1$. Let $x \in \mathcal{O}_1$ be non-zero. Then, the prime-to-m parts of the finite groups $\mathcal{O}_1/x\mathcal{O}_1$ and $\mathcal{O}_2/x\mathcal{O}_2$ are isomorphic.*

Proof. For non-zero $x \in \mathcal{O}_1$, there is a ring homomorphism

$$\varphi : \mathcal{O}_1/x\mathcal{O}_1 \to \mathcal{O}_2/x\mathcal{O}_2.$$

Both rings have size $|N_{K/\mathbf{Q}}(x)|$. Viewing $\mathcal{O}_1/x\mathcal{O}_1$ and $\mathcal{O}_2/x\mathcal{O}_2$ as abelian groups, we will show φ is an isomorphism between the subgroups of elements of order relatively prime to m. It suffices to prove for each prime p not dividing m that the map φ defines an isomorphism between the subgroups of elements with p-power order (it obviously maps one such subgroup to the other). Since the groups $\mathcal{O}_1/x\mathcal{O}_1$ and $\mathcal{O}_2/x\mathcal{O}_2$ have equal size, their subgroups of elements of p-power order have equal size. So it suffices to show the natural map between these p-subgroups is surjective.

In addition to φ, consider the additive map

$$\psi : (\mathcal{O}_2/x\mathcal{O}_2)[p^\infty] \to (\mathcal{O}_1/x\mathcal{O}_1)[p^\infty],$$

where $\psi(a \mod x\mathcal{O}_2) = ma \mod x\mathcal{O}_1$ (which is well-defined since $m\mathcal{O}_2 \subset \mathcal{O}_1$). Then $\varphi(\psi(t)) = mt$ for all $t \in (\mathcal{O}_2/x\mathcal{O}_2)[p^\infty]$. Multiplication by m on the p-group $(\mathcal{O}_2/x\mathcal{O}_2)[p^\infty]$ is an automorphism, so φ is surjective. □

Corollary 3. *Let E_1 and E_2 be ordinary, ℓ-isogenous, elliptic curves over a finite field F. Then the prime-to-ℓ parts of the groups $E_1(L)$ and $E_2(L)$ are isomorphic for every finite extension L/F.*

Proof. Since E_1 and E_2 are ordinary, their endomorphism rings $\mathcal{O}_1$ and $\mathcal{O}_2$ are orders in a quadratic number field. For $i \in \{1, 2\}$, the group structure of $E_i(L)$ is isomorphic (as groups) to that of $\mathcal{O}_i$ modulo the principal ideal $(\pi^n - 1)$, where π is the Frobenius endomorphism of E_i and $n = [L : F]$. Finally, by [4, Prop. 21], because the E_i are ℓ-isogenous the rings $\mathcal{O}_i$ satisfy $\mathcal{O}_1 = \mathcal{O}_2$, $[\mathcal{O}_2 : \mathcal{O}_1] = \ell$, or $[\mathcal{O}_1 : \mathcal{O}_2] = \ell$. The corollary now follows from Lemma 2. □

In light of Corollary 3, it suffices to focus on how the ℓ-Sylow subgroups of the $E_i(L)$ vary in extensions L/F.

4. The ℓ-Sylow subgroup

We continue with the setup from the previous sections but now restrict to the case where the characteristic of F does not equal ℓ so that we may apply the results of [3] and [6]. If the ℓ-Sylow subgroups of the $E_i(F)$ are trivial, then by Corollary 3 the groups $E_1(F)$ and $E_2(F)$ are isomorphic.

Since the extension $F(E[\ell])/F$ is an (abelian) extension with Galois group a subgroup of $\mathrm{GL}_2(\mathbf{Z}/\ell)$, the E_i can only acquire an ℓ-torsion point in an extension L/F such that $[L : F] \mid \ell(\ell-1)$. Therefore, for any extension L/F with $[L : F]$ coprime to $\ell(\ell-1)$ the groups $E_1(L)$ and $E_2(L)$ will be isomorphic. We therefore reduce to the case where the ℓ-Sylow subgroups of the $E_i(F)$ are non-trivial and consider separately the cases where they have odd versus even ℓ-divisibility. We write $\nu_\ell(m)$ for the ℓ-adic valuation of an integer m.

Before continuing with the main results of this section, we recall the results of [3, Props. 4.1 & 4.2] which we will make use of several times below. We summarize the relevant portions as follows:

Let ℓ be an odd prime and q a power of a prime different from ℓ. Let $E/\mathbf{F}_q$ be an elliptic curve and suppose $E[\ell^\infty](\mathbf{F}_q) \simeq \mathbf{Z}/\ell^{n_1}\mathbf{Z} \times \mathbf{Z}/\ell^{n_2}\mathbf{Z}$ with $n_1 \geq 1$. Then

(1) The smallest extension K of $\mathbf{F}_q$ such that $E[\ell^\infty](K)$ is not isomorphic to $E[\ell^\infty](\mathbf{F}_q)$ is $\mathbf{F}_{q^\ell}$, and
(2) If $n_2 \geq 1$ then $E[\ell^\infty](\mathbf{F}_{q^\ell}) \simeq \mathbf{Z}/\ell^{n_1+1}\mathbf{Z} \times \mathbf{Z}/\ell^{n_2+1}\mathbf{Z}$.

Proposition 4. *Let ℓ be odd. Suppose E_1 and E_2 are ordinary, ℓ-isogenous, elliptic curves defined over a finite field F of characteristic different from ℓ with $\nu_\ell(\#E_i(F))$ odd. Then, either $E_1(L) \simeq E_2(L)$ for all finite extensions L/F, or $E_1(L) \not\simeq E_2(L)$ for all finite extensions L/F.*

Proof. By Corollary 3, the groups $E_1(F)$ and $E_2(F)$ are isomorphic if and only if their ℓ-Sylow subgroups are. Since $\nu_\ell(\#E_i(F))$ is odd, we apply [6, Thm. 3], part (2): all vertically isogenous curves have non-isomorphic ℓ-Sylow subgroups and all horizontally isogenous curves (tautologically) have isomorphic ℓ-Sylow subgroups. Since the isogeny $E_1 \to E_2$ is defined over F, whether it is horizontal or vertical is unchanged when performing a base-field extension. Moreover, since the E_i are ordinary, all $\overline{F}$-endomorphisms are defined over F [5, §4] and so the endomorphism rings of Lenstra's structure theorem (1) remain unchanged under base-field extensions as well.

Now compare the groups $E_1(L)$ and $E_2(L)$ for any finite extension L/F. If E_1 and E_2 are horizontally isogenous over F, then they are horizontally isogenous over L and hence the groups $E_1(L)$ and $E_2(L)$ are isomorphic. If the curves are vertically isogenous, then the subgroups $E_1(F)$ and $E_2(F)$ are non-isomorphic whence $E_1(L)$ and $E_2(L)$ are non-isomorphic. □

Proposition 5. *Let ℓ be odd and $\nu_\ell(\#E_i(F)) > 0$ be even. If E_1 and E_2 represent adjacent vertices on the volcano V_E with least one of the E_i outside of the stability zone, then for all L/F the groups $E_1(L)$ and $E_2(L)$ are not isomorphic. If E_1 and E_2 are both within the stability zone, then $E_1(L) \simeq E_2(L)$ for all extensions L/F.*

Proof. If one of E_1 or E_2 is outside the stability zone, or if both E_1 and E_2 are on the crater, then the same argument as in the proof of Proposition 4

applies here to get the desired conclusion. We are left with the case when E_1 and E_2 are inside the stability zone, but at least one of the E_i is not on the crater so that the E_i are vertically isogenous.

Because E_1 and E_2 both lie in the stability zone, the ℓ-Sylow subgroups of $E_1(F)$ and $E_2(F)$ are isomorphic and we can write

$$E_1[\ell^\infty](F) \simeq E_2[\ell^\infty](F) \simeq \mathbf{Z}/\ell^{n_1}\mathbf{Z} \times \mathbf{Z}/\ell^{n_2}\mathbf{Z},$$

with $n_1, n_2 \geq 1$. Now apply [3, Props. 4.1 & 4.2]: if L/F is a field extension with $[L : F]$ coprime to ℓ, then it cannot have a subfield of ℓ-power degree over F, hence the ℓ-Sylow subgroups of the $E_i(L)$ are isomorphic to those of $E_i(F)$. Since the prime-to-ℓ parts of the $E_i(L)$ are isomorphic, it follows that $E_1(L) \simeq E_2(L)$.

If $\mathrm{ord}_\ell([L : F]) = k$, then by repeated applications of [3, Props. 4.1 & 4.2] we have

$$E_1[\ell^\infty](L) \simeq E_2[\ell^\infty](L) \simeq \mathbf{Z}/\ell^{n_1+k}\mathbf{Z} \times \mathbf{Z}/\ell^{n_2+k}\mathbf{Z},$$

and so we have $E_1(L) \simeq E_2(L)$ in this case as well. □

Together, Corollary 3 and Propositions 4 and 5 constitute a proof of Theorem 1.

Remarks.

(1) The case where the ℓ-adic valuation of the $E_i(F)$ is odd is less interesting because either the $E_i(F)$ are non-isomorphic (and hence all base extensions are non-isomorphic), or the endomorphism rings coincide; by Lenstra's structure theorem the groups are isomorphic in all towers over F.

(2) As an alternate proof of Proposition 5 that would avoid the connection with volcanoes, we could have combined the criterion of [2, Thm. 2.7] with the results [3, Props. 4.1 & 4.2] to determine when the groups $E_1(L)$ and $E_2(L)$ are non-isomorphic. The key observation is that the quantity 'e' of [2, Thm. 2.7] divides $\ell - 1$ but must also be a power of ℓ by [3, Props. 4.1 & 4.2]. A short argument would complete the proof.

(3) When $\ell = 2$, [3, Props. 4.1 & 4.2] do not necessarily apply, as evidenced by the following example, generalized from [3, Ex. 4.4]. Let $F = \mathbf{F}_{257}$ and $L = \mathbf{F}_{257^2}$. Set

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

Note that $E_2 = E_1/\langle(-10,0)\rangle$ so $E_1 \to E_2$ is a 2-isogeny. Then one can check that

$$E_1(F)[2^\infty] = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \quad \text{and} \quad E_1(L)[2^\infty] = \mathbf{Z}/2^2\mathbf{Z} \times \mathbf{Z}/2^4\mathbf{Z},$$
$$E_2(F)[2^\infty] = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \quad \text{and} \quad E_2(L)[2^\infty] = \mathbf{Z}/2^3\mathbf{Z} \times \mathbf{Z}/2^3\mathbf{Z}.$$

(4) Recall [2, Ex. 3.2]: Let $q = 3329$, $F = \mathbf{F}_q$, and consider the three elliptic curves

$$E_0 : y^2 = x^3 + 99x$$
$$E_1 : y^2 = x^3 + x + 72$$
$$E_2 : y^2 = x^3 + x + 192.$$

They show $E_0(\mathbf{F}_{q^n}) \simeq E_1(\mathbf{F}_{q^n})$ if and only if $4 \nmid n$, $E_1(\mathbf{F}_{q^n}) \simeq E_2(\mathbf{F}_{q^n})$ if and only if $4 \nmid n$, and $E_0(\mathbf{F}_{q^n}) \simeq E_2(\mathbf{F}_{q^n})$ for all n. The endomorphism rings are given respectively by $\mathcal{O}_0 = \mathbf{Z}[i]$, $\mathcal{O}_1 = \mathbf{Z}[25i]$ and $\mathcal{O}_2 = \mathbf{Z}[5i]$.

We reconsider this example now in light of our results. None of the E_i have $\mathbf{F}_q$-rational 5-torsion and only achieve 5-torsion after a base extension of degree 4. Thus $\nu = 0$ for the $E_i(\mathbf{F}_q)$ and one can check that the $E_i(\mathbf{F}_q)$ are cyclic of order 3226. Over $\mathbf{F}_{q^4}$ we check

- $E_0(\mathbf{F}_{q^4}) \simeq E_2(\mathbf{F}_{q^4}) \simeq \mathbf{Z}/1040\mathbf{Z} + \mathbf{Z}/118092375440\mathbf{Z}$
- $E_1(\mathbf{F}_{q^4}) \simeq \mathbf{Z}/208\mathbf{Z} + \mathbf{Z}/590461877200\mathbf{Z}$,

so that for $E_i(\mathbf{F}_{q^4})$ we have $\nu = 2$. The ℓ-volcano has height 2 and we see that that E_0 lies on the crater because it has maximal endomorphism ring, and the 5-isogenies $E_0 \to E_2 \to E_1$ are descending; note that E_1 lies on the floor since its 5-Sylow subgroup is cyclic.

The curves E_0 and E_2 lie in the stability zone of this volcano and since $E_0(\mathbf{F}_{q^4}) \simeq E_2(\mathbf{F}_{q^4})$, it follows from Proposition 5 that $E_0(\mathbf{F}_{q^{4k}}) \simeq E_2(\mathbf{F}_{q^{4k}})$ for all positive integers k. Moreover, this shows that $E_0(L) \simeq E_2(L)$ for all L in the tower

$$\mathbf{F}_q \subset \mathbf{F}_{q^4} \subset \mathbf{F}_{q^8} \subset \cdots \subset \mathbf{F}_{q^{4k}} \subset \cdots$$

If $M/\mathbf{F}_q$ is an extension that does not lie in this tower, then the $E_i(M)$ will have trivial 5-Sylow subgroup and by Corollary 3 the groups $E_0(M)$ and $E_2(M)$ will be isomorphic. It follows that over all finite extensions K/F the groups $E_0(K)$ and $E_2(K)$ are isomorphic.

On the other hand, a similar argument shows that $E_1(L)$ and $E_2(L)$ are never isomorphic for any finite extension $L/\mathbf{F}_{q^4}$ because E_1 lies outside the stability zone. If $M/\mathbf{F}_q$ is an extension that does not lie in the tower above $\mathbf{F}_{q^4}$ then the 5-Sylow subgroups of $E_1(M)$ and $E_2(M)$ are trivial and so $E_1(M) \simeq E_2(M)$ by Corollary 3 again. Together, this recovers the results of [2, Ex. 3.2].

This gives another example of the type introduced by Wittman in [9, Appendix], since the endomorphism rings of E_1 and E_0 are distinct (in his example, the isogeny in question has degree 2). It is now easy to generalize this to create new examples of curves over finite fields with distinct endomorphism rings that nonetheless have isomorphic groups of rational points in towers.

(5) As stated, Propositions 4 and 5 do not apply in the case of 2-isogenies, a difficulty which has already been alluded to in [2, Thm. 2.7]. It would be interesting to obtain an analog of Propositions 4 and 5 in the case of 2-isogenies.

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. 858

[2] 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. 856, 857, 862, 863, 864

[3] Ionica, Sorina; Joux, Antoine. Pairing the volcano. *Math. Comp.* **82** (2013), no. 281, 581–603. MR2983037, Zbl 1278.11067, arXiv:1110.3602, doi: 10.1090/S0025-5718-2012-02622-6. 860, 861, 862

[4] 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. 859, 860

[5] 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. 857, 861

[6] Miret, Josep M.; Sadornil, Daniel; Tena Ayuso, Juan G.; Tomàs, R.; Valls, Magda. Volcanoes of l-isogenies of elliptic curves over finite fields: the case $l = 3$. *Publ. Mat.* 2007, Proceedings of the Primeras Jornadas de Teoría de Números, 165–180. MR2499692, Zbl 1166.14023, doi: 10.5565/PUBLMAT_PJTN05_08. 859, 860, 861

[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. 858

[8] Tate, John. Endomorphisms of abelian varieties over finite fields. *Invent. Math.* **2** (1966), 134–144. MR0206004, Zbl 0147.20303, doi: 10.1007/BF01404549. 856, 859

[9] 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. 856, 857, 864

(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/2018/24-39.html.