JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Andrew V. SUTHERLAND

A local-global principle forrational isogenies of prime degree

Tome 24, n° 2 (2012), p. 475-485.

<http://jtnb.cedram.org/item?id=JTNB_2012__24_2_475_0>

Journal de Théorie des Nombres
de Bordeaux **24** (2012), 475-485

A local-global principle for rational isogenies of prime degree

par Andrew V. SUTHERLAND

Résumé. Soit K un corps de nombres. Nous étudions un principe local-global pour les courbes elliptiques E/K admettant ou non une isogénie rationnelle de degré premier ℓ. Pour des corps K convenables (dont $K = \mathbb{Q}$), nous démontrons ce principe pour tout $\ell \equiv 1 \bmod 4$ et tout $\ell < 7$ mais exhibons une courbe elliptique d'invariant modulaire $2268945/128$ comme contre-exemple pour $\ell = 7$. Nous montrons alors qu'il s'agit du seul contre-exemple à isomorphisme près lorsque $K = \mathbb{Q}$.

Abstract. Let K be a number field. We consider a local-global principle for elliptic curves E/K that admit (or do not admit) a rational isogeny of prime degree ℓ. For suitable K (including $K = \mathbf{Q}$), we prove that this principle holds for all $\ell \equiv 1 \bmod 4$, and for $\ell < 7$, but find a counterexample when $\ell = 7$ for an elliptic curve with j-invariant $2268945/128$. For $K = \mathbf{Q}$ we show that, up to isomorphism, this is the only counterexample.

Introduction

Let E be a non-singular elliptic curve defined over a number field K, and let ℓ be a prime number. We say that E admits an ℓ-isogeny over K if there is an isogeny $\phi\colon E \to E'$ of degree ℓ defined over K. If $\mathfrak{p}$ is a prime of K where E has good reduction, we say that E admits an ℓ-isogeny locally at $\mathfrak{p}$ if the reduction of E modulo $\mathfrak{p}$ admits an isogeny of degree ℓ defined over the residue field.

If E admits an ℓ-isogeny over K, then E necessarily admits an ℓ-isogeny locally everywhere, that is, at every prime of good reduction. We ask the converse:

If E admits an ℓ-isogeny locally everywhere,
must E admit an ℓ-isogeny over K?

Manuscrit reçu le 24 avril 2011.
Mots clefs. elliptic curve, isogeny, local-global principle.
Classification math. 11G05.

We can immediately answer this question with a counterexample. Consider the elliptic curve $E/\mathbf{Q}$ defined by the Weierstrass equation

$$y^2 + xy = x^3 - x^2 - 107x - 379. \tag{0.1}$$

This curve admits a 7-isogeny locally at every prime of good reduction (and over $\mathbf{R}$) but it does not admit a 7-isogeny over $\mathbf{Q}$. We note that E does admit a 7-isogeny over a quadratic extension of $\mathbf{Q}$. Our first theorem implies that this is necessarily the case, as is the fact that we used a prime $\ell \equiv 3 \bmod 4$.

Theorem 1. *Assume $\sqrt{(\frac{-1}{\ell})\ell} \notin K$, and suppose E/K admits an ℓ-isogeny locally at a set of primes with density one. Then E admits an ℓ-isogeny over a quadratic extension of K, and if $\ell \equiv 1 \bmod 4$ or $\ell < 7$, then E admits an ℓ-isogeny over K.*

Whether an elliptic curve admits an ℓ-isogeny over K (or not) depends only on its j-invariant $j(E)$, which uniquely identifies its isomorphism class over any algebraic closure of K. Let us call a pair $(\ell, j(E))$ exceptional if E/K admits an ℓ-isogeny locally everywhere, but not over K. The pair $(7,\ 2268945/128)$ corresponds to the counterexample above. Theorem 1 admits the possibility of infinitely many exceptional pairs, and this occurs, for example, when $K = \mathbf{Q}(i)$. However, it does not happen when $K = \mathbf{Q}$.

Theorem 2. *The pair $(7,\ 2268945/128)$ is the only exceptional pair for $\mathbf{Q}$.*

The analogous local-global question for ℓ-torsion was addressed by Katz in [8]. In general, an elliptic curve E/K with non-trivial ℓ-torsion locally everywhere may have trivial ℓ-torsion over K. However, Katz shows that such an E must be rationally isogenous to an elliptic curve which has non-trivial ℓ-torsion over K. He proves this by reducing the problem to a purely group-theoretic statement, an approach advocated by Mazur [8, p. 483].

We take a similar line in our treatment of Theorem 1, using a Galois representation to reduce the problem to a question regarding the structure of certain subgroups of $\mathrm{GL}_2(\mathbf{F}_\ell)$, which we are then able to address with purely elementary methods. The proof of Theorem 2 requires more, and here we also use the theory of complex multiplication and, crucially, a theorem of Parent [12] that characterizes the rational points on the modular curve $X_0^+(\ell^2)(\mathbf{Q})$ for certain values of ℓ.

1. Preliminaries

1.1. Galois representations. We follow the notation in [11]. Let us fix a number field K with algebraic closure $\overline{K}$. If S is a finite set of non-archimedean primes of K, let $\overline{K}_S$ denote the maximal algebraic extension of K in $\overline{K}$ unramified outside of S. Given an elliptic curve E/K and a prime number ℓ, the absolute Galois group $G_K = \mathrm{Gal}(\overline{K}/K)$ acts on the

group of ℓ-torsion points $E[\ell]$. Provided S contains the primes that divide ℓ, and the primes where E has bad reduction, this action factors through $G_{K,S} = \mathrm{Gal}(\overline{K}_S/K)$, yielding a representation

$$\rho_{E,\ell}\colon G_{K,S} \to \mathrm{Aut}(E[\ell]) \cong \mathrm{GL}_2(\mathbf{Z}/\ell\mathbf{Z}) \cong \mathrm{GL}_2(\mathbf{F}_\ell).$$

If $\mathfrak{p}$ is a non-archimedean prime of K not in S with residue field $k_\mathfrak{p}$, let $\varphi_\mathfrak{p}$ denote the $|k_\mathfrak{p}|$-power Frobenius automorphism, which we may view as an element of $G_{K,S}$ with the understanding that it is determined only up to conjugacy. We identify the image of $\varphi_\mathfrak{p}$ under $\rho_{E,\ell}$ as a conjugacy class $\varphi_{\mathfrak{p},\ell}$ of $\mathrm{GL}_2(\mathbf{F}_\ell)$, and we have

$$\det(\varphi_{\mathfrak{p},\ell}) \equiv |k_\mathfrak{p}| \bmod \ell, \qquad \mathrm{tr}(\varphi_{\mathfrak{p},\ell}) \equiv |k_\mathfrak{p}| + 1 - |E(k_\mathfrak{p})| \bmod \ell.$$

The Chebotarev density theorem implies that each conjugacy class $\varphi_{\mathfrak{p},\ell}$ in G arises for a set of primes with density $|\varphi_{\mathfrak{p},\ell}|/|G| > 0$.

1.2. Subgroups of $\mathbf{GL_2(F_\ell)}$. We recall some of the classical subgroups of $\mathrm{GL}_2(\mathbf{F}_\ell)$. A *Cartan* subgroup is an absolutely semisimple maximal abelian subgroup, of which there are two types. A *split* Cartan subgroup is isomorphic to $\mathbf{F}_\ell^* \times \mathbf{F}_\ell^*$ and conjugate to the group of diagonal matrices. A *non-split* Cartan subgroup is isomorphic to $\mathbf{F}_{\ell^2}^*$ and conjugate to a group C_{ns} we may define as follows: for $\ell = 2$ let C_{ns} be the unique subgroup of order 3, and for $\ell > 2$ fix a quadratic non-residue $\delta \in \mathbf{F}_\ell^*$ and let

$$C_{ns} = \left\{ \begin{pmatrix} x & \delta y \\ y & x \end{pmatrix} : x, y \in \mathbf{F}_\ell, (x,y) \neq (0,0) \right\}.$$

Every Cartan subgroup has index 2 in its normalizer and contains the group of scalar matrices.

The semisimple elements of $\mathrm{GL}_2(\mathbf{F}_\ell)$ are those of order prime to ℓ. The following proposition characterizes the semisimple subgroups of $\mathrm{GL}_2(\mathbf{F}_\ell)$ in terms of their images in $\mathrm{PGL}_2(\mathbf{F}_\ell)$.

Proposition 1. *Let G be a subgroup of $\mathrm{GL}_2(\mathbf{F}_\ell)$ of order prime to ℓ, and let H be the image of G in $\mathrm{PGL}_2(\mathbf{F}_\ell)$. Then exactly one of the following holds:*

(a) *H is cyclic and G lies in a Cartan subgroup;*
(b) *H is dihedral and G lies in the normalizer of a Cartan subgroup but not in the Cartan subgroup itself;*
(c) *H is isomorphic to A_4, S_4, or A_5.*

Here A_n and S_n denote the alternating and symmetric groups on n letters, respectively.

Proof. See [9, Thm. XI.2.3] or [14]. □

Let Ω denote the set of linear subspaces of $\mathbf{F}_\ell^2$. The group $\mathrm{GL}_2(\mathbf{F}_\ell)$ acts on Ω, and the induced action of $\mathrm{PGL}_2(\mathbf{F}_\ell)$ is faithful, since only scalar matrices act trivially. For an element or subgroup g of $\mathrm{GL}_2(\mathbf{F}_\ell)$ or $\mathrm{PGL}_2(\mathbf{F}_\ell)$, we let Ω/g denote the set of g-orbits of Ω, and define Ω^g to be the set of elements fixed by g. We recall the orbit-counting lemma,

$$|\Omega/G| = \frac{1}{|G|}\sum_{g\in G}|\Omega^g|,$$

and understand that the size of each orbit in Ω/G must divide $|G|$.

We can use Proposition 1 to characterize the action of each element of $\mathrm{GL}_2(\mathbf{F}_\ell)$ on Ω. This yields Proposition 2, which encapsulates the group-theoretic content of two results credited to Atkin [13, §6]. For each h in $\mathrm{PGL}_2(\mathbf{F}_\ell)$, let $\sigma(h)$ denote the sign of h as a permutation of Ω (thus for $\ell > 2$ we have $\sigma(h) = 1$ if and only if $h \in \mathrm{PSL}_2(\mathbf{F}_\ell)$).

Proposition 2. *Let $g \in \mathrm{GL}_2(\mathbf{F}_\ell)$ have image h in $\mathrm{PGL}_2(\mathbf{F}_\ell)$ with order r, let $k = |\Omega^h|$, and let $s = |\Omega/h|$. Then k is $0, 1, 2$, or $\ell + 1$, and the $s - k$ non-trivial h-orbits have size r. When $\ell > 2$ we also have $\sigma(h) = (-1)^s$.*

Proof. The proposition clearly holds for $\ell = 2$, so we assume $\ell > 2$. When $r = 1$, we have $k = s = \ell + 1$ and $\sigma(h) = 1 = (-1)^s$. When $r = \ell$, there are exactly two h-orbits, of sizes 1 and ℓ, and we have $k = 1$, $s = 2$, and $\sigma(h) = 1 = (-1)^s$. The proposition holds in both cases.

Otherwise the cyclic group $H = \langle h\rangle$ has order r prime to ℓ and we are in case (a) of Proposition 1. Thus g lies in a Cartan subgroup C, whose image in $\mathrm{PGL}_2(\mathbf{F}_\ell)$ has order $\ell - 1$ or $\ell + 1$, as C is split or non-split (resp.). We consider the two cases.

If C is split then g is diagonalizable, so $k = |\Omega^h| = |\Omega^g| = 2$, and the same is true for every non-trivial element of H. The orbit-counting lemma yields

$$s = \frac{1}{r}\sum_{h'\in H}\left|\Omega^{h'}\right| = \frac{1}{r}((r-1)2 + \ell + 1) = 2 + \frac{\ell-1}{r}.$$

The sizes of the $(\ell - 1)/r$ non-trivial orbits all divide r and sum to $\ell - 1$, hence they are all equal to r. If r is odd then s is even and $\sigma(h) = 1 = (-1)^s$, and if r is even then $\sigma(h) = (-1)^{s-2} = (-1)^s$. Thus the proposition holds when C is split.

If C is non-split then g has no eigenvalues in $\mathbf{F}_\ell$, hence $k = |\Omega^h| = |\Omega^g| = 0$, and the same is true for every non-trivial element of H. The orbit-counting lemma yields $s = (\ell+1)/r$, and every orbit must have size r. If r is odd, then s is even and $\sigma(h) = 1 = (-1)^s$, otherwise r is even and $\sigma(h) = (-1)^s$. Thus the proposition also holds when C is non-split. □

2. Proof of Theorem 1

We first prove a group-theoretic lemma from which Theorem 1 will follow. In terms of the elliptic curve E of Theorem 1, the group G in Lemma 1 is the image of the Galois representation $\rho_{E,\ell}$. The hypothesis of the lemma is met precisely when E admits an ℓ-isogeny locally everywhere but not globally; the lemma then imposes specific constraints on G and ℓ.

Lemma 1. *Let G be a subgroup of $\mathrm{GL}_2(\mathbf{F}_\ell)$ whose image H in $\mathrm{PGL}_2(\mathbf{F}_\ell)$ does not lie in $\ker\sigma$. Suppose $|\Omega^g| > 0$ for all $g \in G$, but $|\Omega^G| = 0$. The following hold:*

(1) *H is dihedral of order $2n$, where $n > 1$ is an odd divisor of $(\ell-1)/2$;*
(2) *G is properly contained in the normalizer of a split Cartan subgroup;*
(3) *$\ell \equiv 3 \bmod 4$;*
(4) *Ω/G contains an orbit of size 2.*

Proof. No subgroup of $\mathrm{GL}_2(\mathbf{F}_2)$ satisfies the hypothesis of the lemma, so we assume $\ell > 2$. Let G and H be as in the lemma, and note that $\Omega^H = \Omega^G$, $\Omega/H = \Omega/G$, and if $h \in H$ is the image of $g \in G$ then $\Omega^h = \Omega^g$.

We first show that ℓ does not divide $m = |H|$. The orbit-counting lemma yields

$$|\Omega/H| = \frac{1}{m}\sum_{h\in H} |\Omega^h| \geq \frac{1}{m}(\ell + m) > 1,$$

since $|\Omega^h| > 0$ for all $h \in H$ and $|\Omega^h| = \ell+1$ when h is the identity. If $\ell \mid m$ then H contains an element h of order ℓ and Ω/h consists of two orbits, of sizes 1 and ℓ. These must also be the orbits of Ω/H, since $|\Omega/H| > 1$. But this contradicts our assumption that $|\Omega^H| = 0$, thus $\ell \nmid m$.

Since $\ell \nmid m$ we must have $|\Omega^h| \neq 1$ for all $h \in H$, as may be seen from the proof of Proposition 2, thus $|\Omega^h| = 2$ for every non-trivial $h \in H$. We note that H cannot be a cyclic group $\langle h\rangle$, for this would imply $\Omega^h = \Omega^H$, contrary to our hypothesis.

We now show that H is not isomorphic to A_4, A_5, or S_4. The kernel of $\sigma\colon H \to \{\pm 1\}$ must be an index 2 subgroup of H. Neither A_4 nor A_5 contain such a subgroup. Proposition 2 implies that for $h \in H$, the value $\sigma(h) = (-1)^s$ depends only on the order r of h, since either $r = 1$ and $s = \ell + 1$, or $r > 1$ and $s = 2 + (\ell - 1)/r$ (since $k = |\Omega^h| = 2$). But there is no non-trivial homomorphism from S_4 to $\{\pm 1\}$ with this property: the sequence 1,9,8,6 that counts the elements of order 1,2,3,4 (resp.) in S_4 has no subsequence whose sum is 12. It follows that $H \ncong S_4$.

Proposition 1 then implies that H is a dihedral group of order $2n$ for some $n > 1$. If n is even, then H contains $n + 1$ elements of order 2; but σ cannot be constant on a subset of H with size $n+1 > |H|/2$, so n is odd. For an element $h \in H$ of order n, Proposition 2 implies that $s = 2+(\ell-1)/n$ is

an integer, thus n divides $\ell-1$ and in fact divides $(\ell-1)/2$. This completes the proof of (1).

We are in case (b) of Proposition 1, so G lies in the normalizer $N(C)$ of a Cartan subgroup C, which must be split because n does not divide $2(\ell+1)$. The group G must be properly contained in $N(C)$, since n properly divides $\ell-1$. This proves (2).

If $\ell \equiv 1 \bmod 4$, then for each of the n elements of H with order 2 we have $s = 2 + (\ell-1)/2$ with even parity in Proposition 2, and s also has even parity when h is the identity. But this implies that σ is constant on a subset of H with size $n+1 > |H|/2$, which is again a contradiction. Therefore $\ell \equiv 3 \bmod 4$, proving (3).

Let $h \in H$ have order n. Proposition 2 implies that Ω/h consists of two trivial orbits and $(\ell-1)/n$ orbits of size n. It follows that if t is the size of an orbit of Ω/H, then t is congruent to 0, 1, or 2 modulo n, and we also know that t divides $|H| = 2n$ and $t \neq 1$ (since $|\Omega^H| = 0$). Therefore either $t = 2$ or t is a multiple of n. But n does not divide $\ell+1$, so the size of at least one orbit in Ω/H is not divisible by n. This orbit must have size $t = 2$, which proves (4). □

Theorem 1. *Assume $\sqrt{(\frac{-1}{\ell})\ell} \notin K$, and suppose E/K admits an ℓ-isogeny locally at a set of primes with density one. Then E admits an ℓ-isogeny over a quadratic extension of K, and if $\ell \equiv 1 \bmod 4$ or $\ell < 7$, then E admits an ℓ-isogeny over K.*

Proof. Let the finite set S consist of the primes where E has bad reduction and the primes that divide ℓ. Let G be the image of $\rho_{E,\ell}\colon G_{K,S} \to \mathrm{GL}_2(\mathbf{F}_\ell)$, and let $g \in G$. By the Chebotarev density theorem, the conjugacy class of g is equal to $\varphi_{\mathfrak{p},\ell}$ for a set of primes $\mathfrak{p}$ with positive density, thus we may choose $\mathfrak{p}$ so that $g = \varphi_{\mathfrak{p},\ell}$ and E admits an ℓ-isogeny locally at $\mathfrak{p}$. The Frobenius endomorphism $\varphi_{\mathfrak{p}}$ fixes a linear subspace of $E[\ell]$, hence $\varphi_{\mathfrak{p},\ell}$ fixes an element of Ω. Thus $|\Omega^g| > 0$ for all $g \in G$.

If $|\Omega^G| > 0$, then $G_{K,S}$ fixes a linear subspace of $E[\ell]$ which is the kernel of an ℓ-isogeny defined over K (and any quadratic extension). The theorem holds in this case, so we assume $|\Omega^G| = 0$. No subgroup $G \subset \mathrm{GL}_2(\mathbf{F}_2)$ has $|\Omega^G| = 0$ and $|\Omega^g| > 0$ for all $g \in G$, so $\ell \neq 2$.

The hypothesis on K implies that some element of G has a non-square determinant, otherwise $G_{K,S}$ fixes the quadratic Gauss sum $\sum_{n=0}^{\ell-1} \zeta_\ell^{n^2}$, which is equal to $\pm\sqrt{(\frac{-1}{\ell})\ell}$; see, e.g., [7]. It follows that the image of G in $\mathrm{PGL}_2(\mathbf{F}_\ell)$ does not lie in the kernel of σ, and we may apply Lemma 1. Thus $\ell \equiv 3 \bmod 4$ and $\ell \neq 3$ (by part (1) of the lemma), and Ω/G contains an orbit of size 2. Let $x \in \Omega$ be an element of this orbit. The stabilizer of x in $G_{K,S}$ is a subgroup of index 2, corresponding to a quadratic extension of K over which E admits an isogeny of degree ℓ. □

We now show that subgroups of the form permitted by Lemma 1 do in fact exist.

Proposition 3. *Let $\ell \equiv 3 \bmod 4$ be a prime number greater then 3. There exists a subgroup G of $\mathrm{GL}_2(\mathbf{F}_\ell)$ with the following properties:*

(1) *The determinant map from G to $\mathbf{F}_\ell^*$ is surjective;*
(2) *$|\Omega^g| \geq 2$ for all $g \in G$;*
(3) *$|\Omega^G| = 0$.*

Proof. Let α be a generator for $\mathbf{F}_\ell^*$, and for integers i and j define

$$A(i,j) = \begin{pmatrix} \alpha^i & 0 \\ 0 & \alpha^j \end{pmatrix}; \qquad B(i,j) = \begin{pmatrix} 0 & \alpha^i \\ \alpha^j & 0 \end{pmatrix}.$$

Let G be the set of matrices $A(i,j)$ and $B(i,j)$ for which i and j have the same parity. It is easily checked that G is a group. It contains the scalar matrices $A(i,i)$, and the matrix $B(0,0)$ whose determinant -1 is not a quadratic residue in $\mathbf{F}_\ell^*$, since $\ell \equiv 3 \bmod 4$. Therefore (1) holds. Clearly $A(i,j)$ is diagonalizable, and so is $B(i,j)$, with distinct eigenvalues $\alpha^{(i+j)/2}$ and $-\alpha^{(i+j)/2}$. This implies (2). The matrices $A(0,2)$ and $B(0,2)$ have no common eigenspace, which proves (3). □

The group in Proposition 3 has a dihedral image in $\mathrm{PGL}_2(\mathbf{F}_\ell)$ of order $2n$, where $n = (\ell-1)/2$. A similar construction works for any odd $n \geq 3$ dividing $(\ell-1)/2$.

3. A counterexample

The existence of the subgroups prescribed by Lemma 1 and constructed in Proposition 3 does not imply that they actually arise as the image of $\rho_{E,\ell}$ for some elliptic curve E/K. Indeed, if E does not have complex multiplication, then $\rho_{E,\ell}$ is known to be surjective for all sufficiently large ℓ, as shown by Serre in [14]. Surjectivity certainly precludes an exceptional image of the type permitted by Lemma 1, and, as we will show in the proof of Theorem 2, so does complex multiplication.

But there is an elliptic curve $E/\mathbf{Q}$ and a prime ℓ for which the image of $\rho_{E,\ell}$ satisfies the hypothesis of Lemma 1: the curve defined by equation (0.1) of the introduction, with j-invariant $j(E) = 2268945/128$, and $\ell = 7$.

Let $\Phi_N(X,Y)$ denote the classical modular polynomial [10, §5]. For a field F of characteristic not dividing N, an elliptic curve E/F admits a cyclic isogeny of degree N defined over F if and only if $\Phi_N(X, j(E))$ has a linear factor in $F[X]$, as proven in [6]. We note that an isogeny of prime degree is necessarily cyclic.

The irreducible factorization of $\phi(X) = \Phi_7(X, 2268945/128)$ over $\mathbf{Q}[X]$ is given below:

$$\begin{aligned}\phi(X) = (&X^2 - 1306315496294666865/2^{49}\,X + 1567296563714555573025/2^{50})\\ &(X^3 - 40537285293677514686844741 5805\,X^2\\ &\quad + 553855847225363493302022657814343 25/4\,X - 17996436663345^3/8)\\ &(X^3 - 4209728442885/2\,X^2 + 3961627130765133274725/2\,X - 16205314545^3/8).\end{aligned}$$

The absence of a linear factor shows that E does not admit a 7-isogeny over $\mathbf{Q}$, but it does admit a 7-isogeny (two in fact) over a quadratic extension of $\mathbf{Q}$, as required by Theorem 1. The discriminants of the three factors of $\phi(X)$ are each of the form $-7a^2/4^b$ for some positive integers a and b. It follows that the reduction of $\phi(X)$ mod p has two linear factors in $\mathbf{F}_p[X]$ for every odd prime p: either -7 is a quadratic residue mod p and the quadratic factor splits in $\mathbf{F}_p[X]$, or it is not and both cubic factors split into a linear and a quadratic factor in $\mathbf{F}_p[X]$. Thus E admits a 7-isogeny locally at every prime of good reduction (all $p \nmid 70$).

It is easily verified that the cubic factors of $\phi(X)$ have the same splitting field, in which the quadratic factor also splits. Its Galois group is isomorphic to S_3, which we may view as a subgroup of $\mathrm{PGL}_2(\mathbf{F}_7)$ via its action on the roots of $\phi(X)$. Thus we have a dihedral subgroup of $\mathrm{PGL}_2(\mathbf{F}_7)$ with order $2n$, where $n = 3$ divides $(\ell - 1)/2$, as required by Lemma 1. Up to conjugacy, the image of $\rho_{E,7}$ in $\mathrm{GL}_2(\mathbf{F}_7)$ is precisely the group G constructed in Proposition 3.

To determine whether there are any other exceptional pairs of the form $(7, j(E))$, we consider the moduli space of elliptic curves with the required level 7 structure. As explained by Elkies in [4, §4.2], the corresponding modular curve may be constructed as a quotient of $X(7)$ by a suitable subgroup of $\mathrm{PSL}_2(\mathbf{F}_7)$. We are interested in elliptic curves E for which the image H of $\rho_{E,7}$ in $\mathrm{PGL}_2(\mathbf{F}_7)$ is a dihedral group of order 6 not contained in the kernel of σ. Up to conjugacy there is precisely one such H, and its intersection with $\mathrm{PSL}_2(\mathbf{F}_7)$ is a cyclic group of order 3.

As shown in [4], the quotient of $X(7)$ by such a group is isomorphic (over $\overline{\mathbf{Q}}$) to $X_0(49)$, an elliptic curve. We are interested in the twist of $X_0(49)$ by $\mathrm{Gal}(\mathbf{Q}(\sqrt{-7})/\mathbf{Q})$, relative to the Fricke involution w_{49}, since if $(7, j(E))$ is an exceptional pair for $\mathbf{Q}$, then $\mathbf{Q}(\sqrt{-7})$ is the unique quadratic extension of $\mathbf{Q}$ over which E admits a 7-isogeny (by Theorem 1 there is such an extension, and from the proof of Theorem 1 it follows that if $\sqrt{-7} \notin K$ then $(7, j(E))$ will remain exceptional for K). If we make the cusp of $X_0(49)$ at infinity the origin, the cusp at zero is a rational point of order 2, and there are two non-cuspidal irrational 2-torsion points defined over $\mathbf{Q}(\sqrt{-7})$. Our twist makes the two rational cusps irrational, and the irrational 2-torsion points are made rational and swapped by the w_{49} involution. An explicit

computation by Elkies [5] finds that this twist has the equation

$$-7y^2 = x^4 + 2x^3 - 9x^2 - 10x - 3, \tag{3.1}$$

which is a genus 1 curve with rational points $(-1/2, \pm 1/4)$. If (x, y) is a rational solution to (3.1), then the rational map

$$f(x) = -(x-3)^3(x-2)(x^2+x-5)^3(x^2+x+2)^3(x^4-3x^3+2x^2+3x+1)^3/(x^3-2x^2-x+1)^7$$

yields the j-invariant of an elliptic curve that admits a 7-isogeny locally everywhere but not over $\mathbf{Q}$. Applying f to either of the points $(-1/2, \pm 1/4)$ yields the j-invariant $2268945/128$ that we have already exhibited.

Taking either of $(-1/2, \pm 1/4)$ as the origin, the curve in (3.1) is isomorphic over $\mathbf{Q}$ to the elliptic curve with Weierstrass equation

$$y^2 + xy = x^3 - x^2 - 107x + 552. \tag{3.2}$$

This is curve 49a3 in Cremona's tables [3]. It has just two $\mathbf{Q}$-rational points, and these correspond to the two solutions of (3.1) that we already know. Thus $(7,\ 2268945/128)$ is the only exceptional pair for $\mathbf{Q}$ with $\ell = 7$.

However, over a finite extension K of $\mathbf{Q}$ the curve 49a3 may have infinitely many rational points, corresponding to infinitely many exceptional pairs $(7, j(E))$ for K. Over $K = \mathbf{Q}(i)$, for example, the projective point $(-14 : 7 + 29i : 1)$ on the curve 49a3 has infinite order, yielding infinitely many solutions to (3.1). The first of these has x-coordinate $(7i - 29)/58$, and in general, if (u, v) is a solution to (3.2) then there is a solution to (3.1) with x-coordinate $(3u - v + 42)/(u + 2v)$.

4. Proof of Theorem 2

Recall that a pair $(\ell, j(E))$ is said to be exceptional for K when E/K admits an ℓ-isogeny locally everywhere but not over K.

Theorem 2. *The pair* $(7,\ 2268945/128)$ *is the only exceptional pair for* $\mathbf{Q}$.

Proof. By Theorem 1 we need only consider exceptional pairs with $\ell \geq 7$ and $\ell \equiv 3 \bmod 4$. The case $\ell = 7$ is treated above, so we assume $\ell > 7$.

We first show that if $(\ell, j(E))$ is an exceptional pair then E cannot have complex multiplication (CM). Suppose the contrary. Then E has CM by an imaginary quadratic order $\mathcal{O}$, since we are in characteristic zero, and it must have class number $h(\mathcal{O}) = 1$, since E is defined over $\mathbf{Q}$. By Theorem 1 there is an ℓ-isogenous elliptic curve E' that is defined over a quadratic extension of $\mathbf{Q}$ but not over $\mathbf{Q}$ (since we are in an exceptional case). The curve E' must have CM by an imaginary quadratic order $\mathcal{O}'$ with class number $h(\mathcal{O}') = 2$. Since E and E' are ℓ-isogenous and $h(\mathcal{O}') > h(\mathcal{O})$, the order $\mathcal{O}'$ must be properly contained in $\mathcal{O}$ with index ℓ. Via [2, Thm. 7.24], we may compute the ratio $h(\mathcal{O}')/h(\mathcal{O})$ as

$$\frac{h(\mathcal{O}')}{h(\mathcal{O})} = \frac{1}{[\mathcal{O}^* : \mathcal{O}'^*]}\left(\ell - \left(\frac{\operatorname{disc}(\mathcal{O})}{\ell}\right)\right) \geq \frac{1}{3}(\ell - 1).$$

But we already know that $h(\mathcal{O}')/h(\mathcal{O}) = 2/1 = 2$, which yields a contradiction for $\ell > 7$. Therefore E does not have CM.

By Lemma 1, it suffices to consider pairs $(j(E), \ell)$ for which the image of $\rho_{E,\ell}$ in $\mathrm{GL}_2(\mathbb{F}_\ell)$ is contained in the normalizer of a split Cartan group, as explained in the proof of Theorem 1. For such a pair, the j-invariant $j(E)$ corresponds to a rational non-cuspidal point on the modular curve $X_{\mathrm{split}}(\ell)(\mathbf{Q})$, which is isomorphic over $\mathbf{Q}$ to $X_0^+(\ell^2)$, the quotient of $X_0(\ell^2)$ by the Fricke involution w_{ℓ^2}. By Theorem 1.1 of [12], for all $\ell > 7$ congruent to 3 mod 4, the only rational non-cuspidal points on $X_0^+(\ell^2)(\mathbf{Q})$ correspond to elliptic curves with CM.[1] But we have shown that no curve with CM can arise in an exceptional pair, and the theorem follows. □

The argument used to rule out CM in the proof above works over any number field, and when $K \neq \mathbf{Q}$ we have $[\mathcal{O}^* : \mathcal{O}'^*] = 1$, which covers the case $\ell = 7$ as well.

5. Acknowledgments

I thank Nicholas Katz, Barry Mazur, and Ken Ribet for several helpful discussions, and Pierre Parent for directing my attention to his result in [12]. I am especially grateful to Noam Elkies for his explicit computations in the case $\ell = 7$, and to John Cremona for identifying the constraint on K required by Theorem 1.

References

[1] Yuri Bilu, Pierre Parent, and Marusia Rebolledo, *Rational points on $X_0^+(p^r)$*. To appear in Annales de l'institut Fourier, arXiv:1104.4641v1 (2011).

[2] David A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*. John Wiley and Sons, 1989.

[3] John Cremona, *The elliptic curve database for conductors to* 130000. Algorithmic Number Theory Symposium–ANTS VII (F. Hess, S. Pauli, and M. Pohst, eds.), Lecture Notes in Computer Science, vol. **4076**, Springer-Verlag, 2006, pp. 11–29.

[4] Noam D. Elkies, *The Klein quartic in number theory*. The Eightfold Way: The Beauty of Klein's Quartic Curve (Silvio Levy, ed.), Cambridge University Press, 2001, pp. 51–102.

[5] ———, private communication, March 2010.

[6] Jun-Ichi Igusa, *Kroneckerian model of fields of elliptic modular functions*. American Journal of Mathematics **81** (1959), 561–577.

[7] Kenneth Ireland and Michael Rosen, *A classical introduction to modern number theory*, second ed., Springer-Verlag, 1990.

[8] Nicholas M. Katz, *Galois properties of torsion points on abelian varieties*. Inventiones Mathematicae **62** (1981), no. 3, 481–502.

[9] Serge Lang, *Introduction to modular forms*, Springer, 1976.

[10] ———, *Elliptic functions*, second ed., Springer-Verlag, 1987.

[11] Barry Mazur, *An introduction to the deformation theory of Galois representations*. Modular forms and Fermat's last theorem, Springer, 1997.

[12] Pierre J. R. Parent, *Towards the triviality of $X_0^+(p^r)(\mathbb{Q})$ for $r > 1$*. Compositio Mathematica **141** (2005), 561–572.

[1] This is also implied by the recent (and stronger) result in [1], which addresses all $\ell \neq 13$.

[13] René Schoof, *Counting points on elliptic curves over finite fields*. Journal de Théorie des Nombres de Bordeaux **7** (1995), 219–254.
[14] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*. Inventiones Mathematicae **15** (1972), no. 2, 259–331.

Andrew V. Sutherland
Department of Mathematics
Massachusetts Institute of Technology
77 Massachusetts Avenue
Cambridge, MA 02139
E-mail: drew@math.mit.edu
URL: http://math.mit.edu/~drew