ACTA ARITHMETICA
Online First version

Elliptic curves with maximally disjoint division fields

by

Harris B. Daniels (Amherst, MA),
Jeffrey Hatley (Schenectady, NY) and
James Ricci (Amherst, NY)

1. Introduction. Let E be an elliptic curve defined over $\mathbb{Q}$, let $\bar{\mathbb{Q}}$ be a fixed algebraic closure of $\mathbb{Q}$, and for each positive integer n let

$$E[n] = \{P \in E(\bar{\mathbb{Q}}) : [n]P = \mathcal{O}\}$$

denote the n-torsion of E. It is a classical result that $E[n]$ is non-canonically isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ and the group $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts on $E[n]$ component-wise. Therefore, we can construct a Galois representation associated to the n-torsion of E,

$$\bar{\rho}_{E,n} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[n]) \simeq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

By choosing compatible bases and taking an inverse limit ordered by divisibility, we can construct the full-torsion representation associated to E,

$$\rho_E : G_{\mathbb{Q}} \to \mathrm{GL}_2(\hat{\mathbb{Z}}) \simeq \prod_p \mathrm{GL}_2(\mathbb{Z}_p),$$

where the product is taken over all prime numbers.

A natural question is: how large can the image of ρ_E be inside of $\mathrm{GL}_2(\hat{\mathbb{Z}})$? More specifically, can ρ_E be surjective? With these questions in mind, we give the following definition:

Definition 1.1. An integer $n \geq 2$ is said to be *exceptional* for E if $\bar{\rho}_{E,n}$ is not surjective.

We can translate questions about the size of $\mathrm{Im}\,\rho_E$ into a question about which numbers are exceptional for E and, for an exceptional n, how drastically $\rho_{E,n}$ fails to be surjective. It is a standard result that when E is an elliptic curve with complex multiplication (CM), *every* integer except for

2010 *Mathematics Subject Classification*: Primary 14H52; Secondary 11F80.
Key words and phrases: elliptic curves, Galois representations.
Received 28 August 2015; revised 11 February 2016.
Published online *.

possibly 2 is exceptional for E. See [9, Theorem 2.3] for more details. On the other hand, if $E/\mathbb{Q}$ is an elliptic curve that does not have CM, Serre showed in [7] that the index $[\mathrm{GL}_2(\hat{\mathbb{Z}}) : \operatorname{Im}\rho_E]$ is finite. One implication of this is that for each elliptic curve there are only finitely many exceptional primes. Additionally, Serre proved the following theorem.

PROPOSITION 1.2 ([7, Proposition 22]). *For any elliptic curve E defined over $\mathbb{Q}$, the image of $\rho_E : G_{\mathbb{Q}} \to \mathrm{GL}_2(\hat{\mathbb{Z}})$ is contained in a group of index 2 inside $\mathrm{GL}_2(\hat{\mathbb{Z}})$.*

This theorem implies that ρ_E can never be surjective, and thus there exists at least one exceptional number n (not necessarily prime). In the same paper, Serre gave two examples of elliptic curves whose image has index exactly 2 inside $\mathrm{GL}_2(\hat{\mathbb{Z}})$, showing that this lower bound on the index of $\operatorname{Im}\rho_E$ is sharp.

Following Lang and Trotter we give the following definition:

DEFINITION 1.3. An elliptic curve $E/\mathbb{Q}$ is called a *Serre curve* if

$$[\mathrm{GL}_2(\hat{\mathbb{Z}}) : \operatorname{Im}\rho_E] = 2.$$

Furthermore, there is no reason to restrict our attention to Galois representations associated to only *one* elliptic curve. Given a pair of elliptic curves (E_1, E_2) defined over $\mathbb{Q}$ and a positive integer n, we can consider the action of $G_{\mathbb{Q}}$ on $E_1[n] \times E_2[n]$ to get a new Galois representation

$$\bar{\rho}_{(E_1,E_2),n} : G_{\mathbb{Q}} \to \ (\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}))^2,$$

given by $\bar{\rho}_{(E_1,E_2),n}(\sigma) = (\bar{\rho}_{E_1,n}(\sigma), \bar{\rho}_{E_2,n}(\sigma))$. Just as before, we can construct the full-torsion representation associated to the pair (E_1, E_2),

$$\rho_{(E_1,E_2)} : G_{\mathbb{Q}} \to (\mathrm{GL}_2(\hat{\mathbb{Z}}))^2,$$

and it is again natural to ask: how big can the image of $\rho_{(E_1,E_2)}$ be?

Ther is a natural limitation on the size of the image of $\rho_{(E_1,E_2)}$ in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ coming from the Weil pairing. Given an elliptic curve $E/\mathbb{Q}$, let $\mathbb{Q}(E[n])$ be the field of definition of the n-torsion points of E. One consequence of the Weil pairing is that if ζ_n is a primitive nth root of unity, then $\mathbb{Q}(\zeta_n) \subset \mathbb{Q}(E[n])$. Therefore, it must be that $\mathbb{Q}(\zeta_n) \subset \mathbb{Q}(E_1[n]) \cap \mathbb{Q}(E_2[n])$.

The action of an element in the Galois group on an nth root of unity can be related to its image under $\bar{\rho}_{E,n}$ through the determinant. That is, given an elliptic curve $E/\mathbb{Q}$, $\sigma \in G_{\mathbb{Q}}$, and an nth root of unity ζ_n, it must *always* be that

$$\sigma(\zeta_n) = \zeta_n^{\det(\bar{\rho}_{E,n}(\sigma))}. \tag{1.1}$$

Therefore, for each positive integer n, we define

$$D_n := \{(A, B) \in (\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}))^2 : \det A = \det B\},$$
$$D := \{(A, B) \in (\mathrm{GL}_2(\hat{\mathbb{Z}}))^2 : \det A = \det B\}.$$

With these definitions and the observations above we can see that for any pair of elliptic curves (E_1, E_2) defined over $\mathbb{Q}$ and any positive integer n, the image of $\bar{\rho}_{(E_1,E_2),n}$ and $\rho_{(E_1,E_2)}$ must be contained inside of D_n and D respectively. Therefore, any result associated with the size of $\operatorname{Im}\rho_{(E_1,E_2)}$ should be formulated in terms of $[D : \operatorname{Im}\rho_{(E_1,E_2)}]$.

For any two elliptic curves E_1 and E_2 defined over $\mathbb{Q}$, we have

$$\operatorname{Im}\rho_{(E_1,E_2)} \subset (\operatorname{Im}\rho_{E_1} \times \operatorname{Im}\rho_{E_2}) \cap D.$$

Since the right-hand side has index at least 4 inside of D (by Proposition 1.2), we give the following definition in the spirit of Definition 1.3:

Definition 1.4. A pair (E_1, E_2) is called a *Serre pair* if

$$[D : \operatorname{Im}\rho_{(E_1,E_2)}] = 4.$$

In [4], Jones shows that, in some appropriate sense, almost all pairs of elliptic curves are Serre pairs. The proof uses a multi-dimensional large sieve but provides no concrete examples of Serre pairs. In [7, Section 6.3], Serre gives an example (without proof) of a pair of elliptic curves (E, E') for which the representation $\bar{\rho}_{(E,E'),p}$ is surjective for every prime p. As Lemma 1.9 below indicates, this is almost enough to conclude that (E, E') is a Serre pair, but some extra conditions on $\bar{\rho}_{(E,E'),36}$ need to be checked.

In fact, there are no explicit examples of Serre pairs with full proof in the current literature. The main goal of this paper is to rectify this deficiency by providing infinitely many such examples. The first step toward this goal is to find an infinite family of Serre curves, since clearly any Serre pair must be a pair of Serre curves.

Lemma 1.5 ([2, Example 8.2]). *Let ℓ be an odd prime with $\ell \neq 7$. Then the elliptic curve*

$$E_\ell : y^2 + xy = x^3 + \ell$$

is a Serre curve.

Using this lemma we will be able to construct the first examples of Serre pairs coming from the main theorem of this paper:

Theorem 1.6. *Let ℓ_1 and ℓ_2 be odd primes not equal to 7 such that $\gcd(432\ell_1^2 + \ell_1, 432\ell_2^2 + \ell_2) = 1$, and for $i = 1, 2$ let*

$$E_{\ell_i} : y^2 + xy = x^3 + \ell_i.$$

Then (E_{ℓ_1}, E_{ℓ_2}) is a Serre pair.

In fact, we obtain the following interesting corollary, showing that there are indeed many pairs (ℓ_1, ℓ_2) of primes satisfying the hypotheses of Theorem 1.6.

COROLLARY 1.7. *Let ℓ_1 be an odd prime different from 7. Then there exist infinitely many primes ℓ_2 such that (E_{ℓ_1}, E_{ℓ_2}) is a Serre pair.*

Proof. Let $\Delta = 432\ell_1^2 + \ell_1$ and suppose it factors as $\Delta = p_1^{e_1} \cdots p_n^{e_n}$. By Theorem 1.6, it suffices to show that there exist infinitely many primes $\ell_2 \nmid \Delta$ such that

$$432\ell_2 + 1 \not\equiv 0 \bmod p_i \quad \text{for every } i = 1, \ldots, n.$$

First notice that if $\ell_1 = 3$, then by Dirichlet's theorem on primes in arithmetic progressions, there are infinitely many primes ℓ_2 different from 3 and 1297 such that $\ell_2 \not\equiv 3 \bmod 1297$.

Otherwise, if $\ell_1 \neq 3$, then $432\ell_1 \equiv -1$ is a unit modulo Δ and since each p_i divides Δ, we have

$$432\ell_2 + 1 \equiv 0 \bmod p_i \;\Rightarrow\; \ell_2 \equiv \ell_1 \bmod p_i.$$

Therefore, it suffices to show that there are infinitely many ℓ_2 such that $\ell_2 \not\equiv \ell_1 \bmod p_i$ for all $1 \leq i \leq n$. By the Chinese remainder theorem, we can choose x such that $x \not\equiv 0, \ell_1 \bmod p_i$ for each i. An application of Dirichlet's theorem on the sequence $\{x + (p_1 \cdots p_n)k\}_{k \in \mathbb{N}}$ then guarantees the existence of infinitely many primes ℓ_2 with the desired property. ∎

REMARK 1.8. The quantity $432\ell_i^2 + \ell_i$ is the discriminant of the elliptic curve E_i. As we discuss below in Proposition 2.2 and Lemma 2.3, the hypothesis that $\gcd(432\ell_1^2 + \ell_1, 432\ell_2^2 + \ell_2) = 1$ imposes constraints on the ramification in the division fields associated to our elliptic curves.

In order to prove Theorem 1.6 we will need the following lemma:

LEMMA 1.9. *Let (E_1, E_2) be a pair of elliptic curves defined over $\mathbb{Q}$. If*

(1) *for each prime $p \geq 5$, $\operatorname{Im} \bar{\rho}_{(E_1,E_2),p} = D_p$, and*
(2) *$\operatorname{Im} \bar{\rho}_{(E_1,E_2),36} = D_{36}$,*

then (E_1, E_2) is a Serre pair.

Proof. This follows immediately from [4, Lemma 3.1]. ∎

Lemma 1.9 gives us two concrete conditions that we use to verify that our pairs of elliptic curves are in fact Serre pairs.

1.1. Notation and outline. Throughout the rest of this paper, fix two odd primes ℓ_1 and ℓ_2, both different from 7, with $\gcd(432\ell_1^2+\ell_1, 432\ell_2^2+\ell_2)=1$. For $i = 1, 2$ we will write

$$E_i : y^2 + xy = x^3 + \ell_i.$$

Then by Lemma 1.5, E_1 and E_2 are both Serre curves. In particular, as explained in [2], the map

$$\bar{\rho}_{E_i,p^n} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$$

is surjective for every prime p and every integer $n \geq 1$.

Our strategy is to use Lemma 1.9 to prove that (E_1, E_2) is a Serre pair. Thus, our paper divides naturally into two main sections: a study of $\bar{\rho}_{(E_1,E_2),p}$ for all primes $p \geq 5$, and a separate study of $\bar{\rho}_{(E_1,E_2),36}$. In both cases, we interpret the conditions of Lemma 1.9 in terms of the Galois theory of the division fields associated to the Serre curves E_i. Let $K_i = \mathbb{Q}(E_i[p^n])$ denote the Galois number field obtained by adjoining to $\mathbb{Q}$ the coordinates of the p^n-torsion points of E_i. The Weil pairing forces the intersection $K_1 \cap K_2$ to be a non-trivial extension of $\mathbb{Q}$; in particular, the intersection contains the p^n-cyclotomic field $\mathbb{Q}(\zeta_{p^n})$. The main results of this paper state that, apart from the cyclotomic subextension, the division fields K_1 and K_2 are maximally disjoint for all primes p and all integers $n \geq 1$. Theorem 1.6 then follows directly from the conditions found in Lemma 1.9.

2. p-Division fields for $p \geq 5$. For the entirety of this section fix a prime $p \geq 5$ and, since $\ell_1 \neq \ell_2$, assume without loss of generality that $p \neq \ell_1$. Let $K_i = \mathbb{Q}(E_i[p])$ denote the number field obtained by adjoining to $\mathbb{Q}$ the x- and y-coordinates of all p-torsion points of E_i. Since E_i is a Serre curve, we have

$$\mathrm{Gal}(K_i/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}).$$

As explained in the introduction, the Weil pairing forces the inclusion $\mathbb{Q}(\zeta_p) \subset K_i$, where ζ_p denotes a primitive pth root of unity and $\mathbb{Q}(\zeta_p)$ denotes the p-cyclotomic extension of $\mathbb{Q}$. Let $F = K_1 \cap K_2$ denote the intersection of the two division fields; then $F \supset \mathbb{Q}(\zeta_p)$ is strictly larger than $\mathbb{Q}$.

Recall that condition (1) of Lemma 1.9 states the following:

$$\mathrm{Im}\,\bar{\rho}_{(E_1,E_2),p} = \{(A, B) \in (\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}))^2 : \det A = \det B\}. \tag{2.1}$$

This condition can be interpreted using the Galois-theoretic properties of the K_i, as we now describe.

First, recall that the determinant of $\bar{\rho}_{E_i,p}$ is the cyclotomic character χ_p, which cuts out the cyclotomic extension $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ via the canonical isomorphism $\chi_p : \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})^\times$.

Now let $L = K_1K_2$ denote the compositum of the division fields. Then $\mathrm{Gal}(L/\mathbb{Q})$ is a subgroup of the direct product $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. Since the intersection F is a non-trivial extension of $\mathbb{Q}$, $\mathrm{Gal}(L/\mathbb{Q})$ must be a *proper* subgroup. The following result is well-known.

LEMMA 2.1 (Goursat's lemma). *Let G_1 and G_2 be groups, and let H be a subgroup of the direct product $G_1 \times G_2$ such that the natural projections*

$\pi_1 : H \to G_1$ and $\pi_2 : H \to G_2$ are surjective. Let N_1 denote the kernel of π_2 and N_2 denote the kernel of π_1. Then regarding N_i as a subgroup of G_i, the image of H in $G_1/N_1 \times G_2/N_2$ is the graph of an isomorphism $G_1/N_1 \simeq G_2/N_2$.

Proof. See [6, Lemma 5.2.1]. ∎

Write $G_i = \mathrm{Gal}(K_i/\mathbb{Q})$, and for the moment let $H = \mathrm{Gal}(L/\mathbb{Q})$. Goursat's lemma shows that H is a certain fibered product of G_1 and G_2. Furthermore, since $G_1 \simeq G_2 \simeq \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, we see that H is determined by a normal subgroup N of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. For example, if H were equal to the entire direct product $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, then we would have $N = \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, and the common fixed field $F = K_1 \cap K_2$ would be equal to $\mathbb{Q}$.

Goursat's lemma thus gives the following Galois-theoretic interpretation of (2.1): since $\det \bar{\rho}_{E_i,p} = \chi_p$ cuts out $\mathbb{Q}(\zeta_p)$, we have

$$\mathrm{Im}\, \bar{\rho}_{(E_1,E_2),p} = D_p \;\Leftrightarrow\; F = \mathbb{Q}(\zeta_p).$$

So (2.1) is equivalent to the statement that H is the fibered product of G_1 and G_2 over $\mathbb{Q}(\zeta_p)$, which is equivalent to K_1 and K_2 being maximally disjoint. Our goal is to show that $F = \mathbb{Q}(\zeta_p)$.

To that end, set $H := \mathrm{Gal}(L/\mathbb{Q}(\zeta_p))$. Figure 1 illustrates the associated field diagram with edges labeled by Galois groups.

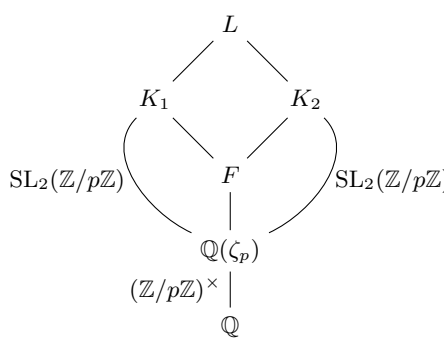

Fig. 1. Division fields for $p \geq 5$

Now, H is a subgroup of the direct product $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, and we wish to show that $H \simeq (\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}))^2$. Since E_1 and E_2 are Serre curves, the natural projections $H \to \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ are surjective, and Goursat's lemma implies that H is determined by a normal subgroup $N \triangleleft \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. As in our previous discussion, we will have $F = \mathbb{Q}(\zeta_p)$ precisely if $N = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$.

Before proving the main result of this section, we collect some lemmas on the ramification behavior of primes in the K_i. One computes that the

curve $E_{\ell_i} : y^2 + xy = x^3 + \ell_i$ has discriminant

$$\Delta(E_{\ell_i}) = -\ell_i(432 + \ell_i).$$

Recall that the only primes of bad reduction for E_i are those dividing $\Delta(E_i)$. The following result states that these are also the only primes other than p which may ramify in $K_i/\mathbb{Q}$.

PROPOSITION 2.2 (Néron, Ogg, Shafarevich). *Let E be an elliptic curve over $\mathbb{Q}$, and let p be a rational prime. Then the following assertions are equivalent:*

- *E has good reduction modulo p.*
- *p is unramified in $\mathbb{Q}(E[n])/\mathbb{Q}$ for all integers $n \geq 1$ with $\gcd(n, p) = 1$.*

Proof. See [8, VII, Theorem 7.1] ∎

By hypothesis we have $\gcd(\Delta(E_1), \Delta(E_2)) = 1$, so ℓ_2 does not ramify in K_1. The next lemma gives a lower bound on the ramification of ℓ_1 in K_1.

LEMMA 2.3. *Let e_{ℓ_i} denote the ramification index of ℓ_i in $K_i/\mathbb{Q}$. Then $e_{\ell_i} \geq p$.*

Proof. This is worked out in detail in [5, Section 3.2] using the theory of Tate curves. For the proof, we drop the i subscripts and write simply $E = E_i$ and $\ell = \ell_i$. First, note that the discriminant of E is

$$\Delta(E) = -\ell(432 + \ell).$$

In particular, the ℓ-adic valuation of $\Delta(E)$ is

$$\nu_\ell(\Delta(E)) = \begin{cases} 1 & \text{if } \ell \neq 3, \\ 2 & \text{if } \ell = 3, \end{cases}$$

and E has bad (split multiplicative) reduction at ℓ. Our elliptic curve has j-invariant $j_E = 1/\Delta(E)$, so in the notation of [5] we have $\alpha_\ell = \nu_p(-\nu_\ell(j_E)) = 0$. By [5, Section 3.2, equations (3.4)–(3.7)], we have

$$e_\ell = \begin{cases} (p-1)p & \text{if } p = \ell, \\ p & \text{if } p \neq \ell. \end{cases}$$

Thus, in either case, $e_\ell \geq p$. ∎

We are now prepared to prove the following.

PROPOSITION 2.4. *Let N denote the kernel of (either) projection map $H \to \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. Then $N = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, and so $\operatorname{Im} \bar{\rho}_{(E_1,E_2),p} = D_p$.*

Proof. By definition

$$\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})/\{\pm I\},$$

where I denotes the identity matrix, and the projective special linear group $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ is a simple group since $p \geq 5$ [1, Proposition 5.1.7]. Thus, H is

determined by a normal subgroup $N \triangleleft \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, and the only possibilities are

$$N \in \big\{\{I\}, \{\pm I\}, \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})\big\}.$$

Recall that $F = K_1 \cap K_2$ and $F \supset \mathbb{Q}(\zeta_p)$. By Goursat's lemma and the Galois correspondence, the index $[\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}) : N]$ is equal to the degree $[F : \mathbb{Q}(\zeta_p)]$. Thus F is strictly larger than $\mathbb{Q}(\zeta_p)$ if and only if $N \neq \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$.

If $N = \{I\}$, then in fact $F = K_1K_2$; this is impossible, as ℓ_1 ramifies in K_1 but not in K_2 by Proposition 2.2 and the fact that $\ell_1 \nmid \Delta(E_2) = \ell_2(432 + \ell_2)$.

If $N = \{\pm I\}$, then $[K_1 : F] = 2$. But by Lemma 2.3, the ramification index of ℓ_1 in $K_1/\mathbb{Q}(\zeta_p)$ is greater than 2, and ℓ_1 is unramified in K_2 (and hence in F), so this impossible.

Thus, the only possibility which our hypotheses allow is $N = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, as desired. ∎

3. p^2-Division fields for $p = 2, 3$. In this section, we deal with condition (2) of Lemma 1.9, so given a pair (E_1, E_2) as before, we now wish to show that

$$\mathrm{Im}\, \bar{\rho}_{(E_1,E_2),36} = D_{36}. \tag{3.1}$$

Similar to the setup in Section 2, for $i = 1, 2$, let $K_{i,n} = \mathbb{Q}(E_i[n])$ denote the n-division field of E_i, which is the number field obtained by adjoining to $\mathbb{Q}$ the x- and y- coordinates of the n-torsion points of E_i. Since E_i is a Serre curve, we have

$$\mathrm{Gal}(K_{i,36}/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z}).$$

Once again, the Weil pairing forces an inclusion $\mathbb{Q}(\zeta_{36}) \subset K_{i,36}$, where ζ_{36} is a primitive 36th root of unity. It follows that $K_{1,36} \cap K_{2,36} \supset \mathbb{Q}(\zeta_{36})$ is a non-trivial extension of $\mathbb{Q}$. Just as in the $p \geq 5$ case, this implies that the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ of the compositum $L = K_{1,36}K_{2,36}$ is a *proper* subgroup of $(\mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z}))^2$, determined (via Goursat's lemma) by a normal subgroup of $\mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z})$. Condition (3.1) is equivalent to the statement that $K_{1,36}$ and $K_{2,36}$ are maximally disjoint in the sense that

$$\mathrm{Im}\, \bar{\rho}_{(E_1,E_2),36} = D_{36} \;\Leftrightarrow\; K_1 \cap K_2 = \mathbb{Q}(\zeta_{36}).$$

For $i = 1, 2$ Figure 2 illustrates the decomposition of $K_{i,36}$ in terms of smaller division fields. The edges are marked by Galois groups, which are determined by the fact that E_i is a Serre curve.

Noting that $\mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z}) \simeq \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$, we see that Figure 2 and Goursat's lemma imply $K_{i,4} \cap K_{i,9} = \mathbb{Q}$. Furthermore, since $\mathrm{Gal}(L/\mathbb{Q})$ is a subgroup of $\mathrm{Gal}(K_{1,36}/\mathbb{Q}) \times \mathrm{Gal}(K_{2,36}/\mathbb{Q})$, the same diagram shows that verifying (3.1) is equivalent to verifying the following three

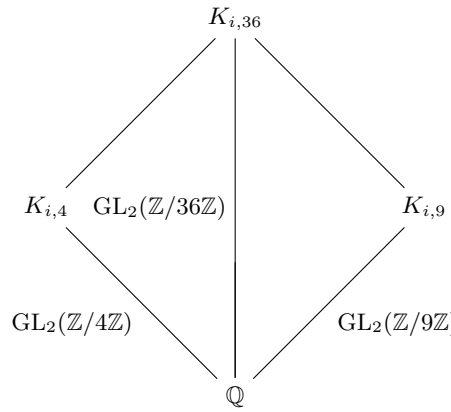

Fig. 2. Decomposition of the 36-division fields for E_i

assertions:

- $K_{1,4} \cap K_{2,4} = \mathbb{Q}(\zeta_4)$;
- $K_{1,9} \cap K_{2,9} = \mathbb{Q}(\zeta_9)$;
- $K_{i,4} \cap K_{j,9} = \mathbb{Q}$ for $i \neq j$.

We now handle each case in turn. For the rest of the section, let $\Delta_i = -\ell_i(432\ell_i + 1)$ denote the discriminant of E_i. Just as in Section 2, our arguments will depend crucially on our hypothesis that $\gcd(\Delta_1, \Delta_2) = 1$.

LEMMA 3.1. *For our pair* (E_1, E_2)*, we have* $K_{1,4} \cap K_{2,4} = \mathbb{Q}(\zeta_4)$.

Proof. The subfield structure of 4-division fields of elliptic curves is explained in detail in [1, Section 5.5]. In particular, every subfield of $K_{i,4}$ which properly contains $\mathbb{Q}(\zeta_4)$ also contains $\mathbb{Q}(\zeta_4, \sqrt{\Delta_i})$, as well as *all* subfields which are quadratic over $\mathbb{Q}$ (see Figure 3). Let $F = K_{1,4} \cap K_{2,4}$, so

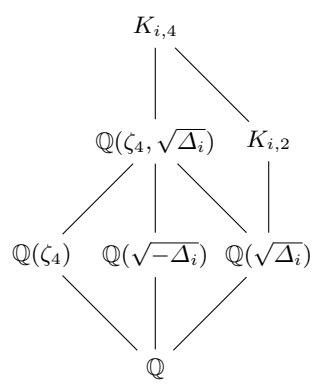

Fig. 3. A portion of the subfield diagram of $K_{i,4}$ from [1, Figure 5.7]

$\mathbb{Q}(\zeta_4) \subset F$. By the subfield diagram, if $[F : \mathbb{Q}(\zeta_4)] > 1$ then we must also have $\mathbb{Q}(\zeta_4, \sqrt{\Delta_1}) \subset F \subset K_{2,4}$. But then the quadratic field $\mathbb{Q}(\sqrt{\Delta_1})$ is also contained in $F \subset K_{2,4}$. However, the only quadratic subfields of $K_{2,4}$ are

$$\mathbb{Q}(\zeta_4), \quad \mathbb{Q}(\sqrt{\Delta_2}), \quad \mathbb{Q}(\sqrt{-\Delta_2}).$$

Since ℓ_1 is an odd prime and $\gcd(\Delta_1, \Delta_2) = 1$, we cannot have equality between $\mathbb{Q}(\sqrt{\Delta_1})$ and any of the aforementioned fields. So we must have $[F : \mathbb{Q}(\zeta_4)] = 1$, which proves the lemma. ∎

The argument for 9-division fields is very similar to that of Lemma 3.1. First we recall a result about the structure of the 3-division fields of elliptic curves.

LEMMA 3.2. *Let $M = \mathbb{Q}(x(E_i[3]))$ denote the number field obtained by adjoining to $\mathbb{Q}$ the x-coordinates of the 3-torsion points of E_i. Then $\mathbb{Q}(\sqrt[3]{\Delta_i}, \zeta_3)$ is the unique subfield of M which has degree 6 over $\mathbb{Q}$. The only other subfield of $K_{i,9}$ which has degree 6 over $\mathbb{Q}$ is $\mathbb{Q}(\zeta_9)$.*

Proof. The first statement is [1, Proposition 5.4.3]. The second statement is visible in [1, Figure 5.4]. ∎

LEMMA 3.3. *For our pair (E_1, E_2), we have $K_{1,9} \cap K_{2,9} = \mathbb{Q}(\zeta_9)$.*

Proof. The subfield structure of 9-division fields of elliptic curves is also explained in detail in [1, Section 5.2]. In particular, by [1, Figure 5.4] every subfield of $K_{i,9}$ which properly contains $\mathbb{Q}(\zeta_9)$ also contains $\mathbb{Q}(\zeta_3, x(E_i[3]))$

Let $F = K_{1,9} \cap K_{2,9}$, so $\mathbb{Q}(\zeta_9) \subset F$. If $[F : \mathbb{Q}(\zeta_9)] > 1$ then we must also have $\mathbb{Q}(\zeta_3, x(E_1[3])) \subset F \subset K_{2,9}$. But then Lemma 3.2 implies that

$$\mathbb{Q}(\sqrt[3]{\Delta_1}, \zeta_3) = \mathbb{Q}(\sqrt[3]{\Delta_2}, \zeta_3),$$

which is impossible since $\gcd(\Delta_1, \Delta_2) = 1$. Thus $[F : \mathbb{Q}(\zeta_9)] = 1$, which proves the lemma. ∎

It remains to consider the possible entanglement between the 4- and 9-division fields of our elliptic curves. By symmetry it suffices to show the following.

LEMMA 3.4. *For our pair (E_1, E_2), we have $K_{1,4} \cap K_{2,9} = \mathbb{Q}$.*

Proof. By [1, Figure 5.4], every subextension of $K_{2,9}$ which is Galois over $\mathbb{Q}$ contains $\mathbb{Q}(\zeta_3)$ as the unique subextension which is quadratic over $\mathbb{Q}$. Therefore, if $F = K_{1,4} \cap K_{2,9}$ satisfies $[F : \mathbb{Q}] > 1$, then $\mathbb{Q}(\zeta_3) \subset F$. But also $F \subset K_{1,4}$, and as shown in Figure 3, the only quadratic subextensions of $K_{1,4}$ are

$$\mathbb{Q}(\zeta_4), \quad \mathbb{Q}(\sqrt{-\Delta_1}), \quad \mathbb{Q}(\sqrt{\Delta_1}).$$

One checks that if $\ell_1 = 3$ then $\Delta_1 = 3 \cdot 1297$; otherwise, $\ell_1 > 3$ and $\nu_{\ell_1}(\Delta_1) = 1$, so in any case none of these extensions is equal to $\mathbb{Q}(\zeta_3)$. It follows that $[F : \mathbb{Q}] = 1$, proving the lemma. ∎

We summarize the results of this section.

PROPOSITION 3.5. *For our chosen pair (E_1, E_2) of elliptic curves, we have*

$$\operatorname{Im} \bar{\rho}_{(E_1,E_2),36} = D_{36}.$$

Proof. This follows immediately from Lemmas 3.1, 3.3, and 3.4. ∎

Proof of Theorem 1.6. The theorem follows immediately from Lemma 1.9 and Propositions 2.4 and 3.5. ∎

4. Serre k-tuples. Given a k-tuple $(E_1, \dots, E_k)$ of elliptic curves, one can generalize the above construction in the obvious way to obtain a representation

$$\rho_{(E_1,\dots,E_k)} : G_{\mathbb{Q}} \to (\mathrm{GL}_2(\hat{\mathbb{Z}}))^k,$$

whose image is contained in

$$D^{(k)} := \{(A_1, \dots, A_k) \in (\mathrm{GL}_2(\hat{\mathbb{Z}}))^k : \det A_1 = \cdots = \det A_k\}.$$

Unsurprisingly, one has

$$[D^{(k)} : \operatorname{Im} \rho_{(E_1,\dots,E_k)}] \geq 2^k.$$

DEFINITION 4.1. For any integer $k \geq 1$, a k-tuple $(E_1, \dots, E_k)$ of elliptic curves is called a *Serre k-tuple* if $[D^{(k)} : \operatorname{Im} \rho_{(E_1,\dots,E_k)}] = 2^k$.

In [4, Theorem 4.3], it is shown that almost all k-tuples of elliptic curves are Serre k-tuples. Theorem 1.6 easily generalizes to the case $k \geq 2$.

THEOREM 4.2. *Let $\ell_1, \dots, \ell_k$ be odd primes not equal to 7 such that $\gcd(432\ell_i^2 + \ell_i, 432\ell_j^2 + \ell_j) = 1$ for each pair $1 \leq i < j \leq k$. For each $1 \leq i \leq k$ let*

$$E_{\ell_i} : y^2 + xy = x^3 + \ell_i.$$

Then $(E_{\ell_1}, \dots, E_{\ell_k})$ is a Serre k-tuple.

Proof. Just as in the $k = 2$ case, showing that $(E_{\ell_1}, \dots, E_{\ell_k})$ is a Serre k-tuple is equivalent to showing that the E_{ℓ_i} have maximally disjoint division fields [3, Corollary 6.7]. Since the discriminants of each elliptic curve in the k-tuple are pairwise relatively prime, Theorem 1.6 shows that the division fields for $E_{\ell_1}, \dots, E_{\ell_k}$ are pairwise maximally disjoint, and the result follows. ∎

REMARK 4.3. The argument in Corollary 1.7, applied inductively, shows that Theorem 4.2 produces infinitely many examples of Serre k-tuples.

5. Final remarks. Throughout this paper, we have relied on the elliptic curves

$$E_i := y^2 + xy = x^3 + \ell_i$$

to prove Theorem 1.6. However, a careful reading of our arguments reveals that only the following facts about the E_i were used:

- E_i is a Serre curve, and
- $\Delta_i = \ell_i(432\ell_i + 1)$

It is clearly necessary for the E_i to be Serre curves, while precise knowledge of the discriminant of E_i allowed us to compare the ramification of ℓ_i in various division fields. While Theorem 1.6 provides infinitely many explicit examples of Serre k-tuples, the arguments in this paper actually prove the following more general statement.

THEOREM 5.1. *Let $E_1, \dots, E_k$ be elliptic curves with respective discriminants $\Delta_1, \dots, \Delta_k$. Suppose that each E_i is a Serre curve, and that for $i = 1, \dots, k$ there exist odd primes $\ell_i > 3$ such that*

- $v_{\ell_i}(\Delta_i) \equiv 1 \bmod 2$*;*
- *E_i has split multiplicative reduction at ℓ_i; and*
- $v_{\ell_i}(\Delta_j) = 0$ *for $i \neq j$.*

Then $(E_1, \dots, E_k)$ is a Serre k-tuple.

Acknowledgements. The authors would like to thank Álvaro Lozano-Robledo, Nathan Jones, and Sam Taylor for their helpful discussions at various points of the writing process. The authors would also like to thank the referee and editors for their useful comments and a quick editorial process.

References

[1] C. Adelmann, *The Decomposition of Primes in Torsion Point Fields*, Springer, Berlin, 2001.
[2] H. Daniels, *An infinite family of Serre curves*, J. Number Theory 155 (2015), 226–247.
[3] N. Jones, *GL_2-representations with maximal image*, Math. Res. Lett. 22 (2015), 803–839.
[4] N. Jones, *Pairs of elliptic curves with maximal Galois representations*, J. Number Theory 133 (2013), 3381–3393.
[5] Á. Lozano-Robledo and B. Lundell, *Bounds for the torsion of elliptic curves over extensions with bounded ramification*, Int. J. Number Theory 6 (2010), 1293–1309.
[6] K. Ribet, *Galois action on division points of Abelian varieties with real multiplications*, Amer. J. Math. 98 (1976), 751–804.
[7] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. 15 (1972), 259–331.
[8] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Springer, New York, 2009.

[9] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer, New York, 1994.

Harris B. Daniels
Department of Mathematics
Amherst College
Box 2239
Amherst, MA 01002-5000, U.S.A.
E-mail: hdaniels@amherst.edu

Jeffrey Hatley
Department of Mathematics
Union College
Bailey Hall 202
Schenectady, NY 12308, U.S.A.
E-mail: hatleyj@union.edu

James Ricci
Department of Mathematics and Computer Science
Daemen College
Duns Scotus 339
4380 Main Street
Amherst, NY 14226, U.S.A.
E-mail: jricci@daemen.edu