Galois representations with non-surjective traces

Chantal David, Concordia University
Hershy Kisilevsky, Concordia University
Francesco Pappalardi, Università Roma Tre

Abstract

Let E be an elliptic curve over $\mathbb{Q}$, and let r be an integer. According to the Lang–Trotter conjecture, the number of primes p such that $a_p(E) = r$ is either finite, or is asymptotic to $C_{E,r}\sqrt{x}/\log x$ where $C_{E,r}$ is a non-zero constant. A typical example of the former is the case of rational ℓ-torsion, where $a_p(E) = r$ is impossible if $r \equiv 1 \pmod{\ell}$. We prove in this paper that, when E has a rational ℓ-isogeny and $\ell \neq 11$, the number of primes p such that $a_p(E) \equiv r \pmod{\ell}$ is finite (for some r modulo ℓ) if and only if E has rational ℓ-torsion over the cyclotomic field $\mathbb{Q}(\zeta_\ell)$. The case $\ell = 11$ is special, and is also treated in the paper. We also classify all those occurences.

1 Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$ and let N_E denote its conductor. For any prime $p \nmid N_E$, let E_p be the elliptic curve over $\mathbb{F}_p$ obtained by reducing E modulo p. Let $a_p(E)$ be the trace of the Frobenius morphism of $E_p/\mathbb{F}_p$. Then, $\#E_p(\mathbb{F}_p) = p + 1 - a_p(E)$, and $|a_p(E)| \leq 2\sqrt{p}$. If $p > 3$, the case $a_p(E) = 0$ corresponds to supersingular reduction mod p.

For a fixed $r \in \mathbb{Z}$, let

$$\pi_{E,r}(x) = \#\left\{p \leq x, p \nmid N_E \ : \ a_p\left(E\right) = r\right\}.$$

If E has complex multiplication, Deuring [6] showed that $\pi_{E,0}(x) \sim \frac{1}{2}\pi(x)$, as the supersingular primes are exactly the primes which are inert in the field of complex multiplication. This is the only (non trivial) case where the asymptotic behavior of $\pi_{E,r}(x)$ is known. In all other cases, for E an elliptic curve over $\mathbb{Q}$, and $r \in \mathbb{Z}$, Lang and Trotter [9] conjectured that there exists a constant $C_{E,r}$ such that

$$\pi_{E,r}(x) \sim C_{E,r}\,\frac{\sqrt{x}}{\log x} \quad \text{ as } x \to \infty. \tag{1}$$

Lang and Trotter define $C_{E,r}$ "explicitly" for any E and r. When the constant is 0, the asymptotic relation is interpreted to mean that there is only a finite number of primes such that $a_p(E) = r$. We want to classify the cases where $C_{E,r} = 0$, i.e., the cases where the Lang-Trotter conjecture predicts only a finite number of primes p with $a_p(E) = r$. It will be clear from the explicit formula for the constants $C_{E,r}$ that $C_{E,r} = 0$ implies that $\pi_{E,r}(x)$ is bounded.

The Lang-Trotter constant is defined from the distributions of the traces $a_p(E)$ modulo m, for m a positive integer. Let $\rho_{E,m}$ be the Galois representation

$$\rho_{E,m} : \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \to \mathrm{Aut}(E[m])$$

where $E[m]$ is the subgroup of m-torsion points of $E(\overline{\mathbb{Q}})$. Since $E[m] \simeq (\mathbb{Z}/m\mathbb{Z})^2$, after choosing a basis for $E[m]$, we can identify $\mathrm{Aut}(E[m])$ with $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. Let $G(m)$ be the image of $\rho_{E,m}$ in $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, and for any subgroup G of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, let G_r be the subset of elements of G of trace r modulo m.

Let E be an elliptic curve without complex multiplication. Serre proved in [15] that the image of the Galois representation on the full torsion subgroup of $E(\overline{\mathbb{Q}})$ is an open subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$. It follows that there exists an integer $M = M_E$ such that $\rho_{E,\ell}$ is surjective for all primes ℓ not dividing M, and such that the image in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ of the Galois representation on the torsion subgroup of $E(\overline{\mathbb{Q}})$ is the full inverse image of $G(M)$. The Lang-Trotter constant $C_{E,r}$ is then defined as

$$C_{E,r} = \frac{2}{\pi} \frac{M\ |G(M)_r|}{|G(M)|} \prod_{\ell \nmid M} \frac{\ell\ |\mathrm{GL}_2(\mathbb{F}_\ell)_r|}{|\mathrm{GL}_2(\mathbb{F}_\ell)|}.$$

For the details, we refer the reader to [9], and to [5] for evidence supporting the conjectural value of the constant $C_{E,r}$. It follows from the definition of the constant that $C_{E,r} = 0$ if and only if $|G(M)_r| = 0$ as the infinite product converges to a positive number. In that case, $a_p(E) \not\equiv r \pmod{M}$ for all $p \nmid MN_E$. The Lang-Trotter conjecture then severely restricts the behavior of $\pi_{E,r}(x)$: if $\pi_{E,r}(x)$ is finite for some $r \in \mathbb{Z}$, then there is a positive integer M such that $\pi_{E,s}(x)$ is finite for all $s \equiv r \pmod{M}$. To our knowledge, the only cases of $C_{E,r} = 0$ presented in the literature are the curves with rational ℓ-torsion [9, p. 37].

For $E/\mathbb{Q}$ an elliptic curve and ℓ a prime, let $S_\ell(E)$ be the complement of the set of traces of E modulo ℓ, i.e.

$$S_\ell(E) = \mathbb{F}_\ell \setminus \{a \in \mathbb{F}_\ell\ :\ a_p(E) \equiv a \pmod{\ell} \text{ for some } p \nmid \ell N_E\}.$$

Serre proved in [15] that if $\ell \geq 5$ and $\rho_{E,\ell}$ is not surjective, then $G(\ell)$ is contained either in a Borel subgroup or in the normalizer of a Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$. This is an exceptional situation and for "most" elliptic curves $E/\mathbb{Q}$, $\rho_{E,\ell}$ is surjective for all primes. Precise estimates can be found in [7, 8]. We classify in this paper all elliptic curves $E/\mathbb{Q}$ for which $G(\ell)$ is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$, and $S_\ell(E) \neq \emptyset$. $G(\ell)$ is contained in a Borel subgroup if and only if E has a rational ℓ-isogeny. By the work of Mazur [10, 11], this can happen only for finitely many values of ℓ. This is not a complete classification of all cases where $C_{E,r} = 0$, as one should also look at exceptional Cartan primes (which are much more difficult since there is no analogue to Mazur's Theorem in that case) and one should also consider the image of $\rho_{E,m}$ for all positive integers m.

Theorem 1.1 *Let $\ell \neq 11$ be a prime, and let E be an elliptic curve over $\mathbb{Q}$ with a rational ℓ-isogeny. Then the following are equivalent:*

(i) $S_\ell(E) \neq \emptyset$;

(ii) E has non-trivial $\mathbb{Q}(\zeta_\ell)$-rational ℓ-torsion.

That (ii) implies (i) is straightforward (see Section 3); we prove in this paper that (i) implies (ii). We can also rephrase (ii) in terms of congruences for the $a_p(E)$'s, which gives the following corollary.

Corollary 1.2 *Let $\ell \neq 11$ be a prime, and let E be an elliptic curve over $\mathbb{Q}$ with a rational ℓ-isogeny, and such that $S_\ell(E) \neq \emptyset$. Then, there is an integer a with $1 \leq a \leq \ell - 1$ such that*

$$a_p(E) \equiv p^a + p^{\ell - a} \pmod{\ell}.$$

The case $\ell = 11$ is different, and does not fit Theorem 1.1. The following theorem will be proven in Section 8.

Theorem 1.3 *Let E be an elliptic curve over $\mathbb{Q}$ with a rational 11-isogeny, and such that $S_{11}(E) \neq \emptyset$. Then, E is isogenous to a twist of an elliptic curve with a $\mathbb{Q}(\zeta_{11})$-rational 11-torsion point.*

We now use theorems 1.1 and 1.3 to classify all possible curves $E/\mathbb{Q}$ with a rational ℓ-isogeny such that $S_\ell(E) \neq \emptyset$. This classification is summarized in the following theorem. Our proof of the non-existence of elliptic curves for which $S_{13}(E) \neq \emptyset$ is conditional to the Birch and Swinnerton-Dyer conjecture for abelian varieties over number fields (see Proposition 6.1).

Theorem 1.4 *Let ℓ be a prime, and let E be an elliptic curve over $\mathbb{Q}$ with a rational ℓ-isogeny, and such that $S_\ell(E) \neq \emptyset$. Let a be as in Corollary 1.2. Then, all possible values of ℓ, $S_\ell(E)$ and a are described in the following table. The last column gives a curve with minimal conductor for which $S_\ell(E)$ is as prescribed, in the notation of Cremona's tables [4].*

ℓ	$S_\ell(E)$	a	$E/\mathbb{Q}$	ℓ	$S_\ell(E)$	a	$E/\mathbb{Q}$
2	$\{1\}$	1	$E14A$	11	$\{3,4,6,7\}$	2	$E121A$
					$(\mathbb{F}_\ell^*)^2$	3	$E121B$
3	$\{1\}$	1	$E14A$		$\{3,4,5,7,10\}$	4	$E121C$
					$\{4,7\}$	–	$E1089F$
5	$\{1\}$	1	$E11A$				
	$\{3,4\}$	3	$E50A$	19	$(\mathbb{F}_\ell^*)^2$	5	$E361A$
				43	$(\mathbb{F}_\ell^*)^2$	11	$E1849A$
7	$\{1\}$	1	$E26B$	67	$(\mathbb{F}_\ell^*)^2$	17	$E4489A$
	$\{4,6\}$	3	$E294A$	163	$(\mathbb{F}_\ell^*)^2$	41	$E26569$
	$\{3,5,6\}$	5	$E49A$				

One notices that all the examples in the table of Theorem 1.4 which do not arise from rational ℓ-torsion over $\mathbb{Q}$ are non semistable elliptic curves. In fact, if E is a semistable elliptic curve over $\mathbb{Q}$, and if the image of the Galois representation $\rho_{E,\ell}$ is not surjective, then it is essentially because E has a $\mathbb{Q}$-rational ℓ-torsion point [15, Proposition 21].

2 Some Lemmas

Let E be an elliptic curve over $\mathbb{Q}$, ℓ a prime, and suppose that E has a rational ℓ-isogeny. Then, the Galois representation $\rho_{E,\ell}$ has the form

$$\rho_{E,\ell} \sim \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix} \tag{2}$$

where χ_1, χ_2 are characters of $G(\ell) = \mathrm{Gal}\left(\mathbb{Q}\left(E[\ell]\right)/\mathbb{Q}\right)$ taking values in $\mathbb{F}_\ell^*$. For $i = 1, 2$, let n_i be the order of χ_i, and let $N_i = \ker(\chi_i)$. N_i is a normal subgroup of $G(\ell)$, and we denote by K_i the fixed field of N_i. Then for $i = 1, 2$,

$$\mathrm{Gal}(K_i/\mathbb{Q}) \simeq G(\ell)/N_i$$

is a cyclic group of order n_i. The character groups of the Galois groups of K_1, K_2 and K_1K_2 are respectively:

$$\widehat{\mathrm{Gal}(K_1/\mathbb{Q})} = \langle \chi_1 \rangle;$$

$$\widehat{\mathrm{Gal}(K_2/\mathbb{Q})} = \langle \chi_2 \rangle;$$

$$\widehat{\mathrm{Gal}(K_1K_2/\mathbb{Q})} = \langle \chi_1, \chi_2 \rangle.$$

By the Weil pairing, $\chi_1\chi_2 = \omega_\ell$ the cyclotomic character, and therefore $\widehat{\mathrm{Gal}(\mathbb{Q}(\zeta_\ell)/\mathbb{Q})} = \langle\omega_\ell\rangle \subseteq \widehat{\mathrm{Gal}(K_1K_2/\mathbb{Q})}$, or equivalently $\mathbb{Q}(\zeta_\ell) \subseteq K_1K_2$.

The following lemma will allow us to reformulate Theorem 1.1 in terms of characters.

Lemma 2.1 *Let ℓ be a prime, and let $E/\mathbb{Q}$ be an elliptic curve with a rational ℓ-isogeny. The followings are equivalent:*

(i) E has a non-trivial $\mathbb{Q}(\zeta_\ell)$-rational ℓ-torsion point;

(ii) E is isogenous to a curve with a non-trivial $\mathbb{Q}(\zeta_\ell)$-rational ℓ-torsion point;

(iii) $K_1K_2 = \mathbb{Q}(\zeta_\ell)$;

(iv) $\langle\chi_1,\chi_2\rangle = \langle\omega_\ell\rangle$.

Proof: The equivalence of (iii) and (iv) follows from general properties of characters of Galois groups: let L_1, L_2 be abelian extensions of a field k, contained in some field K. Then, $L_1 \subseteq L_2 \iff \widehat{\mathrm{Gal}(L_1/k)} \subseteq \widehat{\mathrm{Gal}(L_2/k)}$. It is also clear that (iii) implies (i): we then have $K_1 \subseteq \mathbb{Q}(\zeta_\ell)$, and $K_1 = \mathbb{Q}(P_1)$ where P_1 is the ℓ-torsion point corresponding to χ_1. For (i) implies (iv), let P be the $\mathbb{Q}(\zeta_\ell)$-rational ℓ-torsion point on E. Then, either $\langle P\rangle$ is Galois stable, or $\mathbb{Q}\left(E[\ell]\right) \subseteq \mathbb{Q}(\zeta_\ell)$. In either cases,

$$\rho_{E,\ell} \sim \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix},$$

with $\chi_1 \in \langle\omega_\ell\rangle$, which gives $\langle\chi_1,\chi_2\rangle = \langle\omega_\ell\rangle$. Finally, we have to show that (ii) implies (i): Let $\phi : E' \to E$ be the isogeny where E' has $\mathbb{Q}(\zeta_\ell)$-rational ℓ-torsion. Let P_1, P_2 be a basis for $E'[\ell]$ giving the representation

$$\rho_{E',\ell} \sim \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix}, \text{ with } \chi_1,\chi_2 \in \langle\omega_\ell\rangle. \tag{3}$$

If $E'[\ell] \not\subseteq \ker\phi$, then $Q_1 = \phi(P_1)$, or $Q_2 = \phi(P_2)$ if $Q_1 = 0$, is a non-trivial $\mathbb{Q}(\zeta_\ell)$-rational ℓ-torsion point on E. If $E'[\ell] \subseteq \ker\phi$, let a be the largest integer such that $E'[\ell^a] \subseteq \ker\phi$. Since

$$E'[\ell^{a+1}]/E'[\ell^a] \text{ and } E'[\ell]$$

are isomorphic $\mathbb{F}_\ell[G]$-modules, let P_1' and P_2' be a basis for $E'[\ell^{a+1}]/E'[\ell^a]$ giving the representation (3). Then, either $Q_1' = \phi(P_1')$, or $Q_2' = \phi(P_2')$ if $Q_1' = 0$, is a non-trivial $\mathbb{Q}(\zeta_\ell)$-rational ℓ-torsion point on E. QED.

If E and E' are isogenous curves, then $a_p(E) = a_p(E')$ for all $p \nmid \ell N_E$. We will then classify up to isogeny the curves missing a trace modulo ℓ. The following lemmas describe the Galois representations of isogenous and twisted curves.

Lemma 2.2 *Let E be an elliptic curve over $\mathbb{Q}$ with a rational ℓ-isogeny. Choose $P_1 \in E[\ell]$ such that $P_1^\sigma = \chi_1(\sigma)P_1$ for all $\sigma \in G(\ell)$. Let E' be the isogenous curve $E' = E/\langle P_1 \rangle$. Then,*

$$\rho_{E',\ell} \sim \begin{pmatrix} \chi_2 & * \\ 0 & \chi_1 \end{pmatrix}.$$

Proof: Let ϕ denote the rational ℓ-isogeny between E and E', and let P_1, P_2 be a basis for $E[\ell]$ giving the representation $\rho_{E,\ell}$. We denote by ξ the cocycle in the upper right corner of $\rho_{E,\ell}$. Then, $\phi(P_2)$ is a ℓ-torsion point on E', and for $p \nmid \ell N_E$,

$$\phi(P_2)^{\sigma_p} = \phi(P_2^{\sigma_p}) = \phi(\xi(\sigma_p)P_1 + \chi_2(\sigma_p)P_2) = \chi_2(\sigma_p)\phi(P_2).$$

Since the determinant of $\rho_{E',\ell}$ is the cyclotomic character, this proves the lemma. QED.

Lemma 2.3 *Let E be an elliptic curve over $\mathbb{Q}$ with a rational ℓ-isogeny. Let $D \in \mathbb{Z}$, and let E_D be the twist of E by D. Then*

$$\rho_{E_D,\ell} \sim \begin{pmatrix} \left(\frac{D}{\cdot}\right)\chi_1 & * \\ 0 & \left(\frac{D}{\cdot}\right)\chi_2 \end{pmatrix}.$$

Proof: Let P_1, P_2 be a basis of $E[\ell]$ giving the representation (2), and let ϕ be the $\mathbb{Q}(\sqrt{D})$-isomorphism between E and E_D. Then, $\phi(P_1)$ and $\phi(P_2)$ form a basis for the ℓ-torsion on E_D. For $p \nmid \ell N_E$,

$$\phi(P_1)^{\sigma_p} = \phi^{\sigma_p}\left(P_1^{\sigma_p}\right) = \phi^{\sigma_p}\left(\chi_1(\sigma_p)P_1\right) = \left(\frac{D}{p}\right)\chi_1(\sigma_p)\phi(P_1).$$

Since the determinant of $\rho_{E_D,\ell}$ is the cyclotomic character, this proves the lemma. QED.

Lemma 2.4 *Let E be an elliptic curve over $\mathbb{Q}$. Let $D \neq 1$ be a squarefree integer with $(D, \ell N_E) = 1$, and let E_D be the twist of E by D. Then, $S_\ell(E_D) = S_\ell(E) \cap -S_\ell(E)$.*

Proof: As $(D, \ell N_E) = 1$, the field extensions $K_\ell = \mathbb{Q}(E[\ell])$ and $K_D = \mathbb{Q}(\sqrt{D})$ are disjoint [16, Proposition VII.4.1]. Let $K_{\ell,D} = K_\ell K_D$. Then,

$$\mathrm{Gal}(K_{\ell,D}/\mathbb{Q}) = \mathrm{Gal}(K_\ell/\mathbb{Q}) \times \mathrm{Gal}(K_D/\mathbb{Q}).$$

Let $b = \pm 1$, and let a be a trace of E modulo ℓ, i.e. $a_p(E) \equiv a \pmod{\ell}$ for some $p \nmid \ell N_E$. Then, by the Chebotarev Density Theorem, there is a positive proportion of primes p such that $\left(\frac{D}{p}\right) = b$ and $a_p(E) \equiv a \pmod{\ell}$. As

$$a_p(E_D) = \left(\frac{D}{p}\right) a_p(E),$$

a and $-a$ are traces of E_D modulo ℓ. This proves the result. QED.

3 Mazur's Theorem

We begin by proving the the easy side of Theorem 1.1. Corollary 1.2 also follows from the same arguments.

Proof of Theorem 1.1(ii) $\Rightarrow$ (i): By Lemma 2.1, the hypothesis can be rewritten as $\langle \chi_1, \chi_2 \rangle = \langle \omega_\ell \rangle$. Then, $\chi_1 = \omega_\ell^a$ and $\chi_2 = \omega_\ell^{\ell-a}$ for some integer $1 \leq a \leq \ell - 1$. Then, for all $p \nmid \ell N_E$,

$$a_p(E) \equiv \omega_\ell^a(\sigma_p) + \omega_\ell^{\ell-a}(\sigma_p) \equiv p^a + p^{\ell-a} \pmod{\ell}. \tag{4}$$

But this takes at most $\ell - 1$ values modulo ℓ, as p takes exactly all non-zero values modulo ℓ. QED.

Assuming Theorem 1.1, the same argument also proves Corollary 1.2.

We then have to prove the other implication of Theorem 1.1. By Mazur's Theorem [10, 11], there are only finitely many values of ℓ for which there is an elliptic curve $E/\mathbb{Q}$ with a rational ℓ-isogeny. More precisely, we reproduce here the table of [11] listing the only cases where $X_0(\ell)$ has noncuspidal rational points:

$\ell = 2, 3, 5, 7, 13$ and $X_0(\ell)$ has genus 0;

$\ell = 11, 17, 37$ and $\#Y_0(\ell)(\mathbb{Q}) = 3, 2, 2$ respectively;

$\ell = 19, 43, 67, 163$ and $\#Y_0(\ell)(\mathbb{Q}) = 1$ corresponding to the curve $E/\mathbb{Q}$ with complex multiplication by $\mathbb{Q}(\sqrt{-\ell})$.

The noncuspidal rational points on those modular curves correspond to j-invariants (or equivalently isomorphism classes) of elliptic curves over $\mathbb{Q}$ with a rational ℓ-isogeny. For $\ell = 11$ or $\ell \geq 17$, there are only finitely many possible j-invariants. We treat those separately in Sections 7 and 8.

We then concentrate on $\ell = 2, 3, 5, 7, 13$. Since $X_0(\ell)$ has genus 0, they are infinitely many isomorphism classes of curves with a rational ℓ-isogeny for those ℓ. We consider two cases, depending if n_1 and n_2 are coprime or not. As $\chi_1\chi_2$ is the cyclotomic character, it is necessary to have $\mathrm{lcm}\,(n_1, n_2) = \ell - 1$. If n_1 and n_2 are coprime, there are at most $\ell - 1$ possible traces $\chi_1(\sigma_p) + \chi_2(\sigma_p)$. This generalizes the case of rational ℓ-torsion, where $n_1 = 1$ and $n_2 = \ell - 1$. This case is done in Section 4.

If n_1 and n_2 are not coprime, one expects that $S_\ell(E) = \emptyset$ when there is no "relation" between χ_1 and χ_2. This is proven in Section 5. The final cases are classified in Section 6.

4 Coprime orders

Let E be an elliptic curve over $\mathbb{Q}$ with rational ℓ-torsion. Then, the Galois representation $\rho_{E,\ell}$ has the form

$$\rho_{E,\ell} \sim \begin{pmatrix} 1 & * \\ 0 & \omega_\ell \end{pmatrix}, \tag{5}$$

and for $p \nmid \ell N_E$

$$a_p(E) \equiv 1 + \omega_\ell(\sigma_p) \equiv p+1 \pmod{\ell}.$$

Then, from Dirichlet's Theorem, $S_\ell(E) = \{1\}$ when E has rational ℓ-torsion. This is a particular case of the following lemma.

Lemma 4.1 *Let ℓ be an odd prime, and let $E/\mathbb{Q}$ be an elliptic curve with a rational ℓ-isogeny. Suppose also that $(n_1, n_2) = 1$. Then K_1 is a subfield of the cyclotomic field $\mathbb{Q}(\zeta_\ell)$.*

Proof: Let

$$G_\ell = \mathrm{Gal}\,(\mathbb{Q}(E[\ell])/\mathbb{Q}(\zeta_\ell)) = \{g \in G(\ell) \ : \ \det g = 1\}.$$

As $(n_1, n_2) = 1$,

$$G_\ell = \left\{ g \in G(\ell) \ : \ g = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \right\}.$$

Then, either G_ℓ is trivial, or $G_\ell \simeq \mathbb{F}_\ell$. Let $G(\ell)'$ be the commutator of $G(\ell)$. Clearly, $G(\ell)' \subseteq G_\ell$. If G_ℓ is trivial, then $G(\ell)' = G_\ell$. If not, let $A = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \in G_\ell$ with $a \neq 0$ and $B = \begin{pmatrix} \beta_1 & b \\ 0 & \beta_2 \end{pmatrix} \in G(\ell)$ with $\beta_1 \neq \beta_2$. Then, $AB \neq BA$, so that $G(\ell)' \neq \{1\}$ which proves that $G(\ell)' = G_\ell$. Then, as $K_1/\mathbb{Q}$ is abelian,

$$\mathrm{Gal}\,(\mathbb{Q}(E[\ell])/\mathbb{Q}(\zeta_\ell)) = G_\ell = G(\ell)' \subseteq \mathrm{Gal}\,(\mathbb{Q}(E[\ell])/K_1),$$

i.e. $K_1 \subseteq \mathbb{Q}(\zeta_\ell)$. QED.

This proves Theorem 1.1 in the case where n_1 and n_2 are coprime. Using Mazur's Theorem, we now list all cases of elliptic curves with a rational ℓ-isogeny for $\ell = 2, 3, 5, 7, 13$ and with $(n_1, n_2) = 1$. There is only one case other than rational torsion.

Theorem 4.2 *Let $\ell = 2, 3, 5, 7, 13$, and let $E/\mathbb{Q}$ be an elliptic curve with a rational ℓ-isogeny. Suppose also that $(n_1, n_2) = 1$. Then, either $\ell = 2, 3, 5, 7$ and E is isogenous to a curve with rational ℓ-torsion, or E is isogenous to a curve with $\mathbb{Q}(\sqrt{-7})$-rational 7-torsion. More precisely, the possible values of ℓ, $S_\ell(E)$ and a are described in the following table. The last column gives a curve with minimal conductor for which $S_\ell(E)$ is as prescribed.*

ℓ	$S_\ell(E)$	a	$E/\mathbb{Q}$
2	$\{1\}$	1	$E14A$
3	$\{1\}$	1	$E14A$
5	$\{1\}$	1	$E11A$
7	$\{1\}$	1	$E26B$
	$\{4,6\}$	3	$E294A$

Proof of Theorem 4.2: Using Lemma 2.2, we can always exchange χ_1 and χ_2, then n_1 and n_2, by an isogeny.

$\underline{\ell = 2}$: The only possibility is $n_1 = n_2 = 1$, i.e. E has rational torsion of order 2.

$\underline{\ell = 3}$: The only possibility is $n_1 = 1$ and $n_2 = 2$, i.e. E has rational torsion of order 3.

$\underline{\ell = 5}$: The only possibility is $n_1 = 1$ and $n_2 = 4$, E has rational torsion of order 5.

$\underline{\ell = 7}$: If $n_1 = 1$ and $n_2 = 6$, then E has rational torsion of order 7. If $n_1 = 2$ and $n_2 = 3$, then by Lemma 4.1, $K_1 = \mathbb{Q}(\sqrt{-7})$ and $\chi_1 = \left(\frac{-7}{\cdot}\right)$. As $\chi_1\chi_2 = \omega_7$, we have

$$\rho_{E,7} \sim \begin{pmatrix} \left(\frac{-7}{\cdot}\right) & * \\ 0 & \left(\frac{-7}{\cdot}\right)\omega_7 \end{pmatrix} = \begin{pmatrix} \omega_7^3 & * \\ 0 & \omega_7^4 \end{pmatrix}. \qquad (6)$$

Since $K_1 = \mathbb{Q}(\sqrt{-7})$, E has rational torsion over $\mathbb{Q}(\sqrt{-7})$. Equivalently, E is a twist by -7 of a curve with rational 7-torsion. Indeed, let E' be the twist by -7 of E. It is clear that E' has rational 7-torsion. Then, if $n_1 = 2$ and $n_2 = 3$, $\rho_{E,7}$ is given by (6),

$$a_p(E) \equiv \omega_7^3(\sigma_p) + \omega_7^4(\sigma_p) \equiv p^3 + p^4 \pmod{\ell},$$

and $S_\ell(E) = \{4, 6\}$. This gives one of the cases of the classification of Theorem 1.4. As $X_1(7)$ has genus 0, there are infinitely many isomorphism classes of elliptic curves over $\mathbb{Q}$ such that $\rho_{E,7}$ is given by (6). By inspection of Cremona's tables [4], one finds that such a curve with minimal conductor is $E = E294A2$ of conductor $N_E = 2\cdot3\cdot7^2$. E is the twist by -7 of the curve $E' = E294B2$ of conductor $N_{E'} = 2\cdot3\cdot7^2$, and E' has rational 7-torsion. The curves E and E' have minimal equations

$$\begin{aligned} E = E294A2 &: \ y^2 + xy + y = x^3 + x^2 - 6910x - 232261; \\ E' = E294B2 &: \ y^2 + xy = x^3 - 141x + 657. \end{aligned}$$

$\underline{\ell = 13}$: As there are no elliptic curves over $\mathbb{Q}$ with rational 13-torsion [11, Theorem 2], the only possible case is $n_1 = 4$ and $n_2 = 3$. By Lemma 4.1, K_1 is contained in the cyclotomic field $\mathbb{Q}(\zeta_{13})$, which implies that $K = \mathbb{Q}(\sqrt{13}) \subseteq K_1$. Let $G_K = \mathrm{Gal}(\overline{K}/K)$, and consider E as an elliptic curve over K. Then

$$\rho_{E,13}|_{G_K} \sim \begin{pmatrix} \chi_1|_{G_K} & * \\ 0 & \chi_2|_{G_K} \end{pmatrix}$$

where $\chi_1|_{G_K}$ is the character of order 2 associated with the quadratic extension K_1/K. Twisting by $\chi_1|_{G_K}$, we get a curve E' over $K = \mathbb{Q}(\sqrt{13})$ with a K-rational 13-torsion point. This is impossible by a result of Momose [13, p. 157].

This completes the proof of Theorem 4.2. QED.

5 Non coprime orders

We will prove in that section the following theorem:

Theorem 5.1 *Let $\ell = 2, 3, 5, 7, 13$, and let $E/\mathbb{Q}$ be an elliptic curve with a rational ℓ-isogeny for which $S_\ell(E) \neq \emptyset$. Suppose also that $(n_1, n_2) > 1$. Then, $K_2 \subseteq K_1$ or $K_1 \subseteq K_2$.*

In the next four lemmas, K_1 and K_2 are any cyclic extensions of $\mathbb{Q}$ of degree n_1 and n_2, and character groups $\langle \chi_1 \rangle$ and $\langle \chi_2 \rangle$ respectively. Let $K_0 = K_1 \cap K_2$ and $s = [K_0 : \mathbb{Q}]$.

Lemma 5.2 *Suppose that $K_0 = \mathbb{Q}$. Then, for any $a_1 \in Im(\chi_1)$ and $a_2 \in Im(\chi_2)$, there is a positive proportion of primes p such that*

$$\chi_1(\sigma_p) = a_1 \quad \text{and} \quad \chi_2(\sigma_p) = a_2.$$

Proof: Since $K_0 = \mathbb{Q}$, we have

$$\mathrm{Gal}\,(K_1K_2/\mathbb{Q}) \simeq \mathrm{Gal}\,(K_1/\mathbb{Q}) \times \mathrm{Gal}\,(K_2/\mathbb{Q})\,.$$

Let g be an element of $\mathrm{Gal}\,(K_1K_2/\mathbb{Q})$ such that $\chi_1(g) = a_1$ and $\chi_2(g) = a_2$. By the Chebotarev Density Theorem, there is a positive proportion of primes p such that $\sigma_p = g$. QED.

Lemma 5.3 *Suppose that $(s, n_2/s) = 1$. Then,*

$$\mathrm{Gal}\,\widehat{(K_1K_2/\mathbb{Q})} = \langle \chi_1 \rangle \times \langle \chi_2^s \rangle\,.$$

Proof: Let L be the unique subfield of degree n_2/s of K_2. As s and n_2/s are coprime, L and K_0 are disjoint, and $K_1K_2 = K_1L$ with $K_1 \cap L = \mathbb{Q}$. Then,

$$\mathrm{Gal}\,(K_1K_2/\mathbb{Q}) = \mathrm{Gal}(K_1L/\mathbb{Q}) \simeq \mathrm{Gal}\,(K_1/\mathbb{Q}) \times \mathrm{Gal}\,(L/\mathbb{Q})\,,$$

and as $\widehat{\mathrm{Gal}(L/\mathbb{Q})} = \langle \chi_2^s \rangle$, this proves the lemma. QED.

Lemma 5.4 *If $s = 2$, and $2n_2$ divides $n_1 + n_2$, then $\chi_1\chi_2$ has order dividing $n_1/2$.*

Proof: As $s = 2$,

$$\widehat{\mathrm{Gal}(K_0/\mathbb{Q})} = \left\langle \chi_1^{n_1/2} \right\rangle = \left\langle \chi_2^{n_2/2} \right\rangle,$$

and $\chi_1^{n_1/2} = \chi_2^{n_2/2}$. Then, $(\chi_1\chi_2)^{n_1/2} = \chi_2^{(n_1+n_2)/2}$, which proves the result. QED.

Lemma 5.5 *If $n_1 = n_2 = 12$, and $s = 4$ or $s = 6$, then $\chi_1\chi_2$ has order 6.*

Proof: Similar to the previous lemma. QED.

Proof of Theorem 5.1: There are only finitely many tuples (ℓ, n_1, n_2, s) where $\ell = 2, 3, 5, 7, 13$, $\mathrm{lcm}(n_1, n_2) = \ell - 1$, $(n_1, n_2) > 1$ and $s \,|\, (n_1, n_2)$. We have to show that there are no such tuples associated to the Galois representation of an elliptic curve $E/\mathbb{Q}$ with a rational ℓ-isogeny for which $S_\ell(E) \neq \emptyset$, $K_1 \not\subseteq K_2$ and $K_2 \not\subseteq K_1$. Because we can exchange χ_1 and χ_2 by an isogeny, we may suppose that $n_1 \geq n_2$. The tuples (ℓ, n_1, n_2, n_2) would correspond to representations with $K_2 \subseteq K_1$, and the tuples $(\ell, n_1, n_2, 1)$ would correspond to representations for which $S_\ell(E) = \emptyset$ by Lemma 5.2 as $\mathrm{Im}(\chi_1) + \mathrm{Im}(\chi_2) = \mathbb{F}_\ell$ in each case. Under those restrictions, the possible tuples (ℓ, n_1, n_2, s) are:

$\ell = 5$: (5,4,4,2);

$\ell = 7$: (7,6,6,2), (7,6,6,3);

$\ell = 13$: (13,12,12,2), (13,12,12,3), (13,12,12,4), (13,12,12,6), (13,12,6,2), (13,12,6,3), (13,12,4,2), (13,6,4,2).

By Lemmas 5.4 and 5.5, the tuples

$$(5, 4, 4, 2), (7, 6, 6, 2), (13, 12, 12, 2), (13, 12, 4, 2), (13, 12, 12, 4), (13, 12, 12, 6)$$

cannot be associated with the Galois representation $\rho_{E,\ell}$ of an elliptic curve with a rational ℓ-isogeny. We also prove that the tuple $(13, 6, 4, 2)$ cannot occur. After an isogeny, we consider $(13, 4, 6, 2)$. We have $[K_1K_2 : \mathbb{Q}] = 12$, which implies that $K_1K_2 = \mathbb{Q}(\zeta_{13})$. There is then a unique quadratic subfield of K_1K_2, namely $K = \mathbb{Q}(\sqrt{13})$. We consider E as an elliptic curve over K. Then $\chi_1|_K, \chi_2|_K$ are characters on $\mathrm{Gal}(\overline{K}/K) \subseteq \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ of order 2 and 3 respectively. By twisting the representation by the quadratic character $\chi_1|_K$, one gets an elliptic curve over K with a K-rational 13 torsion point. This is impossible by the results of Momose [13, p. 157].

The remaining tuples are:

$\ell = 7$: (7,6,6,3);

$\ell = 13$: (13,12,12,3), (13,12,6,2), (13,12,6,3).

We now show that if any of those tuples is associated to the Galois representation of an elliptic curve $E/\mathbb{Q}$ with a rational ℓ-isogeny, then $S_\ell(E) = \emptyset$. Indeed, by Lemma 5.3,

$$\mathrm{Gal}\,(\widehat{K_1K_2}/\mathbb{Q}) = \langle \chi_1 \rangle \times \langle \chi_2^s \rangle$$

for all those tuples. Then, as $\chi_2 \in \widehat{\mathrm{Gal}(K_2/\mathbb{Q})} \subseteq \mathrm{Gal}\,\widehat{(K_1K_2/\mathbb{Q})}$, we can write

$$\chi_2 = \chi_1^m \chi_2^{ns}$$

with $0 \le m < n_1$ and $0 \le n < (n_2/s)$ in a unique way. There are of course only a few values of m, n which are possible if χ_1, χ_2 are the diagonal characters of the Galois representation $\rho_{E,\ell}$, with $K_2 \not\subseteq K_1$, or equivalently χ_2 is not a power of χ_1. In particular, m and n must be such that χ_2 and $\chi_1\chi_2$ have order n_2 and $\ell - 1$ respectively. We then compute all possible tuples (m, n) under these conditions, and check that $S_\ell(E) = \emptyset$ in each case.

For example, we do here the computations for the tuple $(7, 6, 6, 3)$. By Lemma 5.3, we know that

$$\mathrm{Gal}\,\widehat{(K_1K_2/\mathbb{Q})} = \langle \chi_1 \rangle \times \left\langle \chi_2^3 \right\rangle.$$

We can then write $\chi_2 = \chi_1^m \chi_2^{3n}$ in a unique way for some $0 \le m \le 5$ and $0 \le n \le 1$. Since χ_2 is not a power of χ_1, we have $n = 1$, and since χ_1 and $\chi_1\chi_2$ have order 6, the only possibilities are $(m, n) = (1, 1)$ or $(m, n) = (4, 1)$. If $(m, n) = (1, 1)$, then $\chi_2 = \chi_1\chi_2^3 \iff \chi_1 = \chi_2^4$ contrary to the hypothesis $K_1 \not\subseteq K_2$. We are then left with one possibility, namely $\chi_2 = \chi_1^4\chi_2^3$, which could occur for the diagonal characters of an elliptic curve with a rational 7-isogeny described by the tuple $(7, 6, 6, 3)$. Then, χ_1 and χ_2^3 are independent characters, i.e. for all $a \in \mathbb{F}_7^*$ and all $b \in \{\pm 1\} \subseteq \mathbb{F}_7^*$, there is a positive proportion of primes p such that

$$\chi_1(\sigma_p) = a \quad \text{and} \quad \chi_2^3(\sigma_p) = b$$

by the Chebotarev Density Theorem. Then, the traces

$$\chi_1(\sigma_p) + \chi_2(\sigma_p) = \chi_1(\sigma_p) + \chi_1^4(\sigma_p)\chi_2^3(\sigma_p)$$

take all values $a \pm a^4$ for all $a \in \mathbb{F}_7^*$, and this last set is $\mathbb{F}_7$.

Treating similarly the remaining 3 tuples listed above, this completes the proof of Theorem 5.1. QED.

By the results of Lemma 4.1 and Theorem 5.1, we can prove Theorem 1.1 for $\ell = 2, 3, 5, 7, 13$. Indeed, if $K_1 \subseteq K_2$

$$\langle \chi_1 \rangle \subseteq \langle \chi_2 \rangle = \langle \chi_1, \chi_2 \rangle = \langle \omega_\ell \rangle.$$

Then $K_1 \subseteq \mathbb{Q}(\zeta_\ell)$, and E has rational torsion over K_1.

6 χ_1 is a power of χ_2

Let $E/\mathbb{Q}$ be an elliptic curve with a rational ℓ-isogeny such that $(n_1, n_2) > 1$ and $S_\ell(E) \neq \emptyset$. Then, by Theorem 5.1, $K_1 \subseteq K_2$ or $K_2 \subseteq K_1$. By exchanging E with an isogenous curve if necessary, we assume in this section that $K_1 \subseteq K_2$. Then, $K_2 = \mathbb{Q}(\zeta_\ell)$ and

$$\chi_1 = \omega_\ell^{\ell - a} \quad \text{and} \quad \chi_2 = \omega_\ell^a$$

with $1 < a < \ell - 1$ and $(a, \ell - 1) = 1$. We treat each of the possible cases in turn. This gives the final cases of Theorem 1.4 for $\ell = 2, 3, 5, 7, 13$.

$\underline{\ell = 5:}$ $a = 3$ is the only possibility. In this case

$$\chi_1 = \omega_5^2 = \left(\frac{5}{\cdot}\right) \quad \text{and} \quad \chi_2 = \omega_5^3 = \left(\frac{5}{\cdot}\right) \omega_5,$$

and $S_5(E) = \{3, 4\}$. Then, $K_1 = \mathbb{Q}(\sqrt{5})$ and E is the twist by 5 of an elliptic curve $E'/\mathbb{Q}$ with rational 5-torsion. There are infinitely many such elliptic curves E as $X_1(5)$ has genus 0. By inspection of Cremona's tables [4], the example with smallest conductor is $E = E50A$. $E50B2$ have rational 5-torsion.

$\underline{\ell = 7:}$ $a = 5$ is the only possibility. In this case

$$\chi_1 = \omega_7^2 \quad \text{and} \quad \chi_2 = \omega_7^5,$$

and $S_7(E) = \{3, 5, 6\}$. Then, K_1 is the cubic field inside $\mathbb{Q}(\zeta_7)$ and E has a rational 7-torsion over K_1. The example with smallest conductor is the curve $E = E49A1$ with complex multiplication by the maximal order in $\mathbb{Q}(\sqrt{-7})$ (see also Section 7). For curves without complex multiplication, the example with smallest conductor is $E = E637A$ with conductor $N_E = 637 = 7^2 \cdot 13$.

$\underline{\ell = 13:}$ The possible values of a are $5, 7, 11$. Then, $[K_1 : \mathbb{Q}] = 3, 2, 6$ respectively, and E has rational 13-torsion over $K_1 \subseteq \mathbb{Q}(\zeta_{13})$. If $a = 7$, $K_1 = \mathbb{Q}(\sqrt{13})$ which is impossible by the result of Momose [13]. We want to generalize this result to $K_1 = Q(\zeta_{13} + \zeta_{13}^{-1})$.

Proposition 6.1 *Assume the Birch and Swinnerton-Dyer conjecture for abelian varieties over number fields. Then, $X_1(13)(K_{13})$ has no noncuspidal K_{13}-rational points, where $K_{13} = Q(\zeta_{13} + \zeta_{13}^{-1})$.*

Proof: The modular curve $X_1(13)$ has genus 2, and has 12 cusps over K_{13}, 6 rational cusps and 6 cusps defined over K_{13}. Let $J_1(13)$ be the Jacobian of $X_1(13)$. According to the Birch and Swinnerton-Dyer conjecture, the rank of $J_1(13)(K_{13})$ is the order of vanishing of the L-series $L(s, J_1(13), K_{13})$ at s=1. Let f_1 and f_2 be a basis of eigenforms for the 2-dimensional space of cusp forms $S_2(\Gamma_1(13))$. Then,

$$L(s, J_1(13), \mathbb{Q}) = L(s, f_1)\ L(s, f_2),$$

and

$$L(s, J_1(13), K_{13}) = \prod_{\chi} L(s, f_1, \chi)\ L(s, f_2, \chi)$$

where the product is taken for all χ characters of $\mathrm{Gal}\,(K_{13}/\mathbb{Q})$. The order of vanishing at $s = 1$ of each

$$L(s, f_i, \chi) = \sum_{n \geq 0} a_n(f_i)\ \chi(n)\ n^{-s}$$

was computed by J. Fearnley using PARI [2], and he showed that each $L(s, f_i, \chi)$ does not vanish at $s = 1$. Assuming the Birch and Swinnerton-Dyer conjecture, this shows that $J_1(13)(K)$ has rank 0.

We now compute $\#X_1(13)(K_{13})$, using Coleman's effective version of Chabauty's estimate [3]: if C is a curve of genus g over a number field K with Mordell-Weil group of rank at most $g-1$, if $\mathfrak{p}$ is an unramified prime of K at which C has good reduction, and if the residue characteristic of $\mathfrak{p}$ is greater than $2g$, then

$$\#C(K) \leq \#C(\mathbb{F}_{\mathfrak{p}}) + 2g - 2.$$

We take $C = X_1(13)$, $K = K_{13} = \mathbb{Q}(\zeta_{13} + \zeta_{13}^{-1})$, and $\mathfrak{p}$ a prime of K_{13} of residue characteristic 5. This gives

$$\#X_1(13)(K_{13}) \leq \#X_1(13)(\mathbb{F}_{25}) + 2. \tag{7}$$

We then have to count the number of points of $X_1(13)$ over the finite field with 25 elements. But, following Ogg [14], we use the fact that the curve $X_1(13)$ is also a moduli space in finite characteristic, and $X_1(13)(\mathbb{F}_{25})$ parametrizes isomorphism classes of elliptic curves over $\mathbb{F}_{25}$ with a $\mathbb{F}_{25}$-rational 13-torsion point. Suppose that $X_1(13)(\mathbb{F}_{25})$ has a non-cuspidal rational point corresponding to an elliptic curve E over $\mathbb{F}_{25}$. Then, we must have $13 \mid 26 - a_{25}(E)$, with $|a_{25}(E)| \leq 10$, where $a_{25}(E)$ is the trace of the Frobenius endomorphism over $\mathbb{F}_{25}$. This implies that $a_{25}(E) = 0$, which is impossible as then E would be a supersingular elliptic curve in characteristic 5, and 5 splits in the quadratic field $\mathbb{Q}\left(\sqrt{a_{25}^2(E) - 4 \cdot 25}\right) = \mathbb{Q}(i)$. It follows that $X_1(13)(\mathbb{F}_{25})$ has no non-cuspidal points, and using (7), we get $\#X_1(13)(K_{13}) \leq 14$. Suppose that $P \in X_1(13)(K_{13})$ is a non-cuspidal point. Then, $P \notin X_1(13)\left(\mathbb{Q}(\sqrt{13})\right)$ by the result of Momose [13], and then P has 3 or 6 Galois conjugates, which are also points on $X_1(13)(K_{13})$. Then, $\#X_1(13)(K_{13}) \geq 15$, which contradicts (7). This proves that, under the Birch and Swinnerton-Dyer conjecture, $X_1(13)(K_{13})$ has no non-cuspidal points. QED.

7 Complex multiplication curves

The case of curves with complex multiplication is well-know, and we recall it here. For such a curve, we know how to compute the $a_p(E)$'s by the work of Deuring [6], who proved that $L(E, s) = L(s, \chi)$ for some Hecke character χ. We use here the explicit formulas given by Stark in [17] for the values of $a_p(E)$ at split primes p.

For $\ell \geq 7$, let E_ℓ be the elliptic curve over $\mathbb{Q}$ with complex multiplication by the maximal order in $\mathbb{Q}(\sqrt{-\ell})$ and conductor $N_{E_\ell} = \ell^2$. Then, $\rho_{E_\ell,\ell}$ is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$. We show in this section that $S_\ell(E_\ell)$ contains exactly half of elements of $\mathbb{F}_\ell^*$, and we exhibit the relation between the 2 characters χ_1 and χ_2 of the Galois representation $\rho_{E_\ell,\ell}$.

Lemma 7.1 *Let E_ℓ be one of the 6 curves defined above. Then,*

$$S_\ell(E_\ell) = \begin{cases} \mathbb{F}_\ell^* \setminus (\mathbb{F}_\ell^*)^2 & \text{for } \ell = 7; \\ (\mathbb{F}_\ell^*)^2 & \text{for } \ell = 11, 19, 43, 67, 163. \end{cases}$$

Proof: For primes p inert in $\mathbb{Q}(\sqrt{-\ell})$, $a_p(E_\ell) = 0$. Let p be a prime which splits in $\mathbb{Q}(\sqrt{-\ell})$, $4p = u^2 + \ell v^2$ for some $u, v \in \mathbb{Z}$. Then from [17, p. 1118]

$$a_p(E_\ell) = \begin{cases} \left(\frac{u}{\ell}\right) u & \text{for } \ell = 7; \\ -\left(\frac{u}{\ell}\right) u & \text{for } \ell = 11, 19, 43, 67, 163. \end{cases}$$

As $\ell \equiv 3 \pmod 4$, $\left(\frac{u}{\ell}\right) u$ is always a square modulo ℓ. Also, for any $a \in \mathbb{F}_\ell^*$, we can choose split primes $p \equiv (a/2)^2 \pmod \ell$. This proves the result. QED.

We now examine the characters χ_1 and χ_2 of the Galois representation $\rho_{E_\ell,\ell}$. If p is a split prime with $4p = u^2 + \ell v^2$ for some $u, v \in \mathbb{Z}$, then the characteristic polynomial $x^2 - a_p(E)x + p$ has a double root

$$\chi_1(\sigma_p) = \chi_2(\sigma_p) = (-1)^{(\ell^2-1)/8} \left(\frac{u}{\ell}\right) \frac{u}{2}$$

modulo ℓ. If p is an inert prime, then the characteristic polynomial $x^2 + p$ has roots

$$\chi_1(\sigma_p) = \pm\sqrt{-p} \quad \text{and} \quad \chi_2(\sigma_p) = -\chi_1(\sigma_p)$$

modulo ℓ. Also, for any $a \in \mathbb{F}_\ell^*$, we can choose an inert prime p such that $\chi_1(\sigma_p) = a$ or $\chi_2(\sigma_p) = a$; indeed, we take $p \equiv -a^2 \pmod \ell$. We now determine how the sign $\chi_1(\sigma_p) = \pm\sqrt{-p}$ is chosen. This will give the relation between χ_1 and χ_2.

Lemma 7.2 *Let χ_1 and χ_2 be the characters of (2) for one of the curves E_ℓ defined above. Suppose that $\chi_1(\sigma_p) \notin (\mathbb{F}_\ell^*)^2$ for some inert prime p. Then, for all inert primes p, $\chi_1(\sigma_p) \notin (\mathbb{F}_\ell^*)^2$ and $\chi_2(\sigma_p) \in (\mathbb{F}_\ell^*)^2$.*

Proof: Let N be the normal subgroup of $G(\ell)$ consisting of the elements fixing the complex multiplication field $\mathbb{Q}(\sqrt{-\ell})$. Then,

$$N = \left\{ \begin{pmatrix} \chi_1(\sigma_p) & * \\ 0 & \chi_2(\sigma_p) \end{pmatrix} \text{ such that } p \text{ splits in } \mathbb{Q}(\sqrt{-\ell}) \right\}.$$

Let $h = \rho_{E_\ell,\ell}(\sigma_p)$ for some inert prime p with $\chi_1(\sigma_p) \notin (\mathbb{F}_\ell^*)^2$. Then, $h^n = \begin{pmatrix} -1 & * \\ 0 & 1 \end{pmatrix}$ for some integer n. Let $g = h^n$. As $G(\ell)$ is the disjoint union of the 2 cosets N and gN, for any inert prime p, $\rho_{E,\ell}(\sigma_p)$ can be written as

$$\begin{pmatrix} -1 & * \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a^2 & * \\ 0 & a^2 \end{pmatrix} = \begin{pmatrix} -a^2 & * \\ 0 & a^2 \end{pmatrix}$$

for some $a \in \mathbb{F}_\ell^*$. This proves the result. QED.

As we can always exchange χ_1 and χ_2 by an isogeny, we can suppose that χ_1 and χ_2 are as in the lemma. Then, χ_1 and χ_2 are characters of order $\ell - 1$ and $(\ell - 1)/2$ respectively, and

$$\chi_2 = \left(\frac{-\ell}{\cdot}\right) \chi_1 = \chi_1^{(\ell+1)/2}.$$

As $\chi_1\chi_2 = \omega_\ell$, this is equivalent to $\chi_1 = \omega_\ell^a$ and $\chi_2 = \omega_\ell^{\ell-a}$ where $a = (\ell + 1)/4$. Together with Lemma 7.1, this gives the last 4 entries of the table of Theorem 1.4.

If E is any other curve in the isomorphism class of E_ℓ, then E is a quadratic twist of E_ℓ by some squarefree integer D. Let $E_{\ell,D}$ denote the twist by D of E_ℓ. If $D \neq 1$ and $(D, \ell) = 1$, then $S_\ell(E_{\ell,D}) = \emptyset$ by Lemma 2.4 and Lemma 7.1. If $\ell = D$, then $E_{\ell,D}$ is isogenous to E_ℓ. If $D \neq \ell$ and $\ell | D$, then E is the twist of a curve isogenous to E_ℓ and $S_\ell(E_{\ell,D}) = \emptyset$.

8 Exceptional ℓ

$\underline{\ell = 11:}$ The modular curve $X_0(11)$ has genus 1, and $X_0(11)(\mathbb{Q})$ has 3 noncuspidal rational points corresponding to the j-invariants $j_1 = -11 \cdot 131^3$, $j_2 = -2^{15}$ and $j_3 = -11^2$. The second j-invariant corresponds to complex multiplication by $\mathbb{Q}(\sqrt{-11})$, and each j-invariant has a model with conductor 11^2. With the notation of Cremona's tables [4], let $E_1 = E121A1$, $E_2 = E121B1$ and $E_3 = E121C1$ such that $j(E_i) = j_i$ for $i = 1, 2, 3$. The minimal equations for E_1, E_2, E_3 are

$$\begin{aligned} E_1 &: y^2 + xy + y = x^3 + x^2 - 30x - 76 \\ E_2 &: y^2 + y = x^3 - x^2 - 7x + 10 \\ E_3 &: y^2 + xy = x^3 + x^2 - 2x - 7. \end{aligned}$$

For those curves, $K_1, K_2 \subseteq \mathbb{Q}(\zeta_{11})$ because they are cyclic extensions of degree dividing 10 ramifying only at the prime 11 [16, Proposition VII.4.1] Then,

$$\chi_1 = \omega_{11}^a \quad \text{and} \quad \chi_2 = \omega_{11}^{11-a}$$

for some $1 < a < 10$, and

$$a_p(E_i) \equiv p^a + p^{11-a} \pmod{11}.$$

By computing the first a_p's for each curve, one checks that E_1, E_2, E_3 corresponds to $a = 2, 3, 4$ respectively (possibly after exchanging χ_1 and χ_2 by considering an isogenous curve). The following congruences then hold:

$$\begin{aligned} a_p(E_1) &\equiv p^2 + p^9 \pmod{11}; \\ a_p(E_2) &\equiv p^3 + p^8 \pmod{11}; \\ a_p(E_3) &\equiv p^4 + p^7 \pmod{11}. \end{aligned}$$

This gives $S_{11}(E_1) = \{3, 4, 6, 7\}$, $S_{11}(E_2) = \{1, 3, 4, 5, 9\}$ (all the squares, as shown in Section 7), and $S_{11}(E_3) = \{3, 4, 5, 7, 10\}$.

For the complex multiplication curve E_2, the twist by -11 is the isogenous curve $E121B2$. Then for all twists $E_{2,D}$ of E_2 by a squarefree integer $D \neq 1, -11$, $S_{11}(E_{2,D}) = \emptyset$ by Lemmas 2.4 and 7.1.

E_1 is isogenous to the twist of E_3 by -11, and for any twist E_D of E_1 or E_3 by a squarefree integer $D \neq 1, -11$, $S_{11}(E_D) = \{4, 7\}$ by Lemma 2.4. Such a twist with minimal conductor is $E = E1089F$, the twist of E_1 by 3.

This proves Theorem 1.3 and Theorem 1.4 for $\ell = 11$. Then, the case $\ell = 11$ does not fit Theorem 1.1. For any twist E_D of E_1 or E_2 as above, $S_\ell(E_D) = \{4, 7\}$ but K_1K_2 contains $\mathbb{Q}(\sqrt{D})$ because

$$\left(\frac{D}{\cdot}\right) \in \mathrm{Gal}(\widehat{K_1K_2}/\mathbb{Q}).$$

$\underline{l = 17:}$ The modular curve $X_0(17)$ has genus 1, and $X_0(17)(\mathbb{Q})$ has 2 noncuspidal rational points corresponding to the j-invariants $j_1 = -17^2 \cdot 101^3/2$ and $j_2 = -17 \cdot 373^3/2^{17}$. Both curves (which are isogenous to each other by the rational 17-isogeny) have a model with conductor $N = 2 \cdot 5^2 \cdot 17^2 = 14450$, namely

$$\begin{aligned} E_1 &: y^2 + xy + y = x^3 - 3041x + 64278 \\ E_2 &: y^2 + xy + y = x^3 - 190891x - 36002922 \end{aligned}$$

(see [1, p. 80]).

One checks that the traces $a_p(E_1)$ are surjective modulo 17 (and then also for the isogenous curve E_2). This is also true for the twists by -1, ± 2, ± 5, ± 10, ± 17, ± 34, ± 85 and ± 170. This is then true for all other twists by Lemma 2.4.

$\underline{l = 37:}$ The modular curve $X_0(37)$ has genus 2, and $X_0(37)(\mathbb{Q})$ has 2 noncuspidal rational points corresponding to the j-invariants $j_1 = -7 \cdot 11^3$ and $j_2 = -7 \cdot 137^3 \cdot 2083^3$. The 2 j-invariants have a model with conductor $N = 1225 = 5^2 \cdot 7^2$, namely

$$\begin{aligned} E_1 &: y^2 + xy + y = x^3 + x^2 - 8x + 6 \\ E_2 &: y^2 + xy + y = x^3 + x^2 - 208083x - 36621194 \end{aligned}$$

(see [12, p. 30]). Then, $j(E_i) = j_i$ for $i = 1, 2$ and $E_2 = E_1/\phi$ where ϕ is the rational 37-isogeny. In the notation of Cremona's tables [4], $E_1 = E1225H1$ and $E_2 = E1225H2$.

We check that the traces $a_p(E_1)$ are surjective modulo 37 (and then the traces $a_p(E_2)$ as the curves are isogenous). We then check surjectivity of the traces modulo 37 for all twists E_D of E_1 with $D = -1, \pm 5, \pm 7, \pm 35$. Together with E_1 and E_2, those twists are all curves of conductor 1225 and j-invariants j_1 and j_2: there exists 8 such curves, in 4 isogeny classes. Finally, one checks surjectivity for the twists by $\pm 37, \pm 185, \pm 259, \pm 1295$; they are curves of conductor $5^2 \cdot 7^2 \cdot 37^2$.

Acknowledgments: The authors would like to thank I. Chen, H. Darmon and A. Schweizer for helpful discussions, and D. Grant for pointing out the paper of Stark. We specially thank J. Fearnley who computed the analytic rank of $J_1(13)$ as described in Proposition 6.1.

References

[1] *Modular functions of one variable.* VI. Proceedings of the Second International Conference, held at the University of Bonn, Bonn, July 2–14, 1976. Edited by J.-P. Serre and D. B. Zagier. Lecture Notes in Mathematics, Vol. 627. Springer-Verlag, Berlin-New York, 1977. ii+339 pp.

[2] C. Batut, K. Belabas, D. Bernardi, H. Cohen and M. Olivier, PARI-GP.

[3] R. Coleman, Effective Chabauty, *Duke Mathematical Journal* **52** (1985), 765-770.

[4] J. E. Cremona, *Algorithms for modular elliptic curves*, Cambridge University Press, 1992.

[5] C. David and F. Pappalardi, Average Frobenius distributions of elliptic curves, *Internat. Math. Res. Notices* 1999, **no. 4**, 165–183.

[6] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, *Abh. Math. Sem. Hansischen Univ.* **14** (1941), 197-272.

[7] W. Duke, Rational elliptic curves with no exceptional primes, *C.R. Acad. Sci. Paris* **325** (1997), 813–818.

[8] D. Grant, A formula for the number of elliptic curves with exceptional primes, *Compositio Math.*, to appear.

[9] S. Lang and H. Trotter, *Frobenius distributions in GL_2-extensions*, Springer-Verlag Lecture Notes in Mathematics **504**, 1976.

[10] B. Mazur, Modular curves and the Eiseinstein ideal, *Publ. Math. I.H.E.S.* **47** (1977), 33-186.

[11] B. Mazur, Rational isogenies of prime degree, *Inventiones Math.* **44** (1978), 129-162.

[12] B. Mazur and P. Swinnerton-Dyer, Arithmetic of Weil curves, *Inventiones Math.* **25** (1974), 1-61.

[13] F. Momose, p-torsion points on elliptic curves defined over quadratic fields, *Nagoya Math. J.* **96** (1984), 115-137.

[14] A. P. Ogg, Rational points on certain elliptic modular curves, *Proc. Symp. Pure Math.*, **24** (1973), 221-231, A.M.S., Providence.

[15] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Inventiones Math.* **15** (1972, 259-331.

[16] J. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, 1986.

[17] H. Stark, Counting points on CM elliptic curves, *Rocky Mountain J. Math.* **26** (1996), 1115-1138.

Concordia University, Department of Mathematics, 1455 de Maisonneuve Blvd. West, Montréal, Quebec H3G 1M8, CANADA
E–mail: chantal@cicma.concordia.ca

Concordia University, Department of Mathematics, 1455 de Maisonneuve Blvd. West, Montréal, Quebec H3G 1M8, CANADA
E–mail: kisilev@cicma.concordia.ca

Università degli Studi di Roma Tre, Dipartimento di Matematica, Via Corrado Segre, 4, 00146, Roma, ITALIA
E–mail: pappa@mat.uniroma3.it