ELLIPTIC CURVES WITH 2-TORSION CONTAINED IN THE 3-TORSION FIELD

J. BRAU AND N. JONES

Abstract. There is a modular curve $X'(6)$ of level 6 defined over $\mathbb{Q}$ whose $\mathbb{Q}$-rational points correspond to j-invariants of elliptic curves E over $\mathbb{Q}$ that satisfy $\mathbb{Q}(E[2]) \subseteq \mathbb{Q}(E[3])$. In this note we characterize the j-invariants of elliptic curves with this property by exhibiting an explicit model of $X'(6)$. Our motivation is two-fold: on the one hand, $X'(6)$ belongs to the list of modular curves which parametrize non-Serre curves (and is not well-known), and on the other hand, $X'(6)(\mathbb{Q})$ gives an infinite family of examples of elliptic curves with non-abelian "entanglement fields," which is relevant to the systematic study of correction factors of various conjectural constants for elliptic curves over $\mathbb{Q}$.

1. Introduction

Let K be a number field, let E be an elliptic curve over K, and for any positive integer n, let $E[n]$ denote the n-torsion of E. For a prime ℓ, let $E[\ell^\infty] := \bigcup_{m \geq 1} E[\ell^m]$, and furthermore put $E_{\text{tors}} := \bigcup_{n \geq 1} E[n]$. Fixing a $\hat{\mathbb{Z}}$-basis of E_{tors}, for any prime ℓ there is an induced $\mathbb{Z}_\ell$-basis of $E[\ell^\infty]$ and for any $n \geq 1$ there is an induced $\mathbb{Z}/n\mathbb{Z}$-basis of $E[n]$. Consider the Galois representations

$$\begin{aligned}
\rho_{E,n} &: \operatorname{Gal}(\overline{K}/K) \longrightarrow \operatorname{Aut}(E[n]) \simeq \operatorname{GL}_2(\mathbb{Z}/n\mathbb{Z}) \\
\rho_{E,\ell^\infty} &: \operatorname{Gal}(\overline{K}/K) \longrightarrow \operatorname{Aut}(E[\ell^\infty]) \simeq \operatorname{GL}_2(\mathbb{Z}_\ell) \\
\rho_{E} &: \operatorname{Gal}(\overline{K}/K) \longrightarrow \operatorname{Aut}(E_{\text{tors}}) \simeq \operatorname{GL}_2(\hat{\mathbb{Z}}),
\end{aligned}$$

each defined by letting $\operatorname{Gal}(\overline{K}/K)$ act on the appropriate set of torsion points, viewed relative to the appropriate basis.

A celebrated theorem of Serre [11] states that, if E is an elliptic curve over a number field K without complex multiplication ("non-CM"), then the Galois representation ρ_E has an open image with respect to the profinite topology on $\operatorname{GL}_2(\hat{\mathbb{Z}})$, which is to say that $[\operatorname{GL}_2(\hat{\mathbb{Z}}) : \rho_E(\operatorname{Gal}(\overline{K}/K))] < \infty$. It is of interest to understand the image of ρ_E. To determine $\rho_E(\operatorname{Gal}(\overline{K}/K))$ in practice, one begins by computing the ℓ-adic image $\rho_{E,\ell^\infty}(\operatorname{Gal}(\overline{K}/K))$ for each prime ℓ. One then has that

$$\rho_E(\operatorname{Gal}(\overline{K}/K)) \hookrightarrow \prod_\ell \rho_{E,\ell^\infty}(\operatorname{Gal}(\overline{K}/K)) \subseteq \prod_\ell \operatorname{GL}_2(\mathbb{Z}_\ell) \simeq \operatorname{GL}_2(\hat{\mathbb{Z}}),$$

and although the image of $\rho_E(\operatorname{Gal}(\overline{K}/K))$ in $\prod_\ell \rho_{E,\ell^\infty}(\operatorname{Gal}(\overline{K}/K))$ projects onto each ℓ-adic factor, the inclusion may nevertheless be onto a proper subgroup. Understanding the image of $\rho_E(\operatorname{Gal}(\overline{K}/K)) \hookrightarrow \prod_\ell \rho_{E,\ell^\infty}(\operatorname{Gal}(\overline{K}/K))$ now amounts to understanding the *entanglement fields*

$$K(E[m_1]) \cap K(E[m_2]),$$

for each pair $m_1, m_2 \in \mathbb{N}$ which are relatively prime[1]. Note that any such intersection is necessarily Galois over K. One of the questions which motivates this note is the following.

Question 1.1. Given a number field K, can one classify the triples (E, m_1, m_2) with E an elliptic curve over K and m_1, m_2 a pair of co-prime integers for which the entanglement field $K(E[m_1]) \cap K(E[m_2])$ is non-abelian over K?

[1]Here and throughout the paper, $K(E[n]) := \overline{K}^{\ker \rho_{E,n}}$ denotes the *n-th division field* of E.

This question is closely related to the study of correction factors of various conjectural constants for elliptic curves over $\mathbb{Q}$. In order to illustrate this point, consider the following elliptic curve analogue Artin's conjecture on primitive roots. For an elliptic curve E over $\mathbb{Q}$, determine the density of primes p such that E has good reduction at p and $\tilde{E}(\mathbb{F}_p)$ is a cyclic group, where $\tilde{E}$ denotes the mod p reduction of E. Note that the condition of $\tilde{E}(\mathbb{F}_p)$ being cyclic is completely determined by $\rho_E(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$. Indeed, $\tilde{E}(\mathbb{F}_p)$ is a cyclic group if and only if p does not split completely in the field extension $\mathbb{Q}(E[\ell])$ for any $\ell \neq p$.

By the Chebotarev density theorem, the set of primes p that do not split completely in $\mathbb{Q}(E[\ell])$ has density equal to

$$\delta_\ell = 1 - \frac{1}{[\mathbb{Q}(E[\ell]) : \mathbb{Q}]}.$$

If we assume that the various splitting conditions at each prime ℓ are independent, then it is reasonable to conjecture that the density of primes p for which $\tilde{E}(\mathbb{F}_p)$ is cyclic is equal to $\prod_\ell \delta_\ell$. However, this assumption of independence is not correct, and this lack of independence is explained by the entanglement fields.

Serre showed in [12] that Hooley's method of proving Artin's conjecture on primitive roots can be adapted to prove that the density of primes p for which $\tilde{E}(\mathbb{F}_p)$ is cyclic is given under GRH by the inclusion-exclusion sum

$$\delta(E) = \sum_{n=1}^{\infty} \frac{\mu(n)}{[\mathbb{Q}(E[n]) : \mathbb{Q}]} \tag{1}$$

where μ denotes the Möbius function. Taking into account entanglements between the various torsion fields implies that

$$\delta(E) = C_E \prod_\ell \delta_\ell$$

where C_E is an *entanglement correction factor*, and explicitely evaluating such densities amounts to computing the correction factors C_E. In [1] it is shown that when all the entanglements fields of an elliptic curve over $\mathbb{Q}$ are abelian, then the image of $\rho_E(\mathrm{Gal}(\overline{K}/K)) \hookrightarrow \prod_\ell \rho_{E,\ell^\infty}(\mathrm{Gal}(\overline{K}/K))$ is normal with abelian quotient, hence is cut out by characters, and the correction factor can be given as a character sum. The structure of $\delta(E)$ as an Euler product and the description of C_E as a character sum allow one to easily determine non-vanishing criteria for the density we are interested in. This method also has the advantage that it is well-suited to deal with many other problems of this nature where the explicit evaluation of (1) becomes problematic. Understanding which non-abelian entanglements can occur is therefore important for the systematic study of such constants.

With respect to entanglement fields, the case $K = \mathbb{Q}$, although it is usually the first case considered, has a complication which doesn't arise over any other number field. Indeed, when the base field is $\mathbb{Q}$, the Kronecker-Weber theorem, together with the containment $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(E[n])$, *forces* the occurrence of non-trivial entanglement fields[2]. It was observed by Serre [11, Proposition 22] that for any elliptic curve E over $\mathbb{Q}$ one has

$$\mathbb{Q}(\sqrt{\Delta_E}) \subseteq \mathbb{Q}(E[2]) \cap \mathbb{Q}(\zeta_n), \tag{2}$$

where $n = 4|\Delta_E|$. This containment forces $\rho_E(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ to lie in an appropriate index two subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$, so that one must have

$$[\mathrm{GL}_2(\hat{\mathbb{Z}}) : \rho_E(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))] \geq 2. \tag{3}$$

Several examples are known of elliptic curves E over $\mathbb{Q}$ for which the entanglement (2) is the only obstruction to surjectivity of ρ_E, i.e. for which equality holds in (3).

Definition 1.2. We call an elliptic curve E defined over $\mathbb{Q}$ a **Serre curve** if $[\mathrm{GL}_2(\hat{\mathbb{Z}}) : \rho_E(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))] = 2$.

In [6] it is shown using sieve methods that, when taken by height, almost all elliptic curves E over $\mathbb{Q}$ are Serre curves (see also [13], which generalizes this to the case $K \neq \mathbb{Q}$, and [9], which sharpens the upper bound to an asymptotic formula). In [2], different ideas are used to deduce stronger upper bounds for the number of elliptic curves in *one-parameter* families which are not Serre curves. These results are obtained

[2]Here and throughout the paper, ζ_n denotes a primitive n-th root of unity.

by viewing non-Serre curves as coming from rational points on modular curves. More precisely, there is a family $\mathcal{X} = \{X_1, X_2, \dots\}$ of modular curves with the property that, for each elliptic curve E, one has

$$E \text{ is not a Serre curve } \iff j(E) \in \bigcup_{X \in \mathcal{X}} j(X(\mathbb{Q})), \tag{4}$$

where j denotes the natural projection followed by the usual j-map:

$$j : X \longrightarrow X(1) \longrightarrow \mathbb{P}^1.$$

In [2], the authors use (4) together with geometric methods to bound the number of non-Serre curves in a given one-parameter family. This brings us to the following question, which serves as additional motivation for the present note.

Question 1.3. Consider the family $\mathcal{X}$ occurring in (4). What is an explicit list of the modular curves in $\mathcal{X}$?

The modular curves in $\mathcal{X}$ of prime level ℓ correspond to maximal proper subgroups of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ and have been studied extensively. Let

$$\mathcal{E}_\ell \subseteq \left\{ X_0(\ell), X^+_{\text{split}}(\ell), X^+_{\text{non-split}}(\ell), X_{A_4}(\ell), X_{S_4}(\ell), X_{A_5}(\ell) \right\} \tag{5}$$

be the set of modular curves whose rational points correspond to j-invariants of elliptic curves E for which $\rho_{E,\ell}$ is not surjective (each of the modular curves $X_{A_4}(\ell)$, $X_{S_4}(\ell)$, and $X_{A_5}(\ell)$ corresponding to the exceptional groups A_4, S_4 and A_5 only occurs for certain primes ℓ). One has

$$\bigcup_{\ell \text{ prime}} \mathcal{E}_\ell \subseteq \mathcal{X}.$$

The family $\mathcal{X}$ must also contain two other modular curves $X'(4)$ and $X''(4)$ of level 4, and another $X'(9)$ of level 9, which have been considered in [4] and [5], respectively.

In this note, we consider a modular curve $X'(6)$ of level 6 which, taken together with those listed above, completes the set $\mathcal{X}$ of modular curves occurring in (4), answering Question 1.3. First, we recall the general construction of modular curves associated to subgroups $H \subseteq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ (for more details, see [3]). Let $X(n)$ denote the complete modular curve of level n, which parametrizes elliptic curves together with chosen $\mathbb{Z}/n\mathbb{Z}$-bases of $E[n]$. Let $H \subseteq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ be a subgroup containing $-I$ for which the determinant map

$$\det\colon H \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$$

is surjective, and consider the quotient curve $X_H := X(n)/H$ together with the j-invariant

$$j\colon X_H \longrightarrow \mathbb{P}^1.$$

For any $x \in \mathbb{P}^1(\mathbb{Q})$, we have that

$$x \in j(X_H(\mathbb{Q})) \iff \begin{array}{c} \exists \text{ an elliptic curve } E \text{ over } \mathbb{Q} \text{ and } \exists g \in \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \\ \text{with } j(E) = x \text{ and } \rho_{E,n}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) \subseteq g^{-1}Hg. \end{array} \tag{6}$$

Thus, to describe $X'(6)$, it suffices to describe the corresponding subgroup $H \subseteq \mathrm{GL}_2(\mathbb{Z}/6\mathbb{Z})$.

There is exactly one index 6 normal subgroup $\mathcal{N} \subseteq \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$, defined by

$$\mathcal{N} := \left\{ \begin{pmatrix} x & -y \\ y & x \end{pmatrix} : \ x^2 + y^2 \equiv 1 \mod 3 \right\} \sqcup \left\{ \begin{pmatrix} x & y \\ y & -x \end{pmatrix} : \ x^2 + y^2 \equiv -1 \mod 3 \right\}. \tag{7}$$

This subgroup fits into an exact sequence

$$1 \longrightarrow \mathcal{N} \longrightarrow \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \longrightarrow 1, \tag{8}$$

and we denote by

$$\theta\colon \ \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \tag{9}$$

the (non-canonical) surjective map in the above sequence. We take $H \subseteq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ to be the graph of θ, viewed as a subgroup of $\mathrm{GL}_2(\mathbb{Z}/6\mathbb{Z})$ via the Chinese Remainder Theorem. The modular curve $X'(6)$ is then defined by

$$X'(6) := X_{H'_6}, \ \text{ where } \ H'_6 := \{(g_2, g_3) \in \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) : \ g_2 = \theta(g_3)\} \subseteq \mathrm{GL}_2(\mathbb{Z}/6\mathbb{Z}). \tag{10}$$

Unravelling (6) in this case, we find that, for every elliptic curve E over $\mathbb{Q}$,

$$j(E) \in j(X'(6)(\mathbb{Q})) \iff E \simeq_{\overline{\mathbb{Q}}} E' \text{ for some } E' \text{ over } \mathbb{Q} \text{ for which } \mathbb{Q}(E'[2]) \subseteq \mathbb{Q}(E'[3]). \tag{11}$$

By considering the geometry of the natural map $X'(6) \longrightarrow X(1)$, the curve $X'(6)$ is seen to have genus zero and one cusp. Since $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the cusps, the single cusp must be defined over $\mathbb{Q}$, thus endowing $X'(6)$ with a rational point. Therefore $X'(6) \simeq_{\mathbb{Q}} \mathbb{P}^1$. We prove the following theorem, which gives an explicit model of $X'(6)$.

Theorem 1.4. *There exists a parameter $t\colon X'(6) \longrightarrow \mathbb{P}^1$, which is a uniformizer at the cusp, and which has the property that*

$$j = 2^{10}3^3t^3(1-4t^3),$$

where $j\colon X'(6) \longrightarrow X(1) \simeq \mathbb{P}^1$ is the usual j-map.

Remark 1.5. By (11), Theorem 1.4 is equivalent to the following statement: for any elliptic curve E over $\mathbb{Q}$, E is isomorphic over $\overline{\mathbb{Q}}$ to an elliptic curve E' satisfying

$$\mathbb{Q}(E'[2]) \subseteq \mathbb{Q}(E'[3])$$

if and only if $j(E) = 2^{10}3^3t^3(1-4t^3)$ for some $t \in \mathbb{Q}$.

Furthermore, we prove the following theorem, which answers Question 1.3. For each prime ℓ, consider the set $\mathcal{G}_{\ell,\max}$ of maximal proper subgroups of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, which surject via determinant onto $(\mathbb{Z}/\ell\mathbb{Z})^\times$:

$$\mathcal{G}_{\ell,\max} := \{H \subsetneq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) :\ \det(H) = (\mathbb{Z}/\ell\mathbb{Z})^\times \text{ and } \nexists H_1 \text{ with } H \subsetneq H_1 \subsetneq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})\}.$$

The group $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ acts on $\mathcal{G}_{\ell,\max}$ by conjugation, and let $\mathcal{R}_\ell$ be a set of representatives of $\mathcal{G}_{\ell,\max}$ modulo this action. By (6), the collection $\mathcal{X}$ occurring in (4) must contain as a subset

$$\mathcal{E}_\ell := \{X_H :\ H \in \mathcal{R}_\ell\}, \tag{12}$$

the set of modular curves attached to subgroups $H \in \mathcal{R}_\ell$ (this gives a more precise description of the set $\mathcal{E}_\ell$ in (5)). Furthermore, the previously mentioned modular curves $X'(4)$, $X''(4)$, and $X'(9)$ correspond to the following subgroups. Let $\varepsilon : \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \longrightarrow \{\pm 1\}$ denote the unique non-trivial character, and we will view $\det\colon \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \longrightarrow (\mathbb{Z}/4\mathbb{Z})^\times \simeq \{\pm1\}$ as taking the values ±1.

$$\begin{aligned} X'(4) &= X_{H_4'}, \text{ where } H_4' := \{g \in \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) :\ \det g = \varepsilon(g \mod 2)\} \subseteq \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}), \\ X''(4) &= X_{H_4''} \text{ where } H_4'' := \left\langle \begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\rangle \subseteq \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \\ X'(9) &= X_{H_9'} \text{ where } H_9' := \left\langle \begin{pmatrix} 0 & 2 \\ 4 & 0 \end{pmatrix}, \begin{pmatrix} 4 & 1 \\ -3 & 4 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle \subseteq \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z}). \end{aligned} \tag{13}$$

For more details on these modular curves, see [4] and [5].

Theorem 1.6. *Let $\mathcal{X}$ be defined by*

$$\mathcal{X} = \{X'(4), X''(4), X'(9), X'(6)\} \cup \bigcup_{\ell \text{ prime}} \mathcal{E}_\ell,$$

where $X'(4)$, $X''(4)$ and $X'(9)$ are defined by (13), $X'(6)$ is defined by (10), and $\mathcal{E}_\ell$ is as in (12). Then, for any elliptic curve E over $\mathbb{Q}$,

$$E \text{ is not a Serre curve} \iff j(E) \in \bigcup_{X \in \mathcal{X}} j(X(\mathbb{Q})).$$

2. Proofs

We now prove Theorems 1.4 and 1.6.

Proof of Theorem 1.4. Consider the elliptic curve $\mathbb{E}$ over $\mathbb{Q}(t)$ given by

$$\mathbb{E}: \ y^2 = x^3 + 3t\left(1-4t^3\right)x + \left(1-4t^3\right)\left(\frac{1}{2} - 4t^3\right),$$

with discriminant and j-invariant $\Delta_{\mathbb{E}}, j(\mathbb{E}) \in \mathbb{Q}(t)$ given, respectively, by

$$\Delta_{\mathbb{E}} = -2^6 3^3 (1-4t^3)^2 \quad \text{and} \quad j(\mathbb{E}) = 2^{10} 3^3 t^3 (1-4t^3). \tag{14}$$

For every $t \in \mathbb{Q}$, the specialization $\mathbb{E}_t$ is an elliptic curve over $\mathbb{Q}$ whose discriminant $\Delta_{\mathbb{E}_t} \in \mathbb{Q}$ and j-invariant $j(\mathbb{E}_t) \in \mathbb{Q}$ are given by evaluating (14) at t. We will show that, for any $t \in \mathbb{Q}$, one has

$$\mathbb{Q}(\mathbb{E}_t[2]) \subseteq \mathbb{Q}(\mathbb{E}_t[3]). \tag{15}$$

By (11) and (14), it then follows that

$$\forall t \in \mathbb{Q}, \quad 2^{10} 3^3 t^3 (1-4t^3) \in j(X'(6)(\mathbb{Q})).$$

Since the natural j-map $j \colon X'(6) \longrightarrow \mathbb{P}^1$ and the map $t \mapsto 2^{10}3^3t^3(1-4t^3)$ both have degree 6, Theorem 1.4 will then follow. To verify (15), we will show that, for every $t \in \mathbb{Q}$, one has

$$\mathbb{Q}(\mathbb{E}_t[2]) \subseteq \mathbb{Q}(\zeta_3, \Delta_{\mathbb{E}_t}^{1/3}). \tag{16}$$

It is a classical fact that, for any elliptic curve E over $\mathbb{Q}$, one has $\mathbb{Q}(\zeta_3, \Delta_E^{1/3}) \subseteq \mathbb{Q}(E[3])$ (for details, see for instance [8, p. 181] and the references given there). Thus, the containment (15) follows from (16). Finally, (16) follows immediately from the factorization

$$(x - e_1(t))\,(x - e_2(t))\,(x - e_3(t)) = x^3 + 3t\left(1-4t^3\right)x + \left(1-4t^3\right)\left(\frac{1}{2} - 4t^3\right)$$

of the 2-division polynomial $x^3 + 3t\left(1-4t^3\right)x + \left(1-4t^3\right)\left(\frac{1}{2} - 4t^3\right)$, where

$$\begin{aligned}
e_1(t) &:= \frac{1}{6}\Delta_{\mathbb{E}_t}^{1/3} + \frac{t}{18(1-4t^3)}\Delta_{\mathbb{E}_t}^{2/3}, \\
e_2(t) &:= \frac{\zeta_3}{6}\Delta_{\mathbb{E}_t}^{1/3} + \frac{\zeta_3^2 t}{18(1-4t^3)}\Delta_{\mathbb{E}_t}^{2/3}, \quad \text{and} \\
e_3(t) &:= \frac{\zeta_3^2}{6}\Delta_{\mathbb{E}_t}^{1/3} + \frac{\zeta_3 t}{18(1-4t^3)}\Delta_{\mathbb{E}_t}^{2/3}.
\end{aligned}$$

This finishes the proof of Theorem 1.4. □

Remark 2.1. Our proof shows that, viewing $\mathbb{E}_t$ as an elliptic curve over $\mathbb{Q}(t)$, we have a containment of function fields

$$\mathbb{Q}(t)(\mathbb{E}_t[2]) \subseteq \mathbb{Q}(t)(\mathbb{E}_t[3]).$$

We will now turn to Theorem 1.6, whose proof employs the following two group-theoretic lemmas.

Lemma 2.2. *(Goursat's Lemma) Let G_0 and G_1 be groups and $G \subseteq G_0 \times G_1$ a subgroup satisfying*

$$\pi_i(G) = G_i \qquad (i \in \{0,1\}),$$

where π_i denotes the canonical projection onto the i-th factor. Then there exists a group Q and surjective homomorphisms $\psi_0 \colon G_0 \to Q$, $\psi_1 \colon G_1 \to Q$ for which

$$G = \{(g_0, g_1) \in G_0 \times G_1 : \psi_0(g_0) = \psi_1(g_1)\}. \tag{17}$$

Proof. See [10, Lemma (5.2.1)]. □

Letting ψ be an abbreviation for the ordered pair (ψ_0, ψ_1), the group G given by (17) is called the *fibered product of G_0 and G_1 over ψ*, and is commonly denoted by $G_0 \times_\psi G_1$. Notice that, for a surjective group homomorphism $f\colon Q \to Q_1$, if $f \circ \psi$ denotes the ordered pair $(f \circ \psi_0, f \circ \psi_1)$ and $G_0 \times_{f\circ\psi} G_1$ denotes the corresponding fibered product, then one has

$$G_0 \times_\psi G_1 \subseteq G_0 \times_{f\circ\psi} G_1. \tag{18}$$

Lemma 2.3. *Let G_0 and G_1 be groups, let $\psi_0\colon G_0 \to Q$ and $\psi_1\colon G_1 \to Q$ be a pair of surjective homomorphisms onto a common quotient group Q, and let $H = G_0 \times_\psi G_1$ be the associated fibered product. If Q is cyclic, then one has the following equality of commutator subgroups:*

$$[H, H] = [G_0, G_0] \times [G_1, G_1].$$

Proof. See [8, Lemma 1, p. 174] (the hypothesis of this lemma is readily verified when Q is cyclic). □

Proof of Theorem 1.6. As shown in [7], one has

$$E \text{ is not a Serre curve} \iff \begin{array}{c} \exists \text{ a prime } \ell \geq 5 \text{ with } \rho_{E,\ell}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) \subsetneq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}), \text{ or} \\ [\rho_{E,36}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})), \rho_{E,36}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))] \subsetneq [\mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z}), \mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z})]. \end{array}$$

For each divisor d of 36, let

$$\pi_{36,d}\colon \mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/d\mathbb{Z}) \tag{19}$$

denote the canonical projection. One checks that, for $\ell \in \{2, 3\}$, any proper subgroup $H \subsetneq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for which $\det(H) = (\mathbb{Z}/\ell\mathbb{Z})^\times$ must satisfy $[H, H] \subsetneq [\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}), \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})]$. We then define

$$\mathcal{G}_{36} := \left\{ H \subseteq \mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z}) : \begin{array}{c} \forall d \in \{2,3\},\ \pi_{36,d}(H) = \mathrm{GL}_2(\mathbb{Z}/d\mathbb{Z}),\ \det(H) = (\mathbb{Z}/36\mathbb{Z})^\times, \\ \text{and } [H, H] \subsetneq [\mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z}), \mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z})] \end{array} \right\}, \tag{20}$$

and note that

$$E \text{ is not a Serre curve} \iff \begin{array}{c} \exists \text{ a prime } \ell \text{ and } H \in \mathcal{G}_{\ell,\max} \text{ for which } \rho_{E,\ell}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) \subseteq H, \\ \text{or } \exists H \in \mathcal{G}_{36} \text{ for which } \rho_{E,36}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) \subseteq H. \end{array} \tag{21}$$

As in the prime level case, we need only consider *maximal* subgroups $H \in \mathcal{G}_{36}$, and because of (6), only up to conjugation by $\mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z})$. Thus, we put

$$\mathcal{G}_{36,\max} := \{H \in \mathcal{G}_{36} :\ \nexists H_1 \in \mathcal{G}_{36} \text{ with } H \subsetneq H_1 \subsetneq \mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z})\},$$

we let $\mathcal{R}_{36} \subseteq \mathcal{G}_{36,\max}$ be a set of representatives of $\mathcal{G}_{36,\max}$ modulo $\mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z})$-conjugation, and we set

$$\mathcal{E}_{36} := \{X_H :\ H \in \mathcal{R}_{36}\}.$$

The equivalence (21) now becomes (see (12))

$$E \text{ is not a Serre curve} \iff \begin{array}{c} \exists \text{ a prime } \ell \text{ and } X_H \in \mathcal{E}_\ell \text{ for which } j(E) \in j(X_H(\mathbb{Q})), \\ \text{or } \exists X_H \in \mathcal{E}_{36} \text{ for which } j(E) \in j(X_H(\mathbb{Q})). \end{array}$$

Thus, Theorem 1.6 will follow from the next proposition.

Proposition 2.4. *With the above notation, one may take*

$$\mathcal{R}_{36} = \{\pi_{36,4}^{-1}(H_4'), \pi_{36,4}^{-1}(H_4''), \pi_{36,9}^{-1}(H_9'), \pi_{36,6}^{-1}(H_6')\},$$

where $\pi_{36,d}$ is as in (19) *and the groups H_4', H_4'', H_9' and H_6' are given by* (13) *and* (10).

Proof. Let $H \in \mathcal{G}_{36,\max}$. If $\pi_{36,4}(H) \neq \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$, then [4] shows that $\pi_{36,4}(H) \subseteq H_4'$ or $\pi_{36,4}(H) \subseteq H_4''$, up to conjugation in $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$. If $\pi_{36,9}(H) \neq \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$, then [5] shows that, up to $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$-conjugation, one has $\pi_{36,9}(H) \subseteq H_9'$. Thus, we may now assume that $\pi_{36,4}(H) = \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ and $\pi_{36,9}(H) = \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$. By Lemma 2.2, this implies that there exists a group Q and a pair of surjective homomorphisms

$$\psi_4\colon \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \longrightarrow Q$$
$$\psi_9\colon \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z}) \longrightarrow Q$$

for which $H = \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \times_\psi \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$. We will now show that in this case, up to $\mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z})$-conjugation, we have

$$H \subseteq \{(g_4, g_9) \in \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z}) :\ \theta(g_9 \pmod 3) = g_4 \pmod 2\}, \tag{22}$$

where $\theta\colon \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ is the map given in (9), whose graph determines the level 6 structure defining the modular curve $X'(6)$. This will finish the proof of Proposition 2.4.

Let us make the following definitions:

$$\begin{aligned} N_4 &:= \ker\psi_4 \subseteq \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}), & N_9 &:= \ker\psi_9 \subseteq \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z}) \\ N_2 &:= \pi_{4,2}(N_4) \subseteq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}), & N_3 &:= \pi_{9,3}(N_9) \subseteq \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) \\ Q_2 &:= \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})/N_2, & Q_3 &:= \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})/N_3, \end{aligned}$$

where $\pi_{4,2}\colon \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ and $\pi_{9,3}\colon \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ denote the canonical projections. We then have the following exact sequences:

$$\begin{aligned} &1 \longrightarrow N_9 \longrightarrow \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z}) \longrightarrow Q \longrightarrow 1 \\ &1 \longrightarrow N_4 \longrightarrow \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \longrightarrow Q \longrightarrow 1 \\ &1 \longrightarrow N_3 \longrightarrow \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) \longrightarrow Q_3 \longrightarrow 1 \\ &1 \longrightarrow N_2 \longrightarrow \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \longrightarrow Q_2 \longrightarrow 1, \end{aligned} \tag{23}$$

as well as

$$\begin{aligned} &1 \longrightarrow K_2 \longrightarrow Q \longrightarrow Q_2 \longrightarrow 1 \\ &1 \longrightarrow K_3 \longrightarrow Q \longrightarrow Q_3 \longrightarrow 1, \end{aligned} \tag{24}$$

where for each $\ell \in \{2,3\}$, the kernel $K_\ell \simeq \dfrac{\ker\pi_{\ell^2,\ell}}{N_{\ell^2} \cap \ker\pi_{\ell^2,\ell}} \subseteq \dfrac{\mathrm{GL}_2(\mathbb{Z}/\ell^2\mathbb{Z})}{N_{\ell^2}} \simeq Q$ is evidently abelian (since $\ker\pi_{\ell^2,\ell}$ is), and has order dividing $\ell^4 = |\ker\pi_{\ell^2,\ell}|$. We will proceed to prove that

$$Q_2 \simeq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \quad \text{and} \quad Q_3 \simeq Q, \tag{25}$$

which is equivalent to

$$N_4 \subseteq \ker\pi_{4,2} \quad \text{and} \quad \ker\pi_{9,3} \subseteq N_9.$$

Writing $\tilde{\psi}_4\colon \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \to Q \to Q_2 \simeq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ and $\tilde{\psi}_9\colon \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z}) \to Q \to Q_2 \simeq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$, we then see by (18) that

$$H = \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \times_\psi \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z}) \subseteq \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \times_{\tilde{\psi}} \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z}).$$

Furthermore, it follows from $Q \simeq Q_3$ that $\tilde{\psi}_9$ factors through the projection $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$. This, together with the uniqueness of $\mathcal{N}$ in (8) and the fact that every automorphism of $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ is inner, implies that (22) holds, up to $\mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z})$-conjugation. Thus, the proof of Proposition 2.4 is reduced to showing that (25) holds.

We will first show that $Q_2 \simeq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$. Suppose on the contrary that $Q_2 \subsetneq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$. Looking at the first exact sequence in (24), we see that Q must then be a 2-group, and since the K_3 has order a power of 3 (possibly 1), we see that $Q \simeq Q_3$, and the third exact sequence in (23) becomes

$$1 \longrightarrow N_3 \longrightarrow \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) \longrightarrow Q \longrightarrow 1.$$

The kernel N_3 must contain an element σ of order 3, and by considering $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$-conjugates of σ, we find that $|N_3| \geq 8$. Since 3 also divides $|N_3|$, we see that $|N_3| \geq 12$, and so Q must be abelian, having order at most 4. Furthermore, since $[\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}), \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})] = \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$, we find that Q has order at most 2, and thus is cyclic. Applying Lemma 2.3, we find that $[H,H] = [\mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z}), \mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z})]$, contradicting (20). Thus, we must have that $Q_2 \simeq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$.

We will now show that $Q_3 \simeq Q$. To do this, we will first take a more detailed look at the structure of the group $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$. Note the embedding of groups $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \hookrightarrow \mathrm{GL}_2(\mathbb{Z})$ given by

$$\begin{aligned} &\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \mapsto \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \\ &\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}. \end{aligned}$$

This embedding, followed by reduction modulo 4, splits the exact sequence

$$1 \to \ker\pi_{4,2} \to \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \to 1.$$

Also note the isomorphism $(\ker \pi_{4,2}, \cdot) \to (M_{2\times 2}(\mathbb{Z}/2\mathbb{Z}), +)$ given by $I + 2A \mapsto A \pmod 2$. These two observations realize $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ as a semi-direct product

$$\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \simeq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \ltimes M_{2\times 2}(\mathbb{Z}/2\mathbb{Z}), \tag{26}$$

where the right-hand factor is an additive group and the action of $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ on $M_{2\times 2}(\mathbb{Z}/2\mathbb{Z})$ is by conjugation. Since $Q_2 \simeq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$, we see that, under (26), one has

$$N_4 \subseteq M_{2\times 2}(\mathbb{Z}/2\mathbb{Z}),$$

and since it is a normal subgroup of $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$, we see that N_4 must be a $\mathbb{Z}/2\mathbb{Z}$-subspace which is invariant under $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$-conjugation. This implies that one of the 5 cases in the following table must hold.

N_4	Q
$M_{2\times 2}(\mathbb{Z}/2\mathbb{Z})$	$\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$
$\{A \in M_{2\times 2}(\mathbb{Z}/2\mathbb{Z}) :\ \mathrm{tr}\, A = 0\}$	$\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \times \{\pm 1\}$
$\left\{\begin{pmatrix}0&0\\0&0\end{pmatrix}, \begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\1&0\end{pmatrix}, \begin{pmatrix}0&1\\1&1\end{pmatrix}\right\}$	$\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \ltimes (\mathbb{Z}/2\mathbb{Z})^2$
$\left\{\begin{pmatrix}0&0\\0&0\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}, \begin{pmatrix}1&0\\1&1\end{pmatrix}, \begin{pmatrix}0&1\\1&0\end{pmatrix}\right\}$	$\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \ltimes (\mathbb{Z}/2\mathbb{Z})^2$
$\left\{\begin{pmatrix}0&0\\0&0\end{pmatrix}, \begin{pmatrix}1&0\\0&1\end{pmatrix}\right\}$	$\mathrm{PGL}_2(\mathbb{Z}/4\mathbb{Z})$

(We have omitted from the table the case that N_4 is trivial, since then $Q \simeq \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$, which has order $2^5 \cdot 3$ and thus cannot be a quotient of $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$.) In the third row of the table, the action of $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ on $(\mathbb{Z}/2\mathbb{Z})^2$ defining the semi-direct product is the usual action by matrix multiplication on column vectors, while in the fourth row of the table, the action is defined via

$$g \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{cases} \begin{pmatrix} x \\ y \end{pmatrix} & \text{if } g \in \left\{\begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\1&0\end{pmatrix}, \begin{pmatrix}0&1\\1&1\end{pmatrix}\right\}, \\ \begin{pmatrix} y \\ x \end{pmatrix} & \text{if } g \in \left\{\begin{pmatrix}1&1\\0&1\end{pmatrix}, \begin{pmatrix}1&0\\1&1\end{pmatrix}, \begin{pmatrix}0&1\\1&0\end{pmatrix}\right\}. \end{cases}$$

Since 9 does not divide $|Q|$, the degree of the projection $Q \twoheadrightarrow Q_3$ is either 1 or 3. Inspecting the table above, we see that in all cases except $Q = \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$, either Q has no normal subgroup of order 3, or for each normal subgroup $K_3 \trianglelefteq Q$ of order 3, $Q_3 \simeq Q/K_3$ has $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ as a quotient group. Since $[\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}), \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})] = \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$, the group $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ cannot have $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ as a quotient group, and so we must have $Q \simeq Q_3$ in these cases, as desired.

When $Q = \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$, we must proceed differently. Suppose that $Q = \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ and (for the sake of contradiction) that $Q \neq Q_3$, so that the projection $Q \twoheadrightarrow Q_3$ has degree 3. Then $Q_3 \simeq \mathbb{Z}/2\mathbb{Z}$, which implies that $N_3 = \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$, so that

$$N_9 \subseteq \pi_{9,3}^{-1}(\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})) \subseteq \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z}).$$

Furthermore, the quotient group $\pi_{9,3}^{-1}(\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z}))/N_9 \simeq \mathbb{Z}/3\mathbb{Z}$, and in particular is abelian. A commutator calculation shows that

$$[\pi_{9,3}^{-1}(\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})), \pi_{9,3}^{-1}(\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z}))] = \pi_{9,3}^{-1}(\mathcal{N}) \cap \mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z}),$$

(see (7)) and that the corresponding quotient group satisfies

$$\pi_{9,3}^{-1}(\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z}))/[\pi_{9,3}^{-1}(\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})), \pi_{9,3}^{-1}(\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z}))] \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

Furthermore, fixing a pair of isomorphisms

$$\eta_1 \colon \left(\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\1&0\end{pmatrix}, \begin{pmatrix}0&1\\1&1\end{pmatrix}\right\}, \cdot\right) \longrightarrow (\mathbb{Z}/3\mathbb{Z}, +),$$
$$\eta_2 \colon (1 + 3 \cdot \mathbb{Z}/9\mathbb{Z}, \cdot) \longrightarrow (\mathbb{Z}/3\mathbb{Z}, +),$$

and defining the characters

$$\chi_1\colon \pi_{9,3}^{-1}(\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})) \longrightarrow \mathbb{Z}/3\mathbb{Z},$$
$$\chi_2\colon \pi_{9,3}^{-1}(\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})) \longrightarrow \mathbb{Z}/3\mathbb{Z}$$

by $\chi_1 = \eta_1 \circ \theta \circ \pi_{9,3}$ and $\chi_2 = \eta_2 \circ \det$, we have that every homomorphism $\chi\colon \pi_{9,3}^{-1}(\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})) \to \mathbb{Z}/3\mathbb{Z}$ must satisfy

$$\chi = a_1\chi_1 + a_2\chi_2,$$

for appropriately chosen $a_1, a_2 \in \mathbb{Z}/3\mathbb{Z}$. In particular,

$$N_9 = \ker(a_1\chi_1 + a_2\chi_2) \tag{27}$$

for some choice of $a_1, a_2 \in \mathbb{Z}/3\mathbb{Z}$. One checks that

$$\exists g \in \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z}),\ x \in \pi_{9,3}^{-1}(\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})) \ \text{ for which } \ \chi_1(gxg^{-1}) \neq \chi_1(x),$$

whereas $\chi_2(gxg^{-1}) = \chi_2(x)$ for any such choice of g and x. Since N_9 is a normal subgroup of $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$, it follows that $a_1 = 0, a_2 \neq 0$ in (27). This implies that $N_9 = \mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$, which contradicts the fact that $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})/N_9 \simeq Q \simeq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ is non-abelian. This contradiction shows that we must have $Q \simeq Q_3$, and this verifies (25), completing the proof of Proposition 2.4. □

As already observed, the proof of Proposition 2.4 completes the proof of Theorem 1.6. □

3. Acknowledgments

This note was written following discussions which started during the CIRM Winter School "Frobenius Distributions of Curves" in Luminy, France. The authors thank the Centre International de Rencontres Mathématiques for its support. They are also grateful to T. Dokchitser and D. Grant for helpful comments on an earlier version.

References

[1] J. Brau *Selmer groups of elliptic curves and Galois representations*, PhD Thesis, University of Cambridge (2014).

[2] A.C. Cojocaru, D. Grant and N. Jones, *One-parameter families of elliptic curves over $\mathbb{Q}$ with maximal Galois representations*, Proc. Lond. Math. Soc. **103**, no. 3 (2011), 654–675.

[3] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, in Modular Functions of One Variable II, Lecture Notes in Mathematics **349** (1973) 143–316.

[4] T. Dokchitser and V. Dokchitser, *Surjectivity of mod 2^n representations of elliptic curves*, Math. Z. **272** (2012), 961–964.

[5] N. Elkies, *Elliptic curves with* 3*-adic Galois representation surjective mod* 3 *but not mod* 9, preprint (2006).

[6] N. Jones, *Almost all elliptic curves are Serre curves*, Trans. Amer. Math. Soc. **362** (2010), 1547-1570.

[7] N. Jones, GL_2*-representations with maximal image*, Math. Res. Lett., to appear.

[8] S. Lang and H. Trotter, *Frobenius distribution in* GL_2 *extensions*, Lecture Notes in Math. **504**, Springer (1976).

[9] V. Radhakrishnan, *Asymptotic formula for the number of non-Serre curves in a two-parameter family*, Ph.D. Thesis, University of Colorado at Boulder (2008).

[10] K. Ribet, *Galois action on division points of Abelian varieties with real multiplications*, Amer. J. Math. **98**, no. 3 (1976), 751–804.

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

[12] J-P. Serre, *Résumé des cours de 1977-1978*, Annuaire du Collège de France 1978, 67–70.

[13] D. Zywina, *Elliptic curves with maximal Galois action on their torsion points*, Bull. Lond. Math. Soc. **42** (2010), 811–826.

(J. Brau)

- J. Brau, Faculty of Mathematics, Centre for Mathematical Sciences, Wilberforce Road, Cambridge CB3 0WA, United Kingdom.

E-mail address, J. Brau: `jb711@cam.ac.uk`

(N. Jones)

- Department of Mathematics, Statistics, and Computer Science, University of Illinois at Chicago, 322 Science and Engineering Offices (M/C 249), 851 S. Morgan Street, Chicago, IL 60607-7045, USA.

E-mail address, N. Jones: `ncjones@uic.edu`