Universiteit
Leiden
The Netherlands

Galois representations of elliptic curves and abelian entanglements

Brau Avila, Julio

Citation
Brau Avila, J. (2015, December 1). *Galois representations of elliptic curves and abelian entanglements*. Retrieved from https://hdl.handle.net/1887/37019

Version:	Corrected Publisher's Version
License:	Licence agreement concerning inclusion of doctoral thesis in the Institutional Repository of the University of Leiden
Downloaded from:	https://hdl.handle.net/1887/37019

Note: To cite this publication please use the final published version (if applicable).

Cover Page

Universiteit Leiden

The handle http://hdl.handle.net/1887/37019 holds various files of this Leiden University dissertation

Author: Brau Avila, Julio
Title: Galois representations of elliptic curves and abelian entanglements
Issue Date: 2015-12-01

Chapter 3

Non-Serre curves

3.1 Introduction

Let E be a non-CM elliptic curve over a number field K. As we have seen in chapters 1 and 2, understanding the image of ρ_E in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ amounts to understanding the ℓ-adic images $\rho_{E,\ell^\infty}(G_K)$ for every prime ℓ as well as 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. We have also seen such entanglement fields appear prominently in Chapter 2. Indeed, using Lemma 2.3.1 we see that the character sum method for the study of conjectural constants can only be applied to the class of elliptic curves whose entanglement fields are abelian extensions of K. This naturally leads to the question: 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 coprime integers for which the entanglement field $K(E[m_1]) \cap K(E[m_2])$ is non-abelian over K? The study of correction factors done in Chapter 2 illustrates why it would be of interest to obtain a complete classification of such examples.

In this chapter we show that there does indeed exist at least one infi-

nite family of curves such that the curves in it do not satisfy the abelian entanglements property. The character sum method as we have developed it cannot be applied to the curves in this family, however we will see that with some additional restrictions it still can be. The family of curves we have found appears to be of a very idiosyncratic nature.

Let us restrict our attention now to elliptic curves over $\mathbb{Q}$. With respect to understanding the 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. Recall from Section 2.4.1 that for any elliptic curve E over $\mathbb{Q}$ one has

$$\mathbb{Q}(\sqrt{\Delta_E}) \subseteq \mathbb{Q}(E[2]) \cap \mathbb{Q}(\zeta_n), \tag{3.1.1}$$

where $n = 4|\Delta_E|$, and that a Serre curve is one whose Galois action on its torsion points is as large as possible. That is, it satisfies that $[\mathrm{GL}_2(\hat{\mathbb{Z}}) : \rho_E(G_{\mathbb{Q}})] = 2$. These are precisely the curves E over $\mathbb{Q}$ for which the entanglement (3.1.1) is the only obstruction to surjectivity of ρ_E. It is also shown in Section 2.4 that Serre curves have abelian entanglements.

Let $E_{r,s}$ denote the curve given by the equation

$$E_{r,s} : Y^2 = X^3 + rX + s.$$

For a varying parameter x let $R(x)$ and $S(x)$ be a given length and width that grow with x and define

$$C(x) := \{E_{r,s} : (r,s) \in \mathbb{Z}^2, |r| \leqslant R(x), |s| \leqslant S(x) \text{ and } 4r^3 + 27s^2 \neq 0\}.$$

In [Jon10] Nathan Jones proves a theorem bounding the mean-square error in the Chebotarev theorem for division fields of elliptic curves and uses this

to count the elliptic curves over $\mathbb{Q}$ which are Serre curves. More precisely, he proves the following theorem (Theorem 4 in [Jon10]).

Theorem 3.1.1 (Jones). *Let $C_{Serre}(x)$ denote the set*

$$\{E_{r,s} \in C(x) : E_{r,s} \text{ is a Serre curve}\}.$$

Assuming that $\min\{R(x), S(x)\} \geqslant x^2$, one has

$$|C(x) - C_{Serre}(x)| \ll \frac{|C(x)| \log^B x}{x},$$

where B is an explicit constant. Thus, in particular,

$$\lim_{x\to\infty} \frac{|C_{Serre}(x)|}{C(x)|} = 1.$$

The main algebraic ingredient used by Jones in his proof is the following lemma (Lemma 5 in [Jon10]) which gives a sufficient condition for an elliptic curve E to be a Serre curve.

Lemma 3.1.2 (Jones). *Suppose E is an elliptic curve over $\mathbb{Q}$ such that:*

1. *For all primes ℓ we have that $\rho_{E,\ell}(G_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$,*
2. *$\rho_{E,72}(G_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{Z}/72\mathbb{Z})$.*

Then E is a Serre curve.

In [Zyw10], Zywina generalizes Theorem 3.1.1 to the case $K \neq \mathbb{Q}$ (see also [Rad08], which sharpens the upper bound to an asymptotic formula). In [GJ11], 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 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

$$E \text{ is not a Serre curve} \iff j(E) \in \bigcup_{X \in \mathcal{X}} j(X(\mathbb{Q})), \tag{3.1.2}$$

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

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

In [GJ11], the authors use (3.1.2) 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 chapter.

Question 3.1.3. *What is an explicit list of modular curves in a family* $\mathcal{X} = \{X_1, X_2, \dots\}$ *satisfying* (3.1.2)*?*

In order to answer this question it will be essential to have a necessary and sufficient condition for an elliptic curve to be a Serre curve. Lemma 3.1.2 above gives a sufficient condition, and this was furthered strengthened by Jones (Corollary 2.12 in [Jon]) to provide a necessary condition as well.

Proposition 3.1.4 (Jones)**.** *Let E be an elliptic curve over $\mathbb{Q}$. Then E is a Serre curve if and only if the following two conditions hold.*

1. *For each prime $\ell \geqslant 5$, $\rho_{E,\ell}(G_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.*
2. *One has $[\rho_{E,36}(G_{\mathbb{Q}}), \rho_{E,36}(G_{\mathbb{Q}})] = [\mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z}), \mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z})]$.*

Let $\mathcal{E}_\ell$ 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. Then we have seen in Section 1.2.3 that

$$\mathcal{E}_\ell \subseteq \left\{X_0(\ell), X^+_{\text{split}}(\ell), X^+_{\text{non-split}}(\ell), X_{A_4}(\ell), X_{S_4}(\ell), X_{A_5}(\ell)\right\} \tag{3.1.3}$$

where 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. We have then

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

If $\rho_{E,\ell}$ is surjective for all primes ℓ and E is not a Serre curve then by Proposition 3.1.4 the obstruction must be coming from the mod 36 representation. By Corollary 1.2.4 we have that if $\rho_{E,\ell}$ is surjective then so is the ℓ-adic representation ρ_{E,ℓ^∞}, however this is not necessarily true for $\ell = 2, 3$. These obstructions are described by two other modular curves $X'(4)$ and $X''(4)$ of level 4, and another $X'(9)$ of level 9, which have been considered in [DD12] and [Elk06], respectively.

Here 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 (3.1.2), answering Question 3.1.3. Let $X(n)$ denote the complete modular curve of level n, and 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. Recall from Section 1.2.3 that for any $x \in \mathbb{P}^1(\mathbb{Q})$, we have that

$$x \in j(X_H(\mathbb{Q})) \iff \begin{array}{c}\exists \text{ an elliptic curve } E \text{ over } \mathbb{Q} \text{ and } \exists g \in \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \\ \text{with } j(E) = x \text{ and } \rho_{E,n}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) \subseteq g^{-1}Hg.\end{array} \tag{3.1.4}$$

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

$$\mathcal{N} := \left\{ \begin{pmatrix} x & -y \\ y & x \end{pmatrix} : \ x^2 + y^2 \equiv 1 \mod 3 \right\} \sqcup \left\{ \begin{pmatrix} x & y \\ y & -x \end{pmatrix} : \ x^2 + y^2 \equiv -1 \mod 3 \right\}. \quad (3.1.5)$$

This subgroup fits into an exact sequence

$$1 \longrightarrow \mathcal{N} \longrightarrow \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \longrightarrow 1, \quad (3.1.6)$$

and we denote by

$$\theta \colon \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \quad (3.1.7)$$

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

$$X'(6) := X_{H'_6}, \ \text{ where } \ H'_6 := \{(g_2, g_3) \in \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) : g_2 = \theta(g_3)\} \subseteq \mathrm{GL}_2(\mathbb{Z}/6\mathbb{Z}). \quad (3.1.8)$$

Unravelling (3.1.4) in this case, we find that, for every elliptic curve E over $\mathbb{Q}$,

$$j(E) \in j(X'(6)(\mathbb{Q})) \iff E \simeq_{\overline{\mathbb{Q}}} E' \ \text{ for some } E' \text{ over } \mathbb{Q} \text{ for which } \mathbb{Q}(E'[2]) \subseteq \mathbb{Q}(E'[3]). \quad (3.1.9)$$

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 3.1.5. *There exists a parameter $t\colon X'(6) \longrightarrow \mathbb{P}^1$, whose inverse 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 3.1.6. By (3.1.9), Theorem 3.1.5 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 3.1.3. 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 $(\mathbb{Z}/\ell\mathbb{Z})^\times$:

$$\mathcal{G}_{\ell,\max} := \{H \subsetneq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) :\ \det(H) = (\mathbb{Z}/\ell\mathbb{Z})^\times \\ \text{and } \nexists H_1 \text{ with } H \subsetneq H_1 \subsetneq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})\}. \quad (3.1.10)$$

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 (3.1.4), the collection $\mathcal{X}$ occurring in (3.1.2) must contain as a subset

$$\mathcal{E}_\ell := \{X_H :\ H \in \mathcal{R}_\ell\}, \quad (3.1.11)$$

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 (3.1.3)). 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 $\det\colon \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \longrightarrow (\mathbb{Z}/4\mathbb{Z})^\times \simeq \{\pm 1\}$ as taking the values ± 1.

$$\begin{aligned} X'(4) = X_{H_4'}, \quad \text{where} \quad H_4' &:= \{g \in \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) : \\ &\qquad \det g = \varepsilon(g \bmod 2)\} \subseteq \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}), \\ X''(4) = X_{H_4''} \quad \text{where} \quad H_4'' &:= \left\langle \begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\rangle \subseteq \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}), \\ X'(9) = X_{H_9'} \quad \text{where} \quad H_9' &:= \left\langle \begin{pmatrix} 0 & 2 \\ 4 & 0 \end{pmatrix}, \begin{pmatrix} 4 & 1 \\ -3 & 4 \end{pmatrix}, \right. \\ &\qquad \left. \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle \subseteq \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z}). \end{aligned} \tag{3.1.12}$$

For more details on these modular curves, see [DD12] and [Elk06].

Theorem 3.1.7. *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 (3.1.12)*, $X'(6)$ is defined by* (3.1.8)*, and $\mathcal{E}_\ell$ is as in* (3.1.11)*. Then, for any elliptic curve E over $\mathbb{Q}$,*

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

3.2 Proofs

We now prove Theorems 3.1.5 and 3.1.7.

Proof of Theorem 3.1.5. 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

$$\Delta_{\mathbb{E}} = -2^6 3^3 (1-4t^3)^2 \quad \text{and} \quad j(\mathbb{E}) = 2^{10}3^3 t^3 (1-4t^3). \tag{3.2.1}$$

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 (3.2.1) at t. We will show that, for any $t \in \mathbb{Q}$, one has

$$\mathbb{Q}(\mathbb{E}_t[2]) \subseteq \mathbb{Q}(\mathbb{E}_t[3]). \tag{3.2.2}$$

By (3.1.9) and (3.2.1), 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 3.1.5 will then follow. To verify (3.2.2), we will show that, for every $t \in \mathbb{Q}$, one has

$$\mathbb{Q}(\mathbb{E}_t[2]) \subseteq \mathbb{Q}(\zeta_3, \Delta_{\mathbb{E}_t}^{1/3}). \tag{3.2.3}$$

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 [LT74, p. 181] and the references given there). Thus, the containment (3.2.2) follows from (3.2.3). Finally, (3.2.3) 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 3.1.5. □

Remark 3.2.1. 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 3.1.7, whose proof employs the following group theoretic lemma. Recall from Section 1.2.2 that if ψ is the abbreviation for the ordered pair (ψ_0, ψ_1), then the group G given by

$$G_1 \times_\psi G_2 := \{(g_1, g_2) \in G_1 \times G_2 : \psi_1(g_1) = \psi_2(g_2)\} \tag{3.2.4}$$

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

$$G_0 \times_\psi G_1 \subseteq G_0 \times_{f\circ\psi} G_1. \tag{3.2.5}$$

Lemma 3.2.2. *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 [LT74, Lemma 1, p. 174] (the hypothesis of this lemma is readily verified when Q is cyclic). □

Proof of Theorem 3.1.7. Using Proposition 3.1.4 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

$$\pi_{36,d} \colon \mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/d\mathbb{Z}) \tag{3.2.6}$$

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

$$\mathcal{G}_{36} := \left\{ H \subseteq \mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z}) : \begin{array}{c} \forall d \in \{2, 3\},\ \pi_{36,d}(H) = \mathrm{GL}_2(\mathbb{Z}/d\mathbb{Z}), \\ \det(H) = (\mathbb{Z}/36\mathbb{Z})^\times, \\ \text{and } [H, H] \subsetneq [\mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z}), \mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z})] \end{array} \right\}, \tag{3.2.7}$$

and note that

$$E \text{ is not a Serre curve} \iff \begin{array}{c} \exists \text{ a prime } \ell \text{ and } H \in \mathcal{G}_{\ell,\max} \text{ for which} \\ \rho_{E,\ell}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) \subseteq H, \\ \text{or } \exists H \in \mathcal{G}_{36} \text{ for which} \\ \rho_{E,36}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) \subseteq H. \end{array} \tag{3.2.8}$$

As in the prime level case, we need only consider *maximal* subgroups $H \in \mathcal{G}_{36}$, and because of (3.1.4), 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 (3.2.8) now becomes (see (3.1.11))

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

Thus, Theorem 3.1.7 will follow from the next proposition.

Proposition 3.2.3. *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 (3.2.6) *and the groups H_4', H_4'', H_9' and H_6' are given by* (3.1.12) *and* (3.1.8).

Proof. Let $H \in \mathcal{G}_{36,\max}$. If $\pi_{36,4}(H) \neq \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$, then [DD12] 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 [Elk06] 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 1.2.7, this implies that there exists

a group Q and a pair of surjective homomorphisms

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

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

$$H \subseteq \{(g_4, g_9) \in \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z}) : \ \theta(g_9 \bmod 3) = g_4 \bmod 2\}, \tag{3.2.9}$$

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 (3.1.7), whose graph determines the level 6 structure defining the modular curve $X'(6)$. This will finish the proof of Proposition 3.2.3.

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:

$$\begin{aligned} 1 &\longrightarrow N_9 \longrightarrow \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z}) \longrightarrow Q \longrightarrow 1\\ 1 &\longrightarrow N_4 \longrightarrow \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \longrightarrow Q \longrightarrow 1\\ 1 &\longrightarrow N_3 \longrightarrow \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) \longrightarrow Q_3 \longrightarrow 1\\ 1 &\longrightarrow N_2 \longrightarrow \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \longrightarrow Q_2 \longrightarrow 1, \end{aligned} \tag{3.2.10}$$

as well as

$$\begin{aligned} 1 &\longrightarrow K_2 \longrightarrow Q \longrightarrow Q_2 \longrightarrow 1\\ 1 &\longrightarrow K_3 \longrightarrow Q \longrightarrow Q_3 \longrightarrow 1, \end{aligned} \tag{3.2.11}$$

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

$$Q_2 \simeq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \quad \text{and} \quad Q_3 \simeq Q, \tag{3.2.12}$$

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 (3.2.5) 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 (3.1.6) and the fact that every automorphism of $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ is inner, implies that (3.2.9) holds, up to $\mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z})$-conjugation. Thus, the proof of Proposition 3.2.3 is reduced to showing that (3.2.12) 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 (3.2.11), we see that Q must then be a 2-group, and since K_3 has order a power of 3 (possibly 1), we see that $Q \simeq Q_3$, and the third exact sequence in (3.2.10) 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 3.2.2, we find that $[H, H] = [\mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z}), \mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z})]$, contradicting (3.2.7). 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

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

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

$$\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \simeq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \ltimes M_{2\times 2}(\mathbb{Z}/2\mathbb{Z}), \tag{3.2.13}$$

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 (3.2.13), 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 we must be in one of the following 5 cases.

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 (3.1.5)) 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

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

and defining the characters

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

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,

$$N_9 = \ker(a_1\chi_1 + a_2\chi_2) \tag{3.2.14}$$

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 (3.2.14). 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 (3.2.12), completing the proof of Proposition 3.2.3. □

As already observed, the proof of Proposition 3.2.3 completes the proof of Theorem 3.1.7. □

3.3 Elliptic curves without abelian entanglements

Let us study in more detail one example coming from the family of curves in Theorem 3.1.5. Consider the curve $E/\mathbb{Q}$ given by minimal Weierstrass equation $Y^2 = X^3 - 63504X + 6223392$. This curve has $j(E) = -2^{10}3^4$, as well as $\Delta = -2^4 3^{11} 7^6$. Machine computation shows that $G(\ell) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ and $\mathbb{Q}(E[2]) \subset \mathbb{Q}(E[3])$. We also have that $\mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{-3})$, which is what we expect since the maximal abelian extension inside $\mathbb{Q}(E[3])$ is precisely $\mathbb{Q}(\sqrt{-3})$.

Suppose we wish to compute the conjectural density of primes p such that $\tilde{E}(\mathbb{F}_p)$ is cyclic. As we have seen, the naive density of this is $\prod_\ell \delta_\ell$, however a correction factor is needed. As the only critical primes are $2, 3$

and 7, the density we are looking for is

$$C_E = \frac{|G(42) \cap \mathcal{S}_{42}|}{G(42)|} \prod_{\ell \neq 2,3,7} \delta_\ell,$$

where we are using the notation of Section 2.4. Now $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ and $\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$ have no simple non-abelian quotients, hence any entanglement between the fields $\mathbb{Q}(E[3])$ and $\mathbb{Q}(E[7])$ would have to contain a non-trivial abelian subfield. However the maximal abelian extensions of $\mathbb{Q}(E[3])$ and $\mathbb{Q}(E[7])$ are $\mathbb{Q}(\zeta_3)$ and $\mathbb{Q}(\zeta_7)$, hence we conclude $\mathbb{Q}(E[3]) \cap \mathbb{Q}(E[7]) = \mathbb{Q}$. This implies that $G(42) = G(6) \times G(7)$, hence

$$C_E = \frac{|G(6) \cap \mathcal{S}_6|}{|G(6)|} \prod_{\ell \neq 2,3} \delta_\ell,$$

Finally, note that because $G(6) = G(3)$ and $G(2)$ is a quotient of $G(6)$, then

$$\frac{|G(6) \cap \mathcal{S}_6|}{|G(6)|} = \frac{|S(2)|}{|G(2)|}.$$

Using machine computation we find that the observed density of primes $p \leqslant 100000000$ is 0.831069 while our computation yields

$$\begin{aligned} C_E &= \prod_{\ell \neq 3} \delta_\ell \\ &\approx 0.831066. \end{aligned}$$

As mentioned in the introduction, another natural question which arises from this is whether one can one classify the triples (E, m_1, m_2) with E an elliptic curve over $\mathbb{Q}$ and m_1, m_2 a pair of coprime integers for which the entanglement field $\mathbb{Q}(E[m_1]) \cap \mathbb{Q}(E[m_2])$ is non-abelian over $\mathbb{Q}$. We are not sure if any other families exist, however one systematic way one could possibly rule out other examples is via the following steps.

(i) Classify the non-abelian groups which arise as common quotients of subgroups H_{m_1} and H_{m_2}, where $H_{m_i} \subset \mathrm{GL}_2(\mathbb{Z}/m_i\mathbb{Z})$ and $\det(H_{m_i}) = (\mathbb{Z}/m_i\mathbb{Z})^\times$ for $i = 1, 2$.

(ii) For each example in step (i), compute the genus of the associated modular curve.

(iii) For each modular curve in step (ii), decide whether or not it has any rational points.

For each of these families of curves it would also be of interest to find a systematic way to compute their entanglement correction factors. For the family we have described here this is easy to do because one of the torsion fields is fully contained in another one. It may occur however, at least in theory, that a curve could have many non-abelian intersections between various of its torsion fields. However it seems unlikely many examples of this type exist.