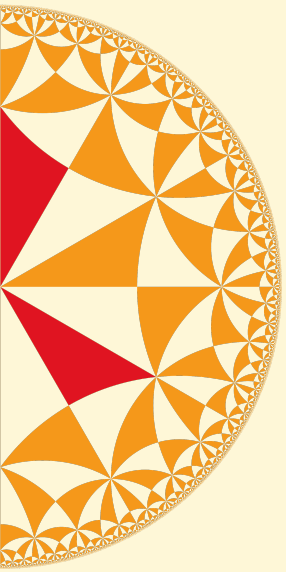
Université Grenoble Alpes



ANNALES DE
L'INSTITUT FOURIER

Harris B. Daniels & Álvaro Lozano-Robledo

Coincidences of division fields

Tome 73, nº 1 (2023), p. 163-202.

https://doi.org/10.5802/aif.3520

Les *Annales de l'Institut Fourier* sont membres du Centre Mersenne pour l'édition scientifique ouverte
www.centre-mersenne.org e-ISSN : 1777-5310

Ann. Inst. Fourier, Grenoble
73, 1 (2023) 163-202

COINCIDENCES OF DIVISION FIELDS

by Harris B. DANIELS & Álvaro LOZANO-ROBLEDO

Abstract. — Let E be an elliptic curve defined over $\mathbb{Q}$, and let $\rho_E\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2,\widehat{\mathbb{Z}})$ be the adelic representation associated to the natural action of Galois on the torsion points of $E(\overline{\mathbb{Q}})$. By a theorem of Serre, the image of ρ_E is open, but the image is always of index at least 2 in $\mathrm{GL}(2,\widehat{\mathbb{Z}})$ due to a certain quadratic entanglement amongst division fields. In this paper, we study other types of abelian entanglements. More concretely, we classify the elliptic curves $E/\mathbb{Q}$, and primes p and q such that $\mathbb{Q}(E[p]) \cap \mathbb{Q}(\zeta_{q^k})$ is non-trivial, and determine the degree of the coincidence. As a consequence, we classify all elliptic curves $E/\mathbb{Q}$ and integers m, n such that the m-th and n-th division fields coincide, i.e., when $\mathbb{Q}(E[n]) = \mathbb{Q}(E[m])$, when the division field is abelian.

Résumé. — Soit E une courbe elliptique définie sur $\mathbb{Q}$ et soit $\rho_E\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2,\widehat{\mathbb{Z}})$ la représentation adélique associée à l'action naturelle de Galois sur les points de torsion de $E(\overline{\mathbb{Q}})$. Par un théorème de Serre, l'image de ρ_E est ouverte mais toujours d'indice au moins 2 dans $\mathrm{GL}(2,\widehat{\mathbb{Z}})$ en raison d'un certain enchevêtrement quadratique entre les corps de division. Dans cet article, nous étudions d'autres types d'enchevêtrements abéliens. Plus concrètement, nous classifions les courbes elliptiques $E/\mathbb{Q}$ et les nombres premiers p et q tels que $\mathbb{Q}(E[p]) \cap \mathbb{Q}(\zeta_{q^k})$ est non trivial et déterminons le degré de l'intersection. En conséquence, nous classifions toutes les courbes elliptiques $E/\mathbb{Q}$ et les entiers m, n tels que les corps de division m-ième et n-ième coïncident, c'est-à-dire lorsque $\mathbb{Q}(E[n]) = \mathbb{Q}(E[m])$, lorsque ce corps de division est abélien.

1. Introduction

Let $E/\mathbb{Q}$ be an elliptic curve, let $n > 1$ be an integer, let $\overline{\mathbb{Q}}$ be a fixed algebraic closure of $\mathbb{Q}$, and let $\mathbb{Q}(E[n]) \subset \overline{\mathbb{Q}}$ be the n-th division field, i.e., $\mathbb{Q}(E[n])$ is the field of definition of the n-torsion subgroup $E[n] \subseteq E(\overline{\mathbb{Q}})$. The absolute Galois group of $\mathbb{Q}$, hereby denoted by $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, acts on $E[n]$ and induces a Galois representation $\rho_{E,n}\colon G_{\mathbb{Q}} \to \mathrm{Aut}(E[n]) \simeq$

Keywords: Elliptic Curves, Division Fields, Galois Representations.
2020 *Mathematics Subject Classification:* 11G05, 14H52.

$\mathrm{GL}(2,\mathbb{Z}/n\mathbb{Z})$. If p is a prime, then $G_{\mathbb{Q}}$ acts on the Tate p-adic module $T_p(E) = \varprojlim E[p^n]$, and on the $\widehat{\mathbb{Z}}$-module $T(E) = \varprojlim E[n]$, and induces p-adic representations $\rho_{E,p^\infty} \colon G_{\mathbb{Q}} \to \mathrm{GL}(2,\mathbb{Z}_p)$, and an adelic Galois representation

$$\rho_E \colon G_{\mathbb{Q}} \to \mathrm{Aut}(T(E)) \simeq \mathrm{GL}(2,\widehat{\mathbb{Z}}).$$

There has been much recent work and interest in understanding the image of the various Galois representations mentioned above (see for example [20, 21, 25, 28, 29]).

Famously, Serre [21] showed that if $E/\mathbb{Q}$ has no complex multiplication, then the image G_E of ρ_E is open (therefore, of finite index) in $\mathrm{GL}(2,\widehat{\mathbb{Z}})$. Further, it is well-known (pointed out by Serre in [21, Proposition 22]) that the index $d_E = [\mathrm{GL}(2,\widehat{\mathbb{Z}}) : G_E] \geqslant 2$. Indeed, if Δ_E is the minimal discriminant of $E/\mathbb{Q}$, then $\mathbb{Q}(\sqrt{\Delta_E}) \subseteq \mathbb{Q}(E[2])$ and there is also some $m > 2$ (the integer $m = 4|\Delta_E|$ works) such that $\mathbb{Q}(\sqrt{\Delta_E}) \subseteq \mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(E[m])$, so that $\mathbb{Q}(E[2]) \cap \mathbb{Q}(\zeta_m)$ is a non-trivial quadratic extension of $\mathbb{Q}$, and therefore $\mathrm{Gal}(\mathbb{Q}(E[2],\zeta_m)) \subsetneq \mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. This *entanglement* of division fields causes the index d_E to be at least 2. When the index d_E is exactly 2, then we say that E is a Serre curve, and these have been studied in [7, 14, 15], for instance.

It is therefore natural to study other types of entanglements of division fields that would cause d_E to be strictly larger than 2. For instance, Brau and Jones [3], and Morrow [19, Theorem 8.7] have classified all elliptic curves $E/\mathbb{Q}$ such that $\mathbb{Q}(E[2]) \subseteq \mathbb{Q}(E[3])$ (in fact, their work classifies all the possible non-abelian fields that can occur as $\mathbb{Q}(E[2]) \cap \mathbb{Q}(E[3])$). In this paper, we consider the following question:

Question 1.1. — *Fix an elliptic curve $E/\mathbb{Q}$, and distinct integers $n, m \geqslant 2$:*

(1) *Are there distinct integers $n, m \geqslant 2$ such that $\mathbb{Q}(E[n]) = \mathbb{Q}(E[m])$?*
(2) *In light of the entanglement described above, are there distinct prime numbers p and q, and $k \geqslant 1$, such that $\mathbb{Q}(E[p]) \cap \mathbb{Q}(\zeta_{q^k})$ is non-trivial?*

If so, can we classify all the elliptic curves E for which (1) *or* (2) *occurs? Note that* (1) *can be interpreted vertically (in towers, i.e., n divides m) or horizontally ($\gcd(n,m) = 1$). We will address both possibilities.*

There has been prior work on abelian entanglements related to Question 1.1, part (2). In [13], González-Jiménez and the second author classified all elliptic curves such that the full n-th division field $\mathbb{Q}(E[n])$ is an abelian extension of $\mathbb{Q}$. More generally, Chou [5] has classified the torsion

subgroups $E(\mathbb{Q}^{\mathrm{ab}})_{\mathrm{tors}}$ that can occur for elliptic curves E over $\mathbb{Q}$, where $\mathbb{Q}^{\mathrm{ab}}$ is the maximal abelian extension of $\mathbb{Q}$ within a fixed algebraic closure. Here we shall extend these works by studying the possibilities for $\mathbb{Q}(E[p])\cap\mathbb{Q}^{\mathrm{ab}}$.

It is worth noting that, by results of [11, 14], almost all elliptic curves are Serre curves (that is, $d_E = 2$). In particular, for almost all elliptic curves $E/\mathbb{Q}$ we have that $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \simeq \mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z})$, for all odd $n \geqslant 2$, and so comparing their degrees one can see that there are no $m \neq n \geqslant 2$ such that $\mathbb{Q}(E[n]) = \mathbb{Q}(E[m])$. Similarly, it follows that for a Serre curve $\mathbb{Q}(E[p]) \cap \mathbb{Q}(\zeta_{q^k})$ is always trivial for all odd primes $p \neq q$, and all $k \geqslant 1$. Thus, examples of coincidences of division fields should be somewhat rare. Nonetheless, with a simple search one can find some examples of such behavior.

Example 1.2. — Let E be the elliptic curve with Cremona label `486d2` which is given by $y^2 = x^3 + 405x - 9882$, and let L be the splitting field of $x^3 + 3$, i.e., $L = \mathbb{Q}(\zeta_3, \sqrt[3]{3})$, with ζ_3 a primitive 3-rd root of unity. Then, as we shall see below,

$$\mathbb{Q}(E[2]) = \mathbb{Q}(E[3]) = \mathbb{Q}(E[6]) = L.$$

Example 1.3. — Let E be the elliptic curve with Cremona label `40a4` which is given by $y^2 = x^3 + 13x - 34$. A simple computation shows that

$$E(\mathbb{Q})_{\mathrm{tors}} = \langle (7, -20) \rangle \simeq \mathbb{Z}/4\mathbb{Z}.$$

Moreover, we have $x^3 + 13x - 34 = (x - 2)(x^2 + 2x + 17)$, where the discriminant of the quadratic factor is -64, and so $\mathbb{Q}(E[2]) = \mathbb{Q}(i)$. Next, factoring the 4-division polynomial of E we obtain

$$f_4(x) = 8(x - 7)(x - 2)(x + 3)(x^2 - 2x + 5)(x^2 + 2x + 17)(x^2 + 6x + 109)$$

which splits completely over $\mathbb{Q}(i)$ and, further, one can verify that

$$\mathbb{Q}(x(E[4])) = \mathbb{Q}(E[4]).$$

Thus,

$$E(\mathbb{Q}(i))_{\mathrm{tors}} = \langle (7, -20), (-3 - 10i, 30 + 10i) \rangle \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$$

Therefore, $\mathbb{Q}(E[2]) = \mathbb{Q}(E[4]) = \mathbb{Q}(i)$. Stevenhagen asked when can one have $\mathbb{Q}(E[2^n]) = \mathbb{Q}(E[2^{n+1}])$ and Rouse and Zureick-Brown comment in a recent paper (see [20, Remark 1.6]) that, as a consequence of their work, this can only happen for $n = 1$ (that is, for $\mathbb{Q}(E[2]) = \mathbb{Q}(E[4])$), and give some examples.

Our first result addresses Question 1.1 in the setting of towers.

THEOREM 1.4. — *Let E be an elliptic curve defined over $\mathbb{Q}$, let p a prime, and let $n \in \mathbb{N}$.*

(1) *Suppose that $\mathbb{Q}(E[p^{n+1}]) = \mathbb{Q}(E[p^n])$. Then, $p = 2$, $n = 1$, and there is a rational number $t \in \mathbb{Q}$ such that E is isomorphic over $\mathbb{Q}$ to an elliptic curve of the form*

$$E_t \colon y^2 = x^3 + A(t)x + B(t),$$

where

$$\begin{aligned} A(t) = {} & -27t^8 + 648t^7 - 4212t^6 - 2376t^5 + 60102t^4 + 79704t^3 \\ & - 105732t^2 - 235224t - 107811, \\ B(t) = {} & 54t^{12} - 1944t^{11} + 24300t^{10} - 97848t^9 - 251262t^8 \\ & + 1722384t^7 + 4821768t^6 - 8697456t^5 - 64323558t^4 \\ & - 140447736t^3 - 157012020t^2 - 90561240t - 21346578. \end{aligned}$$

(2) *If $\mathbb{Q}(E[p^n]) \cap \mathbb{Q}(\zeta_{p^{n+1}}) = \mathbb{Q}(\zeta_{p^{n+1}})$, then $p = 2$.*

Theorem 1.4 will be shown in Section 3. Interestingly, $\mathbb{Q}(E[2^n]) \cap \mathbb{Q}(\zeta_{2^{n+1}}) = \mathbb{Q}(\zeta_{2^{n+1}})$ can indeed occur for all $n > 1$, as we will show at the end of Section 3.3 (see Theorem 3.10).

THEOREM 1.5. — *Let E be the elliptic curve with Cremona label* `32a3`*, which is given by $y^2 = x^3 - 11x - 14$. Then, $\mathbb{Q}(\zeta_{2^{n+1}}) \subseteq \mathbb{Q}(E[2^n])$ for all $n > 1$.*

Our next results address Question 1.1 in a horizontal way. First, we remark that ramification and good reduction impose strong restrictions on equality of division fields.

PROPOSITION 1.6. — *Let $E/\mathbb{Q}$ be an elliptic curve and let $m \geqslant 2$ be an integer, such that there is a prime p of good reduction for $E/\mathbb{Q}$ that does not divide m. Then, $\mathbb{Q}(E[m]) \cap \mathbb{Q}(\zeta_{p^\infty}) = \mathbb{Q}$. In particular, if $n \geqslant 2$ is another integer divisible by p, then $\mathbb{Q}(E[n]) = \mathbb{Q}(E[m])$ is impossible.*

Proof. — If p is a prime of good reduction and $\gcd(p, m) = 1$, then the criterion of Néron–Ogg–Shafarevich shows that $\mathbb{Q}(E[m])/\mathbb{Q}$ is unramified at p. Thus, $\mathbb{Q}(E[m]) \cap \mathbb{Q}(\zeta_{p^\infty}) = \mathbb{Q}$ by ramification-at-p considerations. If in addition p divides n, then $\mathbb{Q}(\zeta_p) \subseteq \mathbb{Q}(E[p]) \subseteq \mathbb{Q}(E[n])$, and the result follows. □

The following theorem answers the question for the intersection of prime division fields for two different primes.

THEOREM 1.7. — *Let $E/\mathbb{Q}$ be an elliptic curve and let $p < q \in \mathbb{Z}$ be distinct primes, and let $n, m \in \mathbb{N}$.*

(1) *If $\mathbb{Q}(E[p^n]) = \mathbb{Q}(E[q^m])$, then $p^n = 2$ and $q^m = 3$. Further, there is some $t \in \mathbb{Q}$ such that E is $\mathbb{Q}$-isomorphic to*
$$E' : y^2 = x^3 - 3t^9(t^3-2)(t^3+2)^3(t^3+4)x - 2t^{12}(t^3+2)^4(t^4-2t^3+4t-2)(t^8+2t^7+4t^6+8t^5+10t^4+8t^3+16t^2+8t+4)$$
or its twist by -3.

(2) *Let $K_p(E) = \mathbb{Q}(E[p]) \cap \mathbb{Q}^{ab}$. Then, $\mathrm{Gal}(K_p(E)/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times \times C$, where C is a cyclic group of order dividing $p-1$. Further, if $E/\mathbb{Q}$ does not have a rational p-isogeny, then C is trivial or quadratic and $K_p(E) = F(\zeta_p)$ with $F/\mathbb{Q}$ a trivial or quadratic extension.*

(3) *In particular, if $\mathbb{Q}(\zeta_{q^n}) \subseteq \mathbb{Q}(E[p])$, then either $\mathbb{Q}(\zeta_{q^n}) = \mathbb{Q}$, $\mathbb{Q}(i)$, or $\mathbb{Q}(\zeta_3)$, or $E/\mathbb{Q}$ has a rational p-isogeny, $p = 2$, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, or 163, and $\varphi(q^n)$ divides $p-1$.*

For example, the curve $E/\mathbb{Q} : y^2 + xy + y = x^3 - x^2 - 2x - 26$, with Cremona label `405d1`, satisfies $\mathbb{Q}(\zeta_9) \subseteq \mathbb{Q}(E[7])$. Finally, our third theorem deals with the particular case of abelian division fields.

THEOREM 1.8. — *Let $E/\mathbb{Q}$ be an elliptic curve and let $n > m \geqslant 2$ be integers, such that $\mathbb{Q}(E[n])/\mathbb{Q}$ is an abelian extension.*

(1) *If $\mathbb{Q}(E[n]) = \mathbb{Q}(E[m])$, then there are two possibilities.*
   (a) *Either $m = 2, n = 4$, and for some $t \in \mathbb{Q}$, $E/\mathbb{Q}$ is $\mathbb{Q}$-isomorphic to*
$$y^2 = x^3 + (-432t^8 + 1512t^4 - 27)x + (3456t^{12} + 28512t^8 - 7128t^4 - 54).$$
   In this case, $\mathbb{Q}(E[2]) = \mathbb{Q}(E[4]) = \mathbb{Q}(i)$.
   (b) *Or $m = 3, n = 6$, with $\mathbb{Q}(E[2]) \subsetneq \mathbb{Q}(E[3]) = \mathbb{Q}(E[6])$, and there is some $t \in \mathbb{Q}$, such that $j(E) = j(t)$ where*
$$j(t) = -\left(\frac{(t^3-3t^2-9t-9)(t^3+3t^2+3t-3)(t^6+12t^5+81t^4+216t^3+243t^2+108t+27)}{t(t+1)^2(t+3)^2(t^2+3)^2(t^2+3t+3)}\right)^3,$$
   Conversely, if $E'/\mathbb{Q}$ is an elliptic curve such that $j(E') = j(t)$ for some $t \in \mathbb{Q}$, then there is a quadratic twist $E''/\mathbb{Q}$ of E' such that $\mathbb{Q}(E''[2]) \subsetneq \mathbb{Q}(E''[3]) = \mathbb{Q}(E''[6])$.

(2) *Let p be prime, such that $\mathbb{Q}(E[p])/\mathbb{Q}$ is abelian, and let $q \neq p$ be another prime. Then, $\mathbb{Q}(E[p]) \cap \mathbb{Q}(\zeta_{q^k})$ can be trivial, quadratic, cyclic cubic (for $p = 2$), or cyclic quartic (for $p = 5$).*

For example, let $E/\mathbb{Q} : y^2 = x^3 - x^2 - 4319x + 100435$, with Cremona label `18176r2`. Then, $\mathrm{Gal}(\mathbb{Q}(E[5])/\mathbb{Q}) \simeq (\mathbb{Z}/4\mathbb{Z})^2$, and $\mathbb{Q}(E[5]) = F(\zeta_5)$ is the compositum of $\mathbb{Q}(\zeta_5)$ and a cyclic quartic field $F \subseteq \mathbb{Q}(\zeta_{16})$.

It is worth pointing out that the family of elliptic curves that appears in part (1) of Theorem 1.4 is a parametrization of the modular curve $\mathtt{X}_{\mathtt{20b}}$ from [20]. Similarly, the family that appears in part (1) of Theorem 1.8 is $\mathtt{X}_{\mathtt{60d}}$. Interestingly, $\mathtt{X}_{\mathtt{60d}}$ parametrizes a subfamily of $\mathtt{X}_{\mathtt{20b}}$ (see Remark 3.7 for more on this). The family that appears in Theorem 1.7 will be constructed in the proof of the theorem at the end of the paper.

Any computations done in this paper have been done using Magma [2] and some code used in this paper was adapted from code written for [7, 8, 9, 18, 26]. For the ease of the reader, anytime a specific elliptic curve is mentioned, we refer to the curve by Cremona reference and include a link to the corresponding LMFDB [27] page.

The structure of the paper is as follows. In Section 2 we introduce the necessary background about Galois representations. Section 3 contains the proof of Theorem 1.4. We first prove the theorem for odd primes in Section 3.1, in Section 3.2 we use [20] to settle the case of $p = 2$ for non-CM curves, and in Section 3.3 we deal with the case of $p = 2$ in the CM case using results from [18]. In Section 4 we show Theorem 1.8, relying on results from [13]. In Section 5 we examine the fields $\mathbb{Q}(E[p]) \cap \mathbb{Q}^{ab}$ so that finally, in Section 6 we can prove Theorem 1.7.

Remark 1.9. — Unfortunately, our methods are not sufficient to classify all the instances when $\mathbb{Q}(E[m]) = \mathbb{Q}(E[n])$ for any natural numbers $n > m \geqslant 2$. We suspect that the only possibilities are $(n, m) \in \{(2, 3), (2, 4), (2, 6), (3, 6)\}$ but the current knowledge on the possible adelic images of $\rho_E \colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2, \widehat{\mathbb{Z}})$ is not sufficient to settle all the possible coincidences. For instance, to conclude a complete list, we would need to know the full list of possible mod-p^2 images, but at the moment this is not known (not even for $p = 3$). More concretely, a more detailed understanding of the classification of mod-9 images would be necessary to rule out, for example, the pair $(6, 9)$, that would be a coincidence between the 6-th and the 9-th division field. With a bit of computational help, we can prove the following result for coincidences in the range $2 \leqslant m < n \leqslant 10$.

Theorem 1.10. — *Let $2 \leqslant m < n \leqslant 10$ be natural numbers, let $E/\mathbb{Q}$ be an elliptic curve, and suppose that $\mathbb{Q}(E[m]) = \mathbb{Q}(E[n])$. Then,*

$$(m, n) \in \{(2, 3), (2, 4), (2, 6), (3, 6), (4, 6), (6, 8), (6, 9), (5, 10)\}.$$

Our results can also show some other special cases, as the following corollary exemplifies (Corollary of Theorem 1.7).

COROLLARY 1.11. — *Let p be a prime, and let $m \geqslant 2$ be an integer divisible by q^n for some odd prime q and $n \geqslant 1$, such that $\varphi(q^n)$ does not divide $p-1$. Then, $\mathbb{Q}(E[p]) = \mathbb{Q}(E[m])$ is impossible.*

Example 1.12. — As a consequence of Corollary 1.11, the division fields $\mathbb{Q}(E[3])$ and $\mathbb{Q}(E[m])$ cannot coincide for any integer m divisible by a prime $p \geqslant 5$.

The proofs of Theorem 1.10 and Corollary 1.11 can be found in Section 7.

Acknowledgements

The authors would like to thank Enrique González-Jiménez, Jackson Morrow, and Filip Najman for helpful comments on an earlier draft of this paper. We would also like to thank the referees for their many helpful comments and suggestions.

2. Galois Representations associated to Elliptic Curves

In this section we cite a number of key results that we will use in the following sections. Let $E/\mathbb{Q}$ be an elliptic curve. For a prime number p, we define the p-adic Tate module of $E/\mathbb{Q}$ by $T_p(E) = \varprojlim E[p^n]$, where the inverse limit is taken with respect to the multiplication-by-p maps $[p]\colon E[p^{n+1}] \to E[p^n]$. The absolute Galois group of $\mathbb{Q}$ acts on $T_p(E)$, and induces a Galois representation

$$\rho_{E,p^\infty}\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(T_p(E)).$$

If we choose a $\mathbb{Z}_p$-basis of $T_p(E)$, then we may consider $\rho_{E,p^\infty}\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(T_p(E)) \simeq \mathrm{GL}(2,\mathbb{Z}_p)$, and we are interested in describing the image of ρ_{E,p^∞} in $\mathrm{GL}(2,\mathbb{Z}_p)$. Much is known about the image of $\rho_{E,p}$, most notably Serre's so-called open image theorem.

THEOREM 2.1 (Serre, [21]). — *Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication and, for each prime p, let $G_p \subseteq \mathrm{GL}(2,\mathbb{Z}_p)$ be the image of ρ_{E,p^∞}. Then, G_p is an open subgroup of $\mathrm{GL}(2,\mathbb{Z}_p)$ for every p (in particular, the index is finite), and $G_p = \mathrm{GL}(2,\mathbb{Z}_p)$ for all but finitely many primes.*

In a recent article [29], Zywina has determined (up to a finite number of j-invariants) a finite list of all possible indices that may occur for the image of the representation $\rho_E\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2,\widehat{\mathbb{Z}})$ that results as inverse image of $\rho_{E,n}\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[n]) \simeq \mathrm{GL}(2,\mathbb{Z}/n\mathbb{Z})$.

Rouse and Zureick-Brown have classified all the possible 2-adic images of $\rho_{E,2^\infty}\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2,\mathbb{Z}_2)$, and Sutherland and Zywina have conjectured the possibilities for the mod p image for all primes p.

Theorem 2.2 (Rouse, Zureick-Brown, [20]). — *Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication. Then, there are exactly* 1208 *possibilities for the 2-adic image $\rho_{E,2^\infty}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$, up to conjugacy in $\mathrm{GL}(2,\mathbb{Z}_2)$. Moreover, the index of $\rho_{E,2^\infty}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ in $\mathrm{GL}(2,\mathbb{Z}_2)$ divides* 64 *or* 96*, and every image is defined at most modulo* 32*.*

Conjecture 2.3 (Sutherland, Zywina, [28]). — *Let $E/\mathbb{Q}$ be an elliptic curve. Let $G \subseteq \mathrm{GL}(2,\mathbb{Z}/p\mathbb{Z})$ be the image of $\rho_{E,p}$. Then, there are precisely* 63 *isomorphism types of images.*

Let us now include here some elementary results that we will use in our proofs in the next section. First, the existence of the Weil pairing implies that the roots of unity $\mathbb{Q}(\zeta_n)$ are contained in the n-th division field.

Proposition 2.4. — *Let $E/\mathbb{Q}$ be an elliptic curve, let n be a positive integer. Then, $\det(\rho_{E,n}) = \chi_n$ is the n-th cyclotomic character. In particular, if we let ζ_n be any primitive n-th root of unity, then $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(E[n])$, and for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ we have $\sigma(\zeta_n) = (\zeta_n)^{\det(\rho_{E,n}(\sigma))}$.*

Proof. — See [6, Lecture 6 Theorem 6.3] and [24, Chapter III, Corollary 8.1.1]. □

Corollary 2.5. — *Let $E/\mathbb{Q}$ be an elliptic curve, let $p > 2$ a prime, let $m, n \geqslant 1$, and suppose that $\mathbb{Q}(\zeta_{p^n}) \subseteq \mathbb{Q}(E[m])$. Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be such that its restriction to $\mathbb{Q}(\zeta_{p^n})$ generates the cyclic group $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q})$. Then, the image of σ through $\rho_{E,m}$ is an element of order divisible by $\varphi(p^n) = p^{n-1}(p-1)$.*

Proof. — This follows immediately from Proposition 2.4, and the fact that if $\mathbb{Q}(\zeta_{p^n}) \subseteq \mathbb{Q}(E[m])$, then the restriction map of Galois groups

$$\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) \simeq (\mathbb{Z}/p^n\mathbb{Z})^\times$$

is surjective, and $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is cyclic because $p > 2$. □

Central to many of our arguments will be the fact that $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(E[n])$, but in order to prove Theorem 1.7 we will need to better understand the

fields of the form $K_E(p) = \mathbb{Q}(E[p]) \cap \mathbb{Q}^{ab}$. In Section 5 we classify just how large the fields $K_E(p)$ can be. In order to do this we break the problem down into cases depending on what maximal group the image of $\rho_{E,p}$ is contained in.

PROPOSITION 2.6 ([21]). — *Let $E/\mathbb{Q}$ be an elliptic curve and let p be a prime. Let G be the image of $\rho_{E,p}\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[p]) \simeq \mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$. Then, there is exists a $\mathbb{Z}/p\mathbb{Z}$-basis for $E[p]$ such that on of the following is true:*

1. *$G = \mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$;*
2. *G is contained in a Borel subgroup of $\mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$;*
3. *G is contained in the normalizer of a split Cartan subgroup of $\mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$;*
4. *G is contained in the normalizer of a non-split Cartan subgroup of $\mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$;*
5. *G is contained in one of a finite list of "exceptional" subgroups.*

Question 1.1 is best phrased and studied within the context of Galois representations. Fix an integer $n \geqslant 2$, and fix a $\mathbb{Z}/n\mathbb{Z}$-basis of $E[n]$. The absolute Galois group of $\mathbb{Q}$ acts on $E[n]$ and induces a Galois representation $\rho_{E,n}\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[n]) \simeq \mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z})$, such that $\mathrm{Ker}(\rho_{E,n}) = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(E[n]))$. Let us denote $\kappa_n = \mathrm{Ker}(\rho_{E,n})$ and $G_n = \Im(\rho_{E,n}) \subseteq \mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z})$. Then, part (1) of Question 1.1 asks when is it possible that $\kappa_m = \kappa_n$ for distinct integers $m, n \geqslant 2$. Theorem 1.4 studies elliptic curves with $\kappa_{p^n} = \kappa_{p^{n+1}}$ or, equivalently, curves E such that $G_{p^{n+1}}$ is isomorphic to G_{p^n}. If we denote the reduction mod p^n map by $\pi_{p^n}\colon \mathrm{GL}(2, \mathbb{Z}/p^{n+1}\mathbb{Z}) \to \mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$ and $Z_{p^n} = \mathrm{Ker}(\pi_{p^n})$, then we are trying to find elliptic curves such that $G_{p^{n+1}} \cap Z_{p^n}$ is trivial.

Example 2.7. — Let us look at Example 1.3 from the point of view of Galois representations. Let $E\colon y^2 = x^3 + 13x - 34$ and let $E(\mathbb{Q}(i))_{\mathrm{tors}} = E[4] = \langle P, Q\rangle$ where $P = (7, -20)$ and $Q = (-3 - 10i, 30 + 10i)$. Then, $\overline{Q} = (-3 + 10i, 30 - 10i) = P + 3Q$. In particular, if we write $\rho_{E,4}$ with respect to the basis $\{P, Q\}$ of $E[4]$, then the image G_4 is

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 3 \end{pmatrix} \right\} \subseteq \mathrm{GL}(2, \mathbb{Z}/4\mathbb{Z}),$$

while $Z_2 = \mathrm{Id} + 2 \cdot M(2, \mathbb{Z}/4\mathbb{Z})$, where $M(2, \mathbb{Z}/4\mathbb{Z})$ are the 2×2 matrices with coordinates in $\mathbb{Z}/4\mathbb{Z}$. Hence, $Z_2 \cap G_4$ is trivial, as claimed, and $\mathrm{Gal}(\mathbb{Q}(E[4])/\mathbb{Q}) \simeq G_4 \simeq G_2 \simeq \mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q})$. Since $\mathbb{Q}(E[2]) \subseteq \mathbb{Q}(E[4])$ we conclude that the 2-nd and 4-th division fields are actually equal.

From the point of view of representations and kernels of reduction maps, our Theorem 1.4 is at the opposite side of the spectrum from the following theorem of Dokchitser, Dokchitser, and Elkies, which determines when $Z_{p^n} \subseteq G_{p^{n+1}}$.

THEOREM 2.8 (Dokchitser, Dokchitser [10], Elkies [12], Serre [21]). — *Let $E/\mathbb{Q}$ be an elliptic curve, let p be a prime, and let $n \geqslant 1$. If ρ_{E,p^n} is surjective, then $\rho_{E,p^{n+1}}$ is surjective, unless $p^n = 2$, 3, or 4. Moreover, the j-invariants of elliptic curves where ρ_{E,p^n} is surjective but $\rho_{E,p^{n+1}}$ is not, are given explicitly by 1-parameter families.*

Indeed, for $n \geqslant 1$ we have $G_{p^n} = \mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$ and $Z_{p^n} \subseteq G_{p^{n+1}}$ if and only if $G_{p^{n+1}} = \mathrm{GL}(2, \mathbb{Z}/p^{n+1}\mathbb{Z})$, because the reduction map π_{p^n} is surjective. Thus, Theorem 2.8 shows that if $\pi_{p^n}(G_{p^{n+1}}) = G_{p^n}$ and $Z_{p^n} \cap G_{p^{n+1}} \neq Z_{p^n}$, then $p^n = 2$, 3, or 4. The fact that the surjectivity of ρ_{E,p^n} implies $\rho_{E,p^{n+1}}$ for $p \geqslant 5$ and $n \geqslant 1$ was known by work of Serre (*cf.* [23, IV-23, Lemma 3]).

3. Coincidences in towers

The goal of this section is to prove Theorem 1.4. In other words, this section is concerned with the possibility of an equality $\mathbb{Q}(E[p^n]) = \mathbb{Q}(E[p^{n+1}])$ for some prime p and $n \geqslant 1$. In the spirit of Question 1.1, we are also interested in whether $\mathbb{Q}(E[p^n]) \cap \mathbb{Q}(\zeta_{p^{n+1}})$ can be larger than $\mathbb{Q}(\zeta_{p^n})$. We answer these questions first for odd primes, and then we shall turn our attention to the case of $p = 2$.

3.1. The Case $p \geqslant 3$

The goal of this section is to prove the case of Theorem 1.4 when p is an odd prime. In fact, we would like to prove that $\mathbb{Q}(E[p^n]) \cap \mathbb{Q}(\zeta_{p^{n+1}}) = \mathbb{Q}(\zeta_{p^n})$.

PROPOSITION 3.1. — *Let $E/\mathbb{Q}$ an elliptic curve and $p \geqslant 3$ be a prime. Then, for every $n \in \mathbb{N}$, the field $\mathbb{Q}(E[p^n])$ does not contain the p^{n+1}-th roots of unity.*

As a corollary, we obtain:

THEOREM 3.2. — *Let $E/\mathbb{Q}$ be an elliptic curve and $p \geqslant 3$ a prime. Then, for every $n \in \mathbb{N}$, we have that $\mathbb{Q}(E[p^n]) \neq \mathbb{Q}(E[p^{n+1}])$.*

Proof. — Suppose that $\mathbb{Q}(E[p^n]) = \mathbb{Q}(E[p^{n+1}])$ for some $p \geqslant 3$ and $n \geqslant 1$. Then, $\mathbb{Q}(\mu_{p^{n+1}}) \subseteq \mathbb{Q}(E[p^{n+1}]) = \mathbb{Q}(E[p^n])$ by Prop. 2.4, which contradicts the conclusion of Prop. 3.1. □

In order to show Proposition 3.1, we will need two lemmas about the elements of $\mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$ with p-power order and a lemma about element with order divisible by $\varphi(p^n)$.

LEMMA 3.3. — *If p is a prime and $A \in \mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$ such that the order of A is p^k for some $k \in \mathbb{N}$, then $1 \leqslant k \leqslant n$ and all such orders occur.*

Proof. — We start by noticing that the matrix $\left(\begin{smallmatrix} 1 & p^{n-k} \\ 0 & 1 \end{smallmatrix}\right)$ has order p^k and so $\mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$ has an element of order p^k for every $1 \leqslant k \leqslant n$. To prove that there are no elements of higher order, we proceed by induction on n. The case of $n = 1$ follows from Lagrange's theorem and the fact that $\#\,\mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z}) = p(p-1)(p^2-1)$.

Next, we assume that the lemma is true for $n = \ell$ and let

$$A \in \mathrm{GL}(2, \mathbb{Z}/p^{\ell+1}\mathbb{Z})$$

such that A has order p^k for some $k \in \mathbb{N}$. We aim to show that $A^{p^{\ell+1}}$ is the identity and so the order of A divides $p^{\ell+1}$. Since $A^{p^k} = \mathrm{Id}$, it follows that $A^{p^k} \equiv \mathrm{Id} \bmod p^\ell$ and, by the induction hypothesis, the order of $A \bmod p^\ell$ must be $p^{k'}$ with $1 \leqslant k' \leqslant \ell$. Thus, we have $A^{p^\ell} \equiv \mathrm{Id} \bmod p^\ell$, and so we may write $A^{p^\ell} = \left(\begin{smallmatrix} 1+ap^\ell & bp^\ell \\ cp^\ell & 1+dp^\ell \end{smallmatrix}\right)$ for some $a, b, c, d \in \{0, 1, \ldots, p-1\}$. By induction on m one can show that

$$(A^{p^\ell})^m = \begin{pmatrix} 1 + map^\ell & mbp^\ell \\ mcp^\ell & 1 + mdp^\ell \end{pmatrix} \in \mathrm{GL}(2, \mathbb{Z}/p^{\ell+1}\mathbb{Z})$$

and so $A^{p^{\ell+1}} \equiv (A^{p^\ell})^p \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \bmod p^{\ell+1}$. Thus, the order of A divides $p^{\ell+1}$, which completes the induction step, and we conclude the proof. □

LEMMA 3.4. — *Let p be a prime, $n \in \mathbb{N}$, and let $\pi_{p,n} \colon \mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z}) \to \mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$ be the natural reduction modulo p map. Then, the elements in $\ker \pi_{p,n}$ have order dividing p^{n-1}.*

Proof. — Again, we proceed by induction on n. The case of $n = 1$ follows from the fact that $\pi_{p,1}$ is the identity map and the only element in the kernel is the identity which has order $1 = p^0 = p^{n-1}$.

Next, assume that the result is true for some $k \in \mathbb{N}$. Let $A \in \ker \pi_{p,k+1}$ and let $\overline{A}$ be the image of A under the reduction map $\mathrm{GL}(2, \mathbb{Z}/p^{k+1}\mathbb{Z}) \to \mathrm{GL}(2, \mathbb{Z}/p^k\mathbb{Z})$. Then, by assumption, we know that

$$\overline{A}^{p^{k-1}} = \mathrm{Id} \in \mathrm{GL}(2, \mathbb{Z}/p^k\mathbb{Z}),$$

thus

$$A^{p^{k-1}} = \begin{pmatrix} 1+p^k a & p^k b \\ p^k c & 1+p^k d \end{pmatrix},$$

for some $a, b, c, d \in \mathbb{Z}/p^k\mathbb{Z}$. Again by induction on m,

$$\left(A^{p^{k-1}}\right)^m = \begin{pmatrix} 1+mp^k a & mp^k b \\ mp^k c & 1+mp^k d \end{pmatrix},$$

and, in particular, $A^{p^k} = \left(A^{p^{k-1}}\right)^p = \mathrm{Id} \in \mathrm{GL}(2, \mathbb{Z}/p^{k+1}\mathbb{Z})$. This finishes the proof. □

Lemma 3.5. — *If $A_n \in \mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$ is a matrix with order divisible by $\varphi(p^{n+1}) = p^n(p-1)$, then $\det(A_n)$ is a square modulo p.*

Proof. — We start by writing $\mathrm{ord}(A_n) = p^n(p-1)k$, for some $k \geqslant 1$. From Lemma 3.3, we know that are no elements of order p^{n+1} in $\mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$ and so p cannot divide k. Thus $\gcd(p^n, (p-1)k) = 1$ and there exist integers x and y such that $1 = x(p-1)k + yp^n$. Letting $B_n = A_n^{x(p-1)k}$ and $C_n = A_n^{yp^n}$, we have that B_n and C_n have order p^n and $(p-1)k$, respectively, and $A_n = A_n^{x(p-1)k+yp^n} = A_n^{x(p-1)k} A_n^{yp^n} = B_n C_n$. Moreover $A_n = B_n C_n = C_n B_n$, since B_n and C_n are both powers of A_n.

Next, let $\pi_{p,n}$ be as in the statement of Lemma 3.4, $B_1 = \pi_{p,n}(B_n)$ and $C_1 = \pi_{p,n}(C_n)$. Since the $\#\,\mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z}) = p(p-1)^2(p+1)$ and the order of B_n is p^n, we know that $\mathrm{ord}(B_1)$ divides p. However, any element in $\mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$ of order dividing p is conjugate to a matrix in the subgroup

$$H = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in \mathbb{Z}/p\mathbb{Z} \right\}.$$

Since conjugation doesn't change the determinant of A_n, we can assume without loss of generality that B_1 is in H. Since B_n has order p^n, Lemma 3.4 gives that B_n does *not* belong to $\mathrm{Ker}(\pi_{p,n})$, and therefore B_1 is *not* the identity element of $\mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$.

Thus, $B_1 = \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)$ for some fixed $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ and since $B_n C_n = C_n B_n$ and π_n is a group homomorphism, we know that $B_1 C_1 = C_1 B_1$. Setting $C_1 = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ and using that B_1 and C_1 commute we have that

$$\alpha \equiv \alpha + \gamma a \bmod p,$$
$$\beta + \alpha a \equiv \beta + \delta a \bmod p.$$

Since $a \not\equiv 0 \bmod p$, it must be that $\gamma \equiv 0$ and $\alpha \equiv \delta \bmod p$. Thus, $C_1 = \left(\begin{smallmatrix} \alpha & \beta \\ 0 & \alpha \end{smallmatrix}\right)$. Finally, we have that $\det(A_1) = \det(B_1)\det(C_1) \equiv \alpha^2$ and $\det(A_n) \equiv \det(A_1) \equiv \alpha^2 \bmod p$, as desired. □

We are now ready to prove Proposition 3.1.

Proof of Proposition 3.1. — Suppose towards a contradiction that there is an elliptic curve $E/\mathbb{Q}$, a prime $p \geqslant 3$, and $n \in \mathbb{N}$ such that $\mathbb{Q}(\mu_{p^{n+1}}) \subseteq \mathbb{Q}(E[p^n])$. Let $\zeta_{p^{n+1}}$ be a fixed primitive p^{n+1}-th root of unity, $\zeta_{p^n} = \zeta_{p^{n+1}}^p$ be the corresponding primitive p^n-th root of unity and let $\sigma \in G_{\mathbb{Q}}$ be any element such that $\sigma\big|_{\mathbb{Q}(\zeta_{p^{n+1}})}$ generates $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q})$. Further, let $A_n = \rho_{E,p^n}(\sigma)$.

By Corollary 2.5, if $\mathbb{Q}(\zeta_{p^{n+1}}) \subseteq \mathbb{Q}(E[p^n])$, then the order of $A_n = \rho_{E,p^n}(\sigma) \in \mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$ is divisible by $\varphi(p^{n+1})$. However, recall that we assumed that σ restricted to $\mathbb{Q}(\zeta_{p^{n+1}})$ generates the full group Galois group of $\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q}$ and so σ restricted to $\mathbb{Q}(\zeta_{p^n})$ generates $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q})$. Therefore, $\det(\rho_{E,p^n}(\sigma)) = \det(A_n)$ must be a generator of $(\mathbb{Z}/p^n\mathbb{Z})^\times$. But from Lemma 3.5, we know that $\det(A_n)$ is a square mod p. Thus, we have reached a contradiction as a quadratic residue cannot be a generator for $p \geqslant 3$, and the proof is complete. □

3.2. The case $p = 2$, without CM

In this subsection we continue the proof of Theorem 1.4 by studying when $\mathbb{Q}(E[2^{n+1}]) = \mathbb{Q}(E[2^n])$ for some $n \geqslant 1$. We shall consider two cases, according to whether $E/\mathbb{Q}$ has complex multiplication. In this section, we consider the non-CM case.

In the non-CM case, the work of Rouse and Zureick-Brown (Theorem 2.2) reduces the proof of Theorem 1.4 in the case of $p = 2$ to a finite computation. Indeed, by Theorem 2.2, if $E/\mathbb{Q}$ is an elliptic curve with no CM, there are 1208 possible images for $\rho_{E,2^\infty}$, each one defined at most modulo 32 (i.e., $\Im\rho_{E,2^\infty}$ is always the full inverse image of $\Im\rho_{E,2^5}$ under the reduction map $\mathrm{GL}(2, \mathbb{Z}_2) \to \mathrm{GL}(2, \mathbb{Z}/32\mathbb{Z})$). An immediate consequence of this fact is that if $n \geqslant 5$, then we cannot have $\Im\rho_{E,2^{n+1}} \simeq \Im\rho_{E,2^n}$, and therefore $\mathrm{Gal}(\mathbb{Q}(E[2^{n+1}])/\mathbb{Q})$ is not isomorphic to $\mathrm{Gal}(\mathbb{Q}(E[2^n])/\mathbb{Q})$. In particular, if $\mathbb{Q}(E[2^{n+1}]) = \mathbb{Q}(E[2^n])$ we must have $n < 5$. The database [20] provides generators of a subgroup $G_5 \subseteq \mathrm{GL}(2, \mathbb{Z}/32\mathbb{Z})$ for each of the 1208 possible images. If we let G_k be the image of G_5 in $\mathrm{GL}(2, \mathbb{Z}/2^k\mathbb{Z})$, for $1 \leqslant k \leqslant 5$, then we have carried out an exhaustive search of the possible 2-adic images for examples where $G_{n+1} \simeq G_n$, for some $1 \leqslant n \leqslant 4$, so that $\mathbb{Q}(E[2^{n+1}]) = \mathbb{Q}(E[2^n])$. There are precisely two types of images with this property, namely `X20b` and `X60d` (in the notation of [20]) and in both cases we had $G_2 \simeq G_1$, i.e., $\mathbb{Q}(E[4]) = \mathbb{Q}(E[2])$. They differ, however, in the fact

that $G_2 \simeq \mathbb{Z}/2\mathbb{Z}$ for $\mathtt{X_{20b}}$ while $G_2 \simeq S_3$ for $\mathtt{X_{60d}}$. Our search, thus, yields the following result.

PROPOSITION 3.6. — *Let $E/\mathbb{Q}$ be an elliptic curve without CM, such that $\mathbb{Q}(E[2^{n+1}]) = \mathbb{Q}(E[2^n])$ for some $n \geqslant 1$. Then $n = 1$, and there is a $t \in \mathbb{Q}$ such that E is $\mathbb{Q}$-isomorphic over $\mathbb{Q}$ to an elliptic curve of the form $E' \colon y^2 = x^3 + A(t)x + B(t)$, where*

$$\begin{aligned} A(t) = {} & -27t^8 + 648t^7 - 4212t^6 - 2376t^5 + 60102t^4 + 79704t^3 \\ & - 105732t^2 - 235224t - 107811, \\ B(t) = {} & 54t^{12} - 1944t^{11} + 24300t^{10} - 97848t^9 - 251262t^8 + 1722384t^7 \\ & + 4821768t^6 - 8697456t^5 - 64323558t^4 - 140447736t^3 \\ & - 157012020t^2 - 90561240t - 21346578. \end{aligned}$$

Remark 3.7. — We point out here that, in fact, the family in Proposition 3.6 contains the family in Theorem 1.8. The family in Theorem 1.8 corresponds to elliptic curves with $\mathbb{Q}(E[2]) = \mathbb{Q}(E[4]) = \mathbb{Q}(i)$, while the family above corresponds to elliptic curves with $\mathbb{Q}(E[2]) = \mathbb{Q}(E[4])$ an S_3 extension of $\mathbb{Q}$, with $\mathbb{Q}(i)$ the unique quadratic subfield. These two curves correspond to $\mathtt{X_{20b}}$ and $\mathtt{X_{60d}}$, in the notation of [20], and the map between these curves can be computed from the information there.

The curves in Proposition 3.6 all have $\Im\rho_{E,4}$ conjugate to a subgroup of

$$G = \left\langle \begin{pmatrix} 1 & 0 \\ 3 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 3 \\ 1 & 0 \end{pmatrix} \right\rangle \subseteq \mathrm{GL}(2, \mathbb{Z}/4\mathbb{Z}),$$

while the curves in Theorem 1.8 have $\Im\rho_{E,4}$ conjugate to[(1)]

$$H = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 3 \end{pmatrix} \right\rangle.$$

Since H is conjugate to a subgroup of G, curves with images in H arise as points on the modular curve X_G.

Example 3.8. — Let $E/\mathbb{Q}$ be the elliptic curve with Cremona label `162d1` which is given by Weierstrass equation $y^2 + xy + y = x^3 - x^2 + 4x - 1$. Using Magma [2] we see that, $E(\mathbb{Q})_{\mathrm{tors}}$ is trivial and that $\mathbb{Q}(E[2]) = \mathbb{Q}(E[4]) = \mathbb{Q}(\alpha)$ where α is a root of $f(x) = 256x^6 + 6624x^4 + 42849x^2 + 82944$.

(1) The image must actually be *equal* to H since $\#H = 2$ and $\mathbb{Q}(i) \subseteq \mathbb{Q}(E[4])$.

3.3. The case $p = 2$, with CM

In this subsection we complete the proof of Theorem 1.4 by studying when $\mathbb{Q}(E[2^{n+1}]) = \mathbb{Q}(E[2^n])$ for some $n \geqslant 1$, and $E/\mathbb{Q}$ has complex multiplication.

PROPOSITION 3.9. — *Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication, and let $n \geqslant 1$. Then $\mathbb{Q}(E[2^n]) \subsetneq \mathbb{Q}(E[2^{n+1}])$.*

Proof. — Suppose first that $E/\mathbb{Q}$ is an elliptic curve with complex multiplication, and $\mathbb{Q}(E[2]) = \mathbb{Q}(E[4])$. Then, the image G_4 of $\rho_{E,4}$ is a group such that its reduction G_2 modulo 2 satisfies $\#G_2 = \#G_4$. A Magma computation shows that any such group is a conjugate of a subgroup of

$$G = \left\langle \begin{pmatrix} 1 & 0 \\ 3 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 3 \\ 1 & 0 \end{pmatrix} \right\rangle \subseteq \mathrm{GL}(2, \mathbb{Z}/4\mathbb{Z}),$$

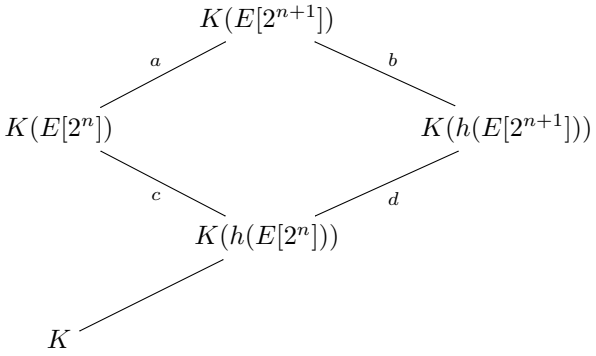
the group that already appeared in Remark 3.7. The modular curve X_G corresponds to X_{20b} (genus 0) in the notation of Rouse and Zureick-Brown, and they have computed the j-line $j\colon X_G \to \mathbb{P}^1$, which is given as follows:

$$j_G(t) = \frac{-4t^8 + 32t^7 + 80t^6 - 288t^5 - 504t^4 + 864t^3 + 1296t^2 - 864t - 1188}{t^4 + 4t^3 + 6t^2 + 4t + 1}.$$

In order to rule out elliptic curves with CM that have an image of $\rho_{E,4}$ that is a conjugate of a subgroup of G, it suffices to show that if j_0 is a rational CM j-invariant, then j_0 is not a value of $j_G(t)$ for some rational value of t. There are precisely 13 such rational CM j-invariants, namely 0, 54000, -12288000, 1728, 287496, -3375, 16581375, 8000, -32768, -884736, -884736000, -147197952000, -262537412640768000, and one can check, one by one (again using Magma, for example) that $j_G(t) = j_0$ is impossible for rational values of t. Hence, $\mathbb{Q}(E[2]) = \mathbb{Q}(E[4])$ is impossible for elliptic curves over $\mathbb{Q}$ with CM.

It remains to show that $\mathbb{Q}(E[2^n]) = \mathbb{Q}(E[2^{n+1}])$ is impossible for $n > 1$ in the CM case. Suppose, for a contradiction, that $E/\mathbb{Q}$ is an elliptic curve with CM by an imaginary quadratic field K and suppose that $\mathbb{Q}(E[2^n]) = \mathbb{Q}(E[2^{n+1}])$ for some $n > 1$. In particular, since $j(E) \in \mathbb{Q}$, we have that $K(j(E)) = K$, and $K(E[2^n]) = K(E[2^{n+1}])$. In this proof, we will argue in

terms of the following diagram:



where h is a Weber function for E (see [18, Definition 2.4]). Our initial assumption is that $a = 1$. Theorem 4.4 of [18] shows that, for any $n \geqslant 2$, we have $d = [H_f(h(E[2^{n+1}])) : H_f(h(E[2^n]))] = 2^2$, where $H_f = K(j(E)) = K$ in this case. Hence, $c = [K(E[2^n]) : K(h(E[2^n]))]$ must be divisible by 4. Theorem 4.1 of [18] shows that c is a divisor of $\#\mathcal{O}_{K,f}^{\times}$, where E has CM by the order $\mathcal{O}_{K,f}$ of K. Since $\#\mathcal{O}_{K,f}^{\times}$ is always a divisor of 4 or 6, we must have $\#\mathcal{O}_{K,f}^{\times} = 4$ and therefore $\mathcal{O}_{K,f} = \mathbb{Z}[i]$ and $K = \mathbb{Q}(i)$, and $j(E) = 1728$. The finite list of possible 2-adic images for elliptic curves over $\mathbb{Q}$ with CM and $j = 1728$ are described in Theorem 1.7 of [18], and one can verify that, in all cases, $[\mathbb{Q}(E[8]) : \mathbb{Q}(E[4])] = 2$ or 4, and $[\mathbb{Q}(E[2^{n+1}]) : \mathbb{Q}(E[2^n])] = 4$ for all $n \geqslant 3$. Hence, this shows that $\mathbb{Q}(E[2^n]) \neq \mathbb{Q}(E[2^{n+1}])$ for any $n \geqslant 1$ and any CM elliptic curve over $\mathbb{Q}$. □

Together, Propositions 3.2, 3.6, and 3.9 imply Theorem 1.4.

We finish this section discussing the possibility of 2^{n+1}-th roots of unity in the 2^n-th division field of an elliptic curve. For example, the elliptic curve $E : y^2 = x^3 + x$ satisfies $\mathbb{Q}(E[2]) = \mathbb{Q}(\zeta_4)$, and the curve $E : y^2 = x^3 + 2x$ satisfies $\mathbb{Q}(\zeta_8) \subseteq \mathbb{Q}(E[4])$. Next, we show that the elliptic curve $y^2 = x^3 - 11x - 14$, with Cremona label `32a3`, satisfies that the 2^n-th division field contains the 2^{n+1}-roots of unity.

THEOREM 3.10. — *Let $E/\mathbb{Q}$ be the elliptic curve $y^2 = x^3 - 11x - 14$ (i.e. the curve with Cremona label `32a3`). Then, $\mathbb{Q}(\zeta_{2^{n+1}}) \subseteq \mathbb{Q}(E[2^n])$ for all $n > 1$.*

Proof. — Let $E/\mathbb{Q}$ be the elliptic curve $y^2 = x^3 - 11x - 14$. In [18, Example 9.4], it is shown that the 2-adic image of $E/\mathbb{Q}$ is given by

$$G = \left\langle A = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix}, C = \begin{pmatrix} -1 & -1 \\ 4 & -1 \end{pmatrix} \right\rangle \subseteq \mathrm{GL}(2, \mathbb{Z}_2).$$

Note that the generators of G are subject to the following relations:

$$BC = CB,\ AB = BA,\ ACA = BC^{-1}.$$

Further, $B^{2^{n-2}} \equiv C^{2^n} \equiv \mathrm{Id} \bmod 2^n$. It follows that $D = ACAC^{-1} = BC^{-2}$ satisfies

$$D^{2^{n-1}} \equiv B^{2^{n-1}} C^{-2^n} \equiv 1 \bmod 2^n.$$

Moreover, $G/\langle D\rangle$ is abelian. It follows that $G/\langle D\rangle \bmod 2^n$ is abelian, of size

$$\frac{|G \bmod 2^n|}{|\langle D\rangle \bmod 2^n|} = \frac{2 \cdot 2^{n-2} \cdot 2^n}{2^{n-1}} = 2^n.$$

Moreover, $D^{2^{n-2}} \equiv B^{2^{n-2}} C^{-2^{n-1}} \equiv C^{-2^{n-1}} \bmod 2^n$. Thus, $C^{2^{n-1}} \equiv \mathrm{Id} \bmod (2^n, \langle D\rangle)$. It follows that $\langle A, C\rangle/\langle D\rangle$ is of size 2^n, and therefore A and C span all of $G/\langle D\rangle$. Hence, $G/\langle D\rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-1}\mathbb{Z}$. We conclude that there is an abelian extension $F_n/\mathbb{Q}$, with $F_n \subseteq \mathbb{Q}(E[2^n])$, such that its Galois group is given by $\mathrm{Gal}(F_n/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-1}\mathbb{Z}$.

Now, notice that the conductor of $E/\mathbb{Q}$ is 32, and therefore, by the criterion of Néron–Ogg–Shafarevich, the extension $\mathbb{Q}(E[2^n])/\mathbb{Q}$ (and therefore $F_n/\mathbb{Q}$) is only ramified above 2. In particular, $F_n/\mathbb{Q}$ is an abelian extension of $\mathbb{Q}$ that is only ramified above 2, and we conclude that $F_n \subseteq \mathbb{Q}(\zeta_{2^\infty})$. Further, $\mathrm{Gal}(\mathbb{Q}(\zeta_{2^\infty})/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2$, and $n > 1$, and so there exists a unique extension $F_n \subseteq \mathbb{Q}(\zeta_{2^\infty})$ such that $\mathrm{Gal}(F_n/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-1}\mathbb{Z}$, namely $F_n = \mathbb{Q}(\zeta_{2^{n+1}})$.

Hence, $F_n = \mathbb{Q}(\zeta_{2^{n+1}}) \subseteq \mathbb{Q}(E[2^n])$ for $n > 1$, as we claimed. □

4. The Abelian Case

In this section we prove Theorem 1.8. We shall rely on the classification of abelian division fields given in [13]. We cite here the main result of that paper for reference:

THEOREM 4.1 ([13, Theorem 1.1]). — *Let $E/\mathbb{Q}$ be an elliptic curve. If there is an integer $n \geqslant 2$ such that $\mathbb{Q}(E[n]) = \mathbb{Q}(\zeta_n)$, then $n = 2, 3, 4$, or 5. More generally, if $\mathbb{Q}(E[n])/\mathbb{Q}$ is abelian, then $n = 2, 3, 4, 5, 6$, or 8. Moreover, $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ is isomorphic to one of the following groups:*

n	2	3	4	5	6	8
$\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$	$\{0\}$ $\mathbb{Z}/2\mathbb{Z}$ $\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$ $(\mathbb{Z}/2\mathbb{Z})^2$	$\mathbb{Z}/2\mathbb{Z}$ $(\mathbb{Z}/2\mathbb{Z})^2$ $(\mathbb{Z}/2\mathbb{Z})^3$ $(\mathbb{Z}/2\mathbb{Z})^4$	$\mathbb{Z}/4\mathbb{Z}$ $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ $(\mathbb{Z}/4\mathbb{Z})^2$	$(\mathbb{Z}/2\mathbb{Z})^2$ $(\mathbb{Z}/2\mathbb{Z})^3$	$(\mathbb{Z}/2\mathbb{Z})^4$ $(\mathbb{Z}/2\mathbb{Z})^5$ $(\mathbb{Z}/2\mathbb{Z})^6$

Furthermore, each possible Galois group occurs for infinitely many distinct j-invariants.

We are ready to present the proof of Theorem 1.8.

Proof of Theorem 1.8. — Suppose first that p and q are distinct primes, with $\mathbb{Q}(E[p])$ abelian, and $\mathbb{Q}(E[p]) \cap \mathbb{Q}(\zeta_{q^k})$ non-trivial, for some $k \geqslant 1$. By Theorem 4.1, we have $p = 2, 3$, or 5. So we distinguish three cases depending on the value of p:

(1) If $p = 2$, then $\mathbb{Q}(E[2])$ is either trivial, quadratic, or cyclic cubic. For any prime q, the curve $y^2 = x^3 + (-1)^{(q-1)/2}qx$ shows that $\mathbb{Q}(E[2]) \cap \mathbb{Q}(\zeta_{q^k})$ can be quadratic. Similarly, if $\mathbb{Q}(\zeta_{q^k})$ contains a cyclic cubic extension (i.e., if 3 divides $(q-1)q$) given by a cubic polynomial $f(x)$, then the curve $y^2 = f(x)$ shows that $\mathbb{Q}(E[2]) \cap \mathbb{Q}(\zeta_{q^k})$ can be a cyclic cubic.

(2) If $p = 3$, the existence of the Weil pairing forces $\mathbb{Q}(\zeta_3) \subseteq \mathbb{Q}(E[3])$. Then, by Theorem 4.1, the field $\mathbb{Q}(E[3])$ is either quadratic, in which case $\mathbb{Q}(E[3]) = \mathbb{Q}(\sqrt{-3})$, or is quartic with Galois group $(\mathbb{Z}/2\mathbb{Z})^2$, so that $\mathbb{Q}(E[3])$ is the compositum of $\mathbb{Q}(\sqrt{-3})$ with another quadratic field K over $\mathbb{Q}$. Thus, $\mathbb{Q}(E[3]) \cap \mathbb{Q}(\zeta_{q^k})$ is at most quadratic.

(3) If $p = 5$, then $\mathbb{Q}(\zeta_5) \subseteq \mathbb{Q}(E[5])$, and $\mathrm{Gal}(\mathbb{Q}(E[5])/\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$, or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, or $(\mathbb{Z}/4\mathbb{Z})^2$. Thus, $\mathbb{Q}(E[5]) \cap \mathbb{Q}(\zeta_{q^k})$ is either quadratic of a cyclic quartic. As an example of the latter, consider $E : y^2 = x^3 - x^2 - 4319x + 100435$. Here $\mathrm{Gal}(\mathbb{Q}(E[5])/\mathbb{Q}) \simeq (\mathbb{Z}/4\mathbb{Z})^2$ and one of the points of order 5 is defined over a cyclic quartic field F defined by $x^4 + 4x^2 + 2 = 0$. This extension has discriminant 2048, and $F \subseteq \mathbb{Q}(\zeta_{16})$. Hence, $\mathbb{Q}(E[5]) = F(\zeta_5)$, and $\mathbb{Q}(E[5]) \cap \mathbb{Q}(\zeta_{16}) = F$, a quartic field.

Thus, in all cases $\mathbb{Q}(E[p]) \cap \mathbb{Q}(\zeta_{q^k})$ is trivial, quadratic, cyclic cubic, or cyclic quartic.

It remains to consider when a full coincidence $\mathbb{Q}(E[n]) = \mathbb{Q}(E[m])$ can occur. Suppose such a coincidence does occur. Then, in particular, $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \simeq \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$. Using the classification of abelian division fields in Theorem 4.1, it follows that

$$(m, n) \in \{(2,3), (2,4), (3,4), (3,6), (4,6), (4,8)\}.$$

By our results in Section 3, $\mathbb{Q}(E[4]) = \mathbb{Q}(E[8])$ cannot happen, and the case of $\mathbb{Q}(E[2]) = \mathbb{Q}(E[4])$ in the abelian case corresponds to the curve $\mathtt{X_{60d}}$ of [20], which is parametrized as in the statement of the theorem (see also Remark 3.7).

The case of $(m,n)=(2,3)$ can be eliminated by seeing that in this case we would have $\mathbb{Q}(E[2])=\mathbb{Q}(E[3])=\mathbb{Q}(E[6])$. Thus, $\mathrm{Gal}(\mathbb{Q}(E[6])/\mathbb{Q})\cong \mathrm{Gal}(\mathbb{Q}(E[3])/\mathbb{Q})\cong \mathrm{Gal}(\mathbb{Q}(E[2]))$ but this is impossible according to the table in Theorem 4.1. Similarly, if $\mathbb{Q}(E[3])=\mathbb{Q}(E[4])$ or if $\mathbb{Q}(E[4])=\mathbb{Q}(E[6])$ are abelian extensions of $\mathbb{Q}$, then $\mathbb{Q}(E[12])=\mathbb{Q}(E[3])\mathbb{Q}(E[4])=\mathbb{Q}(E[6])\mathbb{Q}(E[4])$ would be abelian, but this contradicts Theorem 4.1, which shows that $\mathbb{Q}(E[12])/\mathbb{Q}$ is never an abelian extension.

Thus, it remains to consider the case of $\mathbb{Q}(E[3])=\mathbb{Q}(E[6])$. Since we have shown that $\mathbb{Q}(E[2])=\mathbb{Q}([3])$ cannot occur, we restrict our attention to the case of $\mathbb{Q}(E[2])\subsetneq\mathbb{Q}(E[3])=\mathbb{Q}(E[6])$. In particular, by Theorem 4.1, the extension $\mathbb{Q}(E[2])/\mathbb{Q}$ must be trivial or quadratic, and $\mathbb{Q}(E[6])=\mathbb{Q}(E[3])/\mathbb{Q}$ must be biquadratic. By the results of Section 6.2 of [13], if $\mathbb{Q}(E[3])$ is abelian, then the image of $\rho_{E,3}$ is contained in a split Cartan subgroup of $\mathrm{GL}(2,\mathbb{Z}/3\mathbb{Z})$ and, in particular, $E/\mathbb{Q}$ has two independent 3-isogenies. Moreover, if $\mathbb{Q}(E[2])/\mathbb{Q}$ is trivial or quadratic, then $E/\mathbb{Q}$ has at least one 2-torsion point defined over $\mathbb{Q}$. Notice that if $\mathbb{Q}(E[2])=\mathbb{Q}$, then all 2-torsion points would be $\mathbb{Q}$-rational, and in particular, E would have three distinct 2-isogenies. However, no such isogeny graph can occur for elliptic curves defined over $\mathbb{Q}$ (indeed, it would contradict a theorem of Kenku ([4, Theorem 4.3]) that says that there are at most 8 isogenous curves in a $\mathbb{Q}$-isogeny class; see [4], Tables 1-4, which shows the only possibility in this case is a graph of type R_6). Hence, we must have that $\mathbb{Q}(E[2])/\mathbb{Q}$ is quadratic. Since $\mathbb{Q}(\sqrt{\Delta_E})$ is the unique quadratic (or trivial) extension contained in $\mathbb{Q}(E[2])$ (see [1]), it follows that $\mathbb{Q}(E[2])=\mathbb{Q}(\sqrt{\Delta_E})$. Since $\mathbb{Q}(E[3])/\mathbb{Q}$ is biquadratic and contains ζ_3, it follows that $\mathbb{Q}(E[3])=\mathbb{Q}(\sqrt{-3},\sqrt{\Delta_E})$.

Conversely, if $E/\mathbb{Q}$ is an elliptic curve with one 2-torsion point defined over $\mathbb{Q}$, and $\Im\rho_{E,3}$ is contained in the split Cartan subgroup of $\mathrm{GL}(2,\mathbb{Z}/3\mathbb{Z})$, then we can find a quadratic twist E' of E such that $\mathbb{Q}(E'[3])=\mathbb{Q}(\sqrt{-3})$, and then a quadratic twist E'' of E' by $\Delta_{E'}$ (also a twist of E), such that $\mathbb{Q}(E''[3])=\mathbb{Q}(\sqrt{-3},\sqrt{\Delta_{E'}})$. Note that Δ_E, $\Delta_{E'}$, and $\Delta_{E''}$ differ by 6-th powers, because the curves are quadratic twists of each other, and so $\mathbb{Q}(\sqrt{\Delta_E})=\mathbb{Q}(\sqrt{\Delta_{E'}})=\mathbb{Q}(\sqrt{\Delta_{E''}})$, and $j(E'')=j(E')=j(E)$. Hence

$$\mathbb{Q}(E''[2])=\mathbb{Q}(\sqrt{\Delta_{E''}})\subsetneq\mathbb{Q}(\sqrt{-3},\sqrt{\Delta_{E''}})=\mathbb{Q}(E''[3])=\mathbb{Q}(E''[6]).$$

Thus, every elliptic curve $E/\mathbb{Q}$ with one 2-torsion point defined over $\mathbb{Q}$ and split Cartan mod 3 image has a twist E'' with the property $\mathbb{Q}(E''[2])\subsetneq\mathbb{Q}(E''[3])=\mathbb{Q}(E''[6])$, and viceversa, an elliptic curve E'' with such property has a 2-torsion point over $\mathbb{Q}$ and split Cartan image mod 3. Using Magma [2] we have computed the j-line of the modular curve that parametrizes elliptic curves with split Cartan image mod 3 and a 2-torsion

point over $\mathbb{Q}$, and it is given by

$$j(t) = -\left(\frac{(t^3-3t^2-9t-9)(t^3+3t^2+3t-3)(t^6+12t^5+81t^4+216t^3+243t^2+108t+27)}{t(t+1)^2(t+3)^2(t^2+3)^2(t^2+3t+3)}\right)^3.$$

Hence, we conclude that if E'' is an elliptic curve with

$$\mathbb{Q}(E''[2]) \subsetneq \mathbb{Q}(E''[3]) = \mathbb{Q}(E''[6]),$$

then there is some $t \in \mathbb{Q}$ such that $j(E'') = j(t)$ and, if $E/\mathbb{Q}$ is a curve with $j(E) = j(t)$ for some t, then there is an appropriate quadratic twist with the desired property. This concludes the proof of the theorem. □

Example 4.2. — We illustrate the case of $(n, m) = (3, 6)$ with an example, that is, we are looking for a curve E'' with $\mathbb{Q}(E''[2]) \subsetneq \mathbb{Q}(E''[3]) = \mathbb{Q}(E''[6])$. First, we evaluate the function $j(t)$ at $t = 1$ to obtain $j_1 = 9938375/21952$, and we find an elliptic curve E with $j(E) = j_1$, which is given by

$$E : y^2 + xy = x^3 + 5796284120487x - 9014728680220686983.$$

This curve satisfies $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z}$ and there are two independent 3-isogenies. Next, we compute the field of definition of one of the 3-isogenies: $K = \mathbb{Q}(\sqrt{1137565})$ (this can be accomplished using division polynomials), and find a twist E' of E by 1137565 which is given by:

$$E' : y^2 + xy + y = x^3 + 4x - 6.$$

The curve E' satisfies $E'(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/6\mathbb{Z}$ and $\Delta_{E'} = -2^6 7^3$. Finally, we find a twist E'' of E' by -7 which is given by

$$E'' : y^2 = x^3 + 284445x + 97999902.$$

The curve E'' satisfies $\mathbb{Q}(E''[2]) = \mathbb{Q}(\sqrt{-7})$ and $\mathbb{Q}(E''[3]) = \mathbb{Q}(E''[6]) = \mathbb{Q}(\sqrt{-3}, \sqrt{-7})$, as desired.

Remark 4.3. — It is worth pointing out that in [19, Theorem 8.7] Morrow gives an explicit parametrization of elliptic curves E and primes $p \geqslant 7$ such that $\mathbb{Q}(E[2]) \cap \mathbb{Q}(E[p^n])$ is a cyclic cubic field, for some $n \geqslant 1$.

5. Intersections of division fields and $\mathbb{Q}^{ab}$

In order to prove Theorem 1.7 we start by classifying the possible roots of unity in $\mathbb{Q}(E[p])$. First, we prove that the powers on the prime-to-p roots of unity cannot be very large compared to p.

PROPOSITION 5.1. — *Let $E/\mathbb{Q}$ be an elliptic curve, let $p < q$ be primes, let $n, m \geqslant 1$, and suppose $\mathbb{Q}(\zeta_{q^m}) \subseteq \mathbb{Q}(E[p^n])$. Then, $m = 1$ unless $p = 2$ and $q = 3$ in which case $m \leqslant 2$.*

Proof. — Suppose that $\mathbb{Q}(\zeta_{q^m}) \subseteq \mathbb{Q}(E[p^n])$, for some $m \geqslant 2$. Then, by Corollary 2.5, the order of $\mathrm{Gal}(\mathbb{Q}(E[p^n])/\mathbb{Q})$ is divisible by $\varphi(q^m)$, and therefore divisible by q. Since $\mathrm{Gal}(\mathbb{Q}(E[p^n])/\mathbb{Q})$ is a subgroup of $\mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$, it follows that $q^{m-1}(q-1)$ divides $p^{4(n-1)+1}(p-1)^2(p+1)$. Since $p \neq q$ are primes, we conclude that $p \equiv \pm 1 \bmod q^{m-1}$, and since $q > p$ we must have $p \equiv -1 \bmod q$ and therefore $p = q - 1$, and $m = 2$. This is only possible if $p = 2$ and $q = 3$. □

Before continuing to the proof of Theorem 1.7 we will need to better understand how large $K_E(p) = \mathbb{Q}(E[p]) \cap \mathbb{Q}^{ab}$ can be and what the structure of $\mathrm{Gal}(K_E(p)/\mathbb{Q})$ can be. The size of this field and the possible structure of its Galois group will depend on the image of $\rho_{E,p}$ and as such we will break this section down according to the maximal group that contains $\Im\rho_{E,p}$ (see Proposition 2.6).

5.1. Full Image

From the results of [11, 14] we know that this is in fact the generic case and it turns out to also be the simplest in our context.

PROPOSITION 5.2. — *Let $E/\mathbb{Q}$ be an elliptic curve, let $p, q > 2$ be distinct odd primes, let $n \geqslant 1$, and suppose ρ_{E,p^n} is surjective. Then, the intersection $\mathbb{Q}(\zeta_{q^m}) \cap \mathbb{Q}(E[p^n])$ is trivial.*

Proof. — Suppose that $\mathrm{Gal}(\mathbb{Q}(E[p^n])/\mathbb{Q}) \simeq \mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$. Then, if $p > 2$, the commutator subgroup of $\mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$ is $\mathrm{SL}(2, \mathbb{Z}/p^n\mathbb{Z})$ (see [23]), and therefore the largest abelian quotient of $\mathrm{Gal}(\mathbb{Q}(E[p^n])/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/p^n\mathbb{Z})^\times$. Since $\mathbb{Q}(\zeta_{p^n}) \subseteq \mathbb{Q}(E[p^n])$ by the Weil pairing, it follows that the largest abelian subextension of $L \subseteq \mathbb{Q}(E[p^n])$ is precisely $L = \mathbb{Q}(\zeta_{p^n})$. In particular, $\mathbb{Q}(\zeta_{q^m}) \cap \mathbb{Q}(E[p^n]) \subseteq L = \mathbb{Q}(\zeta_{p^n})$ and therefore, the intersection must be trivial, since $q \neq p$. □

COROLLARY 5.3. — *Let $E/\mathbb{Q}$ be an elliptic curve, $p > 2$ a prime, and $n \geqslant 1$. If ρ_{E,p^n} is surjective then $K_E(p) = \mathbb{Q}(E[p^n]) \cap \mathbb{Q}^{ab} = \mathbb{Q}(\zeta_{p^n})$. Further, in this case we have that $\mathrm{Gal}(K_E(P)/\mathbb{Q}) \simeq (\mathbb{Z}/p^n\mathbb{Z})^\times$.*

5.2. Borel Image

Definition 5.4. — *Let p be a prime, and $n \geqslant 1$. We say that a subgroup B of $\mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$ is Borel if every matrix in B is upper triangular, i.e.,*

$$B \subseteq \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{Z}/p^n\mathbb{Z},\ a, c \in (\mathbb{Z}/p^n\mathbb{Z})^\times \right\}.$$

We say that B is a non-diagonal Borel subgroup if none of the conjugates of B in $\mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$ is formed solely by diagonal matrices. If B is a Borel subgroup, we denote by B_1 the subgroup of B formed by those matrices in B whose diagonal coordinates are $1 \bmod p^n$, and we denote by B_d the subgroup of B formed by diagonal matrices, i.e.,

$$B_1 = B \cap \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{Z}/p^n\mathbb{Z} \right\},$$

and

$$B_d = B \cap \left\{ \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} : a, c \in (\mathbb{Z}/p^n\mathbb{Z})^\times \right\}.$$

Lemma 5.5. — *[17, Lemma 2.2] Let $p > 2$ be a prime, $n \geqslant 1$ and let $B \subseteq \mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$ be a Borel subgroup, such that B contains a matrix $g = \left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right)$ with $a \not\equiv c \bmod p$. Let $B' = h^{-1}Bh$ with $h = \left(\begin{smallmatrix} 1 & b/(c-a) \\ 0 & 1 \end{smallmatrix}\right)$. Then, $B' \subseteq \mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$ is a Borel subgroup conjugated to B satisfying the following properties:*

1. *$B' = B'_d B'_1$, i.e., for every $M \in B'$ there is $U \in B'_d$ and $V \in B'_1$ such that $M = UV$; and*
2. *$B/[B, B] \simeq B'/[B', B']$ and $[B', B'] = B'_1$.*

If follows that $[B, B] = B_1$ and it is a cyclic subgroup of order p^s for some $0 \leqslant s \leqslant n$.

Proposition 5.6. — *Let $E/\mathbb{Q}$ be an elliptic curve, let $p > 2$ be a prime, let $n \geqslant 1$, and suppose $\Im\rho_{E,p^n} \subseteq \mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$ is a Borel subgroup. Then, the Galois group of the maximal abelian subextension $L \subseteq \mathrm{Gal}(\mathbb{Q}(E[p^n])/\mathbb{Q})$ is a subgroup of $(\mathbb{Z}/p^n\mathbb{Z})^\times \times (\mathbb{Z}/p^n\mathbb{Z})^\times$, and L contains $\mathbb{Q}(\zeta_{p^n})$. In particular, if $q \neq p$ is another prime and $\mathbb{Q}(\zeta_{q^m}) \subseteq \mathbb{Q}(E[p^n])$ for some $m \geqslant 1$, then $\varphi(q^m)$ is a divisor of $\varphi(p^n)$. If in addition $q > p$, then $m = 1$ and $q - 1$ is a divisor of $\varphi(p^n)$.*

Proof. — Let $G = \mathrm{Gal}(\mathbb{Q}(E[p^n])/\mathbb{Q}) \simeq \Im\rho_{E,p^n} \subseteq \mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$, and suppose G is a Borel subgroup. Then, G contains a matrix g as in Lemma 5.5,

because otherwise $\det(G)$ would consist only of square classes, and therefore would not be all of $(\mathbb{Z}/p^n\mathbb{Z})^\times$. Thus, by Lemma 5.5, the commutator of G is G_1 and $G/G_1 \simeq G_d$. Thus, $\mathrm{Gal}(L/\mathbb{Q}) \simeq G/G_1$, where L is the maximal abelian subextension $L \subseteq \mathrm{Gal}(\mathbb{Q}(E[p^n])/\mathbb{Q})$, is isomorphic to a subgroup of $(\mathbb{Z}/p^n\mathbb{Z})^\times \times (\mathbb{Z}/p^n\mathbb{Z})^\times$, as desired.

Now, if $q \neq p$ is another prime and $\mathbb{Q}(\zeta_{q^m}) \subseteq \mathbb{Q}(E[p^n])$ for some $m \geqslant 1$, then the compositum $K = \mathbb{Q}(\zeta_{p^n})\mathbb{Q}(\zeta_{q^m})$ is contained in L. Since the primes are distinct, then $\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/p^n\mathbb{Z})^\times \times (\mathbb{Z}/q^m\mathbb{Z})^\times$, and since $K \subseteq L$, it follows that $(\mathbb{Z}/q^m\mathbb{Z})^\times$ must be a subgroup of $(\mathbb{Z}/p^n\mathbb{Z})^\times$. It follows that $\varphi(q^m)$ is a divisor of $\varphi(p^n)$. If in addition we have $q > p$, it follows that $m = 1$, and $q - 1$ divides $\varphi(p^n)$, as claimed. □

Corollary 5.7. — *Let $E/\mathbb{Q}$ be an elliptic curve, $p > 2$ a prime, and $n \geqslant 1$. If $\Im\rho_{E,p^n}$ is contained in a Borel subgroup of $\mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$ then the field $K_E(p) = \mathbb{Q}(E[p^n]) \cap \mathbb{Q}^{ab}$ has $\mathrm{Gal}(K_E(P)/\mathbb{Q})$ isomorphic to a $(\mathbb{Z}/p^n\mathbb{Z})^\times \times C$ where C is a cyclic group of order dividing $\varphi(p^n)$. Thus, $K_p(E)$ is the compositum of $\mathbb{Q}(\zeta_{p^n})$ and a cyclic extension $L/\mathbb{Q}$ with $\mathrm{Gal}(L/\mathbb{Q}) = C$.*

5.3. Exceptional Images

Serre showed that an elliptic curve over $\mathbb{Q}$ cannot have exceptional image for $p \geqslant 17$ (see [22, Lemma 18]). Moreover:

Theorem 5.8 ([16, Theorem 8.1]). — *Let $E/\mathbb{Q}$ be an elliptic curve, and $p \geqslant 3$ a prime number, such that the image $\overline{G}$ of $\rho_{E,p}$ in $\mathrm{PGL}(E[p])$ is isomorphic to $\overline{G} = A_4$, S_4, or A_5. Then, $p \leqslant 13$ and $\overline{G} = S_4$.*

Further, by work of Sutherland and Zywina [25, 28], we know that if $3 \leqslant p \leqslant 13$ and the image of $\rho_{E,p}$ in $\mathrm{PGL}(E[p])$ is isomorphic to S_4, then $p = 5$ or $p = 13$.

Proposition 5.9 ([25, 28]). — *Let $E/\mathbb{Q}$ be an elliptic curve, and $p \geqslant 3$ a prime number, such that the image of $\rho_{E,p}$ in $\mathrm{PGL}(E[p])$ is isomorphic to S_4. Then, $p = 5$, or $p = 13$. Moreover, $\Im\rho_{E,p} \subseteq \mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$ is a conjugate subgroup of*

$$H_5 = \left\langle \begin{pmatrix} 1 & 4 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \right\rangle \subseteq \mathrm{GL}(2, \mathbb{Z}/5\mathbb{Z}), \quad \textit{or}$$

$$H_{13} = \left\langle \begin{pmatrix} 1 & 12 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 8 \end{pmatrix} \right\rangle \subseteq \mathrm{GL}(2, \mathbb{Z}/13\mathbb{Z}).$$

Proof. — See [25, Tables 3 and 4], and [28, Theorems 1.4 and 1.8]. □

PROPOSITION 5.10. — *Let $E/\mathbb{Q}$ be an elliptic curve, let $p > 2$ be a prime, and let $n \geqslant 1$. Moreover, assume that the image of $\rho_{E,p}$ is an exceptional subgroup (i.e., the projective image of $\Im\rho_{E,p}$ in $\mathrm{PGL}(2, \mathbb{Z}/p\mathbb{Z})$ is isomorphic to S_4). Then, $\mathbb{Q}(\zeta_{q^m}) \cap \mathbb{Q}(E[p^n])$ is trivial for any $m \geqslant 1$ and any prime $q \neq p$.*

Proof. — Suppose that E is a curve as in the statement. Then, by Theorem 5.8, we have $p \leqslant 13$, and by Proposition 5.9, we have $p = 5$ or $p = 13$, and $G = \Im\rho_{E,p}$ is a conjugate of H_5 or H_{13}, respectively. A simple computation shows that

$$H_5/[H_5, H_5] \simeq (\mathbb{Z}/5\mathbb{Z})^\times \text{ and } H_{13}/[H_{13}, H_{13}] \simeq (\mathbb{Z}/13\mathbb{Z})^\times$$

and therefore the Galois group of the maximal abelian subextension L_p of $\mathbb{Q}(E[p])$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times$, for $p = 5$, or 13. Since $\mathbb{Q}(\zeta_p) \subseteq \mathbb{Q}(E[p])$, it follows that $L_p = \mathbb{Q}(\zeta_p)$. In particular, if $q \neq p$, then $\mathbb{Q}(\zeta_{q^m}) \cap \mathbb{Q}(E[p]) \subseteq L_p$ must be trivial. Now, if $\mathbb{Q}(\zeta_{q^m}) \subseteq \mathbb{Q}(E[p^n])$, and since $[\mathbb{Q}(E[p^n]) : \mathbb{Q}(E[p])]$ is a power of p, it would follow that $\varphi(q^m)$ is itself a power of p. Hence, $0 \leqslant m \leqslant 1$, and $q - 1 = p^t$ for some $t \geqslant 1$, which is impossible for $p > 2$, unless $m = 0$. Thus, $\mathbb{Q}(\zeta_{q^m}) \cap \mathbb{Q}(E[p^n])$ is trivial for any $q \neq p$ and any $m \geqslant 1$, as desired. □

COROLLARY 5.11. — *Let $E/\mathbb{Q}$ be an elliptic curve and $p > 2$ a prime. If $\rho_{E,p}$ is contained in an exceptional group then $K_E(p) = \mathbb{Q}(E[p]) \cap \mathbb{Q}^{ab} = \mathbb{Q}(\zeta_p)$. Thus, in this case we have that $\mathrm{Gal}(K_E(p)/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$.*

5.4. Split Cartan

In this subsection we give results in the case when the image is contained in the normalizer of a split Cartan group. We define the split Cartan subgroup of $\mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$ by

$$C_s(p) = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in (\mathbb{Z}/p\mathbb{Z})^\times \right\}$$

and let $N_s(p) = C_s(p) \cup \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot C_s(p)$ be its normalizer. Notice that if the image G of $\rho_{E,p}$ is strictly contained in a split Cartan group, then G is abelian, in which case we already know what can happen by our results in Section 4. Thus, we will assume that G is non-abelian.

THEOREM 5.12. — *If G is a subgroup of $N_s(p)$ such that $\det(G) = (\mathbb{Z}/p\mathbb{Z})^\times$, and $G' = [G,G] \neq \{\mathrm{Id}\}$, then G/G' is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times$, or $(\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}/2\mathbb{Z}$, or $\mathbb{Z}/2(p-1)\mathbb{Z}$. Moreover, if G contains an element of zero trace and determinant -1, then $G/G' \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ or $(\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}/2\mathbb{Z}$.*

Before we prove Theorem 5.12, we will need the following lemmas.

LEMMA 5.13. — *Let G and $G' = [G,G]$ be as in Theorem 5.12. Then,*

(1) *If $M = \left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right) \in G$, then $N = \left(\begin{smallmatrix} b & 0 \\ 0 & a \end{smallmatrix}\right) \in G$ also, and $M \equiv N \bmod G'$.*
(2) *Let H be a subgroup of the form $\left\{\left(\begin{smallmatrix} a & 0 \\ 0 & a^{-1} \end{smallmatrix}\right) : a \in (\mathbb{Z}/p\mathbb{Z})^\times\right\} \cap G$, and let $\overline{H}$ be the image of H in G/G'. Then, $\overline{H}$ is either trivial or isomorphic to $\mathbb{Z}/2\mathbb{Z}$.*
(3) *If $\overline{H}$ is non-trivial, and there is a matrix in G of the form $T_a = \left(\begin{smallmatrix} a & 0 \\ 0 & a^{-1} \end{smallmatrix}\right)$ where a is not a quadratic residue mod p, then $\overline{H}$ is generated by $T_a \bmod G'$.*

Proof. — For (1), suppose that $M = \left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right) \in G$. Since $G' \neq \{\mathrm{Id}\}$, there must also be an element in G of the form $L = \left(\begin{smallmatrix} 0 & c \\ d & 0 \end{smallmatrix}\right)$. Therefore,

$$[M,L] = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\begin{pmatrix} 0 & c \\ d & 0 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}^{-1}\begin{pmatrix} 0 & c \\ d & 0 \end{pmatrix}^{-1} = \begin{pmatrix} ab^{-1} & 0 \\ 0 & a^{-1}b \end{pmatrix} \in G'.$$

Thus, $N = M \cdot [M,L]^{-1}$ belongs to G also, and $M \equiv N \bmod G'$, as claimed.

For (2), since H is cyclic, the image $\overline{H}$ is also cyclic. Further, part (1) shows that every element of $\overline{H}$ has order dividing two since

$$\begin{aligned}\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}^2 &\equiv \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \equiv \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}\begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} \\ &\equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod G'.\end{aligned}$$

Thus, $\overline{H}$ is trivial or cyclic of order 2. This shows (2).

For (3), let $\mathcal{N}_p \subset (\mathbb{Z}/p\mathbb{Z})^\times$ be the set of quadratic non-residues mod p. Let $a \in \mathcal{N}_p$ and put $T_a = \left(\begin{smallmatrix} a & 0 \\ 0 & a^{-1} \end{smallmatrix}\right)$. Let us suppose that $\overline{H}$ is non-trivial (therefore of order 2 by part (2)), and $T_a \in G$. Since H is cyclic, H is generated by a matrix T_d for some $d \in (\mathbb{Z}/p\mathbb{Z})^\times$. Notice that $d \in \mathcal{N}_p$, because there is an odd number n with $T_d^n = T_a$ (and therefore $d^n \equiv a \bmod p$) but this would be impossible if d was a square or n was even. Finally, if we write $n = 2k+1$, and since $|\overline{H}| = 2$, we have $T_d^2 \equiv \mathrm{Id} \bmod G'$, and it follows that $T_a = T_d^n = T_d^{2k} T_d \equiv T_d \bmod G'$, and therefore $\overline{H}$ is generated by the class of T_a as well, as desired. □

LEMMA 5.14. — *With notation and assumptions as in Proposition 5.12, and if we assume that G contains a matrix of the form $A_a = \left(\begin{smallmatrix} 0 & -a \\ a^{-1} & 0 \end{smallmatrix}\right)$ for some $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, then*

(1) *Let $\overline{H}$ be the image of subgroup $H = \left\{\left(\begin{smallmatrix} d & 0 \\ 0 & d^{-1} \end{smallmatrix}\right) : d \in (\mathbb{Z}/p\mathbb{Z})^\times\right\} \cap G$ in G/G'. Then, $\overline{H}$ is trivial.*
(2) *The matrix $-\mathrm{Id}$ is a commutator of G, i.e., $-\mathrm{Id} \in G'$.*

Proof. — Let G be a group as in the statement of Proposition 5.12. Since $\det(G) = (\mathbb{Z}/p\mathbb{Z})^\times = \langle g \rangle$, for some primitive root $g \bmod p$, there is a matrix $M \in G \subseteq N_s(p)$ with $\det(M) = g$. Hence, $M = \left(\begin{smallmatrix} gc & 0 \\ 0 & c^{-1} \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} 0 & gc \\ -c^{-1} & 0 \end{smallmatrix}\right)$ for some $c \in (\mathbb{Z}/p\mathbb{Z})^\times$. In the latter case, we define M' by

$$M' = M \begin{pmatrix} 0 & -a \\ a^{-1} & 0 \end{pmatrix} = \begin{pmatrix} gca^{-1} & 0 \\ 0 & ac^{-1} \end{pmatrix}.$$

In particular,

$$MA_aM^{-1}A_a^{-1} = \begin{pmatrix} gc^2 & 0 \\ 0 & (gc^2)^{-1} \end{pmatrix},$$

and

$$M'A_aM'^{-1}A_a^{-1} = \begin{pmatrix} gc^2a^{-2} & 0 \\ 0 & (gc^2a^{-2})^{-1} \end{pmatrix}.$$

Thus, following the notation of Lemma 5.13, part (3), the matrices T_{gc^2} or $T_{g(ca^{-1})^2} \in G' \subseteq G$ and gc^2 , $g(ca^{-1})^2$ are not squares modulo p. By Lemma 5.13, either T_{gc^2} or $T_{g(ca^{-1})^2}$ generate $\overline{H}$, but they both belong to G', and it follows that $\overline{H}$ must be trivial. This proves (1).

For (2), we note that $T_d^{(p-1)/2} = T_{d^{(p-1)/2}}$, and

$$(gd^2)^{(p-1)/2} \equiv g^{(p-1)/2}d^{(p-1)} \equiv -1 \bmod p$$

for any $d \in (\mathbb{Z}/p\mathbb{Z})^\times$. Thus, $-\mathrm{Id} = T_{gc^2}^{(p-1)/2} = T_{gc^2a^{-2}}^{(p-1)/2} \in G'$, as desired. □

LEMMA 5.15. — *With notation as in Proposition 5.12, let $\overline{S}$ be the image of the subgroup $S = G \cap \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ in G/G'. Then, $\overline{S}$ is cyclic with order dividing 2.*

Proof. — First note that

$$S = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, \begin{pmatrix} 0 & -a \\ a^{-1} & 0 \end{pmatrix} : a \in (\mathbb{Z}/p\mathbb{Z})^\times \right\} \cap G.$$

If $S \subseteq H$, with H as in Lemma 5.13, then $\overline{H}$ is trivial or isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Otherwise, there is a matrix of the form $\left(\begin{smallmatrix} 0 & -a \\ a^{-1} & 0 \end{smallmatrix}\right)$ in $S \subseteq G$. Hence,

Lemma 5.14 implies that $H \subseteq G'$ (i.e., $\overline{H}$ is trivial) and $-\mathrm{Id} \in G'$. Now suppose that we have any two elements of $S - H$,

$$A = \begin{pmatrix} 0 & -a \\ a^{-1} & 0 \end{pmatrix} \text{ and } B = \begin{pmatrix} 0 & -b \\ b^{-1} & 0 \end{pmatrix}.$$

Then

$$A^2 = -\mathrm{Id} \in G', \text{ and } AB = \begin{pmatrix} -ab^{-1} & 0 \\ 0 & -a^{-1}b \end{pmatrix} \in H \subseteq G'.$$

Hence $AB \equiv \mathrm{Id} \bmod G'$, and

$$A \equiv A \cdot AB \equiv A^2 \cdot B \equiv B \bmod G'.$$

Thus, $\overline{S}$ is of order 2. □

LEMMA 5.16. — *If G is a subgroup of $N_s(p)$ that contains a matrix τ of zero trace and determinant -1, then there is an element of $\gamma \in C_s(p)$ such that $\gamma\tau\gamma^{-1}$ is one of the following matrices:*

$$\tau_1 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \tau_2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \tau_3 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

In particular, G is conjugate to a subgroup of $N_s(p)$ that contains one of τ_i, for $i = 1$, 2, or 3.

Proof. — If $\tau \in N_s(p)$ has zero trace and determinant -1, then it is of the form $\left(\begin{smallmatrix} \pm 1 & 0 \\ 0 & \mp 1 \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} 0 & a \\ a^{-1} & 0 \end{smallmatrix}\right)$ for some $a \in (\mathbb{Z}/p\mathbb{Z})^\times$. If it is the latter, then the matrix $\gamma = \left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right) \in C_s(p)$ satisfies $\gamma^{-1}\tau\gamma = \tau_3$, as claimed. Finally, since $N_s(p)$ is stable under conjugation by an element γ of its subgroup $C_s(p)$, the last claim follows. □

We are finally ready to prove Theorem 5.12.

Proof of Theorem 5.12. — Suppose that G is a subgroup of $N_s(p)$ such that $\det(G) = (\mathbb{Z}/p\mathbb{Z})^\times$, and $G' = [G, G] \neq \{\mathrm{Id}\}$. Since G' is a subgroup of $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, we know that det induces a map $\overline{\det}\colon G/G' \to (\mathbb{Z}/p\mathbb{Z})^\times$ that is a surjective homomorphism. Moreover, G/G' is abelian. Thus $(G/G_1)/\ker(\overline{\det}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$. But $\ker(\overline{\det}) = \overline{S}$, where $\overline{S}$ is the image of $G \cap \mathrm{SL}(2, \mathbb{Z}/p\mathbb{Z})$ in G/G'. From Lemma 5.15 we have $\overline{S}$ is trivial or isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Hence, G/G' is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times$, or $(\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}/2\mathbb{Z}$, or $\mathbb{Z}/2(p-1)\mathbb{Z}$.

It remains to discard the possibility that $G/G' \simeq \mathbb{Z}/2(p-1)\mathbb{Z}$, under the assumption that G contains an element with zero trace and determinant -1. If this happens, then $\overline{S} \simeq \mathbb{Z}/2\mathbb{Z}$. If so, then G/G' would contain an element of order $2(p-1)$, however we will show that the order of every element in G/G' divides $p-1$. Indeed, every element of $N_s(p)$ has order dividing

$2(p-1)$, so if G/G' had an element of order $2(p-1)$, then G itself would have an element M of exact order $2(p-1)$ such that $M \bmod G'$ also has order $2(p-1)$. Such an element of $N_s(p)$ must be of the form $M = \left(\begin{smallmatrix} 0 & gc \\ c^{-1} & 0 \end{smallmatrix}\right)$, with g a primitive root and $c \not\equiv 0 \bmod p$, so that $M^2 = \left(\begin{smallmatrix} g & 0 \\ 0 & g \end{smallmatrix}\right)$ has order $p-1$. In particular, $M^{(p-1)} = (M^2)^{(p-1)/2} = -\mathrm{Id}$, and since the order of $M \bmod G'$ is $2(p-1)$ we conclude $-\mathrm{Id}$ is not in G'. We will prove that in fact $-\mathrm{Id} \in G'$, which is a contradiction.

Since $-\mathrm{Id}$ belongs to the center of $\mathrm{GL}(2, \mathbb{F}_p)$, the element $-\mathrm{Id}$ belongs to $G' = [G, G]$ if and only if $-\mathrm{Id}$ belongs to the commutator of any subgroup of $N_s(p)$ that is conjugate to G. Thus, by Lemma 5.16, we can assume that G contains an element $\tau = \tau_i$, for $i = 1$, 2, or 3. If $\tau = \tau_1$ or τ_2, then $M\tau M^{-1}\tau^{-1} = -\mathrm{Id} \in G'$ and we are done. Otherwise, suppose $\tau = \tau_3$. Then,

$$M\tau M^{-1}\tau^{-1} = \begin{pmatrix} gc^2 & 0 \\ 0 & (gc^2)^{-1} \end{pmatrix} = T_{gc^2},$$

but since g is a primitive root, then gc^2 is not a square, and $T_{gc^2}^{(p-1)/2} = -\mathrm{Id} \in G'$. Hence, we have reached a contradiction and $G/G' \simeq \mathbb{Z}/(2(p-1))\mathbb{Z}$ is impossible, which concludes the proof of the theorem. □

Corollary 5.17. — *Let $E/\mathbb{Q}$ be an elliptic curve and $p > 2$ a prime. If $\rho_{E,p}$ is contained in the normalizer of a split Cartan subgroup of $\mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$ then $K_E(p) = \mathbb{Q}(E[p]) \cap \mathbb{Q}^{ab} \subseteq \mathbb{Q}(\zeta_p, \sqrt{d})$ for some $d \in \mathbb{Z}$. Thus, in this case we have that $\mathrm{Gal}(K_E(p)/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times$ of $\mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^\times$.*

5.5. Non-split Cartan

In this section we give results in the case that the image of the mod p Galois representation is contained a non-abelian subgroup of the normalizer of the non-split Cartan subgroup of $\mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$.

Let p be a fixed prime and let $\varepsilon \in (\mathbb{Z}/p\mathbb{Z})^\times$ be a fixed quadratic non-residue. We define the non-split Cartan subgroup of $\mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$ by

$$C_{ns}(p) = \left\{ \begin{pmatrix} a & \varepsilon b \\ b & a \end{pmatrix} : a, b, \in \mathbb{Z}/p\mathbb{Z} \text{ and } (a, b) \neq (0, 0) \right\},$$

and its normalizer in $\mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$

$$N_{ns}(p) = C_{ns}(p) \cup \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} C_{ns}(p).$$

From [18, Section 5], we have that $C_{ns}(p) \simeq \mathbb{F}_{p^2}^{\times}$ and $N_{ns}(p) \simeq \langle C_{ns}(p), c\rangle$ where $c = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. If we fix a matrix $A = \left(\begin{smallmatrix} a & \varepsilon b \\ b & a \end{smallmatrix}\right)$ such that $C_{ns}(p) = \langle A\rangle$, then A is diagonalizable when considered over the larger field $(\mathbb{Z}/p\mathbb{Z})[\sqrt{\varepsilon}]$. That is, $A = QDQ^{-1}$ with

$$Q = \begin{pmatrix} \sqrt{\varepsilon} & -\sqrt{\varepsilon} \\ 1 & 1 \end{pmatrix} \text{ and } D = \begin{pmatrix} a + b\sqrt{\varepsilon} & 0 \\ 0 & a - b\sqrt{\varepsilon} \end{pmatrix}.$$

A simple computation shows that

$$\begin{aligned} A^p = QD^pQ^{-1} &= Q \begin{pmatrix} (a + b\sqrt{\varepsilon})^p & 0 \\ 0 & (a - b\sqrt{\varepsilon})^p \end{pmatrix} Q^{-1} \\ &= Q \begin{pmatrix} (a^p + b^p\sqrt{\varepsilon}^p) & 0 \\ 0 & a^p - b^p\sqrt{\varepsilon}^p \end{pmatrix} Q^{-1} \qquad (5.1) \\ &= Q \begin{pmatrix} (a - b\sqrt{\varepsilon}) & 0 \\ 0 & a + b\sqrt{\varepsilon} \end{pmatrix} Q^{-1} = \begin{pmatrix} a & -\varepsilon b \\ -b & a \end{pmatrix} = cAc. \end{aligned}$$

We note that the first equality in the second line above follows from the fact that

$$\mathrm{Gal}((\mathbb{Z}/p\mathbb{Z})[\sqrt{\varepsilon}]/(\mathbb{Z}/p\mathbb{Z})) \simeq \mathbb{Z}/2\mathbb{Z}$$

and is generated by the Frobenius map $x \mapsto x^p$ which maps $\sqrt{\varepsilon} \mapsto -\sqrt{\varepsilon}$ (since $(\sqrt{\varepsilon}^p = \varepsilon^{(p-1)/2}\sqrt{\varepsilon} = -\sqrt{\varepsilon}$ by Euler's criterion, because ε is a quadratic non-residue). Lastly, we point out that since the map $\det\colon C_{ns}(p) \to (\mathbb{Z}/p\mathbb{Z})^{\times}$ is surjective, and if $\langle A\rangle = C_{ns}(p)$, then $\det(A) = \alpha$ where α is a generator of $(\mathbb{Z}/p\mathbb{Z})^{\times}$.

As in the previous section (the split case), we may assume that G, the image of $\rho_{E,p}$ is non-abelian, since we have treated the abelian case separately in Section 4. Thus, we will assume here that $G' = [G, G]$ is not trivial.

LEMMA 5.18. — *Let G be a non-abelian subgroup of $N_{cs}(p)$. Then,*

1. *$G = \langle H, \tau\rangle$, where H is a subgroup of $C_{ns}(p)$ (therefore cyclic) and τ is any element of $N_{cs}(p) - C_{ns}(p)$.*
2. *If $\tau \in N_{cs}(p) - C_{ns}(p)$, then $\tau^2 \in C_{ns}(p)^{p+1} \cap H$.*
3. *Fix $\tau \in N_{cs}(p) - C_{ns}(p)$. Then, every element $g \in G$ is of the form $g = h$ or $g = h\tau$, for some $h \in H$. In particular, $\#G = 2 \cdot \#H$.*
4. *Fix $\tau \in N_{cs}(p) - C_{ns}(p)$. If $h \in H$, then $\tau h\tau^{-1} = h^p$.*
5. *Suppose G contains an element λ of order 2 with zero trace and determinant -1. Then, $\lambda \in N_{cs}(p) - C_{ns}(p)$ and $G = \langle H, \lambda\rangle$. Further, $G \simeq H \rtimes_{\varphi} \mathbb{Z}/2\mathbb{Z}$ with respect to the map $\varphi\colon \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(H)$ that sends λ to $h \mapsto \lambda \cdot h \cdot \lambda^{-1} = h^p$.*

Proof. — Let G be a non-abelian subgroup of $N_{cs}(p)$. Let $H = G \cap C_{ns}(p) \subseteq G$. Since G is non-abelian, and $C_{ns}(p)$ is cyclic abelian, it follows that H is cyclic and $H \neq G$, and there is $\tau \in G - H$, hence $\tau \in N_{ns}(p) - C_{ns}(p)$. Now suppose that γ is also an element of G not in H. Let $\langle A \rangle = C_{ns}(p)$. Then, $\gamma = A^k c$ and $\tau = A^j c$ for some $j, k \geqslant 0$ and c as above. Thus,

$$\gamma \cdot \tau = (A^k c)(A^j c) = A^k (c A^j c) = A^k \cdot A^{jp} = A^{k+jp} \in C_{ns}(p) \cap G = H$$

where we have used Equation (5.1), and so $\gamma = h \cdot \tau^{-1} \in \langle H, \tau \rangle$, where $h' = A^{k+jp}$. Hence, $G = \langle H, \tau \rangle$ as we wanted to show. Moreover, $\tau^2 = (A^j c)(A^j c) = A^j A^{pj} = A^{(p+1)j} \in C_{ns}(p)^{p+1} \cap H$. So $\tau^2 = h''$ and $(h'')^{-1}\tau = \tau^{-1}$. Thus, an arbitrary $\gamma \in G - H$ as above can be written as $\gamma = h'\tau^{-1} = h'(h'')^{-1}\tau = h\tau$ for $h = h'(h'')^{-1} \in H$. Finally, let $h = A^k \in H$. Then:

$$\tau h \tau^{-1} = \tau A^k \tau^{-1} = A^j c A^k c A^{-j} = A^{j+kp-j} = A^{kp} = h^p,$$

as desired for (4).

Finally, suppose that G contains an element λ as in part (5). Then, λ cannot be in $C_{ns}(p)$ because $C_{ns}(p)$ is cyclic of order $p^2 - 1$ and contains a unique element of order 2, namely $-\mathrm{Id}$, whose determinant is 1. Hence, $\lambda \in N_{cs}(p) - C_{ns}(p)$ and our previous work shows that $G = \langle H, \lambda \rangle$ is of order $2 \cdot \#H$. Since λ is of order 2, not in H, and $\lambda \cdot h \cdot \lambda^{-1} = h^p$ for all $h \in H$, it follows that $G \simeq H \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$ as claimed. □

Proposition 5.19. — *Let p be a prime and let G be a subgroup of $N_{ns}(p)$ such that $\det(G) = (\mathbb{Z}/p\mathbb{Z})^\times$, such that G contains an element λ of order 2, zero trace, and determinant -1, and assume that $G' = [G, G] \neq \{\mathrm{Id}\}$. Then, $G/G' \simeq \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^\times$.*

Proof. — Let G be a subgroup of $N_{ns}(p)$ such that $\det(G) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$. By Lemma 5.18, we have $G = \langle H, \tau \rangle$, with $H \subseteq C_{ns}(p) = \langle A \rangle$ and $\tau \in N_{cs}(p) - C_{ns}(p)$. Thus, $H = \langle A^{k_0} \rangle$ for some divisor k_0 of $p^2 - 1$. Let $\tau = A^j c$ for some $j \geqslant 0$. Note that

$$[A^{k_0}, \tau] = A^{k_0} \tau A^{-k_0} \tau^{-1} = A^{k_0 - k_0 p} = A^{-(p-1)k_0} \in H^{p-1}.$$

where we have used Lemma 5.18, part (4), and since $H = \langle A^{k_0} \rangle$, it follows that $H^{p-1} = \langle [A^{k_0}, \tau] \rangle \subseteq G' = [G, G]$. Further, we claim that $G' = H^{p-1}$. In order to show this, it suffices to show that G/H^{p-1} is abelian. Indeed, $G = H \rtimes \langle \lambda \rangle$ by Lemma 5.18, part (5), and in G/H^{p-1} we have $\lambda \cdot h \cdot \lambda^{-1} = h^p \equiv h \bmod H^{p-1}$, for all $h \in H$. Thus, $\lambda h \equiv h\lambda \bmod H^{p-1}$, and G/H^{p-1} is abelian. Therefore, $G' = H^{p-1}$.

Finally, note that H/H^{p-1} injects into $C_{ns}(p)/C_{ns}(p)^{p-1} \simeq (\mathbb{Z}/p\mathbb{Z})^\times$, where the last isomorphism comes from the fact that $C_{ns}(p)$ is cyclic of order p^2-1. Thus, H/H^{p-1} is at most of size $p-1$. Moreover:

$$G/G' = G/H^{p-1} = (H \rtimes \langle\lambda\rangle)/H^{p-1} \simeq (H/H^{p-1}) \times \mathbb{Z}/2\mathbb{Z}.$$

Further, since $G' \subseteq \mathrm{SL}(2,\mathbb{Z}/p\mathbb{Z})$, it follows that $\det\colon G/G' \to (\mathbb{Z}/p\mathbb{Z})^\times$ is also surjective. This implies that $H/H^{p-1} \times \mathbb{Z}/2\mathbb{Z}$ has an element of order $p-1$, and therefore H/H^{p-1} must be of size at least $p-1$. Hence, $H/H^{p-1} \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ and $G/G' \simeq (\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}/2\mathbb{Z}$ as desired. □

Corollary 5.20. — *Let $E/\mathbb{Q}$ be an elliptic curve and $p>2$ a prime. If $\rho_{E,p}$ is contained in the normalizer of a non-split Cartan subgroup of $\mathrm{GL}(2,\mathbb{Z}/p\mathbb{Z})$ then $K_E(p) = \mathbb{Q}(E[p]) \cap \mathbb{Q}^{ab} \subseteq \mathbb{Q}(\zeta_p, \sqrt{d})$ for some $d \in \mathbb{Z}$. Thus, in this case we have that $\mathrm{Gal}(K_E(P)/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times$ of $\mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^\times$.*

5.6. Summary of the results of this section

Before ending this section we give a summary the information in Corollaries 5.3, 5.7, 5.17, and 5.20 in a single place.

Proposition 5.21. — *Let $E/\mathbb{Q}$ be an elliptic curve, $p>2$ a prime, and $K_E(p) = \mathbb{Q}(E[p]) \cap \mathbb{Q}^{ab}$. Then,*

$$\mathrm{Gal}(K_E(p)/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times \times C$$

where C is a cyclic group of order dividing $p-1$. Moreover, $\#C > 2$ only when E has a p-isogeny (i.e., if the image of $\rho_{E,p}$ is contained in a Borel subgroup).

Note that Proposition 5.21 provides a proof of parts (2) and (3) of Theorem 1.7, so in Section 6 we will just need to prove part (1).

6. The proof of Theorem 1.7

In an attempt to simplify the proof of Theorem 1.7 we start this section by proving a few lemmas.

Lemma 6.1. — *For every elliptic curve $E/\mathbb{Q}$ and prime $q>3$, $\mathbb{Q}(E[3]) \cap \mathbb{Q}(\zeta_q)$ is at most quadratic. Thus, $\mathbb{Q}(E[3]) \neq \mathbb{Q}(E[q])$.*

Proof. — Let $E/\mathbb{Q}$ be an elliptic curve, and let $q > 3$ be a prime. From Proposition 5.21, we know that the largest that $K_E(3) = \mathbb{Q}(E[3]) \cap \mathbb{Q}^{ab}$ is at most biquadratic, of the form $F(\zeta_3)$ for some quadratic field $F/\mathbb{Q}$. Further, since $q > 3$ we have $\mathbb{Q}(\zeta_3) \cap \mathbb{Q}(\zeta_q) = \mathbb{Q}$ and $\mathbb{Q}(\zeta_3)$ is quadratic, so $\mathbb{Q}(E[3]) \cap \mathbb{Q}(\zeta_q)$ is at most quadratic.

For the second part of the statement, suppose towards a contradiction that $\mathbb{Q}(E[3]) = \mathbb{Q}(E[q])$. Then, from the first part of the statement, it follows that $\mathbb{Q}(\zeta_q) \subseteq \mathbb{Q}(E[q]) = \mathbb{Q}(E[3])$ must be a quadratic subfield of $\mathbb{Q}(E[3])$. Since the degree of $\mathbb{Q}(\zeta_q)/\mathbb{Q}$ is $q-1$, this means that $q = 3$ contradicting the assumption that $q > 3$. □

LEMMA 6.2. — *For every elliptic curve $E/\mathbb{Q}$ and prime $q > 2$, such that $\mathbb{Q}(E[4])/\mathbb{Q}$ is a non-abelian extension, we have $\mathbb{Q}(E[4]) \neq \mathbb{Q}(E[q])$.*

Proof. — Suppose towards a contradiction that there are an elliptic curve $E/\mathbb{Q}$ and a prime $q > 2$ such that $\mathbb{Q}(E[4]) = \mathbb{Q}(E[q])$. In particular, $\mathbb{Q}(\zeta_q) \subseteq \mathbb{Q}(E[4])$.

First note that the order of elements in $\mathrm{GL}(2, \mathbb{Z}/4\mathbb{Z})$ are $1, 2, 3, 4$, or 6. Thus, if $\mathbb{Q}(\zeta_q) \subset \mathbb{Q}(E[4])$ and $G = G_4 = \Im\rho_{E,4}$ it must be that $G/[G,G]$ has an elements of order $q-1$. Since the order of an element in $G/[G,G]$ divides the order of a representative in G, we know that $q - 1 \in \{1, 2, 3, 4, 6\}$ and thus $q \in \{2, 3, 5, 7\}$. Based on the assumptions $q \neq 2$ and so $q = 3$, 5, or 7.

Now, since $\mathbb{Q}(E[4]) = \mathbb{Q}(E[q])$, it follows that $\mathbb{Q}(E[4q])$ is also the same field. If we let $G_n = \Im\rho_{E,n}$, then we must have that $\mathrm{Gal}(\mathbb{Q}(E[4q])/\mathbb{Q}) \simeq G_{4q} \subseteq \mathrm{GL}(2, \mathbb{Z}/4q\mathbb{Z})$, and the natural reduction maps $G_{4q} \to G_4$ and $G_{4q} \to G_q$ are isomorphisms. In addition $\det(G_{4q}) = (\mathbb{Z}/4q\mathbb{Z})^\times$ and there is a matrix in G_{4q} with zero trace and determinant -1 (namely, the image of a complex conjugation via $\rho_{E,4q} \colon G_{\mathbb{Q}} \to \mathrm{GL}(2, \mathbb{Z}/4\mathbb{Z})$; see [25, Remark 3.1.4]). Further, we have assumed that G_4 and therefore G_{4q} are non-abelian. A search for such subgroups of $\mathrm{GL}(2, \mathbb{Z}/4q\mathbb{Z})$ yields that there are none for $q = 5$ or 7 so q must be 3. The search for subgroups in $\mathrm{GL}(2, \mathbb{Z}/12\mathbb{Z})$ yields two possible maximal groups, call them H_1 and H_2. If we let $\pi_3 \colon \mathrm{GL}(2, \mathbb{Z}/12\mathbb{Z}) \to \mathrm{GL}(2, \mathbb{Z}/3\mathbb{Z})$ and $\pi_4 \colon \mathrm{GL}(2, \mathbb{Z}/12\mathbb{Z}) \to \mathrm{GL}(2, \mathbb{Z}/4\mathbb{Z})$, the we see that $\pi_3(H_1) = \pi_3(H_2) = N_s(3)$ and

$$\pi_4(H_1) = \left\langle \begin{pmatrix} 3 & 3 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 3 \\ 2 & 1 \end{pmatrix} \right\rangle \text{ and } \pi_4(H_2) = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 3 \\ 2 & 1 \end{pmatrix} \right\rangle.$$

Moreover, we have $H_i \simeq \pi_3(H_i) \simeq \pi_4(H_i) \simeq D_4$, for $i = 1, 2$, and a computation of the genus of the modular curves X_{H_i} yields that both have genus 9. Determining the rational points on X_{H_i} for $i = 1$ or 2 would be very difficult, so instead consider the subgroup $\widetilde{H} \subseteq \mathrm{GL}(2, \mathbb{Z}/12\mathbb{Z})$ such

that $\pi_3(\widetilde{H}) = N_s(3)$ and

$$\pi_4(\widetilde{H}) = \left\langle \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 3 & 3 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 3 \\ 2 & 1 \end{pmatrix} \right\rangle$$
$$= \left\langle \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 3 \\ 2 & 1 \end{pmatrix} \right\rangle,$$

but we do not require that π_3 and π_4 are isomorphisms on $\widetilde{H}$. We note that the groups $\pi_4(H_1)$ and $\pi_4(H_2)$ are, respectively, the groups G_{10d} and G_{10b} in the notation of [20], and $\pi_4(\widetilde{H})$ is the group G_{10}.

Let $X_s^+(3)$ and X_{10} be the modular curves that parametrize elliptic curves, respectively, with mod 3 image conjugate to $N_s(3)$, and with mod 4 image conjugate to $\pi_4(\widetilde{H})$ (or equivalently, conjugate to G_{10}). Both $X_s^+(3)$ and X_{10} are curves of genus 0, and the j-invariants of such curves are given by rational functions $j(t)$ and $j'(s)$, respectively. Above we have shown that an elliptic curve $E/\mathbb{Q}$ with $\mathbb{Q}(E[4]) = \mathbb{Q}(E[3])$ would satisfy $j(E) = j(t_0) = j'(s_0)$ for some rational numbers t_0, and s_0. Thus, the point (t_0, s_0) would satisfy the equation $j(t) = j'(s)$, that is

$$j(s) = \frac{1728 \cdot (s^2 - 1/3)^3}{s^2(s^2+1)^2} = \frac{27(t+1)^3(t-3)^3}{t^3} = j'(t).$$

In particular:

$$(s(s^2+1))^2 = s^2(s^2+1)^2 = \frac{4^3(s^2-1/3)^3t^3}{(t+1)^3(t-3)^3} = \left(\frac{4(s^2-1/3)t}{(t+1)(t-3)}\right)^3,$$

and so $s(s^2+1)$ is a perfect cube, say $s(s^2+1) = T^3$ or in projective coordinates $C : S^3 + SU^2 = T^3$. An affine patch of this curve is $A : 1 + y^2 = x^3$, which is the elliptic curve with Cremona label `144a1` and has $A(\mathbb{Q}) = \{\mathcal{O}, (1,0)\}$. Thus, the only points on C are $[T, U, S] = [0, 1, 0]$ and $[1, 0, 1]$. Thus, $s = S/U = 0/1 = 0$ or $s = S/U = 1/0$ is undefined, so $s = 0$ is the only possibility. But if $s = 0$, then $j(s)$ is undefined. Hence, there is no such elliptic curve $E/\mathbb{Q}$ with $\mathbb{Q}(E[4]) = \mathbb{Q}(E[3])$. □

Proposition 6.3. — *Let $E/\mathbb{Q}$ be an elliptic curve and $p < q$ distinct primes in $\mathbb{Z}$ such that $\mathbb{Q}(E[p]) = \mathbb{Q}(E[q])$. Then, it must be that $p = 2$ and $q = 3$.*

Proof. — Let $K_E(p) = \mathbb{Q}(E[p]) \cap \mathbb{Q}^{ab}$ and $K_E(q) = \mathbb{Q}(E[q]) \cap \mathbb{Q}^{ab}$. If $\mathbb{Q}(E[p]) = \mathbb{Q}(E[q])$, then

$$K_E(p) = K_E(q) \quad \text{and} \quad \mathrm{Gal}(K_E(p)/\mathbb{Q}) = \mathrm{Gal}(K_E(q)/\mathbb{Q}).$$

Let $G = \mathrm{Gal}(K_E(p)/\mathbb{Q}) = \mathrm{Gal}(K_E(q)/\mathbb{Q})$.

Suppose that $p > 2$. Applying Proposition 5.21 we get that $G \simeq (\mathbb{Z}/p\mathbb{Z})^\times \times C \simeq (\mathbb{Z}/q\mathbb{Z})^\times \times C'$ where $\#C$ divides $p-1$ and $\#C'$ divides $q-1$. Next, since $\mathbb{Q}(\zeta_q) \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$, it must be that G contains a subgroup isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$. The only way that this can happen is if $p-1$ divides $q-1$ and $q-1$ divides $p-1$, that is $p = q$. Therefore, p cannot be greater than 2.

Next suppose $p = 2$. From Theorem 1.8 we can assume that $\mathbb{Q}(E[2])/\mathbb{Q}$ is a non-abelian extension. In this case,

$$\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \simeq S_3 \quad \text{and} \quad \mathrm{Gal}(K_E(2)/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}.$$

Therefore, $\mathbb{Q}(\zeta_q)/\mathbb{Q}$ is a quadratic extension and the only possibility is $q = 3$. □

Before we prove Theorem 1.7 we need one more lemma and a simplifying remark.

Lemma 6.4. — *There are no elliptic curves $E/\mathbb{Q}$ and $n \geqslant 1$ such that $\mathbb{Q}(E[2^n]) = \mathbb{Q}(E[9])$.*

Proof. — Suppose $E/\mathbb{Q}$ is an elliptic curve and $n \geqslant 1$ such that $\mathbb{Q}(E[2^n]) = \mathbb{Q}(E[9])$. By Theorem 1.8, it cannot happen if $\mathbb{Q}(E[9])$ is abelian over $\mathbb{Q}$, so we shall assume that $\mathbb{Q}(E[9])/\mathbb{Q}$ is non-abelian. A Magma search on subgroups $G \subseteq \mathrm{GL}(2, \mathbb{Z}/9\mathbb{Z})$ shows that if G is a non-abelian subgroup with full determinant map and an element corresponding to complex conjugation, then $G/[G,G]$ is isomorphic to one group in the set

$$S = \{\mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}\}.$$

Since $\mathbb{Q}(\zeta_{2^n}) \cap \mathbb{Q}(\zeta_9) = \mathbb{Q}$, if $\mathbb{Q}(\zeta_{2^n}) \subseteq \mathbb{Q}(E[9])$ and $n \geqslant 2$ then it follows that $(\mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^{n-2}) \times \mathbb{Z}/6\mathbb{Z}$ must be a subgroup of $G/[G,G]$. Thus, $n \leqslant 2$.

If $n = 1$, then $\mathbb{Q}(\zeta_9) \subseteq \mathbb{Q}(E[9]) = \mathbb{Q}(E[2])$ and since $[\mathbb{Q}(E[2]) : \mathbb{Q}] \leqslant 6$, it must be that $\mathbb{Q}(E[2]) = \mathbb{Q}(\zeta_9)$ which is a contradiction because we have assumed $\mathbb{Q}(E[9])$ was non-abelian.

Suppose next that $n = 2$. In this case a Magma search on subgroups $G \subseteq \mathrm{GL}(2, \mathbb{Z}/4\mathbb{Z})$ shows that if G is a non-abelian subgroup with full determinant map and an element corresponding to complex conjugation, then $G/[G,G]$ is isomorphic to one group in the set

$$T = \{\mathbb{Z}/2\mathbb{Z}, (\mathbb{Z}/2\mathbb{Z})^2, (\mathbb{Z}/2\mathbb{Z})^3, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}\}.$$

Comparing the lists S and T, and using the fact that $\mathbb{Q}(i, \zeta_9) \subseteq \mathbb{Q}(E[9]) = \mathbb{Q}(E[4])$, we see that the only possibility is that, if we write $G_E(4) = \Im\rho_{E,4}$

and $G_E(9) = \Im\rho_{E,9}$, then

$$G_E(4)/[G_E(4), G_E(4)] \simeq G_E(9)/[G_E(9), G_E(9)] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}.$$

Let $\pi_2\colon \mathrm{GL}(2, \mathbb{Z}/4\mathbb{Z}) \to \mathrm{GL}(2, \mathbb{Z}/2\mathbb{Z})$ and $\pi_3\colon \mathrm{GL}(2, \mathbb{Z}/9\mathbb{Z}) \to \mathrm{GL}(2, \mathbb{Z}/3\mathbb{Z})$ be the standard reductions maps and let

$$\begin{aligned} C_{ns}(2) &= \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\rangle \subseteq \mathrm{GL}(2, \mathbb{Z}/2\mathbb{Z}) \\ B(3) &= \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \right\rangle \subseteq \mathrm{GL}(2, \mathbb{Z}/3\mathbb{Z}) \\ N_{ns}(3) &= \left\langle \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix} \right\rangle \subseteq \mathrm{GL}(2, \mathbb{Z}/3\mathbb{Z}). \end{aligned}$$

Then, a Magma search among subgroups of $\mathrm{GL}(2, \mathbb{Z}/4\mathbb{Z})$ and $\mathrm{GL}(2, \mathbb{Z}/9\mathbb{Z})$ shows that $G_E(4)$ must be a subgroup of $\pi_2^{-1}(C_{ns}(2))$ and $G_E(9)$ is a subgroup of either $\pi_3^{-1}(B(3))$ or $\pi_3^{-1}(N_{ns}(3))$. Checking the subgroups of each of the possibilities, we see that there are no subgroups of $\pi_2^{-1}(C_{ns}(2))$, with full determinant and an element that has determinant -1 and trace 0, that are isomorphic to a subgroup of $\pi_3^{-1}(B(3))$ or $\pi_3^{-1}(N_{ns}(3))$ and thus it is not possible for $\mathbb{Q}(E[9]) = \mathbb{Q}(E[4])$. □

Remark 6.5. — Before starting the proof of Theorem 1.7 we notice that Proposition 5.1 and Lemma 6.4 allows us to reduce the problem considerably. If $E/\mathbb{Q}$, p, q, m, and n are as in the statement of Theorem 1.7, then we must have that $\mathbb{Q}(\zeta_{q^m}) \subseteq \mathbb{Q}(E[p^n])$. But by Proposition 5.1 this means that either $m = 1$ or $m = 2$, and $p = 2$ and $q = 3$, but $\mathbb{Q}(E[9]) = \mathbb{Q}(E[2^n])$ cannot occur by Lemma 6.4. Thus, we must have $m = 1$.

Proof of Theorem 1.7. — Proposition 5.21 implies parts (2) and (3) of the theorem, so it remains to show (1). From Remark 6.5, we only have to consider the case of $m = 1$. That is, we suppose that $E/\mathbb{Q}$ is an elliptic curve, $p < q$ primes in $\mathbb{Z}$, and $n \geqslant 1$ such that $\mathbb{Q}(E[p^n]) = \mathbb{Q}(E[q])$, and we aim to show that $p^n = 2$ and $q = 3$. By Theorem 1.8, we may assume $\mathbb{Q}(E[q])/\mathbb{Q}$ is non-abelian.

Le $q > p \geqslant 2$. Since $\mathbb{Q}(E[p^n]) = \mathbb{Q}(E[q])$, it must be that $\mathbb{Q}(\zeta_{p^n}) \subseteq \mathbb{Q}(E[q])$. From Proposition 5.21 and the work supporting its proof, and since $q \geqslant 3$, if $K_E(q) = \mathbb{Q}(E[q]) \cap \mathbb{Q}^{ab}$, then

$$\mathrm{Gal}(K_E(q)/\mathbb{Q}) \simeq \begin{cases} (\mathbb{Z}/q\mathbb{Z})^\times & E \text{ is surjective or exceptional at } q, \\ (\mathbb{Z}/q\mathbb{Z})^\times \times \mathbb{Z}/2\mathbb{Z} & E \text{ is Cartan at } q, \\ (\mathbb{Z}/q\mathbb{Z})^\times \times C & E \text{ is Borel at } q, \end{cases}$$

where C is a cyclic group of order dividing $q-1$. Again using the fact that $\mathbb{Q}(\zeta_q)$ and $\mathbb{Q}(\zeta_{p^n})$ intersect trivially, it follows that $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) \simeq C$ for some cyclic group of order dividing $q-1$. Moreover, if E is not Borel at q, then $C \simeq \mathbb{Z}/2\mathbb{Z}$. In the case that E does not have a q-isogeny, the only prime-powered cyclotomic fields that are trivial or quadratic fields are $p^n = 2, 3, 4$. So in this case we would have that $\mathbb{Q}(E[2]) = \mathbb{Q}(E[q])$ (and therefore $q = 3$ is the only possibility), or $\mathbb{Q}(E[3]) = \mathbb{Q}(E[q])$, or $\mathbb{Q}(E[4]) = \mathbb{Q}(E[q])$, but Lemmas 6.1 and 6.2 show the latter two cases cannot happen.

Suppose then that E is Borel at q. First note that if $p = 2$ and $n > 2$, then $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q})$ is not cyclic and therefore we reach a contradiction because C is cyclic (hence the only possibilities would be $\mathbb{Q}(E[2]) = \mathbb{Q}(E[q])$ or $\mathbb{Q}(E[4]) = \mathbb{Q}(E[q])$ which have been already discussed above and lead to $\mathbb{Q}(E[2]) = \mathbb{Q}(E[3])$ which we discuss below). Thus, assume $p > 2$. Since E is Borel at q, it follows that $[\mathbb{Q}(E[q]) : \mathbb{Q}]$ is a divisor of $(q-1)^2 \cdot q$. We distinguish cases according to the type of image modulo p. Let $G_p = \Im\rho_{E,p} \subseteq \mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$.

- Suppose $\rho_{E,p}$ is surjective, so that $G_p = \mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$. Then, $[\mathbb{Q}(E[p^n]) : \mathbb{Q}]$ is a divisor of $[\mathbb{Q}(E[p]) : \mathbb{Q}] \cdot p^k = (p^2-1)(p^2-p)p^k$ for some $k \geqslant 1$ (this follows from the fact that the kernel of the map $\mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z}) \to \mathrm{GL}(2, \mathbb{Z}/p^{n-1}\mathbb{Z})$ is of size p^4, and $\#\,\mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z}) = (p^2-1)(p^2-p)$). If $\mathbb{Q}(E[p^n]) = \mathbb{Q}(E[q])$, and q divides $d_q = [\mathbb{Q}(E[q]) : \mathbb{Q}]$, then q divides $(p^2-1)(p^2-p)p^k = (p-1)^2(p+1)p^{k+1}$, but $p < q$ so this is impossible. This would imply that d_q is a divisor of $(q-1)^2$, and $\mathbb{Q}(E[q])/\mathbb{Q}$ is in fact abelian (the mod q image would be contained in a split Cartan subgroup). However we have assumed $\mathbb{Q}(E[q])/\mathbb{Q}$ is non-abelian.
- Suppose the image of $\rho_{E,p}$ is exceptional. Then, Proposition 5.10 shows that $\mathbb{Q}(\zeta_{q^m}) \cap \mathbb{Q}(E[p^n])$ is trivial for any $m \geqslant 1$ and any prime $q \neq p$, and therefore $\mathbb{Q}(E[q]) = \mathbb{Q}(E[p^n])$ would be impossible.
- Suppose the image of $\rho_{E,p}$ is contained in the normalizer of a (split or non-split) Cartan subgroup of $\mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$. Then, $[\mathbb{Q}(E[p^n]) : \mathbb{Q}]$ is a divisor of $2(p^2-1)p^k$ or $2(p-1)^2p^k$, for some $k \geqslant 1$ (because $\#C_{ns}(p) = p^2-1$ and $\#C_s(p) = (p-1)^2$). Thus, if $\mathbb{Q}(E[p^n]) = \mathbb{Q}(E[q])$, and q divides $d_q = [\mathbb{Q}(E[q]) : \mathbb{Q}]$, then q divides $2(p+1)(p-1)^3p^k$, but $p < q$ so this is impossible. As before, this would imply that $\mathbb{Q}(E[q])/\mathbb{Q}$ is abelian, a contradiction.

Hence, we have reached a contradiction in every case, and therefore $\mathbb{Q}(E[p^n]) = \mathbb{Q}(E[q])$ is impossible.

All that is left to complete the proof of Theorem 1.7 is to parametrize all the elliptic curves that have $\mathbb{Q}(E[2]) = \mathbb{Q}(E[3])$. To do this we search $\mathrm{GL}(2,\mathbb{Z}/6\mathbb{Z})$ for subgroups that have surjective determinant maps and such that the reductions maps $\pi_2\colon \mathrm{GL}(2,\mathbb{Z}/6\mathbb{Z}) \to \mathrm{GL}(2,\mathbb{Z}/2\mathbb{Z})$ and $\pi_3\colon \mathrm{GL}(2,\mathbb{Z}/6\mathbb{Z}) \to \mathrm{GL}(2,\mathbb{Z}/3\mathbb{Z})$ induce isomorphisms when restricted to the given subgroup. The search yields two possibilities for $\Im\rho_{E,6}$, namely

$$H_1 = \left\langle \begin{pmatrix} 5 & 5 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix} \right\rangle \text{ and } H_2 = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix} \right\rangle.$$

Elliptic curves with $\Im\rho_{E,6}$ in H_1 have a rational point of order 3, while elliptic curves with $\Im\rho_{E,6}$ in H_2 are a twist of the previous curves a curve by -3. Checking the genus of the corresponding modular curves X_{H_i} using code from [26] we see that they are both genus 0 and since we have seen an example of this exact image, we know that X_{H_1} (and X_{H_2}) must have (infinitely many) rational points. Computing a model for X_{H_1}, we get exactly the elliptic curve over $\mathbb{Q}(t)$ that is in the statement of the theorem, and the twist by -3 produces the parametrization of elliptic curves with image H_2. This completes the proof of the theorem. □

7. Proofs of Theorem 1.10 and Corollary 1.11

7.1. Proof of Theorem 1.10

In this section we first provide a proof of Theorem 1.10. Let $2 \leqslant m < n \leqslant 10$, and suppose that $E/\mathbb{Q}$ is an elliptic curve such that $\mathbb{Q}(E[m]) = \mathbb{Q}(E[n])$. We have already seen that $(m,n) \in \{(2,3),(2,4),(2,6),(3,6)\}$ are possible, in Theorems 1.4 and 1.7 (note that $\mathbb{Q}(E[2]) = \mathbb{Q}(E[3])$ also implies that $\mathbb{Q}(E[2]) = \mathbb{Q}(E[6])$). Moreover, Theorem 1.7 shows that if $\mathbb{Q}(E[p^a]) = \mathbb{Q}(E[q^b])$, then $p^a = 2$ and $q^b = 3$. Hence, the pairs

$$\{(3,4),(2,5),(3,5),(4,5),(2,7),(3,7),(4,7),(5,7),$$
$$(3,8),(5,8),(7,8),(2,9),(4,9),(5,9),(7,9),(8,9)\}$$

do not occur. Theorem 1.4 says $(4,8)$ and $(3,9)$ do not occur, and also note that $(2,8)$ would imply $(4,8)$, so $(2,8)$ does not occur either.

In order to rule out the pairs in the set

$$L = \{(5,6),(2,10),(3,10),(4,10),(6,10),(7,10),(9,10)\}$$

we have used Magma to compute all the possible subgroups $G_m \subseteq \mathrm{GL}(2,\mathbb{Z}/m\mathbb{Z})$ and $G_n \subseteq \mathrm{GL}(2,\mathbb{Z}/n\mathbb{Z})$ which could correspond to images

of $\rho_{E,m}$ and $\rho_{E,n}$ respectively. In particular, we find all subgroups with full determinant, and such that they contain an element of determinant -1 and zero trace, and then checked that there is no possible isomorphism $G_m \cong G_n$. Therefore $(m,n) \in L$ is impossible.

Similarly, when $(m,n) = (8,10)$ we have computed all possibilities for G_m and G_n, and in this case there are pairs such that $G_m \cong G_n$, but in all such cases G_n is an abelian group. In particular, $\mathbb{Q}(E[10])/\mathbb{Q}$ would be abelian, but the main result of [13] shows that this is impossible.

Finally, in the case of $(m,n) = (6,7)$, we have computed all the possible pairs $G_m \cong G_n$ but, in addition, checked that G_7 is none of the subgroups described in [25], which correspond to one of the possible mod-7 images that occur for elliptic curves over $\mathbb{Q}$. Thus, $(6,7)$ cannot occur.

In summary we have shown that the only possibilities are

$$(m,n) \in \{(2,3),(2,4),(2,6),(3,6),(4,6),(6,8),(6,9),(5,10)\},$$

as claimed. This concludes the proof of Theorem 1.10.

7.2. Proof of Corollary 1.11

Next we provide a proof of Corollary 1.11. Let p be a prime, and let $m \geqslant 2$ be an integer divisible by q^n for some odd prime q and $n \geqslant 1$, such that $\varphi(q^n)$ does not divide $p-1$. Let us suppose for a contradiction that $\mathbb{Q}(E[p]) = \mathbb{Q}(E[m])$. Since q^n divides m, then $\mathbb{Q}(\zeta_{q^n}) \subseteq \mathbb{Q}(E[q^n]) \subseteq \mathbb{Q}(E[m])$, and therefore $\mathbb{Q}(\zeta_{q^n}) \subseteq \mathbb{Q}(E[p])$ as well. By Proposition 5.21 we must have that $\varphi(q^n)$ is a divisor of $p-1$, which contradicts our hypothesis. This concludes the proof of the theorem.

BIBLIOGRAPHY

[1] C. Adelmann, *The decomposition of primes in torsion point fields*, Lecture Notes in Mathematics, vol. 1761, Springer-Verlag, Berlin, 2001, vi+142 pages.

[2] W. Bosma, J. Cannon & C. Playoust, "The Magma algebra system. I. The user language", *J. Symbolic Comput.* **24** (1997), no. 3-4, p. 235-265, Computational algebra and number theory (London, 1993).

[3] J. Brau & N. Jones, "Elliptic curves with 2-torsion contained in the 3-torsion field", *Proc. Amer. Math. Soc.* **144** (2016), no. 3, p. 925-936.

[4] G. Chiloyan & Á. Lozano-Robledo, "A classification of isogeny-torsion graphs of $\mathbb{Q}$-isogeny classes of elliptic curves", *Trans. London Math. Soc.* **8** (2021), no. 1, p. 1-34.

[5] M. Chou, "Torsion of rational elliptic curves over the maximal abelian extension of $\mathbb{Q}$", *Pacific J. Math.* **302** (2019), no. 2, p. 481-509.

[6] B. Conrad & K. Rubin (eds.), *Arithmetic Algebraic Geometry (IAS/Park City Mathematics)*, paperback ed., American Mathematical Society, IAS/Park City Mathematics Institute, 2 2008 (English), 569 pages.

[7] H. B. Daniels, "Torsion subgroups of rational elliptic curves over the compositum of all D_4 extensions of the rational numbers", *J. Algebra* **509** (2018), p. 535-565.

[8] H. B. Daniels, M. Derickx & J. Hatley, "Groups of generalized G-type and applications to torsion subgroups of rational elliptic curves over infinite extensions of $\mathbb{Q}$", *Trans. London Math. Soc.* **6** (2019), no. 1, p. 22-52.

[9] H. B. Daniels, Á. Lozano-Robledo, F. Najman & A. V. Sutherland, "Torsion subgroups of rational elliptic curves over the compositum of all cubic fields", *Math. Comp.* **87** (2018), no. 309, p. 425-458.

[10] T. Dokchitser & V. Dokchitser, "Surjectivity of mod 2^n representations of elliptic curves", *Math. Z.* **272** (2012), no. 3-4, p. 961-964.

[11] W. Duke, "Elliptic curves with no exceptional primes", *C. R. Acad. Sci. Paris Sér. I Math.* **325** (1997), no. 8, p. 813-818.

[12] N. D. Elkies, "Elliptic curves with 3-adic Galois representation surjective mod 3 but not mod 9", `https://arxiv.org/abs/math/0612734`, 2006.

[13] E. González-Jiménez & Á. Lozano-Robledo, "Elliptic curves with abelian division fields", *Math. Z.* **283** (2016), no. 3-4, p. 835-859.

[14] N. Jones, "Almost all elliptic curves are Serre curves", *Trans. Amer. Math. Soc.* **362** (2010), no. 3, p. 1547-1570.

[15] ———, "GL_2-representations with maximal image", *Math. Res. Lett.* **22** (2015), no. 3, p. 803-839.

[16] Á. Lozano-Robledo, "On the field of definition of p-torsion points on elliptic curves over the rationals", *Math. Ann.* **357** (2013), no. 1, p. 279-305.

[17] ———, "Division fields of elliptic curves with minimal ramification", *Rev. Mat. Iberoam.* **31** (2015), no. 4, p. 1311-1332.

[18] Á. Lozano-Robledo, "Galois representations attached to elliptic curves with complex multiplication", `https://arxiv.org/abs/1809.02584`, 2018.

[19] J. S. Morrow, "Composite images of Galois for elliptic curves over $\mathbf{Q}$ and entanglement fields", *Math. Comp.* **88** (2019), no. 319, p. 2389-2421.

[20] J. Rouse & D. Zureick-Brown, "Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois", *Res. Number Theory* **1** (2015), p. Paper No. 12, 34.

[21] J.-P. Serre, "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques", *Invent. Math.* **15** (1972), no. 4, p. 259-331.

[22] ———, "Quelques applications du théorème de densité de Chebotarev", *Inst. Hautes Études Sci. Publ. Math.* (1981), no. 54, p. 323-401.

[23] ———, *Abelian l-adic representations and elliptic curves*, Research Notes in Mathematics, vol. 7, A K Peters, Ltd., Wellesley, MA, 1998, With the collaboration of Willem Kuyk and John Labute, Revised reprint of the 1968 original, 199 pages.

[24] J. H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009, xx+513 pages.

[25] A. V. Sutherland, "Computing images of Galois representations attached to elliptic curves", *Forum Math. Sigma* **4** (2016), p. Paper No. e4, 79.

[26] A. V. Sutherland & D. Zywina, "Modular curves of prime-power level with infinitely many rational points", *Algebra Number Theory* **11** (2017), no. 5, p. 1199-1229.

[27] The LMFDB Collaboration, "The L-functions and modular forms database, Home page of the L-function $L(s, E)$ for elliptic curve isogeny class `234446.a`", 2021, `http://www.lmfdb.org/L/EllipticCurve/Q/234446.a/`, [Online; accessed 23 June 2021].

[28] D. Zywina, "On the possible images of the mod ell representations associated to elliptic curves over Q", https://arxiv.org/abs/1508.07660, 2015.

[29] ———, "Possible indices for the Galois image of elliptic curves over Q", https://arxiv.org/abs/1508.07663, 2015.

Manuscrit reçu le 30 décembre 2019,
révisé le 12 avril 2021,
accepté le 23 juin 2021.

Harris B. DANIELS
Department of Mathematics
Amherst College
Amherst, MA 01002 (USA)
hdaniels@amherst.edu

Álvaro LOZANO-ROBLEDO
Department of Mathematics
University of Connecticut
Storrs, CT 06269 (USA)
alvaro.lozano-robledo@uconn.edu