RACSAM (2016) 110:121–143
DOI 10.1007/s13398-015-0223-9

ORIGINAL PAPER

Torsion of rational elliptic curves over quadratic fields II

Enrique González-Jiménez[1] · José M. Tornero[2]

Received: 29 October 2014 / Accepted: 24 March 2015 / Published online: 30 April 2015

Abstract Let E be an elliptic curve defined over $\mathbb{Q}$ and let $G = E(\mathbb{Q})_{\text{tors}}$ be the associated torsion group. In a previous paper, the authors studied, for a given G, which possible groups $G \leq H$ could appear such that $H = E(K)_{\text{tors}}$, for $[K : \mathbb{Q}] = 2$. In the present paper, we go further in this study and compute, under this assumption and for every such G, all the possible situations where $G \neq H$. The result is optimal, as we also display examples for every situation we state as possible. As a consequence, the maximum number of quadratic number fields K such that $E(\mathbb{Q})_{\text{tors}} \neq E(K)_{\text{tors}}$ is easily obtained.

Keywords Elliptic curves · Torsion subgroup · Rationals · Quadratic fields

Mathematics Subject Classification Primary 11G05 · 11G30; Secondary 11B25 · 11D45 · 14G05

1 Introduction

Let E be an elliptic curve defined over a number field L. The Mordell-Weil Theorem states that the set of L-rational points, $E(L)$, is a finitely generated abelian group. So it canbe

E. González-Jiménez was partially supported by the Grant MTM2012–35849. J. M. Tornero was partially supported by the Grant FQM–218 and P12–FQM–2696.

✉ José M. Tornero
tornero@us.es

Enrique González-Jiménez
enrique.gonzalez.jimenez@uam.es
http://www.uam.es/enrique.gonzalez.jimenez

1 Departamento de Matemáticas, Universidad Autónoma de Madrid, Madrid, Spain

2 Departamento de Álgebra and IMUS, Universidad de Sevilla, P.O. 1160, 41080 Seville, Spain

written as $E(L) = E(L)_{\text{tors}} \oplus \mathbb{Z}^r$, for some non-negative integer r (called the rank of $E(L)$) and some finite torsion subgroup $E(L)_{\text{tors}}$. It is well known that there exist two positive integers n, m such that $n|m$ and $E(L)_{\text{tors}}$ is isomorphic to $\mathcal{C}_n \times \mathcal{C}_m$, where $\mathcal{C}_n$ is the cyclic group of order n [20].

Through this paper, we will often write $G = H$ (respectively $G \leq H$ or $G < H$) for the fact that G is *isomorphic* to H (repectively, isomorphic to a subgroup of H or to a proper subgroup of H) without further detail on the precise isomorphism.

We define some useful sets for the sequel:

- Let $\Phi(d)$ be the set of possible groups that can appear as the torsion subgroup of an elliptic curve defined over any number field L of degree d.
- Let $\Phi_{\mathbb{Q}}(d)$ be the set of possible groups that can appear as the torsion subgroup over a number field of degree d, of an elliptic curve E defined over the rationals.
- Let $G \in \Phi(1)$. We will write $\Phi_{\mathbb{Q}}(d, G)$ the set of possible groups that can appear as the torsion subgroup over any number field L of degree d, of an elliptic curve E defined over the rationals, such that $E(\mathbb{Q})_{\text{tors}} = G$.

Connected to these sets, some known results are:

- Mazur's landmark papers [16,17] established that

$$\Phi(1) = \{\mathcal{C}_n | n = 1, \dots, 10, 12\} \cup \{\mathcal{C}_2 \times \mathcal{C}_{2m} | m = 1, \dots, 4\}.$$

- After this, in a long series of papers by Kenku, Momose and Kamienny ending in [10,11], the quadratic case was given a description:

$$\begin{aligned}\Phi(2) = &\{\mathcal{C}_n | n = 1, \dots, 16, 18\} \cup \{\mathcal{C}_2 \times \mathcal{C}_{2m} | m = 1, \dots, 6\} \\ &\cup \{\mathcal{C}_3 \times \mathcal{C}_{3r} | r = 1, 2\} \cup \{\mathcal{C}_4 \times \mathcal{C}_4\}.\end{aligned}$$

- The sets $\Phi_{\mathbb{Q}}(d)$ have been completely described by Najman [18] for $d = 2, 3$:

$$\begin{aligned}\Phi_{\mathbb{Q}}(2) &= \{\mathcal{C}_n | n = 1, \dots, 10, 12, 15, 16\} \cup \{\mathcal{C}_2 \times \mathcal{C}_{2m} | m = 1, \dots, 6\} \\ &\quad \cup \{\mathcal{C}_3 \times \mathcal{C}_{3r} | r = 1, 2\} \cup \{\mathcal{C}_4 \times \mathcal{C}_4\}, \\ \Phi_{\mathbb{Q}}(3) &= \{\mathcal{C}_n | n = 1, \dots, 10, 12, 13, 14, 18, 21\} \cup \{\mathcal{C}_2 \times \mathcal{C}_{2m} | m = 1, \dots, 4, 7\}.\end{aligned}$$

- The work of Fujita [5] gave the precise list (building upon previous work of Laska and Lorenz [15]) of torsion groups over the maximal elementary abelian 2-extension of $\mathbb{Q}$, of elliptic curves defined over the rationals. The full list of such groups will be denoted by $\Phi_{\mathbb{Q}}(2^\infty)$:

$$\begin{aligned}\Phi_{\mathbb{Q}}(2^\infty) = &\{\mathcal{C}_n | n = 1, 3, 5, 7, 9, 15\} \cup \{\mathcal{C}_2 \times \mathcal{C}_{2m} | m = 1, \dots, 6, 8\} \\ &\cup \{\mathcal{C}_3 \times \mathcal{C}_3\} \cup \{\mathcal{C}_4 \times \mathcal{C}_{4r} | r = 1, \dots, 4\} \cup \{\mathcal{C}_{2s} \times \mathcal{C}_{2s} | s = 3, 4\}.\end{aligned}$$

- The set $\Phi_{\mathbb{Q}}(2, G)$, for non-cyclic G was characterized by Kwon [14].

Finally, in [7], we gave a precise description of the set $\Phi_{\mathbb{Q}}(2, G)$, for all $G \in \Phi(1)$.

Theorem 1 *For $G \in \Phi(1)$, the set $\Phi_{\mathbb{Q}}(2, G)$ is the following:*

G	$\Phi_{\mathbb{Q}}(2, G)$
$\mathcal{C}_1$	$\{\mathcal{C}_1, \mathcal{C}_3, \mathcal{C}_5, \mathcal{C}_7, \mathcal{C}_9\}$
$\mathcal{C}_2$	$\{\mathcal{C}_2, \mathcal{C}_4, \mathcal{C}_6, \mathcal{C}_8, \mathcal{C}_{10}, \mathcal{C}_{12}, \mathcal{C}_{16}, \mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_2 \times \mathcal{C}_6, \mathcal{C}_2 \times \mathcal{C}_{10}\}$
$\mathcal{C}_3$	$\{\mathcal{C}_3, \mathcal{C}_{15}, \mathcal{C}_3 \times \mathcal{C}_3\}$
$\mathcal{C}_4$	$\{\mathcal{C}_4, \mathcal{C}_8, \mathcal{C}_{12}, \mathcal{C}_2 \times \mathcal{C}_4, \mathcal{C}_2 \times \mathcal{C}_8, \mathcal{C}_2 \times \mathcal{C}_{12}, \mathcal{C}_4 \times \mathcal{C}_4\}$
$\mathcal{C}_5$	$\{\mathcal{C}_5, \mathcal{C}_{15}\}$
$\mathcal{C}_6$	$\{\mathcal{C}_6, \mathcal{C}_{12}, \mathcal{C}_2 \times \mathcal{C}_6, \mathcal{C}_3 \times \mathcal{C}_6\}$
$\mathcal{C}_7$	$\{\mathcal{C}_7\}$
$\mathcal{C}_8$	$\{\mathcal{C}_8, \mathcal{C}_{16}, \mathcal{C}_2 \times \mathcal{C}_8\}$
$\mathcal{C}_9$	$\{\mathcal{C}_9\}$
$\mathcal{C}_{10}$	$\{\mathcal{C}_{10}, \mathcal{C}_2 \times \mathcal{C}_{10}\}$
$\mathcal{C}_{12}$	$\{\mathcal{C}_{12}, \mathcal{C}_2 \times \mathcal{C}_{12}\}$
$\mathcal{C}_2 \times \mathcal{C}_2$	$\{\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_2 \times \mathcal{C}_4, \mathcal{C}_2 \times \mathcal{C}_6, \mathcal{C}_2 \times \mathcal{C}_8, \mathcal{C}_2 \times \mathcal{C}_{12}\}$
$\mathcal{C}_2 \times \mathcal{C}_4$	$\{\mathcal{C}_2 \times \mathcal{C}_4, \mathcal{C}_2 \times \mathcal{C}_8, \mathcal{C}_4 \times \mathcal{C}_4\}$
$\mathcal{C}_2 \times \mathcal{C}_6$	$\{\mathcal{C}_2 \times \mathcal{C}_6, \mathcal{C}_2 \times \mathcal{C}_{12}\}$
$\mathcal{C}_2 \times \mathcal{C}_8$	$\{\mathcal{C}_2 \times \mathcal{C}_8\}$

Let us fix now some useful notations:

- We will use letters L and F for generic number fields, whereas K will be reserved for proper quadratic extensions of $\mathbb{Q}$.
- We will denote by $\mathbb{Q}(2^\infty) = \mathbb{Q}\left(\left\{\sqrt{m} | m \in \mathbb{Z}\right\}\right)$, the maximal elementary abelian 2-extension of $\mathbb{Q}$.
- Let E be an elliptic curve defined over a number field L. Without loss of generality we can assume E is defined by a short Weierstrass form
$$E : Y^2 = X^3 + AX + B; \quad A, B \in L,$$
and we will then write,
$$E(L) = \left\{(x, y) \in L^2 | y^2 = x^3 + Ax + B\right\} \cup \{\mathcal{O}\},$$
the set of L-rational points of E, and $\mathcal{O}$ its point at infinity.
- For an elliptic curve E, let Δ_E be, as customary, its discriminant.
- For an elliptic curve E and an integer n, let $E[n]$ be the subgroup of all points whose order is a divisor of n (over $\overline{\mathbb{Q}}$), and let $E(L)[n]$ be the set of points in $E[n]$ with coordinates in L, for any number field L (including the case $L = \mathbb{Q}$).
- Under the same conditions, let $\mathbb{Q}(E[n])$ be the extension generated by all the coordinates of points in $E[n]$.
- For an elliptic curve E defined over the rationals given by a short Weierstrass equation $E : Y^2 = X^3 + AX + B$, and a squarefree integer D, let E_D denote its quadratic twist. That is, the elliptic curve with the Weierstrass equation $E_D : DY^2 = X^3 + AX + B$.

Please mind that, in the sequel, for examples and particular curves we will use the Antwerp–Cremona tables and labels [1,2].

Our aim in this paper is to go further than we did in [7]. More precisely, at the end of [7] we posed three questions (named Problems 1, 2 and 3). Problems 1 and 3 are generalized in the following question:

Question For a given $G \in \Phi(1)$, let $S = \{H_1, \ldots, H_n\} \subset \Phi_{\mathbb{Q}}(2, G)$. Find if there exists a fixed elliptic curve E defined over the rationals and squarefree integers $D_1, \ldots, D_n$ such that:

- $E(\mathbb{Q})_{\text{tors}} = G$,
- $E(\mathbb{Q}(\sqrt{D_i}))_{\text{tors}} = H_i$, for $i = 1, \ldots, n$,

- $G = E(K)_{\text{tors}}$ for every other quadratic extension $K/\mathbb{Q}$.

We will answer this question, which will imply the solution to Problems 1 and 3 in [7] as a direct corollary.

More precisely, we will prove two main results. First, we will compute explicitly how many quadratic extensions $K/\mathbb{Q}$ one can have with a proper extension of the torsion group for a given curve, depending only on the rational torsion structure. This will be done in the following result:

Theorem 2 *Let be $G \in \Phi(1)$ and $H \in \Phi_{\mathbb{Q}}(2, G)$ such that $G \neq H$. Then the number h of possible quadratic fields K such that $E(\mathbb{Q})_{\text{tors}} = G$ and $E(K)_{\text{tors}} = H$ for a fixed rational elliptic curve E is given in the following table:*

G	H	h
$\mathcal{C}_1$	$\mathcal{C}_3$	1, 2
	$\mathcal{C}_5$	1
	$\mathcal{C}_7$	1
	$\mathcal{C}_9$	1
$\mathcal{C}_2$	$\mathcal{C}_4$	1, 2
	$\mathcal{C}_6$	1, 2
	$\mathcal{C}_8$	1, 2
	$\mathcal{C}_{10}$	1
	$\mathcal{C}_{12}$	1
	$\mathcal{C}_{16}$	1
	$\mathcal{C}_2 \times \mathcal{C}_2$	1
	$\mathcal{C}_2 \times \mathcal{C}_6$	1
	$\mathcal{C}_2 \times \mathcal{C}_{10}$	1
$\mathcal{C}_3$	$\mathcal{C}_{15}$	1
	$\mathcal{C}_3 \times \mathcal{C}_3$	1
$\mathcal{C}_4$	$\mathcal{C}_8$	2
	$\mathcal{C}_{12}$	1
	$\mathcal{C}_2 \times \mathcal{C}_4$	1
	$\mathcal{C}_2 \times \mathcal{C}_8$	1
	$\mathcal{C}_2 \times \mathcal{C}_{12}$	1
	$\mathcal{C}_4 \times \mathcal{C}_4$	1
$\mathcal{C}_5$	$\mathcal{C}_{15}$	1
$\mathcal{C}_6$	$\mathcal{C}_{12}$	2
	$\mathcal{C}_2 \times \mathcal{C}_6$	1
	$\mathcal{C}_3 \times \mathcal{C}_6$	1
$\mathcal{C}_8$	$\mathcal{C}_{16}$	2
	$\mathcal{C}_2 \times \mathcal{C}_8$	1
$\mathcal{C}_{10}$	$\mathcal{C}_2 \times \mathcal{C}_{10}$	1
$\mathcal{C}_{12}$	$\mathcal{C}_2 \times \mathcal{C}_{12}$	1
$\mathcal{C}_2 \times \mathcal{C}_2$	$\mathcal{C}_2 \times \mathcal{C}_4$	1, 2, 3
	$\mathcal{C}_2 \times \mathcal{C}_6$	1
	$\mathcal{C}_2 \times \mathcal{C}_8$	1
	$\mathcal{C}_2 \times \mathcal{C}_{12}$	1
$\mathcal{C}_2 \times \mathcal{C}_4$	$\mathcal{C}_2 \times \mathcal{C}_8$	1, 2
	$\mathcal{C}_4 \times \mathcal{C}_4$	1
$\mathcal{C}_2 \times \mathcal{C}_6$	$\mathcal{C}_2 \times \mathcal{C}_{12}$	1

Once this is done, we will solve a more delicate problem. We will compute, for a given $G \in \Phi(1)$, all the possibilities for $\Phi_{\mathbb{Q}}(2, G)$ that actually appear. That is, the full set:

$$\mathcal{H}_{\mathbb{Q}}(2, G) = \{S_1, \ldots, S_n\}$$

satisfying, for all $i = 1, \ldots, n$, that

$$S_i = [H_1, \ldots, H_m]$$

is a list, with $H_j \in \Phi_{\mathbb{Q}}(2, G)\backslash\{G\}$, and there exists an elliptic curve E_i defined over $\mathbb{Q}$ such that:

- $E_i(\mathbb{Q})_{\text{tors}} = G$,
- there are quadratic fields $K_1, \ldots, K_m$ with $E_i(K_j)_{\text{tors}} = H_j$, for all $j = 1, \ldots, m$,
- $E_i(K)_{\text{tors}} = G$, for any other quadratic extension $K/\mathbb{Q}$.

Note that we are admitting the possibility of two (or more) of the H_j being identical. We describe explicitly $\mathcal{H}_{\mathbb{Q}}(2, G)$ in Theorem 3.

Theorem 3 *Let be* $G \in \Phi(1)$ *such that* $\Phi_{\mathbb{Q}}(2, G) \neq \{G\}$. *Then:*

G	$\mathcal{H}_{\mathbb{Q}}(2, G)$
$\mathcal{C}_1$	$\mathcal{C}_3$
	$\mathcal{C}_5$
	$\mathcal{C}_7$
	$\mathcal{C}_9$
	$\mathcal{C}_3, \mathcal{C}_3$
	$\mathcal{C}_3, \mathcal{C}_5$
$\mathcal{C}_2$	$\mathcal{C}_2 \times \mathcal{C}_2$
	$\mathcal{C}_2 \times \mathcal{C}_6$
	$\mathcal{C}_2 \times \mathcal{C}_{10}$
	$\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_6$
	$\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_{10}$
	$\mathcal{C}_2 \times \mathcal{C}_6, \mathcal{C}_6$
	$\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_4, \mathcal{C}_4$
	$\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_6, \mathcal{C}_6$
	$\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_8, \mathcal{C}_8$
	$\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_4, \mathcal{C}_8$
	$\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_4, \mathcal{C}_{12}$
	$\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_4, \mathcal{C}_{16}$
	$\mathcal{C}_2 \times \mathcal{C}_6, \mathcal{C}_4, \mathcal{C}_4$
	$\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_4, \mathcal{C}_4, \mathcal{C}_6$
$\mathcal{C}_3$	$\mathcal{C}_{15}$
	$\mathcal{C}_3 \times \mathcal{C}_3$
$\mathcal{C}_4$	$\mathcal{C}_2 \times \mathcal{C}_4$
	$\mathcal{C}_2 \times \mathcal{C}_8$
	$\mathcal{C}_2 \times \mathcal{C}_{12}$
	$\mathcal{C}_4 \times \mathcal{C}_4$
	$\mathcal{C}_2 \times \mathcal{C}_4, \mathcal{C}_{12}$
	$\mathcal{C}_2 \times \mathcal{C}_4, \mathcal{C}_8, \mathcal{C}_8$
	$\mathcal{C}_2 \times \mathcal{C}_8, \mathcal{C}_8, \mathcal{C}_8$

(continued)

$\mathcal{C}_5$	$\mathcal{C}_{15}$
$\mathcal{C}_6$	$\mathcal{C}_2 \times \mathcal{C}_6$
	$\mathcal{C}_2 \times \mathcal{C}_6, \mathcal{C}_3 \times \mathcal{C}_6$
	$\mathcal{C}_2 \times \mathcal{C}_6, \mathcal{C}_{12}, \mathcal{C}_{12}$
$\mathcal{C}_8$	$\mathcal{C}_2 \times \mathcal{C}_8$
	$\mathcal{C}_2 \times \mathcal{C}_8, \mathcal{C}_{16}, \mathcal{C}_{16}$
$\mathcal{C}_{10}$	$\mathcal{C}_2 \times \mathcal{C}_{10}$
$\mathcal{C}_{12}$	$\mathcal{C}_2 \times \mathcal{C}_{12}$
$\mathcal{C}_2 \times \mathcal{C}_2$	$\mathcal{C}_2 \times \mathcal{C}_4$
	$\mathcal{C}_2 \times \mathcal{C}_6$
	$\mathcal{C}_2 \times \mathcal{C}_8$
	$\mathcal{C}_2 \times \mathcal{C}_{12}$
	$\mathcal{C}_2 \times \mathcal{C}_4, \mathcal{C}_2 \times \mathcal{C}_4$
	$\mathcal{C}_2 \times \mathcal{C}_4, \mathcal{C}_2 \times \mathcal{C}_6$
	$\mathcal{C}_2 \times \mathcal{C}_4, \mathcal{C}_2 \times \mathcal{C}_8$
	$\mathcal{C}_2 \times \mathcal{C}_4, \mathcal{C}_2 \times \mathcal{C}_4, \mathcal{C}_2 \times \mathcal{C}_4$
	$\mathcal{C}_2 \times \mathcal{C}_4, \mathcal{C}_2 \times \mathcal{C}_4, \mathcal{C}_2 \times \mathcal{C}_8$
$\mathcal{C}_2 \times \mathcal{C}_4$	$\mathcal{C}_2 \times \mathcal{C}_8$
	$\mathcal{C}_4 \times \mathcal{C}_4$
	$\mathcal{C}_2 \times \mathcal{C}_8, \mathcal{C}_4 \times \mathcal{C}_4$
	$\mathcal{C}_2 \times \mathcal{C}_8, \mathcal{C}_2 \times \mathcal{C}_8$
	$\mathcal{C}_2 \times \mathcal{C}_8, \mathcal{C}_2 \times \mathcal{C}_8, \mathcal{C}_4 \times \mathcal{C}_4$
$\mathcal{C}_2 \times \mathcal{C}_6$	$\mathcal{C}_2 \times \mathcal{C}_{12}$

In particular, we obtain the following corollary:

Corollary 4 *If E is an elliptic curve defined over $\mathbb{Q}$, then there are at most four quadratic fields K_i, $i = 1, \ldots, 4$, such that $E(K_i)_{\text{tors}} \neq E(\mathbb{Q})_{\text{tors}}$. That is,*

$$\max_{G \in \Phi(1)} \left\{ \#S | S \in \mathcal{H}_{\mathbb{Q}}(2, G) \right\} = 4.$$

We would like to mention this last result has also been proved independently by Najman [19]. His proof uses a very different kind of argument and, in particular, Theorems 2 and 3 do not follow from his results.

2 Some technical results

Aside from the above main results, a number of auxiliary results are needed for our arguments.

We already mentioned this result by Fujita:

Theorem 5 [5, Theorem 2] *Let E be an elliptic curve over $\mathbb{Q}$. Then, the torsion subgroup $E(\mathbb{Q}(2^\infty))_{\text{tors}}$ is isomorphic to one of the following 20 groups:*

$$\begin{array}{ll} \mathcal{C}_N & \text{for } N = 1, 3, 5, 7, 9, 15; \\ \mathcal{C}_2 \times \mathcal{C}_{2N} & \text{for } N = 1, \dots, 6, 8; \\ \mathcal{C}_4 \times \mathcal{C}_{4N} & \text{for } N = 1, \dots, 4; \\ \mathcal{C}_{2N} \times \mathcal{C}_{2N} & \text{for } N = 3, 4; \\ \mathcal{C}_3 \times \mathcal{C}_3. & \end{array}$$

In the same paper one can find the following useful result:

Proposition 6 [5, Proposition 11] *Let E be an elliptic curve over $\mathbb{Q}$ such that $E(\mathbb{Q})_{\text{tors}}$ is cyclic. Then $\mathcal{C}_8 \times \mathcal{C}_8 \not\leq E(\mathbb{Q}(2^\infty))_{\text{tors}}$.*

A classical result which could be found, for instance, in [20, Corollary 8.1.1] is the following:

Proposition 7 *Let E be an elliptic curve over a number field L. If $\mathcal{C}_m \times \mathcal{C}_m = E[m] \leq E(L)$, then L contains the cyclotomic field generated by the m-th roots of unity.*

In another paper by Fujita [4], the following two results can be found:

Theorem 8 [4, Theorem 1] *Let E be an elliptic curve over $\mathbb{Q}$ such that $E(\mathbb{Q})_{\text{tors}}$ is non-cyclic.*

- *If $E(\mathbb{Q})_{\text{tors}} = \mathcal{C}_2 \times \mathcal{C}_8$, then $E(\mathbb{Q}(2^\infty))_{\text{tors}} = \mathcal{C}_4 \times \mathcal{C}_{16}$.*
- *If $E(\mathbb{Q})_{\text{tors}} = \mathcal{C}_2 \times \mathcal{C}_6$, then $E(\mathbb{Q}(2^\infty))_{\text{tors}} = \mathcal{C}_4 \times \mathcal{C}_{12}$.*
- *If $E(\mathbb{Q})_{\text{tors}} = \mathcal{C}_2 \times \mathcal{C}_4$, then $E(\mathbb{Q}(2^\infty))_{\text{tors}} \in \{\mathcal{C}_4 \times \mathcal{C}_8, \mathcal{C}_8 \times \mathcal{C}_8\}$.*
- *If $E(\mathbb{Q})_{\text{tors}} = \mathcal{C}_2 \times \mathcal{C}_2$, then $E(\mathbb{Q}(2^\infty))_{\text{tors}} \in \{\mathcal{C}_4 \times \mathcal{C}_4, \mathcal{C}_4 \times \mathcal{C}_8, \mathcal{C}_8 \times \mathcal{C}_8, \mathcal{C}_4 \times \mathcal{C}_{12}, \mathcal{C}_4 \times \mathcal{C}_{16}\}$.*

Proposition 9 [4, Final remark] *The minimal d for which the following groups can be realized as $E(L_d)_{\text{tors}}$ with some elliptic curve E defined over $\mathbb{Q}$, having non-cyclic rational torsion, and some polyquadratic field L_d with $[L_d : \mathbb{Q}] = 2^d$, is:*

1. *$d = 4$ for $\mathcal{C}_4 \times \mathcal{C}_{16}$.*
2. *$d = 3$ for $\mathcal{C}_4 \times \mathcal{C}_{12}$.*
3. *$d = 4$ for $\mathcal{C}_8 \times \mathcal{C}_8$.*
4. *For all other types, we have $d = 2$.*

3 On 2-divisibility

In this section we are going to use two methods that allow us to decide when there exists a point (or where to look for it) which divides by two a given point of some order. The first method is classical in the literature of elliptic curves [12, Theorem 4.2]. It allows us to decide if a point defined over a number field L containing $\mathbb{Q}(E[2])$ is half a point over L too.

Lemma 10 *Let E be an elliptic curve defined over a number field L given by*

$$E : Y^2 = (X - \alpha)(X - \beta)(X - \gamma),$$

with $\alpha, \beta, \gamma \in L$. For $P = (x_0, y_0) \in E(L)$, there exists $Q \in E(L)$ such that $2Q = P$ if and only if $x_0 - \alpha$, $x_0 - \beta$ and $x_0 - \gamma$ are all squares in L.

For our concerns, this will apply specifically to the following situation:

Proposition 11 *Assume we have an elliptic curve*

$$E:\ Y^2 = X(X-A)(X-B), \quad A, B \in \mathbb{Q}$$

and $\mathcal{C}_2 \times \mathcal{C}_2 \le E(\mathbb{Q})_{\text{tors}}$ and there are no points of order 4 in $E(\mathbb{Q})$. Then, there are 1, 2 or 3 quadratic fields K with $\mathcal{C}_2 \times \mathcal{C}_4 \le E(K)_{\text{tors}}$. All three cases can appear.

Proof Assume that the elliptic curve has $\mathcal{C}_2 \times \mathcal{C}_4 \le E(K)_{\text{tors}}$, with $K = \mathbb{Q}(\sqrt{D})$. Let us first assume that the point who gets divided by two is $(0, 0)$. That is, there is a certain $Q \in E(K)$ such that $2Q = (0, 0)$. By the previous lemma $0, -A, -B$ are then squares in K. This amounts to the existence of $a, b \in \mathbb{Q}$ such that one of the mutually exclusive pairs of equalities holds:

$$\{-A = a^2 D, -B = b^2\} \quad \text{or} \quad \{-A = a^2, -B = b^2 D\} \quad \text{or} \quad \{-A = a^2 D, -B = b^2 D\}.$$

Of these cases, there is only one possible squarefree D satisfying the conditions. The same goes if the divided point is $(A, 0)$ (change $\{A, B\}$ for $\{A, A-B\}$) and if it is $(B, 0)$. All in all there can be 1, 2 or 3 quadratic extensions where the torsion contains $\mathcal{C}_2 \times \mathcal{C}_4$.

In Table 1 (see the appendix for an explanation of the table) one can find an example for each of the three circumstances. □

The second technique is taken from Jeon et al. [9]. This method allows to find, given a point defined over a number field F, an extension L/F and a point defined over L such that it is half of the given point.

Proposition 12 *Let E be an elliptic curve defined over a number field F given by the Weierstrass equation:*

$$E:\ Y^2 = X^3 + AX^2 + BX + y_0^2,$$

and $P = (0, y_0) \in E(F)$. Let α be a root of the quartic polynomial

$$q(x) = x^4 - 2Ax^2 - 8y_0 x + A^2 - 4B.$$

Then the point $Q = ((\alpha^2 - A)/2, \alpha(\alpha^2 - A)/2 - y_0) \in E(L)$, where $L = F(\alpha)$, and $2Q = P$.

It is not difficult to check that the elliptic curve E and the one defined by the quartic polynomial $q(x)$, $v^2 = q(u)$, are isomorphic over F. Then, thanks to [6, Appendix A.2], we know that $q(x)$ splits over a quadratic extension of F for each 2-torsion point of E defined over F.

We will apply this procedure to points of even order N. Note that if $E(\mathbb{Q})_{\text{tors}}$ is cyclic and P, P' are two generators of this cyclic group, then if there exist a number field L and a point $Q \in E(L)$ with $2Q = P$, then there must also be some $Q' \in E(L)$ with $2Q' = P'$. That is, the 2-divisibility holds for either all generators or for none of them.

3.1 The case $N = 2$

Lemma 13 *Let*

$$E:\ Y^2 = X(X^2 + AX + B)$$

be an elliptic curve defined over $\mathbb{Q}$ with $E(\mathbb{Q})_{\text{tors}} = \mathcal{C}_2$. Then, there exists a quadratic field K with $\mathcal{C}_4 \le E(K)_{\text{tors}}$ if and only if $B = s^2$ for some $s \in \mathbb{Q}$.

Moreover, $K = K_\pm := \mathbb{Q}(\sqrt{A \pm 2s})$ in this situation and $K_+ \neq K_-$.

Proof Using Proposition 12, with the point $(0,0)$, we get the roots of the corresponding quartic polynomial $q(x)$ which are

$$\pm\sqrt{A \pm 2\sqrt{B}}.$$

A necessary and sufficient condition then for a point Q to exist over a quadratic field, with $2Q = (0,0)$, is $B = s^2$ for a certain $s \in \mathbb{Q}$. Should this be the case, $Q \in E(K)[4]$, with $K = \mathbb{Q}(\sqrt{A \pm 2s})$.

Please note that we have implicitly assumed that there are no points of order 2 in $E(K')$ other than $(0,0)$ that could be divided by 2 over any quadratic field K'. In fact, this must always be the case, as from [7, Thm. 5 (ii)], $G = \mathcal{C}_2$ implies $\mathcal{C}_2 \times \mathcal{C}_4 \not\leq E(K')_{\text{tors}}$ for any quadratic field K'.

Let us check $K_+ \neq K_-$ for all s. Assume $K_+ = K_-$. Then, $A^2 - 4s^2$ is a rational square. Therefore, $X^2 + AX + s^2$ has two different rational roots. That is, $C_2 \times C_2 \leq E(\mathbb{Q})$, which is a contradiction. □

3.2 The cases $N = 4, 6, 8$

Let $N \geq 4$ be an integer. We are given a curve E defined over a number field L (for our purposes it will mostly be $\mathbb{Q}$, but the result is more general) and a point $P \in E(L)$ of order N, and then we take the Tate normal form of E:

$$\mathcal{T}_{b,c} : \ Y^2 + (1-c)XY - bY = X^3 - bX^2,$$

where $P = (0,0)$. Changing coordinates by means of

$$X \longmapsto X, \quad Y \longmapsto Y + \frac{c-1}{2}x + \frac{b}{2};$$

we obtain a Weierstrass model:

$$\mathcal{T}_{b,c} : \ Y^2 = X^3 + AX^2 + BX + C,$$

with

$$A = \frac{(c-1)^2 - 4b}{4}, \quad B = \frac{b(c-1)}{2}, \quad C = \frac{b^2}{4}.$$

In particular $P = (0, -b/2)$. Then the quartic polynomial $q(x)$ which characterizes the existence of Q such that $2Q = P$ (see Proposition 12) is now:

$$\begin{aligned} q(x) = x^4 &+ \frac{1}{2}(-1 + 4b + 2c - c^2)x^2 + 4bx \\ &+ \frac{1}{16}(1 + 24b + 16b^2 - 4c - 16bc + 6c^2 - 8bc^2 - 4c^3 + c^4). \end{aligned} \tag{1}$$

The Tate normal form also has an important feature, as it parametrizes the different curves defined over the rationals with a common torsion structure [8]. Precisely, if $\mathcal{C}_N \leq E(\mathbb{Q})$, there exists $t \in \mathbb{Q}$ such that E is $\mathbb{Q}$-isomorphic to $\mathcal{T}_{b,c}$ where:

- $c = 0$ and $b = t$ if $N = 4$;
- $c = t$ and $b = t^2 + t$ if $N = 6$;
- $c = (2t-1)(t-1)/t$ and $b = (2t-1)(t-1)$ if $N = 8$.

Lemma 14 *Let E be an elliptic curve defined over $\mathbb{Q}$ with $E(\mathbb{Q})_{\text{tors}} = \mathcal{C}_4$. Let $t \in \mathbb{Q}$ such that E is $\mathbb{Q}$-isomorphic to $\mathcal{T}_{t,0}$. Then, there exists a quadratic field K with $E(K)_{\text{tors}} = \mathcal{C}_8$ if and only if $t = -s^2$ for some $s \in \mathbb{Q}$.*

Moreover, $K = K_\pm := \mathbb{Q}(\sqrt{1 \pm 4s})$ in this situation and $K_+ \neq K_-$.

Proof In this case, the roots of the quartic polynomial given at (1) are

$$\sqrt{-t} \pm \frac{1}{2}\sqrt{1 + 4\sqrt{-t}}, \quad -\sqrt{-t} \pm \frac{1}{2}\sqrt{1 - 4\sqrt{-t}}.$$

A necessary and sufficient condition then for a point Q to exist over a quadratic field, with $2Q = (0, 0)$, is $t = -s^2$ for a certain $s \in \mathbb{Q}$. Should this be the case, $Q \in E(K_\pm)[8]$, with $K_\pm = \mathbb{Q}(\sqrt{1 \pm 4s})$.

As above, it must be $(0, 0)$ the point in $E[4]$ who gets divided by 2. If there were a non-rational point $P \in E(K')$ of order 4 over some quadratic field K' such that there exists $Q \in E(K')$ with $2Q = P$, then $E(K')_{\text{tors}}$ must be a group with an element Q of order 8 which does not generate the whole group (it does not generate $(0, 0)$ in particular), which contradicts our assumption $E(K')_{\text{tors}} = \mathcal{C}_8$.

If $K_+ = K_-$, then $(1+4s)(1-4s)$ is a rational square. Therefore, Δ_E is a rational square. That is, $C_2 \times C_2 \leq E(\mathbb{Q})$, which is a contradiction. □

Remark Note that the assumption $E(K)_{\text{tors}} = \mathcal{C}_8$ is indeed necessary. Since if we relax this hypothesis to $E(K)_{\text{tors}} \leq \mathcal{C}_8$, Lemma 14 is false: the elliptic curve `240d6` has torsion subgroup $\mathcal{C}_4$ (resp. $\mathcal{C}_2 \times \mathcal{C}_8, \mathcal{C}_8, \mathcal{C}_8$) over $\mathbb{Q}$ (resp. $\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{6}), \mathbb{Q}(\sqrt{-6})$) (see Table 1).

Lemma 15 *Let E be an elliptic curve defined over $\mathbb{Q}$ with $E(\mathbb{Q})_{\text{tors}} = \mathcal{C}_6$. Let $t \in \mathbb{Q}$ such that E is $\mathbb{Q}$-isomorphic to $\mathcal{T}_{t^2+t,t}$. Then, there exists a quadratic field K with $\mathcal{C}_{12} \leq E(K)_{\text{tors}}$ if and only if $t = -s^2$ for some $s \in \mathbb{Q}$.*

Moreover, $K = K_\pm := \mathbb{Q}(\sqrt{(1 \pm s)(1 \mp 3s)})$ in this situation and $K_+ \neq K_-$.

Proof In this case, the roots of the polynomial given at (1) are

$$\sqrt{-t} \pm \frac{1}{2}\sqrt{(1 + t)(1 - 4\sqrt{-t} - 3t)}, \quad -\sqrt{-t} \pm \frac{1}{2}\sqrt{(1 + t)(1 + 4\sqrt{-t} - 3t)}.$$

A necessary and sufficient condition then for a point Q to exist over a quadratic field, with $2Q = P$, is $t = -s^2$ for a certain $s \in \mathbb{Q}$. Should this be the case: $Q \in E(K_\pm)[12]$, with $K_\pm = \mathbb{Q}(\sqrt{(1 \pm s)(1 \mp 3s)})$.

Again, the point in $E[6]$ who gets divided by 2 must be rational. This time it is easier, as the only group in $\Phi_{\mathbb{Q}}(2, \mathcal{C}_6)$ with elements of order 12 is precisely $\mathcal{C}_{12}$, so the only two available points are $(0, 0)$ and its inverse, which yield the same situation.

If $K_+ = K_-$ for some s, there exists $r \in \mathbb{Q}$ with

$$(1 + s)(1 - 3s) = r^2(1 - s)(1 + 3s).$$

That is to say, the equation

$$C : z^2 = (1 - s^2)(1 - 9s^2)$$

has a non-trivial rational solution, $s \neq 0, \pm 1, \pm 1/3$ (these solutions correspond to Tate models which do not yield elliptic curves). C defines then an elliptic curve with at least 8 rational points: 6 trivial ones, and 2 more at infinity. But C is $\mathbb{Q}$-isomorphic to `24a1`, whose Mordell group is $\mathcal{C}_2 \times \mathcal{C}_4$. Therefore, the affine points in $C(\mathbb{Q})$ correspond to the trivial points. □

Lemma 16 *Let E be an elliptic curve defined over $\mathbb{Q}$ with $E(\mathbb{Q})_{\text{tors}} = \mathcal{C}_8$. Let $t \in \mathbb{Q}$ such that E is $\mathbb{Q}$-isomorphic to $\mathcal{T}_{(2t-1)(t-1),(2t-1)(t-1)/t}$. Then, there exists a quadratic field K with $\mathcal{C}_{16} \le E(K)_{\text{tors}}$ if and only if $t = s^2/(s^2+1)$ for some $s \in \mathbb{Q}$.*

Moreover, $K = K_\pm := \mathbb{Q}(\sqrt{(s^4-1)(-1 \pm 2s + s^2)})$ in this situation and $K_+ \neq K_-$.

Proof In this case, the roots of the polynomial given at (1) are

$$\sqrt{t(1-t)} \pm \frac{1}{2t}\sqrt{(1-2t)(1-6t+4t^2-4t\sqrt{t(1-t)})},$$
$$-\sqrt{t(1-t)} \pm \frac{1}{2t}\sqrt{(1-2t)(1-6t+4t^2-4t\sqrt{t(1-t)})}.$$

A necessary and sufficient condition then for a point Q to exist over a quadratic field, with $2Q = P$, is $t(1-t) = s^2$ for a certain $s \in \mathbb{Q}$. This equation is a genus zero curve again, parametrized by:

$$t = \frac{r^2}{r^2+1}, \quad s = \frac{r}{r^2+1},$$

for some $r \in \mathbb{Q}$. Should this be the case, $Q \in E(K_\pm)[12]$, with

$$K_\pm = \mathbb{Q}(\sqrt{(r^4-1)(-1 \pm 2r + r^2)}).$$

Once more, the point in $E[8]$ who gets divided by 2 must be rational, as the only group in $\Phi_{\mathbb{Q}}(2, \mathcal{C}_8)$ with elements of order 16 is $\mathcal{C}_{16}$.

Finally, let us check $K_+ \neq K_-$ for all s. If not, there is some $r \in \mathbb{Q}$ with

$$(s^4-1)(-1+2s+s^2) = r^2(s^4-1)(-1-2s+s^2)$$

for a certain s. That implies the equation

$$C: \ z^2 = (-1+2s+s^2)(-1-2s+s^2)$$

has a non-trivial rational solution (non-trivial meaning $s \neq 0$), as the trivial solutions match the Tate models which do not yield elliptic curves. C defines an elliptic curve with at least 4 rational points (2 trivial, 2 at infinity), but in fact it is isomorphic to the curve 32a2 whose Mordell group is $\mathcal{C}_2 \times \mathcal{C}_2$. Hence the affine points in $C(\mathbb{Q})$ are just the trivial points and we are done. □

4 Proof of Theorem 2

For a given $G \in \Phi(1)$ and $H \in \Phi_{\mathbb{Q}}(2, G)$, we calculate the number h of possible quadratic fields K such that, for a given rational elliptic curve E with $E(\mathbb{Q})_{\text{tors}} = G$, we have $E(K)_{\text{tors}} = H$.

4.1 The cyclic case

- Clearly, if $H = \mathcal{C}_2 \times \mathcal{C}_{2m}$ for some integer m, this can only happen over the quadratic field $K = \mathbb{Q}(\sqrt{\Delta_E})$. Note that K is actually always a quadratic extension, as $\mathbb{Q}(E[2]) \neq \mathbb{Q}$. This rules out the cases:
  - $G = \mathcal{C}_2$, $H = \mathcal{C}_2 \times \mathcal{C}_{2m}$, with $m = 1, 3, 5$;
  - $G = \mathcal{C}_4$, $H = \mathcal{C}_2 \times \mathcal{C}_{4m}$, with $m = 1, 2, 3$;
  - $G = \mathcal{C}_r$, $H = \mathcal{C}_2 \times \mathcal{C}_r$, with $r = 6, 8, 10, 12$.

- Assume $G = \mathcal{C}_2$ and $H \leq \mathcal{C}_{4n}$. Lemma 13 shows that there can be 1 or 2 quadratic fields in which this situation holds. When $H = \mathcal{C}_4, \mathcal{C}_8$ in fact both things can happen (see examples in Table 1 at the appendix). However, for the remaining cases, the situation can only hold in one quadratic field. Let us do with a little detail the case $H = \mathcal{C}_{12}$, as the case $H = \mathcal{C}_{16}$ is analogous. So we are assuming $G = \mathcal{C}_2$ and $H = \mathcal{C}_{12}$ for two different quadratic fields. Then, as we also have a quadratic field where the full 2-torsion appears, $\mathcal{C}_6 \times \mathcal{C}_{12}$ should be a subgroup of one of the groups in $\Phi_{\mathbb{Q}}(2^\infty)$, and that is not possible from Theorem 5.
- If $G = \mathcal{C}_{2n}$ and $H = \mathcal{C}_{4n}$ for $n = 2, 3, 4$, Lemmas 14, 15, 16 (respectively) show that there are exactly two quadratic fields where the appropriate torsion extension occurs.
- If $H = \mathcal{C}_4 \times \mathcal{C}_4$ (resp. $H = \mathcal{C}_3 \times \mathcal{C}_{3n}, n = 1, 2$) the quadratic field must be $K = \mathbb{Q}(\sqrt{-1})$ (resp. $K = \mathbb{Q}(\sqrt{-3})$) by 7. This proves the cases

    ◦ $G = \mathcal{C}_4$, $H = \mathcal{C}_4 \times \mathcal{C}_4$;
    ◦ $G = \mathcal{C}_3$, $H = \mathcal{C}_3 \times \mathcal{C}_3$;
    ◦ $G = \mathcal{C}_6$, $H = \mathcal{C}_3 \times \mathcal{C}_6$.

- For any given $G = \mathcal{C}_n$, $H = G \times \mathcal{C}_m$ with $\gcd(n, m) = 1$ can appear at most twice, since $E[m] = \mathcal{C}_m \times \mathcal{C}_m$. More precisely, if $m = 5, 7, 9$ then only one quadratic field may extend the torsion in this way since, if there were two such quadratic fields, the cyclotomic field generated by the m-th roots of unity, $\mathbb{Q}(\zeta_m)$, should be a subfield of the corresponding biquadratic case from Proposition 7, and that is not possible. This proves the cases:

    ◦ $G = \mathcal{C}_1$, $H = \mathcal{C}_m$, with $m = 5, 7, 9$;
    ◦ $G = \mathcal{C}_2$, $H = \mathcal{C}_{10}$;
    ◦ $G = \mathcal{C}_3$, $H = \mathcal{C}_{15}$.

  Now if $m = 3$ then H may appear once or twice. It actually happens twice in the following cases (see examples in Table 1 at the appendix):

    ◦ $G = \mathcal{C}_1$, $H = \mathcal{C}_3$;
    ◦ $G = \mathcal{C}_2$, $H = \mathcal{C}_6$.

- There are only two cases remaining: $G = \mathcal{C}_n$, $H = \mathcal{C}_{3n}$ for $n = 4, 5$. Only one quadratic field is possible in these instances. If there were two quadratic fields where H appears, then $\mathcal{C}_n \times \mathcal{C}_3 \times \mathcal{C}_3$ should be a subgroup of one of the groups in $\Phi_{\mathbb{Q}}(2^\infty)$ for $n = 4, 5$; and that is impossible from Theorem 5.

4.2 The non-cyclic case

Let E be an elliptic curve defined over $\mathbb{Q}$ such that $E(\mathbb{Q})_{\text{tors}} = G$ where G is the following:

- $G = \mathcal{C}_2 \times \mathcal{C}_2$. If $H = \mathcal{C}_2 \times \mathcal{C}_4$ there might be 1, 2 or 3 quadratic extensions, following Proposition 11 in the previous section.
  If $H = \mathcal{C}_2 \times \mathcal{C}_{2n}$ with $n = 3, 6$ appears in two different quadratic extensions, then there are two independent points of order 3 in $\mathbb{Q}(2^\infty)$. As a result, $\mathcal{C}_6 \times \mathcal{C}_6 \leq E(\mathbb{Q}(2^\infty))_{\text{tors}}$, which contradicts Theorem 8.
  If $H = \mathcal{C}_2 \times \mathcal{C}_8$ for two different quadratic extensions, we must have two different points of order 8. Let us call L the composition field of these two quadratic extensions. There are two groups in $\Phi_{\mathbb{Q}}(2^\infty)$ with more than one element of order 8: $\mathcal{C}_4 \times \mathcal{C}_8$ and $\mathcal{C}_8 \times \mathcal{C}_8$. But the first one is not our case: looking at the lattice of subgroups of $\mathcal{C}_4 \times \mathcal{C}_8$ one can realize that both $\mathcal{C}_2 \times \mathcal{C}_8$ have a common subgroup $\mathcal{C}_2 \times \mathcal{C}_4$, while the intersection (in our case) should only be $G = \mathcal{C}_2 \times \mathcal{C}_2$. This implies $E(L)_{\text{tors}}$ had to be $\mathcal{C}_8 \times \mathcal{C}_8$ and

Proposition 9 tells us that under these circumstances $[L : \mathbb{Q}] \geq 16$. Hence only one quadratic extension with $H = \mathcal{C}_2 \times \mathcal{C}_8$ can occur.

- $G = \mathcal{C}_2 \times \mathcal{C}_4$. As we mentioned above, if $H = \mathcal{C}_4 \times \mathcal{C}_4$ the only possible extension is $\mathbb{Q}(\sqrt{-1})/\mathbb{Q}$.
  When $H = \mathcal{C}_2 \times \mathcal{C}_8$ the first part of Lemma 14 can be applied verbatim and it shows that 1 or 2 extensions can appear (both things occur).
- $G = \mathcal{C}_2 \times \mathcal{C}_6$. The only group extension, by Theorem 1 is $H = \mathcal{C}_2 \times \mathcal{C}_{12}$. Lemma 15 tells us (the first part) that either one or two relevant quadratic extensions may appear. Also, from Theorem 8 we know that $E(\mathbb{Q}(2^\infty))_{\text{tors}} = \mathcal{C}_4 \times \mathcal{C}_{12}$, and by Proposition 9 that $E(L)_{\text{tors}} = \mathcal{C}_4 \times \mathcal{C}_{12}$ implies $[L : \mathbb{Q}] \geq 8$.
  But, if there were two quadratic extensions, K_1, K_2 with $E(K_i)_{\text{tors}} = \mathcal{C}_2 \times \mathcal{C}_{12}$, let us write F the composite of K_1 and K_2 (in particular, $[F : \mathbb{Q}] = 4$). Then clearly $E(F)_{\text{tors}} = \mathcal{C}_4 \times \mathcal{C}_{12}$, because it must be contained in $E(\mathbb{Q}(2^\infty))_{\text{tors}}$ and it should be strictly bigger than both $E(K_i)_{\text{tors}}$.
  This is a contradiction and therefore, only one quadratic extension K can appear with $E(K)_{\text{tors}} = H = \mathcal{C}_2 \times \mathcal{C}_{12}$.

Remark These two last cases can also be found in [14], but the proofs there are longer, as we can take advantage of the many results which have appeared concerning this matter since (specially those in [4,5]).

5 Proof of Theorem 3

Now we are going to prove Theorem 3. For this purpose, for a given $G \in \Phi(1)$ let us build a set $\mathcal{S}(G)$ consisting of the groups $H \in \Phi_{\mathbb{Q}}(2, G)\backslash\{G\}$, repeated as many times as the number of possible quadratic fields where H appears in Theorem 2. Our task is checking, for any subset $S \in \mathcal{S}(G)$ if S belongs to $\mathcal{H}_{\mathbb{Q}}(2, G)$ or not.

Example As

$$\Phi_{\mathbb{Q}}(2, \mathcal{C}_1) = \{\mathcal{C}_1, \mathcal{C}_3, \mathcal{C}_5, \mathcal{C}_7, \mathcal{C}_9\}$$

and Theorem 2 tells us that two quadratic extensions can appear with torsion group $\mathcal{C}_3$, we have

$$\begin{aligned} \mathcal{S}(\mathcal{C}_1) = \Big\{ & [\mathcal{C}_3];\ [\mathcal{C}_5];\ [\mathcal{C}_7];\ [\mathcal{C}_9];\ [\mathcal{C}_3, \mathcal{C}_3];\ [\mathcal{C}_3, \mathcal{C}_5];\ [\mathcal{C}_3, \mathcal{C}_7];\ [\mathcal{C}_3, \mathcal{C}_9]; \\ & [\mathcal{C}_5, \mathcal{C}_7];\ [\mathcal{C}_5, \mathcal{C}_9];\ [\mathcal{C}_7, \mathcal{C}_9];\ [\mathcal{C}_3, \mathcal{C}_3, \mathcal{C}_5];\ [\mathcal{C}_3, \mathcal{C}_3, \mathcal{C}_7];\ [\mathcal{C}_3, \mathcal{C}_3, \mathcal{C}_9]; \\ & [\mathcal{C}_3, \mathcal{C}_5, \mathcal{C}_7];\ [\mathcal{C}_3, \mathcal{C}_5, \mathcal{C}_9];\ [\mathcal{C}_3, \mathcal{C}_7, \mathcal{C}_9];\ [\mathcal{C}_5, \mathcal{C}_7, \mathcal{C}_9];\ [\mathcal{C}_3, \mathcal{C}_3, \mathcal{C}_5, \mathcal{C}_7]; \\ & [\mathcal{C}_3, \mathcal{C}_3, \mathcal{C}_5, \mathcal{C}_9];\ [\mathcal{C}_3, \mathcal{C}_3, \mathcal{C}_7, \mathcal{C}_9];\ [\mathcal{C}_3, \mathcal{C}_5, \mathcal{C}_7, \mathcal{C}_9];\ [\mathcal{C}_3, \mathcal{C}_3, \mathcal{C}_5, \mathcal{C}_7, \mathcal{C}_9] \Big\}. \end{aligned}$$

Mind that at Table 1 we have (for all $G \in \Phi(1)$) examples of elliptic curves over $\mathbb{Q}$ satisfying the conditions in Theorem 3, for any $S \in \mathcal{H}_{\mathbb{Q}}(2, G)$. Therefore, now we have to prove that there does not exist any other possible $S \in \mathcal{S}(G)$.

Remark Let be $G \in \Phi(1)$ cyclic and of even order. Then, for any $S \in \mathcal{H}_{\mathbb{Q}}(2, G)$ there always exists a unique non-cyclic $H \in S$, the one corresponding to $\mathbb{Q}(E[2])$ (a quadratic extension in this case), where E is the elliptic curve associated to S.

5.1 The groups $\mathcal{C}_7, \mathcal{C}_9, \mathcal{C}_2 \times \mathcal{C}_8$

These are the easiest cases, since by Theorem 1 we have that these groups are stable under all quadratic extensions. Therefore, in these cases,

$$\mathcal{H}_{\mathbb{Q}}(2, G) = \emptyset.$$

5.2 The groups $\mathcal{C}_5, \mathcal{C}_{10}, \mathcal{C}_{12}, \mathcal{C}_2 \times \mathcal{C}_6$

Using Theorem 2, these cases are almost as easy as the previous ones, since we have that $\mathcal{S}(G)$ has only one element and we have examples in Table 1 for any of those cases, we obtain that

$$\mathcal{H}_{\mathbb{Q}}(2, G) = \mathcal{S}(G).$$

5.3 The group $\mathcal{C}_1$

Consider the groups in $\Phi_{\mathbb{Q}}(2, \mathcal{C}_1)$. Mind that the intersection of two groups must be trivial in this case, hence we must look for (two or more) elements in $\Phi_{\mathbb{Q}}(2, \mathcal{C}_1)$, other than $\mathcal{C}_1$, such that their product lies in $\Phi_{\mathbb{Q}}(2^\infty)$. From that, we easily deduce that

$$\mathcal{H}_{\mathbb{Q}}(2, \mathcal{C}_1) = \Big\{[\mathcal{C}_3];\, [\mathcal{C}_5];\, [\mathcal{C}_7];\, [\mathcal{C}_9];\, [\mathcal{C}_3, \mathcal{C}_3];\, [\mathcal{C}_3, \mathcal{C}_5]\Big\}.$$

5.4 The group $\mathcal{C}_3$

From all cases in $\mathcal{S}(\mathcal{C}_3)$, the only case to discard is $S = [\mathcal{C}_3 \times \mathcal{C}_3, \mathcal{C}_{15}]$. In that case, $\mathcal{C}_3 \times \mathcal{C}_{15}$ should be a subgroup of some group in $\Phi_{\mathbb{Q}}(2^\infty)$. But this does not happen.

$$\mathcal{H}_{\mathbb{Q}}(2, \mathcal{C}_3) = \Big\{[\mathcal{C}_3 \times \mathcal{C}_3];\, [\mathcal{C}_{15}]\Big\}.$$

5.5 The group $\mathcal{C}_8$

By the previous remark, Theorem 2 and Lemma 16 we have that the only possible subsets in $\mathcal{S}(\mathcal{C}_8)$ are $[\mathcal{C}_2 \times \mathcal{C}_8]$ and $[\mathcal{C}_2 \times \mathcal{C}_8, \mathcal{C}_{16}, \mathcal{C}_{16}]$. Mind that $\mathcal{C}_{16}$ appears twice or it does not appear at all, from Lemma 16. Since we have examples in Table 1 for those cases, we have proved:

$$\mathcal{H}_{\mathbb{Q}}(2, \mathcal{C}_8) = \Big\{[\mathcal{C}_2 \times \mathcal{C}_8];\, [\mathcal{C}_2 \times \mathcal{C}_8, \mathcal{C}_{16}, \mathcal{C}_{16}]\Big\}.$$

5.6 The group $\mathcal{C}_2 \times \mathcal{C}_4$

As previously, we have examples in Table 1 for any subset in $\mathcal{S}(\mathcal{C}_2 \times \mathcal{C}_4)$, which proves:

$$\begin{aligned}\mathcal{H}_{\mathbb{Q}}(2, \mathcal{C}_2 \times \mathcal{C}_4) = \Big\{&[\mathcal{C}_2 \times \mathcal{C}_8];\, [\mathcal{C}_4 \times \mathcal{C}_4];\, [\mathcal{C}_2 \times \mathcal{C}_8, \mathcal{C}_2 \times \mathcal{C}_8];\, [\mathcal{C}_2 \times \mathcal{C}_8, \mathcal{C}_4 \times \mathcal{C}_4];\\ &[\mathcal{C}_2 \times \mathcal{C}_8, \mathcal{C}_2 \times \mathcal{C}_8, \mathcal{C}_4 \times \mathcal{C}_4]\Big\}.\end{aligned}$$

5.7 The group $\mathcal{C}_6$

From the examples in Table 1 the only case to discard is $S = [\mathcal{C}_2 \times \mathcal{C}_6, \mathcal{C}_3 \times \mathcal{C}_6, \mathcal{C}_{12}, \mathcal{C}_{12}]$ (as above, Lemma 15 implies that $\mathcal{C}_{12}$ appears twice if it does). But if there exists an elliptic curve E over $\mathbb{Q}$ such that over four quadratic fields has those torsion subgroups, then $\mathcal{C}_3 \times \mathcal{C}_{12}$

is a subgroup of $E(\mathbb{Q}(2^\infty))_{\text{tors}}$. But no group of $\Phi_\mathbb{Q}(2^\infty)$ has such subgroups from Theorem 5. Therefore we have proved:

$$\mathcal{H}_\mathbb{Q}(2, \mathcal{C}_6) = \Big\{[\mathcal{C}_2 \times \mathcal{C}_6]; [\mathcal{C}_2 \times \mathcal{C}_6, \mathcal{C}_3 \times \mathcal{C}_6]; [\mathcal{C}_2 \times \mathcal{C}_6, \mathcal{C}_{12}, \mathcal{C}_{12}]\Big\}.$$

5.8 The group $\mathcal{C}_4$

There must always be exactly one non-cyclic group, and Lemma 14 tells us that $\mathcal{C}_8$, if it appears in a quadratic extension, then it appears in two quadratic extensions. So, a quick comparison between $\mathcal{S}(\mathcal{C}_4)$ and $\mathcal{H}_\mathbb{Q}(2, \mathcal{C}_4)$ in Theorem 3 tells us that it suffices to prove two assertions.

First, there does not exist $S \in \mathcal{H}_\mathbb{Q}(2, \mathcal{C}_4)$ such that one of the following facts happens:

- $H_1, H_2 \in S$ such that $\mathcal{C}_8 \le H_1$ and $\mathcal{C}_{12} \le H_2$;
- $H_1, H_2 \in S$ such that $H_1 = H_2 = \mathcal{C}_{12}$.

Note that there does not exist $H \in \Phi_\mathbb{Q}(2^\infty)$ with elements of order 8 and 12. This proves the first point. On the other hand, $\mathcal{C}_{12}$ cannot appear twice in an element in S, since that would imply there should exist $H \in \Phi_\mathbb{Q}(2^\infty)$ with $\mathcal{C}_3 \times \mathcal{C}_{12} \le H$. But that is impossible too from Theorem 5.

Second and last, we need to prove that if $\mathcal{C}_4 \times \mathcal{C}_4 \in S$, then $S = [\mathcal{C}_4 \times \mathcal{C}_4]$. That is, we have to discard the following elements in $\mathcal{S}(\mathcal{C}_4)$:

$$[\mathcal{C}_4 \times \mathcal{C}_4, \mathcal{C}_{12}], \quad [\mathcal{C}_4 \times \mathcal{C}_4, \mathcal{C}_8, \mathcal{C}_8].$$

Let us prove first $[\mathcal{C}_4 \times \mathcal{C}_4, \mathcal{C}_{12}] \notin \mathcal{S}(\mathcal{C}_4)$. Suppose that there exists an elliptic curve E over $\mathbb{Q}$ and a squarefree integer D such that $E(\mathbb{Q}(\sqrt{D}))_{\text{tors}} = \mathcal{C}_{12}$ and $E(\mathbb{Q}(\sqrt{-1}))_{\text{tors}} = \mathcal{C}_4 \times \mathcal{C}_4$. Let us denote by $L = \mathbb{Q}(\sqrt{D}, \sqrt{-1})$. In our situation $\mathcal{C}_6 \le E_D(\mathbb{Q})_{\text{tors}}$ from [7, Cor. 4] and $\mathcal{C}_2 \times \mathcal{C}_6 \le E_D(\mathbb{Q}(\sqrt{-1}))_{\text{tors}}$. Let $t \in \mathbb{Q}$ be the relevant parameter in the Tate model of E_D (the one we recalled in Sect. 3.1). That is, we can find a $\mathbb{Q}$-isomorphism such that a model for E_D is:

$$Y^2 = (X - t)\left(X^2 - \frac{1}{4}(3t^2 + 2t - 1)X - \frac{t}{4}(t^2 + 2t + 1)\right).$$

Now, since $\mathcal{C}_2 \times \mathcal{C}_2 < E_D(\mathbb{Q}(\sqrt{-1}))_{\text{tors}}$, this means the discriminant of E_D is a square in $\mathbb{Q}(\sqrt{-1})$ (and not in $\mathbb{Q}$), which implies $(1+t)(1+9t) = -r^2$ for some $r \in \mathbb{Q}$. Parametrizing this conic we obtain

$$t = -\frac{81m^2 + 1}{9(9m^2 + 1)}$$

for some $m \in \mathbb{Q}$. Taking this back to the equation above we have the points of order 2: $(A \pm B\sqrt{-1}, 0)$, $(t, 0)$ where

$$A = -\frac{4(1 + 36m^2 + 243m^4)}{27(1 + 9m^2)^3} \text{ and } B = -\frac{24(m + 9m^3)}{27(1 + 9m^2)^3}. \tag{2}$$

Using

$$E(\mathbb{Q}(\sqrt{D}))_{\text{tors}} = \mathcal{C}_{12}, \quad E(\mathbb{Q}(\sqrt{-1}))_{\text{tors}} = \mathcal{C}_4 \times \mathcal{C}_4,$$

we have $E(L)_{\text{tors}} = \mathcal{C}_4 \times \mathcal{C}_{12}$ from Theorem 5. Therefore

$$E_D(L)_{\text{tors}} = \mathcal{C}_4 \times \mathcal{C}_{12},$$

since E and E_D are isomorphic over $\mathbb{Q}(\sqrt{D})$. Let us prove that this is impossible. Assume that all the points of order 2 can be divided by two in L. In particular, there should exist $\gamma \in L$ such that $A \pm B\sqrt{-1} = \gamma^2$. If

$$\gamma = a_0 + a_1\sqrt{-1} + a_2\sqrt{D} + a_3\sqrt{-D},$$

then it is a straightforward computation to check that a necessary condition is that $\gamma = a + b\sqrt{-1}$ or $\gamma = a\sqrt{D} + b\sqrt{-D}$ for some $a, b \in \mathbb{Q}$. Assuming that γ is of one of the forms above, the equality $A \pm B\sqrt{-1} = \gamma^2$ holds if and only if $A = (a^2 - b^2)r$ and $B = 2abr$, where $r = 1$ or $r = D$. Solving this equations on the variables a and b and using the definition of A and B from (2) we obtain

$$a = \pm\frac{2m}{1+9m^2}\sqrt{\frac{2}{3r}}\left(1 + 27m^2 \pm \sqrt{(1+9m^2)(1+81m^2)}\right)^{-\frac{1}{2}}.$$

Then a necessary condition for $a \in \mathbb{Q}$ is that $(1+9m^2)(1+81m^2) = s^2$ for some $s \in \mathbb{Q}$. This equation defines an elliptic curve (`48a1`) over $\mathbb{Q}$, whose Mordell group is $\mathcal{C}_2 \times \mathcal{C}_2$. But apart form the points at infinity, these points correspond to $m = 0$, and this value gives us a Tate model which does not yield an elliptic curve (it corresponds to $t = -1/9$). This proves $[\mathcal{C}_4 \times \mathcal{C}_4, \mathcal{C}_{12}] \notin \mathcal{S}(\mathcal{C}_4)$.

Finally then, let us prove $[\mathcal{C}_4 \times \mathcal{C}_4, \mathcal{C}_8, \mathcal{C}_8] \notin \mathcal{S}(\mathcal{C}_4)$. That is, we have to prove that, if an elliptic curve E over $\mathbb{Q}$ has $E(\mathbb{Q})_{\rm tors} = \mathcal{C}_4$ then there does not exist a squarefree integer D such that $E(\mathbb{Q}(\sqrt{D}))_{\rm tors} = \mathcal{C}_8$ and $E(\mathbb{Q}(\sqrt{-1}))_{\rm tors} = \mathcal{C}_4 \times \mathcal{C}_4$.

If $\mathcal{C}_8 = E(K)_{\rm tors}$ for some quadratic field K then $t = -s^2$ for some $s \in \mathbb{Q}$ from Lemma 14; where t is the relevant parameter in the Tate model of E. That is:

$$E : Y^2 = X^3 + \frac{1}{4}\left(1 + 4s^2\right)X^2 + \frac{s^2}{2}X + \frac{s^4}{4}.$$

As $E(\mathbb{Q}(\sqrt{-1}))_{\rm tors} = \mathcal{C}_4 \times \mathcal{C}_4$ it must have full 2-torsion over $\mathbb{Q}(\sqrt{-1})$ and that means Δ_E is a square in $\mathbb{Q}(\sqrt{-1})$. This implies $1 - 16s^2$ is a square in $\mathbb{Q}(\sqrt{-1})$ (and not in $\mathbb{Q}$), and hence we can write

$$1 - 16s^2 = -r^2,$$

for some $r \in \mathbb{Q}$. Parametrizing this conic we obtain

$$s = \frac{m^2 + 4m + 5}{4(m+1)(m+3)}, \quad r = \frac{2(2+m)}{(m+1)(m+3)},$$

for some $m \in \mathbb{Q}$. Taking this back to the equation of E we find that the full 2-torsion is given by points $(\alpha_i, 0)$, $i = 1, 2, 3$, where

$$\alpha_1 = -\frac{(m+2+\sqrt{-1})^2}{8(m+1)(m+3)}, \quad \alpha_2 = -\frac{(m+2-\sqrt{-1})^2}{8(m+1)(m+3)}, \quad \alpha_3 = -\frac{(5+4m+m^2)^2}{16(m+1)^2(m+3)^2}.$$

As $E(\mathbb{Q}(\sqrt{-1}))_{\rm tors} = \mathcal{C}_4 \times \mathcal{C}_4$, all these points can be halved in $\mathbb{Q}(\sqrt{-1})$, so, by Lemma 13, $\alpha_i - \alpha_j$ must be a square in $\mathbb{Q}(\sqrt{-1})$ for all $i, j \in \{1, 2, 3\}$. In particular

$$\alpha_1 - \alpha_2 = -\frac{(m+2)}{2(m+1)(m+3)}\sqrt{-1}.$$

That is $\alpha_1 - \alpha_2 = r\sqrt{-1}$ where $r \in \mathbb{Q}$. So, if $\alpha_1 - \alpha_2 = \beta^2$ for some $\beta = a + b\sqrt{-1} \in \mathbb{Q}(\sqrt{-1})$, it must be $b = \pm a$, and $\beta = a \pm a\sqrt{-1}$. Then

$$-\frac{(m+2)}{2(m+1)(m+3)} = \pm 2a^2,$$

otherwise said,

$$(m+1)(m+2)(m+3) = \pm z^2,$$

for some $z \in \mathbb{Q}$. These two equations define elliptic curves over $\mathbb{Q}$ and in fact both are isomorphic to `32a2`, whose Mordell group is $\mathcal{C}_2 \times \mathcal{C}_2$. So, the only available solutions are the trivial ones ($z = 0$) given by $m = -1, -2, -3$. But $m = -1, -3$ are not available in the parametrization above (as they divide the numerator of s), while $m = -2$ gives us a Tate model which does not yield an elliptic curve (it corresponds to $t = -1/16$).

Therefore we have proved:

$$\mathcal{H}_{\mathbb{Q}}(2, \mathcal{C}_4) = \Big\{[\mathcal{C}_2 \times \mathcal{C}_4]; [\mathcal{C}_2 \times \mathcal{C}_8]; [\mathcal{C}_2 \times \mathcal{C}_{12}], [\mathcal{C}_4 \times \mathcal{C}_4]; \\ [\mathcal{C}_2 \times \mathcal{C}_4, \mathcal{C}_{12}]; [\mathcal{C}_2 \times \mathcal{C}_4, \mathcal{C}_8, \mathcal{C}_8]; [\mathcal{C}_2 \times \mathcal{C}_8, \mathcal{C}_8, \mathcal{C}_8]\Big\}.$$

5.9 The group $\mathcal{C}_2 \times \mathcal{C}_2$

As before, a comparison between $\mathcal{S}(\mathcal{C}_2 \times \mathcal{C}_2)$ and $\mathcal{H}_{\mathbb{Q}}(2, \mathcal{C}_2 \times \mathcal{C}_2)$ (shown in Table 1 at the appendix) tells us that the proof for this case amounts to proving that, for any $S \in \mathcal{S}(\mathcal{C}_2 \times \mathcal{C}_2)$:

1. If $\mathcal{C}_2 \times \mathcal{C}_{12} \in S$, then $S = [\mathcal{C}_2 \times \mathcal{C}_{12}]$: Suppose that there exists another $H \in \Phi_{\mathbb{Q}}(2, \mathcal{C}_2 \times \mathcal{C}_2)$ such that $H \in S$. Then there exists an elliptic curve defined over $\mathbb{Q}$ and two squarefree integers D, D' such that $E(\mathbb{Q}(\sqrt{D}))_{\text{tors}} = \mathcal{C}_2 \times \mathcal{C}_{12}$ and $E(\mathbb{Q}(\sqrt{D'}))_{\text{tors}} = H$.
   - Suppose that $H = \mathcal{C}_2 \times \mathcal{C}_4$. Then there is a point of order 12 and a point of order 4 in different fields, and therefore they generate different rational points of order 4. That implies we may have $\mathcal{C}_4 \times \mathcal{C}_{12}$ over the biquadratic field $\mathbb{Q}(\sqrt{D}, \sqrt{D'})$, but Proposition 9 tells us that this group can only appear at degree 2^3 or larger.
   - Suppose that $H = \mathcal{C}_2 \times \mathcal{C}_6$. Then we would have $\mathcal{C}_6 \times \mathcal{C}_6 \leq E(\mathbb{Q}(2^\infty))_{\text{tors}}$. This contradicts Theorem 8.
   - Finally, assume that $H = \mathcal{C}_2 \times \mathcal{C}_8$. Then $\mathcal{C}_8 \times \mathcal{C}_{12} \leq E(\mathbb{Q}(2^\infty))_{\text{tors}}$. This again contradicts Theorem 8.
2. $[\mathcal{C}_2 \times \mathcal{C}_6, \mathcal{C}_2 \times \mathcal{C}_8] \not\subset S$. Were this the case we would have $\mathcal{C}_6 \times \mathcal{C}_8 \leq E(\mathbb{Q}(2^\infty))_{\text{tors}}$ which is not possible (Theorem 8).
3. $S \neq [\mathcal{C}_2 \times \mathcal{C}_6, \mathcal{C}_2 \times \mathcal{C}_4, \mathcal{C}_2 \times \mathcal{C}_4]$. We will not give full details here, as they are similar to those in the previous subsection. Let E be an elliptic curve defined over $\mathbb{Q}$ such that $E(\mathbb{Q})_{\text{tors}} = \mathcal{C}_2 \times \mathcal{C}_2$ and there exist three squarefree integers D_1, D_2, D such that

$$E(\mathbb{Q}(\sqrt{D_i}))_{\text{tors}} = \mathcal{C}_2 \times \mathcal{C}_4 \text{ for } i = 1, 2,$$
$$E(\mathbb{Q}(\sqrt{D}))_{\text{tors}} = \mathcal{C}_2 \times \mathcal{C}_6.$$

   We are going to prove that this is impossible. In other words, $\mathcal{C}_4 \times \mathcal{C}_{12} \leq E(L)_{\text{tors}}$ is not possible for any triquadratic field L. This is equivalent to the same statement, but for the elliptic curve E_D, since E and E_D are isomorphic over $\mathbb{Q}(\sqrt{D})$. For this purpose, we are going to use the general curve with torsion $\mathcal{C}_2 \times \mathcal{C}_6$ by Kubert [13] in the form given by

Elkies [3]:

$$E' : Y^2 = \left(X + t^2\right)\left(X + (t+1)^2\right)\left(X + (t^2+t)^2\right)$$

with 3-torsion points at $X = 0$. Now mind that, if the curve $Y^2 = X(X^2 + aX + b)$ has a 4-torsion point T such that $2T = (0, 0)$, then the first coordinate of T is a square root of b. For E', there are three choices of b, all equivalent. This is because, projectively, E' can be written as

$$Y^2 = \left(X + (tu)^2\right)\left(X + (tv)^2\right)\left(X + (uv)^2\right)$$

with $t + u + v = 0$. In our case the three possible b's are:

$$t^3(2+t)(1+2t),\ -(-1+t)(1+t)^3(1+2t),\ (-1+t)t^3(1+t)^3(2+t).$$

Once E_D has full 4-torsion over some number field L then L must contain $\sqrt{-1}$ from Proposition 7; so there are really only two other square roots that one needs to specify to determine the triquadratic field. If two of the b's yield points defined over the same quadratic field then either one of these b's is a square or two of them multiply to a square. But this is already enough because each possibility yields an elliptic curve of rank zero (`24a1` and `48a1`) and the torsion points on both curves correspond to singular curves in the equation E'.

4. If $[\mathcal{C}_2 \times \mathcal{C}_4, \mathcal{C}_2 \times \mathcal{C}_4, \mathcal{C}_2 \times \mathcal{C}_4] \subset S$, then $S = [\mathcal{C}_2 \times \mathcal{C}_4, \mathcal{C}_2 \times \mathcal{C}_4, \mathcal{C}_2 \times \mathcal{C}_4]$. A group $\mathcal{C}_2 \times \mathcal{C}_6$ cannot appear in S from the argument above. And $\mathcal{C}_2 \times \mathcal{C}_8$ cannot appear either because there would be a point of order 8 in a quadratic extension, coming from halving a point of order 4, but we have already obtained all possible quadratic extension where the torsion grows (3, in fact, from Proposition 11). All the remaining cases do happen, as shown in Table 1. Therefore we have proved:

$$\mathcal{H}_{\mathbb{Q}}(2, \mathcal{C}_2 \times \mathcal{C}_2) = \Big\{ [\mathcal{C}_2 \times \mathcal{C}_4]\,;\, [\mathcal{C}_2 \times \mathcal{C}_6]\,;\, [\mathcal{C}_2 \times \mathcal{C}_8]\,;\, [\mathcal{C}_2 \times \mathcal{C}_{12}]\,; \\ [\mathcal{C}_2 \times \mathcal{C}_4, \mathcal{C}_2 \times \mathcal{C}_4]\,;\, [\mathcal{C}_2 \times \mathcal{C}_4, \mathcal{C}_2 \times \mathcal{C}_6]\,;\, [\mathcal{C}_2 \times \mathcal{C}_4, \mathcal{C}_2 \times \mathcal{C}_8]\,; \\ [\mathcal{C}_2 \times \mathcal{C}_4, \mathcal{C}_2 \times \mathcal{C}_4, \mathcal{C}_2 \times \mathcal{C}_4]\,;\, [\mathcal{C}_2 \times \mathcal{C}_4, \mathcal{C}_2 \times \mathcal{C}_4, \mathcal{C}_2 \times \mathcal{C}_8] \Big\}.$$

5.10 The group $\mathcal{C}_2$

Some quick remarks on $\mathcal{H}_{\mathbb{Q}}(2, \mathcal{C}_2)$ beforehand:

First, no element of $\mathcal{H}_{\mathbb{Q}}(2, \mathcal{C}_2)$ can contain both $\mathcal{C}_{10}$ (or $\mathcal{C}_2 \times \mathcal{C}_{10}$) and $\mathcal{C}_m$ with some $m \geq 4$. The reason for this is that no element in $\Phi_{\mathbb{Q}}(2^\infty)$ has points of order 10 and points of order m. This, together with the remark at the beginning of the section, shows that:

- $\mathcal{C}_2 \times \mathcal{C}_{10}$ can only appear in an element of $\mathcal{H}_{\mathbb{Q}}(2, \mathcal{C}_2)$ as $[\mathcal{C}_2 \times \mathcal{C}_{10}]$.
- $\mathcal{C}_{10}$ can only appear as $[\mathcal{C}_{10}, \mathcal{C}_2 \times \mathcal{C}_2]$.

Second, there are some pairs which cannot appear together in an element of $\mathcal{H}_{\mathbb{Q}}(2, \mathcal{C}_2)$:

- $\mathcal{C}_6$ (or $\mathcal{C}_2 \times \mathcal{C}_6$) and $\mathcal{C}_8$, as there is no $H \in \Phi_{\mathbb{Q}}(2^\infty)$ with points of order 6 and points of order 8.
- $\mathcal{C}_8$ and $\mathcal{C}_{16}$. Assume $\mathcal{C}_8 = \langle P \rangle$ and $\mathcal{C}_{16} = \langle Q \rangle$ are the torsion subgroups in two different quadratic extensions. Consider the group homomorphism

$$\varphi : \mathcal{C}_8 \times \mathcal{C}_{16} \longrightarrow E(\mathbb{Q}(2^\infty)) \\ (nP, mQ) \longmapsto nP + mQ$$

which verifies $\ker(\varphi) = \langle(4P, 8Q)\rangle$, as the rational point of order 2 is the only one who has its inverse in both quadratic extensions. So $E(\mathbb{Q}(2^\infty))_{\text{tors}}$ contains a group of 64 elements with (at least) an element of order 8 and no elements of order 16. From Theorem 5 this would imply there exists an elliptic curve E defined over $\mathbb{Q}$ such that $E(\mathbb{Q})_{\text{tors}} = \mathcal{C}_2$ and $\mathcal{C}_8 \times \mathcal{C}_8 \leq E(\mathbb{Q}(2^\infty))_{\text{tors}}$ and this contradicts Proposition 6.

Another important remark here is the following: let E be an elliptic curve defined over $\mathbb{Q}$ such that there is a quadratic extension $K/\mathbb{Q}$ with $\mathcal{C}_n = E(K)_{\text{tors}}$, and $4|n$, then there must be another quadratic extension $K'/\mathbb{Q}$ with $\mathcal{C}_m = E(K')_{\text{tors}}$ with $4|m$. Moreover, there are no more extensions where the torsion grows, apart from the splitting field of $X^3 + AX + B$ which gives a non-cyclic torsion group. This can be deduced from Lemma 13 as there are either 2 or no quadratic extension where one can get points of order 4 and, therefore, groups $\mathcal{C}_n$ and $\mathcal{C}_m$ with $n, m \in 4\mathbb{Z}$. The following pairs may then appear:

$$\{\mathcal{C}_4, \mathcal{C}_4\}, \{\mathcal{C}_4, \mathcal{C}_8\}, \{\mathcal{C}_4, \mathcal{C}_{12}\}, \{\mathcal{C}_4, \mathcal{C}_{16}\}, \{\mathcal{C}_8, \mathcal{C}_8\}, \{\mathcal{C}_8, \mathcal{C}_{12}\}, \{\mathcal{C}_8, \mathcal{C}_{16}\}, \{\mathcal{C}_{12}, \mathcal{C}_{16}\},$$

although the last three ones can already be ruled out from the arguments above.

Let us then construct the elements $S \in \mathcal{H}_{\mathbb{Q}}(2, \mathcal{C}_2)$ in ascending order of $\#S$:

- $\#S = 1$: In this case $S \in \{[\mathcal{C}_2 \times \mathcal{C}_2], [\mathcal{C}_2 \times \mathcal{C}_6], [\mathcal{C}_2 \times \mathcal{C}_{10}]\}$. All of these cases can occur (see examples in Table 1).
- $\#S = 2$: In Table 1 we can find examples of:

$$[\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_6], [\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_{10}], [\mathcal{C}_2 \times \mathcal{C}_6, \mathcal{C}_6].$$

  These are all the possibilities, from Theorem 1 and the previous remarks.
- $\#S = 3$ with $\mathcal{C}_2 \times \mathcal{C}_2 \in S$. We have example for all the possible cases (after taking into account the preliminary remarks), which are:

$$[\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_4, \mathcal{C}_4], \quad [\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_4, \mathcal{C}_8], \quad [\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_4, \mathcal{C}_{12}],$$
$$[\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_4, \mathcal{C}_{16}], \quad [\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_8, \mathcal{C}_8], \quad [\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_6, \mathcal{C}_6].$$

- $\#S = 3$ with $\mathcal{C}_2 \times \mathcal{C}_6 \in S$. We have examples for $[\mathcal{C}_2 \times \mathcal{C}_6, \mathcal{C}_4, \mathcal{C}_4]$ and the rest can be ruled out. Precisely:

$$[\mathcal{C}_2 \times \mathcal{C}_6, \mathcal{C}_4, \mathcal{C}_8], \quad [\mathcal{C}_2 \times \mathcal{C}_6, \mathcal{C}_4, \mathcal{C}_{16}], \quad [\mathcal{C}_2 \times \mathcal{C}_6, \mathcal{C}_8, \mathcal{C}_8]$$

  cannot appear because there is no $H \in \Phi_{\mathbb{Q}}(2^\infty)$ with points of order 6 and points of order 8. Also

$$[\mathcal{C}_2 \times \mathcal{C}_6, \mathcal{C}_4, \mathcal{C}_{12}]$$

  is not an option, as that would imply $\mathcal{C}_3 \times \mathcal{C}_{12}$ is a subgrup of some $H \in \Phi_{\mathbb{Q}}(2^\infty)$. Finally,

$$[\mathcal{C}_2 \times \mathcal{C}_6, \mathcal{C}_6, \mathcal{C}_6]$$

  is not an option. Were this the case, we would have three $\mathcal{C}_3$ subgroups (different pairwise, as they appear in different quadratic extensions) of some $H \in \Phi_{\mathbb{Q}}(2^\infty)$, which is not possible.
- $\#S = 4$ with $\mathcal{C}_2 \times \mathcal{C}_2 \in S$. We have examples (see Table 1 as usual) for

$$S = [\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_4, \mathcal{C}_4, \mathcal{C}_6],$$

and the remaining possibilities do not happen, in a similar way as the previous case. In fact,

$$[\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_4, \mathcal{C}_8, \mathcal{C}_6],\ [\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_4, \mathcal{C}_{16}, \mathcal{C}_6],\ [\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_8, \mathcal{C}_8, \mathcal{C}_6]$$

all have points of order 6 and points of order 8, while

$$[\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_4, \mathcal{C}_{12}, \mathcal{C}_6],$$

would imply $\mathcal{C}_3 \times \mathcal{C}_{12} \leq H$ for some group $H \in \Phi_{\mathbb{Q}}(2^\infty)$.
- $\#S = 4$ with $\mathcal{C}_2 \times \mathcal{C}_6 \in S$. The only case would be $S = [\mathcal{C}_2 \times \mathcal{C}_6, \mathcal{C}_4, \mathcal{C}_4, \mathcal{C}_6]$ and in fact it does not occur, as it would imply $\mathcal{C}_3 \times \mathcal{C}_{12}$ is a subgroup for a certain $H \in \Phi_{\mathbb{Q}}(2^\infty)$.
- $\#S = 5$. The only possible case would be $S = [\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_4, \mathcal{C}_4, \mathcal{C}_6, \mathcal{C}_6]$, which would imply, again, $\mathcal{C}_3 \times \mathcal{C}_{12} \leq H$, for some $H \in \Phi_{\mathbb{Q}}(2^\infty)$.

Therefore we have proved:

$$\begin{aligned}\mathcal{H}_{\mathbb{Q}}(2, \mathcal{C}_2 \times \mathcal{C}_2) = \Big\{ & [\mathcal{C}_2 \times \mathcal{C}_2]\,;[\mathcal{C}_2 \times \mathcal{C}_6]\,;[\mathcal{C}_2 \times \mathcal{C}_{10}]\,;[\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_6]\,;[\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_{10}]\,;\\ & [\mathcal{C}_2 \times \mathcal{C}_6, \mathcal{C}_6]\,;[\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_4, \mathcal{C}_4]\,;[\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_6, \mathcal{C}_6]\,;\\ & [\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_8, \mathcal{C}_8]\,;[\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_4, \mathcal{C}_8]\,;[\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_4, \mathcal{C}_{12}]\,;\\ & [\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_4, \mathcal{C}_{16}]\,;[\mathcal{C}_2 \times \mathcal{C}_6, \mathcal{C}_4, \mathcal{C}_4]\,;[\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_4, \mathcal{C}_4, \mathcal{C}_6] \Big\}.\end{aligned}$$

This finishes the proof of Theorem 3.

Acknowledgments Both authors are grateful to Noam Elkies, for his insight in the problem concerning curves with $\mathcal{C}_2 \times \mathcal{C}_6$ torsion, and in particular for pointing out to them the parametrization in [3]. Also, Yasutsugu Fujita was very kind to explain to us in detail his argument for Proposition 9 and we thank him for this here. Last, the referees this paper was sent to did a painstaking and exhaustive work which greatly improved its overall quality, and both authors are enormously grateful for that.

Appendix: Computations

Let $G \in \Phi(1)$, $S = [H_1, \ldots, H_m] \in \mathcal{H}_{\mathbb{Q}}(2, G)$, E an elliptic curve defined over $\mathbb{Q}$ such that $E(\mathbb{Q})_{\text{tors}} = G$ and let $D_1, \ldots, D_m \in \mathbb{Z}$, squarefree, such that

$$E(\mathbb{Q}(\sqrt{D_i}))_{\text{tors}} = H_i \quad \text{for } i = 1, \ldots, m.$$

Let us write

$$F_S = \mathbb{Q}\left(\sqrt{D_1}, \ldots, \sqrt{D_m}\right).$$

Table 1 shows an example of every possible situation, where at

- the first column is S,
- the second column is $S \in \mathcal{H}_{\mathbb{Q}}(2, G)$,
- the third column is $\#S$,
- the fourth column is $E(F_S)_{\text{tors}}$,
- the fifth column is the degree of F_S over $\mathbb{Q}$,
- the sixth column is the label of the elliptic curve E with minimal conductor satisfying the conditions above,
- the seventh column displays the $D's$ corresponding to the respective $H's$ in S.

Table 1 $h = \#S$ for $S \in \mathcal{H}_{\mathbb{Q}}(2, G)$, $d = [F_S : \mathbb{Q}]$

G	$\mathcal{H}_{\mathbb{Q}}(2, G)$	h	$E(F_S)_{\text{tors}}$	d	label	$D's$
$\mathcal{C}_1$	$\mathcal{C}_3$	1	$\mathcal{C}_3$	2	19a2	−3
	$\mathcal{C}_5$	1	$\mathcal{C}_5$	2	75a2	5
	$\mathcal{C}_7$	1	$\mathcal{C}_7$	2	208d1	−1
	$\mathcal{C}_9$	1	$\mathcal{C}_9$	2	54a2	−3
	$\mathcal{C}_3, \mathcal{C}_3$	2	$\mathcal{C}_3 \times \mathcal{C}_3$	4	175b2	5, −15
	$\mathcal{C}_3, \mathcal{C}_5$	2	$\mathcal{C}_{15}$	4	50a4	−3, 5
$\mathcal{C}_2$	$\mathcal{C}_2 \times \mathcal{C}_2$	1	$\mathcal{C}_2 \times \mathcal{C}_2$	2	46a1	−23
	$\mathcal{C}_2 \times \mathcal{C}_6$	1	$\mathcal{C}_2 \times \mathcal{C}_6$	2	36a3	−3
	$\mathcal{C}_2 \times \mathcal{C}_{10}$	1	$\mathcal{C}_2 \times \mathcal{C}_{10}$	2	450a3	−15
	$\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_6$	2	$\mathcal{C}_2 \times \mathcal{C}_6$	4	14a3	−7, −3
	$\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_{10}$	2	$\mathcal{C}_2 \times \mathcal{C}_{10}$	4	150b3	−15, 5
	$\mathcal{C}_2 \times \mathcal{C}_6, \mathcal{C}_6$	2	$\mathcal{C}_6 \times \mathcal{C}_6$	4	98a3	−7, 21
	$\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_4, \mathcal{C}_4$	3	$\mathcal{C}_2 \times \mathcal{C}_4$	4	15a5	5, −1, −5
	$\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_4, \mathcal{C}_4$	3	$\mathcal{C}_4 \times \mathcal{C}_4$	4	64a4	−1, 2, −2
	$\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_8, \mathcal{C}_8$	3	$\mathcal{C}_4 \times \mathcal{C}_8$	4	2880r6	−1, 6, −6
	$\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_4, \mathcal{C}_8$	3	$\mathcal{C}_2 \times \mathcal{C}_8$	4	24a6	−2, 2, −1
	$\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_4, \mathcal{C}_{12}$	3	$\mathcal{C}_2 \times \mathcal{C}_{12}$	4	30a3	−15, 5, −3
	$\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_4, \mathcal{C}_{16}$	3	$\mathcal{C}_2 \times \mathcal{C}_{16}$	4	3150bk1	−7, 105, −15
	$\mathcal{C}_2 \times \mathcal{C}_6, \mathcal{C}_4, \mathcal{C}_4$	3	$\mathcal{C}_2 \times \mathcal{C}_{12}$	4	450g1	−15, −3, 5
	$\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_6, \mathcal{C}_6$	3	$\mathcal{C}_6 \times \mathcal{C}_6$	8	98a4	2, −7, 21
	$\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_4, \mathcal{C}_4, \mathcal{C}_6$	4	$\mathcal{C}_2 \times \mathcal{C}_{12}$	8	30a7	10, −5, −2, −3
$\mathcal{C}_3$	$\mathcal{C}_{15}$	1	$\mathcal{C}_{15}$	2	50a3	5
	$\mathcal{C}_3 \times \mathcal{C}_3$	1	$\mathcal{C}_3 \times \mathcal{C}_3$	2	19a1	−3
$\mathcal{C}_4$	$\mathcal{C}_2 \times \mathcal{C}_4$	1	$\mathcal{C}_2 \times \mathcal{C}_4$	2	17a1	−1
	$\mathcal{C}_2 \times \mathcal{C}_8$	1	$\mathcal{C}_2 \times \mathcal{C}_8$	2	192c6	−2
	$\mathcal{C}_2 \times \mathcal{C}_{12}$	1	$\mathcal{C}_2 \times \mathcal{C}_{12}$	2	150c3	−15
	$\mathcal{C}_4 \times \mathcal{C}_4$	1	$\mathcal{C}_4 \times \mathcal{C}_4$	2	40a4	−1
	$\mathcal{C}_2 \times \mathcal{C}_4, \mathcal{C}_{12}$	2	$\mathcal{C}_2 \times \mathcal{C}_{12}$	4	90c1	−15, −3
	$\mathcal{C}_2 \times \mathcal{C}_4, \mathcal{C}_8, \mathcal{C}_8$	2	$\mathcal{C}_2 \times \mathcal{C}_8$	4	15a7	15, 3, 5
	$\mathcal{C}_2 \times \mathcal{C}_8, \mathcal{C}_8, \mathcal{C}_8$	2	$\mathcal{C}_4 \times \mathcal{C}_8$	4	240d6	−1, 6, −6
$\mathcal{C}_5$	$\mathcal{C}_{15}$	1	$\mathcal{C}_{15}$	2	50b1	5
$\mathcal{C}_6$	$\mathcal{C}_2 \times \mathcal{C}_6$	1	$\mathcal{C}_2 \times \mathcal{C}_6$	2	14a4	−7
	$\mathcal{C}_2 \times \mathcal{C}_6, \mathcal{C}_3 \times \mathcal{C}_6$	2	$\mathcal{C}_6 \times \mathcal{C}_6$	4	14a1	−7, −3
	$\mathcal{C}_2 \times \mathcal{C}_6, \mathcal{C}_{12}, \mathcal{C}_{12}$	3	$\mathcal{C}_2 \times \mathcal{C}_{12}$	4	30a1	−15, −3, 5

Remark With the previous notation, we have computed for any curve in the Antwerp–Cremona tables [2]: G, S and $E(F_S)_{\text{tors}}$. Interestingly, for a given S, the group $E(F_S)_{\text{tors}}$ seem to be fully determined, except for the cases

$$G = \mathcal{C}_2; \quad S = [\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_4, \mathcal{C}_4]\,;$$

Table 1 continued

G	$\mathcal{H}_{\mathbb{Q}}(2, G)$	h	$E(F_S)_{\text{tors}}$	d	label	$D's$
$\mathcal{C}_8$	$\mathcal{C}_2 \times \mathcal{C}_8$	1	$\mathcal{C}_2 \times \mathcal{C}_8$	2	`15a4`	-1
	$\mathcal{C}_2 \times \mathcal{C}_8, \mathcal{C}_{16}, \mathcal{C}_{16}$	3	$\mathcal{C}_2 \times \mathcal{C}_{16}$	4	`210e1`	$-7, 105, -15$
$\mathcal{C}_{10}$	$\mathcal{C}_2 \times \mathcal{C}_{10}$	1	$\mathcal{C}_2 \times \mathcal{C}_{10}$	2	`66c1`	33
$\mathcal{C}_{12}$	$\mathcal{C}_2 \times \mathcal{C}_{12}$	1	$\mathcal{C}_2 \times \mathcal{C}_{12}$	2	`90c3`	-15
$\mathcal{C}_2 \times \mathcal{C}_2$	$\mathcal{C}_2 \times \mathcal{C}_4$	1	$\mathcal{C}_2 \times \mathcal{C}_4$	2	`33a1`	-11
	$\mathcal{C}_2 \times \mathcal{C}_6$	1	$\mathcal{C}_2 \times \mathcal{C}_6$	2	`30a6`	-3
	$\mathcal{C}_2 \times \mathcal{C}_8$	1	$\mathcal{C}_2 \times \mathcal{C}_8$	2	`63a2`	-3
	$\mathcal{C}_2 \times \mathcal{C}_{12}$	1	$\mathcal{C}_2 \times \mathcal{C}_{12}$	2	`960o6`	6
	$\mathcal{C}_2 \times \mathcal{C}_4, \mathcal{C}_2 \times \mathcal{C}_4$	2	$\mathcal{C}_4 \times \mathcal{C}_4$	4	`17a2`	$17, -1$
	$\mathcal{C}_2 \times \mathcal{C}_4, \mathcal{C}_2 \times \mathcal{C}_4$	2	$\mathcal{C}_4 \times \mathcal{C}_8$	4	`1200j4`	$-5, 5$
	$\mathcal{C}_2 \times \mathcal{C}_4, \mathcal{C}_2 \times \mathcal{C}_6$	2	$\mathcal{C}_2 \times \mathcal{C}_{12}$	4	`90c2`	$6, -3$
	$\mathcal{C}_2 \times \mathcal{C}_4, \mathcal{C}_2 \times \mathcal{C}_8$	2	$\mathcal{C}_4 \times \mathcal{C}_8$	4	`75b3`	$-5, 5$
	$\mathcal{C}_2 \times \mathcal{C}_4, \mathcal{C}_2 \times \mathcal{C}_4, \mathcal{C}_2 \times \mathcal{C}_4$	3	$\mathcal{C}_4 \times \mathcal{C}_4$	4	`15a2`	$-5, 5, -1$
	$\mathcal{C}_2 \times \mathcal{C}_4, \mathcal{C}_2 \times \mathcal{C}_4, \mathcal{C}_2 \times \mathcal{C}_8$	3	$\mathcal{C}_4 \times \mathcal{C}_8$	4	`510e5`	$-34, 34, -1$
$\mathcal{C}_2 \times \mathcal{C}_4$	$\mathcal{C}_2 \times \mathcal{C}_8$	1	$\mathcal{C}_2 \times \mathcal{C}_8$	2	`15a3`	5
	$\mathcal{C}_4 \times \mathcal{C}_4$	1	$\mathcal{C}_4 \times \mathcal{C}_4$	2	`195a3`	-1
	$\mathcal{C}_2 \times \mathcal{C}_8, \mathcal{C}_4 \times \mathcal{C}_4$	2	$\mathcal{C}_4 \times \mathcal{C}_8$	4	`15a1`	$5, -1$
	$\mathcal{C}_2 \times \mathcal{C}_8, \mathcal{C}_2 \times \mathcal{C}_8$	2	$\mathcal{C}_4 \times \mathcal{C}_8$	4	`1230f2`	$41, -1$
	$\mathcal{C}_2 \times \mathcal{C}_8, \mathcal{C}_2 \times \mathcal{C}_8, \mathcal{C}_4 \times \mathcal{C}_4$	3	$\mathcal{C}_4 \times \mathcal{C}_8$	4	`210e3`	$-6, 6, -1$
$\mathcal{C}_2 \times \mathcal{C}_6$	$\mathcal{C}_2 \times \mathcal{C}_{12}$	1	$\mathcal{C}_2 \times \mathcal{C}_{12}$	2	`90c6`	6

$$G = \mathcal{C}_2 \times \mathcal{C}_2; \quad S = [\mathcal{C}_2 \times \mathcal{C}_4, \mathcal{C}_2 \times \mathcal{C}_4]$$

where two different $E(F_S)$ appear as we run through the entire set of curves in [2]. Given the amount of computations we have carried out, we think it is safe to conjecture that this is precisely the case.

Remark Comparing the results in Table 1 with the set $\Phi_{\mathbb{Q}}(2^{\infty})$ we can conclude that the only groups in $\Phi_{\mathbb{Q}}(2^{\infty})$ which do *not* appear if we consider the groups $E(F_S)_{\text{tors}}$ are:

$$\mathcal{C}_4 \times \mathcal{C}_{12}, \quad \mathcal{C}_4 \times \mathcal{C}_{16}, \quad \mathcal{C}_8 \times \mathcal{C}_8.$$

These are, precisely, the groups discussed at Proposition 9. Our computations suggest that this is in fact the case, but we have not proved this in detail.

References

1. Birch, B.J., Kuyk, W. (eds.): Modular Functions of One Variable IV. Lecture Notes in Mathematics 476. Springer, New York (1975)
2. Cremona, J.E.: Elliptic curve data for conductors up to 300,000 (2013). http://www.warwick.ac.uk/~masgaj/ftp/data/
3. Elkies, N.D.: Wiles Minus Epsilon Implies Fermat. Elliptic Curves, Modular Forms, and Fermat's Last Theorem (Hong Kong, 1993), Ser. Number Theory, I, pp. 38–40. International Press, Cambridge (1995)

4. Fujita, Y.: Torsion subgroups of elliptic curves with non-cyclic torsion over $\mathbb{Q}$ in elementary abelian 2-extensions of $\mathbb{Q}$. Acta Arith. **115**, 29–45 (2004)
5. Fujita, Y.: Torsion subgroups of elliptic curves in elementary abelian 2-extensions of $\mathbb{Q}$. J. Number Theory **114**, 124–134 (2005)
6. González-Jiménez, E.: Covering techniques and rational points on some genus 5 curves. Contemp. Math. AMS (to appear)
7. González-Jiménez, E., Tornero, J.M.: Torsion of rational elliptic curves over quadratic fields. Rev. R. Acad. Cienc. Exactas Fís. Nat. Ser. A Math. RACSAM **108**, 923–934 (2014)
8. Husemoller, D.: Elliptic Curves. Graduate Texts in Mathematics 111. Springer, New York (2004)
9. Jeon, D., Kim, C.H., Lee, Y.: Infinite families of elliptic curves over dihedral quartic number field. . J. Number Theory **133**, 115–122 (2013)
10. Kamienny, S.: Torsion points on elliptic curves and q-coefficients of modular forms. Invent. Math. **109**, 129–133 (1992)
11. Kenku, M.A., Momose, F.: Torsion points on elliptic curves defined over quadratic fields. Nagoya Math. J. **109**, 125–149 (1988)
12. Knapp, A.W.: Elliptic Curves. Mathematical Notes, 40. Princeton University Press, Princeton (1992)
13. Kubert, D.S.: Universal bounds on the torsion of elliptic curves. Proc. Lond. Math. Soc. **33**, 193–237 (1976)
14. Kwon, S.: Torsion subgroups of elliptic curves over quadratic extensions. J. Number Theory **62**, 144–162 (1997)
15. Laska, M., Lorenz, M.: Rational points on elliptic curves over $\mathbb{Q}$ in elementary abelian 2-extensions of $\mathbb{Q}$. J. Reine Angew. Math. **355**, 163–172 (1985)
16. Mazur, B.: Modular curves and the Eisenstein ideal. Publ. Math. Inst. Hautes Études. Sci. **47**, 33–186 (1977)
17. Mazur, B.: Rational isogenies of prime degree. Invent. Math. **44**, 129–162 (1978)
18. Najman, F.: Torsion of elliptic curves over cubic fields and sporadic points on $X_1(n)$. Math. Res. Lett. (to appear)
19. Najman, F.: The number of twists with large torsion of an elliptic curve. Rev. R. Acad. Cienc. Exactas Fís. Nat. Ser. A Math. RACSAM. (2014). doi:10.1007/s13398-014-0199-x
20. Silverman, J.H.: The Arithmetic of Elliptic Curves. Graduate Texts in Mathematics 106. Springer, New York (2009)