COMPLETE CLASSIFICATION OF THE TORSION STRUCTURES OF RATIONAL ELLIPTIC CURVES OVER QUINTIC NUMBER FIELDS

ENRIQUE GONZÁLEZ–JIMÉNEZ

Abstract. We classify the possible torsion structures of rational elliptic curves over quintic number fields. In addition, let E be an elliptic curve defined over $\mathbb{Q}$ and let $G = E(\mathbb{Q})_{\rm tors}$ be the associated torsion subgroup. We study, for a given G, which possible groups $G \subseteq H$ could appear such that $H = E(K)_{\rm tors}$, for $[K : \mathbb{Q}] = 5$. In particular, we prove that at most there is one quintic number field K such that the torsion grows in the extension $K/\mathbb{Q}$, i.e., $E(\mathbb{Q})_{\rm tors} \subsetneq E(K)_{\rm tors}$.

1. Introduction

Let E/K be an elliptic curve defined over a number field K. The Mordell-Weil Theorem states that the set of K-rational points, $E(K)$, is a finitely generated abelian group. Denote by $E(K)_{\rm tors}$, the torsion subgroup of $E(K)$, which is isomorphic to $\mathcal{C}_m \times \mathcal{C}_n$ for two positive integers m, n, where m divides n and where $\mathcal{C}_n$ is a cyclic group of order n.

One of the main goals in the theory of elliptic curves is to characterize the possible torsion structures over a given number field, or over all number fields of a given degree. In 1978 Mazur [25] published a proof of Ogg's conjecture (previously established by Beppo Levi), a milestone in the theory of elliptic curves. In that paper, he proved that the possible torsion structures over $\mathbb{Q}$ belong to the set:

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

and that any of them occurs infinitely often. A natural generalization of this theorem is as follows. Let $\Phi(d)$ be the set of possible isomorphic torsion structures $E(K)_{\rm tors}$, where K runs through all number fields K of degree d and E runs through all elliptic curves over K. Thanks to the uniform boundedness theorem [26], $\Phi(d)$ is a finite set. Then the problem is to determine $\Phi(d)$. Mazur obtained the rational case ($d = 1$). The generalization to quadratic fields ($d = 2$) was obtained by Kamienny, Kenku and Momose [17, 22]. For $d \geq 3$ a complete answer for this problem is still open, although there have been some advances in the last years.

However, more is known about the subset $\Phi^\infty(d) \subseteq \Phi(d)$ of torsion subgroups that arise for infinitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves defined over number fields of degree d. For $d = 1$ and $d = 2$ we have $\Phi^\infty(d) = \Phi(d)$, the cases $d = 3$ and $d = 4$ have been determined by Jeon et al. [15, 16], and recently the cases $d = 5$ and $d = 6$ by Derickx and Sutherland [7].

Restricting our attention to the complex multiplication case, we denote $\Phi^{\rm CM}(d)$ the analogue of the set $\Phi(d)$ but restricting to elliptic curves with complex multiplication (CM elliptic curves in the sequel). In 1974 Olson [30] determined the set of possible torsion structures over $\mathbb{Q}$ of CM elliptic curves:

$$\Phi^{\rm CM}(1) = \{\mathcal{C}_1\,, \mathcal{C}_2\,, \mathcal{C}_3\,, \mathcal{C}_4\,, \mathcal{C}_6\,, \mathcal{C}_2 \times \mathcal{C}_2\}.$$

2010 *Mathematics Subject Classification.* Primary: 11G05, 14G05; Secondary: 14H52, 11R21.
Key words and phrases. Elliptic curves, torsion subgroup, rationals, quintic number fields.
The author was partially supported by the grant MTM2015–68524–P..

The quadratic and cubic cases were determined by Zimmer et al. [27, 8, 31]; and recently, Clark et al. [5] have computed the sets $\Phi^{\rm CM}(d)$, for $4 \le d \le 13$. In particular, they proved

$$\Phi^{\rm CM}(5) = \Phi^{\rm CM}(1) \cup \{\, \mathcal{C}_{11} \,\}.$$

In addition to determining $\Phi(d)$, there are many authors interested in the question of how the torsion grows when the field of definition is enlarged. We focus our attention when the underlying field is $\mathbb{Q}$. In analogy to $\Phi(d)$, let $\Phi_{\mathbb{Q}}(d)$ be the subset of $\Phi(d)$ such that $H \in \Phi_{\mathbb{Q}}(d)$ if there is an elliptic curve $E/\mathbb{Q}$ and a number field K of degree d such that $E(K)_{\rm tors} \simeq H$. One of the first general result is due to Najman [29], who determined $\Phi_{\mathbb{Q}}(d)$ for $d = 2, 3$. Chou [4] has given a partial answer to the classification of $\Phi_{\mathbb{Q}}(4)$. Recently, the author with Najman [11] have completed the classification of $\Phi_{\mathbb{Q}}(4)$ and $\Phi_{\mathbb{Q}}(p)$ for p prime. Moreover, in [11] it has been proved that $E(K)_{\rm tors} = E(\mathbb{Q})_{\rm tors}$ for all elliptic curves E defined over $\mathbb{Q}$ and all number fields K of degree d, where d is not divisible by a prime ≤ 7. In particular, $\Phi_{\mathbb{Q}}(d) = \Phi(1)$ if d is not divisible by a prime ≤ 7.

Our first result determines $\Phi_{\mathbb{Q}}(5)$.

Theorem 1. *The sets $\Phi_{\mathbb{Q}}(5)$ and $\Phi_{\mathbb{Q}}^{\rm CM}(5)$ are given by*

$$\begin{array}{rcl} \Phi_{\mathbb{Q}}(5) & = & \{\, \mathcal{C}_n \mid n = 1, \dots, 12, 25\} \cup \{\, \mathcal{C}_2 \times \mathcal{C}_{2m} \mid m = 1, \dots, 4\}\,, \\ \Phi_{\mathbb{Q}}^{\rm CM}(5) & = & \{\, \mathcal{C}_1\,, \mathcal{C}_2\,, \mathcal{C}_3\,, \mathcal{C}_4\,, \mathcal{C}_6\,, \mathcal{C}_{11}\,, \mathcal{C}_2 \times \mathcal{C}_2 \,\}\,. \end{array}$$

Remark. $\Phi_{\mathbb{Q}}(5) = \Phi_{\mathbb{Q}}(1) \cup \{\, \mathcal{C}_{11}, \mathcal{C}_{25} \,\}$ *and* $\Phi_{\mathbb{Q}}^{\rm CM}(5) = \Phi^{\rm CM}(5) = \Phi^{\rm CM}(1) \cup \{\, \mathcal{C}_{11} \,\}$.

For a fixed $G \in \Phi(1)$, let $\Phi_{\mathbb{Q}}(d, G)$ be the subset of $\Phi_{\mathbb{Q}}(d)$ such that E runs through all elliptic curves over $\mathbb{Q}$ with $E(\mathbb{Q})_{\rm tors} \simeq G$. For each $G \in \Phi(1)$ the sets $\Phi_{\mathbb{Q}}(d, G)$ have been determined for $d = 2$ in [23, 13], for $d = 3$ in [12] and partially for $d = 4$ in [10].

Our second result determines $\Phi_{\mathbb{Q}}(5)$ for any $G \in \Phi(1)$.

Theorem 2. *For $G \in \Phi(1)$, we have $\Phi_{\mathbb{Q}}(5, G) = \{G\}$, except in the following cases:*

G	$\Phi_{\mathbb{Q}}\,(5, G)$
$\mathcal{C}_1$	$\{\mathcal{C}_1\,, \mathcal{C}_5\,, \mathcal{C}_{11}\,\}$
$\mathcal{C}_2$	$\{\mathcal{C}_2\,, \mathcal{C}_{10}\,\}$
$\mathcal{C}_5$	$\{\mathcal{C}_5\,, \mathcal{C}_{25}\,\}$

Moreover, there are infinitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves $E/\mathbb{Q}$ with $H \in \Phi_{\mathbb{Q}}\,(5, G)$, except for the case $H = \mathcal{C}_{11}$ where only the elliptic curves `121a2`, `121c2`, `121b1` *have eleven torsion over a quintic number field.*

In fact, it is possible to give a more detailed description of how the torsion grows. For this purpose for any $G \in \Phi(1)$ and any positive integer d, we define the set

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

where $S_i = [H_1, ..., H_m]$ is a list of groups $H_j \in \Phi_{\mathbb{Q}}(d, G) \setminus \{G\}$, such that, for each $i = 1, \dots, n$, there exists an elliptic curve $E_i/\mathbb{Q}$ that satisfies the following properties:

- $E_i(\mathbb{Q})_{\rm tors} \simeq G$, and
- there are number fields $K_1, ..., K_m$ (non–isomorphic pairwise) whose degrees divide d with $E_i(K_j)_{\rm tors} \simeq H_j$, for all $j = 1, ..., m$; and for each j there does not exist $K_j' \subset K_j$ such that $E_i(K_j')_{\rm tors} \simeq H_j$.

We are allowing the possibility of two (or more) of the H_j being isomorphic. The above sets have been completely determined for the quadratic case ($d = 2$) in [14], for the cubic case ($d = 3$) in [12] and computationally conjectured for the quartic case ($d = 4$) in [10]. The quintic case ($d = 5$) is treated in this paper, and the next result determined $\mathcal{H}_{\mathbb{Q}}(5, G)$ for any $G \in \Phi(1)$:

Theorem 3. *For $G \in \Phi(1)$, we have $\mathcal{H}_{\mathbb{Q}}(5, G) = \emptyset$, except in the following cases:*

G	$\mathcal{H}_{\mathbb{Q}}(5, G)$
$\mathcal{C}_1$	$\mathcal{C}_5$
	$\mathcal{C}_{11}$
$\mathcal{C}_2$	$\mathcal{C}_{10}$
$\mathcal{C}_5$	$\mathcal{C}_{25}$

In particular, for any elliptic curve $E/\mathbb{Q}$, there is at most one quintic number field K, up to isomorphism, such that $E(K)_{\rm tors} \neq E(\mathbb{Q})_{\rm tors}$.

Remark. *Notice that for any CM elliptic curve $E/\mathbb{Q}$ and any quintic number field K it has $E(K)_{\rm tors} = E(\mathbb{Q})_{\rm tors}$, except to the elliptic curve* `121b1` *and $K = \mathbb{Q}(\zeta_{11})^+ = \mathbb{Q}(\zeta_{11} + \zeta_{11}^{-1})$ where $E(\mathbb{Q})_{\rm tors} \simeq \mathcal{C}_1$ and $E(K)_{\rm tors} \simeq \mathcal{C}_{11}$.*

Let us define

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

The values $h_{\mathbb{Q}}(d)$ have been computed for $d = 2$ and $d = 3$ in [14] and [12] respectively. For $d = 4$ we computed a lower bound in [10]. For $d = 5$ we have:

Corollary 4. $h_{\mathbb{Q}}(5) = 1$.

Remark. *In particular, we have deduced the following:*

d	2	3	4	5
$h_{\mathbb{Q}}(d)$	4	3	≥ 9	1

Notation. We will use the Antwerp–Cremona tables and labels [1, 6] when referring to specific elliptic curves over $\mathbb{Q}$.

For conjugacy classes of subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ we will use the labels introduced by Sutherland in [34, §6.4].

We will write $G \simeq H$ (or $G \lesssim H$) for the fact that G is isomorphic to H (or to a subgroup of H resp.) without further detail on the precise isomorphism.

For a positive integer n we will write $\varphi(n)$ for the Euler-totient function of n.

We use $\mathcal{O}$ to denote the point at infinity of an elliptic curve (given in Weierstrass form).

2. Mod n Galois representations associated to elliptic curves

Let $E/\mathbb{Q}$ be an elliptic curve and n a positive integer. We denote by $E[n]$ the n-torsion subgroup of $E(\overline{\mathbb{Q}})$, where $\overline{\mathbb{Q}}$ is a fixed algebraic closure of $\mathbb{Q}$. That is, $E[n] = \{P \in E(\overline{\mathbb{Q}}) \,|\, [n]P = \mathcal{O}\}$. The absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $E[n]$ by its action on the coordinates of the points, inducing a Galois representation

$$\rho_{E,n} \,:\, \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}(E[n]).$$

Notice that since $E[n]$ is a free $\mathbb{Z}/n\mathbb{Z}$-module of rank 2, fixing a basis $\{P, Q\}$ of $E[n]$, we identify $\mathrm{Aut}(E[n])$ with $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Then we rewrite the above Galois representation as

$$\rho_{E,n} \,:\, \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

Therefore we can view $\rho_{E,n}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ as a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, determined uniquely up to conjugacy, and denoted by $G_E(n)$ in the sequel. Moreover, $\mathbb{Q}(E[n]) = \{x, y \mid (x, y) \in E[n]\}$ is Galois and since $\ker \rho_{E,n} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(E[n]))$, we deduce that $G_E(n) \simeq \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$.

Let $R = (x(R), y(R)) \in E[n]$ and $\mathbb{Q}(R) = \mathbb{Q}(x(R), y(R)) \subseteq \mathbb{Q}(E[n])$, then by Galois theory there exists a subgroup $\mathcal{H}_R$ of $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ such that $\mathbb{Q}(R) = \mathbb{Q}(E[n])^{\mathcal{H}_R}$. In particular, if we denote by H_R the image of $\mathcal{H}_R$ in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, we have:

- $[\mathbb{Q}(R) : \mathbb{Q}] = [G_E(n) : H_R]$.
- $\mathrm{Gal}(\widehat{\mathbb{Q}(R)}/\mathbb{Q}) \simeq G_E(n)/N_{G_E(n)}(H_R)$, where $\widehat{\mathbb{Q}(R)}$ denotes the Galois closure of $\mathbb{Q}(R)$ in $\overline{\mathbb{Q}}$, and $N_{G_E(n)}(H_R)$ denotes the normal core of H_R in $G_E(n)$.

We have deduced the following result.

Lemma 5. *Let $E/\mathbb{Q}$ be an elliptic curve, n a positive integer and $R \in E[n]$. Then $[\mathbb{Q}(R) : \mathbb{Q}]$ divides $|G_E(n)|$. In particular $[\mathbb{Q}(R) : \mathbb{Q}]$ divides $|\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})|$.*

In practice, given the conjugacy class of $G_E(n)$ we can deduce the relevant arithmetic-algebraic properties of the fields of definition of the n-torsion points: since $E[n]$ is a free $\mathbb{Z}/n\mathbb{Z}$-module of rank 2, we can identify the n-torsion points with $(a, b) \in (\mathbb{Z}/n\mathbb{Z})^2$ (i.e. if $R \in E[n]$ and $\{P, Q\}$ is a $\mathbb{Z}/n\mathbb{Z}$-basis of $E[n]$, then there exist $a, b \in \mathbb{Z}/n\mathbb{Z}$ such that $R = aP + bQ$). Therefore H_R is the stabilizer of (a, b) by the action of $G_E(n)$ on $(\mathbb{Z}/n\mathbb{Z})^2$. In order to compute all the possible degrees (jointly with the Galois group of its Galois closure in $\overline{\mathbb{Q}}$) of the fields of definition of the n-torsion points we run over all the elements of $(\mathbb{Z}/n\mathbb{Z})^2$ of order n.

Now, observe that $\langle R\rangle \subset E[n]$ is a subgroup of order n. Equivalently, $E/\mathbb{Q}$ admits a cyclic n-isogeny (non-rational in general). The field of definition of this isogeny is denoted by $\mathbb{Q}(\langle R\rangle)$. A similar argument could be used to obtain a description of $\mathbb{Q}(\langle R\rangle)$ using Galois theory. In particular, if $\langle R\rangle$ is $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable then the isogeny is defined over $\mathbb{Q}$. To compute the relevant arithmetic-algebraic properties of the field $\mathbb{Q}(\langle R\rangle)$ is similar to the case $\mathbb{Q}(R)$, replacing the pair (a, b) by the $\mathbb{Z}/n\mathbb{Z}$-module of rank 1 generated by (a, b) in $(\mathbb{Z}/n\mathbb{Z})^2$.

In the case $E/\mathbb{Q}$ be a non-CM elliptic curve and $p \leq 11$ be a prime, Zywina [35] has described all the possible subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ that occur as $G_E(p)$.

For each possible subgroup $G_E(p) \subseteq \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ for $p \in \{2, 3, 5, 11\}$, Table 1 lists in the first and second column the corresponding labels in Sutherland and Zywina notations, and the following data:

- d_0: the index of the largest subgroup of $G_E(p)$ that fixes a $\mathbb{Z}/p\mathbb{Z}$-submodule of rank 1 of $E[p]$; equivalently, the degree of the minimal extension $L/\mathbb{Q}$ over which E admits a L-rational p-isogeny.
- d_v: is the index of the stabilizers of $v \in (\mathbb{Z}/p\mathbb{Z})^2$, $v \neq (0, 0)$, by the action of $G_E(p)$ on $(\mathbb{Z}/p\mathbb{Z})^2$; equivalently, the degrees of the extension $L/\mathbb{Q}$ over which E has a L-rational point of order p.
- d: is the order of $G_E(p)$; equivalently, the degree of the minimal extension $L/\mathbb{Q}$ for which $E[p] \subseteq E(L)$.

Note that Table 1 is partially extracted from Table 3 of [34]. The difference is that [34, Table 3] only lists the minimum of d_v, which is denoted by d_1 therein.

For the CM case, Zywina [35, §1.9] gives a complete description of $G_E(p)$ for any prime p.

3. Isogenies.

In this paper a rational n-isogeny of an elliptic curve $E/\mathbb{Q}$ is a (surjective) morphism $E \longrightarrow E'$ defined over $\mathbb{Q}$ where $E'/\mathbb{Q}$ and the kernel is cyclic of order n. The rational n-isogenies of elliptic curves over $\mathbb{Q}$, have been described completely in the literature, for all $n \geq 1$. The following result gives all the possible values of n.

Sutherland	Zywina	d_0	d_v	d
2Cs	G_1	1	1	1
2B	G_2	1	1 , 2	2
2Cn	G_3	3	3	3
$\mathrm{GL}(2,\mathbb{Z}/2\mathbb{Z})$		3	3	6
3Cs.1.1	$H_{1,1}$	1	1 , 2	2
3Cs	G_1	1	2 , 4	4
3B.1.1	$H_{3,1}$	1	1 , 6	6
3B.1.2	$H_{3,2}$	1	2 , 3	6
3Ns	G_2	2	4	8
3B	G_3	1	2 , 6	12
3Nn	G_4	4	8	16
$\mathrm{GL}(2,\mathbb{Z}/3\mathbb{Z})$		4	8	48
11B.1.4	$H_{1,1}$	1	5 , 110	110
11B.1.5	$H_{2,1}$	1	5 , 110	110
11B.1.6	$H_{2,2}$	1	10 , 55	110
11B.1.7	$H_{1,2}$	1	10 , 55	110
11B.10.4	G_1	1	10 , 110	220
11B.10.5	G_2	1	10 , 110	220
11Nn	G_3	12	120	240
$\mathrm{GL}(2,\mathbb{Z}/11\mathbb{Z})$		12	120	13200

Sutherland	Zywina	d_0	d_v	d
5Cs.1.1	$H_{1,1}$	1	1 , 4	4
5Cs.1.3	$H_{1,2}$	1	2 , 4	4
5Cs.4.1	G_1	1	2 , 4 , 8	8
5Ns.2.1	G_3	2	8 , 16	16
5Cs	G_2	1	4	16
5B.1.1	$H_{6,1}$	1	1 , 20	20
5B.1.2	$H_{5,1}$	1	4 , 5	20
5B.1.4	$H_{6,2}$	1	2 , 20	20
5B.1.3	$H_{5,2}$	1	4 , 10	20
5Ns	G_4	2	8 , 16	32
5B.4.1	G_6	1	2 , 20	40
5B.4.2	G_5	1	4 , 10	40
5Nn	G_7	6	24	48
5B	G_8	1	4 , 20	80
5S4	G_9	6	24	96
$\mathrm{GL}(2,\mathbb{Z}/5\mathbb{Z})$		6	24	480

Table 1. Image groups $G_E(p)$, for $p \in \{2,3,5,11\}$, for non-CM elliptic curves $E/\mathbb{Q}$.

Theorem 6 ([25, 18, 19, 20, 21])**.** *Let $E/\mathbb{Q}$ be an elliptic curve with a rational n-isogeny. Then $n \leq 19$ or $n \in \{21, 25, 27, 37, 43, 67, 163\}$.*

A direct consequence of the Galois theory applied to the theory of cyclic isogenies is the following (cf. Lemma 3.10 [4]).

Lemma 7. *Let $E/\mathbb{Q}$ be an elliptic curve such that $E(K)[n] \simeq \mathcal{C}_n$ over a Galois extension $K/\mathbb{Q}$. Then E has a rational n-isogeny.*

4. $\mathcal{P}$-primary torsion subgroup

Let E/K be an elliptic curve defined over a number field K. For a given set of primes $\mathcal{P} \subset \mathbb{Z}$, let $E(K)[\mathcal{P}^\infty]$ denote the $\mathcal{P}$-primary torsion subgroup of $E(K)_{\mathrm{tors}}$, that is, the direct product of the p-Sylow subgroups of $E(K)$ for $p \in \mathcal{P}$. If $\mathcal{P} = \{p\}$, let us denote by $E(K)[p^\infty]$.

Proposition 8. *Let $E/\mathbb{Q}$ be an elliptic curve and $K/\mathbb{Q}$ be a quintic number field.*

(1) If P is a point of prime order p in $E(K)$, then $p \in \{2,3,5,7,11\}$.

(2) If $E(K)[n] = E[n]$, then $n = 2$.

Proof. (1) Lozano-Robledo [24] has determined that the set of primes p for which there exists a number field K of degree ≤ 5 and an elliptic curve $E/\mathbb{Q}$ such that the p divides the order of $E(K)_{\rm tors}$ is given by $S_{\mathbb{Q}}(5) = \{2, 3, 5, 7, 11, 13\}$. Then to finish the proof we must remove the prime $p = 13$. This follows from Lemma 5 since 5 does not divide the order of $\mathrm{GL}_2(\mathbb{F}_{13})$, that is $2^5 \cdot 3^2 \cdot 7 \cdot 13$.

(2) Let E/K be the base change of E over the number field K. If $E[n] \subseteq E(K)$ then $\mathbb{Q}(\zeta_n) \subseteq K$. In particular $\varphi(n) \,|\, [K : \mathbb{Q}]$. The only possibility if $[K : \mathbb{Q}] = 5$ is $n = 2$. □

4.1. p-primary torsion subgroup ($p \neq 5, 11$).

Lemma 9. *Let $E/\mathbb{Q}$ be an elliptic curve and $K/\mathbb{Q}$ a quintic number field. Then, for any prime $p \neq 5, 11$:*

$$E(K)[p^\infty] = E(\mathbb{Q})[p^\infty].$$

In particular, if $P \in E(K)[p^\infty]$ and p^n is its order, then $n \leq 3, 2, 1$, if $p = 2, 3, 7$, respectively, and $n = 0$ otherwise.

Proof. Let $P \in E(K)[p^n]$. By Lemma 5, $[\mathbb{Q}(P) : \mathbb{Q}]$ divides $|\,\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})| = p^{4n-3}(p^2-1)(p-1)$. If $p \in \{2, 3, 7\}$ then $\mathbb{Q}(P) = \mathbb{Q}$. Together with Proposition 8 (2), we deduce $E(K)[p^\infty] = E(\mathbb{Q})[p^\infty]$. If $p \geq 13$ and $n > 0$, then $[p^{n-1}]P \in E(K)$ is a point or order p, a contradiction with Proposition 8 (1). That is, $E(K)[p^\infty] = E(\mathbb{Q})[p^\infty] = \{\mathcal{O}\}$ if $p \geq 13$. □

4.2. 5-primary torsion subgroup.

Lemma 10. *Let $E/\mathbb{Q}$ be an elliptic curve and $K/\mathbb{Q}$ a quintic number field. Then*

$$E(K)[5^\infty] \lesssim \mathcal{C}_{25}.$$

In particular if $E(K)[5^\infty] \neq \{\mathcal{O}\}$ then E has non-CM. Moreover:

1. *if $E(\mathbb{Q})[5^\infty] \simeq \mathcal{C}_5$, then $G_E(5)$ is labeled `5B.1.1` or `5Cs.1.1`;*
2. *if $E(K)[5^\infty] \simeq \mathcal{C}_5$ and $E(\mathbb{Q})[5^\infty] = \{\mathcal{O}\}$, then $G_E(5)$ is labeled `5B.1.2`;*
3. *if $E(K)[5^\infty] \simeq \mathcal{C}_{25}$, then $E(\mathbb{Q})[5^\infty] \simeq \mathcal{C}_5$. Moreover, K is Galois if $G_E(5)$ is labeled `5B.1.1`.*

Proof. First suppose that E has CM. Then by the classification $\Phi_{\mathbb{Q}}^{\rm CM}(5)$ we deduce that $E(K)[5^\infty] = \{\mathcal{O}\}$. From now on we assume that E is non-CM. First, it is not possible $E[5] \subseteq E(K)$ by Proposition 8 (2). Now, the characterization of $\Phi(1)$ tells us that $E(\mathbb{Q})[5^\infty] \lesssim \mathcal{C}_5$. We observe in Table 1 that $d_v = 1$ (resp. $d_v = 5$) for some $v \in (\mathbb{Z}/5\mathbb{Z})^2$ of order 5 if and only if $G_E(5)$ is labeled by `5Cs.1.1` or `5B.1.1` (resp. `5B.1.2`), which proves (1) (resp. (2)). We are going to prove that $E(K)[5^\infty] \lesssim \mathcal{C}_{25}$. First, we prove (3). Assume that there exists a quintic number field K such that $E(K)[25] = \langle P \rangle \simeq \mathcal{C}_{25}$. Then $G_E(25)$ satisfies:

$$G_E(25) \equiv G_E(5) \pmod 5 \qquad \text{and} \qquad [G_E(25) : H_P] = 5.$$

Note that in general we do not have an explicit description of $G_E(25)$, but using `Magma` [2] we do a simulation with subgroups of $GL_2(\mathbb{Z}/25\mathbb{Z})$.

First assume that $G_E(5)$ is labeled by `5B.1.2`, then $G_E(5)$ is conjugate in $\mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$ to the subgroup (cf. [35, Theorem 1.4 (iii)])

$$H_{5,1} = \left\langle \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle \subset \mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z}).$$

Since we do not have a characterization of $G_E(25)$, we check using `Magma` that for any subgroup G of $GL_2(\mathbb{Z}/25\mathbb{Z})$ satisfying $G \equiv H \pmod 5$ for some conjugate H of $H_{5,1}$ in $\mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$, and for any

$v \in (\mathbb{Z}/25\mathbb{Z})^2$ of order 25, we have $[G : G_v] \neq 5$ (where G_v be the stabilizer of v by the action of G on $(\mathbb{Z}/25\mathbb{Z})^2$). Therefore for any point $P \in E[25]$ it has $[G_E(25) : H_P] \neq 5$. In particular this proves that if $G_E(5)$ is labeled by `5B.1.2`, then there is not 5^n-torsion over a quintic number field, for $n > 1$. This finishes the first part of (3).

Now assume that $G_E(5)$ is labeled by `5B.1.1`. That is, $G_E(5)$ is conjugate in $\mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$ to the subgroup (cf. [35, Theorem 1.4 (iii)])

$$H_{6,1} = \left\langle \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle \subset \mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z}).$$

A similar argument as the one used before, we check that for any subgroup G of $GL_2(\mathbb{Z}/25\mathbb{Z})$ satisfying $G \equiv H \pmod 5$ for some conjugate H of $H_{6,1}$ in $\mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$, and for any $v \in (\mathbb{Z}/25\mathbb{Z})^2$ of order 25 such that $[G : G_v] = 5$ we have that $G/N_G(G_v) \simeq \mathcal{C}_5$. Therefore we have deduced that if $E/\mathbb{Q}$ is an elliptic curve such that $G_E(5)$ is labeled by `5B.1.1` and there exists a quintic number field K with a K-rational point of order 25, then K is Galois. Note that in this case there does not exist a point of order 5^n for $n > 2$ over any quintic number field: suppose that K' is a quintic number field such that there exists $P \in E(K')[5^n]$. Then $[5^{n-2}]P \in E(K')[25]$. Therefore K' is Galois and, by Lemma 7, E has a rational 5^n-isogeny. In contradiction with Theorem 6. This completes the proof of (3).

Finally we assume that $G_E(5)$ is labeled by `5Cs.1.1`. That is, $G_E(5)$ is conjugate in $\mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$ to the subgroup (cf. [35, Theorem 1.4 (iii)])

$$H_{1,1} = \left\langle \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \right\rangle \subset \mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z}).$$

In this case using a similar algorithm as above we check that if there exists a quintic number field K such that $E(K)[25] \simeq \mathcal{C}_{25}$ then K is Galois or the Galois closure of K in $\overline{\mathbb{Q}}$ is isomorphic to $\mathcal{F}_5$, where $\mathcal{F}_5$ denotes the Fröbenius group of order 20. In the former case, this proves that there does not exist a point of order 5^n for $n > 2$ over any Galois quintic number field. Now, assume that K is not Galois, then $G_E(125)$ satisfies:

$$\begin{aligned} G_E(125) &\equiv G_E(5) \pmod 5 \quad , \quad [G_E(125) : H_P] = 5, \\ G_E(125) &\equiv G_E(25) \pmod{25} \quad , \quad [G_E(25) : H_{5P}] = 5. \end{aligned}$$

We check that for any subgroup G of $GL_2(\mathbb{Z}/125\mathbb{Z})$ satisfying $G \equiv H \pmod 5$ for some conjugate H of $H_{1,1}$ in $\mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$, and for any $v \in (\mathbb{Z}/125\mathbb{Z})^2$ of order 125 such that $[G : G_v] = 5$ and $G/N_G(G_v) \simeq \mathcal{F}_5$ we obtain that $[G' : G'_w] \neq 5$ for any $w \in (\mathbb{Z}/25\mathbb{Z})^2$ of order 25; where $G' \equiv G \pmod{25}$. We deduce that there do not exist points of order 125 over quintic number fields. So, $E(K)[5^\infty] \lesssim \mathcal{C}_{25}$.

This finishes the proof. □

4.3. 11-primary torsion subgroup.

Lemma 11. *Let $E/\mathbb{Q}$ be an elliptic curve and $K/\mathbb{Q}$ a quintic number field. Then*

$$E(K)[11^\infty] \lesssim \mathcal{C}_{11}.$$

In particular, if $E(K)[11^\infty] \neq \{\mathcal{O}\}$ then E is labeled ***121a2****,* ***121c2****, or* ***121b1****, $K = \mathbb{Q}(\zeta_{11})^+$ and $E(K)_{\mathrm{tors}} \simeq \mathcal{C}_{11}$.*

Proof. First, suppose that $E/\mathbb{Q}$ is non-CM. Then Table 1 shows that there exists a point of order 11 over a quintic number field if and only if $G_E(11)$ is labeled `11B.1.4` or `11B.1.5`. Or in Zywina notation, $G_E(11)$ is conjugate in $\mathrm{GL}_2(\mathbb{Z}/11\mathbb{Z})$ to the subgroups $H_{1,1}$ or $H_{2,1}$. Then Zywina [35, Theorem 1.6(v)] proved that E is isomorphic (over $\mathbb{Q}$) to `121a2` or `121c2` respectively.

Now, let us suppose that $E/\mathbb{Q}$ has CM. Recall that there are thirteen $\mathbb{Q}$-isomorphic classes of elliptic curve with CM (cf. [33, A §3]), each of them has CM by an order in the imaginary quadratic field with discriminant $-D$, where $D \in \{3,4,7,8,11,19,43,67,163\}$. In this context, Zywina [35, §1.9] gives a complete characterization of the conjugacy class of $G_E(p)$ in $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, for any prime p. Let us apply these results for the case $p = 11$. The proof splits on whether $j(E) \neq 0$ (Proposition 1.14 [35]) or $j(E) = 0$ (Proposition 1.16 (iv) [35]):

- $j(E) \neq 0$. Depending whether $-D$ is a quadratic residue modulo 11:
  - if $D \in \{7,8,19,43\}$ then $G_E(11)$ is conjugate to `11Ns`.
  - if $D \in \{3,4,6,7,163\}$ then $G_E(11)$ is conjugate to `11Nn`.
  - if $D = 11$:
    - if E is `121b1` then $G_E(11)$ is conjugate to `11B.1.3`,
    - if E is `121b2` then $G_E(11)$ is conjugate to `11B.1.8`,
    - otherwise $G_E(11)$ is conjugate to `11B.10.3`.
- $j(E) = 0$. Then $G_E(11)$ is conjugate to `11Nn.1.4` or `11Ns`.

The following table lists for each possible $G_E(11)$ as above, the value d_1, the minimum of the indexes of the stabilizers of $v \in (\mathbb{Z}/11\mathbb{Z})^2$, $v \neq (0,0)$, by the action of $G_E(11)$ on $(\mathbb{Z}/11\mathbb{Z})^2$; equivalently, the minimum degree of the extension $L/\mathbb{Q}$ over which E has a L-rational point of order 11.

`11Ns`	`11Nn`	`11B.1.3`	`11B.1.8`	`11B.10.3`	`11Nn.1.4`
20	120	5	10	10	40

The above table proves that $E/\mathbb{Q}$ has a point of order 11 over a quintic number fields if and only if E is the curve `121b1`.

Finally, Table 3 shows that the torsion of the elliptic curves `121a2`, `121c2` and `121b1` grows in a quintic number field to $\mathcal{C}_{11}$ only over the field $\mathbb{Q}(\zeta_{11})^+$, and over that field the torsion is $\mathcal{C}_{11}$. □

Remark. *If in the above statement the quintic number field is replaced by a number field K of degree d such that $d \neq 5$ and $d \leq 9$, then there does not exist any elliptic curve $E/\mathbb{Q}$ with a point of order 11 over K.*

4.4. $\{p,q\}$-primary torsion subgroup.

Lemma 12. *Let $E/\mathbb{Q}$ be an elliptic curve and $K/\mathbb{Q}$ a quintic number field. Let $p,q \in \{2,3,5,7,11\}$, $p \neq q$, such that pq divides the order of $E(K)_{\mathrm{tors}}$. Then*

$$E(\mathbb{Q})[\{p,q\}^\infty] = E(K)[\{p,q\}^\infty] \quad \text{or} \quad E(K)[\{p,q\}^\infty] \simeq \mathcal{C}_{10}.$$

In the former case, $E(\mathbb{Q})_{\mathrm{tors}} = E(\mathbb{Q})[\{p,q\}^\infty] \simeq G$, where $G \in \{\mathcal{C}_6, \mathcal{C}_{10}, \mathcal{C}_2 \times \mathcal{C}_6\}$.

Proof. First we may suppose $p \neq 11$ by Lemma 11. Assume that $p,q \in \{2,3,7\}$, then by Lemma 9 we have that the $\{p,q\}$-primary torsion is defined over $\mathbb{Q}$. That is, $E(K)[\{p,q\}^\infty] = E(\mathbb{Q})[\{p,q\}^\infty]$. Let $G \in \Phi(1)$ such that $E(\mathbb{Q})_{\mathrm{tors}} \simeq G$. Then $G \in \{\mathcal{C}_6, \mathcal{C}_2 \times \mathcal{C}_6\}$.

It remains to prove the case $p = 5$ and $q \in \{2,3,7\}$. Without loss of generality we can assume that the 5-primary torsion is not defined over $\mathbb{Q}$, otherwise $E(K)[\{5,q\}^\infty] = E(\mathbb{Q})[\{5,q\}^\infty]$ and the unique possibility is $\mathcal{C}_{10}$. In particular, by Lemma 10 we have that E has non-CM and the 5-primary torsion of E over K is cyclic of order 5 or 25, and $E(\mathbb{Q})[5^\infty] = \{\mathcal{O}\}$ or $E(\mathbb{Q})[5^\infty] \simeq \mathcal{C}_5$ respectively. Depending on $q \in \{2,3,7\}$ we have:

- $q = 2$:

- ⋆ $E(K)[5^\infty] \simeq \mathcal{C}_5$. If $E(K)[2^\infty] \simeq \mathcal{C}_2$ then there are infinitely many elliptic curves such that $E(K)[\{2,5\}^\infty] \simeq \mathcal{C}_{10}$ (see Proposition 15). In fact, the above 2-primary torsion is the unique possibility since if $\mathcal{C}_4 \lesssim E(\mathbb{Q})$ then $\mathcal{C}_{20} \not\lesssim E(K)$ and if $E[2] \lesssim E(\mathbb{Q})$ then $\mathcal{C}_2 \times \mathcal{C}_{10} \not\lesssim E(K)$ (see Remark below Theorem 7 of [10]).
- ⋆ $E(K)[5^\infty] \simeq \mathcal{C}_{25}$. Assume that $E(K)[2] \neq \{\mathcal{O}\}$. If $G_E(5)$ is labeled `5B.1.1` then K is Galois and therefore, by Lemma 7, E has a rational 50-isogeny, that is not possible by Theorem 6. Now suppose that $G_E(5)$ is labeled `5Cs.1.1`. Since $E(K)[2^\infty] = E(\mathbb{Q})[2^\infty]$ and $E(\mathbb{Q}(\zeta_5)) = E[5]$ (by Table 1) we deduce $\mathcal{C}_5 \times \mathcal{C}_{10} \lesssim E(\mathbb{Q}(\zeta_5))$. But this is not possible since Bruin and Najman [3, Theorem 6] have proved that any elliptic curve defined over $\mathbb{Q}(\zeta_5)$ have torsion subgroup isomorphic to a group in the following set
$$\Phi(\mathbb{Q}(\zeta_5)) = \{\, \mathcal{C}_n \mid n = 1, \dots, 10, 12, 15, 16\} \cup \{\, \mathcal{C}_2 \times \mathcal{C}_{2m} \mid m = 1, \dots, 4\} \cup \{\mathcal{C}_5 \times \mathcal{C}_5\}.$$

• $q = 3$: A necessary condition if 15 divides $E(K)_{\rm tors}$ is that the 5-torsion is not defined over $\mathbb{Q}$ and the 3-torsion is defined over $\mathbb{Q}$. By Lemma 10, $G_E(5)$ is labeled `5B.1.2`. Zywina [35, Theorem 1.4] has showed that its j-invariant is of the form
$$J_5(t) = \frac{(t^4 + 228t^3 + 494t^2 - 228t + 1)^3}{t(t^2 - 11t - 1)^5}, \qquad \text{for some } t \in \mathbb{Q}.$$
On the other hand, we have proved that the 3-torsion is defined over $\mathbb{Q}$. Then, by Table 1, $G_E(3)$ is labeled `3Cs.1.1` or `3B.1.1`. Again Zywina [35, Theorem 1.2] characterizes the j-invariant of $E/\mathbb{Q}$ depending on the conjugacy class of $G_E(3)$:

- ⋆ `3Cs.1.1`: $J_1(s) = 27\dfrac{(s+1)^3(s+3)^3(s^2+3)^3}{s^3(s^2+3s+3)^3}$, for some $s \in \mathbb{Q}$. We must have an equality of j-invariants: $J_1(s) = J_5(t)$. In particular, grouping cubes we deduce:
$$t(t^2 - 11t - 1)^2 = r^3, \qquad \text{for some } t, r \in \mathbb{Q}.$$
This equation defines a curve C of genus 2, which in fact transforms (according to `Magma`) to[1] $C' : y^2 = x^6 + 22x^3 + 125$. The jacobian of C' has rank 0, so we can use the Chabauty method, and determine that the points on C' are
$$C'(\mathbb{Q}) = \{(1 : \pm 1 : 0)\}.$$
Therefore C' has no affine points and we obtain
$$C(\mathbb{Q}) = \{(0,0)\} \cup \{(1 : 0 : 0)\}.$$
Then $t = 0$, and since t divides the denominator of $J_5(t)$ we have reached a contradiction to the existence of such curve E.

- ⋆ `3B.1.1`: $J_3(s) = 27\dfrac{(s+1)(s+9)^3}{s^3}$, for some $s \in \mathbb{Q}$. A similar argument with the equality $J_3(s) = J_5(t)$ gives us the equation:
$$C : 27(s+1)(s+9)^3 t(t^2 - 11t - 1)^5 = s^3(t^4 + 228t^3 + 494t^2 - 228t + 1)^3.$$
In this case the above equation defines a genus 1 curve which has the following points:
$$\{(-2/27, -1/8), (-27/2, -2), (-27/2, 1/2), (0,0), (-2/27, 8)\} \cup \{(0 : 1 : 0), (1/27 : 1 : 0), (1 : 0 : 0)\}.$$
The curve C is $\mathbb{Q}$-isomorphic to the elliptic curve `15a3`, which Mordell-Weil group (over $\mathbb{Q}$) is of order 8. Therefore we deduce that $s = -2/27, -27/2$, and in particular
$$j(E) \in \{-5^2/2, -5^2 \cdot 241^3/2^3\}.$$

[1] A remarkable fact is that this genus 2 curve is *new modular* of level 45 (see [9]).

Therefore there are two $\overline{\mathbb{Q}}$-isomorphic classes of elliptic curves. Each pair of elliptic curves in the same $\overline{\mathbb{Q}}$-isomorphic class is related by a quadratic twist. Najman [28] has made an exhaustive study of how the torsion subgroup changes upon quadratic twists. In particular Proposition 1 (c) [28] asserts that if $E/\mathbb{Q}$ is neither `50a3` nor `450b4`, and it satisfies $E(\mathbb{Q})_{\rm tors} \simeq \mathcal{C}_3$ and the (-3)-quadratic twist E^{-3}, satisfies $E^{-3}(\mathbb{Q})_{\rm tors} \not\simeq \mathcal{C}_3$, then for any quadratic twist we must have $E^d(\mathbb{Q}) \simeq \mathcal{C}_1$ for all $d \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$. We apply this result to the elliptic curves `50a1` and `450b2` that have j-invariant $-5^2/2$ and $-5^2 \cdot 241^3/2^3$ respectively. Both curves have cyclic torsion subgroup (over $\mathbb{Q}$) of order 3 and the corresponding torsion subgroup of the (-3)-quadratic twist is trivial. Thus we are left with two elliptic curves (`50a1` and `450b2`) to finish the proof. Applying the algorithm described in Section 7 we compute that the 5-torsion does not grow over any quintic number field for both curves.

- $q = 7$. Similar to the the case $q = 3$, we deduce that $E/\mathbb{Q}$ has the 7-torsion defined over $\mathbb{Q}$ and $G_E(5)$ is labeled `5B.1.2`. Looking at Table 1 we deduce that $E/\mathbb{Q}$ has a rational 5-isogeny, since $d_0 = 1$ for `5B.1.2`. Then, since $E/\mathbb{Q}$ has a point of order 7 defined over $\mathbb{Q}$, there exists a rational 35-isogeny, which contradicts Theorem 6. □

4.5. $\{p, q, r\}$**-primary torsion subgroup.**

Lemma 13. *Let $E/\mathbb{Q}$ be an elliptic curve and $K/\mathbb{Q}$ a quintic number field. Let $p, q, r \in \{2, 3, 5, 7, 11\}$, $p \neq q \neq r$, such that pqr divides the order of $E(K)_{\rm tors}$. Then $E(K)[\{p, q, r\}^\infty] = \{\mathcal{O}\}$.*

Proof. Lemma 12 shows that there do not exist three different primes p, q, r such that pqr divides the order of $E(K)_{\rm tors}$. □

5. Proof of Theorems 1, 2 and 3

We are ready to prove Theorems 1, 2 and 3.

Proof of Theorem 1. Since we have $\Phi_{\mathbb{Q}}(1) \subseteq \Phi_{\mathbb{Q}}(5)$, let us prove that the unique torsion structures that remain to add to $\Phi_{\mathbb{Q}}(1)$ to obtain $\Phi_{\mathbb{Q}}(5)$ are $\mathcal{C}_{11}$ and $\mathcal{C}_{25}$. Let $H \in \Phi_{\mathbb{Q}}(5)$ be such that $H \notin \Phi_{\mathbb{Q}}(1)$. Lemma 12 shows that $|H| = p^n$, for some prime p and a positive integer n. Now, Lemma 9 shows that $p \in \{5, 11\}$. If $p = 11$ then $n = 1$ by Lemma 11. If $p = 5$ then $n = 2$ by Lemma 10, and an example with torsion subgroup isomorphic to $\mathcal{C}_{25}$ is given in Table 3. This finish the proof for the set $\Phi_{\mathbb{Q}}(5)$.

Now the CM case. Notice that $\Phi_{\mathbb{Q}}^{\rm CM}(1) \subseteq \Phi_{\mathbb{Q}}^{\rm CM}(5) \subseteq \Phi^{\rm CM}(5)$. We have that the unique torsion structure that belongs to $\Phi^{\rm CM}(5)$ and not to $\Phi_{\mathbb{Q}}^{\rm CM}(1)$ is $\mathcal{C}_{11}$. But in Lemma 11 we have proved that the elliptic curve `121b1` has torsion subgroup isomorphic to $\mathcal{C}_{11}$ over $\mathbb{Q}(\zeta_{11})^+$. Therefore $\Phi_{\mathbb{Q}}^{\rm CM}(5) = \Phi^{\rm CM}(5)$. This finishes the proof. □

The determination of $\Phi_{\mathbb{Q}}(5, G)$ will rest on the following result:

Proposition 14. *Let $E/\mathbb{Q}$ be an elliptic curve and $K/\mathbb{Q}$ a quintic number field such that $E(\mathbb{Q})_{\rm tors} \simeq G$ and $E(K)_{\rm tors} \simeq H$.*

(1) Let $p \in \{2, 3, 7\}$ and G of order a power of p, then $H = G$.
(2) If $H = \mathcal{C}_{25}$, then $G = \mathcal{C}_5$.

Proof. The item (1) follows from Lemma 9 and (2) from Lemma 10 (3). □

Proof of Theorem 2. Let $E/\mathbb{Q}$ be an elliptic curve and $K/\mathbb{Q}$ a quintic number field such that

$$E(\mathbb{Q})_{\rm tors} \simeq G \qquad \text{and} \qquad E(K)_{\rm tors} \simeq H.$$

The group $H \in \Phi_{\mathbb{Q}}(5)$ (row in Table 2) that does not appear in some $\Phi_{\mathbb{Q}}(5, G)$ for any $G \in \Phi(1)$ (column in Table 2), with $G \subseteq H$ can be ruled out using Proposition 14. In Table 2 we use:

- (1) and (2) to indicate which part of Proposition 14 is used,
- the symbol $-$ to mean the case is ruled out because $G \not\subset H$,
- with a ✓, if the case is possible and, in fact, it occurs. There are two types of check marks in Table 2:
  - ✓ (without a subindex) means that $G = H$.
  - $\checkmark_5$ means that $H \neq G$ can be achieved over a quintic number field K, and we have collected examples of curves and quintic number fields in Table 3.

H \ G	$\mathcal{C}_1$	$\mathcal{C}_2$	$\mathcal{C}_3$	$\mathcal{C}_4$	$\mathcal{C}_5$	$\mathcal{C}_6$	$\mathcal{C}_7$	$\mathcal{C}_8$	$\mathcal{C}_9$	$\mathcal{C}_{10}$	$\mathcal{C}_{12}$	$\mathcal{C}_2 \times \mathcal{C}_2$	$\mathcal{C}_2 \times \mathcal{C}_4$	$\mathcal{C}_2 \times \mathcal{C}_6$	$\mathcal{C}_2 \times \mathcal{C}_8$
$\mathcal{C}_1$	✓	–	–	–	–	–	–	–	–	–	–	–	–	–	–
$\mathcal{C}_2$	(1)	✓	–	–	–	–	–	–	–	–	–	–	–	–	–
$\mathcal{C}_3$	(1)	–	✓	–	–	–	–	–	–	–	–	–	–	–	–
$\mathcal{C}_4$	(1)	(1)	–	✓	–	–	–	–	–	–	–	–	–	–	–
$\mathcal{C}_5$	$\checkmark_5$	–	–	–	✓	–	–	–	–	–	–	–	–	–	–
$\mathcal{C}_6$	(1)	(1)	(1)	–	–	✓	–	–	–	–	–	–	–	–	–
$\mathcal{C}_7$	(1)	–	–	–	–	–	✓	–	–	–	–	–	–	–	–
$\mathcal{C}_8$	(1)	(1)	–	(1)	–	–	–	✓	–	–	–	–	–	–	–
$\mathcal{C}_9$	(1)	–	(1)	–	–	–	–	–	✓	–	–	–	–	–	–
$\mathcal{C}_{10}$	(1)	$\checkmark_5$	–	–	(1)	–	–	–	–	✓	–	–	–	–	–
$\mathcal{C}_{11}$	$\checkmark_5$	–	–	–	–	–	–	–	–	–	–	–	–	–	–
$\mathcal{C}_{12}$	(1)	(1)	(1)	(1)	–	(1)	–	–	–	–	✓	–	–	–	–
$\mathcal{C}_{25}$	(2)	–	–	–	$\checkmark_5$	–	–	–	–	–	–	–	–	–	–
$\mathcal{C}_2 \times \mathcal{C}_2$	(1)	(1)	–	–	–	–	–	–	–	–	–	✓	–	–	–
$\mathcal{C}_2 \times \mathcal{C}_4$	(1)	(1)	–	(1)	–	–	–	–	–	–	–	(1)	✓	–	–
$\mathcal{C}_2 \times \mathcal{C}_6$	(1)	(1)	(1)	–	–	(1)	–	–	–	–	–	(1)	–	✓	–
$\mathcal{C}_2 \times \mathcal{C}_8$	(1)	(1)	–	(1)	–	–	–	(1)	–	–	–	(1)	(1)	–	✓

TABLE 2. The table displays either if the case happens for $G = H$ (✓), if it occurs over a quintic ($\checkmark_5$), if it is impossible because $G \not\subset H$ ($-$) or if it is ruled out by Proposition 14 (1) and (2).

It remains to prove that there are infinitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves $E/\mathbb{Q}$ with $H \in \Phi_{\mathbb{Q}}(5, G)$, except for the case $H = \mathcal{C}_{11}$. Note that for any elliptic curve $E/\mathbb{Q}$ with $E(\mathbb{Q})_{\text{tors}}$, there is always an extension $K/\mathbb{Q}$ of degree 5 such that $E(K)_{\text{tors}} = E(\mathbb{Q})_{\text{tors}}$. Then for any $G \in \Phi(1) \cap \Phi_{\mathbb{Q}}(5)$ the statement is proved. Now, since $\Phi_{\mathbb{Q}}(5) \setminus \Phi(1) = \{\mathcal{C}_{11}, \mathcal{C}_{25}\}$, the only case that remains to prove is $H = \mathcal{C}_{25}$. This case will be proved in Proposition 16. □

Proof of Theorem 3. Let $E/\mathbb{Q}$ be an elliptic curve such that the torsion grows to $\mathcal{C}_{11}$ over a quintic number field K. Then by Lemma 11 we know that $K = \mathbb{Q}(\zeta_{11})^+$ and the torsion does not grow for any other quintic number field. Therefore to finish the proof it remains to prove that there does not exist an elliptic curve $E/\mathbb{Q}$ and two non-isomorphic quintic number fields K_1, K_2 such that $E(K_i)_{\text{tors}} \simeq H \in \Phi_{\mathbb{Q}}(5)$, $i = 1, 2$, and $E(\mathbb{Q})_{\text{tors}} \not\simeq H$. Note that the compositum K_1K_2 satisfies $[K_1K_2 : \mathbb{Q}] \leq [K_1 : \mathbb{Q}][K_2 : \mathbb{Q}] = 25$. Now, by Theorem 2 we deduce $H \in \{\mathcal{C}_5, \mathcal{C}_{10}, \mathcal{C}_{25}\}$:

- First suppose that $H \in \{\mathcal{C}_5, \mathcal{C}_{10}\}$. Then by Lemma 10, $G_E(5)$ is labeled `5B.1.2`. Now, since $K_1 \not\simeq K_2$ we deduce $K_1K_2 = \mathbb{Q}(E[5])$ and, in particular, $\mathrm{Gal}(\widehat{K_1K_2}/\mathbb{Q}) \simeq G_E(5)$. In this case we have that $G_E(5) \simeq \mathcal{F}_5$, where $\mathcal{F}_5$ denotes the Fröbenius group of order 20. Diagram 1 shows the lattice subgroup of $\mathcal{F}_5$, where $\mathcal{H}_{k,i}$ denotes the k-th subgroup of index i in $\mathcal{F}_5$. Note that all the index 5 subgroups $\mathcal{H}_{k,5}$ are conjugates in $\mathcal{F}_5$. That is, their associated fixed quintic number fields are isomorphic. This proves that $K_1 \simeq K_2$.

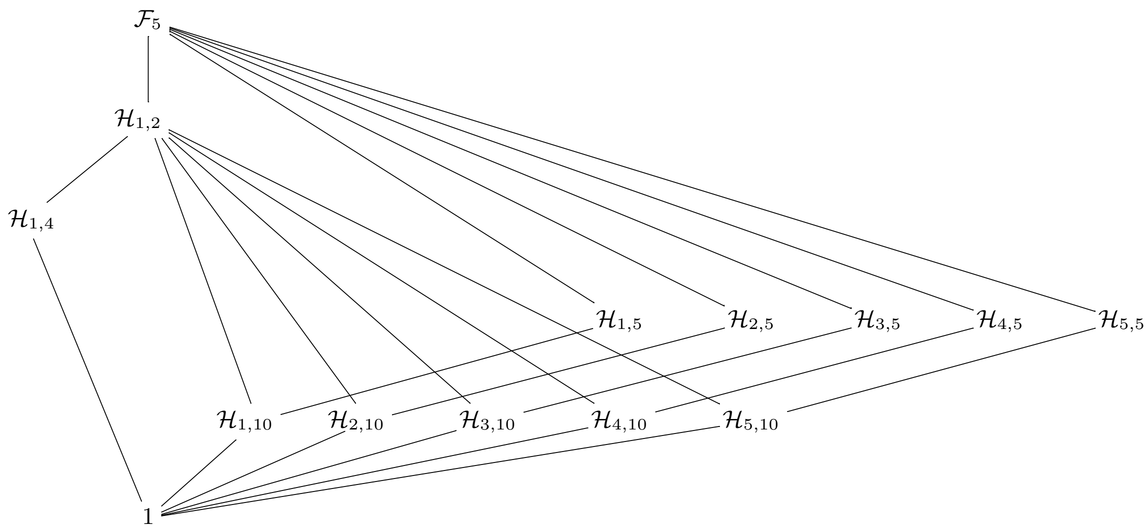

DIAGRAM 1. Lattice subgroup of $\mathcal{F}_5$

• Finally suppose that $H = \mathcal{C}_{25}$. In this case we use a similar argument as above but replacing $G_E(5)$ by $G_E(25)$. We know by Lemma 10 that $G_E(5)$ is labeled `5B.1.1` or `5Cs.1.1`, but we do not have an explicit description of $G_E(25)$. For that reason we apply an analogous algorithm as the one used in the proof of Lemma 10 (3). By [35, Theorem 1.4 (iii)]) we have that $G_E(5)$ is conjugate in $\mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$ to

$$H_{6,1} = \left\langle \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle \quad \text{or} \quad H_{1,1} = \left\langle \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \right\rangle,$$

depending if $G_E(5)$ is labeled `5B.1.1` or `5Cs.1.1` respectively.

Suppose that $K_1 \not\simeq K_2$, then $K_1K_2 = \mathbb{Q}(E[25])$. Therefore $\mathrm{Gal}(\widehat{K_1K_2}/\mathbb{Q}) \simeq G_E(25)$ and $|G_E(25)| \leq 25$. Now, we fix $\mathcal{H}$ to be $H_{6,1}$ or $H_{1,1}$ and since we do not have an explicit description of $G_E(25)$ we run a `Magma` program where the input is a subgroup G of $GL_2(\mathbb{Z}/25\mathbb{Z})$ satisfying

- $|G| \leq 25$,
- $G \equiv H \pmod 5$ for some conjugate H of $\mathcal{H}$ in $\mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$,
- there exists $v \in (\mathbb{Z}/25\mathbb{Z})^2$ of order 25 such that $[G : G_v] = 5$.

If $\mathcal{H} = H_{6,1}$ the above algorithm does not return any subgroup G. In the case $\mathcal{H} = H_{1,1}$ all the subgroups returned are isomorphic either to $\mathcal{F}_5$ or to $\mathcal{C}_{20}$. If $G \simeq \mathcal{F}_5$ then we have proved that it has five index 5 subgroups, all of them at the same conjugation class. If $G \simeq \mathcal{C}_{20}$ there is only one subgroup of index 5. We have reached a contradiction with $K_1 \not\simeq K_2$. This finishes the proof. □

6. Infinite families of rational elliptic curves where the torsion grows over a quintic number field.

Let $E/\mathbb{Q}$ be an elliptic curve and K a quintic number field such that $E(\mathbb{Q})_{\mathrm{tors}} \simeq G \in \Phi(1)$ and $E(K)_{\mathrm{tors}} \simeq H \in \Phi_{\mathbb{Q}}(5)$. Theorem 3 shows that $G \not\simeq H$ in the following cases:

$$(G, H) \in \{ (\mathcal{C}_1, \mathcal{C}_5), (\mathcal{C}_1, \mathcal{C}_{11}), (\mathcal{C}_2, \mathcal{C}_{10}), (\mathcal{C}_5, \mathcal{C}_{25}) \}.$$

By Lemma 11 we have that the pair $(\mathcal{C}_1, \mathcal{C}_{11})$ only occurs in three elliptic curves. For the rest of the above pairs we are going to prove that there are infinitely many non–isomorphic classes of elliptic curves and quintic number fields satisfying each pair.

6.1. $(\mathcal{C}_1, \mathcal{C}_5)$ **and** $(\mathcal{C}_2, \mathcal{C}_{10})$**.** Let $E/\mathbb{Q}$ be an elliptic curve and K a quintic number field such that $E(\mathbb{Q})[5] = \{\mathcal{O}\}$ and $E(K)[5] \simeq \mathcal{C}_5$. Then Theorem 2 tells us that:

$$E(\mathbb{Q})_{\rm tors} \simeq \mathcal{C}_1 \text{ and } E(K)_{\rm tors} \simeq \mathcal{C}_5, \qquad \text{or} \qquad E(\mathbb{Q})_{\rm tors} \simeq \mathcal{C}_2 \text{ and } E(K)_{\rm tors} \simeq \mathcal{C}_{10}.$$

First notice that E has non-CM, since $\mathcal{C}_5$ is not a subgroup of any group in $\Phi^{\rm CM}(5)$. Then Lemma 10 shows that $G_E(5)$ is labeled `5B.1.2` ($H_{5,1}$ in Zywina's notation). Then Zywina [35, Theorem 1.4(iii)] proved that there exists $t \in \mathbb{Q}$ such that E is isomorphic (over $\mathbb{Q}$) to $\mathcal{E}_{5,t}$:

$$\mathcal{E}_{5,t} \,:\, y^2 = x^3 - 27(t^4 + 228t^3 + 494t^2 - 228t + 1)x + 54(t^6 - 522t^5 - 10005t^4 - 10005t^2 + 522t + 1).$$

Table 1 shows that the degree of the field of definition of a point of order 5 in E is 4 or 5. Moreover, we can compute explicitly the number fields factorizing the 5-division polynomial $\psi_5(x)$ attached to E. We define the following polynomial of degree 5:

$$\begin{aligned} p_5(x) = x^5 &+ (-15t^2 - 450t - 15)x^4 + (90t^4 - 65880t^3 + 22860t^2 + 11880t + 90)x^3 \\ &+(-270t^6 - 1015740t^5 - 7086690t^4 + 5725080t^3 - 4520610t^2 - 82620t - 270)x^2 \\ &+(405t^8 - 8874360t^7 - 58872420t^6 - 253721160t^5 - 1423822050t^4 + 637175160t^3 + 18109980t^2 \\ &+223560t + 405)x - 243t^{10} - 22886226t^9 - 485812647t^8 + 3223702152t^7 - 34272829350t^6 \\ &-21920257260t^5 - 53316735462t^4 - 2958964344t^3 - 74726631t^2 - 211410t - 243. \end{aligned}$$

Then $p_5(x)$ divides $\psi_5(x)$ and we have $E(\mathbb{Q}(\alpha))[5] = \langle R \rangle \simeq \mathcal{C}_5$, where $p_5(\alpha) = 0$ and α is the x-coordinate of R.

Now suppose that $E(\mathbb{Q})_{\rm tors} \simeq \mathcal{C}_2$, then $G_E(2)$ is labeled `2B`. Then Zywina [35, Theorem 1.1] proved that its j-invariant is of the form

$$J_2(s) = 256\frac{(s+1)^3}{s}, \qquad \text{for some } s \in \mathbb{Q}.$$

Therefore we have $J_2(s) = j(\mathcal{E}_{5,t})$ for some $s, t \in \mathbb{Q}$. In other words we have a solution of the next equation

$$256\frac{(s+1)^3}{s} = \frac{(t^4 + 228t^3 + 494t^2 - 228t + 1)^3}{t(t^2 - 11t - 1)^5}.$$

This equation defines a curve C of genus 0 with $(0,0) \in C(\mathbb{Q})$, which can be parametrize (according to `Magma` and making a linear change of the projective coordinate in order to simplify the parametrization) by:

$$(s,t) = \left(\frac{-512(5r+1)(5r^2-1)^5}{(5r-1)(5r+3)(5r^2+10r+1)^5} \,,\, \frac{2(5r+3)^2}{(5r-1)^2(5r+1)} \right), \qquad \text{where } r \in \mathbb{Q}.$$

Finally, replacing the above value for t in $\mathcal{E}_{5,t}$ and simplifying the Weierstrass equation we obtain:

$$E_r : y^2 = x^3 - 2(5r^2 + 2r + 1)(5r^4 - 40r^3 - 30r^2 + 1)x^2 + 84375(5r-1)(5r+3)(5r^2 + 10r + 1)^5 x.$$

Thus we have proved the following result:

Proposition 15. *There exist infinitely many $\overline{\mathbb{Q}}$-isomorphic classes of elliptic curves $E/\mathbb{Q}$ such that $E(\mathbb{Q})_{\rm tors} \simeq \mathcal{C}_1$ (resp. $\mathcal{C}_2$) and infinitely many quintic number fields K such that $E(K)_{\rm tors} \simeq \mathcal{C}_5$ (resp. $\mathcal{C}_{10}$).*

6.2. $(\mathcal{C}_5, \mathcal{C}_{25})$. Let $E/\mathbb{Q}$ be an elliptic curve such that $G_E(5)$ is labeled by `5B.1.1` and there exists a quintic number field K with the property $E(K)_{\rm tors} \simeq \mathcal{C}_{25}$. Then, by Lemma 10 (3), K is Galois. In particular $E/\mathbb{Q}$ has a rational 25-isogeny. Then, we observe in [24, Table 3] that its j-invariant must be of the form:

$$j_{25}(h) = \frac{(h^{10}+10h^8+35h^6-12h^5+50h^4-60h^3+25h^2-60h+16)^3}{(h^5+5h^3+5h-11)}, \qquad \text{for some } h \in \mathbb{Q}.$$

On the other hand, Zywina [35, Theorem 1.4(iii)] proved that there exists $s \in \mathbb{Q}$ such that E is isomorphic (over $\mathbb{Q}$) to $\mathcal{E}_{6,s}$:

$$\mathcal{E}_{6,s} \,:\, y^2 = x^3 - 27(s^4-12s^3+14s^2+12s+1)x + 54(s^6-18s^5+75s^4+75s^2+18s+1).$$

The above j-invariants should be equal, so $j(\mathcal{E}_{6,s}) = j_{25}(h)$ for some $s, h \in \mathbb{Q}$. This equality defines a non-irreducible curve over $\mathbb{Q}$ whose irreducible components are a genus 16 curve and a genus 0 curve. It is possible to give a parametrization of the above genus 0 curve such that $s = t^5$, where $t \in \mathbb{Q}$. That is, there exists $t \in \mathbb{Q}$ such that E is $\mathbb{Q}$-isomorphic to $\mathcal{E}_{6,t^5}$.

Now, let us define the quintic polynomial $p_{25}(x)$:

$$\begin{aligned}
p_{25}(x) = {}& x^5 + (-5t^{10} - 12t^8 - 12t^7 - 24t^6 + 30t^5 - 60t^4 + 36t^3 - 24t^2 + 12t - 5)x^4 \\
&+(10t^{20} + 48t^{18} + 48t^{17} + 96t^{16} + 24t^{15} + 240t^{14} - 144t^{13} + 96t^{12} - 48t^{11} + 236t^{10} + 48t^8 + 48t^7 + 96t^6 \\
&-264t^5 + 240t^4 - 144t^3 + 96t^2 - 48t + 10)x^3 + (-10t^{30} - 72t^{28} - 72t^{27} - 144t^{26} - 252t^{25} - 360t^{24} \\
&+216t^{23} - 144t^{22} + 72t^{21} + 1914t^{20} + 720t^{18} + 720t^{17} + 1440t^{16} - 1800t^{15} + 3600t^{14} - 2160t^{13} + 1440t^{12} \\
&-720t^{11} + 1914t^{10} - 72t^8 - 72t^7 - 144t^6 + 612t^5 - 360t^4 + 216t^3 - 144t^2 + 72t - 10)x^2 \\
&+(5t^{40} + 48t^{38} + 48t^{37} + 96t^{36} + 312t^{35} + 240t^{34} - 144t^{33} + 96t^{32} - 48t^{31} - 4516t^{30} - 1584t^{28} - 1584t^{27} \\
&-3168t^{26} + 19944t^{25} - 7920t^{24} + 4752t^{23} - 3168t^{22} + 1584t^{21} - 18114t^{20} - 1584t^{18} - 1584t^{17} - 3168t^{16} - \\
&12024t^{15} - 7920t^{14} + 4752t^{13} - 3168t^{12} + 1584t^{11} - 4516t^{10} + 48t^8 + 48t^7 + 96t^6 - 552t^5 + 240t^4 - 144t^3 \\
&+96t^2 - 48t + 5)x - t^{50} - 12t^{48} - 12t^{47} - 24t^{46} - 114t^{45} - 60t^{44} + 36t^{43} - 24t^{42} + 12t^{41} + 2371t^{40} \\
&+816t^{38} + 816t^{37} + 1632t^{36} - 17880t^{35} + 4080t^{34} - 2448t^{33} + 1632t^{32} - 816t^{31} + 47294t^{30} - 13896t^{28} \\
&-13896t^{27} - 27792t^{26} + 34740t^{25} - 69480t^{24} + 41688t^{23} - 27792t^{22} + 13896t^{21} + 47294t^{20} + 816t^{18} + \\
&816t^{17} + 1632t^{16} + 13800t^{15} + 4080t^{14} - 2448t^{13} + 1632t^{12} - 816t^{11} + 2371t^{10} - 12t^8 - 12t^7 - 24t^6 \\
&+174t^5 - 60t^4 + 36t^3 - 24t^2 + 12t - 1.
\end{aligned}$$

Then $p_{25}(x)$ divides the 25-division polynomial of $\mathcal{E}_{6,t^5}$. Fixing $t \in \mathbb{Q}$, we have that $\mathbb{Q}(\alpha)/\mathbb{Q}$ is a Galois extension of degree 5 and $E(\mathbb{Q}(\alpha)) = \langle R \rangle \simeq \mathcal{C}_{25}$, where $p_{25}(\alpha) = 0$ and the x-coordinate of R is 3α. Note that $[5]R = (3t^{10} - 18t^5 + 3, 108t^5) \in E(\mathbb{Q})$.

We have proved the following result:

Proposition 16. *There exist infinitely many $\overline{\mathbb{Q}}$-isomorphic classes of elliptic curves $E/\mathbb{Q}$ and infinitely many quintic number fields K such that $E(K)_{\rm tors} \simeq \mathcal{C}_{25}$. All of them satisfy $E(\mathbb{Q})_{\rm tors} \simeq \mathcal{C}_5$.*

6.2.1. *A 5-triangle tale.* Let $E/\mathbb{Q}$ be an elliptic curve such that $G_E(5)$ is labeled by `5Cs.1.1` ($H_{1,1}$ in Zywina's notation). Zywina [35, Theorem 1.4(iii)] proved that there exists $t \in \mathbb{Q}$ such that E is isomorphic (over $\mathbb{Q}$) to $\mathcal{E}_{1,t} = \mathcal{E}_{5,t^5}$. We observe in Table 1 that there exists a $\mathbb{Z}/5\mathbb{Z}$-basis $\{P_1, P_2\}$ of $E[5]$ such that $E(\mathbb{Q})_{\rm tors} = \langle P_2 \rangle \simeq \mathcal{C}_5$, $E(\mathbb{Q}(\zeta_5))_{\rm tors} = E[5] = \langle P_1, P_2 \rangle$. Now, since $\langle P_1 \rangle$ and $\langle P_2 \rangle$ are distinct $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable cyclic subgroups of $E(\overline{\mathbb{Q}})$ of order 5, there exist two rational 5-isogenies:

$$E_1 \xleftarrow{\ \phi_1\ } E \xrightarrow{\ \phi_2\ } E_2,$$

where the elliptic curves $E_1 = E/\langle P_1\rangle$ and $E_2 = E/\langle P_2\rangle$ are defined over $\mathbb{Q}$. Using Velu's formulae we can compute explicit equations of these elliptic curves:

$$E_1 = \mathcal{E}_{6,t^5}, \qquad E_2 = \mathcal{E}_{5,s(t)}, \text{ where } s(t) = \frac{t(t^4+3\,t^3+4\,t^2+2\,t+1)}{t^4-2\,t^3+4\,t^2-3\,t+1},$$

Then we have $G_{E_1}(5)$ is labeled by `5B.1.1` and $G_{E_2}(5)$ is labeled by `5B.1.2`. We observe that the elliptic curve E_1 is the one obtained in the previous section, that is, $E_1(\mathbb{Q}(\alpha)) = \langle R\rangle \simeq \mathcal{C}_{25}$, where $p_{25}(\alpha) = 0$ and the x-coordinate of R is 3α. In particular, E_1 has a rational 25-isogeny. Note that $[5]R = Q_2 = (3t^{10} - 18t^5 + 3, 108t^5)$ is such that $E_1(\mathbb{Q})[5] = \langle Q_2\rangle \simeq \mathcal{C}_5$ and $E_1(L)[5] = E_1[5] = \langle Q_1, Q_2\rangle$ with $[L : \mathbb{Q}] = 20$. If $\widehat{\phi_1} : E_1 \longrightarrow E$ denotes the dual isogeny of ϕ_1, then we have $\phi_2 \circ \widehat{\phi_1}(\langle R\rangle) = \mathcal{O} \in E_2$. That is, $\phi_2 \circ \widehat{\phi_1},: E_2 \longrightarrow E_1$ is a rational 25-isogeny.

Remark. *There are only seven elliptic curves (**11a1**, **550k2**, **1342c2**, **33825be2**, **165066d2**, **185163a2** and **192698c2**) with conductor less than* 350.000 *such that the corresponding mod* 5 *Galois representation is labeled **5Cs.1.1**. All of them give the corresponding* 5*-triangle with the associated elliptic curve (**11a3**, **550k3**, **1342c1**, **33825be3**, **165066d1**, **185163a1** and **192698c1** resp.) with* $\mathcal{C}_{25}$ *torsion over the corresponding quintic number field. Notice that there are no more elliptic curves with conductor less than* 350.000 *and torsion isomorphic to* $\mathcal{C}_{25}$ *over a quintic number field.*

7. EXAMPLES

Given an elliptic curve $E/\mathbb{Q}$, we describe a method to compute the quintic number field where the torsion could grow. If E is `121a2`, `121c2` or `121b1` we have proved in Lemma 11 that the torsion grows to $\mathcal{C}_{11}$ over the quintic number field $\mathbb{Q}(\zeta_{11})^+$. For the rest of the elliptic curves, we first compute $E(\mathbb{Q})_{\text{tors}} \simeq G \in \Phi(1)$. If $G \neq \mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_5$, then by Theorem 2 the torsion remains stable under any quintic extension. If $G = \mathcal{C}_1$ or $\mathcal{C}_2$ then, by Theorem 2, the torsion could grow to $\mathcal{C}_5$ or $\mathcal{C}_{10}$ respectively. Now compute the 5-division polynomial $\psi_5(x)$. It follows that the quintic number fields where the torsion could grow are contained in the number fields attached to the degree 5 factors of $\psi_5(x)$. In the case $G = \mathcal{C}_5$ the torsion could grow to $\mathcal{C}_{25}$, and the method is similar, replacing the 5-division polynomial by the 25-division polynomial. We explain this method with an example.

Example. *Let E be the elliptic curve **11a2**. We compute $E(\mathbb{Q})_{\text{tors}} \simeq \mathcal{C}_1$. Now, the* 5*-division polynomial has two degree* 5 *irreducible factors: $p_1(x)$ and $p_2(x)$. Let $\alpha_i \in \overline{\mathbb{Q}}$ such that $p_i(\alpha_i) = 0$, $i = 1, 2$. We deduce $\mathbb{Q}(\sqrt[5]{11}) = \mathbb{Q}(\alpha_1) = \mathbb{Q}(\alpha_2)$ and $E(\mathbb{Q}(\sqrt[5]{11}))_{\text{tors}} \simeq \mathcal{C}_5$.*

Table 3 shows examples where the torsion grows over a quintic number field. Each row shows the label of an elliptic curve $E/\mathbb{Q}$ such that $E(\mathbb{Q})_{\text{tors}} \simeq G$, in the first column, and $E(K)_{\text{tors}} \simeq H$, in the second column, and the quintic number field K in the third column.

G	H	quintic	label
$\mathcal{C}_1$	$\mathcal{C}_5$	$\mathbb{Q}(\sqrt[5]{11})$	`11a2`
	$\mathcal{C}_{11}$	$\mathbb{Q}(\zeta_{11})^+$	`121a2` , `121c2` , `121b1`
$\mathcal{C}_2$	$\mathcal{C}_{10}$	$\mathbb{Q}(\sqrt[5]{12})$	`66c3`
$\mathcal{C}_5$	$\mathcal{C}_{25}$	$\mathbb{Q}(\zeta_{11})^+$	`11a3`

TABLE 3. Examples of elliptic curves such that $G \in \Phi(1)$, $H \in \Phi_{\mathbb{Q}}(5, G)$ and $G \neq H$.

Remark. *Note that, although we have proved in Propositions 15 and 16 that there are infinitely many elliptic curves over* $\mathbb{Q}$ *such that the torsion grows over a quintic number field, these elliptic curve seems to appear not very often. We have computed for all elliptic curves over* $\mathbb{Q}$ *with conductor less than* 350.000 *from* [6] *(a total of* 2.188.263 *elliptic curves) and we have found only* 1256 *cases where the torsion grows. Moreover, only* 40 *cases when it grows to* $\mathcal{C}_{10}$ *and* 7 *to* $\mathcal{C}_{25}$ *(the elliptic curves* `11a3`, `550k3`, `1342c1`, `33825be3` `165066d1`, `185163a1` *and* `192698c1`*).*

Acknowledgements. *We thank Álvaro Lozano-Robledo, Filip Najman, and David Zureick-Brown for useful conversations. The author would like to thank the anonymous referee for useful comments and suggestions.*

References

[1] B.J. Birch and W. Kuyk (eds.), *Modular Functions of One Variable IV*. Lecture Notes in Mathematics **476**. Springer (1975). 3

[2] W. Bosma, J. Cannon, C. Fieker, and A. Steel (eds.). *Handbook of Magma functions, Edition 2.20*. http://magma.maths.usyd.edu.au/magma, 2015. 6

[3] P. Bruin and F. Najman, *A criterion to rule out torsion groups for elliptic curves over number fields*, Res. Number Theory **2**, 3 (2016). 9

[4] M. Chou, Torsion of rational elliptic curves over quartic Galois number fields. J. Number Theory **160** (2016), 603–628. 2, 5

[5] P. L. Clark, P. Corn, A. Rice, and J. Stankewicz. *Computation on elliptic curves with complex multiplication*, LMS J. Comput. Math. **17** (2014), 509–539. 2

[6] J.E. Cremona, *Elliptic curve data for conductors up to 350.000.* Available on http://johncremona.github.io/ecdata/, 2015. 3, 16

[7] M. Derickx and A. V. Sutherland, *Torsion subgroups of elliptic curves over quintic and sextic number fields.* Proc. Amer. Math. Soc., to appear. 1

[8] G. Fung, H. Ströher, H. Williams, and H. Zimmer. *Torsion groups of elliptic curves with integral j-invariant over pure cubic fields*. J. Number Theory **36** (1990) 12–45. 2

[9] E. González-Jiménez and J. González. *Modular curves of genus 2*. Math. Comp. **72** (2003) 397–418. 9

[10] E. González-Jiménez and Á. Lozano–Robledo, *On torsion of rational elliptic curves over quartic fields.* Math. Comp., to appear. 2, 3, 9

[11] E. González–Jiménez and F. Najman, *Growth of torsion groups of elliptic curves upon base changes.* arXiv:1609.02515. 2

[12] E. González–Jiménez, F. Najman, and J.M. Tornero, *Torsion of rational elliptic curves over cubic fields.* Rocky Mountain J. Math. **46** (2016), no. 6, 1899–1917. 2, 3

[13] E. González–Jiménez and J.M. Tornero, *Torsion of rational elliptic curves over quadratic fields.* Rev. R. Acad. Cienc. Exactas Fís. Nat. Ser. A Math. RACSAM **108** (2014), 923–934. 2

[14] E. González–Jiménez and J.M. Tornero, *Torsion of rational elliptic curves over quadratic fields II.* Rev. R. Acad. Cienc. Exactas Fís. Nat. Ser. A Math. RACSAM **110** (2016), 121–143. 3

[15] D. Jeon, C.H. Kim, and A. Schweizer, *On the torsion of elliptic curves over cubic number fields*, Acta Arith. **113** (2004), 291–301. 1

[16] D. Jeon, C.H. Kim, and E. Park, *On the torsion of elliptic curves over quartic number fields*, J. London Math. Soc. (2) **74** (2006), 1–12. 1

[17] S. Kamienny, *Torsion points on elliptic curves and q–coefficients of modular forms*. Invent. Math. **109** (1992) 129–133. 1

[18] M. A. Kenku, *The modular curve $X_0(39)$ and rational isogeny*, Math. Proc. Cambridge Philos. Soc. **85** (1979), 21–23. 5

[19] M. A. Kenku, *The modular curves $X_0(65)$ and $X_0(91)$ and rational isogeny*, Math. Proc. Cambridge Philos. Soc. **87** (1980), 15–20. 5

[20] M. A. Kenku, *The modular curve $X_0(169)$ and rational isogeny*, J. London Math. Soc. (2) **22** (1980), 239–244. 5

[21] M. A. Kenku, *The modular curve $X_0(125)$, $X_1(25)$ and $X_1(49)$*, J. London Math. Soc. (2) **23** (1981), 415–427. 5

[22] M.A. Kenku and F. Momose, *Torsion points on elliptic curves defined over quadratic fields.* Nagoya Math. J. **109** (1988) 125–149. 1

[23] S. Kwon, *Torsion subgroups of elliptic curves over quadratic extensions.* J. Number Theory **62** (1997) 144–162. 2

[24] A. Lozano–Robledo. *On the field of definition of p-torsion points on elliptic curves over the rationals*. Math. Ann. **357** (2013) 279–305. 6, 14
[25] B. Mazur, *Rational isogenies of prime degree*. Invent. Math. **44** (1978) 129–162. 1, 5
[26] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*. Invent. Math. **124** (1996), 437–449. 1
[27] H. Müller, H. Ströher, and H. Zimmer, *Torsion groups of elliptic curves with integral j-invariant over quadratic fields*. J. Reine Angew. Math. **397** (1989) 100–161. 2
[28] F. Najman, *The number of twists with large torsion of an elliptic curve*. Rev. R. Acad. Cienc. Exactas Fis. Nat. Ser. A Math. RACSAM **109** (2015), 535–547. 10
[29] F. Najman, *Torsion of elliptic curves over cubic fields and sporadic points on $X_1(n)$*. Math. Res. Letters, **23** (2016) 245–272. 2
[30] L. Olson, *Points of finite order on elliptic curves with complex multiplication*. Manuscripta Math. **14** (1974) 195–205. 1
[31] A. Pethő, T. Weis, and H. Zimmer, *Torsion groups of elliptic curves with integral j-invariant over general cubic number fields*. Int. J. Algebra Comput. **7** (1997) 353–413. 2
[32] J. H. Silverman, *The arithmetic of elliptic curves*, Second Edition, Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.
[33] J-H. Silverman, *Advanced topics in the arithmetic of elliptic curves*. Graduate Texts in Mathematics, vol. 151. Springer-Verlag, New York, 1994. 8
[34] A.V. Sutherland, *Computing images of Galois representations attached to elliptic curves*. Forum Math. Sigma **4** (2016), e4, 79 pp. 3, 4
[35] D. Zywina, *On the possible images of the mod ℓ representations associated to elliptic curves over $\mathbb{Q}$*. arXiv:1508.07660. 4, 6, 7, 8, 9, 12, 13, 14

Universidad Autónoma de Madrid, Departamento de Matemáticas, Madrid, Spain
E-mail address: enrique.gonzalez.jimenez@uam.es