TORSION OF RATIONAL ELLIPTIC CURVES OVER QUADRATIC FIELDS

ENRIQUE GONZÁLEZ–JIMÉNEZ AND JOSÉ M. TORNERO

Abstract. Let E be an elliptic curve defined over $\mathbb{Q}$. We study the relationship between the torsion subgroup $E(\mathbb{Q})_{\text{tors}}$ and the torsion subgroup $E(K)_{\text{tors}}$, where K is a quadratic number field.

1. Introduction

Let E 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. So it can be written as $E(K) \simeq E(K)_{\text{tors}} \oplus \mathbb{Z}^r$, for some non-negative integer r (rank of $E(K)$) and some finite torsion subgroup $E(K)_{\text{tors}}$. It is well known that there exist two positive integers n, m such that $E(K)_{\text{tors}}$ is isomorphic to $\mathcal{C}_n \times \mathcal{C}_m$, where $\mathcal{C}_n$ is the cyclic group of order n [24].

This paper focuses on a particular problem concerning the torsion part, which we will explain now. We define sets $S(d)$ and $\Phi(d)$ as follows:

- $S(d)$ is the set of primes that can appear as the order of a torsion point of an elliptic curve E defined over a number field of degree d.
- $\Phi(d)$ is the set of possible groups that can appear as the torsion subgroup of an elliptic curve defined over a certain number field K of degree d.

Mazur's landmark papers [17, 18] established that $S(1) = \{2, 3, 5, 7\}$ and

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

After this, a long series of papers by Kenku, Momose and Kamienny ending in [10, 12] slowly unfolded the quadratic case to finally reach a full description of $S(2) = \{2, 3, 5, 7, 11, 13\}$ and $\Phi(2)$:

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

We do not have, as of today, such a precise description of $\Phi(d)$ for $d \geq 3$ although work by Parent [22] has obtained $S(3)$ and Derickx, Kamienny, Stein and Stoll have announced [4] that they have established the sets $S(d)$ for $d = 4, 5$. A fundamental result here is the celebrated Uniform Boundness Theorem, a long–standing conjecture finally proved by Merel [19], which states that there exists a constant $B(d)$ such that $|G| \leq B(d)$, for all $G \in \Phi(d)$. Although Merel's proof was not explicit, further versions (an Oesterlé's 1994 unpublished paper and Parent [23]) have given precise values for $B(d)$.

2010 *Mathematics Subject Classification.* Primary: 11G05,11R11; Secondary:14G05.

Key words and phrases. Elliptic curves, Torsion subgroup, rationals, quadratic fields.

The first author was partially supported by the grant MTM2012–35849. The second author was partially supported by the grants FQM–218 and P08–FQM–03894, FSE and FEDER (EU).

Let us fix some useful notations:

- Let E be an elliptic curve defined over a number field. Without loss of generality we can assume E is defined by a short Weierstrass form
$$E : Y^2 = X^3 + AX + B; \quad A, B \in K,$$
and we will write,
$$E(K) = \big\{(x, y) \in K^2 \mid y^2 = x^3 + Ax + B\big\} \cup \{\mathcal{O}\},$$
the set of K–rational points of E, and $\mathcal{O}$ its point at infinity.
- Let $S_{\mathbb{Q}}(d)$ be the set of primes that can appear as the order of a torsion point defined over a number field of degree d, on an elliptic curve E defined over the rationals.
- 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.
- 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 $E(K)[n]$ be the set of points in $E[n]$ with coordinates in K, for any number field K (including the case $K = \mathbb{Q}$).
- 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 square–free integer D, let E_D denote its quadratic twist. That is, the elliptic curve with a Weierstrass equation $E_D : DY^2 = X^3 + AX + B$.

Please mind that, in the sequel, for examples and precise curves we will use the Antwerp–Cremona tables and labels [1, 3].

The set $S_{\mathbb{Q}}(d)$ is known for $d \leq 42$, and there is a conjectural description by Lozano–Robledo [16] which encompasses both the known cases and experimental data. For example, $S_{\mathbb{Q}}(1) = S_{\mathbb{Q}}(2) = \{2, 3, 5, 7\}$. The sets $\Phi_{\mathbb{Q}}(d)$ have been completely described by Najman [20] for $d = 2, 3$. Concretely, he proved:

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

The remarkable fact is that although the set $\Phi(3)$ is still unknown, Najman has determined the set $\Phi_{\mathbb{Q}}(3)$.

It is also worth noting that Fujita [6] has explicitely determined the torsion subgroups over the maximal elementary 2–extension of $\mathbb{Q}$ (that is $\mathbb{Q}\left(\{\sqrt{m} \mid m \in \mathbb{Z}\}\right)$ that may arise from an elliptic curve defined over $\mathbb{Q}$. This classification might be of great help in the open problems that we will pose later.

Definition 1. *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 a certain number field K of degree d, of an elliptic curve E defined over the rationals, such that $E(\mathbb{Q})_{\rm tors} = G$.*

Our aim in this paper is, first to compute and then to understand better, $\Phi_{\mathbb{Q}}(2, G)$. That is, the behaviour of a particular torsion group of $\Phi(1)$ when we enlarge the base field $\mathbb{Q}$ by means of a quadratic extension.

In order to guess what $\Phi_{\mathbb{Q}}(2, G)$ may look like, we carried out an exhaustive computation, obtaining the groups $E(K)_{\text{tors}}$, for all curves E defined over the rationals with conductor less than 300000 from [3]. The main result of this paper is the following:

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

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

2. The set $\Phi_{\mathbb{Q}}(2, G)$

A very important and partial result of our problem, concretely the case of G being non–cyclic, has already been completely solved by Kwon [14]. More precisely, the result goes as follows:

$$\text{(1)} \qquad \Phi_{\mathbb{Q}}(2, \mathcal{C}_2 \times \mathcal{C}_{2n}) = \begin{cases} \{\mathcal{C}_2 \times \mathcal{C}_{2m} \mid m = 1, 2, 3, 4, 6\} & \text{if } n = 1, \\ \{\mathcal{C}_2 \times \mathcal{C}_{2m} \mid m = 2, 4\} \cup \{\mathcal{C}_4 \times \mathcal{C}_4\} & \text{if } n = 2, \\ \{\mathcal{C}_2 \times \mathcal{C}_{2m} \mid m = 3, 6\} & \text{if } n = 3, \\ \{\mathcal{C}_2 \times \mathcal{C}_8\} & \text{if } n = 4. \end{cases}$$

The last three cases were carefully detailed, including necessary and sufficient conditions on the coefficients of a short Weierstrass equation of the elliptic curve and the discriminant of the quadratic field, to determine which of the possible groups actually happened for a given case. The first case, however, lacked of characterisation and it is determined by ruling the other possibilities out. This appears to be a common fact in the study of torsion subgroups: the simpler the structure is, the more difficult becomes to describe in effective terms (see, for instance, [7]).

The next auxiliary result is a particular case of Lemma 1.1 in [15]. However, we need some details from the proof (see [2]).

Theorem 3. *Let E be an elliptic curve defined over $\mathbb{Q}$, D a square-free integer and $K = \mathbb{Q}(\sqrt{D})$. There exists a pair of homomorphisms*

$$E(K) \xrightarrow{\Psi} E(\mathbb{Q}) \times E_D(\mathbb{Q}) \xrightarrow{\overline{\Psi}} E(K)$$

such that $\overline{\Psi}\circ\Psi=[2]$ *and* $\Psi\circ\overline{\Psi}=[2]\times[2]$.

Moreover, $\ker(\Psi)\subset E(K)[2]$, $\ker(\overline{\Psi})\subset E(\mathbb{Q})[2]\times E_D(\mathbb{Q})[2]$ *and* $\operatorname{coker}(\Psi)$, $\operatorname{coker}(\overline{\Psi})$ *are groups where every non–zero element has order* 2.

Proof. Let σ be the non–trivial element of $\mathrm{Gal}(K/\mathbb{Q})$ and $\alpha\in K$. Let us write, for any $P=(x,y)$,

$$\sigma P=(\sigma(x),\sigma(y))\quad\text{and}\quad\phi(P,\alpha)=(x,\alpha y).$$

Recall the canonical K–isomorphisms between E and its D–twist E_D:

$$\begin{tikzcd} E(K) \arrow[r, "\phi(\,\cdot\,,1/\sqrt{D})"] & E_D(K) \arrow[r, "\phi(\,\cdot\,,\sqrt{D})"] & E(K) \end{tikzcd}$$

Let $P\in E(K)$. As $\sigma(P+\sigma P)=P+\sigma P$, we have $P+\sigma P\in E(\mathbb{Q})$. Consider now $P-\sigma P$. We have that, either $\sigma(P-\sigma P)=\mathcal{O}$, in which case $P=\sigma P$ and $P\in E(\mathbb{Q})$, or $\sigma(P-\sigma P)=-(P-\sigma P)\neq\mathcal{O}$. Should this be the case, if we write $R=P-\sigma P=(x_R,y_R)$ we have $\sigma(x_R,y_R)=(x_R,-y_R)$. Therefore, $y_R=z_R\sqrt{D}$ for some $z_R\in\mathbb{Q}$, and in this case it is clear that

$$\phi\left((x_R,y_R),1/\sqrt{D}\right)=(x_R,z_R)\in E_D(\mathbb{Q}).$$

So we define Ψ as follows:

$$\begin{array}{rcl}\Psi:E(K) & \longrightarrow & E(\mathbb{Q})\times E_D(\mathbb{Q})\\ P & \longmapsto & \left(P+\sigma P,\ \phi\left(P-\sigma P,1/\sqrt{D}\right)\right)\end{array}$$

Ψ is clearly a homomorphism: it is straightforward if we write it

$$\Psi:E(K)\longrightarrow E(K)\times E_D(K),$$

and we have just shown $\mathrm{Im}(\Psi)\subset E(\mathbb{Q})\times E_D(\mathbb{Q})$.

On the other hand, let us consider a point $R=(x_R,y_R)\in E_D(\mathbb{Q})$. Clearly

$$\phi(R,\sqrt{D})=\left(x_R,y_R\sqrt{D}\right)\in E(K),$$

and we define then

$$\begin{array}{rcl}\overline{\Psi}:E(\mathbb{Q})\times E_D(\mathbb{Q}) & \longrightarrow & E(K)\\ (P,R) & \longmapsto & P+\phi(R,\sqrt{D}).\end{array}$$

Analogously, it is not difficult to see $\overline{\Psi}$ is a homomorphism. We could have defined (exactly the same way) $\overline{\Psi}:E(K)\times E_D(K)\longrightarrow E(K)$; which is clearly a homomorphism, and then we have it restricted to the subgroup $E(\mathbb{Q})\times E_D(\mathbb{Q})$.

With these definitions, the results from the theorem can be easily deduced. □

Corollary 4. *Let E be an elliptic curve defined over $\mathbb{Q}$, D an square-free integer and $K=\mathbb{Q}(\sqrt{D})$. If n is odd, then there exists an isomorphism*

$$E(K)[n]\simeq E(\mathbb{Q})[n]\times E_D(\mathbb{Q})[n].$$

Our description of $\Phi_{\mathbb{Q}}(2,G)$, for the eleven cyclic groups in $\Phi(1)$, will rest in the following result:

Theorem 5. *Let E be an elliptic curve defined over $\mathbb{Q}$, K a quadratic number field, $G\in\Phi_{\mathbb{Q}}(1)$ and $H\in\Phi_{\mathbb{Q}}(2)$ such that $E(\mathbb{Q})_{\mathrm{tors}}\simeq G$ and $E(K)_{\mathrm{tors}}\simeq H$.*

(i) *If $\mathbb{Q}(E[3])=\mathbb{Q}\left(\sqrt{-3}\right)$, then $\mathcal{C}_3\subset G$.*

(ii) *If $\mathcal{C}_2\not\subset G$, then $\mathcal{C}_2\not\subset H$.*

(iii) *If G is cyclic, $\mathcal{C}_2 \subseteq G$ and $\mathcal{C}_4 \not\subset G$, then $\mathcal{C}_2 \times \mathcal{C}_4 \not\subset H$.*
(iv) *If $G = \mathcal{C}_4$, then $H \neq \mathcal{C}_{16}$.*
(v) *If $G = \mathcal{C}_3$, then $H \neq \mathcal{C}_9$.*
(vi) *If $H = \mathcal{C}_{15}$, then $G = \mathcal{C}_3$ or $G = \mathcal{C}_5$.*

Proof. (i) is Proposition 2.1 from [21]. Note (see Section 3) that if $E(K)$ has full 3–torsion, then $K = \mathbb{Q}\left(\sqrt{-3}\right)$.

(ii) Direct, as the hypothesis implies the irreducibility of $X^3 + AX + B$ over $\mathbb{Q}$ (hence over K).

(iii) With no loss of generality, assume E to have the form

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

If $\mathcal{C}_2 \times \mathcal{C}_2 \subset E(K)$, it must then be $K = \mathbb{Q}(\sqrt{\Delta_E})$, with $\Delta_E = A^2 - 4B$, which we will call D from now on. The full set of points with order two is

$$(0,0), \qquad \left(-\frac{1}{2}(A - \sqrt{D}), 0\right), \qquad \left(-\frac{1}{2}(A + \sqrt{D}), 0\right).$$

Let us assume there is a point of order 4. Then one of the previous points is the double of such a point, hence (see [13] Thm. 4.2.) one of the following pairs consists of two squares in K:

$$\left\{\frac{1}{2}(A - \sqrt{D}),\ \frac{1}{2}(A + \sqrt{D})\right\}, \quad \left\{\frac{1}{2}(-A + \sqrt{D}),\ \sqrt{D}\right\}, \quad \left\{-\sqrt{D},\ -\frac{1}{2}(A + \sqrt{D})\right\}.$$

Only the first possibility can hold. Now an element $a + b\sqrt{D} \in (K^*)^2$ if and only if there exist $x, y \in \mathbb{Q}$ such that

$$a = x^2 + Dy^2, \qquad b = 2xy;$$

so we must have

$$\begin{cases} A/2 &= x^2 + Dy^2 \\ 1 &= 4xy \end{cases} \qquad \begin{cases} A/2 &= t^2 + Dz^2 \\ -1 &= 4tz \end{cases}$$

Clearly both systems have a solution if and only if one of them has. The first gives rise to

$$y = \frac{1}{4x}, \qquad x^2 = \frac{A}{4} \pm \frac{\sqrt{B}}{2},$$

so we must assume $B = C^2$ and then $x^2 = A/4 \pm C/2$. Therefore, our curve must have the form (renaming x and C as $\alpha/2$ and β, purely for aesthetic purposes):

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

but for every E in this familiy of curves we have $\mathcal{C}_4 \subset E(\mathbb{Q})$, as the point $(-\beta, \alpha\beta)$ has order 4. Note that the non–vanishing of Δ_E is equivalent here to $\alpha^2(\alpha+4\beta) \neq 0$.

(iv) Assume we have $K = \mathbb{Q}(\sqrt{D})$ and E, with $E(\mathbb{Q})_{\text{tors}} \simeq \mathcal{C}_4$, $E(K) \simeq \mathcal{C}_{16}$. Then, from Ψ,

$$0 \to \ker(\Psi) \xrightarrow{i} E(K) \xrightarrow{\Psi} E(\mathbb{Q}) \times E_D(\mathbb{Q}) \xrightarrow{\pi} \operatorname{coker}(\Psi) \to 0,$$

and considering the torsion part, we have $\ker(\Psi)$ is either trivial or $\mathcal{C}_2$ and $E_D(\mathbb{Q})_{\text{tors}} \simeq \mathcal{C}_{2n}$, with $n = 1, \ldots, 6$. So the only possibility is $\ker(\Psi) \simeq \mathcal{C}_2$, $E_D(\mathbb{Q})_{\text{tors}} \simeq \mathcal{C}_8$. But then $\operatorname{coker}(\Psi) \simeq \mathcal{C}_4$, which contradicts Theorem 3.

(v) Direct from Corollary 4, with $n = 9$.

(vi) If $H = \mathcal{C}_{15}$, then Najman [20, Theorem 2, c)] has shown that E is the elliptic curve `50b1` or `50a3` with $K = \mathbb{Q}(\sqrt{5})$; and `50b2` or `450b4` with $K = \mathbb{Q}(\sqrt{-15})$.

Both `50b1` and `50b2` have $G = \mathcal{C}_5$, while `50a3` and `450b4` have $G = \mathcal{C}_3$. Therefore, $H = \mathcal{C}_{15}$ will only appear in $\Phi_{\mathbb{Q}}(2, G)$ for $G = \mathcal{C}_3, \mathcal{C}_5$. □

Proof. (Theorem 2) The sets $\Phi_{\mathbb{Q}}(2, G)$ were first conjectured by the computations mentioned above. The relevant results can be found in Table 2. In particular, this shows that all groups said to be in $\Phi_{\mathbb{Q}}(2, G)$ belong to this set.

Table 1. The cases not treated in [14]. The table displays either if the case happens (✓), if it is impossible because $G \not\subset H$ ($-$) or if it is ruled out by Theorem 5 ((i)–(vi)).

	$\mathcal{C}_1$	$\mathcal{C}_2$	$\mathcal{C}_3$	$\mathcal{C}_4$	$\mathcal{C}_5$	$\mathcal{C}_6$	$\mathcal{C}_7$	$\mathcal{C}_8$	$\mathcal{C}_9$	$\mathcal{C}_{10}$	$\mathcal{C}_{12}$
$\mathcal{C}_1$	✓	−	−	−	−	−	−	−	−	−	−
$\mathcal{C}_2$	(ii)	✓	−	−	−	−	−	−	−	−	−
$\mathcal{C}_3$	✓	−	✓	−	−	−	−	−	−	−	−
$\mathcal{C}_4$	(ii)	✓	−	✓	−	−	−	−	−	−	−
$\mathcal{C}_5$	✓	−	−	−	✓	−	−	−	−	−	−
$\mathcal{C}_6$	(ii)	✓	(ii)	−	−	✓	−	−	−	−	−
$\mathcal{C}_7$	✓	−	−	−	−	−	✓	−	−	−	−
$\mathcal{C}_8$	(ii)	✓	−	✓	−	−	−	✓	−	−	−
$\mathcal{C}_9$	✓	−	(v)	−	−	−	−	−	✓	−	−
$\mathcal{C}_{10}$	(ii)	✓	−	−	(ii)	−	−	−	−	✓	−
$\mathcal{C}_{12}$	(ii)	✓	(ii)	✓	−	✓	−	−	−	−	✓
$\mathcal{C}_{15}$	(vi)	−	✓	−	✓	−	−	−	−	−	−
$\mathcal{C}_{16}$	(ii)	✓	−	(iv)	−	−	−	✓	−	−	−
$\mathcal{C}_2 \times \mathcal{C}_2$	(ii)	✓	−	−	−	−	−	−	−	−	−
$\mathcal{C}_2 \times \mathcal{C}_4$	(ii)	(iii)	✓	−	−	−	−	−	−	−	−
$\mathcal{C}_2 \times \mathcal{C}_6$	(ii)	✓	(ii)	−	−	✓	−	−	−	−	−
$\mathcal{C}_2 \times \mathcal{C}_8$	(ii)	(iii)	−	✓	−	−	−	✓	−	−	−
$\mathcal{C}_2 \times \mathcal{C}_{10}$	(ii)	✓	−	−	(ii)	−	−	−	−	✓	−
$\mathcal{C}_2 \times \mathcal{C}_{12}$	(ii)	(iii)	(ii)	✓	−	(iii)	−	−	−	−	✓
$\mathcal{C}_3 \times \mathcal{C}_3$	(i)	−	✓	−	−	−	−	−	−	−	−
$\mathcal{C}_3 \times \mathcal{C}_6$	(i), (ii)	(i)	(ii)	−	−	✓	−	−	−	−	−
$\mathcal{C}_4 \times \mathcal{C}_4$	(ii)	(iii)	−	✓	−	−	−	−	−	−	−

The groups H from $\Phi_{\mathbb{Q}}(2)$ that do not appear in some $\Phi_{\mathbb{Q}}(2, G)$, with $G < H$ can be ruled out from $\Phi_{\mathbb{Q}}(2, G)$ most of the times using the previous theorem.

Table 1 (row $=$ H, column $=$ G) deals with the case $G \neq \mathcal{C}_2 \times \mathcal{C}_{2m}$. The non–cyclic case being treated in (1) (cf. [14]).

□

3. Real vs. imaginary quadratic extensions

A natural question might be if there is any substantial difference between the real and imaginary quadratic case. Our computations (see Section 5) show it is not so, except for some well–known cases.

In fact, from the Weil pairing [24] we know that, for a number field K, if $\mathcal{C}_m \times \mathcal{C}_m \subset E(K)$, then K contains the cyclotomic field generated by the m–th roots of unity. In the quadratic case, that implies:

- $\mathcal{C}_3 \times \mathcal{C}_3$ and $\mathcal{C}_3 \times \mathcal{C}_6$ can only appear in the imaginary extension $\mathbb{Q}\left(\sqrt{-3}\right)$.
- $\mathcal{C}_4 \times \mathcal{C}_4$ can only appears in the imaginary extension $\mathbb{Q}\left(\sqrt{-1}\right)$.

For all the remaining cases, groups in $\Phi_{\mathbb{Q}}(2)$ appear in both real and imaginary cases. This is shown in Table 2. Consider all elliptic curves, defined over the rationals with:

- $E(\mathbb{Q})_{tors}$ as given in the first column
- $E(\mathbb{Q}(\sqrt{D}))_{tors}$ as given in the second column, for some D as given in the fourth (resp. sixth) column for the real case (resp. imaginary case).

Then

- The seventh (penultimate) column is the number of curves with conductor less than 300000 which meet this situation, for a real extension $\mathbb{Q} \subset K$.
- The eighth (last) column is is the number of curves with conductor less than 300000 which meet this situation, for an imaginary extension $\mathbb{Q} \subset K$.

Notice that the only cases where "$-$" appears are the ones remarked above.

4. On the number of quadratic extensions with proper extension of the torsion subgroup

Consider the following problem, closely related to our original one. Take an elliptic curve, defined over the rationals, and allow the base field to be extended to a quadratic number field. How many cases of proper extension in the corresponding torsion groups can we predict to appear?

To begin with, for a fixed curve E, then only a small amount of quadratic extensions will be interesting from the point of view of the torsion subgroup. This is a known result; see for instance, [14, Corollary 2] for a different approach or [9, Lemma 3.4] for a similar proof than the one presented here, which we include because it suits our forthcoming arguments.

Theorem 6. *Let E be an elliptic curve defined over the rationals. Then, for all but finitely many quadratic extensions $K/\mathbb{Q}$, $E(K)_{\text{tors}} = E(\mathbb{Q})_{\text{tors}}$.*

Proof. The proof is actually the method used in our computations above.

The order of a torsion point defined over a quadratic extension must be $m \in \mathcal{T} = \{1, \dots, 10, 12, 15, 16\}$. Therefore, for a given curve E defined over $\mathbb{Q}$, one only has to compute the m–th division polynomials $\psi_m(X)$ (m odd) or $\psi_m(X)/(2Y)$ (m even) [24], for all $m \in \mathcal{T}$, and look for irreducible quadratic and linear factors in $\mathbb{Q}[X]$.

For quadratic factors, we must consider their splitting fields. For linear factors $X - \alpha$, we must take the extension (maybe trivial) $\mathbb{Q}\left(\sqrt{\alpha^3 + A\alpha + B}\right)$, where $E : y^2 = x^3 + Ax + B$. These extensions, which are obviously finitely many, are the only quadratic ones where the torsion subgroup may grow. □

One might in fact give an upper bound for the number of quadratic extensions where $E(K)_{\text{tors}} \neq E(\mathbb{Q})_{\text{tors}}$, simply considering the number of linear factors that may appear in $\psi_m(X)$ or $\psi_m(X)/(2Y)$, with $m \in \mathcal{T}$ being a prime power.

If we want to be more precise we can use Theorem 2 to reduce the number of the division polynomials that must be taken into account. For instance, if $E(\mathbb{Q})_{\text{tors}} = \mathcal{C}_3$, we know that $E(K)_{\text{tors}} \in \{\mathcal{C}_3, \mathcal{C}_5, \mathcal{C}_{15}, \mathcal{C}_3 \times \mathcal{C}_3\}$, hence both torsion subgroups are different if and only if $E(K)$ has either a point of order 5 or a non–rational point of order 3. As $\deg(\psi_3) = 4$ and $\deg(\psi_5) = 12$ there are, at most, 16 quadratic extensions where the torsion grows.

Corollary 7. *For any elliptic curve E defined over the rational field, $G = E(\mathbb{Q})_{\mathrm{tors}}$. The number of quadratic extensions K verifying $E(K)_{\mathrm{tors}} \neq G$ is bounded by a constant k_G that only depends on G, and is given by:*

G	k_G	G	k_G	G	k_G	G	k_G	G	k_G
$\mathcal{C}_1$	80	$\mathcal{C}_4$	43	$\mathcal{C}_7$	0	$\mathcal{C}_{10}$	1	$\mathcal{C}_2 \times \mathcal{C}_4$	38
$\mathcal{C}_2$	182	$\mathcal{C}_5$	4	$\mathcal{C}_8$	128	$\mathcal{C}_{12}$	1	$\mathcal{C}_2 \times \mathcal{C}_6$	7
$\mathcal{C}_3$	16	$\mathcal{C}_6$	12	$\mathcal{C}_9$	0	$\mathcal{C}_2 \times \mathcal{C}_2$	42	$\mathcal{C}_2 \times \mathcal{C}_8$	0

The result is by no means accurate. In fact, it is not very complicated to sharpen the bound for odd-order groups, the even-order ones being much less understood (in practical terms). Our experimental data suggests that, in fact, the bound might well be 4 quadratic extensions for all cases.

Example.– The elliptic curve `30a7` has minimal Weierstrass equation:

$$E : Y^2 + XY + Y = X^3 - 5334X - 150368$$

and $E(\mathbb{Q})_{tors} = \mathcal{C}_2$. Even more:

D	-5	-3	-2	-10
$E(\mathbb{Q}(\sqrt{D}))_{tors}$	$\mathcal{C}_4$	$\mathcal{C}_6$	$\mathcal{C}_4$	$\mathcal{C}_2 \times \mathcal{C}_2$

Theorem 6 allows us to give a different proof of the following result mentioned by Gouvêa and Mazur [8].

Theorem 8. *Given an elliptic curve E, defined over $\mathbb{Q}$, there is a finite amount of quadratic twists $E_D(\mathbb{Q})$ such that $E_D(\mathbb{Q})$ has points of order greater than 2.*

The number of such quadratic twists is bounded in terms of $G = E(\mathbb{Q})_{tors}$ as in the previous result.

Proof. Let us consider $K = \mathbb{Q}(\sqrt{D})$ and the morphism $\omega : E(K) \longrightarrow E_D(\mathbb{Q})$, given by the composition

$$E(K) \xrightarrow{\Psi} E(\mathbb{Q}) \times E_D(\mathbb{Q}) \xrightarrow{\pi_2} E_D(\mathbb{Q}),$$

where Ψ is the mapping given in Theorem 3. That is,

$$\omega(P) = \phi(P - \sigma P, 1/\sqrt{D}).$$

It is clear that $\ker(\omega) = E(\mathbb{Q})$ and, as in Theorem 3, if we consider the long exact sequence

$$0 \to E(\mathbb{Q}) \longrightarrow E(K) \xrightarrow{\omega} E_D(\mathbb{Q}) \longrightarrow \mathrm{coker}(\omega) \to 0,$$

One can see that, for all $P \in E_D(\mathbb{Q})$, $[2]P = \omega(\phi(P, \sqrt{D}))$. That is, any non–zero element of $\mathrm{coker}(\omega)$ has order 2. Now, looking at the finite part, Theorem 6 shows that for almost all D, we have $E(\mathbb{Q})_{\mathrm{tors}} = E(K)_{\mathrm{tors}}$, so $\mathrm{Img}(\omega)$ is trivial, and $E_D(\mathbb{Q})_{\mathrm{tors}} \simeq \mathrm{coker}(\omega)$, which has only elements of order at most 2. □

However, some questions arise in this context which we have not yet an answer to.

Problem 1.– Let us fix $G \in \Phi(1)$. Consider the set of all elliptic curves E, defined over $\mathbb{Q}$, with $G = E(\mathbb{Q})_{tors}$ and, when E varies in this set, give a sharp bound for the maximal number of quadratic extensions $K/\mathbb{Q}$ with $G \neq E(K)_{\mathrm{tors}}$.

Problem 2.– Is there a precise (and easy) description of which are the possible extensions $K/\mathbb{Q}$ with $E(\mathbb{Q})_{\text{tors}} \neq E(K)_{\text{tors}}$, ideally in terms of some invariant(s) of the curve?

Problem 3.– For a given $G \in \Phi(1)$, one can see experimentally that not all subsets of $\Phi_{\mathbb{Q}}(2, G)$ appear when one considers an arbitrary curve E with $G = E(\mathbb{Q})_{\text{tors}}$ and all quadratic extensions $K/\mathbb{Q}$. Find a precise description of all the combinations that may occur.

In connection to the last problem, one can prove that there are curves with stable torsion:

Proposition 9. *Let $G \in \Phi(1)$, with $G \neq \mathcal{C}_{2n}$. Then there exists an elliptic curve E such that, for all quadratic extensions $K/\mathbb{Q}$,*

$$G = E(\mathbb{Q})_{\text{tors}} = E(K)_{\text{tors}}.$$

Proof. Clearly the groups $G = \mathcal{C}_{2n}$ do not satisfy this property, as there is a quadratic extension where full 2–torsion is achieved.

The fact that, for all other groups, there are curves with stable torsion for all quadratic extensions can be checked in Table 2. □

Finally, some comments about the other possible strategy mentioned at the beginning of the section. If we fix the field, then a thorough study of possible groups is possible [11] studying the non–cuspidal points of certain modular curves.

This technique was in fact the main tool in the search (and hunt) for the most unusual group appearing in $\Phi_{\mathbb{Q}}(2)$, which is $\mathcal{C}_{15}$. As we mentioned before, it only appears in 4 very specific cases [20].

5. Computations

Table 2 is the result of our computations with the curves in the Antwerp–Cremona tables, with conductor less than 300000 (a total of 1887909 elliptic curves) must be read as follows:

1. The first column is $G \in \Phi(1)$.
2. The second column is $H \in \Phi_2(\mathbb{Q}, G)$.
3. Columns 3rd to 6th display specific examples:
   - The third column is the elliptic curve E with minimal conductor such that $E(\mathbb{Q})_{\text{tors}} \simeq G$, $E(K)_{\text{tors}} \simeq H$, with $K = \mathbb{Q}(\sqrt{D})$, $D > 0$ being the integer in the fourth column.
   - Columns 5th and 6th are analogous, with $D < 0$.
   - When these four colums are merged, $H = G$ and the curve in the cell verifies $E(\mathbb{Q})_{\text{tors}} = E(K)_{\text{tors}}$ for all quadratic extensions $K/\mathbb{Q}$.
4. Columns 7th and 8th indicate the total amount of curves found verifying the corresponding situation (7th for real extensions, 8th for complex, merged for stable torsion groups).

Acknowledgement: The authors would like to thank J. Silverman and N. Elkies for their suggestions and ideas.

References

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

[2] Chahal, J.S.: *A note on the rank of quadratic twists of an elliptic curve.* Math. Nach. **161** (1993) 55–58.

[3] Cremona, J. E.: *Elliptic curve data for conductors up to 300.000.* Available on ... `http://www.warwick.ac.uk/~masgaj/ftp/data/`, 2013.

[4] Derickx, M., Kamienny, S., Stein, W., Stoll, M.: *Torsion points on elliptic curves over number fields of small degree.* In preparation.

[5] Edixhoven, B.: *Rational torsion points on elliptic curves over number fields (after Kamienny and Mazur).* Séminaire Bourbaki 1993/94. Astérisque **227** (1995) 209–227.

[6] Fujita, Y.: *Torsion subgroups of elliptic curves in elementary* 2*–extensions of* $\mathbb{Q}$. J. Number Theory **144** (2005) 124–134.

[7] García–Selfa, I.; González–Jiménez, E.; Tornero, J.M.: *Galois theory, discriminants and torsion subgroup of elliptic curves.* J. Pure Appl. Algebra **214** (2010) 1340–1346.

[8] Gouvêa, F.; Mazur, B.: *The square-free sieve and the rank of elliptic curves.* J. Amer. Math. Soc. **4** (1991) 1–23.

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

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

[11] Kamienny, S.; Najman, F.: *Torsion groups of elliptic curves over quadratic fields.* Acta Arith. **152** (2012) 291–305.

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

[13] Knapp, A.W.: *Elliptic curves.* Princeton University Press (1992).

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

[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. **335** (1985) 163–172.

[16] Lozano–Robledo, A.: *On the field of definition of p-torsion points on elliptic curves over the rationals.* Math. Ann. **357** (2013) 279–305.

[17] Mazur, B.: *Modular curves and the Eisenstein ideal.* Publ. Math. Inst. Hautes Études. Sci. **47** (1977) 33–186.

[18] Mazur, B.: *Rational isogenies of prime degree.* Invent. Math. **44** (1978) 129–162.

[19] Merel, L.: *Bornes pour la torsion des courbes elliptiques sur les corps de nombres.* Invent. Math. **124** (1996), 437–449.

[20] Najman, F.: *Torsion of rational elliptic curves over cubic fields and sporadic points on* $X_1(n)$. arXiv: 1211.2188.

[21] Palladino, L.: *Elliptic curves with* $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$ *and counterexamples to local–global divisibility by* 9. J. Théor. Nombres Bordeaux **22** (2010) 139–160.

[22] Parent, P.: *No 17-torsion on elliptic curves over cubic number fields*, J. Théor. Nombres Bordeaux **15** (2003), 831–838.

[23] Parent, P.: *Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres*, J. Reine Angew. Math. **506** (1999), 85–116.

[24] Silverman, J.H.: *The arithmetic of elliptic curves.* Springer (1986).

Universidad Autónoma de Madrid, Departamento de Matemáticas and Instituto de Ciencias Matemáticas (ICMat), Madrid, Spain

E-mail address: `enrique.gonzalez.jimenez@uam.es`

URL: `http://www.uam.es/enrique.gonzalez.jimenez`

Departamento de Álgebra, Universidad de Sevilla. P.O. 1160. 41080 Sevilla, Spain.

E-mail address: `tornero@us.es`

TABLE 2. (See Section 5 for a precise explanation)

$\mathcal{C}_1$	$\mathcal{C}_1$	11a2				898000	
	$\mathcal{C}_3$	50b3	5	19a2	-3	38916	72257
	$\mathcal{C}_5$	50a4	5	99d1	-3	1581	2261
	$\mathcal{C}_7$	338f1	13	208d1	-1	229	295
	$\mathcal{C}_9$	432e3	3	54a2	-3	87	105
$\mathcal{C}_2$	$\mathcal{C}_4$	15a6	5	15a5	-1	105300	119253
	$\mathcal{C}_6$	80b3	3	14a3	-3	10594	15658
	$\mathcal{C}_8$	72a5	3	24a6	-1	1026	1014
	$\mathcal{C}_{10}$	150b3	5	198e1	-3	202	234
	$\mathcal{C}_{12}$	240b3	3	30a3	-3	99	119
	$\mathcal{C}_{16}$	22050eo1	105	3150bk1	-15	3	1
	$\mathcal{C}_2 \times \mathcal{C}_2$	14a5	2	14a3	-7	488583	256109
	$\mathcal{C}_2 \times \mathcal{C}_6$	100a1	5	36a3	-3	322	257
	$\mathcal{C}_2 \times \mathcal{C}_{10}$	2178m1	33	450a3	-15	6	4
$\mathcal{C}_3$	$\mathcal{C}_3$	19a3				33340	
	$\mathcal{C}_{15}$	50a3	5	450b4	-15	1	1
	$\mathcal{C}_3 \times \mathcal{C}_3$	–	–	19a1	-3	–	1710
$\mathcal{C}_4$	$\mathcal{C}_8$	15a7	3	15a8	-3	2403	1244
	$\mathcal{C}_{12}$	150c1	5	90c1	-3	56	72
	$\mathcal{C}_2 \times \mathcal{C}_4$	15a7	15	15a8	-15	13990	9271
	$\mathcal{C}_2 \times \mathcal{C}_8$	1344m5	2	192c6	-2	11	18
	$\mathcal{C}_2 \times \mathcal{C}_{12}$	112710cj1	17	150c3	-15	3	2
	$\mathcal{C}_4 \times \mathcal{C}_4$	–	–	40a4	-1	–	56
$\mathcal{C}_5$	$\mathcal{C}_5$	11a1				1127	
	$\mathcal{C}_{15}$	50b1	5	50b2	-15	1	1
$\mathcal{C}_6$	$\mathcal{C}_{12}$	30a1	5	30a1	-3	157	167
	$\mathcal{C}_2 \times \mathcal{C}_6$	14a2	2	14a1	-7	3431	1652
	$\mathcal{C}_3 \times \mathcal{C}_6$	–	–	14a1	-3	-	64
$\mathcal{C}_7$	$\mathcal{C}_7$	26b1				66	
$\mathcal{C}_8$	$\mathcal{C}_{16}$	210e1	105	210e1	-15	12	6
	$\mathcal{C}_2 \times \mathcal{C}_8$	21a3	7	15a4	-1	85	64
$\mathcal{C}_9$	$\mathcal{C}_9$	54b3				17	
$\mathcal{C}_{10}$	$\mathcal{C}_2 \times \mathcal{C}_{10}$	66c1	33	66c2	-2	25	11
$\mathcal{C}_{12}$	$\mathcal{C}_2 \times \mathcal{C}_{12}$	2730bd1	65	90c3,	-15	10	5
$\mathcal{C}_2 \times \mathcal{C}_2$	$\mathcal{C}_2 \times \mathcal{C}_2$	120b2				36913	
	$\mathcal{C}_2 \times \mathcal{C}_4$	15a2	5	15a2	-1	17911	12914
	$\mathcal{C}_2 \times \mathcal{C}_6$	150c2	5	30a6	-3	370	459
	$\mathcal{C}_2 \times \mathcal{C}_8$	72a4	3	63a2	-3	61	47
	$\mathcal{C}_2 \times \mathcal{C}_{12}$	960o6	6	167310w2	-39	4	1
$\mathcal{C}_2 \times \mathcal{C}_4$	$\mathcal{C}_2 \times \mathcal{C}_4$	24a1				1054	
	$\mathcal{C}_2 \times \mathcal{C}_8$	15a1	5	21a1	-3	146	61
	$\mathcal{C}_4 \times \mathcal{C}_4$	–	–	15a1	-1	–	64
$\mathcal{C}_2 \times \mathcal{C}_6$	$\mathcal{C}_2 \times \mathcal{C}_6$	30a2				71	
	$\mathcal{C}_2 \times \mathcal{C}_{12}$	90c6	6	2730bd2	-14	8	7
$\mathcal{C}_2 \times \mathcal{C}_8$	$\mathcal{C}_2 \times \mathcal{C}_8$	210e2				6	