ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 46, Number 6, 2016

TORSION OF RATIONAL ELLIPTIC CURVES OVER CUBIC FIELDS

ENRIQUE GONZÁLEZ-JIMÉNEZ, FILIP NAJMAN AND JOSÉ M. TORNERO

ABSTRACT. Let E be an elliptic curve defined over $\mathbb{Q}$. We study the relationship between the torsion subgroup $E(\mathbb{Q})_{\rm tors}$ and the torsion subgroup $E(K)_{\rm tors}$, where K is a cubic number field. In particular, we study the number of cubic number fields K such that $E(\mathbb{Q})_{\rm tors} \neq E(K)_{\rm tors}$.

1. Introduction. Let K be a number field. The Mordell-Weil theorem states that the set of K-rational points of an elliptic curve E defined over K is a finitely generated abelian group, that is, $E(K) \simeq E(K)_{\rm tors} \oplus \mathbb{Z}^r$, where $E(K)_{\rm tors}$ is the torsion subgroup and r is the rank. Moreover, it is well known that $E(K)_{\rm tors} \simeq \mathcal{C}_m \times \mathcal{C}_n$ for two positive integers n and m, where m divides n and where $\mathcal{C}_n$ is a cyclic group of order n hereafter.

Let d be a positive integer. The set $\Phi(d)$ of possible torsion structures of elliptic curves defined over number fields of degree d has been studied in depth by several authors. The case $d = 1$ was obtained by Mazur **[15, 16]**:

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

The case $d = 2$ was completed by Kamienny **[9]** and Kenku and Momose **[13]**. There are no other cases where $\Phi(d)$ has been completely determined.

The second author **[18]** has extended this study to the set $\Phi_{\mathbb{Q}}(d)$ of possible torsion structures over a number field of degree d of an elliptic

---

2010 AMS *Mathematics subject classification.* Primary 11G05, Secondary 11R16, 14G05, 14H52.

Keywords and phrases. Elliptic curves, torsion subgroup, rationals, cubic fields.

The first author was supported by grant MTM2015-68524-P. The third author was supported by grants FQM-218, MTM2013-46231-P and P12-FQM-2696 (FSE and FEDER (EU)).

Received by the editors on December 9, 2014, and in revised form on February 3, 2015.

DOI:10.1216/RMJ-2016-46-6-1899

curve defined over $\mathbb{Q}$. He has obtained a complete description of $\Phi_{\mathbb{Q}}(2)$ and $\Phi_{\mathbb{Q}}(3)$. For convenience, we will state here only the latter set:

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

Fix a possible torsion structure over $\mathbb{Q}$, say $G \in \Phi(1)$. Recently, in **[5]**, the set $\Phi_{\mathbb{Q}}(2, G)$ of possible torsion structures over a quadratic number field of an elliptic curve defined over $\mathbb{Q}$ such that $E(\mathbb{Q})_{\text{tors}} \simeq G \in \Phi(1)$ was determined. The first goal of this paper is giving a complete description (see Theorem 1.2) of $\Phi_{\mathbb{Q}}(3, G)$, as was done in **[5,** Theorem 2] for the case $d = 2$.

Moreover, in **[6]**, the first and third authors obtained, for $d = 2$ and for all $G \in \Phi(1)$, the set

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

where, for any $i = 1, \dots, n$, $S_i = [H_1, \dots, H_m]$ is a list, with $H_i \in \Phi_{\mathbb{Q}}(d, G) \setminus \{G\}$, and there exists an elliptic curve E_i defined over $\mathbb{Q}$ such that:

- $E_i(\mathbb{Q})_{\text{tors}} = G$.
- There are number fields $K_1, \dots, K_m$ (non-isomorphic pairwise) of degree d with $E_i(K_j)_{\text{tors}} = H_j$, for all $j = 1, \dots, m$.

Note that we are allowing the possibility of two (or more) of the H_j to be isomorphic. From these results, we obtain the following corollary **[6, 19]**.

Corollary 1.1. *If E is an elliptic curve defined over $\mathbb{Q}$, then there are at most four quadratic fields K_i, $i = 1, \dots, 4$ (non-isomorphic pairwise), such that $E(K_i)_{\text{tors}} \neq E(\mathbb{Q})_{\text{tors}}$, that is,*

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

Here, we obtain the equivalent description for the case $d = 3$, that is, we give a complete description of $\mathcal{H}_{\mathbb{Q}}(3, G)$ for a given $G \in \Phi(1)$ (see Theorem 1.4). Precisely, the main results of this paper are as follows.

Theorem 1.2. *For $G \in \Phi(1)$, the set $\Phi_{\mathbb{Q}}(3, G)$ is the following*:

G	$\Phi_{\mathbb{Q}}(3, G)$
$\mathcal{C}_1$	$\{\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3, \mathcal{C}_4, \mathcal{C}_6, \mathcal{C}_7, \mathcal{C}_{13}, \mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_2 \times \mathcal{C}_{14}\}$
$\mathcal{C}_2$	$\{\mathcal{C}_2, \mathcal{C}_6, \mathcal{C}_{14}\}$
$\mathcal{C}_3$	$\{\mathcal{C}_3, \mathcal{C}_6, \mathcal{C}_9, \mathcal{C}_{12}, \mathcal{C}_{21}, \mathcal{C}_2 \times \mathcal{C}_6\}$
$\mathcal{C}_4$	$\{\mathcal{C}_4, \mathcal{C}_{12}\}$
$\mathcal{C}_5$	$\{\mathcal{C}_5, \mathcal{C}_{10}\}$
$\mathcal{C}_6$	$\{\mathcal{C}_6, \mathcal{C}_{18}\}$
$\mathcal{C}_7$	$\{\mathcal{C}_7, \mathcal{C}_{14}\}$
$\mathcal{C}_8$	$\{\mathcal{C}_8\}$
$\mathcal{C}_9$	$\{\mathcal{C}_9, \mathcal{C}_{18}\}$
$\mathcal{C}_{10}$	$\{\mathcal{C}_{10}\}$
$\mathcal{C}_{12}$	$\{\mathcal{C}_{12}\}$
$\mathcal{C}_2 \times \mathcal{C}_2$	$\{\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_2 \times \mathcal{C}_6\}$
$\mathcal{C}_2 \times \mathcal{C}_4$	$\{\mathcal{C}_2 \times \mathcal{C}_4\}$
$\mathcal{C}_2 \times \mathcal{C}_6$	$\{\mathcal{C}_2 \times \mathcal{C}_6\}$
$\mathcal{C}_2 \times \mathcal{C}_8$	$\{\mathcal{C}_2 \times \mathcal{C}_8\}$

Remark 1.3. The elements of the sets $\Phi_{\mathbb{Q}}(3, G)$ were actually found using the computations that can be found in the appendix. These computations also prove that all the listed groups actually are in $\Phi_{\mathbb{Q}}(3, G)$. The main part of our work has therefore been to prove that there were indeed no more groups in these sets.

Theorem 1.4. *Let E be an elliptic curve defined over $\mathbb{Q}$. Then*:

(i) *There is at most one cubic number field K, up to isomorphism, such that*

$$E(K)_{\text{tors}} \simeq H \neq E(\mathbb{Q})_{\text{tors}},$$

for a fixed $H \in \Phi_{\mathbb{Q}}(3)$.

(ii) *There are at most three cubic number fields K_i, $i = 1, 2, 3$ (non-isomorphic pairwise), such that*

$$E(K_i)_{\text{tors}} \neq E(\mathbb{Q})_{\text{tors}}.$$

Moreover, the elliptic curve `162b2` *is the unique rational elliptic curve where the torsion grows over three non-isomorphic cubic fields.*

(iii) *Let* $G \in \Phi(1)$ *be such that* $\Phi_{\mathbb{Q}}(3, G) \neq \{G\}$. *Then the set* $\mathcal{H}_{\mathbb{Q}}(3, G)$ *consists of the following elements* (*the third row is* $h = \#S$, *for each* $S \in \mathcal{H}_{\mathbb{Q}}(3, G)$):

G	$\mathcal{H}_{\mathbb{Q}}(3,G)$	h
$\mathcal{C}_1$	$\mathcal{C}_2$	1
	$\mathcal{C}_4$	
	$\mathcal{C}_6$	
	$\mathcal{C}_2 \times \mathcal{C}_2$	
	$\mathcal{C}_2 \times \mathcal{C}_{14}$	
	$\mathcal{C}_2, \mathcal{C}_3$	2
	$\mathcal{C}_2, \mathcal{C}_7$	
	$\mathcal{C}_2, \mathcal{C}_{13}$	
	$\mathcal{C}_3, \mathcal{C}_4$	
	$\mathcal{C}_3, \mathcal{C}_2 \times \mathcal{C}_2$	
	$\mathcal{C}_4, \mathcal{C}_7$	
	$\mathcal{C}_7, \mathcal{C}_2 \times \mathcal{C}_2$	
	$\mathcal{C}_2, \mathcal{C}_3, \mathcal{C}_7$	3

G	$\mathcal{H}_{\mathbb{Q}}(3,G)$	h
$\mathcal{C}_2$	$\mathcal{C}_6$	1
	$\mathcal{C}_{14}$	
$\mathcal{C}_3$	$\mathcal{C}_6$	1
	$\mathcal{C}_{12}$	
	$\mathcal{C}_2 \times \mathcal{C}_6$	
	$\mathcal{C}_6, \mathcal{C}_9$	2
	$\mathcal{C}_6, \mathcal{C}_{21}$	
$\mathcal{C}_4$	$\mathcal{C}_{12}$	1
$\mathcal{C}_5$	$\mathcal{C}_{10}$	1
$\mathcal{C}_6$	$\mathcal{C}_{18}$	1
$\mathcal{C}_7$	$\mathcal{C}_{14}$	1
$\mathcal{C}_9$	$\mathcal{C}_{18}$	1
$\mathcal{C}_2 \times \mathcal{C}_2$	$\mathcal{C}_2 \times \mathcal{C}_6$	1

The best previously known result [**8,** Lemma 3.3] stated that the torsion subgroup of a rational elliptic curve grows strictly in only finitely many cubic number fields.

Notation 1.5. Please note that, in the sequel, for examples and precise curves we will use the Antwerp-Cremona tables and labels [**1, 3**]. We will write $G = H$ (respectively, $G < H$ or $G \leq H$) for the fact that G is *isomorphic* to H (or to a subgroup of H) without further details on the precise isomorphism.

2. Auxiliary results.

We will fix once and for all some notation. We will use a short Weierstrass equation for an elliptic curve E,

$$E : Y^2 = X^3 + AX + B, \quad A, B \in \mathbb{Z},$$

with discriminant Δ.

For such 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 a number field K. Let us recall the following well-known result **[21,** Chapter III, subsection 8.1.1].

Proposition 2.1. *Let E be an elliptic curve over a number field K. If $\mathcal{C}_m \times \mathcal{C}_m \le E(K)$, then K contains the cyclotomic field $\mathbb{Q}(\zeta_m)$ generated by the mth roots of unity.*

Let us fix the set-up, following **[18]**. Let $K/\mathbb{Q}$ be a cubic extension, and let L be the normal closure of K over $\mathbb{Q}$. Finally, let M be the only subextension $\mathbb{Q} \subset M \subset L$ such that $[L : M] = 3$. Therefore, we have two possible situations:

- The extension $K/\mathbb{Q}$ is Galois. Then, $\mathbb{Q} = M$ and $K = L$.
- The extension $K/\mathbb{Q}$ is not Galois. Then, we have:

$$\begin{tikzcd}
 & L \arrow[dl, dash, "3"'] \arrow[dr, dash, "2"] & \\
M \arrow[dr, dash, "2"'] & & K \arrow[dl, dash, "3"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Remark 2.2. Let $\alpha \in \mathbb{Q}$. If there is some $\beta \in K$ with $\alpha = \beta^2$, then $\beta \in \mathbb{Q}$.

Now we will recall some results from **[18]** which will come in handy.

Proposition 2.3. *Let E be an elliptic curve defined over $\mathbb{Q}$, K, L and M as above, $G \in \Phi_{\mathbb{Q}}(1)$ and $H \in \Phi_{\mathbb{Q}}(3)$ such that $E(\mathbb{Q})_{\text{tors}} \simeq G$ and $E(K)_{\text{tors}} \simeq H$.*

(i) *If G has a non-trivial 2-Sylow subgroup, G and H have the same 2-Sylow subgroup* **[18,** Lemma 8].

(ii) *If $\mathcal{C}_4 \not\le G$, then $\mathcal{C}_8 \not\le H$ and, if $\mathcal{C}_4 \le H$, then $M = \mathbb{Q}(i)$ and $\Delta \in (-1) \cdot (\mathbb{Q}^*)^2$* **[4]**, **[18,** Corollary 12].

(iii) $E(K)[5] = E(\mathbb{Q})[5]$ [**18,** Lemma 21].
(iv) *If* $H = \mathcal{C}_{21}$, *then* E *is the elliptic curve* `162b1` *and* $K = \mathbb{Q}(\zeta_9)^+$ [**18,** Theorem 2].
(v) *If* $G = \mathcal{C}_7$, *then* $H \neq \mathcal{C}_2 \times \mathcal{C}_{14}$ [**18,** Proof of Proposition 29].
(vi) *If* $E(M)$ *has no points of order* 3, *neither does* $E(L)$ [**18,** Lemma 13].

Also, some results on isogenies will be needed:

Proposition 2.4. *Let* E *be an elliptic curve defined over* $\mathbb{Q}$, K *and* L *as above.*

(i) *Assume that* E *has a rational* n*-isogeny. Then either* $1 \leq n \leq 19$, *or* $n \in \{21, 25, 27, 37, 43, 67, 163\}$ [**10, 11, 12, 16**].
(ii) *Assume that* n *is odd and not divisible by* 3. *If* $E(K)$ *has a point of order* n, *then* E *has a rational isogeny of degree* n [**18,** Lemma 18].
(iii) *If* F *is a number field and* E *has two independent isogenies over* F *with degrees* n *and* m, E *is isogenous* (*over* F) *to an elliptic curve with an* mn*-isogeny* [**18,** Lemma 7].
(iv) *If* $K = L$, n *is an odd integer and* $E(K)$ *has a point of order* n, *then* E *has a rational* n*-isogeny* [**18,** Lemma 19].
(v) *Let* F *be a quadratic number field,* n *an odd integer and* $E/\mathbb{Q}$ *an elliptic curve such that* $\mathcal{C}_n \leq E(F)$. *Then* E *has a rational* n*-isogeny* [**18,** Lemma 5].
(vi) *Assume that* $E(K)$ *has a point of order* 9. *Then either* $E/\mathbb{Q}$ *has a* 9*-isogeny or it has two independent* 3*-isogenies* [**18,** Proposition 14].

Lemma 2.5. *Let* p *be a prime,* f *a* p*-isogeny on* $E/\mathbb{Q}$, *and let* $\ker(f)$ *be generated by* P. *Then the field of definition* $\mathbb{Q}(P)$ *of* P (*and all of its multiples*) *is a cyclic* (*Galois*) *extension of* $\mathbb{Q}$ *of order dividing* $p-1$.

Proof. First note that the fact that $F = \mathbb{Q}(P)$ is Galois over $\mathbb{Q}$ follows immediately from the Galois-invariance of $\langle P \rangle$. Let χ be the character of the isogeny,

$$\chi : \mathrm{Gal}\,(F/\mathbb{Q}) \longrightarrow \mathrm{Aut}\,(\langle P \rangle).$$

which, to each element of $\mathrm{Gal}\,(F/\mathbb{Q})$, adjoins its action on $\langle P\rangle$. It is easy to check that this is a homomorphism.

Suppose that χ is not an injection. Then there exists an element σ, not the identity, such that $\chi(\sigma) = \mathrm{id}$, so $\langle\sigma\rangle$ acts trivially on P. Denoting $F_0 = F^\sigma$ (the fixed field of $\langle\sigma\rangle$), every automorphism of $\mathrm{Gal}\,(F/F_0)$ fixes P, and hence P is F_0-rational, which is in contradiction with the minimality of F.

Since $\mathrm{Gal}\,(F/\mathbb{Q})$ is isomorphic to a subgroup of $\mathrm{Aut}\,\langle P\rangle$, which is isomorphic to $\mathcal{C}_{p-1}$, we are finished. $\square$

Lemma 2.6. *If $E(K)$ has a point of order 3 over a cubic field K, then E has a 3-isogeny over $\mathbb{Q}$.*

Proof. $E(L)$ has a point of order 3, so $E(M)$ has a point of order 3 from Proposition 2.3 (vi). And, by Proposition 2.4 (v), E has a 3-isogeny over $\mathbb{Q}$. $\square$

Lemma 2.7. *If $E(K)$ has a point of order 9, then $E(\mathbb{Q})$ has a point of order 3.*

Proof. By Proposition 2.4 (vi), $E/\mathbb{Q}$ has either an isogeny of degree 9 or two isogenies of degree 3.

First, suppose it has two isogenies of degree 3 and no 3-torsion. Then it follows that $\mathbb{Q}(E[3])$ is a biquadratic field and the intersection of $\mathbb{Q}(E[3])$ and K must be trivial (that is, $\mathbb{Q}$), which contradicts the fact that $E(K)$ has nontrivial 3-torsion. Hence, $E(\mathbb{Q})$ has a 3-torsion point.

Now suppose $E/\mathbb{Q}$ has a 9-isogeny f, such that $\ker(f) = \langle P\rangle$, and such that P is K-rational. Then the isogeny character

$$\chi : \mathrm{Gal}\,(K/\mathbb{Q}) \longrightarrow \mathrm{Aut}\,(\langle P\rangle)$$

sends the generator σ of $\mathrm{Gal}\,(K/\mathbb{Q})$ into an element of order 3 in $\mathrm{Aut}\,(\langle P\rangle)$, i.e., into **[4, 7]**. Both of these act trivially on $\langle 3P\rangle$, implying that $E(\mathbb{Q})$ has nontrivial 3-torsion. $\square$

Remark 2.8. Now we will consider the case where we have K_1 and K_2 as two different cubic number fields. Let us write, as usual, K_1K_2

for the compositum field of both extensions. Then one of the following two situations hold:

- $[K_1K_2 : \mathbb{Q}] = 9$.
- $[K_1K_2 : \mathbb{Q}] = 6$. In this case, K_1 and K_2 are isomorphic and K_1K_2 is the Galois closure of both fields over $\mathbb{Q}$.

3. Proof of Theorem 1.2. Note that, from Proposition 2.3 (i), if $G = \mathcal{C}_{2n}$, for some $n \neq 0$, then $\mathcal{C}_2 \times \mathcal{C}_2 \not\subset H$.

Also from Proposition 2.3 (i) and the description of $\Phi_{\mathbb{Q}}(3)$, we can solve the non-cyclic cases from Theorem 1.2 easily, as we know that

$$\Phi_{\mathbb{Q}}(3, \mathcal{C}_2 \times \mathcal{C}_{2n}) \leq \begin{cases} \{\mathcal{C}_2 \times \mathcal{C}_2, \, \mathcal{C}_2 \times \mathcal{C}_6, \, \mathcal{C}_2 \times \mathcal{C}_{14}\} & \text{if } n = 1, \\ \{\mathcal{C}_2 \times \mathcal{C}_{2n}\} & \text{if } n \neq 1. \end{cases}$$

The only case that will not happen and we cannot immediately discard is $G = \mathcal{C}_2 \times \mathcal{C}_2$, $H = \mathcal{C}_2 \times \mathcal{C}_{14}$. But this case cannot happen as, from Proposition 2.4 (ii), (iii), that would imply E has a 28-isogeny, contradicting Proposition 2.4 (i). This finishes the non-cyclic case.

Let us move therefore to the cyclic case. The groups H from $\Phi_{\mathbb{Q}}(3)$ that do not appear in some $\Phi_{\mathbb{Q}}(3, G)$, with a $G < H$ and G cyclic can be ruled out from $\Phi_{\mathbb{Q}}(3, G)$, most of the times using the previous results. In Table 1, we indicate:

- with (i)–(vi), which part of Proposition 2.3 is used,
- with (**2.7**), the case is ruled out from Lemma 2.7,
- with $-$, the case is ruled out because $G \not\subset H$,
- with $\checkmark$, the case is possible (and in fact, it occurs).

Table 1 (row $= H$, column $= G$) deals with case G being cyclic.

Table 1.

	$\mathcal{C}_1$	$\mathcal{C}_2$	$\mathcal{C}_3$	$\mathcal{C}_4$	$\mathcal{C}_5$	$\mathcal{C}_6$	$\mathcal{C}_7$	$\mathcal{C}_8$	$\mathcal{C}_9$	$\mathcal{C}_{10}$	$\mathcal{C}_{12}$
$\mathcal{C}_1$	$\checkmark$	–	–	–	–	–	–	–	–	–	–
$\mathcal{C}_2$	$\checkmark$	$\checkmark$	–	–	–	–	–	–	–	–	–
$\mathcal{C}_3$	$\checkmark$	–	$\checkmark$	–	–	–	–	–	–	–	–
$\mathcal{C}_4$	$\checkmark$	(i)	–	$\checkmark$	–	–	–	–	–	–	–
$\mathcal{C}_5$	(iii)	–	–	–	$\checkmark$	–	–	–	–	–	–
$\mathcal{C}_6$	$\checkmark$	$\checkmark$	$\checkmark$	–	–	$\checkmark$	–	–	–	–	–
$\mathcal{C}_7$	$\checkmark$	–	–	–	–	–	$\checkmark$	–	–	–	–
$\mathcal{C}_8$	(ii)	(i)	–	(i)	–	–	–	$\checkmark$	–	–	–
$\mathcal{C}_9$	(**2.7**)	–	$\checkmark$	–	–	–	–	–	$\checkmark$	–	–
$\mathcal{C}_{10}$	(iii)	(iii)	–	–	$\checkmark$	–	–	–	–	$\checkmark$	–
$\mathcal{C}_{12}$	(?)	(i)	$\checkmark$	$\checkmark$	–	(i)	–	–	–	–	$\checkmark$
$\mathcal{C}_{13}$	$\checkmark$	–	–	–	–	–	–	–	–	–	–
$\mathcal{C}_{14}$	(?)	$\checkmark$	–	–	–	–	$\checkmark$	–	–	–	–
$\mathcal{C}_{18}$	(**2.7**)	(**2.7**)	(?)	–	–	$\checkmark$	–	–	$\checkmark$	–	–
$\mathcal{C}_{21}$	(iv)	–	$\checkmark$	–	–	–	–	–	–	–	–
$\mathcal{C}_2 \times \mathcal{C}_2$	$\checkmark$	(i)	–	–	–	–	–	–	–	–	–
$\mathcal{C}_2 \times \mathcal{C}_4$	(?)	(i)	–	(i)	–	–	–	–	–	–	–
$\mathcal{C}_2 \times \mathcal{C}_6$	(?)	(i)	–	–	–	(i)	–	–	–	–	–
$\mathcal{C}_2 \times \mathcal{C}_8$	(ii)	(i)	–	(i)	–	–	–	(i)	–	–	–
$\mathcal{C}_2 \times \mathcal{C}_{14}$	$\checkmark$	(i)	–	–	–	–	(v)	–	–	–	–

Let us now discard the remaining cases.

The case $G = \mathcal{C}_1$**,** $H = \mathcal{C}_{12}$**.** In this case, from Proposition 2.3 (ii), (vi), we already know that $M = \mathbb{Q}(i)$ and $E(M)[3] \neq \{\mathcal{O}\}$. Again, as above, having points of order 3 in both M and K implies that these are independent points, and hence, $E[3](L) \simeq \mathcal{C}_3 \times \mathcal{C}_3$, from which it follows that $M = \mathbb{Q}(\zeta_3)$, which is a contradiction.

The case $G = \mathcal{C}_1$**,** $H = \mathcal{C}_{14}$**.** In this case, E must have a rational 7-isogeny, from Proposition 2.4 (ii). Then, from Lemma 2.5, we know that K is a cyclic cubic Galois extension; hence, $K = L$. Under these circumstances, $E(K)[2]$ cannot be $\mathcal{C}_2$, as K is either the splitting field of $X^3 + AX + B$ (in which case $E(K)[2] = \mathcal{C}_2 \times \mathcal{C}_2$) or is irreducible over K, in which case there are no points of order 2 in $E(K)$.

The case $G = \mathcal{C}_1$, $H = \mathcal{C}_2 \times \mathcal{C}_4$. Assume our curve is given in Weierstrass short form

$$Y^2 = X^3 + AX + B.$$

If G is cyclic and H is not, K must be the splitting field of X^3+AX+B. So, in this case, $\mathbb{Q} = M$, and $K = L$, but this contradicts Proposition 2.3 (ii).

The case $G = \mathcal{C}_1$, $H = \mathcal{C}_2 \times \mathcal{C}_6$. As in the previous case, $\mathbb{Q} = M$, and $K = L$. But there are points of order 3 in $E(L)$, so $E(M)[3] \neq \{\mathcal{O}\}$, but this contradicts $G = \mathcal{C}_1$, as $\mathbb{Q} = M$.

The case $G = \mathcal{C}_3$, $H = \mathcal{C}_{18}$. As we gain exactly one 2-torsion point in the passing from $\mathbb{Q}$ to K, we already know that K is not Galois and, in fact, L must be the splitting field of $X^3 + AX + B$. Then, from Lemma 2.5 and Proposition 2.4 (vi), we have that $E(\mathbb{Q})$ must have two isogenies of degree 3.

Now we look at how $\mathrm{Gal}\,(L/\mathbb{Q})$ acts on $E[9]$. The L-rational points have to be sent to L-rational points. So if P is an L-rational point of order 9, the generators of $\mathrm{Gal}\,(L/\mathbb{Q})$ cannot both send P to a multiple of P, because this would imply that $\langle P \rangle$ is $\mathrm{Gal}\,(L/\mathbb{Q})$-invariant (and hence, $\mathrm{Gal}\,(\overline{\mathbb{Q}}/\mathbb{Q})$-invariant), which would imply a 9-isogeny over $\mathbb{Q}$. So this means that $E[9](L)$ is strictly larger than C_9. The only possibility is that $E[9](L) = C_3 \times C_9$, and this implies $M = \mathbb{Q}(\sqrt{-3})$ because of Proposition 2.1.

As L is the splitting field of $X^3 + AX + B$, this really implies $E(L)_{\text{tors}} \leq C_6 \times C_{18}$. Moreover, as the quadratic subextension of L is $\mathbb{Q}(\sqrt{-3})$, L is a pure cubic field and our curve is a Mordell curve $Y^2 = X^3 + n$, for some $n \in \mathbb{Z}$. But the only elliptic curve with j-invariant 0 defined over $\mathbb{Q}$ which has full 3-torsion over $\mathbb{Q}(\sqrt{-3})$ is `27a1` (and also its -3 twist), and by simply computing that this curve has L-torsion $C_6 \times C_6$, we are finished.

4. Proof of Theorem 1.4.

Proof of (i). Let E be an elliptic curve defined over $\mathbb{Q}$ such that $E(\mathbb{Q})_{\text{tors}} \simeq G \in \Phi(1)$ and $H \in \Phi_{\mathbb{Q}}(3)$. Let us prove that there is at most one cubic number field K such that $E(K)_{\text{tors}} \simeq H \neq G$.

First, let $H = G \times \mathcal{C}_m$ be such that $\gcd(|G|, m) = 1$. Suppose that there exist two cubic fields K_1 and K_2 such that $E(K_i)_{\text{tors}} \simeq H$, $i = 1, 2$. Then $\mathcal{C}_m \times \mathcal{C}_m \leq E(L)_{\text{tors}}$, where L is the degree 9 number field obtained by composition of K_1 and K_2. Therefore, $\mathbb{Q}(\zeta_m) \subset L$, which implies that $\varphi(m)$ divides 9. This eliminates the following possibilities:

- $G = \mathcal{C}_1$ and $H \in \{\mathcal{C}_3, \mathcal{C}_4, \mathcal{C}_6, \mathcal{C}_7, \mathcal{C}_{13}\}$;
- $G = \mathcal{C}_2$ and $H \in \{\mathcal{C}_6, \mathcal{C}_{14}\}$;
- $G = \mathcal{C}_3$ and $H \in \{\mathcal{C}_{12}, \mathcal{C}_{21}\}$;
- $G = \mathcal{C}_4$ and $H = \mathcal{C}_{12}$;
- $G = \mathcal{C}_2 \times \mathcal{C}_2$ and $H = \mathcal{C}_2 \times \mathcal{C}_6$;

On the other hand, if the order of G is odd, then there is at most one H of even order with $G < H$. The cubic field is the one defined by the 2-division polynomial of the elliptic curve. This argument therefore crosses out the cases:

- $G = \mathcal{C}_1$ and $H \in \{\mathcal{C}_2, \mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_2 \times \mathcal{C}_{14}\}$;
- $G = \mathcal{C}_3$ and $H \in \{\mathcal{C}_6, \mathcal{C}_2 \times \mathcal{C}_6\}$;
- $G = \mathcal{C}_5$ and $H = \mathcal{C}_{10}$;
- $G = \mathcal{C}_7$ and $H = \mathcal{C}_{14}$;
- $G = \mathcal{C}_9$ and $H = \mathcal{C}_{18}$.

The remaining cases to be dealt with are $G = \mathcal{C}_3$ with $H = \mathcal{C}_9$ and $G = \mathcal{C}_6$ with $H = \mathcal{C}_{18}$. These are essentially the same since $\mathcal{C}_6 = \mathcal{C}_2 \times \mathcal{C}_3$ and $\mathcal{C}_{18} = \mathcal{C}_2 \times \mathcal{C}_9$. Assume we have $\langle P \rangle \simeq \mathcal{C}_9$, $\langle Q \rangle \simeq \mathcal{C}_9$, where P and Q are defined over two non-isomorphic cubic fields. Therefore, P is not a multiple of Q and Q is not a multiple of P and $\mathcal{C}_3 \times \mathcal{C}_3 \leq \langle P, Q \rangle$. This is impossible, since both P and Q would be defined over a field of degree 9, which cannot contain $\mathbb{Q}(\zeta_3)$.

This proves the first statement of Theorem 1.4.

Proofs of (ii) and (iii). First note that if

$$E : Y^2 = f(X)$$

is an elliptic curve defined over $\mathbb{Q}$ such that $E(\mathbb{Q})_{\text{tors}} \simeq G$ has odd order, then $f(X)$ is an irreducible cubic polynomial. Now, denote by K the cubic field defined by $f(X)$, then $H = E(K)_{\text{tors}}$ satisfies that $G \neq H$ and H is of even order. Moreover, H is the unique group of even order such that $H \in S$, for any $S \in \mathcal{H}_{\mathbb{Q}}(3, G)$ because $f(X)$ is the 2-division polynomial of E.

Now, for any $G \in \Phi(1)$, let us construct the elements $S \in \mathcal{H}_{\mathbb{Q}}(3, G)$ in ascending order of $\#S$. In Table 1 (see the Appendix) we show examples for all possible cases of S (after taking into account the preliminary remark) for any $G \in \Phi(1)$. Now, by (i), we know that there are not repeated elements in any $S \in \mathcal{H}_{\mathbb{Q}}(3, G)$. Then the possible cases with $\#S > 1$ come from $G = \mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$:

$\boxed{G = \mathcal{C}_1}$

We show examples in Table 1 for any $S \in \mathcal{H}_{\mathbb{Q}}(3, \mathcal{C}_1)$ with $\#S = 2$ except for the following cases:

$$[\mathcal{C}_4, \mathcal{C}_{13}],\ [\mathcal{C}_3, \mathcal{C}_6],\ [\mathcal{C}_6, \mathcal{C}_7],\ [\mathcal{C}_6, \mathcal{C}_{13}],$$
$$[\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_{13}],\ [\mathcal{C}_2 \times \mathcal{C}_{14}, \mathcal{C}_3],\ [\mathcal{C}_2 \times \mathcal{C}_{14}, \mathcal{C}_7],\ [\mathcal{C}_2 \times \mathcal{C}_{14}, \mathcal{C}_{13}].$$

- As for $[\mathcal{C}_4, \mathcal{C}_{13}]$, if such a curve existed, then it would have to have discriminant $-Y^2$ (as it gains 4-torsion, see Proposition 2.3 (ii)) for some rational Y. On the other hand, the curve must have a 13-isogeny over $\mathbb{Q}$, which implies its discriminant is of the form [**18,** Lemma 27]
$$\Delta = \Box \cdot t(t^2 + 6t + 13),$$
where $\Box$ is a rational square. Therefore, such a curve would give a rational non-trivial (meaning $Y \neq 0$) solution of the equation
$$Y^2 = X^3 - 6X^2 + 13X,$$
but one easily checks that there are none.
- Looking at $[\mathcal{C}_3, \mathcal{C}_6]$ we find that E gains full 3-torsion over the compositum of two cubic extensions, K_1 and K_2, because the fields cannot be isomorphic; hence, the points of order 3 in K_1 and K_2 are independent. This implies $\mathbb{Q}(\zeta_3) \subset K_1K_2$, which is impossible as $[K_1K_2 : \mathbb{Q}] = 9$ in this case.
- Let us look at the pair $[\mathcal{C}_6, \mathcal{C}_7]$. The existence of $\mathcal{C}_6$ implies a 3-isogeny over $\mathbb{Q}$ and the existence of $\mathcal{C}_7$ implies a rational 7-isogeny; hence, E has a 21-isogeny. Therefore, E is a twist of an elliptic curve in the `162b` isogeny class. It can be seen that only one elliptic curve in each of the four families of twists

gains 7-torsion in a cubic extension. Thus, there are in fact a total of four curves that we need to check. For each of the four curves we can check whether the curve gains any 3-torsion in the fields where it gains 2-torsion, and discard all the cases.

- The case $[\mathcal{C}_6, \mathcal{C}_{13}]$ can be ruled out as, from Proposition 2.4 (iii) and Lemma 2.6, it would imply the existence of a curve with a rational 39-isogeny, contradicting Proposition 2.4 (i).
- The case $[\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_{13}]$ is very similar to the first one, the only difference being that, gaining full 2-torsion over a cubic field, the discriminant must be a square. Anyway, the corresponding equation
$$Y^2 = X^3 + 6X^2 + 13X,$$
still has no solutions with $Y \neq 0$.
- Let us look at the case $[\mathcal{C}_2 \times \mathcal{C}_{14}, \mathcal{C}_3]$. A curve featuring these torsion extensions would have a 21-isogeny from Proposition 2.4 (ii), (iv) and Lemma 2.6 and also would gain full 2-torsion over a cubic field, so as in the previous case its discriminant must be a square. But the elliptic curves with a 21-isogeny have discriminant $-2\cdot\square$, where $\square$ is a rational square [**1,** pages 78–80]. Hence, this case is not possible.
- We can remove the case $[\mathcal{C}_2 \times \mathcal{C}_{14}, \mathcal{C}_7]$, similarly as the second case. In this case, we would have two cubic extensions K_1 and K_2 which must verify $[K_1K_2 : \mathbb{Q}] = 9$, as $X^3 + AX + B$ splits completely in one of them and remains irreducible in the other. As $\mathbb{Q}(\zeta_7) \subset K_1K_2$ using Proposition 2.1 above, we reach a contradiction.
- The last case, that of $[\mathcal{C}_2 \times \mathcal{C}_{14}, \mathcal{C}_{13}]$, is also removable as it would similarly imply the existence of a rational elliptic curve with a 91-isogeny.

Now, we need to prove that the only $S \in \mathcal{H}_{\mathbb{Q}}(3, \mathcal{C}_1)$ with $\#S = 3$ is $[\mathcal{C}_2, \mathcal{C}_3, \mathcal{C}_7]$. For this purpose we have to remove the cases:
$$[\mathcal{C}_2, \mathcal{C}_3, \mathcal{C}_{13}],\ [\mathcal{C}_2, \mathcal{C}_7, \mathcal{C}_{13}],\ [\mathcal{C}_3, \mathcal{C}_4, \mathcal{C}_7],\ [\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_3, \mathcal{C}_7].$$

- The first case can be ruled out as $[\mathcal{C}_6, \mathcal{C}_{13}]$ above, for it implies the existence of a rational curve with a 39-isogeny.
- The second case, as $[\mathcal{C}_2 \times \mathcal{C}_{14}, \mathcal{C}_{13}]$ above, would imply the existence of a rational elliptic curve with a 91-isogeny. Hence, it cannot happen.

- The third case is eliminated by noting that the discriminant of such a curve should be $-Y^2$ (for it gains 4-torsion) and $-2 \cdot \square$, where $\square$ is a rational square (for it has a 21-isogeny).
- The last case is similar to the case $[\mathcal{C}_2 \times \mathcal{C}_{14}, \mathcal{C}_3]$ above.

Looking with greater detail at the case $[\mathcal{C}_2, \mathcal{C}_3, \mathcal{C}_7]$ we find that if a curve gains torsion in such a way in three non-isomorphic cubic fields, it must have a 21-isogeny and in fact (as in the $[\mathcal{C}_6, \mathcal{C}_7]$ case) it can only be a very precise curve a family of twists in the `162b` isogeny class. There are only four such curves and `162b2` is the only one that grows strictly in three cubic extensions.

$\boxed{G = \mathcal{C}_2}$

The only case to discard here is $[\mathcal{C}_6, \mathcal{C}_{14}]$. If such a curve (say E) existed, it would follow that E would have a 3-isogeny and 7-isogeny, and hence, a 21-isogeny. E would also have to contain $\mathcal{C}_2$, since the odd isogeny cannot kill this torsion. But there do not exist elliptic curves with 21-isogenies and nontrivial 2-torsion over $\mathbb{Q}$ [**1,** pages 78–80].

$\boxed{G = \mathcal{C}_3}$

We show examples in Table 1 for any $S \in \mathcal{H}_{\mathbb{Q}}(3, \mathcal{C}_3)$ with $\#S = 2$, except for the cases:

$$[\mathcal{C}_9, \mathcal{C}_{12}]\,,\ [\mathcal{C}_{12}, \mathcal{C}_{21}]\,,\ [\mathcal{C}_2 \times \mathcal{C}_6, \mathcal{C}_9]\,,\ [\mathcal{C}_2 \times \mathcal{C}_6, \mathcal{C}_{21}]\,.$$

- $[\mathcal{C}_9, \mathcal{C}_{12}]$. From Proposition 2.4 (vi), our curve has either a 9-isogeny or two independent 3-isogenies and $\mathbb{Q}(E[3]) = \mathbb{Q}(\zeta_3)$. Moreover, from Proposition 2.3 (iii), $\Delta \in (-1) \cdot (\mathbb{Q}^*)^2$.

  Assume that E has two independent 3-isogenies and $\mathbb{Q}(E[3]) = \mathbb{Q}(\zeta_3)$. From [**20,** page 147], we get

  $$\Delta = -216 \frac{b^3(h^6 - 6h^2b^2 + 12b^3)}{h^6}, \quad b, h \in \mathbb{Q}.$$

  Note there is a misprint in the original article: h^4 in the numerator should be replaced by h^6.

  As $\Delta = -y^2$ for some $y \in \mathbb{Q}$, the existence of E implies there are $b, h, y \in \mathbb{Q}$ with

  $$\left(\frac{y}{bh}\right)^2 = 6\left(\frac{b}{h^2}\right)\left[1 - 6\left(\frac{b}{h^2}\right)^2 - 12\left(\frac{b}{h^2}\right)^3\right],$$

that is a rational point on the curve

$$Y^2 = 6X\left(1 - 6X^2 - 12X^3\right),$$

but its Mordell-Weil group is trivial, and the trivial points do not yield an elliptic curve E.

So we are bound to assume that E has a 9-isogeny. From [**7,** Appendix], it follows that E is a twist of $u^2 = v^3 + av + b$, where

$$a = -3x(x^3 - 24), \quad b = 2(x^6 - 36x^6 + 216),$$

for some $x \in \mathbb{Q}$. Then the discriminant of this curve is

$$2^{12}3^6(c^3 - 27)u^{12},$$

where the twelfth power may appear because of the twisting. As this should be in $(-1) \cdot (\mathbb{Q}^*)^2$, it should give a point on

$$Y^2 = X^3 - 27.$$

The points in this curve can be easily computed (we have done it with `Magma` [**2**]); there is only the point at infinity and a point of order 2 that discriminant 0, so we are done.

- Second and fourth cases are not possible, as the only curve whose torsion grows to $\mathcal{C}_{21}$ is `162b1`, and this curve fits neither of these cases (see Table 1).
- $[\mathcal{C}_2 \times \mathcal{C}_6, \mathcal{C}_9]$. This case parallels the first one. The only formal change is that, as we gain full 2-torsion in a cubic extension, $\Delta \in (\mathbb{Q}^*)^2$. Hence, the same arguments lead us to state that such a curve must yield either a point on

$$Y^2 = -6X\left(1 - 6X^2 - 12X^3\right),$$

if it has two independent rational 3-isogenies, or a point on

$$Y^2 = X^3 + 27,$$

should it have a rational 9-isogeny. As both cases can be checked to be impossible, we are finished.

Finally, we see that there are no $S \in \mathcal{H}_{\mathbb{Q}}(3, \mathcal{C}_3)$ with $\#S = 3$. Such S should have two groups of odd order. These must be $\mathcal{C}_9$ and $\mathcal{C}_{21}$. But again the unique elliptic curve over $\mathbb{Q}$ with $\mathcal{C}_{21}$ over a cubic field is `162b1` and, for this curve, this is not the case (see Table 1).

APPENDIX

A. Computations. Let $G \in \Phi(1)$, $S = [H_1, \ldots, H_m] \in \mathcal{H}_{\mathbb{Q}}(3, G)$, E an elliptic curve defined over $\mathbb{Q}$ such that $E(\mathbb{Q})_{\text{tors}} = G$, and let $K_1, \ldots, K_m$ be cubic fields, such that

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

Table 1 shows an example of every possible situation, where

- the first column is G,
- the second column is $S \in \mathcal{H}_{\mathbb{Q}}(3, G)$,
- the third column is $\#S$,
- the fourth column is the label of the elliptic curve E with minimal conductor satisfying the conditions above,
- the fifth column displays a defining cubic polynomial corresponding to the respective K_i of H_i in S,
- the sixth column displays the discriminant of the corresponding K_i.

Table 1: $h = \#S$ for $S \in \mathcal{H}_{\mathbb{Q}}(3, G)$.

G	$\mathcal{H}_{\mathbb{Q}}(3,G)$	h	label	cubics	Δ
$\mathcal{C}_1$	$\mathcal{C}_2$	1	11a2	$x^3 - x^2 + x + 1$	-44
	$\mathcal{C}_4$		338b2	$x^3 - x^2 - 4x + 12$	-676
	$\mathcal{C}_6$		108a2	$x^3 - 2$	-108
	$\mathcal{C}_2 \times \mathcal{C}_2$		196a1	$x^3 - x^2 - 2x + 1$	49
	$\mathcal{C}_2 \times \mathcal{C}_{14}$		1922c1	$x^3 - x^2 - 10x + 8$	961
	$\mathcal{C}_2, \mathcal{C}_3$	2	19a2	$x^3 - 2x - 2$ $x^3 - x^2 - 6x - 12$	-76 -1083
	$\mathcal{C}_2, \mathcal{C}_7$		294a1	$x^3 - x^2 - 2x - 6$ $x^3 - x^2 - 2x + 1$	-1176 49
	$\mathcal{C}_2, \mathcal{C}_{13}$		147b1	$x^3 - x^2 + 5x + 1$ $x^3 - x^2 - 2x + 1$	-588 49
	$\mathcal{C}_3, \mathcal{C}_4$		162d2	$x^3 - 2$ $x^3 - 3x - 4$	-108 -324
	$\mathcal{C}_3, \mathcal{C}_2 \times \mathcal{C}_2$		196b2	$x^3 - x^2 + 5x + 1$ $x^3 - x^2 - 2x + 1$	-588 49
	$\mathcal{C}_4, \mathcal{C}_7$		338b1	$x^3 - x^2 - 4x + 12$ $x^3 - x^2 - 4x - 1$	-676 169

(Continued on next page)

Table 1. (Continued from previous page)

G	$\mathcal{H}_{\mathbb{Q}}(3,G)$	h	label	cubics	Δ
	$\mathcal{C}_7, \mathcal{C}_2 \times \mathcal{C}_2$		`3969a1`	$x^3-21x-35$ $x^3-21x-28$	3969 3969
	$\mathcal{C}_2, \mathcal{C}_3, \mathcal{C}_7$	3	`162b2`	$x^3-3x-10$ x^3-2 x^3-3x-1	-648 -108 81
$\mathcal{C}_2$	$\mathcal{C}_6$	1	`14a3`	x^3-7	-1323
	$\mathcal{C}_{14}$		`49a3`	x^3-x^2-2x+1	49
$\mathcal{C}_3$	$\mathcal{C}_6$	1	`19a1`	x^3-2x-2	-76
	$\mathcal{C}_{12}$		`162d1`	x^3-3x-4	-324
	$\mathcal{C}_2 \times \mathcal{C}_6$		`196b1`	x^3-x^2-2x+1	49
	$\mathcal{C}_6, \mathcal{C}_9$	2	`19a3`	x^3-2x-2 x^3-x^2-6x+7	-76 361
	$\mathcal{C}_6, \mathcal{C}_{21}$		`162b1`	$x^3-3x-10$ x^3-3x-1	-648 81
$\mathcal{C}_4$	$\mathcal{C}_{12}$	1	`90c1`	x^3-x^2-3x-3	-300
$\mathcal{C}_5$	$\mathcal{C}_{10}$	1	`11a1`	x^3-x^2+x+1	-44
$\mathcal{C}_6$	$\mathcal{C}_{18}$	1	`14a4`	x^3-x^2-2x+1	49
$\mathcal{C}_7$	$\mathcal{C}_{14}$	1	`26b1`	x^3-x-2	-104
$\mathcal{C}_8$		0			
$\mathcal{C}_9$	$\mathcal{C}_{18}$	1	`54b3`	x^3+3x-2	-216
$\mathcal{C}_{10}$		0			
$\mathcal{C}_{12}$		0			
$\mathcal{C}_2 \times \mathcal{C}_2$	$\mathcal{C}_2 \times \mathcal{C}_6$	1	`30a6`	x^3-3	-243
$\mathcal{C}_2 \times \mathcal{C}_4$		0			
$\mathcal{C}_2 \times \mathcal{C}_6$		0			
$\mathcal{C}_2 \times \mathcal{C}_8$		0			

REFERENCES

1. B.J. Birch and W. Kuyk, eds., *Modular functions of one variable*, IV, Lect. Notes Math. **476**, Springer, New York, 1975.

2. W. Bosma, J. Cannon and C. Fieker, et al., eds., *Handbook of Magma functions*, edition 2.20, `http://magma.maths.usyd.edu.au/magma`, 2013.

3. J.E. Cremona, *Elliptic curve data for conductors up to* 320.000, available at `http://www.warwick.ac.uk/~masgaj/ftp/data/`, 2014.

4. T. Dokchitser and V. Dokchitser, *Surjectivity of* $\bmod 2^n$ *representations of elliptic curves*, Math. Z. **272** (2012), 961–964.

5. E. González-Jiménez and J.M. Tornero, *Torsion of rational elliptic curves over quadratic fields* Rev. Roy. Acad. Cienc. Exactas **110** (2016), 121–143.

6. ———, *Torsion of rational elliptic curves over quadratic fields*, II, submitted.

7. P. Ingram, *Diophantine analysis and torsion on elliptic curves*, Proc. Lond. Math. Soc. **94** (2007) 137–154.

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

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

10. M.A. Kenku, *The modular curves* $X_0(65)$ *and* $X_0(91)$ *and rational isogeny*, Math. Proc. Cambr. Philos. Soc. **87** (1980), 15–20.

11. ———, *The modular curve* $X_0(169)$ *and rational isogeny*, J. Lond. Math. Soc. **22** (1980), 239–244.

12. ———, *The modular curves* $X_0(125)$, $X_1(25)$ *and* $X_1(49)$, J. Lond. Math. Soc. **23** (1981), 415–427.

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

14. A.W. Knapp, *Elliptic curves*, in *Mathematical notes* **40**, Princeton University Press, Princeton, 1992.

15. B. Mazur, *Modular curves and the Eisenstein ideal*, Publ. Math. Inst. Hautes Etud. Sci. **47** (1977), 33–186.

16. ———, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162.

17. F. Najman, *Torsion of elliptic curves over cubic fields*, J. Num. Th. **132** (2012), 26–36.

18. ———, *Torsion of rational elliptic curves over cubic fields and sporadic points on* $X_1(n)$, Math. Res. Lett. **23** (2016), 245-272.

19. ———, *The number of twists with large torsion of an elliptic curve*, Rev. Roy. Acad. Cienc. Exactas **109** (2015), 535-547.

20. L. Paladino, *Elliptic curves with* $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$ *and counterexamples to local-global divisibility by* 9, J. Th. Nombr. Bordeaux **22** (2010), 139–160.

21. J.H. Silverman, *The arithmetic of elliptic curves*, Springer, New York, 1986.

Universidad Autónoma de Madrid, Departamento de Matemáticas and Instituto de Ciencias Matemáticas (ICMat), Madrid, Spain
Email address: **enrique.gonzalez.jimenez@uam.es**

University of Zagreb, Bijenička cesta 30, 10000 Zagreb, Croatia
Email address: **fnajman@math.hr**

Departamento de Álgebra and IMUS, Universidad de Sevilla, P.O. 1160, 41080 Sevilla, Spain
Email address: **tornero@us.es**