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, m, where m divides n and where $\mathcal{C}_n$ is a cyclic group of order n from now on.

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 deeply studied 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 not any 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 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 write here only the latter set:

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

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 $E(\mathbb{Q})_{\rm tors} \simeq G \in \Phi(1)$ was determined. The first goal of this paper is giving a complete description (see Theorem 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 author obtained, for $d = 2$ and for all $G \in \Phi(1)$, the set

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

Date: Sunday 9$^{\rm th}$ November, 2014 : 17:58.

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

The first author was partially supported by the grant MTM2012–35849. The third author was partially supported by the grants FQM–218 and P12–FQM–2696 (FSE and FEDER (EU)).

where, for any $i = 1, ..., n$, $S_i = [H_1, ..., H_m]$ 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:

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

Note that we are allowing the possibility of two (or more) of the H_j being isomorphic. From these results, it follows [6, 19]:

Corollary 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 $E(K_i)_{\rm tors} \neq E(\mathbb{Q})_{\rm tors}$. That is,*

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

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 3). Precisely, the main results of this paper are the following:

Theorem 2. *For $G \in \Phi(1)$, the set $\Phi_{\mathbb{Q}}(3, G)$ is the following:*

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

The sets $\Phi_{\mathbb{Q}}(3, G)$ were first implies by the computations that can be found in the appendix. These computations also prove that all the listed groups actually are in $\Phi_{\mathbb{Q}}(3, G)$.

Theorem 3. *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*

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

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*

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

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

(iii) *Let be $G \in \Phi(1)$ such that $\Phi_{\mathbb{Q}}(3, G) \neq \{G\}$. Then the set $\mathcal{H}_{\mathbb{Q}}(3, G)$ consists of the following elements (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 result previously known [8, Lemma 3.3] stated that the torsion subgroup of a rational elliptic curve grows strictly in only finitely many cubic number fields.

Notation: Please mind that, in the sequel, for examples and precise curves we will use the Antwerp–Cremona tables and labels [1, 2]. 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 detail on the precise isomorphism.

2. Auxiliary results

We will fix once and for all some notations. 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 which 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, Ch. III, 8.1.1]

Proposition 4. *Let E be an elliptic curve over a number field K. If $\mathcal{C}_m \times \mathcal{C}_m \leq E(K)$, then K contains the cyclotomic field $\mathbb{Q}(\zeta_m)$ generated by the m–th roots of unity.*

Let us fix the set–up, following [18]. Let $K/\mathbb{Q}$ be a cubic extension, and L 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 posible 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

$$\begin{tikzcd}[column sep=small]
 & L \arrow[dr, dash, "2"] \arrow[ddl, dash, "3"'] & \\
 & & K \arrow[ddl, dash, "3"] \\
M \arrow[dr, dash, "2"'] & & \\
 & \mathbb{Q} &
\end{tikzcd}$$

Remark. 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 5. *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 $\mathcal{C}_4 \not\leq G$, then $\mathcal{C}_8 \not\leq H$ and, if $\mathcal{C}_4 \leq H$, 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 Prop. 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 6. *Let E be an elliptic curve defined over $\mathbb{Q}$, K and L as above.*

(i) *Assume E has a rational n-isogeny. Then either $1 \leq n \leq 19$, or $n \in \{21, 25, 27, 37, 43, 67, 163\}$* [16, 10, 11, 12].
(ii) *Assume 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 isogeneous (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 $E(K)$ 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 7. *Let p be 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. □

Lemma 8. *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 5 (vi). And by Proposition 6 (v), E has a 3–isogeny over $\mathbb{Q}$. □

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

Proof. By Proposition 6 (vi) $E/\mathbb{Q}$ has either an isogeny of degree 9 or 2 isogenies of degree 3.

First suppose it has 2 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 non–trivial 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 $[4]$ or $[7]$. Both of these act trivially on $\langle 3P\rangle$, implying that $E(\mathbb{Q})$ has non–trivial 3–torsion. □

Remark. Now and then we will consider the case where we have K_1 and K_2 two different cubic number fields. Let us write as usual K_1K_2 for the compositum field of both extensions. Then one of these 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 2

Note that from Proposition 5 (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 5 (i) and the description of $\Phi_{\mathbb{Q}}(3)$, we can solve the non–cyclic cases from Theorem 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 discard already 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 6 (ii) and (iii), that would imply E has a 28–isogeny, contradicting Proposition 6 (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 the table below we indicate:

- With (i) - (vi), which part of Proposition 5 is used,
- With (**9**), the case is ruled out from Lemma 9,
- With $-$, the case is ruled out because $G \not\subset H$,
- With $\checkmark$, the case is possible (and in fact, it occurs).

The table (row= H, column= G) deals with the case G cyclic.

	$\mathcal{C}_1$	$\mathcal{C}_2$	$\mathcal{C}_3$	$\mathcal{C}_4$	$\mathcal{C}_5$	$\mathcal{C}_6$	$\mathcal{C}_7$	$\mathcal{C}_8$	$\mathcal{C}_9$	$\mathcal{C}_{10}$	$\mathcal{C}_{12}$
$\mathcal{C}_1$	$\checkmark$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$
$\mathcal{C}_2$	$\checkmark$	$\checkmark$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$
$\mathcal{C}_3$	$\checkmark$	$-$	$\checkmark$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$
$\mathcal{C}_4$	$\checkmark$	(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)	$-$	$-$	$-$	$\checkmark$	$-$	$-$	$-$
$\mathcal{C}_9$	(**9**)	$-$	$\checkmark$	$-$	$-$	$-$	$-$	$-$	$\checkmark$	$-$	$-$
$\mathcal{C}_{10}$	(iii)	(iii)	$-$	$-$	$\checkmark$	$-$	$-$	$-$	$-$	$\checkmark$	$-$
$\mathcal{C}_{12}$	(?)	(i)	$\checkmark$	$\checkmark$	$-$	(i)	$-$	$-$	$-$	$-$	$\checkmark$
$\mathcal{C}_{13}$	$\checkmark$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$
$\mathcal{C}_{14}$	(?)	$\checkmark$	$-$	$-$	$-$	$-$	$\checkmark$	$-$	$-$	$-$	$-$
$\mathcal{C}_{18}$	(**9**)	(**9**)	(?)	$-$	$-$	$\checkmark$	$-$	$-$	$\checkmark$	$-$	$-$
$\mathcal{C}_{21}$	(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 5 (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 6 (ii). Then, from Lemma 7 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 5 (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 7 and Proposition 6 (vi) we have that $E(\mathbb{Q})$ must have 2 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 $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$–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 4.

As L is the splitting field of X^3+AX+B, this really implies $E(L)_{tors} \leq C_6 \times C_{18}$. 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 3

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 be $H = G \times \mathcal{C}_m$ 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 essentialy 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 imposible, 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 3.

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

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

is an elliptic curve defined over $\mathbb{Q}$ such that $E(\mathbb{Q})_{\mathrm{tors}} \simeq G$ has odd order, then $f(X)$ is an irreducible cubic polynomial. Now, denote by K the cubic field defined by $f(X)$, then $H = E(K)_{\mathrm{tors}}$ 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 Appendix) we show examples for all the 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 have examples in Table 1 for any $S \in \mathcal{H}_{\mathbb{Q}}(3, \mathcal{C}_1)$ with $\#S = 2$ except for the 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 5 (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]
$$\Delta = \square \cdot t(t^2 + 6t + 13)$$
where $\square$ 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 4 family of twists gains 7–torsion in a cubic extension. Thus there are in fact 4 curves that we need to check, all in all. For each of the 4 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 6 (iii) and Lemma 8, it would imply the existence of a curve with a rational 39–isogeny, contradicting Proposition 6 (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 6 (ii,iv) and Lemma 8 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, pp. 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 $[K_1 K_2 : \mathbb{Q}] = 9$, as $X^3 + AX + B$ splits completely in one of them and remains irreducible in the other. As $\mathbb{Q}(\zeta_7) \subset K_1 K_2$ using Proposition 4 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 4 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 non–trivial 2–torsion over $\mathbb{Q}$ [1, pp. 78–80].

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

We have 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 6 (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 5 (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, p. 147] we get[1]

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

  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 point do not yield an elliptic curve E.

  So we are bound to assume 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 discriminat of this curve is

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

  where the twelfth power may appear because of 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` [3]); 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

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

[1] Note there is a misprint in the original article, h^4 in the numerator should be replaced by h^6.

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: Computations

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

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

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 the coefficients of corresponding defining cubic polynomial to the respective $H's$ in S.

References

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

[2] Cremona, J. E.: *Elliptic curve data for conductors up to 320.000.* Available on `http://www.warwick.ac.uk/ masgaj/ftp/data/`, 2014.

[3] Bosma, W.; Cannon, J.; Fieker, C; Steel, A (eds.): *Handbook of Magma functions, Edition 2.20.* `http://magma.maths.usyd.edu.au/magma`, 2013.

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

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

[6] González–Jiménez, E.; Tornero, J.M.: *Torsion of rational elliptic curves over quadratic fields II.* Submitted.

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

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

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

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

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

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

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

[14] Knapp, A.W.: Elliptic curves. Mathematical Notes, **40**. Princeton University Press (1992).

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

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

[17] Najman, F.: *Torsion of elliptic curves over cubic fields*. J. Number Theory **132** (2012), no. 1, 26–36.
[18] Najman, F.: *Torsion of rational elliptic curves over cubic fields and sporadic points on* $X_1(n)$. Math. Res. Lett., to appear.
[19] Najman, F.: *The number of twists with large torsion of an elliptic curve*. Rev. R. Acad. Cienc. Exactas Fís. Nat. Ser. A Math. RACSAM, to appear.
[20] Paladino, 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.
[21] 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

University of Zagreb, Bijenička cesta 30, 10000 Zagreb, Croatia
E-mail address: fnajman@math.hr
URL: http://web.math.pmf.unizg.hr/~fnajman/

Departamento de Álgebra, Universidad de Sevilla. P.O. 1160. 41080 Sevilla, Spain.
E-mail address: tornero@us.es

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

G	$\mathcal{H}_{\mathbb{Q}}(3,G)$	h	label	cubics
$\mathcal{C}_1$	$\mathcal{C}_2$	1	11a2	$[-12419196912, -10135152, 0, 1]$
	$\mathcal{C}_4$		338b2	$[872683713, 799551, -513, 1]$
	$\mathcal{C}_6$		108a2	$[-80, -24, -24, 1]$
	$\mathcal{C}_2 \times \mathcal{C}_2$		196a1	$[-5832, -2916, 18, 1]$
	$\mathcal{C}_2 \times \mathcal{C}_{14}$		1922c1	$[191319746769, -8017245, -216621, 1]$
	$\mathcal{C}_2, \mathcal{C}_3$	2	19a2	$[432, -864, 0, -1]$, $[577, 1155, 2307, 1]$
	$\mathcal{C}_2, \mathcal{C}_7$		294a1	$[8909298, -29835, 324, 1]$, $[2000376, -142884, -126, 1]$
	$\mathcal{C}_2, \mathcal{C}_{13}$		147b1	$[1928016, -8208, 648, 1]$, $[2000376, -142884, -126, 1]$
	$\mathcal{C}_3, \mathcal{C}_4$		162d2	$[-5200640, -19968, -600, 1]$, $[-2020032, 28944, 90, 1]$
	$\mathcal{C}_3, \mathcal{C}_2 \times \mathcal{C}_2$		196b2	$[-4076477, -8565, -6927, 1]$, $[-16003008, -571536, 252, 1]$
	$\mathcal{C}_4, \mathcal{C}_7$		338b1	$[100472373, 1906011, -153, 1]$, $[64064520, -492804, -1170, 1]$
	$\mathcal{C}_7, \mathcal{C}_2 \times \mathcal{C}_2$		3969a1	$[30005640, -142884, -1890, 1]$, $[-6578496, -46656, 1269, 1]$
	$\mathcal{C}_2, \mathcal{C}_3, \mathcal{C}_7$	3	162b2	$[190144, 32880, -15, 1]$, $[-1324783, 70851, 51, 1]$, $[1417176, -26244, -486, 1]$
$\mathcal{C}_2$	$\mathcal{C}_6$	1	14a3	$[-5581197, -3861, -3231, 1]$
	$\mathcal{C}_{14}$		49a3	$[26004888, -142884, -1638, 1]$
$\mathcal{C}_3$	$\mathcal{C}_6$	1	19a1	$[857881, 18003, -69, 1]$
	$\mathcal{C}_{12}$		162d1	$[-95707, -933, -777, 1]$
	$\mathcal{C}_2 \times \mathcal{C}_6$		196b1	$[2000376, -142884, -126, 1]$
	$\mathcal{C}_6, \mathcal{C}_9$	2	19a3	$[-432, 864, 0, 1]$, $[40824, -2916, -126, 1]$
	$\mathcal{C}_6, \mathcal{C}_{21}$		162b1	$[8882, -267, 132, 1]$, $[14984, -564, -570, 1]$
$\mathcal{C}_4$	$\mathcal{C}_{12}$	1	90c1	$[-11243584, -11472, -2892, 1]$
$\mathcal{C}_5$	$\mathcal{C}_{10}$	1	11a1	$[-74368, -384, -336, 1]$
$\mathcal{C}_6$	$\mathcal{C}_{18}$	1	14a4	$[5832, -2916, -18, 1]$
$\mathcal{C}_7$	$\mathcal{C}_{14}$	1	26b1	$[44396, -960, 87, 1]$
$\mathcal{C}_8$		0		
$\mathcal{C}_9$	$\mathcal{C}_{18}$	1	54b3	$[-12331008, -13824, -72, 1]$
$\mathcal{C}_{10}$		0		
$\mathcal{C}_{12}$		0		
$\mathcal{C}_2 \times \mathcal{C}_2$	$\mathcal{C}_2 \times \mathcal{C}_6$	1	30a6	$[-3621888, -8640, -1476, 1]$
$\mathcal{C}_2 \times \mathcal{C}_4$		0		
$\mathcal{C}_2 \times \mathcal{C}_6$		0		
$\mathcal{C}_2 \times \mathcal{C}_8$		0		