GLASNIK MATEMATIČKI
Vol. 56(76)(2021), 47 – 61

EXPLICIT CHARACTERIZATION OF THE TORSION GROWTH OF RATIONAL ELLIPTIC CURVES WITH COMPLEX MULTIPLICATION OVER QUADRATIC FIELDS

Enrique González–Jiménez
Universidad Autónoma de Madrid, Spain

Abstract. In a series of papers we classify the possible torsion structures of rational elliptic curves base-extended to number fields of a fixed degree. In this paper we turn our attention to the question of how the torsion of an elliptic curve with complex multiplication defined over the rationals grows over quadratic fields. We go further and we give an explicit characterization of the quadratic fields where the torsion grows in terms of some invariants attached to the curve.

1. Introduction

For over a century mathematicians have been enamored with the study of elliptic curves. Of particular interest has been characterizing the possible torsion structures of elliptic curves defined over a number field of fixed degree. The set of possible groups (up to isomorphism) is denoted by $\Phi(d)$ and much progress in understanding this set has been made in the last few decades. Thanks to Merel ([27]), it is known that $\Phi(d)$ is finite. Beyond this, there are only two cases published in the literature. The case when $d = 1$ was proven by Mazur ([26]) and the case when $d = 2$ by Kamienny ([24]) and Kenku and Momose ([25]). Recently, Derickx, Etropolski, van Hoeij, Morrow, and Zureick-Brown have released an article [8] with a complete description of $\Phi(3)$. As of now, the case when $d > 3$ remains open.

The purpose of this paper is somewhat different: we are interested in studying how the torsion grows when the field of definition is enlarged. That

2020 *Mathematics Subject Classification.* 11G05, 11G15.
Key words and phrases. Elliptic curves, complex multiplication, torsion subgroup, rationals, quadratic fields.
The author was partially supported by the grant PGC2018-095392-B-I00.

is, we will restrict to the case when the field of definition of the elliptic curve is actually $\mathbb{Q}$, but considered over a larger number field. In this context, the first problem is to characterize the set $\Phi_{\mathbb{Q}}(d)$ of possible groups (up to isomorphism) that can appear as the torsion subgroup of an elliptic curve defined over $\mathbb{Q}$ base extended to a field of degree d. The set $\Phi_{\mathbb{Q}}(d)$ has been completely classified for $d = 2, 3, 4, 5, 7$ and for any positive integer d whose prime divisors are greater than 7 (cf. [29, 4, 18, 13]). The case $d = 6$ has been studied in [7, 23].

Another problem that we are interested in is understanding the behavior of a particular torsion group $G \in \Phi(1)$ when we enlarge the base field $\mathbb{Q}$. That is, if $E/\mathbb{Q}$ is an elliptic curve such that $E(\mathbb{Q})_{\rm tors} \simeq G$, what groups (up to isomorphism) are of the form $E(K)_{\rm tors}$ as K runs over all number fields of degree d? Let $\Phi_{\mathbb{Q}}(d, G)$ denote the subset of $\Phi_{\mathbb{Q}}(d)$ such that E runs through all elliptic curves over $\mathbb{Q}$ such that $E(\mathbb{Q})_{\rm tors} \simeq G$. The set $\Phi_{\mathbb{Q}}(d, G)$ has been determined for $d = 2, 3, 4, 5, 7$ and for any positive integer d whose prime divisors are greater than 7 (cf. [21, 20, 17, 18, 13]). The case $d = 6$ has been studied in [7].

In fact, we can refine the previous question even further. We start by noting that if E is an elliptic curve defined over $\mathbb{Q}$ and K a number field such that the torsion of E grows from $\mathbb{Q}$ to K, then of course the torsion of E also grows from $\mathbb{Q}$ to any extension of K. With this in mind, we say that the torsion growth over K is primitive if $E(K')_{\rm tors} \subsetneq E(K)_{\rm tors}$ for any subfield $K' \subsetneq K$. We denote by $\mathcal{H}_{\mathbb{Q}}(d, E)$ the list formed by $E(\mathbb{Q})_{\rm tors}$ together with the groups H such that there exists a number field K (up to isomorphism) of degree dividing d such that E has primitive torsion growth over K and $E(K)_{\rm tors} \simeq H$. We point out here that we are allowing two (or more) of the torsion subgroups H to be isomorphic if the corresponding number fields are not isomorphic. We call $\mathcal{H}_{\mathbb{Q}}(d, E)$ the set of torsion configurations (of degree d) of the elliptic curve $E/\mathbb{Q}$. We let $\mathcal{H}_{\mathbb{Q}}(d)$ denote the set of $\mathcal{H}_{\mathbb{Q}}(d, E)$ as E runs over all elliptic curves defined over $\mathbb{Q}$ such that $\mathcal{H}_{\mathbb{Q}}(d, E) \neq \{E(\mathbb{Q})_{\rm tors}\}$. Finally, for any $G \in \Phi(1)$ we define $\mathcal{H}_{\mathbb{Q}}(d, G)$ as the set of lists $\mathcal{H}_{\mathbb{Q}}(d, E)$ where E runs over all the elliptic curves defined over $\mathbb{Q}$ such that $E(\mathbb{Q})_{\rm tors} \simeq G$ and $\mathcal{H}_{\mathbb{Q}}(d, E) \neq \{G\}$. Denote by $h_{\mathbb{Q}}(d)$ the maximum of the cardinality of the sets S when $S \in \mathcal{H}_{\mathbb{Q}}(d)$, in other words, $h_{\mathbb{Q}}(d)$ gives the maximum number of field extensions of degrees dividing d where there is primitive torsion growth. The sets $\mathcal{H}_{\mathbb{Q}}(d, G)$ and $\mathcal{H}_{\mathbb{Q}}(d)$ and the integer $h_{\mathbb{Q}}(d)$, have been determined for $d = 2, 3, 5, 7$ and for any positive integer d whose prime divisors are greater than 7 (cf. [22, 20, 13, 18]). The cases $d = 4$ and $d = 6$ have been studied in [17] and [7] respectively.

Finally, once we have a complete classification of the sets $\Phi_{\mathbb{Q}}(d)$, $\Phi_{\mathbb{Q}}(d, G)$ and $\mathcal{H}_{\mathbb{Q}}(d, G)$ for a fixed d, there is the much harder problem (cf. [21, Problem 2]).

PROBLEM 1.1. *Let E be an elliptic curve defined over $\mathbb{Q}$ and d a positive integer. Is there a precise (and easy) description of which are the possible number fields K of degree dividing d where the torsion growth over K is primitive, ideally in terms of some invariant(s) of the curve?*

In [19] the authors present a fast algorithm that takes as input an elliptic curve defined over $\mathbb{Q}$ and an integer d and returns all the number fields of degree dividing d where there is primitive torsion growth. But this algorithm does not provide a solution to our problem since it does not compute the number fields in terms of the invariants of the elliptic curve.

Ideally we would like an answer to this problem in complete generality. As a first step towards that goal we describe completely the torsion growth of elliptic curves with complex multiplication (CM) over $\mathbb{Q}$ base-extended to a quadratic field. The case of base extending to cubic number fields is solved in [15]. In an ongoing project [16], we will solve the problem for number fields of low degree ($d \leq 23$).

We define $\Phi^{\rm CM}(d)$, $\Phi_{\mathbb{Q}}^{\rm CM}(d)$, $\Phi_{\mathbb{Q}}^{\rm CM}(d,G)$, $\mathcal{H}_{\mathbb{Q}}^{\rm CM}(d,G)$, $\mathcal{H}_{\mathbb{Q}}^{\rm CM}(d)$, $h_{\mathbb{Q}}^{\rm CM}(d)$, to be the sets and constants defined analogously to the ones above but restricted to elliptic curves with complex multiplication.

The set $\Phi^{\rm CM}(1)$ was determined by Olson ([30]):

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

To the best of the author's knowledge[1], the first classification of the quadratic and cubic case was was done by Clark in [5, Theorem 4]. Although it appears for the first time in print in [6], where Clark, Corn, Rice, and Stankewicz computed the sets $\Phi^{\rm CM}(d)$, for $2 \leq d \leq 13$. In particular,

$$\Phi^{\rm CM}(2) = \Phi^{\rm CM}(1) \cup \{\mathcal{C}_7\,,\mathcal{C}_{10}\,,\mathcal{C}_2\times\mathcal{C}_4\,,\mathcal{C}_2\times\mathcal{C}_6\,,\mathcal{C}_3\times\mathcal{C}_3\,\}\,.$$

Moreover, Bourdon, Clark and Stankewicz ([2]) determine $\Phi^{\rm CM}(p)$ for any prime p, and Bourdon and Pollack ([3]) generalize to $\Phi^{\rm CM}(d)$ for all odd d, showing the answer explicitly for all odd $d < 100$.

The main results of this paper are the following.

THEOREM 1.1. $\Phi_{\mathbb{Q}}^{CM}(2) = \Phi^{CM}(2) \setminus \{\mathcal{C}_7\,,\mathcal{C}_{10}\}$.

THEOREM 1.2. *Let $G \in \Phi^{CM}(1)$. The sets $\Phi_{\mathbb{Q}}^{CM}(2,G)$ and $\mathcal{H}_{\mathbb{Q}}^{CM}(2,G)$ appear in Table 1. In particular, $h_{\mathbb{Q}}^{CM}(2) = 3$.*

Finally, we give an affirmative answer to Problem 1.1 for the case of elliptic curves defined over $\mathbb{Q}$ with CM base changed to quadratic fields in terms of what we define as the CM-invariants of the curve (see §2.4 for the definition).

[1] Müller, Ströher, and Zimmer in [28]; and Fung, Müller, Pethő, Ströher, Weis, Williams, and Zimmer in [11, 31] determine all torsion subgroups of elliptic curves with algebraic integer j-invariant over quadratic and cubic fields respectively. Note that elliptic curves with CM form a subclass of elliptic curves with integral j-invariant. But they do not identify the CM case within this larger classification problem.

TABLE 1. $\Phi_{\mathbb{Q}}^{\mathrm{CM}}(2,G)$ and $\mathcal{H}_{\mathbb{Q}}^{\mathrm{CM}}(2,G)$ for $G \in \Phi^{\mathrm{CM}}(1)$.

G	$\Phi_{\mathbb{Q}}^{CM}(2,G) \setminus \{G\}$	$\mathcal{H}_{\mathbb{Q}}^{CM}(2,G)$
$\mathcal{C}_1$	$\{\mathcal{C}_3\}$	$\mathcal{C}_3$
		$\mathcal{C}_3\,,\mathcal{C}_3$
$\mathcal{C}_2$	$\{\mathcal{C}_4\,,\mathcal{C}_6\,,\mathcal{C}_2\times\mathcal{C}_2\,,\mathcal{C}_2\times\mathcal{C}_6\}$	$\mathcal{C}_2\times\mathcal{C}_2$
		$\mathcal{C}_2\times\mathcal{C}_6$
		$\mathcal{C}_2\times\mathcal{C}_2\,,\mathcal{C}_6$
		$\mathcal{C}_2\times\mathcal{C}_6\,,\mathcal{C}_6$
		$\mathcal{C}_2\times\mathcal{C}_2\,,\mathcal{C}_4\,,\mathcal{C}_4$
$\mathcal{C}_3$	$\{\mathcal{C}_3\times\mathcal{C}_3\}$	$\mathcal{C}_3\times\mathcal{C}_3$
$\mathcal{C}_4$	$\{\mathcal{C}_2\times\mathcal{C}_4\}$	$\mathcal{C}_2\times\mathcal{C}_4$
$\mathcal{C}_6$	$\{\mathcal{C}_2\times\mathcal{C}_6\}$	$\mathcal{C}_2\times\mathcal{C}_6$
$\mathcal{C}_2\times\mathcal{C}_2$	$\{\mathcal{C}_2\times\mathcal{C}_4\}$	$\mathcal{C}_2\times\mathcal{C}_4$
		$\mathcal{C}_2\times\mathcal{C}_4\,,\mathcal{C}_2\times\mathcal{C}_4$

THEOREM 1.3. *Let E be an elliptic curve defined over $\mathbb{Q}$ with CM and $G = E(\mathbb{Q})_{tors}$. Let k and $\mathfrak{cm}$ its corresponding CM-invariants. Table 2 gives an explicit description of torsion growth over quadratic fields of E depending only on the integers k and $\mathfrak{cm}$. The 4^{th} column gives a list of the form $H_1,\dots,H_n$ and the 5^{th} column gives $\sqrt{d_1},\dots,\sqrt{d_n}$ such that $E(\mathbb{Q}(\sqrt{d_i}))_{tors} \simeq H_i$, for $i = 1,\dots,n$.*

Notation: Let n denote a positive integer, we will denote by $\mathcal{C}_n = \mathbb{Z}/n\mathbb{Z}$ the cyclic group of order n. Given an elliptic curve $E : y^2 = x^3 + Ax + B$, $A, B \in K$, and a number field K we denote by $j(E)$ its j-invariant, by $\Delta(E)$ the discriminant of that short Weierstrass model, and by $E(K)_{\mathrm{tors}}$ the torsion subgroup of the Mordell-Weil group of E over K.

2. Preliminary results

In this section we introduce some basic known facts that will be used in the proofs of the above theorems.

2.1. *Twists.* Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve defined over $\mathbb{Q}$. Then any elliptic curve defined over $\mathbb{Q}$ isomorphic over $\overline{\mathbb{Q}}$ to E has a short Weierstrass model of the form:

(i)	$E^d : y^2 = x^3 + d^2Ax + d^3B$	if $j(E) \neq 0, 1728$,
(ii)	$E^d : y^2 = x^3 + dAx$	if $j(E) = 1728$,
(iii)	$E^d : y^2 = x^3 + dB$	if $j(E) = 0$,

where d is an integer in $\mathbb{Q}^*/(\mathbb{Q}^*)^{n(E)}$ and $n(E) = 2$ (resp. 4 or 6) if $j(E) \neq 0, 1728$ (resp. $j(E) = 1728$ or $j(E) = 0$) (cf. [32, X §5]). The elliptic curve

TABLE 2. Explicit description of torsion growth over quadratic fields of elliptic curves defined over $\mathbb{Q}$ with CM.

$\mathfrak{cm}$	k such that $E = E^k_{\mathfrak{cm}}$	G	$\mathcal{H}_{\mathbb{Q}}(2,E) \setminus \{G\}$	quadratics
3	1	$\mathcal{C}_6$	$\mathcal{C}_2 \times \mathcal{C}_6$	$\sqrt{-3}$
	$16, -432$	$\mathcal{C}_3$	$\mathcal{C}_3 \times \mathcal{C}_3$	$\sqrt{-3}$
	r^2 $(r \neq \pm 1, \pm 4)$		$-$	$-$
	-27	$\mathcal{C}_2$	$\mathcal{C}_2 \times \mathcal{C}_6$	$\sqrt{-3}$
	r^3 $(r \neq 1, -3)$		$\mathcal{C}_2 \times \mathcal{C}_2\,, \mathcal{C}_6$	$\sqrt{-3}, \sqrt{r}$
	$2r^3$ $(r \neq -6, 2)$	$\mathcal{C}_1$	$\mathcal{C}_3, \mathcal{C}_3$	$\sqrt{2r}, \sqrt{-6r}$
	$\neq r^2, r^3, 2r^3$		$\mathcal{C}_3$	$\sqrt{k}$
12	1	$\mathcal{C}_6$	$\mathcal{C}_2 \times \mathcal{C}_6$	$\sqrt{3}$
	3	$\mathcal{C}_2$	$\mathcal{C}_2 \times \mathcal{C}_6$	$\sqrt{3}$
	$\neq 1, 3$		$\mathcal{C}_2 \times \mathcal{C}_2,\, \mathcal{C}_6$	$\sqrt{3}, \sqrt{k}$
27	1	$\mathcal{C}_3$	$-$	$-$
	$\neq 1$	$\mathcal{C}_1$	$\mathcal{C}_3$	$\sqrt{k}$
4	-1	$\mathcal{C}_2 \times \mathcal{C}_2$	$\mathcal{C}_2 \times \mathcal{C}_4,\, \mathcal{C}_2 \times \mathcal{C}_4$	$\sqrt{-1}, \sqrt{2}$
	-4		$\mathcal{C}_2 \times \mathcal{C}_4$	$\sqrt{2}$
	$-r^2$ $(r \neq \pm 1, \pm 2)$		$-$	$-$
	4	$\mathcal{C}_4$	$\mathcal{C}_2 \times \mathcal{C}_4$	$\sqrt{-1}$
	r^2 $(r \neq \pm 2)$	$\mathcal{C}_2$	$\mathcal{C}_2 \times \mathcal{C}_2\,, \mathcal{C}_4\,, \mathcal{C}_4$	$\sqrt{-1}, \sqrt{2r}, \sqrt{-2r}$
	$\neq \pm r^2$		$\mathcal{C}_2 \times \mathcal{C}_2$	$\sqrt{-k}$
16	$1, 2$	$\mathcal{C}_4$	$\mathcal{C}_2 \times \mathcal{C}_4$	$\sqrt{2}$
	$\neq 1, 2$	$\mathcal{C}_2$	$\mathcal{C}_2 \times \mathcal{C}_2\,, \mathcal{C}_4\,, \mathcal{C}_4$	$\sqrt{2}, \sqrt{k}, \sqrt{2k}$
7	$-$	$\mathcal{C}_2$	$\mathcal{C}_2 \times \mathcal{C}_2$	$\sqrt{-7}$
28	$-$	$\mathcal{C}_2$	$\mathcal{C}_2 \times \mathcal{C}_2$	$\sqrt{7}$
8	$-$	$\mathcal{C}_2$	$\mathcal{C}_2 \times \mathcal{C}_2$	$\sqrt{2}$
11	$-$	$\mathcal{C}_1$	$-$	$-$
19	$-$	$\mathcal{C}_1$	$-$	$-$
43	$-$	$\mathcal{C}_1$	$-$	$-$
67	$-$	$\mathcal{C}_1$	$-$	$-$
163	$-$	$\mathcal{C}_1$	$-$	$-$

E^d is called the d-twist of E, and in the particular case $j(E) \neq 0, 1728$ it is called the d-quadratic twist of E.

2.2. *Division polynomials.* One of the main tools that we will use in this paper are the division polynomials of an elliptic curve (cf. [34, §3.2]). Let n be a positive integer and E be an elliptic curve, we define the primitive n-division polynomial $\Psi_n(x)$ recursively, by dividing the (classical) n-division polynomial by the primitive m-division polynomial for all proper factors m

of n. Then $\Psi_n(x)$ is characterized by the property that its roots are the x-coordinates of the points of exact order n of E. Note that in general the n-division polynomial is defined so that its roots are the x-coordinates of the points of order dividing n, that is, the points in $E[n]$.

2.3. *Quadratic twists.* Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve defined over $\mathbb{Q}$, $d \in \mathbb{Q}$ squarefree, $E^{[d]} : y^2 = x^3 + Ad^2x + Bd^3$, and $E^{(d)} : dy^2 = x^3 + Ax + B$. Note that if $j(E) \neq 0, 1728$ then $E^{[d]} = E^d$ is its d-quadratic twist, meanwhile if $j(E) = 1728$ then $E^{[d]} = E^{d^2}$; and if $j(E) = 0$ then $E^{[d]} = E^{d^3}$. We have the following isomorphisms:

$$\begin{array}{ccc} E & \longrightarrow & E^{(d)} \\ (x, y) & \mapsto & (x, y/\sqrt{d}) \end{array} \qquad \text{and} \qquad \begin{array}{ccc} E^{(d)} & \longrightarrow & E^{[d]} \\ (x, y) & \mapsto & (dx, d^2y)\,. \end{array}$$

In the special case of quadratic twists there are two interesting results that will be useful in the sequel.

1. The composition of the above two maps gives an isomorphism between E and $E^{[d]}$ such that if $P = (\alpha, \beta) \in E$ then $P' = (d\alpha, d^{3/2}\beta) \in E^{[d]}$. In particular if $P \in E[n]$ then $P' \in E^{[d]}[n]$ for any positive integer n. On the other hand, suppose that we have $P = (\alpha, \beta) \in E[n]$ with $\alpha \in K$, in particular α is a root of $\Psi_n(x)$. In order to determine if there exist an square free integer d such that $P' \in E^{[d]}(K)[n]$ we only need to check if there exists $\gamma \in K$ such that $\alpha^3 + A\alpha + B = d\gamma^2$.
2. If n is an odd integer: $E(\mathbb{Q}(\sqrt{d}))[n] \simeq E(\mathbb{Q})[n] \oplus E^{[d]}(\mathbb{Q})[n]$.

2.4. *Elliptic curves over* $\mathbb{Q}$ *with CM.* Thanks to the classical theory of complex multiplication, there are only thirteen classes (up to $\overline{\mathbb{Q}}$-isomorphism) of elliptic curves defined over $\mathbb{Q}$ with CM (cf. [33, A §3]). Each of these thirteen j-invariants corresponds to an order $R = \mathbb{Z} + \mathfrak{f}\mathcal{O}_K$ of conductor $\mathfrak{f}$ in a quadratic imaginary field $K = \mathbb{Q}(\sqrt{-D})$, where $\mathcal{O}_K$ is the ring of integer of K. The thirteen possibilities are

$$(-D, \mathfrak{f}) \in \left\{ \begin{array}{c} (-3,1), (-3,2), (-3,3), (-4,1), (-4,2), (-7,1), (-7,2) \\ (-8,1), (-11,1), (-19,1), (-43,1), (-67,1), (-163,1) \end{array} \right\}.$$

For the sake of simplicity we will denote by $\mathfrak{cm}$ the absolute value of the discriminant of the CM quadratic order R, that is $\mathfrak{cm} = D \cdot \mathfrak{f}^2$. Table 3 gives a representative elliptic curve $E_{\mathfrak{cm}}$ over $\mathbb{Q}$ for each $\mathfrak{cm}$.

Let E be an elliptic curve defined over $\mathbb{Q}$ with CM, by §2.1 we have that E is $\mathbb{Q}$-isomorphic to a curve $E^k_{\mathfrak{cm}}$ for some $\mathfrak{cm}$ as in Table 3, and k an integer in $\mathbb{Q}^*/(\mathbb{Q}^*)^{n(E)}$. Then k and $\mathfrak{cm}$ are uniquely determined by E. We call them the CM-invariants of the elliptic curve E.

3. Torsion over $\mathbb{Q}$

Let E be an elliptic curve defined over $\mathbb{Q}$ with CM. In this section we compute the torsion subgroup of E depending on its CM-invariants $(\mathfrak{cm}, k)$.

TABLE 3. Isomorphism classes of elliptic curves defined over $\mathbb{Q}$ with CM.

$\mathfrak{cm}$	$E_{\mathfrak{cm}} : y^2 = f_{\mathfrak{cm}}(x)$	$j(E_{\mathfrak{cm}})$
3	$y^2 = x^3 + 1$	0
12	$y^2 = x^3 - 15x + 22$	$2^4 \cdot 3^3 \cdot 5^3$
27	$y^2 = x^3 - 480x + 4048$	$-2^{15} \cdot 3 \cdot 5^3$
4	$y^2 = x^3 + x$	$2^6 \cdot 3^3 = 1728$
16	$y^2 = x^3 - 11x + 14$	$2^3 \cdot 3^3 \cdot 11^3$
7	$y^2 = x^3 - 2835x - 71442$	$-3^3 \cdot 5^3$
28	$y^2 = x^3 - 595x + 5586$	$3^3 \cdot 5^3 \cdot 17^3$
8	$y^2 = x^3 - 4320x + 96768$	$2^6 \cdot 5^3$
11	$y^2 = x^3 - 9504x + 365904$	-2^{15}
19	$y^2 = x^3 - 608x + 5776$	$-2^{15} \cdot 3^3$
43	$y^2 = x^3 - 13760x + 621264$	$-2^{18} \cdot 3^3 \cdot 5^3$
67	$y^2 = x^3 - 117920x + 15585808$	$-2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$
163	$y^2 = x^3 - 34790720x + 78984748304$	$-2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$

Note that this is a well-known[2] result but for the sake of completeness we include here the details of the proofs since they are going to be useful for the study of the torsion growth to quadratic fields.

Suppose that E has CM-invariants $(\mathfrak{cm}, k)$, then E is $\mathbb{Q}$-isomorphic to $E_{\mathfrak{cm}}^k$. Thanks to Olson's classification of $\Phi^{\mathrm{CM}}(1)$, in order to determine $E(\mathbb{Q})_{\mathrm{tors}}$ we only need to study if the 2-, 3- and 4-division polynomials have rational roots. Note that if the n-division polynomial of E has no rational roots, then neither does the n-division polynomial of any quadratic twist of E. In the cases where $j(E) \notin \{0, 1728\}$ there are only quadratic twists. In particular it is only necessary to study the 2-, 3- and 4-division polynomials for $E_{\mathfrak{cm}}$. In the following cases the n-division polynomial $\Psi_n(x)$ refers to the elliptic curve $E_{\mathfrak{cm}}$.

- $\mathfrak{cm} \in \{11, 19, 43, 67, 163\}$: $E(\mathbb{Q})_{\mathrm{tors}}$ is trivial since $\Psi_2(x)$ and $\Psi_3(x)$ have no rational roots.
- $\mathfrak{cm} \in \{7, 28, 8\}$: $E(\mathbb{Q})_{\mathrm{tors}} \simeq \mathcal{C}_2$ since $\Psi_2(x)$ has only one rational root and, $\Psi_3(x)$ and $\Psi_4(x)$ have no rational roots.
- $\mathfrak{cm} = 16$: $\Psi_3(x)$ has no rational roots, but $\Psi_2(x)$ has only one rational root. Let us check if there are points of order 4. $\Psi_4(x)$ has two rational roots $r_1, r_2 \in \mathbb{Q}$ and $f_{16}(r_i) = is_i^2$ for $s_1, s_2 \in \mathbb{Q}$. That is, only for $k = 1, 2$ the k-quadratic twist has points of order 4. Therefore $E_{16}^k(\mathbb{Q})_{\mathrm{tors}} \simeq \mathcal{C}_2$ for $k \neq 1, 2$ and $E_{16}^k(\mathbb{Q})_{\mathrm{tors}} \simeq \mathcal{C}_4$ for $k = 1, 2$.
- $\mathfrak{cm} = 27$: $\Psi_2(x)$ has no rational roots and $\Psi_3(x)$ has only one rational

[2] For example: the case $\mathfrak{cm} = 3$ was first computed by Fueter ([12]); the case $\mathfrak{cm} = 4$ in [30, §3].

root $r \in \mathbb{Q}$. Now, $f_{27}(r) = s^2$ for some $s \in \mathbb{Q}$. Therefore, $E^k_{27}(\mathbb{Q})_{\text{tors}} \simeq \mathcal{C}_3$ if $k = 1$ and $E^k_{27}(\mathbb{Q})_{\text{tors}}$ is trivial if $k \neq 1$.

• $\mathfrak{cm} = 12$: $\Psi_2(x)$ has only one rational root and $\Psi_4(x)$ has not rational roots. Now, $\Psi_3(x)$ has only one rational root $r \in \mathbb{Q}$ and $f_{12}(r) = s^2$ for some $s \in \mathbb{Q}$. Therefore, $E^k_{12}(\mathbb{Q})_{\text{tors}} \simeq \mathcal{C}_6$ if $k = 1$ and $E^k_{12}(\mathbb{Q})_{\text{tors}} \simeq \mathcal{C}_2$ if $k \neq 1$.

Let us study the non-quadratic twists:

• $\mathfrak{cm} = 4$. In this case the elliptic curve E is $\mathbb{Q}$-isomorphic to $E^k_4 : y^2 = x^3 + kx$ for some $k \in \mathbb{Q}^*/(\mathbb{Q}^*)^4$. The point $(0, 0) \in E^k_4(\mathbb{Q})$ is of order 2 for any k. Let us see if there are points of order 3: $\Psi_3(x) = 3x^4 + 6kx^2 - k^2$, then $z = -1/3(3 \pm 2\sqrt{3})k$ are the roots of the polynomial $\Psi_3(\sqrt{x})$, but $z \neq x^2$ for any $x, k \in \mathbb{Q}$. Therefore there are no points of order 3 for any k. Now, let us check the existence of points of order 4: $\Psi_4(x) = 2(x^2 - k)(x^4 + 6kx^2 + k^2)$. Analogously to the previous case, the factor $x^4 + 6kx^2 + k^2$ has no rational roots for any k. But the first factor $x^2 - k$ has rational roots if $k = r^2$ for some $r \in \mathbb{Q}$, in that case $x = \pm r$. Then $f_4(\pm r) = \pm 2r^3$ is a rational square if and only if $r = \pm 2$. Therefore we conclude that $E^k_4(\mathbb{Q})_{\text{tors}} \simeq \mathcal{C}_4$ if $k = 4$; $E^k_4(\mathbb{Q})_{\text{tors}} \simeq \mathcal{C}_2 \times \mathcal{C}_2$ if $k = -r^2$; and $E^k_4(\mathbb{Q})_{\text{tors}} \simeq \mathcal{C}_2$ otherwise.

• $\mathfrak{cm} = 3$. In this case the elliptic curve E is $\mathbb{Q}$-isomorphic to $E^k_3 : y^2 = x^3 + k$ for some $k \in \mathbb{Q}^*/(\mathbb{Q}^*)^6$. It has points of order 2 if and only if $k = s^3$ for some squarefree $s \in \mathbb{Q}$. In this case it is not possible to have full 2-torsion over $\mathbb{Q}$ since $x^3 + r^3 = (x - r)(x^2 + rx + r^2)$ and $x^2 + rx + r^2$ is irreducible over $\mathbb{Q}$ for any $r \in \mathbb{Q}$. Let us study if there are points of order 3. We look at the primitive 3-division polynomial $\Psi_3(x) = 3x(x^3 + 4k)$. If $x = 0$ then $f_3(0) = k$. Therefore there is a rational point of order 3 with x-coordinate 0 if and only $k = r^2$ for some $r \in \mathbb{Q}$. If $x^3 + 4k = 0$ then $k = \pm 2r^3$ for some squarefree $r \in \mathbb{Q}$ and $x = \mp 2r$. Since $f_3(\mp 2r) = \pm 6r^3$, a similar argument to the case $x = 0$ allows us to conclude $r = \mp 6$. That is $k = -432$. We have obtained that there are points of order 3 if and only if $k = r^2$ or $k = -432$. Therefore $E^k_3(\mathbb{Q})_{\text{tors}} \simeq \mathcal{C}_6$ if $k = s^3$ and $k = r^2$, that is $k = 1$; $E^k_3(\mathbb{Q})_{\text{tors}} \simeq \mathcal{C}_3$ if $k = r^2 \neq 1$ or $k = -432$; $E^k_3(\mathbb{Q})_{\text{tors}} \simeq \mathcal{C}_2$ if $k = r^3 \neq 1$; and $E^k_3(\mathbb{Q})_{\text{tors}}$ is trivial otherwise.

We have proved the following result.

Proposition 3.1. *Let E be an elliptic curve defined over $\mathbb{Q}$ with CM. Table 4 gives an explicit description of the torsion subgroup of E depending only on its CM-invariants k and $\mathfrak{cm}$.*

4. Torsion growth over quadratic fields

4.1. *Proof of Theorem 1.1.* Let $H \in \Phi^{\text{CM}}(2) \setminus \{\mathcal{C}_5, \mathcal{C}_7\}$. Table 2 shows examples of elliptic curves E defined over $\mathbb{Q}$ with CM and quadratic fields K such that $E(K)_{\text{tors}} \simeq H$. Now, by Olson's classification we know that there are no elliptic curves with CM defined over $\mathbb{Q}$ with points of order 5 (resp.

TABLE 4. Torsion of elliptic curves defined over $\mathbb{Q}$ with CM.

$\mathfrak{cm}$	k	$E^k_{\mathfrak{cm}}(\mathbb{Q})_{\text{tors}}$
3	1	$\mathcal{C}_6$
	$-432, r^2 \neq 1$	$\mathcal{C}_3$
	$r^3 \neq 1$	$\mathcal{C}_2$
	$\neq r^2, r^3, -432$	$\mathcal{C}_1$
12	1	$\mathcal{C}_6$
	$\neq 1$	$\mathcal{C}_2$
27	1	$\mathcal{C}_3$
	$\neq 1$	$\mathcal{C}_1$
4	4	$\mathcal{C}_4$
	$-r^2$	$\mathcal{C}_2 \times \mathcal{C}_2$
	$\neq 4, -r^2$	$\mathcal{C}_2$
16	$1, 2$	$\mathcal{C}_4$
	$\neq 1, 2$	$\mathcal{C}_2$

$\mathfrak{cm}$	$E^k_{\mathfrak{cm}}(\mathbb{Q})_{\text{tors}}$
7	$\mathcal{C}_2$
28	
8	
11	$\mathcal{C}_1$
19	
43	
67	
163	

7) over $\mathbb{Q}$. Finally, (2.) in §2.3 shows that there cannot be points of order 5 (resp. 7) over a quadratic field. Therefore $\mathcal{C}_{10}, \mathcal{C}_7 \notin \Phi^{\text{CM}}_{\mathbb{Q}}(2)$.

REMARK 4.1. Let K be a quadratic field, and let E be an elliptic curve defined over K with CM by a quadratic order of discriminant $-\mathfrak{cm}$ such that $E(K)_{\text{tors}} \notin \{\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3, \mathcal{C}_4, \mathcal{C}_6, \mathcal{C}_2 \times \mathcal{C}_2\}$. Bourdon, Clark and Stankewicz ([2, Theorem 1.4]) have proved that K is the quadratic field listed in Table 5, and over that field E is isomorphic to $\mathcal{E}_{\alpha,\beta} : y^2 + (1-\alpha)xy - \beta y = x^3 - \beta x^2$ where $\mathcal{E}_{0,0} : x^3 + y^3 = z^3$. In the last column we show whether the elliptic curve $\mathcal{E}_{\alpha,\beta}$ is a base change of an elliptic curve over $\mathbb{Q}$ to the quadratic field K. In the affirmative case there always appear two elliptic curves defined over $\mathbb{Q}$. These elliptic curves are isomorphic over the quadratic field K. Note that there is a typo in [2, Theorem 1.4] since the two elliptic curves in the above table with $\mathfrak{cm} = 12$ are isomorphic over $K = \mathbb{Q}(\sqrt{3})$, so there should appear only one.

4.2. *Proof of Theorems 1.2 and 1.3.* The first part of Theorem 1.2 is to determine the set $\Phi^{\text{CM}}_{\mathbb{Q}}(2, G)$. If $G \in \Phi^{\text{CM}}(1)$, $G \neq \mathcal{C}_2 \times \mathcal{C}_2$, Table 2 shows examples of elliptic curves E defined over $\mathbb{Q}$ with CM and quadratic fields K for any possible torsion structure in $\Phi_{\mathbb{Q}}(2, G) \cap \Phi^{\text{CM}}_{\mathbb{Q}}(2)$ (cf. [21, Theorem 2]). If $G = \mathcal{C}_2 \times \mathcal{C}_2$, $\Phi_{\mathbb{Q}}(2, G) \cap \Phi^{\text{CM}}_{\mathbb{Q}}(2) = \{\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_2 \times \mathcal{C}_4, \mathcal{C}_2 \times \mathcal{C}_6\}$ (cf. [21, Theorem 2]). Then to finish the first part of Theorem 1.2 we must prove that if E is an elliptic curve defined over $\mathbb{Q}$ with CM such that $E(\mathbb{Q})_{\text{tors}} \simeq \mathcal{C}_2 \times \mathcal{C}_2$ then the torsion cannot grow to $\mathcal{C}_2 \times \mathcal{C}_6$ over a quadratic field. By Proposition 3.1 (see Table 4), E should have $\mathfrak{cm} = 4$. But since there are no elliptic curves in the family E^k_4 with points of order 3 over $\mathbb{Q}$ there cannot be points of order 3 over a quadratic field (by (2.) in §2.3).

TABLE 5

K	α	β	$\mathfrak{cm}$	$E(K)_{\rm tors}$	Base Change from $\mathbb{Q}$?
$\mathbb{Q}(\sqrt{-3})$	0	0	3	$\mathcal{C}_3\times\mathcal{C}_3$	E_3^{16} and E_3^{-432}
$\mathbb{Q}(\sqrt{-1})$	$-\frac{1}{8}$	0	4	$\mathcal{C}_2\times\mathcal{C}_4$	E_4^{4} and E_4^{-1}
$\mathbb{Q}(\sqrt{2})$	$1+\frac{3}{4}\sqrt{2}$	0	4	$\mathcal{C}_2\times\mathcal{C}_4$	E_4^{-4} and E_4^{-1}
$\mathbb{Q}(\sqrt{2})$	$-\frac{1}{32}$	0	16	$\mathcal{C}_2\times\mathcal{C}_4$	E_{16}^{1} and E_{16}^{2}
$\mathbb{Q}(\sqrt{2})$	$\frac{1+\sqrt{2}}{8}$	0	8	$\mathcal{C}_2\times\mathcal{C}_4$	No
$\mathbb{Q}(\sqrt{-7})$	$\frac{-31+3\sqrt{-7}}{512}$	0	7	$\mathcal{C}_2\times\mathcal{C}_4$	No
$\mathbb{Q}(\sqrt{-7})$	$\frac{-1+3\sqrt{-7}}{32}$	0	7	$\mathcal{C}_2\times\mathcal{C}_4$	No
$\mathbb{Q}(\sqrt{-3})$	$-\frac{2}{9}$	$-\frac{1}{3}$	3	$\mathcal{C}_2\times\mathcal{C}_6$	E_3^{1} and E_3^{-27}
$\mathbb{Q}(\sqrt{3})$	$\frac{1-\sqrt{3}}{9}$	$\frac{-2+\sqrt{3}}{3}$	12	$\mathcal{C}_2\times\mathcal{C}_6$	E_{12}^{1} and E_{12}^{3}
$\mathbb{Q}(\sqrt{3})$	$\frac{4}{9}$	$\frac{1}{3}$	12	$\mathcal{C}_2\times\mathcal{C}_6$	E_{12}^{1} and E_{12}^{3}
$\mathbb{Q}(\sqrt{-3})$	$\frac{-1+\sqrt{-3}}{2}$	-1	3	$\mathcal{C}_7$	No
$\mathbb{Q}(\sqrt{-1})$	$\sqrt{-1}$	$\sqrt{-1}$	4	$\mathcal{C}_{10}$	No

The second part of Theorem 1.2 is to determine $\mathcal{H}_{\mathbb{Q}}^{\rm CM}(2,G)$ for any $G\in\Phi^{\rm CM}(1)$. Notice that this is a direct consequence of Theorem 1.3, then we will prove Theorem 1.3 first. That is, we are going to justify all the entries in Table 2 following a similar argument to the one in section §3.

For any elliptic curve E defined over $\mathbb{Q}$ with CM, Proposition 3.1 gives an explicit description of $G=E(\mathbb{Q})_{\rm tors}$ in terms of its CM-invariants. Now thanks to the classification of $\Phi_{\mathbb{Q}}^{\rm CM}(2,G)$ we know the possible torsion growth over quadratic fields. In this case we only need to study if the 2-, 3- and 4-division polynomials have linear or quadratic factors.

Remember that if E has CM-invariants $(\mathfrak{cm},k)$, then E is $\mathbb{Q}$-isomorphic to $E_{\mathfrak{cm}}^k$ and in the cases where $\mathfrak{cm}\notin\{3,4\}$ there are only quadratic twists. In particular it is only necessary to study the 2-, 3- and 4-division polynomials for $E_{\mathfrak{cm}}$. In the following cases $\Psi_n(x)$ denotes the n-division polynomial of $E_{\mathfrak{cm}}$.

• $\mathfrak{cm}\in\{11,19,43,67,163\}$: $E_{\mathfrak{cm}}^k(\mathbb{Q})_{\rm tors}\simeq\mathcal{C}_1$ and, since $\Phi_{\mathbb{Q}}^{\rm CM}(2,\mathcal{C}_1)=\{\mathcal{C}_1,\mathcal{C}_3\}$, there is no torsion growth over quadratic fields.

• $\mathfrak{cm}\in\{7,28,8\}$: $E_{\mathfrak{cm}}^k(\mathbb{Q})_{\rm tors}\simeq\mathcal{C}_2$ and $\Phi_{\mathbb{Q}}^{\rm CM}(2,\mathcal{C}_2)=\{\mathcal{C}_2,\mathcal{C}_4,\mathcal{C}_6,\mathcal{C}_2\times\mathcal{C}_2,\mathcal{C}_2\times\mathcal{C}_6\}$. Similarly to the previous case there cannot be points of order 3 over quadratic fields, that is, neither torsion growth to $\mathcal{C}_6$ nor $\mathcal{C}_2\times\mathcal{C}_6$. Now since the torsion over $\mathbb{Q}$ is $\mathcal{C}_2$ we have that the full 2-torsion is defined over $\mathbb{Q}(\sqrt{\Delta(E_{\mathfrak{cm}})})$. In our cases we have $\mathbb{Q}(\sqrt{\Delta(E_7)})=\mathbb{Q}(\sqrt{-7})$, $\mathbb{Q}(\sqrt{\Delta(E_{28})})=\mathbb{Q}(\sqrt{7})$, and $\mathbb{Q}(\sqrt{\Delta(E_8)})=\mathbb{Q}(\sqrt{2})$. Finally let us check if there is torsion growth to $\mathcal{C}_4$.

- $\mathfrak{cm} = 7$: $\Psi_4(x) = 2(x^2-126x-5103)(x^2+567)(x^2+126x+6237)$. The second and third quadratic irreducible factors have squarefree part of the discriminant equal to -7. Then a possible point of order 4 should be defined over the field of definition of the full 2-torsion. But this is impossible since $\mathcal{C}_2 \times \mathcal{C}_4$ is not a subgroup of a group in $\Phi_{\mathbb{Q}}^{\mathrm{CM}}(2, \mathcal{C}_2)$. Now, $\alpha = 63+36\sqrt{7}$ is a root of the first quadratic factor of $\Psi_4(x)$. We have $f_7(\alpha) = \sqrt{7}u(2^2 3^3\sqrt{7})^2$, where $u = 8+3\sqrt{7}$ is a fundamental unit of the quadratic field $\mathbb{Q}(\sqrt{7})$. Therefore $f_7(\alpha) \neq d\beta^2$ for any $d \in \mathbb{Q}$ and $\beta \in \mathbb{Q}(\sqrt{7})$. This proves that there are no points of order 4 over any quadratic field.
- $\mathfrak{cm} = 28$: $\Psi_4(x)$ has only one irreducible factor of degree ≤ 2. One of its roots is $\alpha = 14+\sqrt{-7}$ and we have $f_{28}(\alpha) = -7\sqrt{-7}(1+\sqrt{-7})^4/4$. Similarly to the previous case: $f_{28}(\alpha) \neq d\beta^2$ for any $d \in \mathbb{Q}$ and $\beta \in \mathbb{Q}(\sqrt{-7})$ and there are no points of order 4 over quadratic fields.
- $\mathfrak{cm} = 8$: There is only one irreducible factor of $\Psi_4(x)$ of degree ≤ 2. In this case its roots are defined over $\mathbb{Q}(\sqrt{2})$. Since $\mathbb{Q}(\sqrt{\Delta(E_8)}) = \mathbb{Q}(\sqrt{2})$ we obtain that there are no points of order 4.

We have proved that there is only torsion growth to $\mathcal{C}_2 \times \mathcal{C}_2$ over $\mathbb{Q}(\sqrt{\Delta(E_{\mathfrak{cm}})})$.

• $\mathfrak{cm} = 16$: If $k = 1, 2$ then $E_{16}^k(\mathbb{Q})_{\mathrm{tors}} \simeq \mathcal{C}_4$. For these cases the torsion only grows to $\mathcal{C}_2 \times \mathcal{C}_4$ over $\mathbb{Q}(\sqrt{\Delta(E_{16})}) = \mathbb{Q}(\sqrt{2})$ since $\Phi_{\mathbb{Q}}^{\mathrm{CM}}(2, \mathcal{C}_4) = \{\mathcal{C}_4, \mathcal{C}_2 \times \mathcal{C}_4\}$. Now if $k \neq 1, 2$, then $E_{16}^k(\mathbb{Q})_{\mathrm{tors}} \simeq \mathcal{C}_2$. By (2.) at section §2.3) there are not points of order 3 over quadratic fields since there are not points of order 3 over $\mathbb{Q}$ for any quadratic twist of E_{16}. Finally, let us study if there are points of order 4 over some quadratic field. The factorization of the 4-division polynomial in irreducible factors is: $\Psi_4(x) = 2(x-1)(x-3)(x^4+4x^3-42x^2+100x-79)$. Now $f_{16}(1) = 4$ and $f_{16}(3) = 8$. Therefore there are points of order 4 over the quadratic fields $\mathbb{Q}(\sqrt{k})$ and $\mathbb{Q}(\sqrt{2k})$. Since $k \neq 1, 2$, the torsion subgroup over those quadratic fields is isomorphic to $\mathcal{C}_4$.

• $\mathfrak{cm} = 27$: If $k = 1$, then $E_{27}^1(\mathbb{Q})_{\mathrm{tors}} \simeq \mathcal{C}_3$. Since $\Phi_{\mathbb{Q}}^{\mathrm{CM}}(2, \mathcal{C}_3) = \{\mathcal{C}_3, \mathcal{C}_3 \times \mathcal{C}_3\}$ the torsion can only grow to $\mathcal{C}_3 \times \mathcal{C}_3$. But this can only happen over $\mathbb{Q}(\sqrt{-3})$. We compute that the torsion subgroup over $\mathbb{Q}(\sqrt{-3})$ is $\mathcal{C}_3$ too. Then there is no torsion growth for $k = 1$. Now suppose $k \neq 1$, then $E_{27}^k(\mathbb{Q})_{\mathrm{tors}} \simeq \mathcal{C}_1$ and $\Phi_{\mathbb{Q}}^{\mathrm{CM}}(2, \mathcal{C}_1) = \{\mathcal{C}_1, \mathcal{C}_3\}$. By (2.) in §2.3 with $n = 3$ we have that the torsion growth to $\mathcal{C}_3$ over a quadratic field only over $\mathbb{Q}(\sqrt{k})$.

• $\mathfrak{cm} = 12$: If $k = 1$, then $E_{12}^1(\mathbb{Q})_{\mathrm{tors}} \simeq \mathcal{C}_6$ and $\Phi_{\mathbb{Q}}^{\mathrm{CM}}(2, \mathcal{C}_6) = \{\mathcal{C}_6, \mathcal{C}_2 \times \mathcal{C}_6\}$. Thus the torsion only grows to $\mathcal{C}_2 \times \mathcal{C}_6$ over $\mathbb{Q}(\sqrt{\Delta(E_{12}^1)}) = \mathbb{Q}(\sqrt{3})$. Now if $k \neq 1$, then $E_{12}^k(\mathbb{Q})_{\mathrm{tors}} \simeq \mathcal{C}_2$ and $\Phi_{\mathbb{Q}}^{\mathrm{CM}}(2, \mathcal{C}_2) = \{\mathcal{C}_2, \mathcal{C}_4, \mathcal{C}_6, \mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_2 \times \mathcal{C}_6\}$. We have that $\mathcal{C}_2 \times \mathcal{C}_2$ is isomorphic to a subgroup of the torsion subgroup over $\mathbb{Q}(\sqrt{\Delta(E_{12}^1)}) = \mathbb{Q}(\sqrt{3})$. A similar argument to the case $\mathfrak{cm} = 27$ allows us to determine that there are points of order 3 over $\mathbb{Q}(\sqrt{k})$. Therefore if $k = 3$, the torsion grows only to $\mathcal{C}_2 \times \mathcal{C}_6$ over $\mathbb{Q}(\sqrt{3})$. Finally, if $k \neq 1, 3$ we have torsion growth to $\mathcal{C}_2 \times \mathcal{C}_2$ over $\mathbb{Q}(\sqrt{3})$, and $\mathcal{C}_6$ over $\mathbb{Q}(\sqrt{k})$. It remains to check that there are no points of order 4 over quadratic fields. $\Psi_4(x)$ has only one irreducible factor of degree ≤ 2. One of its roots is $\alpha = 2 + \sqrt{-3}$ and we have $f_{12}(\alpha) = -\sqrt{-3}(3 - \sqrt{-3})^2$. Therefore: $f_{12}(\alpha) \neq d\beta^2$ for any $d \in \mathbb{Q}$ and $\beta \in \mathbb{Q}(\sqrt{-3})$. This proves that there are no points of order 4 over any quadratic fields.

Finally we deal with the non-quadratic twists.

- $\mathfrak{cm} = 4$. We split the proof depending on the torsion over $\mathbb{Q}$:
- $E_4^k(\mathbb{Q})_{\text{tors}} \simeq \mathcal{C}_2 \times \mathcal{C}_2$ if $k = -r^2$. We have $\Phi_{\mathbb{Q}}^{\text{CM}}(2, \mathcal{C}_2 \times \mathcal{C}_2) = \{\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_2 \times \mathcal{C}_4\}$. Let us study if there are points of order 4 over a quadratic field. Note that, since $E_4^{-r^2}$ is the r-quadratic twist of E_4^{-1}, it is enough to study the factorization of the 4-division polynomial $\Psi_4(x)$ of E_4^{-1}. The polynomial $\Psi_4(x)$ has the roots $\pm i$, $\pm 1 \pm \sqrt{2}$ and evaluating the polynomial $g(x) = x^3 - x$ for these values we obtain:

  $$g(i) = (i-1)^2 \,, \quad g(1+\sqrt{2}) = (2+\sqrt{2})^2 \,, \quad g(-1+\sqrt{2}) - (2-\sqrt{2})^2.$$

  Therefore there are points of order 4 over a quadratic fields if and only if $r = \pm 1$ over $\mathbb{Q}(i), \mathbb{Q}(\sqrt{2})$ or $r = \pm 2$ over $\mathbb{Q}(\sqrt{2})$. That is, over those quadratic fields and the corresponding values of r we obtain that the torsion subgroup is isomorphic to $\mathcal{C}_2 \times \mathcal{C}_4$. For the rest of the values of r there is no torsion growth over any quadratic field for the elliptic curve $E_4^{-r^2}$.
- $E_4^k(\mathbb{Q})_{\text{tors}} \simeq \mathcal{C}_4$ if $k = 4$. There is only one possibility to grow over a quadratic field: $\mathcal{C}_2 \times \mathcal{C}_4$ over $\mathbb{Q}(i)$, since $\Delta(E_4^4) = -2^{12}$.
- $E_4^k(\mathbb{Q})_{\text{tors}} \simeq \mathcal{C}_2$ if $k \neq 4, -r^2$. By (2.) in §2.3 there are no points of order 3 over quadratic fields since there are no points of order 3 over $\mathbb{Q}$ for any value of k. First suppose $k = r^2$. Then $E_4^{r^2}$ is the r-quadratic twist of E_4. Let us study if there are points of order 4 using the 4-division polynomial of E_4: $\Psi_4(x) = 2(x^2-1)(x^4+6x^2+1)$. Since $f_4(\pm 1) = \pm 2$ there are points of order 4 over a quadratic field only in the case $\mathbb{Q}(\sqrt{\pm 2r})$. The last possibility for torsion growth is $\mathcal{C}_2 \times \mathcal{C}_2$ over $\mathbb{Q}(\sqrt{-1})$. This finishes the case $k = r^2$. Finally we deal with the general case: $k \neq r^2$. We have $\mathcal{C}_2 \times \mathcal{C}_2$ is isomorphic to a subgroup of the torsion subgroup over $\mathbb{Q}(\sqrt{-k})$ since $\Delta(E_4^k) = -k(8k)^2$. To finish the proof of this case we are going to prove that there are no points of order 4 over quadratic fields. We have $\Psi_4(x) = 2(x^2-k)(x^4+6kx^2+k^2)$. Let us denote by $g(x)$ the second factor, then $z = (-3 \pm 2\sqrt{2})k$ are the roots of the polynomial $g(\sqrt{x})$, but $z \neq x^2$ for any $x \in \mathbb{Q}(\sqrt{2})$ and $k \in \mathbb{Q}$. The first factor have the roots $x = \pm\sqrt{k}$, but $(\pm\sqrt{k})^3 + k(\pm\sqrt{k}) = \pm 2\sqrt{k}^3$ is never an square over $\mathbb{Q}(\sqrt{k})$. We conclude that there is only torsion growth over quadratic fields to $\mathcal{C}_2 \times \mathcal{C}_2$ over $\mathbb{Q}(\sqrt{-k})$.

• $\mathtt{cm} = 3$. Note that this case has been dealt by Dey[3] ([9]) with a slightly different approach. We split the proof depending on the torsion over $\mathbb{Q}$:

- $E_3^k(\mathbb{Q})_{\text{tors}} \simeq \mathcal{C}_6$ if $k = 1$. The torsion only grows to $\mathcal{C}_2 \times \mathcal{C}_6$ over the quadratic field $\mathbb{Q}(\sqrt{\Delta(E_3^1)}) = \mathbb{Q}(\sqrt{-3})$.
- $E_3^k(\mathbb{Q})_{\text{tors}} \simeq \mathcal{C}_3$ if $k = -432$ or $k = r^2 \neq 1$. Here the torsion can only grow to $\mathcal{C}_3 \times \mathcal{C}_3$ over $\mathbb{Q}(\sqrt{-3})$. We check that $E_3^{-432}(\mathbb{Q}(\sqrt{-3}))_{\text{tors}} \simeq \mathcal{C}_3 \times \mathcal{C}_3$. Now suppose $k = r^2 \neq 1$. We must have all the roots of $\Psi_3(x) = 3x(x^3 + 4r^2)$ defined over $\mathbb{Q}(\sqrt{-3})$. Therefore $r = 4s^3$, but since $k \in \mathbb{Q}^*/(\mathbb{Q}^*)^6$ the unique possibility is $r = 4$, i.e. $k = 16$. We check that $E_3^{16}(\mathbb{Q}(\sqrt{-3}))_{\text{tors}} \simeq \mathcal{C}_3 \times \mathcal{C}_3$. For the rest of the values the torsion does not grow over quadratic fields.
- $E_3^k(\mathbb{Q})_{\text{tors}} \simeq \mathcal{C}_2$ if $k = r^3 \neq 1$. Note that in this case E_3^k is the r-quadratic twist of E_3, therefore it is enough to study the n-division polynomials $\Psi_n(x)$ of E_3. Since the torsion over $\mathbb{Q}$ is isomorphic to $\mathcal{C}_2$, we could only have torsion growth $\mathcal{C}_4, \mathcal{C}_6, \mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_2 \times \mathcal{C}_6$. Let us check if there are points of order 4 over quadratic fields: The unique factor of $\Psi_4(x)$ of degree ≤ 2 is $g(x) = x^2 + 2x - 2$. We have that $\alpha = \sqrt{3} - 1$ is a root of $g(x)$. Then $f_3(\alpha) = 3\sqrt{3}u$, where $u = 2 - \sqrt{3}$ is a fundamental unit of the quadratic field $\mathbb{Q}(\sqrt{3})$. Therefore $f_3(\alpha) \neq r\beta^2$ for any $r \in \mathbb{Q}$ and $\beta \in \mathbb{Q}(\sqrt{3})$. In conclusion, there are no points of order 4 over quadratic fields. Now we study if there are points of order 3. We have $\Psi_3(x) = 4x(x^3 + 4)$ and $f_3(0) = 1$. Therefore there are points of order 3 over $\mathbb{Q}(\sqrt{r})$. Finally we have full 2-torsion over $\mathbb{Q}(\Delta(E_3)) = \mathbb{Q}(\sqrt{-3})$. We conclude that there are torsion growth to $\mathcal{C}_2 \times \mathcal{C}_2$ and $\mathcal{C}_6$ if $k \neq -3$; and $\mathcal{C}_2 \times \mathcal{C}_6$ if $r = -3$.
- $E_3^k(\mathbb{Q})_{\text{tors}} \simeq \mathcal{C}_1$ if $k \neq r^2, r^3, -432$. We need to check only if there are points of order 3 over quadratic fields. We have $\Psi_3(x) = 3x(x^3 + 4k)$. If $x = 0$ then $y^2 = k$. Thus, the torsion grows to $\mathcal{C}_3$ over $\mathbb{Q}(\sqrt{k})$. The second factor $x^3 + 4k$ has roots over a quadratic field if and only if $k = 2r^3$. In that case the root is $\alpha = -2r$ and we have $\alpha^3 + k = -6r^3$ is a square over a quadratic field only over $\mathbb{Q}(\sqrt{-6r})$. Since $k = 2r^3$ we must have $r \neq 2, -6$.

Remark 4.2. All the computations were done using `Magma` ([1]) and the source code is available at the author's webpage [14].

Acknowledgements.

The author would like to thank Harris B. Daniels, who read the earlier versions of this paper carefully. Finally, the author thanks the anonymous referees for their useful comments and suggestions.

---

[3]Note that there is a typo in Theorem 1(3) in [9] since it is necessary to add the case $c = -27$ and $d \neq -3$ (in Dey's notation).

References

[1] W. Bosma, J. Cannon, C. Fieker, and A. Steel (eds.), Handbook of Magma functions, Edition 2.23, `http://magma.maths.usyd.edu.au/magma`, 2019.

[2] A. Bourdon, P. L. Clark, amd J. Stankewicz, *Torsion points on CM elliptic curves over real number fields*, Trans. Amer. Math. Soc. **369** (2017), 8457–8496.

[3] A. Bourdon and P. Pollack, *Torsion subgroups of CM elliptic curves over odd degree number fields*, Int. Math. Res. Not. IMRN **2017** (2017), 4923–4961.

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

[5] P. L. Clark, *Bounds for torsion on abelian varieties with integral moduli*, `https://arxiv.org/abs/math/0407264v2`.

[6] P. L. Clark, P. Corn, A. Rice and J. Stankewicz, *Computation on elliptic curves with complex multiplication*, LMS J. Comput. Math. **17** (2014), 509–535.

[7] H. B. Daniels and E. González-Jiménez, *On the torsion of rational elliptic curves over sextic fields*, Math. Comp. **89** (2020), 411–435.

[8] M. Derickx, A. Etropolski, M. van Hoeij, J. Morrow and D. Zureick-Brown, *Sporadic cubic torsion*, to appear in Algebra Number Theory.

[9] P. K. Dey, *Torsion groups of a family of elliptic curves over number fields*, Czechoslovak Math. J. **69(144)** (2019), 161–171.

[10] L. Dieulefait, E. González-Jiménez and J. Jiménez Urroz, *On fields of definition of torsion points of elliptic curves with complex multiplication* Proc. Amer. Math. Soc. **139** (2011), 1961–1969.

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

[12] R. Fueter, *Ueber kubische diophantische Gleichungen*, Comment. Math. Helv. **2** (1930), 69–89.

[13] E. González-Jiménez, *Complete classification of the torsion structures of rational elliptic curves over quintic number fields*, J. Algebra **478** (2017), 484–505.

[14] E. González-Jiménez, Magma scripts and electronic transcript of computations for the paper *"Explicit characterization of the torsion growth of rational elliptic curves with complex multiplication over quadratic fields"*, `http://matematicas.uam.es/~enrique.gonzalez.jimenez`

[15] E. González-Jiménez, *Torsion growth over cubic fields of rational elliptic curves with complex multiplication*, Publ. Math. Debrecen **97** (2020), 63–76.

[16] E. González-Jiménez, *Torsion of rational elliptic curves with complex multiplication over number fields of low degree*, in preparation.

[17] E. González-Jiménez and Á. Lozano-Robledo, *On the torsion of rational elliptic curves over quartic fields*, Math. Comp. **87** (2018), 1457–1478.

[18] E. González-Jiménez and F. Najman, *Growth of torsion groups of elliptic curves upon base change*, Math. Comp. **89** (2020), 1457–1485.

[19] E. González-Jiménez and F. Najman, *An algorithm for determining torsion growth of elliptic curves*, to appear in Exp. Math.

[20] E. González-Jiménez, F. Najman and J.M. Tornero, *Torsion of rational elliptic curves over cubic fields*, Rocky Mountain J. Math. **46** (2016), 1899–1917.

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

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

[23] T. Gužvić, *Torsion growth of rational elliptic curves in sextic number fields*, J. Number Theory **220** (2021), 330–345.

[24] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. **109** (1992), 221–229.

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

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

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

[28] H. Müller, H. Ströher and H. Zimmer, *Torsion groups of elliptic curves with integral j-invariant over quadratic fields*, J. Reine Angew. Math. **397** (1989), 100–161.

[29] F. Najman, *Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$*, Math. Res. Lett. **23** (2016), 245–272.

[30] L. Olson, *Points of finite order on elliptic curves with complex multiplication*, Manuscripta Math. **14** (1974), 195–205.

[31] A. Pethő, T. Weis and H. Zimmer. *Torsion groups of elliptic curves with integral j-invariant over general cubic number fields*, Internat. J. Algebra Comput. **7** (1997) 353–413.

[32] J-H. Silverman, The arithmetic of elliptic curves, Springer-Verlag, New York, 2009.

[33] J-H. Silverman, Advanced topics in the arithmetic of elliptic curves, Springer-Verlag, New York, 1994.

[34] L. C. Washington, Elliptic curves. Number theory and cryptography, Chapman & Hall, Boca Ratón, 2008.

E. González–Jiménez
Departamento de Matemáticas
Universidad Autónoma de Madrid
Madrid
Spain
E-mail: enrique.gonzalez.jimenez@uam.es
URL: http://matematicas.uam.es/~enrique.gonzalez.jimenez

Received: 10.2.2020.
Revised: 14.1.2021.