Publ. Math. Debrecen
97/1-2 (2020), 63–76
DOI: 10.5486/PMD.2020.8697

Torsion growth over cubic fields of rational elliptic curves with complex multiplication

By ENRIQUE GONZÁLEZ-JIMÉNEZ (Madrid)

Abstract. This article is a contribution to the project of classifying the torsion growth of elliptic curves upon base-change. In this article, we treat the case of elliptic curves defined over the rationals with complex multiplication. For this particular case, we give a description of the possible torsion growth over cubic fields, and a completely explicit description of this growth in terms of some invariants attached to a given elliptic curve.

1. Introduction

The arithmetic of elliptic curves is one of the most fascinating areas of arithmetic geometry. Let E be an elliptic curve defined over a number field K, then the Mordell–Weil Theorem asserts that the set of K-rational points on E, denoted by $E(K)$, forms a finitely generated abelian group. The subgroup of points of finite order, denoted by $E(K)_{\mathrm{tors}}$, is called the torsion subgroup, and it is well known that is isomorphic to $\mathcal{C}_n \times \mathcal{C}_m$ for some positive integers n, m, where $\mathcal{C}_n = \mathbb{Z}/n\mathbb{Z}$ denotes the cyclic group of order n. Over the past several years, many people have been actively studying torsion subgroups of elliptic curves. Thanks to Merel [25], it is known that given a positive integer d, the set $\Phi(d)$ of possible groups (up to isomorphism) that can appear as the torsion subgroup $E(K)_{\mathrm{tors}}$, where K runs through all number fields K of degree d and E runs through all

Mathematics Subject Classification: Primary: 11G05; Secondary: 11G15.
Key words and phrases: elliptic curves, complex multiplication, torsion subgroup, rationals, cubic fields.
The author was partially supported by the grant PGC2018-095392-B-I00 (MCIU/AEI/FEDER, UE).

elliptic curves over K, is finite. Only the cases $d = 1$ and $d = 2$ are known (by [24]; and [22]–[23], respectively). A few years ago, Derickx, Etropolski, van Hoeij, Morrow and Zureick-Brown announced the solution of the case $d = 3$, but the results are still in preparation [8]. For $d > 3$, the problem remains open.

This paper focuses on a particular approach concerning torsion growth: we are interested in studying how the torsion subgroup of an elliptic curve defined over $\mathbb{Q}$ changes when we consider the elliptic curve over a number field of degree d. We denote the set of possible groups, up to isomorphism, that can appear as the torsion subgroup over a number field of degree d, of an elliptic curve defined over $\mathbb{Q}$ (resp. such that $E(\mathbb{Q})_{\rm tors} \simeq G$) by $\Phi_{\mathbb{Q}}(d)$ (resp. $\Phi_{\mathbb{Q}}(d, G)$, where $G \in \Phi(1)$ is fixed). Thanks to Merel's theorem on the boundedness of the torsion of elliptic curves, we know that for a given integer d, the set $\Phi_{\mathbb{Q}}(d)$ is finite.

Note 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. We say that the torsion growth over K is primitive if $E(K')_{\rm tors} \subsetneq E(K)_{\rm tors}$ for any subfield $K' \subsetneq K$.

Given an elliptic curve E defined over $\mathbb{Q}$ and a positive integer d, there is an obvious algorithm[1] that computes all the pairs (K, H) (up to isomorphism), where K is a number field of degree dividing d, E has primitive torsion growth over K, and $E(K)_{\rm tors} \simeq H$. We denote the list formed by the groups H in the above computation by $\mathcal{H}_{\mathbb{Q}}(d, E)$. Note that we are allowing the possibility of two (or more) of the torsion subgroups H being isomorphic if the corresponding number fields K are not isomorphic. Furthermore, the set $\mathcal{H}_{\mathbb{Q}}(d, E)$ is finite. We call the set $\mathcal{H}_{\mathbb{Q}}(d, E)$ the set of torsion configurations of degree d of the elliptic curve $E/\mathbb{Q}$. We let $\mathcal{H}_{\mathbb{Q}}(d)$ (resp. $\mathcal{H}_{\mathbb{Q}}(d, G)$, where $G \in \Phi(1)$ is fixed) denote the set of $\mathcal{H}_{\mathbb{Q}}(d, E)$ as E runs over all elliptic curves defined over $\mathbb{Q}$ (resp. such that $E(\mathbb{Q})_{\rm tors} \simeq G$). Let $h_{\mathbb{Q}}(d)$ denote the maximum cardinality of S when $S \in \mathcal{H}_{\mathbb{Q}}(d)$. Then $h_{\mathbb{Q}}(d)$ is the maximum number of field extensions of degree dividing d where there is primitive torsion growth.

[1]By Merel's theorem, there exists an effective bound $B(d)$ such that $\#E(K)_{\rm tors} \leq B(d)$. So to determine the number fields of degree d' dividing d where torsion grows, one checks whether there are any irreducible factor of degree d' of the p^n-division polynomial of E where $p^n \leq B_d$. We point out here that in practice this algorithm would not be very useful. For this reason, we have developed a fast algorithm usable in practice [17].

The sets $\Phi_{\mathbb{Q}}(d)$, $\Phi_{\mathbb{Q}}(d,G)$ and $\mathcal{H}_{\mathbb{Q}}(d,G)$, for any $G \in \Phi(1)$, have been completely determined for $d = 2,3,5,7$ and for any positive integer d whose prime divisors are greater than 7 (cf. [27], [19], [20], [18], [11] and [16]). The set $\Phi_{\mathbb{Q}}(4)$ is also known (see [4] and [16]), and the set $\Phi_{\mathbb{Q}}(6)$ has been studied in [7] and [21]. The other sets have been treated for $d = 4$ in [15], and $d = 6$ in [7].

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

The set $\Phi^{\mathrm{CM}}(1)$ was determined by Olson [28]:

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

To the best of the author's knowledge[2], the first to classify the quadratic and cubic case was Clark [5, Theorem 4], although this result appears in print for the first time in [6], where Clark, Corn, Rice and Stankewicz computed the sets $\Phi^{\mathrm{CM}}(d)$, for $2 \le d \le 13$. In particular, they show that

$$\Phi^{\mathrm{CM}}(3) = \Phi^{\mathrm{CM}}(1) \cup \{\,\mathcal{C}_9\,,\,\mathcal{C}_{14}\,\}\,.$$

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

In the present paper, our main results correspond to the study of torsion subgroups of elliptic curves with complex multiplication defined over $\mathbb{Q}$ under base change to cubic fields:

Theorem 1. $\Phi_{\mathbb{Q}}^{\mathrm{CM}}(3) = \Phi^{\mathrm{CM}}(3)$.

Theorem 2. *Let be* $G \in \Phi^{\mathrm{CM}}(1)$.

- *If* $G \in \{\mathcal{C}_4,\mathcal{C}_6,\mathcal{C}_2\times\mathcal{C}_2\}$, *then* $\Phi_{\mathbb{Q}}^{\mathrm{CM}}(3,G)=\{G\}$. *In particular,* $\mathcal{H}_{\mathbb{Q}}^{\mathrm{CM}}(3,G)=\emptyset$.
- *If* $G \in \{\mathcal{C}_1,\mathcal{C}_2,\mathcal{C}_3\}$, *then the sets* $\Phi_{\mathbb{Q}}^{\mathrm{CM}}(3,G)$ *and* $\mathcal{H}_{\mathbb{Q}}^{\mathrm{CM}}(3,G)$ *are the following:*

[2] Müller, Ströher and Zimmer in [26]; and Fung, Müller, Pethő, Ströher, Weis, Williams and Zimmer in [10] and [29] 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.

G	$\Phi_{\mathbb{Q}}^{\mathrm{CM}}(3,G)\setminus\{G\}$	$\mathcal{H}_{\mathbb{Q}}^{\mathrm{CM}}(3,G)$
$\mathcal{C}_1$	$\{\mathcal{C}_2,\mathcal{C}_3,\mathcal{C}_6\}$	$\mathcal{C}_2$
		$\mathcal{C}_6$
		$\mathcal{C}_2,\mathcal{C}_3$
$\mathcal{C}_2$	$\{\mathcal{C}_6,\mathcal{C}_{14}\}$	$\mathcal{C}_6$
		$\mathcal{C}_{14}$
$\mathcal{C}_3$	$\{\mathcal{C}_6,\mathcal{C}_9\}$	$\mathcal{C}_6$
		$\mathcal{C}_6,\mathcal{C}_9$

In particular, $h_{\mathbb{Q}}^{\mathrm{CM}}(3)=2$.

Remark 3. Theorem 2 shows that there is no torsion growth to $\mathcal{C}_4$ or $\mathcal{C}_2\times\mathcal{C}_2$ over cubic fields.

Our aim in this paper is to go further and gather more detailed information about torsion growth in these cases. More precisely, once we have given a description of the possible torsion growth over cubic fields, we give a completely explicit description of this growth in terms of invariants attached to the elliptic curve in question. The case of quadratic growth is solved in [13]. In an ongoing paper [14], we will solve the problem for number fields of low degree.

Theorem 4. *Table 1 gives an explicit description of torsion growth over cubic fields of any elliptic curve defined over $\mathbb{Q}$ with CM depending only in its corresponding CM-invariants (see §2.4 for the definition).*

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

2. Proof of the Theorems

2.1. Preliminaries. Let E be an elliptic curve, and n a positive integer. Denote by $E[n]$ the set of points on E of order dividing n. The x-coordinates of the points on $E[n]$ correspond to the roots of the n-division polynomial $\Psi_n(x)$ of E (cf. [31, §3.2]). By abuse of notation, in this paper we use $\Psi_n(x)$ to denote the primitive n-division polynomial of E, that is, the classical n-division polynomial divided by the m-division polynomials of E for proper factors m of n. Then $\Psi_n(x)$ is

$\mathfrak{cm}$	k such that $E = E^k_{\mathfrak{cm}}$	$G \simeq E(\mathbb{Q})_{\rm tors}$	$\mathcal{H}_{\mathbb{Q}}(E,3)$	cubics $\mathbb{Q}(\alpha)$
	1	$\mathcal{C}_6$	$-$	$-$
	16		$\mathcal{C}_6$, $\mathcal{C}_9$	$\sqrt[3]{2},\ \alpha^3-3\alpha-1=0$
	-432	$\mathcal{C}_3$	$\mathcal{C}_6$	$\sqrt[3]{2}$
	r^2 $(r\neq \pm 1,\pm 4)$		$\mathcal{C}_6$	$\sqrt[3]{k}$
3	-27	$\mathcal{C}_2$	$\mathcal{C}_6$	$\sqrt[3]{2}$
	r^3 $(r\neq 1,-3)$		$-$	$-$
	-108		$\mathcal{C}_6$	$\sqrt[3]{2}$
	$-3r^2$ $(r\neq \pm 6)$	$\mathcal{C}_1$	$\mathcal{C}_2$, $\mathcal{C}_3$	$\sqrt[3]{3r^2},\ \sqrt[3]{12r^2}$
	$\neq r^2, r^3, -3r^2$		$\mathcal{C}_2$	$\sqrt[3]{k}$
	1	$\mathcal{C}_6$	$-$	$-$
12	-3	$\mathcal{C}_2$	$\mathcal{C}_6$	$\sqrt[3]{2}$
	$\neq 1,-3$		$-$	$-$
	1	$\mathcal{C}_3$	$\mathcal{C}_6$, $\mathcal{C}_9$	$\sqrt[3]{2},\ \alpha^3-3\alpha-1=0$
27	-3	$\mathcal{C}_1$	$\mathcal{C}_2$, $\mathcal{C}_3$	$\sqrt[3]{2},\ \sqrt[3]{3}$
	$\neq 1,-3$		$\mathcal{C}_2$	$\sqrt[3]{2}$
	4	$\mathcal{C}_4$	$-$	$-$
4	$-r^2$	$\mathcal{C}_2\times\mathcal{C}_2$	$-$	$-$
	$\neq 4, -r^2$	$\mathcal{C}_2$	$-$	$-$
16	$1,2$	$\mathcal{C}_4$	$-$	$-$
	$\neq 1,2$	$\mathcal{C}_2$	$-$	$-$
7	-7	$\mathcal{C}_2$	$\mathcal{C}_{14}$	$\alpha^3+\alpha^2-2\alpha-1=0$
	$\neq -7$		$-$	$-$
28	7	$\mathcal{C}_2$	$\mathcal{C}_{14}$	$\alpha^3+\alpha^2-2\alpha-1=0$
	$\neq 7$		$-$	$-$
8	$-$	$\mathcal{C}_2$	$-$	$-$
11	$-$	$\mathcal{C}_1$	$\mathcal{C}_2$	$\alpha^3-\alpha^2+\alpha+1=0$
19	$-$	$\mathcal{C}_1$	$\mathcal{C}_2$	$\alpha^3-\alpha^2+3\alpha-1=0$
43	$-$	$\mathcal{C}_1$	$\mathcal{C}_2$	$\alpha^3-\alpha^2-\alpha+3=0$
67	$-$	$\mathcal{C}_1$	$\mathcal{C}_2$	$\alpha^3-\alpha^2-3\alpha+5=0$
163	$-$	$\mathcal{C}_1$	$\mathcal{C}_2$	$\alpha^3-8\alpha-10=0$

Table 1. Explicit description of torsion growth over cubic fields of elliptic curves defined over $\mathbb{Q}$ with complex multiplication.

characterized by the property that its roots are the x-coordinates of the points of exact order n of E. In particular, if $E(\mathbb{Q})$ has no points of order n, then a necessary condition to have points of order n over a cubic field is that $\Psi_n(x)$ has an irreducible factor of degree 3.

Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve defined over $\mathbb{Q}$, and $d \in \mathbb{Q}$ square-free. The d-quadratic twist of E is defined by $E^d : y^2 = x^3 + Ad^2x + Bd^3$. Attached to E^d, we have the $\mathbb{Q}$-isomorphic curve $E^{(d)} : dy^2 = x^3 + Ax + B$. The isomorphism maps the point $(x, y) \in E^{(d)}$ to $(dx, d^2y) \in E^d$. Now, let n be a positive integer, and $\Psi_n(x)$ the n-division polynomial of E. So, to determine if there exists a square-free integer d such that the d-quadratic twist of E has a point of order n defined over some number field K, it is enough to check if one of the roots of $\Psi_n(x)$, say α, belongs to K and $\alpha^3 + A\alpha + B = d\beta^2$ for some $\beta \in K$. Note that if $\alpha \in \mathbb{Q}$, then a necessary condition for the existence of d is that the degree of K is even.

In the Appendix, we give the necessary background information about elliptic curves defined over $\mathbb{Q}$ with CM. This information will be used to prove Theorems 1, 2 and 4.

2.2. Proof of Theorem 1. In Table 1, we give examples for all the cases in $\Phi^{\mathrm{CM}}(3)$, therefore all those torsion subgroups appear in $\Phi^{\mathrm{CM}}_{\mathbb{Q}}(3)$. This completes the proof of Theorem 1.

Remark 5. Let K be a cubic field, and let E be an elliptic curve defined over K with CM by a quadratic order of discriminant $-\mathfrak{cm}$ such that $E(K)_{\mathrm{tors}} \notin \Phi^{\mathrm{CM}}(3) \{\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3, \mathcal{C}_4, \mathcal{C}_6, \mathcal{C}_2 \times \mathcal{C}_2\}$. Bourdon, Clark and Stankewicz [2, Theorem 1.4] proved that K is isomorphic to $\mathbb{Q}(\alpha_i)$ where α_i is listed below

i	α_i	β_i	$\mathfrak{cm}$	$E(K)_{\mathrm{tors}}$
1	$\alpha_1^3 - 15\alpha_1^2 - 9\alpha_1 - 1 = 0$	$(\alpha_1^2 + 10\alpha_1 + 1)/4$	3	$\mathcal{C}_9$
2	$\alpha_2^3 + 105\alpha_2^2 - 33\alpha_2 - 1 = 0$	$(-17\alpha_2^2 + 100\alpha_2 + 1)/76$	27	$\mathcal{C}_9$
3	$\alpha_3^3 - 4\alpha_3^2 + 3\alpha_3 + 1 = 0$	$-2\alpha_3^2 + 4\alpha_3 + 1$	7	$\mathcal{C}_{14}$
4	$\alpha_4^3 - 186\alpha_4^2 + 3\alpha_4 + 1 = 0$	$(2\alpha_4^2 + 10\alpha_4 - 1)/27$	28	$\mathcal{C}_{14}$

and over that field E is isomorphic to $\mathcal{E}_i : y^2 + (1 - \alpha_i)xy - \beta_i y = x^3 - \beta_i x^2$. Let δ be such that $\delta^3 - 3\delta - 1 = 0$, then $\mathbb{Q}(\delta)$ is isomorphic to $\mathbb{Q}(\alpha_i)$ for $i = 1, 2$. Then the elliptic curve $\mathcal{E}_1$ (resp. $\mathcal{E}_2$) is isomorphic over $\mathbb{Q}(\delta)$ to E_3^{16} (resp. E_{27}^{1}). Similarly, if γ satisfies $\gamma^3 + \gamma^2 - 2\gamma - 1 = 0$, then $\mathbb{Q}(\gamma)$ is isomorphic to $\mathbb{Q}(\alpha_i)$ for $i = 3, 4$ and $\mathcal{E}_3$ (resp. $\mathcal{E}_4$) is isomorphic over $\mathbb{Q}(\gamma)$ to E_7^{-7} (resp. E_{28}^{7}). (See Table 1). Then the torsion subgroups $\mathcal{C}_9$ and $\mathcal{C}_{14}$ occur for elliptic curves defined over $\mathbb{Q}$ base change to cubic fields.

2.3. Proof of Theorem 2. For any $G \in \Phi(1)$, the set $\Phi_{\mathbb{Q}}(3,G)$ has been characterized in [18, Theorem 1.2]. In particular, for each $G \in \Phi^{\mathrm{CM}}(1)$, we have:

$$\begin{aligned}\Phi_{\mathbb{Q}}^{\mathrm{CM}}(3,G) &\subseteq \Phi_{\mathbb{Q}}(3,G) \cap \Phi_{\mathbb{Q}}^{\mathrm{CM}}(3) \\ &= \begin{cases} \{G\} & \text{if } G \in \{\mathcal{C}_4, \mathcal{C}_6, \mathcal{C}_2 \times \mathcal{C}_2\}, \\ \mathcal{C}_3, \mathcal{C}_6, \mathcal{C}_9\} & \text{if } G = \mathcal{C}_3, \\ \mathcal{C}2, \mathcal{C}_6, \mathcal{C}_{14}\} & \text{if } G = \mathcal{C}_2, \\ \mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3, \mathcal{C}_4, \mathcal{C}_6, \mathcal{C}_2 \times \mathcal{C}_2\} & \text{if } G = \mathcal{C}_1. \end{cases}\end{aligned}$$

Actually, except for $G = \mathcal{C}_1$, we have $\Phi_{\mathbb{Q}}^{\mathrm{CM}}(3,G) = \Phi_{\mathbb{Q}}(3,G) \cap \Phi_{\mathbb{Q}}^{\mathrm{CM}}(3)$, since there are explicit examples of each case in Table 1. Furthermore, for $G = \mathcal{C}_1$, we have examples with torsion growth $\mathcal{C}_2, \mathcal{C}_3$, and $\mathcal{C}_6$ over cubic fields. Then it remains to discard the cases $\mathcal{C}_4$ and $\mathcal{C}_2 \times \mathcal{C}_2$. In Table 2, we check that if E is an elliptic curve defined over $\mathbb{Q}$ with CM and trivial torsion, then $\mathfrak{cm} \in \{27, 11, 19, 43, 67, 163\}$ or $\mathfrak{cm} = 3$ with $E : y^2 = x^3 + k$ and $k \neq r^2, r^3, -432$. With this in mind, we split the proof into cases.

Case $\mathfrak{cm} \in \{27, 11, 19, 43, 67, 163\}$. Note that for these curves, the corresponding j-invariants are neither 0 nor 1728. Then we have just quadratic twists, in particular, it is only necessary to study the n-division polynomials for $E_{\mathfrak{cm}}$. In the following cases, the n-division polynomial $\Psi_n(x)$ refers to the elliptic curve $E_{\mathfrak{cm}}$. We have that the field of definition of the full 2-torsion, $\mathbb{Q}(E[2])$, is the splitting field of $\Psi_2(x) = f_{\mathfrak{cm}}(x)$. We have that those polynomials are irreducible, and the cubic fields that they define are not a Galois extension. This proves that torsion $\mathcal{C}_2 \times \mathcal{C}_2$ is not possible over a cubic field for those cases. Since $\Psi_4(x)$ is irreducible of degree 6, there are no points of order 4 over a cubic field for any of the treated cases.

Case $E : y^2 = x^3 + k$ with $k \neq r^2, r^3, -432$. Here $\Psi_2(x) = x^3 + k$ is irreducible, since $k \neq r^3$, and the cubic field it defines never is a Galois extension for any k. Now $\Psi_4(x) = 2(x^6 + 20kx^3 - 8k^2)$, and $z = -(10 \pm 6\sqrt{3})k$ is a root of $\Psi_4(\sqrt[3]{x})$. But $z = x^3$ never occurs for x in a cubic field. We have proved that there are neither points of order 4 nor full 2-torsion over cubic fields.

This finishes the first part of the proof of Theorem 2. The second part is a direct consequence of the classification obtained in [18]. In Table 1, we give examples for each set in $\mathcal{H}_{\mathbb{Q}}(3,G)$, showing that all its elements belong to $\Phi_{\mathbb{Q}}^{\mathrm{CM}}(3,G)$, and thus completing the proof of Theorem 2.

2.4. Proof of Theorem 4. Let E be an elliptic curve defined over $\mathbb{Q}$ with CM. We have an explicit description in Table 2 of $E(\mathbb{Q})_{\text{tors}}$ in terms of its CM-invariants. Now due to the classification of $\Phi_{\mathbb{Q}}^{\text{CM}}(3,G)$ for each $G \in \Phi^{\text{CM}}(1)$, we know the possible torsion growth over cubic fields. In this case, we only need to compute the n-division polynomials for $n \in \{2,3,7,9\}$ and check if they have (irreducible) factors of degree 3.

First note that the torsion growth over a cubic field can only be cyclic by Theorem 2. Moreover, if the torsion over $\mathbb{Q}$ has odd order, then the 2-division polynomial $\Psi_2(x)$ is irreducible of order 3. Let α be a root of $\Psi_2(x)$, and define $K = \mathbb{Q}(\alpha)$. Then over K the torsion is cyclic of even order.

We split the proof depending on whether the twists are quadratic or not. That is, depending on whether $\mathfrak{cm} \in \{3,4\}$ or not. We start by supposing that $\mathfrak{cm} \notin \{3,4\}$, and let $\Psi_n(x)$ denote the n-division polynomial of $E_{\mathfrak{cm}}$.

Case $\mathfrak{cm} \in \{11,19,43,67,163\}$. The torsion over $\mathbb{Q}$ is trivial, therefore the torsion can grow to $\mathcal{C}_2, \mathcal{C}_3$ or $\mathcal{C}_6$. We have that all the irreducible factors of $\Psi_3(x)$ are of even order, so there are no points of order 3 over cubic fields. Only torsion growth to $\mathcal{C}_2$ over the cubic field $\mathbb{Q}(\alpha)$ is possible, where $\Psi_2(\alpha) = 0$.

Case $\mathfrak{cm} = 8$. We have $E_8^k(\mathbb{Q})_{\text{tors}} \simeq \mathcal{C}_2$ and $\Phi_{\mathbb{Q}}^{\text{CM}}(3,\mathcal{C}_2) = \{\mathcal{C}_2, \mathcal{C}_6, \mathcal{C}_{14}\}$. Therefore we only need to check if $\Psi_3(x)$ and $\Psi_7(x)$ have irreducible factors of degree 3. Again all the factors are of even degree. So there is no torsion growth over cubic fields.

Case $\mathfrak{cm} \in \{7,28\}$. Again $E_{\mathfrak{cm}}^k(\mathbb{Q})_{\text{tors}} \simeq \mathcal{C}_2$. In both cases, $\Psi_3(x)$ is irreducible (of degree 4), so there are no points of order 3 over cubic fields, and $\Psi_7(x)$ has only a degree 3 factor. In particular, these factors define cubic fields $\mathbb{Q}(\beta)$ that are isomorphic to $\mathbb{Q}(\alpha)$, where $\alpha^3 + \alpha^2 - 2\alpha - 1 = 0$.

- For $\mathfrak{cm} = 7$: $\beta = 36\alpha - 9$ and $f_7(\beta) = -7(2^2 3^3 \alpha)^2$. That is, only for $k = -7$ we do have points of order 7 over a cubic field.
- For $\mathfrak{cm} = 28$: $\beta = 4\alpha^2 - 4\alpha + 13$ and $f_{28}(\beta) = 7(4(-3\alpha^2 + 3\alpha + 1))^2$. In this case, we only have 7-torsion for $k = 7$.

Case $\mathfrak{cm} = 16$. For $k = 1, 2$ we have no torsion growth over a cubic field, since for those values, we get $E_{16}^k(\mathbb{Q})_{\text{tors}} \simeq \mathcal{C}_4$. Now suppose $k \neq 1, 2$, so that $E_{16}^k(\mathbb{Q})_{\text{tors}} \simeq \mathcal{C}_2$. We have that there is no torsion growth over cubics, since $\Psi_3(x)$ and $\Psi_7(x)$ are irreducible of degrees 4 and 24, respectively.

Case $\mathfrak{cm} = 27$. Let $k=1$, then $E^1_{27}(\mathbb{Q})_{\text{tors}} \simeq \mathcal{C}_3$ and $\Phi^{\text{CM}}_{\mathbb{Q}}(3, \mathcal{C}_3) = \{\mathcal{C}_3, \mathcal{C}_6, \mathcal{C}_9\}$. We have that the torsion grows to $\mathcal{C}_6$ and $\mathcal{C}_9$ over $\mathbb{Q}(\sqrt[3]{2})$ and $\mathbb{Q}(\alpha)$, where $\alpha^3 - 3\alpha - 1 = 0$, respectively. Now suppose $k \neq 1$, then $E^k_{27}(\mathbb{Q})_{\text{tors}} \simeq \mathcal{C}_1$. There is a degree 3 irreducible factor of $\Psi_3(x)$ such that if α is a root of this factor, then $\alpha = -4(2\sqrt[3]{9} + 3\sqrt[3]{3} + 1)$. Since $f_{27}(\alpha) = -3(4(4\sqrt[3]{9} + 6\sqrt[3]{3} + 9))^2$, we have that there are points of order 3 over a cubic field if and only if $k = -3$ and the cubic field is $\mathbb{Q}(\sqrt[3]{3})$. On the other hand, the torsion grows to $\mathcal{C}_2$ over $\mathbb{Q}(\sqrt[3]{2})$ for any k.

Case $\mathfrak{cm} = 12$. For $k = 1$, we have no torsion growth over a cubic field, since $E^1_{12}(\mathbb{Q})_{\text{tors}} \simeq \mathcal{C}_6$. Let $k \neq 1$, then $E^k_{12}(\mathbb{Q})_{\text{tors}} \simeq \mathcal{C}_2$. There is no torsion growth over a cubic field to $\mathcal{C}_{14}$, since all the irreducible factors of $\Psi_7(x)$ are of degree divisible by 6. Now the 3-division polynomial $\Psi_3(x)$ satisfies $\Psi_3(\alpha) = 0$ where $\alpha = -2\sqrt[3]{4} - 2\sqrt[3]{2} - 1$. In this case, we have $f_{12}(\alpha) = -3(2(\sqrt[3]{4} + \sqrt[3]{3} + 1))^2$. That is, there are points of order 3 over a cubic field K if and only if $k = -3$ and $K = \mathbb{Q}(\sqrt[3]{2})$.

Finally, the non-quadratic twists:

Case $\mathfrak{cm} = 4$. For $k = 4$ and $k = -r^2$, the torsion subgroup over $\mathbb{Q}$ is isomorphic to $\mathcal{C}_4$ and $\mathcal{C}_2 \times \mathcal{C}_2$, respectively. Therefore, for those values, there is no torsion growth over cubic fields. Suppose $k \neq 4, -r^2$, then $E^k_4(\mathbb{Q})_{\text{tors}} \simeq \mathcal{C}_2$. Then the torsion can grow over a cubic field to $\mathcal{C}_6$ or $\mathcal{C}_{14}$. Let $\Psi_3(x)$ and $\Psi_7(x)$ be the 3- and 7-division polynomials, respectively, of E^k_4. Then:

- $\Psi_3(x) = k^2 g_3(x^2/k)$, where $g_3(x) = 3x^2 + 6x - 1$ is irreducible.
- $\Psi_7(x) = k^{12} g_7(x^2/k)$, where $g_7(x) = 7x^{12} + 308x^{11} - 2954x^{10} - 19852x^9 - 35231x^8 - 82264x^7 - 111916x^6 - 42168x^5 + 15673x^4 + 14756x^3 + 1302x^2 + 196x - 1$ is irreducible.

Then there cannot be points of order 3 or 7 over cubic fields. We have proved that for the family of curves with $\mathfrak{cm} = 4$, there is no torsion growth over cubic fields.

Case $\mathfrak{cm} = 3$. In this case, the elliptic curve has the model $E^k_3 : y^2 = x^3 + k$ for $k \in \mathbb{Q}^*/(\mathbb{Q}^*)^6$. Note that this case has been studied by Dey and Roy [9], although they used different techniques. We split the proof depending on the torsion over $\mathbb{Q}$:

- $E^k_3(\mathbb{Q})_{\text{tors}} \simeq \mathcal{C}_6$, then $k = 1$, and there is no torsion growth over cubic fields.
- $E^k_3(\mathbb{Q})_{\text{tors}} \simeq \mathcal{C}_3$, then $k = -432$ or $k = r^2 \neq 1$. Here the torsion grows to $\mathcal{C}_6$ over $\mathbb{Q}(\sqrt[3]{k})$, since the 2-division polynomial is $x^3 + k$, and k is not a cube in $\mathbb{Q}$. The other possible torsion growth over a cubic is $\mathcal{C}_9$. First let $k = -432$, then $g(x) = x^3 + 36x^2 - 1728$ is the unique degree 3 irreducible

factor of the 9-division polynomial of E_3^{-432}. Let α be a root of $g(x)$, then $\alpha^3 - 432$ is not a square in $\mathbb{Q}(\alpha)$. Then there is no torsion growth over $\mathbb{Q}(\alpha)$. Now suppose $k = r^2 \neq 1$ and $P_3 = (0, r)$ is a point of order 3 over $\mathbb{Q}$. Then $P_9 = (\beta, r\gamma) \in \mathbb{Q}(\alpha, \beta)$ satisfies $3P_9 = P_3$, where $\alpha^3 - 3\alpha - 1 = 0$, $\gamma = 2\alpha^2 - 4\alpha - 1$, and $\beta^3 - r^2\gamma^2 + r^2 = 0$. Therefore, the field of definition of P_9 is of degree 3 or 9. We are going to check in which conditions this field is of degree 3 – equivalently, when there is torsion growth to $\mathcal{C}_9$ over a cubic field. We need that $\beta \in \mathbb{Q}(\alpha)$. Note that $\beta^3 = r^2(\gamma^2 - 1) = 4(\alpha^2 - \alpha - 1)^3 r^2$. In other words, the equation $z^3 = 4r^2$ has solutions over $\mathbb{Q}(\alpha)$. But this only happens if and only if $r = 4s^3$, $s \in \mathbb{Q}$; and $k = 16$ is the unique possibility, since k must belong to $\mathbb{Q}^*/(\mathbb{Q}^*)^6$.

- $E_3^k(\mathbb{Q})_{\text{tors}} \simeq \mathcal{C}_2$, then $k = r^3 \neq 1$. In this case, E_3^k is the r-quadratic twist of E_3. Let $\Psi_n(x)$ be the n-division polynomial of E_3. In this case, the torsion can grow over a cubic field to $\mathcal{C}_6$ or $\mathcal{C}_{14}$. The last case is not possible, since all the irreducible factors of $\Psi_7(x)$ are of degree divisible by 6. On the other hand, $\Psi_3(x) = 3x(x^3+4)$ and $f_3(\sqrt[3]{4}) = -3$. Then, there are points of order 3 over a cubic field K if and only if $r = -3$ (i.e., $k = -27$) and $K = \mathbb{Q}(\sqrt[3]{2})$.
- $E_3^k(\mathbb{Q})_{\text{tors}} \simeq \mathcal{C}_1$, then $k \neq r^2, r^3, -432$. We have $\Phi_{\mathbb{Q}}^{\text{CM}}(3, \mathcal{C}_1) = \{\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3, \mathcal{C}_6\}$. We are going to study the n-division polynomial, $\Psi_n(x)$, of E_3^k:
  - $\Psi_2(x) = x^3 + k$ is irreducible, then there is a point of order 2 over $\mathbb{Q}(\sqrt[3]{k})$.
  - $\Psi_3(x) = 3x(x^3 + 4k)$. Note that if $x = 0$, then the equation $y^2 = k$ has solution over a cubic field if and only if k is a square over $\mathbb{Q}$. But we have assumed that $k \neq r^2$. Let $\alpha \neq 0$ be another root of $\Psi_3(x) = 0$. Then $y^2 = \alpha^3 + k = \alpha^3 + 4k - 3k = -3k$ has solution over a cubic field if and only if $k = -3s^2$ for some $r \in \mathbb{Q}$. In particular, the cubic field is $\mathbb{Q}(\sqrt[3]{12s^2})$.

Finally, we study the torsion growth over a cubic field K to $\mathcal{C}_6$. Necessarily, $k = -3s^2$ and the cubic fields of definition of the points of order 2 and 3 must be equal to K. From the equality $\mathbb{Q}(\sqrt[3]{3s^2}) = \mathbb{Q}(\sqrt[3]{12s^2})$, we obtain $K = \mathbb{Q}(\sqrt[3]{4})$. On the other hand, $\sqrt[3]{3s^2} \in K$ if and only if $s = 6t^3$; but necessarily, $t = \pm 1$, since $k \in \mathbb{Q}^*/(\mathbb{Q}^*)^6$. Then we conclude that the torsion grows over a cubic field K to $\mathcal{C}_6$ if and only if $k = -108$ and $K = \mathbb{Q}(\sqrt[3]{2})$.

Remark 6. All the computations in this paper have been done using `Magma` [1], and the source code is available in the online supplement [12].

Appendix. Elliptic curve over $\mathbb{Q}$ with CM.

Here we give a summary of the necessary information related to elliptic curves over $\mathbb{Q}$ with CM used in this paper. Let E be an elliptic curve defined over $\mathbb{Q}$ with CM by 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. Then R is one of the thirteen orders that correspond to the first and second column of Table 2. Each order corresponds to a $\overline{\mathbb{Q}}$-isomorphic class of elliptic curves defined over $\mathbb{Q}$ with CM. The corresponding j-invariant appears at the third column. The fourth column, $\mathfrak{cm}$, denotes the absolute value of the discriminant of the CM quadratic order R. Note that the integer $\mathfrak{cm}$ gives the $\overline{\mathbb{Q}}$-isomorphic class of E. The fifth column gives a pair of integers $[A_{\mathfrak{cm}}, B_{\mathfrak{cm}}]$ such that if we denote by $f_{\mathfrak{cm}}(x) = x^3 + A_{\mathfrak{cm}}x + B_{\mathfrak{cm}}$, then $E_{\mathfrak{cm}} : y^2 = f_{\mathfrak{cm}}(x)$ is an elliptic curve with $j(E_{\mathfrak{cm}})$ equal to the j-invariant j at the same row. That is, $E_{\mathfrak{cm}}$ is a representative for each class. Now by the theory of twists of elliptic curves (cf. [30, X §5]) applied to elliptic curves defined over $\mathbb{Q}$ with CM, we have:

- If $\mathfrak{cm} \in \{12, 27, 16, 7, 28, 11, 19, 43, 67, 163\}$ (i.e., $j(E) \neq 0, 1728$), then E is $\mathbb{Q}$-isomorphic to the k-quadratic twist of $E_{\mathfrak{cm}}$ for some square-free integer k. That is, E has a short Weierstrass model of the form $E^k_{\mathfrak{cm}} : y^2 = x^3 + k^2 A_{\mathfrak{cm}} x + k^3 B_{\mathfrak{cm}}$.
- If $\mathfrak{cm} = 3$ (i.e., $j(E) = 0$), then E has a short Weierstrass model of the form $E^k_3 : y^2 = x^3 + k$, where k is an integer such that $k \in \mathbb{Q}^*/(\mathbb{Q}^*)^6$.
- If $\mathfrak{cm} = 4$ (i.e., $j(E) = 1728$), then E has a short Weierstrass model of the form $E^k_4 : y^2 = x^3 + kx$, where k is an integer such that $k \in \mathbb{Q}^*/(\mathbb{Q}^*)^4$.

Note that k and $\mathfrak{cm}$ are uniquely determined by E. We call them the CM-invariants of the elliptic curve E.

Finally, given an elliptic curve E defined over $\mathbb{Q}$ with CM, in the last two columns of Table 2, we give a characterization of its torsion subgroup (over $\mathbb{Q}$) depending on its CM-invariants $(\mathfrak{cm}, k)$ (see [13, Table 3, §2]).

$-D$	$\mathfrak{f}$	j	$\mathfrak{cm}$	$[A_{\mathfrak{cm}}, B_{\mathfrak{cm}}]$	k	$E^k_{\mathfrak{cm}}(\mathbb{Q})_{\text{tors}}$
-3	1	0	3	[0,1]	1	$\mathcal{C}_6$
					$-432, r^2 \neq 1$	$\mathcal{C}_3$
					$r^3 \neq 1$	$\mathcal{C}_2$
					$\neq r^2, r^3, -432$	$\mathcal{C}_1$
	2	$2^4 \cdot 3^3 \cdot 5^3$	12	$[-15, 22]$	1	$\mathcal{C}_6$
					$\neq 1$	$\mathcal{C}_2$
	3	$-2^{15} \cdot 3 \cdot 5^3$	27	$[-480, 4048]$	1	$\mathcal{C}_3$
					$\neq 1$	$\mathcal{C}_1$
-4	1	$2^6 \cdot 3^3 = 1728$	4	$[1, 0]$	4	$\mathcal{C}_4$
					$-r^2$	$\mathcal{C}_2 \times \mathcal{C}_2$
					$\neq 4, -r^2$	$\mathcal{C}_2$
	2	$2^3 \cdot 3^3 \cdot 11^3$	16	$[-11, 14]$	$1, 2$	$\mathcal{C}_4$
					$\neq 1, 2$	$\mathcal{C}_2$
-7	1	$-3^3 \cdot 5^3$	7	$[-2835, -71442]$	–	$\mathcal{C}_2$
	2	$3^3 \cdot 5^3 \cdot 17^3$	28	$[-595, 5586]$	–	$\mathcal{C}_2$
-8	1	$2^6 \cdot 5^3$	8	$[-4320, 96768]$	–	$\mathcal{C}_2$
-11	1	-2^{15}	11	$[-9504, 365904]$	–	$\mathcal{C}_1$
-19	1	$-2^{15} \cdot 3^3$	19	$[-608, 5776]$	–	$\mathcal{C}_1$
-43	1	$-2^{18} \cdot 3^3 \cdot 5^3$	43	$[-13760, 621264]$	–	$\mathcal{C}_1$
-67	1	$2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$	67	$[-117920, 15585808]$	–	$\mathcal{C}_1$
-163	1	$-2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$	163	$[-34790720, 78984748304]$	–	$\mathcal{C}_1$

Table 2. Elliptic curves defined over $\mathbb{Q}$ with CM. Torsion over $\mathbb{Q}$.

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.

References

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

[2] A. Bourdon, P. L. Clark and 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, 2004, arXiv:math/0407264.

[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), 411–439.

[8] M. Derickx. A. Etropolski, M. van Hoeij, J. Morrow and D. Zureick-Brown, Sporadic cubic torsion, in preparation.

[9] P. K. Dey and B. Roy, Torsion groups of Mordell curves over cubic and sextic fields, 2019, arXiv:1908.07791.

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

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

[12] E. González-Jiménez, Magma scripts and electronic transcript of computations for the paper "Torsion growth of rational elliptic curves with complex multiplication over cubic fields", http://matematicas.uam.es/ enrique.gonzalez.jimenez.

[13] E. González-Jiménez, Explicit characterization of the torsion growth of rational elliptic curves with complex multiplication over quadratic fields, 2019, arXiv:1909.00637.

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

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

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

[17] E. González-Jiménez and F. Najman, An algorithm for determining torsion growth of elliptic curves, *Exp. Math.* (2019) (*to appear*).

[18] 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.

[19] 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.

[20] 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.

[21] T. Gužvić, Torsion growth of rational elliptic curves in sextic number fields, 2019, arXiv:1910.01561.

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

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

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

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

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

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

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

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

[30] J-H. Silverman, The Arithmetic of Elliptic Curves, Second Edition, Graduate Texts in Mathematics, Vol. **106**, *Springer*, *Dordrecht*, 2009.

[31] L. C. Washington, Elliptic Curves. Number Theory and Cryptography, Second Edition, *Chapman* & *Hall/CRC*, *Boca Ranton, FL*, 2008.

ENRIQUE 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 July 16, 2019; revised February 2, 2020)