TORSION GROWTH OVER CUBIC FIELDS
OF RATIONAL ELLIPTIC CURVES WITH COMPLEX MULTIPLICATION

ENRIQUE GONZÁLEZ-JIMÉNEZ

Abstract. This article is a contribution to the project of classifying the torsion growth of elliptic curve upon base-change. In this article we treat the case of elliptic curve 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 in Number Theory or Algebraic 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 \( E(K)_{\text{tors}} \), is called the torsion subgroup and it is well known that is isomorphic to \( \mathbb{C}_n \times \mathbb{C}_m \) for some positive integers \( n, m \), where \( \mathbb{C}_n = \mathbb{Z}/n\mathbb{Z} \) denotes the cyclic group of order \( n \). The study of torsion subgroups is had been treated for several active people last years. Thanks to Merel [19], 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 \( E(K)_{\text{tors}} \), where \( K \) runs through all number fields \( K \) of degree \( d \) and \( E \) runs through all elliptic curves over \( K \), is finite. Only the cases \( d = 1 \) and \( d = 2 \) are known (by [18]; and [16, 17] respectively).

This paper focuses on a particular approach concerning torsion growth: we are interested in studying how does the torsion subgroup of an elliptic curve defined over \( \mathbb{Q} \) change when we consider the elliptic curve over a number field of degree \( d \). 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 \( E(K')_{\text{tors}} \nsubseteq E(K)_{\text{tors}} \) for any subfield \( K' \subsetneq K \).

We introduce some useful definition for the sequel:

- Let \( \Phi_\mathbb{Q}(d) \) be the set of possible groups (up to isomorphisms) that can appear as the torsion subgroup over a number field of degree \( d \), of an elliptic curve defined over \( \mathbb{Q} \).
- Fixed \( G \in \Phi(1) \), let \( \Phi_\mathbb{Q}(d, G) \) be the subset of \( \Phi_\mathbb{Q}(d) \) such that \( E \) runs through all elliptic curves over \( \mathbb{Q} \) such that \( E(\mathbb{Q})_{\text{tors}} \cong G \).
- Let \( E \) be an elliptic curve defined over \( \mathbb{Q} \) and \( d \) a positive integer. We denote by \( \mathcal{H}_\mathbb{Q}(d, E) \) the multiset of groups \( H \) such that there exist \( K/\mathbb{Q} \), an extension of degree dividing \( d \), with \( H \cong E(K)_{\text{tors}} \neq E(\mathbb{Q})_{\text{tors}} \) and the torsion growth in \( K \) is primitive. 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. We let $\mathcal{H}_Q(d)$ denote the set of $\mathcal{H}_Q(d,E)$ as $E$ runs over all elliptic curves defined over $\mathbb{Q}$. Finally, for any $G \in \Phi(1)$ we define $\mathcal{H}_Q(d,G)$ as the set of multisets $\mathcal{H}_Q(d,E)$ where $E$ runs over all the elliptic curve defined over $\mathbb{Q}$ such that $E(\mathbb{Q})_{\text{tors}} \cong G$. Denote by $h_Q(d)$ the maximum of the cardinality of $S$ when $S \in \mathcal{H}_Q(d)$, then $h_Q(d)$ gives the maximum number of field extension of degrees dividing $d$ where there is primitive torsion growth.

The sets $\Phi_Q(d)$, $\Phi_Q(d,G)$ and $\mathcal{H}_Q(d,G)$, for any $G \in \Phi(1)$, have been completely classified for $d = 2, 3, 5, 7$ and for any positive integer $d$ whose prime divisors are greater than 7 (cf. [21, 14, 15, 13, 7, 12]). The set $\Phi_Q(4)$ is known [2, 12]. The other sets have been treated for $d = 4$ in [11] and $d = 6$ in [4]. We denote by $\Phi_{\text{CM}}(d)$, $\Phi_{\text{CM}}(d,G)$, $\mathcal{H}_{\text{CM}}(d,G)$, which are defined as the analogues above sets but restricting to elliptic curves with complex multiplication (CM).

The set $\Phi_{\text{CM}}(1)$ was determined by Olson [22]:

$$\Phi_{\text{CM}}(1) = \{C_1, C_2, C_3, C_4, C_6, C_2 \times C_2\}.$$ 

The quadratic cases by Müller et al [20] and the cubic case by several authors headed by Zimmer [6, 23]:

$$\Phi_{\text{CM}}(3) = \Phi_{\text{CM}}(1) \cup \{C_9, C_{14}\}.$$ 

Recently, Clark et al. [3] have computed the sets $\Phi_{\text{CM}}(d)$, for $4 \leq d \leq 12$.

Restricting to elliptic curve with complex multiplication defined over $\mathbb{Q}$ we obtain the following results:

**Theorem 1.** $\Phi_{\text{CM}}(3) = \Phi_{\text{CM}}(3)$.

**Theorem 2.** Let be $G \in \Phi_{\text{CM}}(1)$. Then

- If $G \in \{C_4, C_6, C_2 \times C_2\}$ then $\Phi_{\text{CM}}(3,G) = \{G\}$. In particular, $\mathcal{H}_{\text{CM}}(3,G) = \emptyset$.
- If $G \in \{C_1, C_2, C_3\}$ then the sets $\Phi_{\text{CM}}(3,G)$ and $\mathcal{H}_{\text{CM}}(3,G)$ are the following:

| $G$ | $\Phi_{\text{CM}}(3,G) \setminus \{G\}$ | $\mathcal{H}_{\text{CM}}(3,G)$ |
|-----|---------------------------------|------------------|
| $C_1$ | $\{C_2, C_3, C_6\}$ | $C_2$ |
|     |                                 | $C_6$ |
|     |                                 | $C_2, C_3$ |
| $C_2$ | $\{C_6, C_{14}\}$ | $C_6$ |
|     |                                 | $C_{14}$ |
| $C_3$ | $\{C_6, C_9\}$ | $C_6$ |
|     |                                 | $C_6, C_9$ |

In particular, $h_{\text{CM}}(3) = 2$.

Our aim in this paper is to go further. More precisely, one we have given a description of the possible torsion growth over cubic fields we are going to give a completely explicit description of this
growth in terms of some invariants attached to a given elliptic curve. The case of quadratic growth is solved in [9]. In an ongoing paper [10] we will solve the problem for number fields of low degree.

**Theorem 3.** Table 4 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 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 $E(K)_{\text{tors}}$ the torsion subgroup of the Mordell-Weil group of $E$ over $K$. For a positive integer $n$, we denote by $C_n = \mathbb{Z}/n\mathbb{Z}$ 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. [25, §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 factors by the $m$-division polynomials of $E$ for 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 $E$. In particular if $E$ is defined over $\mathbb{Q}$, $E$ has not points of order $n$ and one is interested to compute if there are points of order $n$ over a cubic field, then a necessary condition is that $\Psi_n(x)$ has an irreducible factor of degree 3.

Let $E : y^2 = x^3 + Ax + B$ be an an elliptic curve defined over $\mathbb{Q}$ and $\Psi_n(x)$ its $n$-division polynomial. To determine if there exist an 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 the roots of $\Psi_n(x)$, say $\alpha$, belongs to $K$ and $\alpha^3 + A\alpha + B = d\beta^2$ for $\beta \in K$.

At the Appendix appears the necessary information related to elliptic curves defined over $\mathbb{Q}$ with CM that it will be used to proof Theorem 1, 2, and 3.

### 2.2. Proof of Theorem 1

There are examples in Table 4 for all the cases in $\Phi^{\text{CM}}(3)$, therefore all those torsion subgroups appear in $\Phi^{\text{CM}}_Q(3)$. This proves Theorem 1.

### 2.3. Proof of Theorem 2

It has been characterized the set $\Phi_{Q(3,G)}$ for any $G \in \Phi(1)$ (see Theorem 1.2 in [13]). In particular we have $\Phi_{Q}(3,G) \subseteq \Phi_{Q}(3,G) \cap \Phi^{\text{CM}}_Q(3)$ for any $G \in \Phi^{\text{CM}}(1)$. Actually, except for $G = C_1$, the above relation is an equality since there are examples of any case in Table 1. For trivial torsion we have $\Phi_{Q}(3,C_1) \cap \Phi^{\text{CM}}_Q(3) = \{C_1, C_2, C_3, C_4, C_6, C_2 \times C_2\}$. In Table 4 we have examples of elliptic curves $E$ with trivial torsion that over cubic fields it grows to $C_2, C_3, \text{and } C_6$. Then it remains to discard the cases $C_4$ and $C_2 \times C_2$. In the Table 2 we check that if $E$ is an elliptic curve defined over $\mathbb{Q}$ with CM then $cm \in \{27, 11, 19, 43, 67, 163\}$ or $cm = 3$ with $E : y^2 = x^3 + k$ with $k \neq r^2, r^3, -432$. We split the proof depending in the cases above.

- $cm \in \{27, 11, 19, 43, 67, 163\}$: 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 $E_{cm}$. In the following cases the $n$-division polynomial $\Psi_n(x)$ refers to the elliptic curve $E_{cm}$. We have that the field of definition of the full 2-torsion, $Q(E[2])$, is the splitting field of $\Psi_2(x) = f_m(x)$. We have that those polynomials are irreducible and the cubic fields that they define are not a Galois extension. This proves
Table 1. Explicit description of torsion growth over cubic fields of elliptic curves defined over \( \mathbb{Q} \) with complex multiplication

| \( \text{cm} \) | \( k \) such that \( E = E_{\text{cm}}^k \) | \( G \simeq E(\mathbb{Q})_{\text{tors}} \) | \( \mathcal{H}_E(3) \) | \text{cubics } \mathbb{Q}(\alpha) |
|---|---|---|---|---|
| 3 | 16 | \( C_6 \) | \( C_6, C_9 \) | \( \sqrt[3]{2}, \alpha^3 - 3\alpha - 1 = 0 \) |
| | \( -432 \) | \( C_3 \) | \( C_6 \) | \( \frac{3}{\sqrt[3]{2}} \) |
| | \( r^2 \ (r \neq \pm 1, \pm 4) \) | \( C_2 \) | \( C_6 \) | \( \sqrt[3]{2} \) |
| | \( -27 \) | \( C_6 \) | \( \sqrt[3]{2} \) | \( \sqrt[3]{3}r^2, \sqrt[3]{12}r^2 \) |
| | \( r^3 \ (r \neq 1, -3) \) | \( C_2 \) | \( C_6 \) | \( \sqrt[3]{3}r^2, \sqrt[3]{12}r^2 \) |
| | \( -108 \) | \( C_1 \) | \( C_2, C_3 \) | \( \sqrt[3]{3}r^2, \sqrt[3]{12}r^2 \) |
| | \( -3r^2 \ (r \neq \pm 6) \) | \( C_2 \) | \( C_6 \) | \( \sqrt[3]{3}r^2, \sqrt[3]{12}r^2 \) |
| | \( \neq r^2, r^3, -3r^2 \) | \( C_2 \) | \( C_6 \) | \( \sqrt[3]{3}r^2, \sqrt[3]{12}r^2 \) |
| 4 | 1 | \( C_6 \) | \( C_6, C_9 \) | \( \sqrt[3]{2}, \alpha^3 - 3\alpha - 1 = 0 \) |
| | \( -3 \) | \( C_2 \) | \( C_6 \) | \( \frac{3}{\sqrt[3]{2}} \) |
| | \( \neq 1, -3 \) | \( C_3 \) | \( C_6, C_9 \) | \( \sqrt[3]{2}, \alpha^3 - 3\alpha - 1 = 0 \) |
| | \( -3 \) | \( C_1 \) | \( C_2, C_3 \) | \( \sqrt[3]{2}, \sqrt[3]{3} \) |
| | \( \neq 1, -3 \) | \( C_2 \) | \( C_6 \) | \( \sqrt[3]{3}r^2, \sqrt[3]{12}r^2 \) |
| 16 | 4 | \( C_4 \) | \( - \) | \( - \) |
| | \( -r^2 \) | \( C_2 \times C_2 \) | \( - \) | \( - \) |
| | \( \neq 4, -r^2 \) | \( C_4 \) | \( - \) | \( - \) |
| | \( 1, 2 \) | \( C_2 \) | \( - \) | \( - \) |
| | \( \neq 1, 2 \) | \( C_2 \) | \( - \) | \( - \) |
| 7 | \( -7 \) | \( C_2 \) | \( C_{14} \) | \( \alpha^3 + \alpha^2 - 2\alpha - 1 = 0 \) |
| | \( \neq -7 \) | \( C_2 \) | \( C_{14} \) | \( \alpha^3 + \alpha^2 - 2\alpha - 1 = 0 \) |
| 28 | \( 7 \) | \( C_2 \) | \( C_{14} \) | \( \alpha^3 + \alpha^2 - 2\alpha - 1 = 0 \) |
| | \( \neq 7 \) | \( C_2 \) | \( C_{14} \) | \( \alpha^3 + \alpha^2 - 2\alpha - 1 = 0 \) |
| 8 | \( - \) | \( C_2 \) | \( - \) | \( - \) |
| 11 | \( - \) | \( C_1 \) | \( C_2 \) | \( \alpha^3 - \alpha^2 + \alpha + 1 = 0 \) |
| 19 | \( - \) | \( C_1 \) | \( C_2 \) | \( \alpha^3 - \alpha^2 + 3\alpha - 1 = 0 \) |
| 43 | \( - \) | \( C_1 \) | \( C_2 \) | \( \alpha^3 - \alpha^2 - \alpha + 3 = 0 \) |
| 67 | \( - \) | \( C_1 \) | \( C_2 \) | \( \alpha^3 - \alpha^2 - 3\alpha + 5 = 0 \) |
| 163 | \( - \) | \( C_1 \) | \( C_2 \) | \( \alpha^3 - 8\alpha - 10 = 0 \) |
that torsion $C_2 \times C_2$ is not possible over a cubic field for those cases. In the other hand $\Psi_4(x)$ is irreducible of degree 6 then there are not points of order 4 over cubic field for any of the treated cases.

- $E : y^2 = x^3 + k$ 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 that 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 above. We have examples at Table 1 for any set in $H_{Q}(3, G)$ such that all its elements belong to $\Phi_{Q}^{CM}(3, G)$. This completes the proof of Theorem 2.

2.4. Proof of Theorem 3. We are going to prove Table 11. Let $E$ be an elliptic curve defined over $Q$ with CM. We have an explicit description at Table 2 of $E(Q)_{\text{tors}}$ in terms of its CM-invariants. Now thanks to the classification of $\Phi_{Q}^{CM}(3, G)$ for any $G \in \Phi_{Q}^{CM}(1)$ 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 $Q$ has odd order, then the 2-division polynomial $\Psi_2(x)$ is irreducible of order 3. Let $\alpha$ be a root of $\Psi_2(x)$ and define $K = Q(\alpha)$. Then over $K$ the torsion is cyclic of even order.

We split the proof depending if the twists are quadratic or not. That is, depending if $cm \notin \{3, 4\}$ or not. Suppose $cm \notin \{3, 4\}$ and let $\Psi_n(x)$ denotes the $n$-division polynomial of $E_{cm}$.

- $cm \in \{11, 19, 43, 67, 163\}$. The torsion over $Q$ is trivial, therefore the torsion can grow to $C_2, C_3$ or $C_6$. We have that all the irreducible factor of $\Psi_2(x)$ are of even order, then no points of order 3 over cubic fields. Only torsion growth to $C_2$ over the cubic field $Q(\alpha)$, where $\Psi_2(\alpha) = 0$.

- $cm = 8$. We have $E^k_{8}(Q)_{\text{tors}} \simeq C_2$ and $\Phi_{Q}^{CM}(3, C_2) = \{C_2, C_6, C_{14}\}$. 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. Then no torsion growth over cubic fields.

- $cm \in \{7, 28\}$. Again $E^k_{cm}(Q)_{\text{tors}} \simeq C_2$. In both cases $\Psi_3(x)$ is irreducible (of degree 4), then 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 $Q(\beta)$ that are isomorphic to $Q(\alpha)$, where $\alpha^3 + \alpha^2 - 2\alpha - 1 = 0$.

- For $cm = 7$: $\beta = 36\alpha - 9$ and $f_7(\beta) = -7(2^23\alpha^2)^2$. That is, only for $k = -7$ we have points of order 7 over a cubic field.

- For $cm = 28$: $\beta = 4\alpha^2 - 4\alpha + 13$ and $f_{28}(\beta) = 7(4(-3\alpha^2 + 3\alpha + 1))^2$. In this case only for $k = 7$.

- $cm = 16$: For $k = 1, 2$ we have not torsion growth over a cubic field since for those values $E^k_{16}(Q)_{\text{tors}} \simeq C_4$. Now suppose $k \neq 1, 2$. Then $E^k_{16}(Q)_{\text{tors}} \simeq C_2$. We have that there is not torsion growth over cubics since $\Psi_3(x)$ and $\Psi_7(x)$ are irreducible of degrees 4 and 24 respectively.

- $cm = 27$: Let $k = 1$, then $E^1_{27}(Q)_{\text{tors}} \simeq C_3$ and $\Phi_{Q}^{CM}(3, C_3) = \{C_3, C_6, C_9\}$. We have that the torsion growth to $C_6$ and $C_9$ over $Q(\sqrt{2})$ and $Q(\alpha)$, where $\alpha^3 - 3\alpha - 1 = 0$, respectively. Now suppose $k \neq 1$ then $E^k_{27}(Q)_{\text{tors}} \simeq C_1$. There is a degree 3 irreducible factor of $\Psi_3(x)$ such that if $\alpha$ is a root of this factor, then $\alpha = -4(2\sqrt{3} + 3\sqrt{3} + 1)$. Since $f_7(\alpha) = -3(4\sqrt{3} + 6\sqrt{3} + 9)^2$ we have that there are points of order 3 over a cubic field if and only if $k = -3$ and the cubic field is $Q(\sqrt{3})$. In

In
the other hand, the torsion growth to $C_2$ over $\mathbb{Q}(\sqrt[3]{2})$ for any $k$.

- $\text{cm} = 12$: For $k = 1$ we have not torsion growth over a cubic field since $E_{12}^1(\mathbb{Q})_{\text{tors}} \simeq C_6$. Let $k \neq 1$, then $E_{12}^k(\mathbb{Q})_{\text{tors}} \simeq C_2$. There are not torsion growth over a cubic field to $C_{14}$ since all the irreducible factor 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:

- $\text{cm} = 4$. For $k = 4$ and $k = -r^2$ the torsion subgroup over $\mathbb{Q}$ is isomorphic to $C_4$ and $C_2 \times C_2$ respectively. Therefore for those values there are not torsion growth over cubic fields. Suppose $k \neq 4, -r^2$, then $E_k^k(\mathbb{Q})_{\text{tors}} \simeq C_2$. Then the torsion can grow over a cubic field to $C_6$ or $C_{14}$. Let $\Psi_3(x)$ and $\Psi_7(x)$ the 3- and 7-division polynomial, respectively, of $E_4^k$.

\[\Psi_3(x) = k^2 f_3(x^2/k), \text{ where } f_3(x) = 3x^2 + 6x - 1 \text{ is irreducible.}\]

\[\Psi_7(x) = k^{12} f_7(x^2/k), \text{ where } f_7(x) = 7x^{12} + 308x^{11} - 2954x^{10} - 19852x^9 - 35231x^8 - 82264x^7 - 111916x^6 - 42168x^5 + 15673x^4 + 14756x^3 + 1302x^2 + 196x - 1 \text{ is irreducible.}\]

Then there can not be points of order 3 or 7 over cubic fields. We have proved that for the family of curves with $\text{cm} = 4$ there is not torsion growth over cubic fields.

- $\text{cm} = 3$. In this case the elliptic curve is called Mordell curve and has the model $E_3^k : y^2 = x^3 + k$ for $k \in \mathbb{Q}^*/(\mathbb{Q}^*)^0$. Note that this case has been studied by Dey and Roy [3], although they used different techniques. We split the proof depending on the torsion over $\mathbb{Q}$:

\[E_3^k(\mathbb{Q})_{\text{tors}} \simeq C_6, \text{ then } k = 1 \text{ and there are not torsion growth over cubic fields.}\]

\[E_3^k(\mathbb{Q})_{\text{tors}} \simeq C_3, \text{ then } k = -432 \text{ or } k = r^2 \neq 1. \text{ Here the torsion grows to } C_6 \text{ over } \mathbb{Q}(\sqrt[3]{k}), \text{ since the 2-division polynomial is } x^3 + k \text{ and } k \text{ is not a cube in } \mathbb{Q}. \text{ The other possible torsion growth over a cubic is } C_9. \text{ First let } k = -432, \text{ then } g(x) = x^3 + 36x^2 - 1728 \text{ is the unique degree 3 irreducible factor of the 9-division polynomial of } E_3^{-432}. \text{ Let } \alpha \text{ be a root of } g(x), \text{ then } \alpha^3 - 432 \text{ is not an square in } \mathbb{Q}(\alpha). \text{ Then there is not torsion growth over } \mathbb{Q}(\alpha). \text{ Now suppose } k = r^2 \neq 1 \text{ and } P_3 = (0, r) \text{ a point of order } 3 \text{ over } \mathbb{Q}. \text{ Then } P_3 = (\beta, r\gamma) \in \mathbb{Q}(\alpha, \beta) \text{ satisfies } 3P_3 = P_3, \text{ where } \alpha^3 - 3\alpha - 1 = 0, \gamma = 2\alpha^2 - 4\alpha - 1, \text{ and } \beta^3 - r^2\gamma^2 + r^2 = 0. \text{ Therefore, in principle, the field of definition of } P_3 \text{ is of degree } 9. \text{ We are going to check in which conditions this field is of degree } 3. \text{ Equivalently, when there is torsion growth to } C_9 \text{ over a cubic field. We need that } \beta \in \mathbb{Q}(\alpha). \text{ Note that } \beta^3 = r^2(\gamma^2 - 1) = 4(\alpha^2 - \alpha - 1)^2 r^2. \text{ In other words, the equation } z^3 = 4r^2 \text{ has solutions over } \mathbb{Q}(\alpha). \text{ But this only happens if and only if } r = 4s^3, s \in \mathbb{Q}; \text{ and } k = 16 \text{ is the unique possibility since } k \text{ must belong to } \mathbb{Q}^*/(\mathbb{Q}^*)^6.\]

\[E_3^k(\mathbb{Q})_{\text{tors}} \simeq C_2, \text{ then } k = 3^r \neq 1. \text{ In this case } E_3^k \text{ is the r-quadratic twist of } E_3. \text{ Let } \Psi_m(x) \text{ be the n-division polynomial of } E_3. \text{ In this case the torsion can grow over a cubic field to } C_6 \text{ or } C_{14}. \text{ The last case is not possible since all the irreducible factor of } \Psi_7(x) \text{ are of degree divisible by } 6. \text{ In the other hand } \Psi_3(x) = 3x(x^3 + 4) \text{ and } f_3(\sqrt[3]{4}) = -3. \text{ Then, there are points of order } 3 \text{ over a cubic field } K \text{ if and only if } r = -3 \text{ (i.e. } k = -27) \text{ and } K = \mathbb{Q}(\sqrt[3]{2}).\]

\[E_3^k(\mathbb{Q})_{\text{tors}} \simeq C_1, \text{ then } k \neq r^2, r^3, -432. \text{ We have } \Phi_{3}^{CM}(3, C_1) = \{C_1, C_2, C_3, C_6\}. \text{ We are going to study the n-division polynomial, } \Psi_n(x), \text{ of } E_3^k:\]

- $\Psi_2(x) = x^3 + k$ is irreducible, then there is a point of order 2 over $\mathbb{Q}(\sqrt[3]{k})$. 

Note that if $x = 0$ then the equation $y^2 = k$ has solution over a cubic field if and only if $k$ is an 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 $C_6$. Necessary $k = -3s^2$ 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 $K = \mathbb{Q}(\sqrt[3]{4})$. In 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 finish that the torsion growth over a cubic field $K$ to $C_6$ if and only if $k = -108$ and $K = \mathbb{Q}(\sqrt[3]{2})$.

**Remark:** All the computation have been done using Magma [1] and the source code is available in the online supplement [3].

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

The necessary information related to elliptic curves with CM to be used in this paper appear in this Appendix. Let $E$ be an elliptic curve defined over $\mathbb{Q}$ with CM by an order $R = \mathbb{Z} + \mathfrak{f}O_K$ of conductor $\mathfrak{f}$ in a quadratic imaginary field $K = \mathbb{Q}(\sqrt{-D})$, where $O_K$ 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 correspond to a $\mathbb{Q}$-isomorphic class of elliptic curves defined over $\mathbb{Q}$ with CM. The corresponding $j$-invariant appears at the third column. 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 $\mathbb{Q}$-isomorphic class of $E$. 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. [24, X §5]) applied to elliptic curve 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 squarefree integer $k$. That is, $E$ has a short Weierstrass model of the form $E_{\mathfrak{cm}}^k : y^2 = x^3 + k^2A_{\mathfrak{cm}}x + k^3B_{\mathfrak{cm}}$.
- If $\mathfrak{cm} = 3$ (i.e. $j(E) = 0$) then $E$ has a short Weierstrass model of the form $E_3^k : y^2 = x^3 + k$, 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 $E_4^k : y^2 = x^3 + kx$, 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, at 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 Table 3 at [9 §2]).
Table 2. Elliptic curves defined over $\mathbb{Q}$ with CM. Torsion over $\mathbb{Q}$.

| $-D$ | $j$ | $\text{cm}$ | $[A_{\text{cm}}, B_{\text{cm}}]$ | $k$ | $E_{\text{cm}}(\mathbb{Q})_{\text{tors}}$ |
|------|-----|-------------|-----------------|-----|------------------|
| $-3$ | 1   | 0           | 3               | $[0,1]$ | $C_1$ |
|      | 2   | $2^4 \cdot 3^3 \cdot 5^3$ | 12 | $[-15, 22]$ | $C_0$ |
|      | 3   | $-2^{15} \cdot 3 \cdot 5^3$ | 27 | $[-150, 1048]$ | $C_1$ |
| $-4$ | 1   | $2^6 \cdot 3^3 = 1728$ | 4 | $[1,0]$ | $C_4$ |
|      | 2   | $2^3 \cdot 3^3 \cdot 11^3$ | 16 | $[-11, 14]$ | $C_1 \times C_2$ |
| $-7$ | 1   | $-3^3 \cdot 5^3$ | 7 | $[-2835, -71442]$ | $C_2$ |
|      | 2   | $3^3 \cdot 5^3 \cdot 7^3$ | 28 | $[-595, 15586]$ | $C_2$ |
| $-8$ | 1   | $2^6 \cdot 5^3$ | 8 | $[-4320, 96768]$ | $C_2$ |
|      | 11  | $-2^{15}$ | 11 | $[-9504, 265904]$ | $C_1$ |
|      | 19  | $-2^{15} \cdot 3^3$ | 19 | $[508, 5776]$ | $C_1$ |
|      | 43  | $-2^{18} \cdot 3^3 \cdot 5^3$ | 43 | $[-13760, 621264]$ | $C_1$ |
|      | 67  | $2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$ | 67 | $[-1179020, 155880]8$ | $C_1$ |
| $-163$ | 1 | $-2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$ | 163 | $[-34790720, 78984748304]$ | $C_1$ |

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

[3] 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.

[4] H. B. Daniels, and E. González-Jiménez, *On the torsion of rational elliptic curves over sextic fields*. To appear in Math. Comp.

[5] P. K. Dey, and B. Roy, *Torsion groups of Mordell curves over cubic and sextic fields*. Preprint (2019).

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

[7] E. González-Jiménez, *Complete classification of the torsion structures of rational elliptic curves over quintic number fields*. J. Algebra **478** (2017), 484–505.
[8] 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

[9] E. González-Jiménez. Explicit description of the growth of the torsion subgroup of rational elliptic curves with complex multiplication over quadratic fields. Submitted.

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

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

[12] E. González-Jiménez, and F. Najman. Growth of torsion groups of elliptic curves upon base change. To appear in Math. Comp.

[13] E. González-Jiménez, F. Najman, and J.M. Tornero. Torsion of rational elliptic curves over cubic fields. Rocky Mountain J. Math. 46 (2016), no. 6, 1899–1917.

[14] 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.

[15] 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.

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

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

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

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

[20] 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.

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

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

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

[24] J-H. Silverman. The arithmetic of elliptic curves. Graduate Texts in Mathematics, 106. 2nd edition. Springer-Verlag, New York, 2009.

[25] L. C. Washington. Elliptic Curves: Number Theory and Cryptography, Second Edition, Chapman & Hall, Boca Raton, 2008.

Departamento de Matemáticas, Universidad Autónoma de Madrid, Madrid, Spain

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

URL: http://matematicas.uam.es/~enrique.gonzalez.jimenez