Journal of Algebra 478 (2017) 484–505

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Complete classification of the torsion structures of rational elliptic curves over quintic number fields

Enrique González-Jiménez [1]

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

ARTICLE INFO

Article history:
Received 9 June 2016
Available online 15 February 2017
Communicated by Gerhard Hiss

MSC:
primary 11G05, 14G05
secondary 14H52, 11R21

Keywords:
Elliptic curves
Torsion subgroup
Rationals
Quintic number fields

ABSTRACT

We classify the possible torsion structures of rational elliptic curves over quintic number fields. In addition, let E be an elliptic curve defined over $\mathbb{Q}$ and let $G = E(\mathbb{Q})_{\text{tors}}$ be the associated torsion subgroup. We study, for a given G, which possible groups $G \subseteq H$ could appear such that $H = E(K)_{\text{tors}}$, for $[K : \mathbb{Q}] = 5$. In particular, we prove that at most there is one quintic number field K such that the torsion grows in the extension $K/\mathbb{Q}$, i.e., $E(\mathbb{Q})_{\text{tors}} \subsetneq E(K)_{\text{tors}}$.

1. Introduction

Let E/K be an elliptic curve defined over a number field K. The Mordell–Weil Theorem states that the set of K-rational points, $E(K)$, is a finitely generated abelian group. Denote by $E(K)_{\text{tors}}$, the torsion subgroup of $E(K)$, which is isomorphic to $\mathcal{C}_m \times \mathcal{C}_n$ for two positive integers m, n, where m divides n and where $\mathcal{C}_n$ is a cyclic group of order n.

One of the main goals in the theory of elliptic curves is to characterize the possible torsion structures over a given number field, or over all number fields of a given degree.

E-mail address: enrique.gonzalez.jimenez@uam.es.
[1] The author was partially supported by the grant MTM2015-68524-P.

http://dx.doi.org/10.1016/j.jalgebra.2017.01.012

In 1978 Mazur [25] published a proof of Ogg's conjecture (previously established by Beppo Levi), a milestone in the theory of elliptic curves. In that paper, he proved that the possible torsion structures over $\mathbb{Q}$ belong to the set:

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

and that any of them occurs infinitely often. A natural generalization of this theorem is as follows. Let $\Phi(d)$ be the set of possible isomorphic torsion structures $E(K)_{\rm tors}$, where K runs through all number fields K of degree d and E runs through all elliptic curves over K. Thanks to the uniform boundedness theorem [26], $\Phi(d)$ is a finite set. Then the problem is to determine $\Phi(d)$. Mazur obtained the rational case ($d = 1$). The generalization to quadratic fields ($d = 2$) was obtained by Kamienny, Kenku and Momose [17,22]. For $d \geq 3$ a complete answer for this problem is still open, although there have been some advances in the last years.

However, more is known about the subset $\Phi^\infty(d) \subseteq \Phi(d)$ of torsion subgroups that arise for infinitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves defined over number fields of degree d. For $d = 1$ and $d = 2$ we have $\Phi^\infty(d) = \Phi(d)$, the cases $d = 3$ and $d = 4$ have been determined by Jeon et al. [15,16], and recently the cases $d = 5$ and $d = 6$ by Derickx and Sutherland [7].

Restricting our attention to the complex multiplication case, we denote $\Phi^{\rm CM}(d)$ the analogue of the set $\Phi(d)$ but restricting to elliptic curves with complex multiplication (CM elliptic curves in the sequel). In 1974 Olson [30] determined the set of possible torsion structures over $\mathbb{Q}$ of CM elliptic curves:

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

The quadratic and cubic cases were determined by Zimmer et al. [27,8,31]; and recently, Clark et al. [5] have computed the sets $\Phi^{\rm CM}(d)$, for $4 \leq d \leq 13$. In particular, they proved

$$\Phi^{\rm CM}(5) = \Phi^{\rm CM}(1) \cup \{\,\mathcal{C}_{11}\,\}.$$

In addition to determining $\Phi(d)$, there are many authors interested in the question of how the torsion grows when the field of definition is enlarged. We focus our attention when the underlying field is $\mathbb{Q}$. In analogy to $\Phi(d)$, let $\Phi_{\mathbb{Q}}(d)$ be the subset of $\Phi(d)$ such that $H \in \Phi_{\mathbb{Q}}(d)$ if there is an elliptic curve $E/\mathbb{Q}$ and a number field K of degree d such that $E(K)_{\rm tors} \simeq H$. One of the first general result is due to Najman [29], who determined $\Phi_{\mathbb{Q}}(d)$ for $d = 2, 3$. Chou [4] has given a partial answer to the classification of $\Phi_{\mathbb{Q}}(4)$. Recently, the author with Najman [11] have completed the classification of $\Phi_{\mathbb{Q}}(4)$ and $\Phi_{\mathbb{Q}}(p)$ for p prime. Moreover, in [11] it has been proved that $E(K)_{\rm tors} = E(\mathbb{Q})_{\rm tors}$ for all elliptic curves E defined over $\mathbb{Q}$ and all number fields K of degree d, where d is not divisible by a prime ≤ 7. In particular, $\Phi_{\mathbb{Q}}(d) = \Phi(1)$ if d is not divisible by a prime ≤ 7.

Our first result determines $\Phi_{\mathbb{Q}}(5)$.