Journal of Number Theory 183 (2018) 291–308

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

On the cyclic torsion of elliptic curves over cubic number fields

Jian Wang [1]

Department of Mathematics, University of Southern California, Los Angeles, CA 90089, USA

A R T I C L E I N F O

Article history:
Received 21 April 2017
Accepted 1 August 2017
Available online 30 August 2017
Communicated by S.J. Miller

MSC:
11G05
11G18

Keywords:
Torsion subgroup
Elliptic curves
Modular curves

A B S T R A C T

Let E be an elliptic curve defined over a number field K. Then its Mordell–Weil group $E(K)$ is finitely generated: $E(K) \cong E(K)_{tor} \times \mathbb{Z}^r$. In this paper, we discuss the cyclic torsion subgroup of elliptic curves over cubic number fields. For $N = 169, 143, 91, 65, 77$ or 55, we show that $\mathbb{Z}/N\mathbb{Z}$ is not a subgroup of $E(K)_{tor}$ for any elliptic curve E over a cubic number field K.

1. Introduction

Let E be an elliptic curve defined over a number field K. Then its Mordell–Weil group $E(K)$ is finitely generated:

$$E(K) \cong E(K)_{tor} \times \mathbb{Z}^r$$

E-mail address: blandye@gmail.com.

[1] Current address: Department of Mathematical Sciences, Tsinghua University, Beijing, 100084, China.

http://dx.doi.org/10.1016/j.jnt.2017.08.001

For a fixed elliptic E over a field K, the torsion component $E(K)_{tor}$ can be calculated due to the Nagell–Lutz–Cassels theorem [3]. However, if we consider a class of elliptic curves, it is usually difficult to list exactly all the possible group structures of $E(K)_{tor}$. The following problem is one of this kind.

Problem 1.1. For an integer $d \geq 1$, what are the possible group structures of $E(K)_{tor}$ with $[K : \mathbb{Q}] = d$?

For $d = 1$, i.e. $K = \mathbb{Q}$, by the work of Kubert [20] and Mazur [23], the torsion group $E(\mathbb{Q})_{tor}$ of an elliptic curve E over the rational number field is isomorphic to one of the following:

$$\mathbb{Z}/m\mathbb{Z}, \qquad m = 1 - 10, 12;$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}, \qquad m = 1 - 4.$$

For $d = 2$, by the work of Kenku–Momose [18] and Kamienny [14], the torsion group $E(K)_{tor}$ of an elliptic curve over a quadratic number field is isomorphic to one of the following:

$$\mathbb{Z}/m\mathbb{Z}, \qquad m = 1 - 16, 18;$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}, \qquad m = 1 - 6;$$
$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3m\mathbb{Z}, \qquad m = 1 - 2;$$
$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$$

For $d = 3$, Parent [33,34] showed that the prime divisors of the order of $E(K)_{tor}$ are ≤ 13. Jeon–Kim–Schweizer [13] determined all the torsion structures that appear infinitely often when we run through all elliptic curves over all cubic fields:

$$\mathbb{Z}/m\mathbb{Z}, \qquad m = 1 - 16, 18, 20;$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}, \qquad m = 1 - 7.$$

Najman [27] discovered a *sporadic* elliptic curve over a cubic field with torsion group isomorphic to $\mathbb{Z}/21\mathbb{Z}$. In view of these facts, our ultimate aim is to show that the torsion group $E(K)_{tor}$ of an elliptic curve E over a cubic number field is isomorphic to one of the following:

$$\mathbb{Z}/m\mathbb{Z}, \qquad m = 1 - 16, 18, 20 - 21;$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}, \qquad m = 1 - 7.$$

For the cyclic case, it suffices to show that $\mathbb{Z}/N\mathbb{Z}$ is not a subgroup of $E(K)_{tor}$ for any elliptic curve E over a cubic number field K when N is among the following list