Journal of Number Theory 157 (2015) 54–63

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Positivity of constants related to elliptic curves

Sungjin Kim

ARTICLE INFO

Article history:
Received 1 August 2014
Received in revised form 5 April 2015
Accepted 10 April 2015
Available online 9 June 2015
Communicated by David Goss

Keywords:
Elliptic curves
Density
Distribution

ABSTRACT

Let E be an elliptic curve defined over $\mathbb{Q}$. It is known that the structure of the reduction $E(\mathbb{F}_p)$ is

$$E(\mathbb{F}_p) \simeq \mathbb{Z}/d_p\mathbb{Z} \oplus \mathbb{Z}/e_p\mathbb{Z} \tag{1}$$

with $d_p | e_p$. The constant

$$C_{E,j} = \sum_{k=1}^{\infty} \frac{\mu(k)}{[\mathbb{Q}(E[jk]) : \mathbb{Q}]}$$

appears as the density of primes p with good reduction for E and $d_p = j$ (under the GRH in the non-CM case, unconditionally in the CM case). We give appropriate conditions for this constant to be positive when $j > 1$.

1. Introduction

Let E be an elliptic curve over $\mathbb{Q}$, and p be a prime of good reduction for E. Denote $E(\mathbb{F}_p)$ by the group of $\mathbb{F}_p$-rational points of E. It is known that the structure of $E(\mathbb{F}_p)$ is

$$E(\mathbb{F}_p) \simeq \mathbb{Z}/d_p\mathbb{Z} \oplus \mathbb{Z}/e_p\mathbb{Z} \tag{2}$$

E-mail address: i707107@math.ucla.edu.

http://dx.doi.org/10.1016/j.jnt.2015.04.017

with $d_p | e_p$. The cyclicity problem asks for the density of primes p of good reduction for E such that $d_p = 1$. We exclude the degenerate case $\mathbb{Q}(E[2]) = \mathbb{Q}$, where we have $C_E = 0$ trivially. Thus, all the results stated below are under the assumption $\mathbb{Q}(E[2]) \neq \mathbb{Q}$.

Let N be the conductor of the elliptic curve E and denote $\mathfrak{f}(x, E)$ by the number of primes p of good reduction for E such that $d_p = 1$. A. Cojocaru and M.R. Murty (see [CM]) obtained that if E does not have complex multiplication (non-CM curves), then

$$\mathfrak{f}(x, E) = C_E \mathrm{Li}(x) + O_N(x^{5/6}(\log x)^{2/3}),$$

under the Generalized Riemann Hypothesis (GRH) for the Dedekind zeta functions of division fields. For elliptic curves with complex multiplication (CM curves), they obtained

$$\mathfrak{f}(x, E) = C_E \mathrm{Li}(x) + O_N(x^{3/4}(\log Nx)^{1/2}),$$

under the GRH. An unconditional error term in CM case is $O(x \log x)^{-A}$ for any positive A. Precisely, A. Akbary and V.K. Murty (see [AM]) obtained

$$\mathfrak{f}(x, E) = C_E \mathrm{Li}(x) + O_{A,B}(x(\log x)^{-A}),$$

for any positive constant A, B, and the $O_{A,B}$ is uniform for $N \leq (\log x)^B$. Here, $C_E = \sum_{k=1}^{\infty} \frac{\mu(k)}{[\mathbb{Q}(E[k]):\mathbb{Q}]}$.

A. Cojocaru (see [C]) obtained the density of primes p of good reduction for E such that $d_p = j$ for $j > 1$. It is

$$C_{E,j} = \sum_{k=1}^{\infty} \frac{\mu(k)}{[\mathbb{Q}(E[jk]) : \mathbb{Q}]},$$

under the GRH for the Dedekind zeta functions of division fields. For CM curves, it can be shown unconditionally. Denote by $A(E)$ the associated Serre's constant for the elliptic curve E, which has the property:

$$\text{If } (k, A(E)) = 1, \text{ then the Galois representation:}$$
$$\mathrm{Gal}(\mathbb{Q}(E[k])/\mathbb{Q}) \to \mathrm{GL}(2, \mathbb{Z}/k\mathbb{Z}) \text{ is surjective.}$$

The positivity of C_E in non-CM case is achievable under the GRH, and the result is unconditional in the CM case. However, it was not known whether $C_{E,j} > 0$ for some $j > 1$. In this note, we obtain the positivity under appropriate conditions.

Theorem 1.1. *Let E be a non-CM elliptic curve over $\mathbb{Q}$, and N the conductor of E. Let $A(E)$ be the associated Serre's constant. Suppose also that $\mathbb{Q}(E[2]) \neq \mathbb{Q}$. Let $j > 1$ be an integer satisfying $(j, 2NA(E)) = 1$. Then $C_{E,j} > 0$ under the GRH for the division fields.*