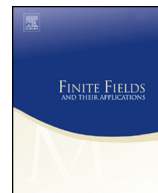




Contents lists available at ScienceDirect

## Finite Fields and Their Applications

[www.elsevier.com/locate/ffa](http://www.elsevier.com/locate/ffa)


# Average behaviors of invariant factors in Mordell–Weil groups of CM elliptic curves modulo $p$

Sungjin Kim

Department of Mathematics, University of California, Math Science Building 6160,  
Los Angeles, United States

## ARTICLE INFO

*Article history:*

Received 13 January 2014

Received in revised form 14 July 2014

Accepted 15 July 2014

Available online 7 August 2014

Communicated by Neal Koblitz

*MSC:*

11G05

*Keywords:*

Elliptic curve

Invariants

Average

## ABSTRACT

Let  $E$  be an elliptic curve defined over  $\mathbb{Q}$  and with complex multiplication by  $\mathcal{O}_K$ , the ring of integers in an imaginary quadratic field  $K$ . Let  $p$  be a prime of good reduction for  $E$ . It is known that  $E(\mathbb{F}_p)$  has a structure

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

with uniquely determined  $d_p|e_p$ . We give an asymptotic formula for the average order of  $e_p$  over primes  $p \leq x$  of good reduction, with improved error term  $O(x^2/\log^A x)$  for any positive number  $A$ , which previously was set as  $O(x^2/\log^{1/8} x)$  by [12]. Further, we obtain an upper bound estimate for the average of  $d_p$ , and a lower bound estimate conditionally on nonexistence of Siegel-zeros for Hecke L-functions.

© 2014 Elsevier Inc. All rights reserved.

*E-mail address:* [707107@gmail.com](mailto:707107@gmail.com).

<http://dx.doi.org/10.1016/j.ffa.2014.07.003>

1071-5797/© 2014 Elsevier Inc. All rights reserved.

## 1. Introduction

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

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

with uniquely determined  $d_p|e_p$ . By Hasse's bound, we have

$$|E(\mathbb{F}_p)| = p + 1 - a_p \quad (3)$$

with  $|a_p| < 2\sqrt{p}$ . We fix some notation before stating results. Let  $\bar{\mathbb{Q}}$  be the algebraic closure of  $\mathbb{Q}$ . Let  $E[k]$  be the  $k$ -torsion points of the group  $E(\bar{\mathbb{Q}})$ . Denote by  $\mathbb{Q}(E[k])$  the  $k$ -th division field of  $E$ , which is obtained by adjoining the coordinates of  $E[k]$  to  $\mathbb{Q}$ . Denote by  $n_k$  the field extension degree  $[\mathbb{Q}(E[k]) : \mathbb{Q}]$ . Let  $\text{Li}(x)$  be the logarithmic integral defined by  $\int_2^x \frac{1}{\log t} dt$ . We use the notation  $F = O(G)$  if  $F(x) \leq CG(x)$  holds for sufficiently large  $x$  and a positive constant  $C$ .

Recently, T. Freiberg and P. Kurlberg [4] started investigating the average order of  $e_p$ . They obtained that for any  $x \geq 2$ , there exists a constant  $c_E \in (0, 1)$  such that

$$\sum_{p \leq x} e_p = c_E \text{Li}(x^2) + O(x^{19/10}(\log x)^{6/5}) \quad (4)$$

under the Generalized Riemann Hypothesis (GRH), and

$$\sum_{p \leq x} e_p = c_E \text{Li}(x^2) \left( 1 + O\left(\frac{\log \log x}{\log^{1/8} x}\right) \right) \quad (5)$$

unconditionally when  $E$  has a complex multiplication (CM). Here, the implied constants depend at most on  $E$ , and the GRH is for the Dedekind zeta functions of the field extensions  $\mathbb{Q}(E[k])$  over  $\mathbb{Q}$ . (In the summation, we take 0 in place of  $e_p$  when  $E$  has a bad reduction at  $p$ .) More recently, J. Wu [12] improved their error terms in both cases

$$\sum_{p \leq x} e_p = c_E \text{Li}(x^2) + O(x^{11/6}(\log x)^{1/3}) \quad (6)$$

under GRH, and

$$\sum_{p \leq x} e_p = c_E \text{Li}(x^2) + O(x^2/(\log x)^{9/8}) \quad (7)$$

unconditionally when  $E$  has CM.

In this paper, we improve the unconditional error term in the CM case by using a number field analogue of the Bombieri–Vinogradov theorem due to [6, Theorem 1]. Also, the result is uniform in the conductor of the elliptic curves under consideration.

Download English Version:

<https://daneshyari.com/en/article/4582841>

Download Persian Version:

<https://daneshyari.com/article/4582841>

[Daneshyari.com](https://daneshyari.com)