



# The average exponent of elliptic curves modulo $p$ DOUBLON DE HAL-01094035

Jie Wu

## ► To cite this version:

Jie Wu. The average exponent of elliptic curves modulo  $p$  DOUBLON DE HAL-01094035. Journal of Number Theory, 2014, 135, pp.28-35. <hal-00711948>

**HAL Id: hal-00711948**

**<https://hal.science/hal-00711948v1>**

Submitted on 26 Jun 2012

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



HAL Authorization

# THE AVERAGE EXPONENT OF ELLIPTIC CURVES MODULO $p$

J. WU

ABSTRACT. Let  $E$  be an elliptic curve defined over  $\mathbb{Q}$ . For a prime  $p$  of good reduction for  $E$ , denote by  $e_p$  the exponent of the reduction of  $E$  modulo  $p$ . Under GRH, we prove that there is a constant  $C_E \in (0, 1)$  such that

$$\frac{1}{\pi(x)} \sum_{p \leq x} e_p = \frac{1}{2} C_E x + O_E(x^{5/6} (\log x)^{4/3})$$

for all  $x \geq 2$ , where the implied constant depends on  $E$  at most. When  $E$  has complex multiplication, the same asymptotic formula with a weaker error term  $O_E(1/(\log x)^{1/14})$  is established unconditionally. These improve some recent results of Freiberg and Kurlberg.

## 1. INTRODUCTION

Let  $E$  be an elliptic curve defined over  $\mathbb{Q}$ . For a prime  $p$  of good reduction for  $E$  the reduction of  $E$  modulo  $p$  is an elliptic curve  $E_p$  defined over the finite field  $\mathbb{F}_p$  with  $p$  elements. Denote by  $E_p(\mathbb{F}_p)$  the group of  $\mathbb{F}_p$ -rational points of  $E_p$ . Its structure as a group, for example, the existence of large cyclic subgroups, especially of prime order, is of interest because of applications to elliptic curve cryptography [5, 8]. It is well known that the finite abelian group  $E_p(\mathbb{F}_p)$  has structure

$$(1.1) \quad E_p(\mathbb{F}_p) \simeq (\mathbb{Z}/d_p\mathbb{Z}) \oplus (\mathbb{Z}/e_p\mathbb{Z})$$

for uniquely determined positive integers  $d_p$  and  $e_p$  with  $d_p \mid e_p$ . Here  $e_p$  is the size of the maximal cyclic subgroup of  $E_p(\mathbb{F}_p)$ , called the exponent of  $E_p(\mathbb{F}_p)$ . The study about  $e_p$  as a function of  $p$  has received considerable attention [11, 3, 1, 2], where the following problems were considered:

- lower bounds for the maximal values of  $e_p$ ,
- the frequency of  $e_p$  taking its maximal value, i.e., the density of the primes  $p$  for which  $E_p(\mathbb{F}_p)$  is a cyclic group,
- the smallest prime  $p$  for which the group  $E_p(\mathbb{F}_p)$  is cyclic (elliptic curve analogue of Linnik's problem).

Very recently motivated by a question of Silverman, Freiberg and Kurlberg [4] investigated the average order of  $e_p$ . Before stating their results, let us fix some notation. Given a positive integer  $k$ , let  $E[k]$  denote the group of  $k$ -torsion points of  $E$  (called *the  $k$ -division group of  $E$* ) and let  $L_k := \mathbb{Q}(E[k])$  be the field obtained by adjoining to  $\mathbb{Q}$  the coordinates of the points of  $E[k]$  (called *the  $k$ -division field*

---

*Date:* June 26, 2012.

*2010 Mathematics Subject Classification.* 11G05, 11R45.

*Key words and phrases.* Elliptic curves over global fields, density theorems.

of  $E$ ). Write

$$(1.2) \quad n_{L_k} := [L_k : \mathbb{Q}].$$

Denote by  $\mu(n)$  the Möbius function, by  $\pi(x)$  the prime-counting function and by  $\zeta_{L_k}(s)$  the Dedekind zeta function associated with  $L_k$ , respectively. Assuming the Generalized Riemann Hypothesis (GRH) for  $\zeta_{L_k}(s)$  for all positive integers  $k$ , Freiberg and Kurlberg [4, Theorem 1.1] shew that

$$(1.3) \quad \frac{1}{\pi(x)} \sum_{p \leq x} e_p = \frac{1}{2} C_E x + O_E(x^{9/10} (\log x)^{11/5})$$

for all  $x \geq 2$ , where

$$(1.4) \quad C_E := \sum_{k=1}^{\infty} \frac{1}{n_{L_k}} \sum_{dm=k} \frac{\mu(d)}{m} = \prod_p \left( 1 - \sum_{\nu=1}^{\infty} \frac{p-1}{p^{\nu} n_{L_{p^{\nu}}}} \right).$$

The implied constant depends on  $E$  at most. When  $E$  has complex multiplication (CM), they [4, Theorem 1.2] also proved that (1.3) holds unconditionally with a weaker error term

$$(1.5) \quad O_E \left( x \frac{\log_3 x}{\log_2 x} \right),$$

where  $\log_{\ell}$  denotes the  $\ell$ -fold iterated logarithm.

The aim of this short note is to propose more precise result than (1.3) and (1.5).

**Theorem 1.1.** *Let  $E$  be an elliptic curve over  $\mathbb{Q}$ .*

(a) *Assuming GRH for the Dedekind zeta function  $\zeta_{L_k}$  for all positive integers  $k$ , we have*

$$(1.6) \quad \frac{1}{\pi(x)} \sum_{p \leq x} e_p = \frac{1}{2} C_E x + O_E(x^{5/6} (\log x)^{4/3}).$$

(b) *If  $E$  has CM, then we have unconditionally*

$$(1.7) \quad \frac{1}{\pi(x)} \sum_{p \leq x} e_p = \frac{1}{2} C_E x + O_E \left( \frac{x}{(\log x)^{1/14}} \right).$$

Here  $C_E$  is given as in (1.4) and the implied constants depend on  $E$  at most.

**Remark.** (a) Our proof of Theorem 1.1 is a refinement of Freiberg and Kurlberg's method [4] with some simplification.

(b) For comparison of (1.3) and (1.6), we have  $\frac{9}{10} = 0.9$  and  $\frac{5}{6} = 0.833 \dots$ .

(c) The quality of (1.7) can be compared with the following result of Kurlberg and Pomerance [6, Theorem 1.2] concerning the multiplicative order of a number modulo  $p$ : Given a rational number  $g \neq 0, \pm 1$  and prime  $p$  not dividing the numerator of  $g$ , let  $\ell_g(p)$  denote the multiplicative order of  $g$  modulo  $p$ . Assuming GRH for  $\zeta_{\mathbb{Q}(g^{1/k}, e^{2\pi i/k})}(s)$  for all positive integers  $k$ , one has

$$\frac{1}{\pi(x)} \sum_{p \leq x} \ell_g(p) = \frac{1}{2} C_g x + O \left( \frac{x}{(\log x)^{1/2-1/\log_3 x}} \right),$$

where  $C_g$  is a positive constant depending on  $g$ .

## 2. PRELIMINARY

Let  $E$  be an elliptic curve over  $\mathbb{Q}$  with conductor  $N_E$  and let  $k \geq 1$  be an integer. For  $x \geq 1$ , define

$$\pi_E(x; k) := \sum_{\substack{p \leq x \\ p \nmid N_E, k \mid d_p}} 1.$$

The evaluation of this function will play a key role in the proof of Theorem 1.1. Using the Hasse inequality (see (3.1) below), it is not difficult to check that  $p \nmid d_p$  for  $p \nmid N_E$ . Thus the conditions  $p \nmid N_E$  and  $k \mid d_p$  are equivalent to  $p \nmid kN_E$  and  $k \mid d_p$ , that is  $p \nmid kN_E$  and  $E_p(\mathbb{F}_p)$  contains a subgroup isomorphic to  $\mathbb{Z}/k\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}$ . Hence by [9, Lemma 1], we have

$$\sum_{\substack{p \leq x \\ p \text{ splits completely in } L_k}} 1 = \pi_E(x; k) + O(\log(N_E x)).$$

In order to evaluate the sum on the left-hand side, we need effective versions of the Chebotarev density theorem. They were first derived by Lagarias and Odlyzko [7], refined by Serre [12], and subsequently improved by M. Murty, V. Murty and Saradha [10]. With the help of these results, one can deduce the following lemma (cf. [4, Lemma 3.3]).

**Lemma 2.1.** *Let  $E$  be an elliptic curve over  $\mathbb{Q}$  with conductor  $N_E$ .*

(a) *Assuming GRH for the Dedekind zeta function  $\zeta_{L_k}(s)$ , we have*

$$(2.1) \quad \pi_E(x; k) = \frac{\text{Li}(x)}{n_{L_k}} + O(x^{1/2} \log(N_E x))$$

*uniformly for  $x \geq 2$  and  $k \geq 1$ , where the implied constant is absolute.*

(b) *There exist two absolute constants  $B > 0$  and  $C > 0$  such that*

$$(2.2) \quad \pi_E(x; k) = \frac{\text{Li}(x)}{n_{L_k}} + O(xe^{-B(\log x)^{5/14}})$$

*uniformly for  $x \geq 2$  and  $CN_E^2 k^{14} \leq \log x$ , where the implied constant is absolute.*

The next lemma (cf. [4, Proposition 3.2] or [2, Propositions 3.5 and 3.6]) gathers some properties of the division fields  $L_k$  of  $E$  and estimates for  $n_{L_k}$ , which will be useful later. Denote by  $\varphi(k)$  the Euler function.

**Lemma 2.2.** (a) *The field  $L_k$  contains  $\mathbb{Q}(e^{2\pi i/k})$ . Therefore  $\varphi(k) \mid n_{L_k}$  and a rational prime  $p$  which splits completely in  $L_k$  satisfies  $p \equiv 1 \pmod{k}$ .*

(b)  *$n_{L_k}$  divides  $|\text{GL}_2(\mathbb{Z}/k\mathbb{Z})| = k^3 \varphi(k) \prod_{p \mid k} (1 - p^{-2})$ .*

(c) *If  $E$  is a non-CM curve, then there exists a constant  $B_E \geq 1$  (depending only on  $E$ ) such that  $|\text{GL}_2(\mathbb{Z}/k\mathbb{Z})| \leq B_E n_{L_k}$  for each  $k \geq 1$ . Moreover, we have  $|\text{GL}_2(\mathbb{Z}/k\mathbb{Z})| = n_{L_k}$  whenever  $(k, M_E) = 1$  (where  $M_E$  is Serre's constant).*

(d) *If  $E$  has CM, then  $\varphi(k)^2 \ll n_{L_k} \leq k^2$ .*

## 3. PROOF OF THEOREM 1.1

Let  $a_E(p) := p + 1 - |E_p(\mathbb{F}_p)|$ , then

$$e_p = \begin{cases} (p + 1 - a_E(p))/d_p & \text{if } p \nmid N_E, \\ 0 & \text{otherwise.} \end{cases}$$

By using Hasse's inequality

$$(3.1) \quad |a_E(p)| < 2\sqrt{p}$$

for all primes  $p \nmid N_E$ , it is easy to see that

$$(3.2) \quad \sum_{p \leq x} e_p = \sum_{p \leq x, p \nmid N_E} \frac{p}{d_p} + O\left(\frac{x^{3/2}}{\log x}\right).$$

In order to evaluate the last sum, we first notice that the Hasse inequality (3.1) implies  $d_p \leq 2\sqrt{p}$ . Thus we can use the formula

$$\frac{1}{k} = \sum_{dm|k} \frac{\mu(d)}{m}$$

to write

$$(3.3) \quad \sum_{\substack{p \leq x \\ p \nmid N_E}} \frac{p}{d_p} = \sum_{\substack{p \leq x \\ p \nmid N_E}} p \sum_{dm|d_p} \frac{\mu(d)}{m} = \sum_{k \leq 2\sqrt{x}} \sum_{dm=k} \frac{\mu(d)}{m} \sum_{\substack{p \leq x \\ p \nmid N_E, k|d_p}} p.$$

Let  $y \leq 2\sqrt{x}$  be a parameter to be chosen later and define

$$S_1 := \sum_{k \leq y} \sum_{dm=k} \frac{\mu(d)}{m} \sum_{\substack{p \leq x \\ p \nmid N_E, k|d_p}} p,$$

$$S_2 := \sum_{y < k \leq 2\sqrt{x}} \sum_{dm=k} \frac{\mu(d)}{m} \sum_{\substack{p \leq x \\ p \nmid N_E, k|d_p}} p.$$

With the help of Lemma 2.1(a), a simple partial integration allows us to deduce (under GRH)

$$(3.4) \quad \begin{aligned} \sum_{\substack{p \leq x \\ p \nmid N_E, k|d_p}} p &= \int_{2-}^x t \, d\pi_E(t; k) = x\pi_E(x; k) - \int_2^x \pi_E(t; k) \, dt \\ &= \frac{x\text{Li}(x)}{n_{L_k}} - \frac{1}{n_{L_k}} \int_2^x \text{Li}(t) \, dt + O_E(x^{3/2} \log x) \\ &= \frac{\text{Li}(x^2)}{n_{L_k}} + O_E(x^{3/2} \log x). \end{aligned}$$

On the other hand, by Lemma 2.2 we infer that

$$(3.5) \quad \sum_{k \leq y} \frac{1}{n_{L_k}} \sum_{dm=k} \frac{\mu(d)}{m} = C_E + O(y^{-1}).$$

Thus combining (3.4) with (3.5) and using the following trivial inequality

$$(3.6) \quad \left| \sum_{dm=k} \frac{\mu(d)}{m} \right| \leq \frac{\varphi(k)}{k} \leq 1,$$

we find

$$(3.7) \quad \begin{aligned} S_1 &= \text{Li}(x^2) \sum_{k \leq y} \frac{1}{n_{L_k}} \sum_{dm=k} \frac{\mu(d)}{m} + O_E \left( x^{3/2} \log x \sum_{k \leq y} \left| \sum_{dm=k} \frac{\mu(d)}{m} \right| \right) \\ &= C_E \text{Li}(x^2) + O_E \left( \frac{x^2}{y \log x} + x^{3/2} y \log x \right). \end{aligned}$$

Next we treat  $S_2$ . By [4, Lemma 3.1 and Proposition 3.2(a)], we see that  $k \mid d_p$  implies that  $k^2 \mid (p+1 - a_E(p))$  and also  $k \mid (p-1)$ , hence  $k \mid (a_E(p) - 2)$ . With the aid of this and the Brun-Titchmarsh inequality, we can deduce that

$$\begin{aligned} S_2 &\ll x \sum_{y < k \leq 2\sqrt{x}} \left( \sum_{\substack{|a| \leq 2\sqrt{x}, a \neq 2 \\ a \equiv 2 \pmod{k}}} \sum_{\substack{p \leq x, a_E(p)=a \\ k^2 \mid p+1-a}} 1 + \sum_{\substack{p \leq x, a_E(p)=2 \\ k^2 \mid p-1}} 1 \right) \\ &\ll x \sum_{y < k \leq 2\sqrt{x}} \left( \frac{\sqrt{x}}{k} \cdot \frac{x}{k \varphi(k) \log(8x/k^2)} + \frac{x}{k^2} \right). \end{aligned}$$

By virtue of the elementary estimate

$$\sum_{n \leq t} \frac{1}{\varphi(k)} = D \log t + O(1) \quad (t \geq 1)$$

with some positive constant  $D$ , a simple integration by parts leads to

$$(3.8) \quad S_2 \ll \frac{x^{5/2}}{y^2 \log(8x/y^2)} + \frac{x^2}{y}.$$

Inserting (3.7) and (3.8) into (3.3), we find

$$(3.9) \quad \sum_{p \leq x, p \nmid N_E} \frac{p}{d_p} = C_E \text{Li}(x^2) + O_E \left( x^{3/2} y \log x + \frac{x^{5/2}}{y^2 \log(8x/y^2)} + \frac{x^2}{y} \right),$$

where we have used the fact that the term  $x^2 y^{-1} (\log x)^{-1}$  can be absorbed by  $x^{5/2} y^{-2} (\log(8x/y^2))^{-1}$  since  $y \leq 2\sqrt{x}$ . Now the asymptotic formula (1.6) follows from (3.2) and (3.9) with the choice of  $y = x^{1/3} (\log x)^{-2/3}$ .

The proof of (1.7) is very similar to that of (1.6). Next we shall only point out some important differences.

Similar to (3.4), we can apply Lemma 2.1(b) to prove (unconditionally)

$$\sum_{\substack{p \leq x \\ p \nmid N_E, k \mid d_p}} p = \frac{\text{Li}(x^2)}{n_{L_k}} + O_E \left( x^2 \exp\{-B(\log x)^{5/14}\} \right)$$

for  $k \leq (C^{-1} N_E^{-2} \log x)^{1/14}$ . As before from this and (3.5)-(3.6), we can deduce that

$$(3.10) \quad S_1 = C_E \text{Li}(x^2) + O_E \left( x^2 y^{-1} (\log x)^{-1} + x^2 y e^{-B(\log x)^{5/14}} \right)$$

for  $y \leq (C^{-1}N_E^{-2} \log x)^{1/14}$ .

The treatment of  $S_2$  is different. First we divide the sum over  $k$  in  $S_2$  into two parts according to  $y < k \leq x^{1/4}(\log x)^{3/4}$  or  $x^{1/4}(\log x)^{3/4} < k \leq 2\sqrt{x}$ .

When  $E$  has CM, we have (see [3, page 692])

$$\sum_{\substack{p \leq x \\ p \nmid N_E, k \mid d_p}} 1 \ll \frac{x}{\varphi(k)^2 \log x}$$

for  $k \leq x^{1/4}(\log x)^{3/4}$ . Thus the contribution from  $y < k \leq x^{1/4}(\log x)^{3/4}$  to  $S_2$  is

$$\ll \frac{x^2}{\log x} \sum_{y < k \leq x^{1/4}(\log x)^{3/4}} \frac{1}{\varphi(k)^2} \ll \frac{x^2}{y \log x}.$$

Clearly the inequality (3.8) (taking  $y = x^{1/4}(\log x)^{3/4}$ ) implies that the contribution from  $x^{1/4}(\log x)^{3/4} < k \leq 2\sqrt{x}$  to  $S_2$  is

$$\ll \sum_{x^{1/4}(\log x)^{3/4} < k \leq 2\sqrt{x}} \sum_{\substack{p \leq x \\ p \nmid N_E, k \mid d_p}} p \ll \frac{x^2}{(\log x)^{5/2}}.$$

By combining these two estimates, we obtain

$$(3.11) \quad S_2 \ll \frac{x^2}{y \log x} + \frac{x^2}{(\log x)^{5/2}}.$$

Inserting (3.10) and (3.11) into (3.3), we find

$$(3.12) \quad \sum_{p \leq x, p \nmid N_E} \frac{p}{d_p} = C_E \text{Li}(x^2) + O_E \left( \frac{x^2}{y \log x} + \frac{x^2}{(\log x)^{5/2}} + x^2 y e^{-B(\log x)^{5/14}} \right)$$

for  $y \leq (C^{-1}N_E^{-2} \log x)^{1/14}$ .

Now the asymptotic formula (1.7) follows from (3.2) and (3.12) with the choice of  $y = (C^{-1}N_E^{-2} \log x)^{1/14}$ .

## REFERENCES

- [1] A. C. Cojocaru, *Cyclicity of CM elliptic curves modulo  $p$* , Trans. AMS. **355** (2003), 2651–2662.
- [2] A. C. Cojocaru and M. Ram Murty, *Cyclicity of elliptic curves modulo  $p$  and elliptic curve analogue of Linnik’s problem*, Math. Ann. **330** (2004), no. 7, 601–625.
- [3] W. Duke, *Almost all reductions modulo  $p$  of an elliptic curve have a large exponent*, C. R. Acad. Sci. Paris, Ser. **1337** (2003), 689–692.
- [4] T. Freiberg and P. Kurlberg, *On the average exponent of elliptic curves modulo  $p$* , arXiv:1203.4382v1. (21 pages)
- [5] N. Koblitz, *Elliptic curve cryptosystems*, Math. Comp. **48** (1987), 203–209.
- [6] P. Kurlberg and C. Pomerance, *On a problem of Arnold: the average multiplicative order of a given integer*, to appear in Algebra and Number Theory.
- [7] J. Lagarias and A. Odlyzko, *Effective versions of the Chebotarev Density Theorem*, in: Algebraic Number Fields (A. Fröhlich edit.), New York, Academic Press (1977), 409–464.

- [8] V. S. Miller, *Use of elliptic curves in cryptography*, Advances in cryptology — CRYPTO 85 (Santa Barbara, Calif., 1985), Lecture Notes in Comput. Sci. **218**, Springer, Berlin, 1986, 417–426.
- [9] M.-R. Murty, *On Artin's conjecture*, J. Number Theory **16** (1983), 147–168.
- [10] M.-R. Murty, V.-K. Murty and N. Saradha, *Modular forms and the Chebotarev density theorem*, Amer. J. Math. **110** (1988), 253–281.
- [11] R. Schoof, *The exponent of the group of points on the reductions of an elliptic curve*, in : Arithmetic algebraic geometry (Texel, 1989), in : Progr. Math. **89** (1991), Birkhäuser, Boston, MA, 325–335.
- [12] J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Etudes Sci. Publ. Math. **54** (1981), 123–201.

INSTITUT ELIE CARTAN UMR 7502, CNRS, UNIVERSITÉ DE LORRAINE, INRIA, 54506  
VANDŒUVRE-LÈS-NANCY, FRANCE

*E-mail address:* Jie.Wu@univ-lorraine.fr