Journal of Number Theory 169 (2016) 353–368

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Average results on the order of a modulo p

Sungjin Kim [1]

Department of Mathematics, University of California, Los Angeles, Math Science Building 6617A, United States

ARTICLE INFO

Article history:
Received 11 January 2016
Received in revised form 17 May 2016
Accepted 20 May 2016
Available online 21 July 2016
Communicated by David Goss

Keywords:
Order
Modulo p
Average
Reciprocal

ABSTRACT

Let $a > 1$ be an integer. Denote by $l_a(p)$ the multiplicative order of a modulo primes p. We prove that if $\frac{x}{\log x \log\log x} = o(y)$, then

$$\frac{1}{y}\sum_{a\le y}\sum_{p\le x}\frac{1}{l_a(p)} = \log x + C\log\log x + O(1) + O\left(\frac{x}{y\log\log x}\right),$$

which is an improvement over a theorem by Felix [Fe]. Additionally, we also prove two other related average results.

1. Introduction

Throughout this paper, we use the letter p to denote a prime number. Let $a > 1$ be an integer. If p does not divide a, we denote the multiplicative order of a modulo p by $l_a(p)$. If p divides a, then $l_a(p)$ is not defined and the term corresponding to this case will not appear in the sums throughout this paper. Artin's Conjecture on Primitive Roots

E-mail address: 707107@gmail.com.

[1] Present addresses: Concordia University Irvine, 1530 Concordia, Irvine, CA 92612; Santa Monica College, 1900 Pico Blvd, Santa Monica, CA 90405.

http://dx.doi.org/10.1016/j.jnt.2016.05.019
0022-314X/© 2016 Published by Elsevier Inc.

(AC) states that if a is nonunit, nonsquare, then $l_a(p) = p - 1$ for a positive proportion of primes p where the proportion is a rational multiple of the Artin's constant $A = \prod_p \left(1 - \frac{1}{p(p-1)}\right)$. Assuming the Generalized Riemann Hypothesis (GRH), Hooley [Ho] proved that $l_a(p) = p-1$ for positive proportion of primes $p \le x$. It is expected that $l_a(p)$ is large for a majority of primes $p \le x$. In [EM], Erdős and Murty showed that $l_a(p) \ge p^{1/2+\epsilon(p)}$ for all but $o(\pi(x))$ primes $p \le x$ where $\epsilon(p) \to 0$. With a much simpler method, they showed a weaker result namely that $l_a(p) > \frac{\sqrt{p}}{\log p}$ for all but $O(x/\log^3 x)$ primes $p \le x$. Pappalardi [P] showed that there exist $\alpha, \delta > 0$ such that $l_a(p) \ge p^{1/2} \exp(\log^\delta p)$ for all but $O(x/\log^{1+\alpha} x)$. Kurlberg and Pomerance [KP2] applied Fouvry [Fo] to show that there is $\gamma > 0$ such that $l_a(p) > p^{1/2+\gamma}$ for a positive proportion of primes $p \le x$.

Therefore, it is natural to expect that the average reciprocal of $l_a(p)$ is quite small. Murty and Srinivasan [MS] showed that $\sum_{p<x} \frac{1}{l_a(p)} = O(\sqrt{x})$ and that $\sum_{p<x} \frac{1}{l_a(p)} = O(x^{1/4})$ implies AC for a. Pappalardi [P] proved that for some positive constant γ,

$$\sum_{p<x} \frac{1}{l_a(p)} = O\left(\frac{\sqrt{x}}{\log^{1+\gamma} x}\right).$$

For fixed a, it seems that it is very difficult to obtain $O(x^c)$ for some $c < 1/2$ with current knowledge. However, we expect that averaging over a would give some information. The following result by Felix [Fe] supports that $l_a(p)$ is mostly large:

If $\frac{x}{\log x} = o(y)$, then

$$\frac{1}{y} \sum_{a \le y} \sum_{p \le x} \frac{1}{l_a(p)} = \log x + O(\log\log x) + O\left(\frac{x}{y}\right).$$

Felix remarked that the first error term $O(\log\log x)$ is in fact of the shape $C \log\log x + O(1)$ by applying Fiorilli's method [Fi], but did not explicitly find C. We find the C in Theorem 1.1. This detailed estimate takes effect when $\frac{x}{(\log\log x)^2} = o(y)$. We apply a deep result on exponential sums by Bourgain [B] to obtain Corollary 2.2 which will be the key for all average results in this paper.

Theorem 1.1. *If* $\frac{x}{\log x \log\log x} = o(y)$, *then*

$$\frac{1}{y} \sum_{a \le y} \sum_{p \le x} \frac{1}{l_a(p)} = \log x + C \log\log x + O(1) + O\left(\frac{x}{y \log\log x}\right),$$

where

$$C = 2\gamma - 2 \sum_p \frac{\log p}{p^2 - p + 1} + \frac{\zeta(2)\zeta(3)}{\zeta(6)} \sum_{k=1}^{\infty} \frac{\mu(k)}{k^2} \left(-2 \sum_{p|k} \frac{(p-1)p \log p}{p^2 - p + 1} + \log k\right) \prod_{p|k} \left(1 + \frac{p-1}{p^2 - p + 1}\right).$$