Some Theorems on Multiplicative Orders Modulo p on Average

Sungjin Kim

Santa Monica College/California State University Northridge
Department of Mathematics
i707107@math.ucla.edu

Dec 17, 2017

Extended Definition of Multiplicative Order

• Let $a, n \geq 1$ be integers. The **ordinary definition** of $\ell_a(n)$ takes $\ell_a(n) = 0$ if $(a, n) \neq 1$.

Extended Definition of Multiplicative Order

• Let $a, n \geq 1$ be integers. The **ordinary definition** of $\ell_a(n)$ takes $\ell_a(n) = 0$ if $(a, n) \neq 1$.

• If $(a, n) = 1$ then denote by $\ell_a(n)$ the multiplicative order of a modulo n. If $(a, n) \neq 1$, we write $n = n_1 n_2$ where any prime divisors of n_1 divide a and $(a, n_2) = 1$. Define $\ell_a(n) = \ell_a(n_2)$. This **extended definition** of $\ell_a(n)$ is used by Murty, Saidak [MS, Section 8].

Extended Definition of Multiplicative Order

• Let $a, n \geq 1$ be integers. The **ordinary definition** of $\ell_a(n)$ takes $\ell_a(n) = 0$ if $(a, n) \neq 1$.
• If $(a, n) = 1$ then denote by $\ell_a(n)$ the multiplicative order of a modulo n. If $(a, n) \neq 1$, we write $n = n_1 n_2$ where any prime divisors of n_1 divide a and $(a, n_2) = 1$. Define $\ell_a(n) = \ell_a(n_2)$. This **extended definition** of $\ell_a(n)$ is used by Murty, Saidak [MS, Section 8].
Example) We compute $\ell_4(6)$. The ordinary definition gives $\ell_4(6) = 0$, but the extended definition gives $\ell_4(6) = \ell_4(3) = 2$.

Extended Definition of Multiplicative Order

• Let $a, n \geq 1$ be integers. The **ordinary definition** of $\ell_a(n)$ takes $\ell_a(n) = 0$ if $(a, n) \neq 1$.
• If $(a, n) = 1$ then denote by $\ell_a(n)$ the multiplicative order of a modulo n. If $(a, n) \neq 1$, we write $n = n_1 n_2$ where any prime divisors of n_1 divide a and $(a, n_2) = 1$. Define $\ell_a(n) = \ell_a(n_2)$. This **extended definition** of $\ell_a(n)$ is used by Murty, Saidak [MS, Section 8].
Example) We compute $\ell_4(6)$. The ordinary definition gives $\ell_4(6) = 0$, but the extended definition gives $\ell_4(6) = \ell_4(3) = 2$.
• $\omega(n) := \sum_{p|n} 1$ be the number of distinct prime divisors of n and $\Omega(n) := \sum_{p^k|n} 1$ be the number of prime power divisors of n, and set $\omega(1) = \Omega(1) = 0$.

Definitions and Notations-continued

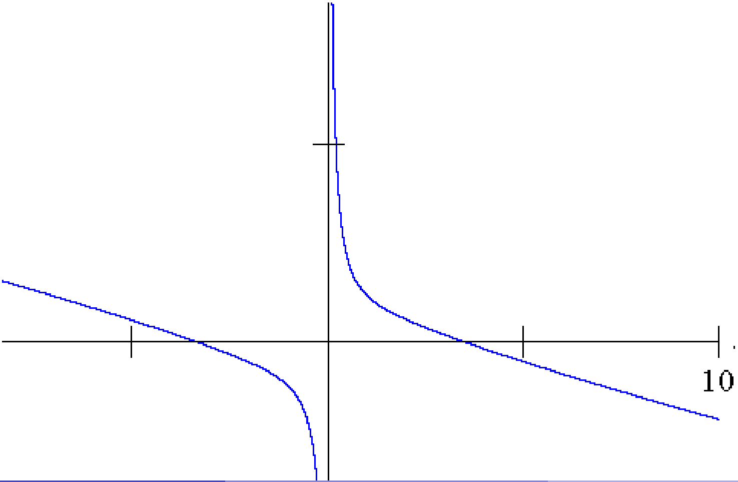
- The number $\alpha \approx 3.42$ is the unique positive root of an equation:

$$f_1(K) := -\frac{K}{4} + \frac{1}{K}\left(\log\left(\frac{K^2}{2}+1\right)+1\right) = 0.$$

Definitions and Notations-continued

- The number $\alpha \approx 3.42$ is the unique positive root of an equation:

$$f_1(K) := -\frac{K}{4} + \frac{1}{K}\left(\log\left(\frac{K^2}{2}+1\right)+1\right) = 0.$$



Previous Results

Theorem

If $y > \exp((\alpha+\epsilon)\sqrt{\log x})$, *then for any positive constant* $B > 1$,

$$y^{-1}\sum_{a\le y}\sum_{p\le x}\frac{\ell_a(p)}{p-1} = C\mathrm{Li}(x) + O\left(\frac{x}{\log^B x}\right). \tag{1}$$

Moreover, for any positive constant $B > 2$,

$$y^{-1}\sum_{a\le y}\left(\sum_{p<x}\frac{\ell_a(p)}{p-1} - C\mathrm{Li}(x)\right)^2 \ll \frac{x^2}{\log^B x}. \tag{2}$$

Here, C *is the Stephens' constant:*

$$C = \prod_p\left(1 - \frac{p}{p^3-1}\right)$$

Theorem

Let $y > \exp((\alpha + \epsilon)\sqrt{\log x})$ *and* $P_a(x) := \{p \le x | \ell_a(p) = p - 1\}$. *Then the following estimates also hold for any* $B > 1$:

$$y^{-1} \sum_{a \le y} P_a(x) = A\mathrm{Li}(x) + O\left(\frac{x}{\log^B x}\right), \tag{3}$$

where $A = \prod_p \left(1 - \frac{1}{p(p-1)}\right)$ *is the Artin's constant.*
Moreover, for any positive constant $B > 2$,

$$y^{-1} \sum_{a \le y} (P_a(x) - A\mathrm{Li}(x))^2 \ll \frac{x^2}{\log^B x}. \tag{4}$$

Theorem

If $y > \exp((\alpha+\epsilon)\sqrt{\log x})$*, then for any positive constant* $B > 1$*,*

$$y^{-2}\sum_{a\le y}\sum_{b\le y}\sum_{\substack{p\le x\\ \exists n, p | a^n - b}} 1 = C\mathrm{Li}(x) + O\left(\frac{x}{\log^B x}\right). \tag{5}$$

Moreover, for any positive constant $B > 2$*,*

$$y^{-2}\sum_{a\le y}\sum_{b\le y}\left(\sum_{\substack{p\le x\\ \exists n, p | a^n - b}} 1 - C\mathrm{Li}(x)\right)^2 \ll \frac{x^2}{\log^B x}. \tag{6}$$

Erdos-Kac Theorem [EK]

For any real number u,

$$\lim_{x\to\infty} \frac{1}{x} \# \left\{ n \le x : \frac{g(n) - \log\log x}{\sqrt{\log\log x}} \le u \right\} = G(u)$$

where $g(n) = \omega(n)$ or $\Omega(n)$ and $G(u) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{u} \exp\left(-\frac{t^2}{2}\right) dt$.

Results of Erdos-Pomerance [EP]

Let $\phi(n)$ be the Euler Phi function. Then $\omega(\phi(n))$ and $\Omega(\phi(n))$ also follow a normal distribution after a suitable normalization: For any real number u,

$$\lim_{x\to\infty} \frac{1}{x}\#\left\{ n \le x : \frac{g(\phi(n)) - \frac{1}{2}(\log\log x)^2}{\frac{1}{\sqrt{3}}(\log\log x)^{\frac{3}{2}}} \le u \right\} = G(u).$$

This holds with $\phi(n)$ replaced by the Carmichael Lambda function $\lambda(n)$. Furthermore, they conjectured that: For any real number u,

$$\lim_{x\to\infty} \frac{1}{x}\#\left\{ n \le x : (n,a) = 1,\ \frac{g(\ell_a(n)) - \frac{1}{2}(\log\log x)^2}{\frac{1}{\sqrt{3}}(\log\log x)^{\frac{3}{2}}} \le u \right\} = \frac{\phi(a)}{a} G(u).$$

Results of Murty-Saidak [MS]

Assuming the quasi-Generalized Riemann Hypothesis (GRH) and $\ell_a(n)$ is in the extended definition: For any real number u,

$$\lim_{x\to\infty} \frac{1}{x} \# \left\{ n \le x : \frac{g(\ell_a(n)) - \frac{1}{2}(\log\log x)^2}{\frac{1}{\sqrt{3}}(\log\log x)^{\frac{3}{2}}} \le u \right\} = G(u).$$

Main Results

Theorem

If $y > \exp((\alpha + \epsilon)\sqrt{\log x})$, *then for any fixed real number* u,

$$\lim_{x\to\infty} \frac{1}{x} \# \left\{ n \le x : \frac{\frac{1}{y}\sum_{a\le y} g(\ell_a(n)) - \frac{1}{2}(\log\log x)^2}{\frac{1}{\sqrt{3}}(\log\log x)^{\frac{3}{2}}} \le u \right\} = G(u). \quad (7)$$

Theorem

If $y > \exp((\alpha + \epsilon)\sqrt{\log x})$, *then for any* $B > 1$,

$$\frac{1}{y}\sum_{a\le y}\sum_{p\le x} \tau(\ell_a(p)) = K_1 x + (K_1 + K_2)\mathrm{Li}(x) + O\left(\frac{x}{\log^B x}\right) \quad (8)$$

where

$$K_1 = \prod_p \left(1 + \frac{1}{p^3 - p}\right) \approx 1.231291.$$

The Method of Stephens [S]

The use of character sums: Stephens defined a character sum $c_r(\chi)$ where χ is a Dirichlet character modulo p for $r|p-1$:

$$c_r(\chi) = \frac{1}{p-1} \sum_{\substack{a<p \\ \ell_a(p)=\frac{p-1}{r}}} \chi(a). \tag{9}$$

From [S, Lemma 1], we have for any Dirichlet character χ modulo p,

$$|c_r(\chi)| \leq \frac{1}{\mathrm{ord}(\chi)}.$$

For the principal character χ_0 modulo p, we have

$$c_r(\chi_0) = \frac{\phi\left(\frac{p-1}{r}\right)}{p-1}.$$

The Method of Murty-Saidak

The use of Kubilius-Shapiro Theorem [E, Chapter 12]:

Lemma (Kubilius-Shapiro)

Let $f(n)$ be a strongly additive function. Let

$$A(x) := \sum_{p \le x} \frac{f(p)}{p}, \quad B(x)^2 := \sum_{p \le x} \frac{f(p)^2}{p}.$$

Suppose that for any $\epsilon > 0$,

$$\lim_{x \to \infty} \frac{1}{B(x)^2} \sum_{\substack{p \le x \\ |f(p)| > \epsilon B(x)}} \frac{f(p)^2}{p} = 0.$$

Then for any fixed real number u,

$$\lim_{x \to \infty} \frac{1}{x} \# \left\{ n \le x : \frac{f(n) - A(x)}{B(x)} \le u \right\} = G(u).$$

Method - For the First Theorem

• The main point is to reduce the problems to estimating $A(x)$ and $B(x)$ with suitable strongly additive function $f(n)$.

Method - For the First Theorem

• The main point is to reduce the problems to estimating $A(x)$ and $B(x)$ with suitable strongly additive function $f(n)$.
• Then use a simplified version of Stephens' method in estimating $A(x)$ and $B(x)$.

Method - For the Second Theorem

- Proving the Mean Value Theorem

Theorem

Let K_1, K_2 be the constants in Theorem 1. Then we have for any $A > 0$,

$$\sum_{p \le x} \frac{1}{p-1} \sum_{d \mid p-1} \tau(d)\phi(d) = K_1 x + (K_1 + K_2)\mathrm{Li}(x) + O\left(\frac{x}{\log^A x}\right). \quad (10)$$

As a byproduct, we obtain a curious identity

$$\sum_{p \le x} \frac{\tau(p-1)\phi(p-1)}{p-1} = \frac{6}{\pi^2} x + \left(\frac{6}{\pi^2} + K_4\right)\mathrm{Li}(x) + O\left(\frac{x}{\log^A x}\right).$$

- Then use a simplified version of Stephens' method.

References

- M. R. Murty, F. Saidak, *Non-Abelian Generalizations of the Erdős-Kac Theorem*, Canad. J. Math. Vol. 56(2), 2004, pp. 356–372.
- P. D. T. A. Elliott, *Probabilistic Number Theory II: Central Limit Theorems*, Springer 1980.
- P. Erdős, M. Kac, *The Gaussian law of errors in the theory of additive number theoretic functions*, Amer. J. Math. 62(1940), pp. 738–742.
- P. Erdős, C. Pomerance, *On the Normal Order of Prime Factors of $\phi(n)$*, Rocky Mountain Journal of Mathematics, Volume 15, Number 2, Spring 1985.
- P. J. Stephens, *Prime Divisors of Second Order Linear Recurrences II*, Journal of Number Theory, Volume 8, Issue 3, August 1976.