ON THE ORDER OF a MODULO n, ON AVERAGE

KIM, SUNGJIN
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF CALIFORNIA, LOS ANGELES
MATH SCIENCE BUILDING 6617A
E-MAIL: 707107@GMAIL.COM

Abstract. Let $a > 1$ be an integer. Denote by $l_a(n)$ the multiplicative order of a modulo integer $n \geq 1$. We prove that there is a positive constant δ such that if $x^{1-\delta} = o(y)$, then

$$\frac{1}{y}\sum_{a<y}\frac{1}{x}\sum_{\substack{a<n<x\\(a,n)=1}} l_a(n) = \frac{x}{\log x}\exp\left(B\frac{\log\log x}{\log\log\log x}(1+o(1))\right)$$

where

$$B = e^{-\gamma}\prod_p\left(1-\frac{1}{(p-1)^2(p+1)}\right).$$

It was known for $y = x$ in [KP, Page 3] in which they refer to [LS].

1. Introduction

Let $a > 1$ be an integer. If n be coprime to a, we write $d = l_a(n)$ if d is the multiplicative order of a modulo n. Then d is the smallest positive integer in the congruence $a^d \equiv 1 \pmod{n}$.

The Carmichael's lambda function $\lambda(n)$ is defined by the exponent of the group $(\mathbb{Z}/n\mathbb{Z})^*$. It was known in [EPS] that

$$\frac{1}{x}\sum_{n<x}\lambda(n) = \frac{x}{\log x}\exp\left(B\frac{\log\log x}{\log\log\log x}(1+o(1))\right).$$

Assuming GRH for Kummer extensions $\mathbb{Q}(\zeta_d, a^{1/d})$, P. Kurlberg and C. Pomerance [KP] showed that

$$\frac{1}{x}\sum_{n<x} l_a(n) = \frac{x}{\log x}\exp\left(B\frac{\log\log x}{\log\log\log x}(1+o(1))\right)$$

with $B = e^{-\gamma}\prod_p\left(1-\frac{1}{(p-1)^2(p+1)}\right)$. The upper bound implicit is unconditional because $l_a(n) \leq \lambda(n)$. An unconditional average result over all possible nonzero residue classes is obtained by F. Luca and I. Shparlinski [LS]:

$$\frac{1}{x}\sum_{n<x}\frac{1}{\phi(n)}\sum_{a<n} l_a(n) = \frac{x}{\log x}\exp\left(B\frac{\log\log x}{\log\log\log x}(1+o(1))\right).$$

As pointed out in [KP], by partial summation, we have the following statistics on average order:

$$\frac{1}{x^2}\sum_{a<x}\sum_{a<n<x} l_a(n) = \frac{x}{\log x}\exp\left(B\frac{\log\log x}{\log\log\log x}(1+o(1))\right).$$

For fixed a, it seems that it is very difficult to remove GRH in P. Kurlberg and C. Pomerance's result with current knowledge. However, we expect that averaging over a would give some information. So, we take average over $a < y$, but we do not want to have too large y such as $y > x$. For all the average results in this paper, we assume that $y < x$, and try to obtain y as small as possible. By applying a deep result on exponential sums by Bourgain [B], we prove the unconditional average result on a shorter interval.

Theorem 1.1. *There is a positive constant δ such that, if $x^{1-\delta} = o(y)$, then*

$$\frac{1}{y}\sum_{a<y}\frac{1}{x}\sum_{\substack{a<n<x\\(a,n)=1}} l_a(n) = \frac{x}{\log x}\exp\left(B\frac{\log\log x}{\log\log\log x}(1+o(1))\right)$$

where

$$B = e^{-\gamma}\prod_p\left(1-\frac{1}{(p-1)^2(p+1)}\right).$$

2. Backgrounds

2.1. **Equidistribution.** A sequence $\{a_n\}$ of real numbers are said to be equidistributed modulo 1 if the following is satisfied:

Definition 2.1. *Let $0 \le a < b \le 1$. Suppose that*

$$\lim_{N\to\infty}\frac{1}{N}|\{n \le N \ : \ a_n \in (a,b) \bmod 1\}| = b-a.$$

Then we say that $\{a_n\}$ is equidistributed modulo 1.

A well-known criterion by Weyl [W] is

Theorem 2.1. *For any integer $k \ne 0$, suppose that*

$$\lim_{N\to\infty}\frac{1}{N}\sum_{n\le N} e^{2\pi i k a_n} = 0.$$

Then the sequence $\{a_n\}$ is equidistributed modulo 1.

There was a series of efforts to obtain a quantitative form of the equidistribution theorem. Erdős and Turán [ET] succeeded in obtaining the following result:

Theorem 2.2. *Let $\{a_n\}$ be a sequence of real numbers. Then for some positive constants c_1 and c_2,*

$$\sup_{0\le a<b\le 1}||\{n \le N : a_n \in (a,b) \bmod 1\}| - (b-a)N| \le c_1\frac{N}{M+1} + c_2\sum_{m=1}^{M}\frac{1}{m}\left|\sum_{n\le N} e^{2\pi i m a_n}\right|.$$

H. Montgomery [M] obtained $c_1 = 1$, $c_2 = 3$. C. Mauduit, J. Rivat, A. Sárközy [MRS] obtained $c_1 = c_2 = 1$. Thus, we have a quantitative upper bound of discrepancy when we have good upper bounds for exponential sums.

2.2. **Exponential Sums in $\mathbb{Z}_n^*$.** We define arithmetic functions $a_n(d)$ and $b_n(d)$ for $1 \le d|\lambda(n)$ as follows:

$$a_n(d) = |\{0 < a < n : \ l_a(n) = d\}|,$$

$$b_n(d) = |\{0 < a < n : \ a^d \equiv 1 \pmod{n}\}|.$$

Then

$$a_n(d) = \sum_{d'|d}\mu\left(\frac{d}{d'}\right) b_n(d').$$

We give some algebraic remarks about the function $b_n(d)$. First, we see that

$$H_{n,d} := \{0 < a < n : \ a^d \equiv 1 \pmod{n}\}$$

forms a subgroup of $\mathbb{Z}_n^*$ of order $b_n(d)$. The following proposition is from elementary group theory:

Proposition 2.1. *Let $H_{n,d}$ and $b_n(d)$ be defined as above. For any $k|n$, denote by π_k the reduction modulo n/k. Then we have*

$$\pi_k : H_{n,d} \longrightarrow H_{n/k,d}$$

where π_k is a group homomorphism with kernel

$$K = \{0 < a < n : \ a^d \equiv 1(n), \ a \equiv 1(n/k)\}.$$

By the First Isomorphism Theorem, we have

$$|K| = \frac{b_n(d)}{|\pi_k(H_{n,d})|} \le k.$$

Note that the map π_k restricted to $H_{n,d}$ is not always surjective. To see this, let $p > 2$ prime number, and $a = p + 1$, $d = p$, $n/k = p^2$, $n = p^3$. Then

$$a^p \equiv p^2 + 1 \ (\text{mod } p^3).$$

Thus,

$$a^p \equiv 1 \ (\text{mod } p^2).$$

But for any $a' \equiv a \ (\text{mod } p^2)$, so that $a' = p^2 j + p + 1$ for some integer j, we have

$$(a')^p \equiv (p+1)^p \ (\text{mod } p^3) \equiv p^2 + 1 \ (\text{mod } p^3).$$

From this, we see that the element $a = p+1 \in H_{n/k}$ is not a preimage of π_k. The proof of $|K| \le k$ is clear by $a \equiv 1(n/k)$.

J. Bourgain [B] proved a nontrivial exponential sum result when a subgroup H of $\mathbb{Z}_n^*$ has order greater than n^ϵ for $\epsilon > 0$.

Theorem 2.3. *Let $n \ge 1$. For any $\epsilon > 0$, there exist a constant $\delta = \delta(\epsilon) > 0$ such that for any subgroup H of $\mathbb{Z}_n^*$ with $|H| > n^\epsilon$,*

$$\max_{(m,n)=1} \left| \sum_{a \in H} e^{2\pi i m \frac{a}{n}} \right| < n^{-\delta} |H|.$$

Corollary 2.1. *Let $\epsilon > 0$ be arbitrary, and let $y \ge 1$. Assume that $d|\lambda(n)$ and $b_n(d) > n^\epsilon$. Then there exists $\delta = \delta(\epsilon) > 0$ such that*

$$\sum_{a<y, \ a^d \equiv 1(n)} 1 = \frac{y}{n} b_n(d) + O(b_n(d) n^{-\delta}).$$

If $d|\lambda(n)$, the congruence $a^d \equiv 1$ yields $b_n(d)$ roots in $\mathbb{Z}_n$. Thus, we need to count $a < y$ satisfying those $b_n(d)$ congruences modulo n. Considering $\frac{y}{n} = \lfloor \frac{y}{n} \rfloor + \frac{y}{n} - \lfloor \frac{y}{n} \rfloor$, it is enough to prove the result for $y < n$. We apply the Erdős-Turán inequality to the set $\{\frac{a}{n} : 0 < a < n, \ a^d \equiv 1(n)\}$. Then

$$\left| |\{0 < a < n : a^d \equiv 1(n), \frac{a}{n} \in (0, \frac{y}{n}) \text{ mod } 1\}| - \frac{y}{n} b_n(d) \right| \le \frac{b_n(d)}{n} + \sum_{m=1}^{n-1} \frac{1}{m} \left| \sum_{a \in \mathbb{Z}_n, \ a^d \equiv 1(n)} e^{2\pi i m \frac{a}{n}} \right|.$$

Unlike the prime modulus case, we immediately encounter a problem. The exponential sum result (Theorem 2.3) is only for $(m, n) = 1$, but the sum takes all $1 \le m < n$. Then we have too many terms with $(m, n) \ne 1$. Therefore, we need some modification in applying the Erdős-Turán inequality. A starting point is to observe that we can take M arbitrary in the Erdős-Turán inequality.

Proof of Corollary 2.1)

Assuming that $k|n$ and $b_n(d) > n^\epsilon$, we have

$$n^\epsilon < b_n(d) \le k |\pi_k(H_{n,d})|.$$

Then

$$\frac{n^\epsilon}{k} < |\pi_k(H_{n,d})|.$$

If we can assume that

$$\left(\frac{n}{k}\right)^{\epsilon''} < \frac{n^\epsilon}{k}$$

for some positive $\epsilon'' < \epsilon$, then we can use Theorem 2.3 with ϵ'' and $\delta'' = \delta(\epsilon'')$. This is achieved by

$$k < n^{\frac{\epsilon-\epsilon''}{1-\epsilon''}}.$$

Let $\epsilon' = \frac{\epsilon-\epsilon''}{1-\epsilon''}$ and we take $M+1 = \lfloor n^{\epsilon'} \rfloor$ in the Erdős-Turán inequality. Then we have reduced the number of terms appearing in the sum on the right side. We rewrite the sum by substituting $(m,n) = k$, $\frac{m}{k} = j$ and apply Theorem 2.3 to the exponential sums inside. This is possible due to

$$\left(\frac{n}{k}\right)^{\epsilon''} < |\pi_k(H_{n,d})|$$

and $\pi_k(H_{n,d})$ being a subgroup of $\mathbb{Z}^*_{n/k}$. The sum on the right becomes

$$\begin{aligned}
\sum_{m<n^{\epsilon'}} \frac{1}{m}\left|\sum_{a\in H_{n,d}} e^{2\pi i m\frac{a}{n}}\right| &\leq \sum_{\substack{k|n \\ k<n^{\epsilon'}}} \frac{1}{k} \sum_{(j,\frac{n}{k})=1} \frac{1}{j}\left|\sum_{a\in H_{n,d}} e^{2\pi i j\frac{a}{n/k}}\right| \\
&= \sum_{\substack{k|n \\ k<n^{\epsilon'}}} \frac{1}{k} \sum_{(j,\frac{n}{k})=1} \frac{1}{j}\frac{b_n(d)}{|\pi_k(H_{n,d})|}\left|\sum_{a\in \pi_k(H_{n,d})} e^{2\pi i j\frac{a}{n/k}}\right| \\
&\leq \sum_{\substack{k|n \\ k<n^{\epsilon'}}} \frac{1}{k} \sum_{(j,\frac{n}{k})=1} \frac{1}{j}\frac{b_n(d)}{|\pi_k(H_{n,d})|}|\pi_k(H_{n,d})|\left(\frac{n}{k}\right)^{-\delta''} \\
&\leq n^{-\delta''(1-\epsilon')}b_n(d)(1+\log n)^2.
\end{aligned}$$

Thus, the Erdős-Turán inequality gives

$$\left||\{0<a<n : a^d \equiv 1(n), \frac{a}{n} \in (0,\frac{y}{n}) \bmod 1\}| - \frac{y}{n}b_n(d)\right| \leq \frac{b_n(d)}{n^{\epsilon'}} + b_n(d)n^{-\delta''(1-\epsilon')}(1+\log n)^2.$$

Therefore we can take $0<\delta<\min(\epsilon', \delta''(1-\epsilon'))$. This completes the proof of Corollary 2.1.

Corollary 2.1 plays a key role in proving Theorem 1.1. Note that the upper bound provided in Corollary 2.1 is significantly better than the trivial bound which is:

$$\sum_{a<y,\ a^d\equiv 1(n)} 1 = \frac{y}{n}b_n(d) + O(b_n(d)).$$

3. Proof of Theorems

3.1. Proof of Theorem 1.1. We start with the change of order in summation:

$$\begin{aligned}
\sum_{a<y}\sum_{n<x} l_a(n) &= \sum_{d<x} d \sum_{\substack{n<x \\ d|\lambda(n)}} \sum_{\substack{a<y \\ l_a(n)=d}} 1 \\
&= \sum_{d<x} d \sum_{\substack{n<x \\ d|\lambda(n)}} \sum_{\substack{d'|d \\ b_n(d')<n^{\epsilon}}} \mu\left(\frac{d}{d'}\right) \sum_{\substack{a<y \\ a^{d'}\equiv 1(n)}} 1 + \sum_{d<x} d \sum_{\substack{n<x \\ d|\lambda(n)}} \sum_{\substack{d'|d \\ b_n(d')\geq n^{\epsilon}}} \mu\left(\frac{d}{d'}\right) \sum_{\substack{a<y \\ a^{d'}\equiv 1(n)}} 1 \\
&= \sum_{d<x} d \sum_{\substack{n<x \\ d|\lambda(n)}} \sum_{\substack{d'|d \\ b_n(d')<n^{\epsilon}}} \mu\left(\frac{d}{d'}\right)\left(\frac{y}{n}b_n(d') + O(b_n(d'))\right) \\
&\quad + \sum_{d<x} d \sum_{\substack{n<x \\ d|\lambda(n)}} \sum_{\substack{d'|d \\ b_n(d')\geq n^{\epsilon}}} \mu\left(\frac{d}{d'}\right)\left(\frac{y}{n}b_n(d') + O(b_n(d')n^{-\delta})\right) \\
&= \sum_{d<x} d \sum_{\substack{n<x \\ d|\lambda(n)}} \frac{y}{n}a_n(d) + O(E_1) + O(E_2),
\end{aligned}$$

where

$$
\begin{aligned}
E_1 &= \sum_{d<x} d \sum_{\substack{n<x \\ d|\lambda(n)}} \sum_{\substack{d'|d \\ b_n(d')<n^\epsilon}} \left|\mu\left(\frac{d}{d'}\right)\right| b_n(d') \\
&\ll \sum_{d<x} d \sum_{\substack{n<x \\ d|\lambda(n)}} \sum_{d'|d} n^\epsilon \\
&\ll \sum_{d<x} d\tau(d) \sum_{\substack{n<x \\ d|\lambda(n)}} n^\epsilon \\
&= \sum_{n<x} n^\epsilon \sum_{d|\lambda(n)} d\tau(d) \\
&\ll x^{2+\epsilon+o(1)},
\end{aligned}
$$

and

$$
\begin{aligned}
E_2 &= \sum_{d<x} d \sum_{\substack{n<x \\ d|\lambda(n)}} \sum_{\substack{d'|d \\ b_n(d')\geq n^\epsilon}} \left|\mu\left(\frac{d}{d'}\right)\right| b_n(d')n^{-\delta} \\
&\ll \sum_{d<x} d \sum_{\substack{n<x \\ d|\lambda(n)}} b_n(d)n^{-\delta} \sum_{d'|d} 1 \\
&= \sum_{n<x} \sum_{d|\lambda(n)} db_n(d)\tau(d)n^{-\delta} \\
&\leq \sum_{n<x} n^{1-\delta} \sum_{d|\lambda(n)} d\tau(d) \\
&\ll x^{3-\delta+o(1)}.
\end{aligned}
$$

Now we treat the main term:

$$
\sum_{d<x} d \sum_{\substack{n<x \\ d|\lambda(n)}} \frac{1}{n} a_n(d) = \sum_{n<x} \frac{1}{n} \sum_{d|\lambda(n)} da_n(d).
$$

Taking δ to satisfy $2+\epsilon \leq 3-\delta$, we have

$$
\sum_{a<y} \sum_{n<x} l_a(n) = y \sum_{n<x} \frac{1}{n} \sum_{d|\lambda(n)} da_n(d) + O(x^{3-\delta+o(1)}).
$$

Let $u(n) = \frac{1}{\phi(n)} \sum_{d|\lambda(n)} da_n(d)$ be the average multiplicative order of the elements of $(\mathbb{Z}/n\mathbb{Z})^*$. The following is proven in [LS, Theorem 6]:

Theorem 3.1.

$$
\frac{1}{x} \sum_{n<x} u(n) = \frac{x}{\log x} \exp\left(B \frac{\log\log x}{\log\log\log x}(1+o(1))\right).
$$

What we have for the main term is the middle term in the following inequalities:

$$
\frac{1}{\log\log x} \sum_{n<x} u(n) \ll \sum_{n<x} \frac{\phi(n)}{n} u(n) \leq \sum_{n<x} u(n).
$$

Since $\log\log\log x = o\left(\frac{\log\log x}{\log\log\log x}\right)$, it follows that

$$
\sum_{n<x} \frac{\phi(n)}{n} u(n) = \frac{x^2}{\log x} \exp\left(B \frac{\log\log x}{\log\log\log x}(1+o(1))\right).
$$

Hence, we have

$$\sum_{a<y}\sum_{n<x} l_a(n) = \frac{yx^2}{\log x}\exp\left(B\frac{\log\log x}{\log\log\log x}(1+o(1))\right) + O(x^{3-\delta+o(1)}).$$

Moreover, if for some $0 < \delta' < \delta$, and $x^{1-\delta'} = o(y)$, then the error term can be included in the term with $o(1)$. The terms that appear when $n \leq a$, are also included in the term with $o(1)$. This completes the proof of Theorem 1.1.

References

[B] J. Bourgain, *Exponential sum estimates over subgroups of $\mathbb{Z}_q^*$, q arbitrary*, Journal d'Analyse Mathematique, December 2005, Volume 97, Issue 1, pp 317-355.

[EPS] P. Erdős, C. Pomerance, E. Schmutz, *Carmichael's Lambda Function*, Acta Arithmetica, LVIII4, 1991.

[ET] P. Erdős, P. Turán, *On a Problem in the Theory of Uniform Distribution I, II*, Nederll. Akad. Wetensch, 51, pp. 1146-1154, 1262-1269.

[KP] P. Kurlberg, C. Pomerance, *On a Problem of Arnold: the average multiplicative order of a given integer*, Algebra and Number Theory, 7 (2013), pp. 981-999.

[KP2] P. Kurlberg, C. Pomerance, *On the period of the linear congruential and power generators*, Acta Arith. 119 (2005), pp. 305-335.

[LS] F. Luca and I. E. Shparlinski, *Average multiplicative orders of elements modulo n*, Acta Arith., 109(4): pp. 387-411, 2003.

[M] H. Montgomery, *Ten Lectures on the Interface Between Analytic Number Theory and Harmonic Analysis*, CBMS Regional Conference Series in Mathematics, Number 84, AMS.

[MRS] C. Mauduit, J. Rivat, A. Sárközy, *On the Pseudo-Random Properties of n^c*, Illinois Journal of Mathematics, Volume 46, Number 1, Spring 2002, pp. 185-197.

[W] H. Weyl, *Über ein Problem aus dem Gebiete der diophantischen*, Ges. Abh. I (Springer: Berlin 1968), 487-497. Approximationen