Multiplicative Orders Modulo n on Average

Sungjin Kim

Santa Monica College/California State University Northridge
Department of Mathematics
707107@gmail.com

Dec 17, 2018

Definitions

- If $(a, n) = 1$ then denote by $\ell_a(n)$ the multiplicative order of a modulo n.

Definitions

• If $(a, n) = 1$ then denote by $\ell_a(n)$ the multiplicative order of a modulo n.
Example) We compute $\ell_2(15)$. Since $2^j \not\equiv 1$ for $j = 1, 2, 3$ and $2^4 \equiv 1 \mod 15$, we have $\ell_2(15) = 4$.

Euler and Carmichael Function

• Euler ϕ-function: $\phi(n) := n\prod_{p|n}\left(1-\frac{1}{p}\right)$ is the order of the group $(\mathbb{Z}/n\mathbb{Z})^*$.

• Carmichael λ-function: $\lambda(n) := \mathrm{LCM}\{\lambda(p^e) : p^e||n\}$ where $\lambda(p^e)$ is defined by

$$\lambda(p^e) = \phi(p^e) = p^{e-1}(p-1),$$

$$\lambda(2^e) = \phi(2^e), \quad \text{if } e \text{ is } 0, 1, \text{ or } 2$$

$$\lambda(2^e) = \frac{1}{2}\phi(2^e), \quad \text{if } e \geq 3$$

is the exponent of the group $(\mathbb{Z}/n\mathbb{Z})^*$.

Previous Results-1

Note that Erdős, Pomerance, Schmutz [EPS, Theorem 3] proved

Theorem

For $x \geq 16$, we have

$$\sum_{n \leq x} \lambda(n) = \frac{x^2}{\log x} \exp\left(B \frac{\log\log x}{\log\log\log x}(1 + o(1)) \right) \tag{1}$$

where

$$B = e^{-\gamma} \prod_{p} \left(1 - \frac{1}{(p-1)^2(p+1)} \right) \approx 0.34537.$$

Theorem (Kim, 2016, [K1])

There is a positive constant $\delta > 0$ such that, if $y > x^{1-\delta}$, then

$$\frac{1}{y} \sum_{a \leq y} \sum_{n \leq x} \ell_a(n) = \frac{x^2}{\log x} \exp\left(B \frac{\log\log x}{\log\log\log x}(1 + o(1)) \right), \tag{2}$$

Previous Results-2

Let $R(n)$ be the number of $a \in (\mathbb{Z}/n\mathbb{Z})^*$ such that $\ell_a(n) = \lambda(n)$, and $N_a(x)$ be the number of $n \leq x$ with $(a, n) = 1$ such that $\ell_a(n) = \lambda(n)$.

Theorem (Li, Pomerance, 2009, [LP1])

If $y > \exp((2+\epsilon)\sqrt{\log x \log\log x})$, *then we have as* $x \to \infty$,

$$\frac{1}{y}\sum_{a \leq y} N_a(x) \sim \sum_{n \leq x} \frac{R(n)}{n}.$$

Main Results

Theorem

If $y > \exp((\alpha+\epsilon)\sqrt{\log x})$, *then there is* $c > 0$ *such that for* $x \to \infty$,

$$\frac{1}{y}\sum_{a\le y}\sum_{n\le x}\ell_a(n) = \frac{x^2}{\log x}\exp\left(B\frac{\log\log x}{\log\log\log x}(1+o(1))\right), \tag{3}$$

Theorem

If $y > \exp((\alpha+\epsilon)\sqrt{\log x})$, *then there is* $c > 0$ *such that for* $x \to \infty$,

$$\frac{1}{y}\sum_{a\le y}N_a(x) = \sum_{n\le x}\frac{R(n)}{n} + O(x\exp(-c\sqrt{\log x})). \tag{4}$$

Definitions and Notations-continued

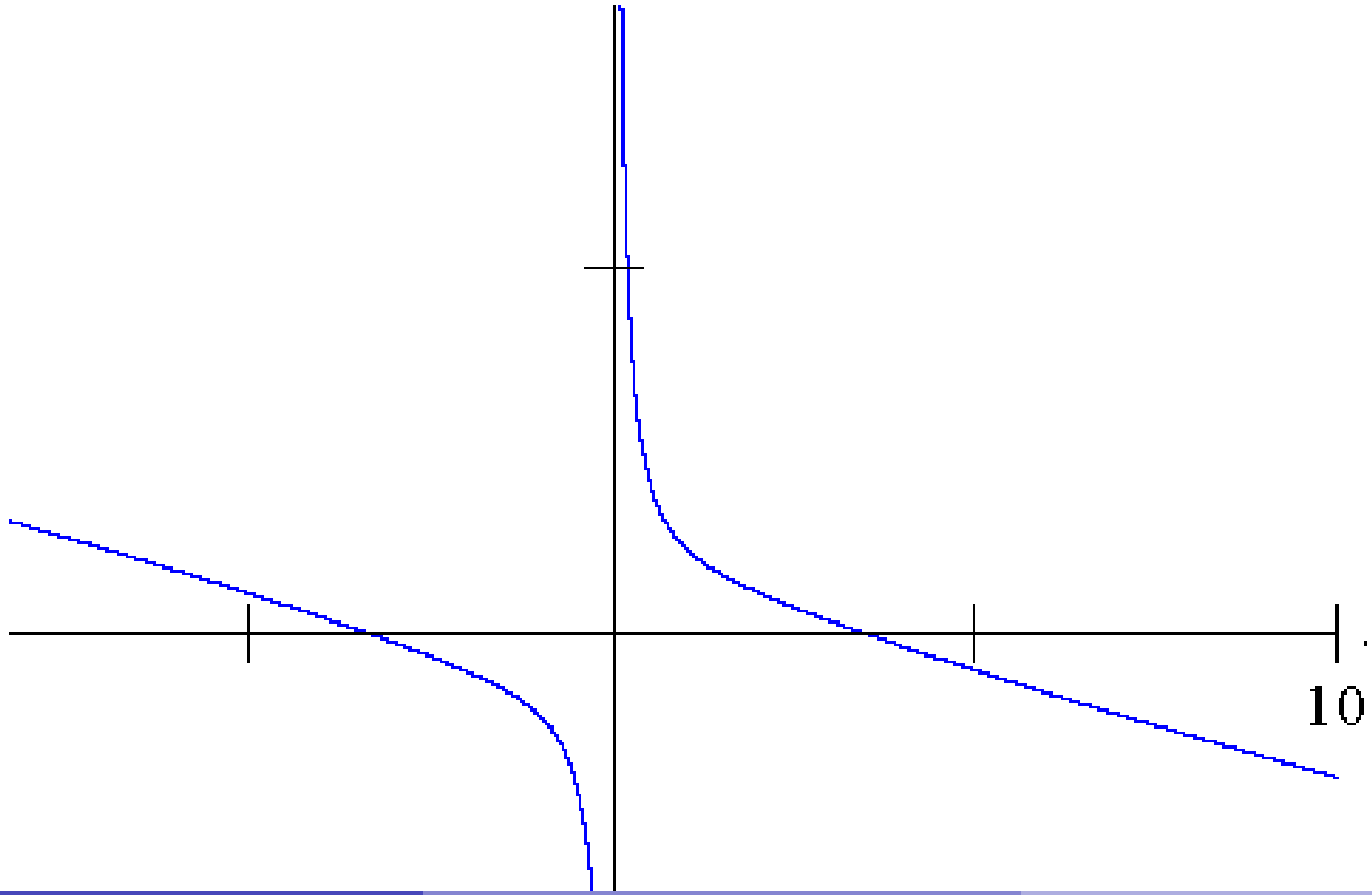
- The number $\alpha \approx 3.42$ is the unique positive root of an equation:

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

Definitions and Notations-continued

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

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



The Method of Stephens [S] for mod p

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

$$c_r(\chi) = \frac{1}{p-1} \sum_{\substack{a<p \\ \ell_a(p)=\frac{p-1}{r}}} \chi(a). \tag{5}$$

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 Stephens for mod n - Introduced in [LP1]

Following the definitions in [LP1],

$$\Delta_q(n) = \#\{\text{cyclic factors } C_{q^\nu} \text{ in } (\mathbb{Z}/n\mathbb{Z})^* : q^\nu || \lambda(n)\},$$

$$R(n) = \phi(n) \prod_{q|\phi(n)} \left(1 - \frac{1}{q^{\Delta_q(n)}}\right). \tag{6}$$

Let

$$E(n) = \{a \in (\mathbb{Z}/n\mathbb{Z})^* : a^{\frac{\lambda(n)}{\mathrm{rad}(\lambda(n))}} \equiv 1 \pmod{n}\},$$

and we say that χ is elementary character if χ is trivial on $E(n)$. For each square free $k|\phi(n)$, let $\rho_n(k)$ be the number of elementary characters mod n of order k. Then

$$\rho_n(k) = \prod_{q|k} (q^{\Delta_q(n)} - 1).$$

For a character χ mod n, let

$$c(\chi) = \frac{1}{\phi(n)} \sum_{b}{}' \chi(b),$$

where the sum is over λ-primitive roots in $[1, n]$. Then

$$|c(\chi)| \leq \bar{c}(\chi),$$

where

$$\bar{c}(\chi) = \begin{cases} \frac{1}{\rho_n(\mathrm{ord}(\chi))} & \text{if } \chi \text{ is elementary,} \\ 0 & \text{otherwise.} \end{cases}$$

The Method of Stephens for mod n - Extension of [LP1]

Let $h|\lambda(n)$ and q is a prime such that $q^v||\frac{\lambda(n)}{h}$.
Put $(\mathbb{Z}/n\mathbb{Z})^* \simeq G(n)$ in a primary decomposition of a $\mathbb{Z}$-module structure.

$$\Delta_{q,h}(n) = \left|\left\{\text{cyclic factors } C_{q^{v'}} \text{ in } G(n) : q^v||\frac{\lambda(n)}{h},\ v' \geq v\right\}\right|.$$

Let $S_q(n)$ be the q-Sylow subgroup of $G(n)$. Let $S_{q,h}(n) = \mathrm{ann}_{S_q(n)}(q^v)$ and $T_{q,h}(n) = \mathrm{ann}_{S_q(n)}(q^{v-1})$.

Further, we put

$$G_h(n) = \mathrm{ann}_{G(n)}\left(\frac{\lambda(n)}{h}\right) = \prod_{q\mid\frac{\lambda(n)}{h}} S_{q,h}(n),$$

$$E_h(n) = \mathrm{ann}_{G(n)}\left(\frac{\lambda(n)/h}{\mathrm{rad}(\lambda(n)/h)}\right) = \prod_{q\mid\frac{\lambda(n)}{h}} T_{q,h}(n),$$

$$S_{q,h}(n)/T_{q,h}(n) \simeq (\mathbb{Z}/q\mathbb{Z})^{\Delta_{q,h}(n)},$$

so that

$$|S_{q,h}(n)| = q^{\Delta_{q,h}(n)}|T_{q,h}(n)|.$$

Denote by $R_h(n)$ the number of elements $a \in (\mathbb{Z}/n\mathbb{Z})^*$ with $\ell_a(n) = \frac{\lambda(n)}{h}$. Then,

$$R_h(n) = \prod_{q\mid\frac{\lambda(n)}{h}} |S_{q,h}(n) - T_{q,h}(n)| = |G_h(n)| \prod_{q\mid\frac{\lambda(n)}{h}} \left(1 - \frac{1}{q^{\Delta_{q,h}(n)}}\right).$$

Clearly, we have $G_1(n) = G(n)$, $E_1(n) = E(n)$, $S_{q,1}(n) = S_q(n)$, $\Delta_{q,1}(n) = \Delta_q(n)$, and $R_1(n) = R(n)$.

We say that a character $\underline{\chi}$ of $G_h(n)$ is *h-elementary modulo n* if $\underline{\chi}$ is trivial on $E_h(n)$. Then h-elementary characters can be considered as characters of $G_h(n)/E_h(n)$. Thus, the order of such characters must be square-free. For each square-free $k|\lambda(n)/h$, the number of h-elementary character of $G_h(n)$ which has order k is obtained by

$$\rho_{n,h}(k) = \prod_{q|k}(q^{\Delta_{q,h}(n)} - 1).$$

For a Dirichlet character χ modulo n, let

$$c_h(\chi) = \frac{1}{\phi(n)} \sum_{\substack{b\in(\mathbb{Z}/n\mathbb{Z})^* \\ \ell_b(n)=\frac{\lambda(n)}{h}}} \chi(b).$$

Denote by $k = \mathrm{ord}(\underline{\chi})$ the order of the restriction of χ onto $G_h(n)$.

Then, we see that $c_h(\chi)$ only depends on $\underline{\chi}$. Decomposing the indices b into cosets of $E_h(n)$, we have

$$\phi(n)c_h(\chi) = \begin{cases} \frac{\mu(k)R_h(n)}{\rho_{n,h}(k)} & \text{if } \underline{\chi} \text{ is } h\text{-elementary,} \\ 0 & \text{otherwise.} \end{cases}$$

Since $|R_h(n)| \leq |G_h(n)|$, we have $|c_h(\chi)| \leq \overline{c_h}(\chi)$ where

$$\overline{c_h}(\chi) = \begin{cases} \frac{1}{[G(n):G_h(n)]\rho_{n,h}(k)} & \text{if } \underline{\chi} \text{ is } h\text{-elementary,} \\ 0 & \text{otherwise.} \end{cases}$$

Lemma

Let $t_{a,h}(n) = 1$ *if* $\ell_a(n) = \frac{\lambda(n)}{h}$ *and* 0 *otherwise. Then*

$$t_{a,h}(n) = \sum_{\chi \bmod n} c_h(\chi)\chi(a). \tag{7}$$

Lemma

Let $k|n$ *and* $h|\lambda(n)$*. Then we have*

$$\sideset{}{^*}\sum_{\chi \bmod k} \overline{c_h}(\chi\chi_{0,n}) \leq \tau(\phi(k))$$

where Σ^* *is over non-principal primitive characters,* $\tau(n) = \sum_{d|n} 1$*.*

$$\sum_{a\le y}\sum_{n\le x}\ell_a(n) = \sum_{a\le y}\sum_{n\le x}\sum_{h\mid\lambda(n)}\frac{\lambda(n)}{h}t_{a,h}(n)$$

$$= \sum_{a\le y}\sum_{n\le x}\sum_{h\mid\lambda(n)}\frac{\lambda(n)}{h}\sum_{\chi \bmod n} c_h(\chi)\chi(a)$$

$$= \sum_{a\le y}\sum_{n\le x}\sum_{h\mid\lambda(n)}\frac{\lambda(n)}{h}c_h(\chi_{0,n})\chi_{0,n}(a)$$

$$+ \sum_{a\le y}\sum_{n\le x}\sum_{h\mid\lambda(n)}\frac{\lambda(n)}{h}\sideset{}{^\bullet}\sum_{\chi \bmod n} c_h(\chi)\chi(a)$$

$$= y\sum_{n\le x}\frac{\phi(n)u(n)}{n} + \sum_{a\le y}\sum_{n\le x}\sum_{h\mid\lambda(n)}\frac{\lambda(n)}{h}\sideset{}{^\bullet}\sum_{\chi \bmod n} c_h(\chi)\chi(a) + E$$

$$= y\Sigma_1 + \Sigma_2 + E$$

where $\Sigma^\bullet$ is over non-principal characters and $E = O(x^2 \log x)$.

Estimation of Σ_1

Since $\frac{n}{\log\log n} \ll \phi(n) \leq n$, it follows from [LS, Theorem 6] that

$$\sum_{n\leq x} \frac{\phi(n)u(n)}{n} = \frac{x^2}{\log x} \exp\left(B\frac{\log\log x}{\log\log\log x}(1+o(1))\right). \tag{8}$$

Here,

$$u(n) = \frac{1}{\phi(n)} \sum_{a\in(\mathbb{Z}/n\mathbb{Z})^*} \ell_a(n).$$

Estimation of Σ_2

$$\Sigma_2 = \sum_{n\le x}\sum_{k|n}\sum_{h|\lambda(n)}\frac{\lambda(n)}{h}\sideset{}{^*}\sum_{\chi \bmod k} c_h(\chi\chi_{0,n})\sum_{a\le y}\chi(a)\chi_{0,n}(a)$$

$$= \sum_{n\le x}\sum_{k|n}\sum_{h|\lambda(n)}\frac{\lambda(n)}{h}\sideset{}{^*}\sum_{\chi \bmod k} c_h(\chi\chi_{0,n})\sum_{d|n}\chi(d)\mu(d)\sum_{a\le \frac{y}{d}}\chi(a),$$

Here, * means summed over primitive characters.

$$|\Sigma_2| \le x\sum_{d\le x}|\mu(d)|\sum_{m\le \frac{x}{d}}\sum_{\substack{k\le \frac{x}{dm}\\(k,d)=1}}\sum_{h|\lambda(dkm)}\frac{1}{h}\sideset{}{^*}\sum_{\chi \bmod k}|c_h(\chi\chi_{0,dkm})|\left|\sum_{a\le \frac{y}{d}}\chi(a)\right|$$

$$\le x\sum_{d\le x}|\mu(d)|\sum_{m\le \frac{x}{d}}\sum_{k\le \frac{x}{dm}}\sum_{h|\lambda(dkm)}\frac{1}{h}\sideset{}{^*}\sum_{\chi \bmod k}\overline{c_h}(\chi\chi_{0,dkm})\left|\sum_{a\le \frac{y}{d}}\chi(a)\right|$$

Estimation of Σ_2-continued

For simplicity, let $w = \frac{x}{dm}$, and $z = \frac{y}{d}$. We try bounding the size of

$$S(z,w) := \sum_{m\le z}\sum_{k\le w}\sum_{h|\lambda(dkm)} \frac{1}{h} \sideset{}{^*}\sum_{\chi \bmod k} \overline{c_h}(\chi\chi_{0,dkm}) \left|\sum_{a\le \frac{y}{d}} \chi(a)\right|$$

1. Estimate when d is large.
By [LuP, Theorem 1],

$$\begin{aligned} S(z,w) &\ll \frac{y}{d}\sum_{m\le z}(\log x) w \exp\left(2.5\sqrt{\frac{\log w}{\log\log w}}\right) \\ &\ll \frac{xy}{d^2}\exp\left(3\sqrt{\frac{\log x}{\log\log x}}\right). \end{aligned}$$

Estimation of Σ_2-continued

Denote the inner sum over $k \leq w$ by $S_m(z, w)$.

2. When $w \leq z^{\frac{3}{2}}$.

By Polya-Vinogradov Inequality and [LuP, Theorem 1],

$$S_m(z, w) \ll wz^{\frac{3}{4}} \exp\left(3\sqrt{\frac{\log x}{\log\log x}}\right).$$

3. When $w > z^{\frac{3}{2}}$.

Estimation of Σ_2-continued

By Hölder inequality, we have for any $r \geq 1$,

$$S_m(z,w) \leq A^{1-\frac{1}{2r}} B^{\frac{1}{2r}} \tag{9}$$

where

$$A = \sum_{k \leq w} \sum_{h | \lambda(dkm)} \frac{1}{h} \sideset{}{^*}\sum_{\chi \bmod k} \overline{c_h}(\chi\chi_{0,dkm})^{\frac{2r}{2r-1}},$$

and

$$B = \sum_{k \leq w} \sum_{h | \lambda(dkm)} \frac{1}{h} \sideset{}{^*}\sum_{\chi \bmod k} \left| \sum_{a \leq z} \chi(a) \right|^{2r}.$$

Then

$$A \ll w \exp\left(3\sqrt{\frac{\log x}{\log\log x}}\right).$$

Estimation of Σ_2-continued

We have $B \ll (\log x) T(w,z)$ with

$$T(w,z) = \sum_{k \le w} \sideset{}{^*}\sum_{\chi \bmod k} \left| \sum_{a \le z} \chi(a) \right|^{2r} = \sum_{k \le w} \sideset{}{^*}\sum_{\chi \bmod k} \left| \sum_{a \le z^r} \tau_r'(a) \chi(a) \right|^2 .$$

By the large sieve inequality,

$$T(w,z) \le (w^2 + z^r) \sum_{a \le z^r} \tau_r'(a)^2 \tag{10}$$

where $\tau_r'(a)$ is the number of ways writing a as a product of r positive integers each not exceeding r.

Estimation of Σ_2-continued

Applying an estimate by O. Bordellès (see [B])

Lemma

Let $c > 0$. If $z \geq 1$ and $r - 1 \leq c \log z$, then

$$\sum_{a \leq z^r} \tau_r'(a)^2 \leq \left(\frac{(1+c)^{r-1}}{(r-1)!} z \log^{r-1} z \right)^r . \tag{11}$$

We apply Stirling's formula to obtain the estimate:

Lemma

$$T(w,z)^{\frac{1}{2r}} \ll z \exp\left(f(K)\sqrt{\log w} + O(\log r) \right), \tag{12}$$

where

$$f(K) = f_1(K) + \frac{K}{4} = \frac{1}{K}\left(\log\left(\frac{K^2}{2} + 1 \right) + 1 \right),$$

$$z = \exp(K\sqrt{\log w}), \quad r = \left\lceil \frac{2\log w}{\log z} \right\rceil, \quad and \quad c = \frac{2}{K^2}.$$

Estimation of Σ_2-continued

Therefore, we obtain the following estimates:

Lemma

(1) If $z > \exp(4.18\sqrt{\log w})$, *then*

$$A^{1-\frac{1}{2r}} B^{\frac{1}{2r}} \ll wz^{\frac{13}{16}} \exp\left(f(4.18)\sqrt{\log w}\right) \exp\left(4\sqrt{\frac{\log x}{\log\log x}}\right),$$

(2) If $\exp((\alpha+\epsilon/2)\sqrt{\log w}) < z \leq \exp(5\sqrt{\log w})$, *then*

$$A^{1-\frac{1}{2r}} B^{\frac{1}{2r}} \ll wz^{\frac{3}{4}} \exp\left(f(\alpha+\epsilon/2)\sqrt{\log w}\right) \exp\left(4\sqrt{\frac{\log x}{\log\log x}}\right).$$

Recall $w = \frac{x}{dm}$, $z = \frac{y}{d}$.

- If $\exp((\alpha + \epsilon/2)\sqrt{\log(\frac{x}{dm})}) < \frac{y}{d}$, then

$$\sum_{d \le x} |\mu(d)| S(z, w) \ll \sum_{d \le x} \sum_{m \le \frac{x}{d}} \frac{xy}{md^{\beta}} \exp(-c'\sqrt{\log x})) \ll xy \exp(-c\sqrt{\log x})$$

for some $\beta > 1$.

- If $\exp((\alpha + \epsilon/2)\sqrt{\log(\frac{x}{dm})}) \ge \frac{y}{d}$, we have $\exp((\epsilon/2)\sqrt{\log x}) \le d$. Then

$$\sum_{d \le x} |\mu(d)| S(z, w) \ll xy \exp(-c\sqrt{\log x}).$$

Therefore, $|\Sigma_2| \ll x^2 y \exp(-c\sqrt{\log x})$

References

- O. Bordellès, *Explicit Upper Bounds for the Average Order of $d_n(m)$ and Application to Class Number*, Journal of Inequalities in Pure and Applied Mathematics, Volume 3, Issue 3, Article 38, 2002
- P. Erdős, C. Pomerance, E. Schmutz, *Carmichael's Lambda Function*, Acta Arithmetica, LVIII4, 1991.
- S. Li, C. Pomerance, *The Artin-Carmichael Primitive Root Problem on Average*, Mathematika 55, 2009, pp.167–176.
- F. Luca, C. Pomerance, *On the Average Number of Divisors of the Euler Function*, Publ. Math. Debrecen, 70/1-2 (2007), pp 125-148.
- F. Luca, I. E. Shparlinski, *Average multiplicative orders of elements modulo n*, Acta Arith., 109(4): pp. 387-411, 2003.
- S. Kim, *On the Order of a mod n, on Average*, International Journal of Number Theory, Volume 12, No. 08, January 2016.
- P. J. Stephens, *Prime Divisors of Second Order Linear Recurrences II*, Journal of Number Theory, Volume 8, Issue 3, August 1976