SOME THEOREMS ON MULTIPLICATIVE ORDERS MODULO p ON AVERAGE

KIM, SUNGJIN

Abstract. Let p be a prime, $a \geq 1$, and $\ell_a(p)$ be the multiplicative order of a modulo p. We prove various theorems concerning the averages of $\ell_a(p)$ over $p \leq x$ and $a \leq y$. We prove that these theorems hold for $y > \exp((\alpha+\epsilon)\sqrt{\log x})$ where $\alpha \approx 3.42$. This is an improvement over $y > \exp(c_1\sqrt{\log x})$ with $c_1 \geq 12e^9$ given in [S2]. We also provide the average of $\tau(\ell_a(p))$ over $p \leq x$, $a \leq y$, and $y > \exp((\alpha+\epsilon)\sqrt{\log x})$, where $\tau(n)$ is the divisor function $\sum_{d|n} 1$.

1. Introduction

Let $a \geq 1$ be an integer. We let $\ell_a(n)$ be the multiplicative order of a modulo n if $(a,n) = 1$. For $(a,n) \neq 1$, $\ell_a(n)$ is defined as in [MS, Section 8]: If we write $n = n_1 n_2$ with any prime divisors of n_1 divide a and $(n_2, a) = 1$, then we let $\ell_a(n) := \ell_a(n_2)$. This way of defining $\ell_a(n)$ is called an extended definition of multiplicative order of a modulo n where the ordinary definition takes $\ell_a(n) = 0$ if $(a,n) \neq 1$. This has an advantage over the ordinary definition that $\ell_a(n)|\phi(n)$ is always true regardless of a and n being coprime. Let $\omega(n) := \sum_{p|n} 1$ 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 $\omega(1) = \Omega(1) = 0$.

Artin's Conjecture on Primitive Roots (AC) states that for any non-square integer $a \neq 0, \pm 1$, $\ell_a(p) = p-1$ for infinitely many primes p. Assuming the Generalized Riemann Hypothesis (GRH) for Dedekind zeta functions for Kummerian extensions, Hooley [H] showed that the set of primes with $\ell_a(p) = p-1$ has a positive density in the set of primes. We may predict that $\ell_a(p)$ would be close to $p-1$ for many primes $p \leq x$. In [K2], we also observed that the average of $1/\ell_a(p)$ is small. Precisely, if $\frac{x}{\log x \log\log x} = o(y)$, then

$$\frac{1}{y}\sum_{a\leq y}\sum_{p\leq x}\frac{1}{\ell_a(p)} = \log x + K\log\log x + O(1) + O\left(\frac{x}{y\log\log x}\right)$$

for some explicit constant K. Due to the fact that $1/\ell_a(p)$ is mostly small, the length y of averaging had to be large. For the multiplicative orders on average, we may apply the large sieve inequality and the character sums to reduce y significantly. This was carried out by Stephens (see [S2, Theorem 1]) who showed that if $y > \exp(c_1\sqrt{\log x})$ then for any positive constant $B > 1$,

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

where C is the Stephens' constant:

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

and $\sum'$ is the sum over primes $p \leq x$ which are relatively prime to a. Although the value of the positive constant c_1 is not explicitly given in [S2], we see that c_1 is at least $12e^9$. This is because the proof of [S2, Lemma 7] requires the constants c_9 and c_1 to satisfy $c_9 > 0$ and $\log c_1 - c_9 - 2\log 2 - \log 3 > 9$. The optimal value for c_1 using Stephens' method is any positive number greater than $2\sqrt{2}e \approx 7.6885$. See Section 2 for the proof of this claim. This can be done by applying the best known estimates on the smooth numbers [HT, Theorem 1.2] and the asymptotic formula [Br, (1.8)] for Dickman's function $\rho(u)$. We prove that c_1 can be further dropped to $\alpha + \epsilon$ for any $\epsilon > 0$, where $\alpha \approx 3.42$ is the unique positive root of the equation

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

The corresponding second moment result [S2, Theorem 2] and [S1, Theorem 1, 2] can also be improved.

Theorem 1.1. *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 $B > 2$,

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

Let $P_a(x) := \{p \le x | \ell_a(p) = p-1\}$. Then the following estimates also hold:

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

where $A = \prod_p\left(1 - \frac{1}{p(p-1)}\right)$ is the Artin's constant.

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

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

Stephens also proved in [S2, Theorem 3] that the average number of prime divisors of $a^n - b$ for $p \le x$ averaged over the pairs (a, b) of integers in the box $(0, y]^2$ is also asymptotic to $C\mathrm{Li}(x)$, and proved the corresponding second moment result in [S2, Theorem 4]. The number y is rather large compared to those in [S2, Theorems 1, 2]. ($y > x(\log x)^{c_2}$ in [S2, Theorem 3], and $y > x^2(\log x)^{c_2}$ in [S2, Theorem 4] respectively.) He mentioned that these could probably be improved by using the large sieve inequality as in [S2, Theorems 1, 2]. However, he did not carry out the improvement in [S2]. Here, we state the improvement and prove them.

Theorem 1.2. *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 $B > 2$,

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

It is well-known by Erdős and Kac [EK] that $\omega(n)$ and $\Omega(n)$ follow a normal distribution after a suitable normalization. More precisely, 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 $G(u) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{u}\exp\left(-\frac{t^2}{2}\right)dt$.

Let $\phi(n)$ be the Euler Phi function. Erdős and Pomerance [EP] proved that $\omega(\phi(n))$ and $\Omega(\phi(n))$ also follow a normal distribution after a suitable normalization. Thus, for any real number u,

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

They also proved that this holds with $\phi(n)$ replaced by the Carmichael Lambda function $\lambda(n)$ [C, Section 4.6]. Furthermore, they conjectured that for any real number u,

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

In [MS, Section 8, Theorem 4'], Murty and Saidak proved, assuming that the Dedekind zeta function for $\mathbb{Q}(\zeta_q, a^{1/q})$ for primes q does not have zeros on $\Re(s)>\theta$ for some $1/2\le\theta<1$ (quasi-Generalized Riemann Hypothesis, quasi-GRH), that for any real number u,

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

They used this to prove the conjecture by Erdős and Pomerance conditionally on the quasi-GRH. Throughout this paper, we will always use the extended definition of $\ell_a(n)$ and index p in the summation will be always prime. We provide an unconditional average result as an application of [E, Theorem 12.2].

Theorem 1.3. *If $y>\exp((\alpha+\epsilon)\sqrt{\log x})$, then for any fixed real number u,*

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

Another interesting series of problems is to consider averages of the divisor function $\tau(n)=\sum_{d|n}1$ composed with various arithmetic functions. For the divisor function composed with Euler function and Carmichael λ-function, see [LP2], also [K1]. For the averages of $\tau(\ell_a(p))$, we have the following result.

Theorem 1.4. *If $y>\exp((\alpha+\epsilon)\sqrt{\log x})$, then for any $B>1$,*

$$\frac{1}{y}\sum_{a\le y}\sum_{p\le x}\tau(\ell_a(p))=K_1x+(K_1+K_2)\mathrm{Li}(x)+O\left(\frac{x}{\log^B x}\right) \tag{8}$$

where

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

Theorem 1.1 and 1.2 improve [S2, Theorem 1, 2, 3, and 4] by providing a wider range of y (These are N in [S2]). The proofs follow closely the method in [S2] where the large sieve inequality and Hölder inequality play crucial roles. The improvements are due to Lemma 3.1 and 3.2 (see §3) which replace [S2, Lemma 3 through 7]. Let $\tau_{r,y}(a)$ be the number of ways to write a as an ordered product of r positive integers, each of which is at most y. Let $\tau_r(a)$ be the number of ways to write a as an ordered product of r positive integers. Lemma 3 through 5 in [S2] treat the second moment divisor sum $\sum_{a\le y^r}(\tau_{r,y}(a))^2$ by replacing one $\tau_{r,y}(a)$ with its maximum, and obtaining an upper bound of the first moment divisor sum $\sum_{a\le y^r}\tau_{r,y}(a)\le y^r$. Then Lemma 6 and 7 in [S2] obtain upper bound of the maximum of $\tau_{r,y}(a)$ via the estimates of smooth numbers (see [Br], [HT]). The method presented in this paper follows a different path to treat the second moment divisor sum. Lemma 3.2 gives a combinatorial inequality giving $\left(\sum_{a\le y}\tau_r(a)\right)^r$ as an upper bound of the second moment divisor sum. Then Lemma 3.1 gives a uniform upper bound for the first moment divisor sum $\sum_{a\le y}\tau_r(a)$. The presence of $(r-1)!$ in the denominator in Lemma 3.1 is a main contributor for the improvements. Note also that the lemmas in [S2] do not have this denominator. We may also compare [S2, Lemma 8] and Lemma 3.3, which is applied the proof of Theorems 1.1 through 1.4. The proof of Theorem 1.3 relies on Kubilius-Shapiro Theorem (see §7) and the average estimates for $\omega(\ell_a(p))$ and $\Omega(\ell_a(p))$ (see §6). The proof of Theorem 1.4 is a consequence of a version of Titchmarsh Divisor Problem proved in [F] (see §8). For an earlier version of Titchmarsh Divisor Problem, see [BFI].

2. Optimal Constant in Stephens' Method

We need estimates of smooth numbers in the following form. See [Br, (1.8)] and [HT, Theorem 1.2].

Theorem 2.1 (de Bruijn)**.**

$$\log \rho(u) = -u\left[\log u + \log\log u - 1\right] + O\left(\frac{u}{\log u}\right).$$

Theorem 2.2 (Hildebrand, Tenenbaum)**.**

$$\log(\psi(x,y)/x) = \left\{1 + O(\exp(-(\log u)^{3/5-\epsilon}))\right\}\log\rho(u),$$

where $\max(2, (\log x)^{1+\epsilon}) \le y \le x$.

Combining the above two theorems, we have

$$\log(\psi(x,y)/x) = -u\log u - u\log\log u + u + O\left(\frac{u}{\log u}\right),$$

where $\max(2, (\log x)^{1+\epsilon}) \le y \le x$. We remark that the choice of r is as in [S2].

$$r = \left\lceil \frac{2\log x}{\log N}\right\rceil, \quad N = \exp((\beta\log x)^{\delta}), \quad \delta = \frac{1}{2} + \frac{c}{\log(\beta\log x)}, \quad \text{and } \beta > 2,$$

with $\beta > 2$ and $c > 0$ are to be determined.

Here, β will replace 9 which appears in $\psi(N, 9\log x)$ in [S2]. Note that it is assumed $N^r \le x^8$ in [S2, Lemma 5]. If we require $N^r \le x^2$, then we may use any $\beta > 2$ in $\psi(N, \beta\log x)$.

The bound given in Stephens result for the character sum S_4 defined in [S2] is

$$S_4 \ll x^{1-\frac{1}{2r}}(x^2 + N^r)^{\frac{1}{2r}} N^{\frac{1}{2}} \psi(N, \beta\log x)^{\frac{1}{2}}.$$

Assuming that $\log N \asymp \sqrt{\log x}$, we have

$$S_4 \ll xN^{-\frac{1}{4}}N^{\frac{1}{2}}N^{\frac{1}{2}}\exp\left[\frac{1}{2}\log\psi(N,\beta\log x)\right] \ll xN\exp\left[-\frac{1}{4}\log N + \frac{1}{2}\log N + \frac{1}{2}\log\frac{\psi(N,\beta\log x)}{N}\right].$$

Recall that we try to obtain a nontrivial cancellation on S_4 rather than the trivial bound xN.

By Theorem 2.2, we are able to write the square of the exponential on the RHS as

$$\exp\left[\frac{1}{2}\log N - u\log u - u\log\log u + u + O\left(\frac{u}{\log u}\right)\right],$$

where $u = \frac{\log N}{\log(\beta\log x)} = \frac{\delta\log N}{\log\log N}$.

Substituting u and δ above, and applying $\log(1+x) = O(x)$ for $|x| < 1$, we obtain

$$\begin{aligned}
&\exp\left[\frac{1}{2}\log N - u\log u - u\log\log u + u + O\left(\frac{u}{\log u}\right)\right] \\
&= \exp\left[\frac{1}{2}\log N - \frac{\delta\log N}{\log\log N}(\log\delta + \log\log N - \log\log\log N)\right. \\
&\left. - \frac{\delta\log N}{\log\log N}\log(\log\delta + \log\log N - \log\log\log N) + \frac{\delta\log N}{\log\log N} + O\left(\frac{\log N}{(\log\log N)^2}\right)\right] \\
&= \exp\left[(\delta - \delta\log\delta)\frac{\log N}{\log\log N} - \frac{c\log N}{\log(\beta\log x)} + O\left(\frac{\log N\log\log\log N}{(\log\log N)^2}\right)\right] \\
&= \exp\left[(1 - \log\delta - c)\frac{\log N}{\log(\beta\log x)} + O\left(\frac{\log N\log\log\log N}{(\log\log N)^2}\right)\right].
\end{aligned}$$

To ensure the nontrivial cancellation, we need to require

$$1 - \log\delta - c < 0.$$

Knowing that δ can be made arbitrarily close to $1/2$, we require $c > 1 + \log 2$. Putting this back in N and using $\beta > 2$, we need to require

$$N = \exp\left[(\beta \log x)^{\frac{1}{2} + \frac{c}{\log(\beta \log x)}}\right] > \exp\left[\sqrt{2\log x}\; e^c\right] = \exp\left[(2\sqrt{2}e + \epsilon)\sqrt{\log x}\right]$$

3. Lemmas

We begin with the following uniform result on divisor sums (see [B, (1.2)]).

Lemma 3.1. *Let $r \geq 1$ and define $\tau_r(a)$ to be the number of ways to write a as an ordered product of r positive integers. If $y \geq 1$, then we have*

$$\sum_{a \leq y} \tau_r(a) \leq \frac{1}{(r-1)!} y(\log y + r - 1)^{r-1}. \tag{9}$$

Proof. The proof is by induction. The case $r = 1$ is trivially true. Suppose that we have proved the inequality for a fixed $r \geq 1$. Then we have

$$\begin{aligned}\sum_{a \leq y} \tau_{r+1}(a) &= \sum_{d \leq y} \sum_{a \leq \frac{y}{d}} \tau_r(a) \leq \sum_{d \leq y} \frac{1}{(r-1)!} \frac{y}{d} \left(\log \frac{y}{d} + r - 1\right)^{r-1} \\ &\leq \frac{y}{(r-1)!} \left((\log y + r - 1)^{r-1} + \int_1^y \frac{1}{t} \left(\log \frac{y}{t} + r - 1\right)^{r-1} dt \right) \\ &\leq \frac{y}{r!} \left(r(\log y + r - 1)^{r-1} + (\log y + r - 1)^r \right) \leq \frac{y}{r!} (\log y + r)^r.\end{aligned}$$

Therefore, we have proved the inequality for $r + 1$. ☐

One might wonder if we may use a well-known asymptotic formula

$$\sum_{a \leq y} \tau_r(a) = \frac{1}{(r-1)!} y(\log y)^{r-1} + O\left(y(\log y)^{r-2}\right).$$

The above formula holds for fixed r and $y \to \infty$. For our purpose, we need to control both r and y at the same time. Thus, Lemma 3.1 in that aspect, will be a better choice than the above formula. Lemma 3.1 has been used in [B] to prove an upper bound of class numbers of number fields.

Corollary 3.1. *Let $c > 0$. If $y \geq 1$ and $r - 1 \leq c \log y$, then*

$$\sum_{a \leq y} \tau_r(a) \leq \frac{(1+c)^{r-1}}{(r-1)!} y \log^{r-1} y. \tag{10}$$

Proof. This follows by applying Lemma 3.1 and replacing $r - 1$ inside the parenthesis by $c \log y$. ☐

We define $\tau_{r,y}(a)$ to be the number of ways of writing a as ordered product of r positive integers, each of which does not exceed y.

Lemma 3.2. *We have for any $r \geq 1$ and $y \geq 1$,*

$$\sum_{a \leq y^r} (\tau_{r,y}(a))^2 \leq \left(\sum_{a \leq y} \tau_r(a) \right)^r. \tag{11}$$

Proof. We have

$$\begin{aligned}\sum_{a \leq y^r} (\tau_{r,y}(a))^2 &= \sum_{a_1, \ldots, a_r \leq y} \tau_{r,y}(a_1 \cdots a_r) \leq \sum_{a_1, \ldots, a_r \leq y} \tau_{r,y}(a_1) \cdots \tau_{r,y}(a_r) \\ &= \left(\sum_{a \leq y} \tau_{r,y}(a) \right)^r = \left(\sum_{a \leq y} \tau_r(a) \right)^r.\end{aligned}$$

Here, the first identity is due to a combinatorial argument. Let a be a positive integer satisfying $a \leq y^r$. Then $\tau_{r,y}(a) > 0$ if and only if $a_1 \cdots a_r = a$ has a solution in positive integers $a_1, \ldots, a_r$ satisfying $a_i \leq y$

for each $i \le r$. For each fixed a with $\tau_{r,y}(a) > 0$, the r-fold summation will count the number of solutions which is exactly $\tau_{r,y}(a)$. $\square$

Combining Lemma 3.2 and Corollary 3.1, we have the following.

Corollary 3.2. *Let $c > 0$. If $y \ge 1$ and $r - 1 \le c \log y$, then*

$$\sum_{a \le y^r} (\tau_{r,y}(a))^2 \le \left(\frac{(1+c)^{r-1}}{(r-1)!} y \log^{r-1} y \right)^r . \tag{12}$$

We use the character sums S_4 and S_{10} in [S2] with a slight modification, and give upper estimates of

$$S_4 := \sum_{p \le x} \sideset{}{^*}\sum_{\chi (\mathrm{mod}\ p)} \frac{1}{\mathrm{ord}(\chi)} \left| \sum_{a \le y} \chi(a) \right| \tag{13}$$

and

$$S_{10} := \sum_{p \le x} \sum_{q \le x} \sum_{\chi_1 (\mathrm{mod}\ p)} \sideset{}{^*}\sum_{\chi_2 (\mathrm{mod}\ q)} \frac{1}{\mathrm{ord}(\chi_1)\mathrm{ord}(\chi_2)} \left| \sum_{a \le y} \chi_1\chi_2(a) \right| . \tag{14}$$

The sum $\sum^*$ denotes the sum over non-principal primitive characters and $\mathrm{ord}(\chi)$ denotes the order of the character χ in the corresponding moduli.

Lemma 3.3. *If $y > \exp((\alpha+\epsilon)\sqrt{\log x})$, then there is a positive constant c_2 such that*

$$\max(xS_4, S_{10}) \ll x^2 y \exp\left(-c_2 \sqrt{\log x}\right). \tag{15}$$

Proof. As in [S2], we apply the Hölder's inequality and the large sieve inequality. Then for any $r \ge 1$,

$$\begin{aligned} S_4 &\le \left(\sum_{p \le x} \sideset{}{^*}\sum_{\chi (\mathrm{mod}\ p)} \left(\frac{1}{\mathrm{ord}(\chi)} \right)^{\frac{2r}{2r-1}} \right)^{1-\frac{1}{2r}} \left(\sum_{p \le x} \sideset{}{^*}\sum_{\chi (\mathrm{mod}\ p)} \left| \sum_{a \le y} \chi(a) \right|^{2r} \right)^{\frac{1}{2r}} \\ &\ll \left(\sum_{p \le x} \tau(p-1) \right)^{1-\frac{1}{2r}} (x^2 + y^r)^{\frac{1}{2r}} \left(\sum_{a \le y^r} (\tau_{r,y}(a))^2 \right)^{\frac{1}{2r}} \\ &\ll x^{1-\frac{1}{2r}} y \left(\frac{(1+c)^{r-1}}{(r-1)!} (\log y)^{r-1} \right)^{\frac{1}{2}}, \end{aligned}$$

where the last inequality is by Corollary 3.2 provided if $r - 1 \le c \log y$.

We may assume that $y = \exp(K\sqrt{\log x})$ for a function $K := K(x)$ satisfying $0 < K \le 4\sqrt{\log\log x}$ by [S1, Theorem 1]. This is to look for a possibility of obtaining K smaller than the constant c_1 obtained in [S2, Theorem 1]. Also, we want to choose a positive integer r to satisfy $y^{r-1} < x^2 \le y^r$. Then,

$$\log y = K\sqrt{\log x}, \quad \log\log y = \log K + \frac{1}{2}\log\log x, \text{ and } r - 1 < \frac{2\log x}{\log y} = \frac{2}{K}\sqrt{\log x} \le r.$$

In view of the last inequality for r, it is reasonable to put $c = \frac{2}{K^2}$ for $r - 1 \le c \log y$ to hold. Moreover, by $y^{r-1} < x^2$, we have

$$x^{-\frac{1}{2r}} < y^{\frac{-r+1}{4r}} = y^{-\frac{1}{4}+\frac{1}{4r}},$$

and by $x^2 \le y^r$ and $\frac{2}{K}\sqrt{\log x} \le r$, we have

$$y^{\frac{1}{4r}} = \exp\left(K\sqrt{\log x}\frac{1}{4r} \right) \le \exp\left(K\sqrt{\log x}\frac{K}{8\sqrt{\log x}} \right) = \exp\left(\frac{K^2}{8} \right).$$

By Stirling's formula [MV, Theorem C1] and $K \le 4\sqrt{\log\log x}$, we have

$$S_4 \ll xy \exp\left(-\frac{1}{4}\log y + \frac{r-1}{2}\log\left(1+\frac{2}{K^2}\right) - \frac{1}{2}\log(r-1)! + \frac{r-1}{2}\log\log y\right)$$
$$\ll xy\exp\left(\sqrt{\log x}\left(-\frac{K}{4} + \frac{1}{K}\log\left(1+\frac{2}{K^2}\right) - \frac{1}{K}\log 2 + \frac{1}{K} + \frac{2\log K}{K}\right) + O(\log\log x)\right).$$

If $\alpha + \epsilon < K \le 4\sqrt{\log\log x}$, then we see that

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

This shows that $S_4 \ll xy\exp(-c\sqrt{\log x})$ for some positive constant c.

For S_{10}, we rearrange the sum as follows:

$$\sum_{p\le x}\sum_{q\le x}\sum_{\chi_1 (\mathrm{mod}\ p)}\sideset{}{^*}\sum_{\chi_2 (\mathrm{mod}\ q)} \frac{1}{\mathrm{ord}(\chi_1)\mathrm{ord}(\chi_2)}\left|\sum_{a\le y}\chi_1\chi_2(a)\right| = \sum_{p\le x}\sum_{\chi_1 (\mathrm{mod}\ p)}\frac{1}{\mathrm{ord}(\chi_1)}\widetilde{S_4}.$$

Fix $p \le x$ and χ_1 mod p, then the inner sum $\widetilde{S_4}$ is treated the same way as S_4. We have

$$\widetilde{S_4} = \sum_{q\le x}\sideset{}{^*}\sum_{\chi_2 (\mathrm{mod}\ q)}\frac{1}{\mathrm{ord}(\chi_2)}\left|\sum_{a\le y}\chi_1\chi_2(a)\right|$$
$$\le \left(\sum_{q\le x}\sideset{}{^*}\sum_{\chi_2 (\mathrm{mod}\ q)}\left(\frac{1}{\mathrm{ord}(\chi_2)}\right)^{\frac{2r}{2r-1}}\right)^{1-\frac{1}{2r}}\left(\sum_{q\le x}\sideset{}{^*}\sum_{\chi_2 (\mathrm{mod}\ q)}\left|\sum_{a\le y}\chi_1\chi_2(a)\right|^{2r}\right)^{\frac{1}{2r}}$$
$$\ll \left(\sum_{q\le x}\tau(q-1)\right)^{1-\frac{1}{2r}}(x^2+y^r)^{\frac{1}{2r}}\left(\sum_{a\le y^r}|\tau_{r,y}(a)\chi_1(a)|^2\right)^{\frac{1}{2r}}$$
$$\ll x^{1-\frac{1}{2r}}y\left(\frac{(1+c)^{r-1}}{(r-1)!}(\log y)^{r-1}\right)^{\frac{1}{2}}.$$

The same choice of r and c as in the proof of the bound for S_4, yields

$$S_{10} \ll \sum_{p\le x}\sum_{\chi_1 (\mathrm{mod}\ p)}\frac{1}{\mathrm{ord}(\chi_1)}xy\exp(-c\sqrt{\log x})$$
$$\ll \sum_{p\le x}\tau(p-1)xy\exp(-c\sqrt{\log x}) \ll x^2y\exp(-c\sqrt{\log x}).$$

□

Note that if $y > \exp(4\sqrt{\log x\log\log x})$ as in [S1, Theorem 1], then it can be proved by the method in [S1, (27)] that the result is stronger in this range of y. In fact, there is a positive constant c_3 such that

$$\max(xS_4, S_{10}) \ll x^2y\exp\left(-c_3\sqrt{\log x\log\log x}\right).$$

Thus, we have the result.

4. Proof of Theorem 1.1

In [S2, Theorem 1], Stephens defined a character sum $c_r(\chi)$ where χ is a Dirichlet character modulo p for $r|p-1$ as

$$c_r(\chi) = \frac{1}{p-1}\sum_{\substack{a<p \\ \ell_a(p)=\frac{p-1}{r}}}\chi(a). \tag{16}$$

From [S2, Lemma 1], we have for any Dirichlet character χ modulo p,

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

For the principal character χ_0 modulo p, we have

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

Now, we are ready to prove Theorem 1.1.

Proof of Theorem 1.1. The contribution of $a \le y$ for which $p|a$ and $p \le x$ is $O(\log\log x)$ since $\ell_a(p) = 1$ in this case. Then

$$\begin{aligned} y^{-1}\sum_{a\le y}\sum_{\substack{p\le x\\(a,p)=1}} \frac{\ell_a(p)}{p-1} &= y^{-1}\sum_{a\le y}\sum_{\substack{p\le x\\(a,p)=1}} \sum_{\substack{r|p-1\\ \ell_a(p)=\frac{p-1}{r}}} r^{-1} \\ &= y^{-1}\sum_{a\le y}\sum_{p\le x}\sum_{r|p-1} r^{-1}\sum_{\chi(\mathrm{mod}\ p)} c_r(\chi)\chi(a) \\ &= y^{-1}\sum_{p\le x}\sum_{r|p-1} r^{-1}\sum_{\chi(\mathrm{mod}\ p)} c_r(\chi)\sum_{a\le y}\chi(a). \end{aligned}$$

By Lemma 3.3, the contribution of nonprincipal characters modulo p to this sum is

$$\ll y^{-1}S_4\log x \ll x\exp(-c\sqrt{\log x}).$$

By [S2, Lemma 12], the contribution of principal character modulo p to this sum is

$$= \sum_{p\le x}\sum_{r|p-1}\frac{\phi\left(\frac{p-1}{r}\right)}{r(p-1)} + O(\log\log x) + O\left(y^{-1}\frac{x}{\log x}\right) = C\mathrm{Li}(x) + O\left(\frac{x}{\log^A x}\right).$$

Thus, (1) follows. The proof of (3) follows by a similar argument if we replace $\sum_{r|p-1} r^{-1}$ by $r = 1$ and $c_r(\chi)$ by $c_1(\chi)$.

For (2), it is enough to show that

$$y^{-1}\sum_{a\le y}\left(\sum_{p\le x}\frac{\ell_a(p)}{p-1} - \sum_{p\le x}\sum_{r|p-1}\frac{\phi\left(\frac{p-1}{r}\right)}{r(p-1)}\right)^2 = O\left(x^2\exp(-c_2\sqrt{\log x})\right).$$

Again, the contribution of $a \le y$ for which $p|a$ is $O((\log\log x)^2)$. Thus, we consider

$$\begin{aligned} y^{-1}\sum_{a\le y}\sum_{p\le x}\sum_{q\le x}\frac{\ell_a(p)\ell_a(q)}{(p-1)(q-1)} &= y^{-1}\sum_{a\le y}\sum_{\substack{p\le x\\q\le x}}\sum_{\substack{r|p-1\\s|q-1}} r^{-1}s^{-1}\sum_{\chi_1(\mathrm{mod}\ p)} c_r(\chi_1)\chi_1(a)\sum_{\chi_2(\mathrm{mod}\ q)} c_s(\chi_2)\chi_2(a) \\ &= y^{-1}\sum_{\substack{p\le x\\q\le x}}\sum_{\substack{r|p-1\\s|q-1}} r^{-1}s^{-1}\sum_{\chi_1(\mathrm{mod}\ p)} c_r(\chi_1)\sum_{\chi_2(\mathrm{mod}\ q)} c_s(\chi_2)\sum_{a\le y}\chi_1\chi_2(a). \end{aligned}$$

The contribution of nonprincipal characters modulo p is, by Lemma 3.3,

$$\ll y^{-1}(\log x)^2 S_{10} \ll x^2\exp(-c\sqrt{\log x}).$$

The contribution of principal characters modulo p

$$= \sum_{\substack{p\le x\\q\le x}}\sum_{\substack{r|p-1\\s|q-1}} r^{-1}s^{-1}\frac{\phi\left(\frac{p-1}{r}\right)}{p-1}\frac{\phi\left(\frac{q-1}{s}\right)}{q-1} + O((\log\log x)^2) + O\left(y^{-1}\left(\frac{x}{\log x}\right)^2\right).$$

Then by [S2, Lemma 12], (2) follows. The proof of (4) is by a similar argument if we replace $\sum_{r|p-1} r^{-1}$ and $\sum_{s|p-1} s^{-1}$ by $r = 1$ and $s = 1$, also $c_r(\chi_1)$ and $c_s(\chi_2)$ by $c_1(\chi_1)$ and $c_1(\chi_2)$ respectively. $\square$

5. Proof of Theorem 1.2

Proof of Theorem 1.2. Note that there is some integer n such that a prime p divides $a^n - b$ if and only if $\ell_b(p)|\ell_a(p)$. Thus, we begin with putting $\ell_b(p) = w$, $\ell_a(p) = wt$, and changing the order of summations,

$$y^{-2}\sum_{\substack{a\le y\\ b\le y}}\sum_{\substack{p\le x\\ \ell_b(p)|\ell_a(p)}} 1 = y^{-2}\sum_{\substack{a\le y\\ b\le y}}\sum_{p\le x}\sum_{\substack{w|p-1\\ t|\frac{p-1}{w}}}\sum_{\chi_1,\chi_2 (\text{mod } p)} c_w(\chi_1)c_{wt}(\chi_2)\chi_1(a)\chi_2(b)$$

$$= y^{-2}\sum_{p\le x}\sum_{\substack{w|p-1\\ t|\frac{p-1}{w}}}\sum_{\chi_1,\chi_2 (\text{mod } p)} c_w(\chi_1)c_{wt}(\chi_2)\sum_{a\le y}\chi_1(a)\sum_{b\le y}\chi_2(b).$$

The contribution of all pairs of characters (χ_1, χ_2) for which one of χ_1 or χ_2 is nonprincipal, is

$$\ll y^{-2}\sum_{p\le x}\tau_3(p-1)\tau_2(p-1)\sideset{}{^*}\sum_{\chi (\text{mod } p)}\frac{1}{\text{ord}(\chi)}\left|\sum_{a\le y}\chi(a)\right| y.$$

We split this sum into two parts where $\tau_3(p-1)\tau_2(p-1) < \exp(c_3\sqrt{\log x})$ and $\tau_3(p-1)\tau_2(p-1) \ge \exp(c_3\sqrt{\log x})$. We take $c_3 = c_2/2$ where c_2 is the positive constant in Lemma 3.3. Then the first part is $O(x\exp(-c\sqrt{\log x}))$ by Lemma 3.3. The second part is $O(x\log^N x\exp(-c_3\sqrt{\log x}))$ for a fixed $N > 0$, since we have

$$\sum_{p\le x}\tau_3^2(p-1)\tau_2^3(p-1) \ll \sum_{n\le x}\tau_3^2(n)\tau_2^3(n) \ll x\log^{71} x,$$

by Selberg-Delange method [T, Theorem 5, pp. 191]. Thus, we have for some $c > 0$,

$$y^{-1}\sum_{p\le x}\tau_3(p-1)\tau_2(p-1)\sideset{}{^*}\sum_{\chi (\text{mod } p)}\frac{1}{\text{ord}(\chi)}\left|\sum_{a\le y}\chi(a)\right| \ll x\exp(-c\sqrt{\log x}).$$

The contribution of all pairs of characters (χ_1, χ_2) for which χ_1 and χ_2 both are principal is by [S2, Lemma 12] and $\sum_{d|n}\phi(d) = n$,

$$= y^{-2}\sum_{p\le x}\sum_{\substack{w|p-1\\ t|\frac{p-1}{w}}}\frac{\phi\left(\frac{p-1}{w}\right)}{p-1}\frac{\phi\left(\frac{p-1}{wt}\right)}{p-1}\left(y + O\left(\frac{y}{p}\right)\right)^2 = \sum_{p\le x}\sum_{w|p-1}\frac{\phi\left(\frac{p-1}{w}\right)}{w(p-1)}\left(1 + O\left(\frac{1}{p}\right)\right)^2$$

$$= C\text{Li}(x) + O\left(\frac{x}{\log^A x}\right).$$

This completes the proof of (5).

For the proof of (6), it is enough to show that

$$y^{-2}\sum_{\substack{a\le y\\ b\le y}}\left(\sum_{\substack{p\le x\\ \ell_b(p)|\ell_a(p)}} 1 - \sum_{\substack{p\le x\\ w|p-1}}\frac{\phi(\frac{p-1}{w})}{w(p-1)}\right)^2 = O\left(x^2\exp(-c\sqrt{\log x})\right).$$

We write the sum on the left $y^{-2}\sum(\sum_1 - \sum_2)^2$ after expanding the inner square as $y^{-2}\sum(\sum_1^2 + \sum_2^2 - 2\sum_1\sum_2)$. Then by putting $\ell_b(p) = w$, $\ell_a(p) = wt$, $\ell_b(q) = u$, and $\ell_a(q) = us$ respectively, and by changing the order of the summations in $y^{-2}\sum\sum_1^2$, we have

$$y^{-2}\sum_{a\le y}\sum_{b\le y}\sum_{\substack{p\le x\\ \ell_b(p)|\ell_a(p)}}\sum_{\substack{q\le x\\ \ell_b(q)|\ell_a(q)}} 1$$
$$= y^{-2}\sum_{p\le x}\sum_{q\le x}\sum_{\substack{w|p-1\\ t|\frac{p-1}{w}}}\sum_{\substack{u|q-1\\ s|\frac{q-1}{u}}}\sum_{\substack{\chi_1,\chi_2 (\mathrm{mod}\ p)\\ \chi_3,\chi_4 (\mathrm{mod}\ q)}} c_w(\chi_1)c_{wt}(\chi_2)c_u(\chi_3)c_{us}(\chi_4)\sum_{a\le y}\chi_1\chi_3(a)\sum_{b\le y}\chi_2\chi_4(b).$$

The contribution of the 4-tuple of characters $(\chi_1,\chi_2,\chi_3,\chi_4)$ such that all four characters are principal is precisely $y^{-2}\sum\sum_2^2$. Similarly expanding the sum $y^{-2}\sum\sum_1\sum_2$ using the character sums, we see that those contribution of tuples of all four principal characters is cancelled in $y^{-2}\sum(\sum_1^2+\sum_2^2-2\sum_1\sum_2)$. Thus, we consider the contribution of the 4-tuple of characters $(\chi_1,\chi_2,\chi_3,\chi_4)$ such that at least one of these four characters is nonprincipal. Among these, it is easily seen that the contribution of $p=q$ is $O(x/\log x)$. We assume that $p\neq q$. Then if one of χ_1 or χ_3 is nonprincipal, then $\chi_1\chi_3$ is nonprincipal mod pq. Similarly, if one of χ_2 or χ_4 is nonprincipal, then $\chi_2\chi_4$ is nonprincipal mod pq. Therefore, the contribution is bounded by

$$y^{-2}\sum_{p\le x}\sum_{q\le x}\tau_3(p-1)\tau_3(q-1)\tau_2(p-1)\tau_2(q-1)\sum_{\chi_1\ (\mathrm{mod}\ p)}\sideset{}{^*}\sum_{\chi_2\ (\mathrm{mod}\ q)}\frac{1}{\mathrm{ord}(\chi_1)\mathrm{ord}(\chi_2)}\left|\sum_{a\le y}\chi_1\chi_2(a)\right|y.$$

We split this sum into two parts where $\tau_3(p-1)\tau_3(q-1)\tau_2(p-1)\tau_2(q-1)<\exp(c_3\sqrt{\log x})$ and $\tau_3(p-1)\tau_3(q-1)\tau_2(p-1)\tau_2(q-1)\ge\exp(c_3\sqrt{\log x})$ with $c_3=c_2/2$. The first part is $O(x^2\exp(-c\sqrt{\log x}))$ by Lemma 3.3. The second part is $O(x^2\log^N x\exp(-c_3\sqrt{\log x}))$ since $\sum_{p\le x}\sum_{q\le x}\tau_3^2(p-1)\tau_2^3(p-1)\tau_3^2(q-1)\tau_2^3(q-1)=O(x^2\log^N x)$ for a fixed $N>0$. Thus, we have

$$y^{-1}\sum_{p\le x}\sum_{q\le x}\tau_3(p-1)\tau_3(q-1)\tau_2(p-1)\tau_2(q-1)\sum_{\chi_1\ (\mathrm{mod}\ p)}\sideset{}{^*}\sum_{\chi_2\ (\mathrm{mod}\ q)}\frac{1}{\mathrm{ord}(\chi_1)\mathrm{ord}(\chi_2)}\left|\sum_{a\le y}\chi_1\chi_2(a)\right|$$
$$\ll x^2\exp(-c\sqrt{\log x}).$$

This completes the proof of (6). □

6. Average Estimates for $g(\ell_a(p))$

The following results are proven in [EP, Lemma 2.1, 2.2]. The function g is either one of $\Omega(n)=\sum_{p^k|n}1$ or $\omega(n)=\sum_{p|n}1$.

Lemma 6.1 (Erdős-Pomerance)**.**

$$\sum_{p\le x} g(p-1)=\pi(x)\log\log x+O(\pi(x)), \tag{17}$$

$$\sum_{p\le x} g(p-1)^2=\pi(x)(\log\log x)^2+O(\pi(x)\log\log x). \tag{18}$$

Also by partial summation, the following are proven in [EP, Lemma 2.3, 2.4].

Corollary 6.1 (Erdős-Pomerance)**.**

$$\sum_{p\le x}\frac{g(p-1)}{p}=\frac{1}{2}(\log\log x)^2+O(\log\log x), \tag{19}$$

$$\sum_{p\le x}\frac{g(p-1)^2}{p}=\frac{1}{3}(\log\log x)^3+O((\log\log x)^2). \tag{20}$$

It is possible to obtain the following results on average by applying Lemma 3.3.

Lemma 6.2. *If $y > \exp((\alpha+\epsilon)\sqrt{\log x})$, then*

$$\sum_{p\le x}\frac{1}{y}\sum_{a\le y} g(\ell_a(p)) = \pi(x)\log\log x + O(\pi(x)), \tag{21}$$

$$\sum_{p\le x}\left(\frac{1}{y}\sum_{a\le y} g(\ell_a(p))\right)^2 = \pi(x)(\log\log x)^2 + O(\pi(x)\log\log x). \tag{22}$$

Here, $g(n)=\omega(n)$ or $\Omega(n)$.

Proof. We first consider $g(n)=\omega(n)$. We write the LHS of (21) as

$$\begin{aligned}\sum_{p\le x}\frac{1}{y}\sum_{a\le y}\omega(\ell_a(p)) &= \frac{1}{y}\sum_{p\le x}\sum_{a\le y}\sum_{s\mid p-1}\sum_{q\mid\frac{p-1}{s}}\sum_{\ell_a(p)=\frac{p-1}{s}} 1\\ &= \frac{1}{y}\sum_{p\le x}\sum_{a\le y}\sum_{s\mid p-1}\sum_{q\mid\frac{p-1}{s}}\sum_{\chi(\mathrm{mod}\ p)} c_s(\chi)\chi(a)\\ &= \frac{1}{y}\sum_{p\le x}\sum_{s\mid p-1}\sum_{q\mid\frac{p-1}{s}}\sum_{\chi(\mathrm{mod}\ p)} c_s(\chi)\sum_{a\le y}\chi(a).\end{aligned}$$

Note that the sum over p and q are over prime numbers. The contribution of non-principal characters to the sum is

$$\ll \frac{1}{y}\sum_{p\le x}\tau_3(p-1)\sideset{}{^*}\sum_{\chi(\mathrm{mod}\ p)}\frac{1}{\mathrm{ord}(\chi)}\left|\sum_{a\le y}\chi(a)\right|,$$

where the sum $\sum^*$ denotes the sum over non-principal primitive characters. Splitting the sum into $\tau_3(p-1)\le\exp\left(\frac{c_2}{2}\sqrt{\log x}\right)$ and $\tau_3(p-1)>\exp\left(\frac{c_2}{2}\sqrt{\log x}\right)$, we obtain that the contribution of non-principal characters is, by Lemma 3.3,

$$\ll x\exp(-c_3\sqrt{\log x}),$$

where c_3 is an absolute positive constant.

For the principal character χ_0 modulo p, the contribution is

$$\begin{aligned}\sum_{p\le x}\sum_{s\mid p-1}\sum_{q\mid\frac{p-1}{s}}\frac{\phi\left(\frac{p-1}{s}\right)}{p-1}\left(1+O\left(\frac{1}{p}\right)\right) &= \sum_{p\le x}\sum_{s\mid p-1}\sum_{q\mid\frac{p-1}{s}}\frac{\phi\left(\frac{p-1}{s}\right)}{p-1} + O\left(\sum_{p\le x}\sum_{s\mid p-1}\sum_{q\mid\frac{p-1}{s}}\frac{\phi\left(\frac{p-1}{s}\right)}{p(p-1)}\right)\\ &= \sum_{p\le x}\frac{1}{p-1}\sum_{s\mid p-1}\phi(s)\omega(s) + O\left(\sum_{p\le x}\frac{1}{p(p-1)}\sum_{s\mid p-1}\phi(s)\omega(s)\right).\end{aligned}$$

By the elementary identity and estimate

$$\sum_{s\mid n}\phi(s)\omega(s) = n\sum_{q^k\|n}\left(1-\frac{1}{q^k}\right) = n\omega(n) + O\left(n\sum_{q\mid n}\frac{1}{q}\right) = O(n\omega(n)),$$

the contribution of principal character becomes

$$\sum_{p\le x}\omega(p-1) + O(\pi(x)).$$

Then the result (21) for $g(n)=\omega(n)$ follows by Lemma 6.1.

For the proof of (22), we write the LHS of (22) for $g(n)=\omega(n)$ as

$$\begin{aligned}\sum_{p\le x}\left(\frac{1}{y}\sum_{a\le y}\omega(\ell_a(p))\right)^2 &= \frac{1}{y^2}\sum_{p\le x}\sum_{a\le y}\sum_{b\le y}\omega(\ell_a(p))\omega(\ell_b(p))\\ &= \frac{1}{y^2}\sum_{p\le x}\sum_{a\le y}\sum_{b\le y}\sum_{\substack{s|p-1\\ t|p-1}}\sum_{\substack{q|\frac{p-1}{s}\\ r|\frac{p-1}{t}}}\sum_{\ell_a(p)=\frac{p-1}{s}}\sum_{\ell_b(p)=\frac{p-1}{t}}1\\ &= \frac{1}{y^2}\sum_{p\le x}\sum_{a\le y}\sum_{b\le y}\sum_{\substack{s|p-1\\ t|p-1}}\sum_{\substack{q|\frac{p-1}{s}\\ r|\frac{p-1}{t}}}\left(\sum_{\chi_1 (\mathrm{mod}\ p)}c_s(\chi_1)\chi_1(a)\right)\left(\sum_{\chi_2 (\mathrm{mod}\ p)}c_t(\chi_2)\chi_2(b)\right)\\ &= \frac{1}{y^2}\sum_{p\le x}\sum_{\substack{s|p-1\\ t|p-1}}\sum_{\substack{q|\frac{p-1}{s}\\ r|\frac{p-1}{t}}}\sum_{\substack{\chi_1 (\mathrm{mod}\ p)\\ \chi_2 (\mathrm{mod}\ p)}}c_s(\chi_1)c_t(\chi_2)\sum_{a\le y}\chi_1(a)\sum_{b\le y}\chi_2(b).\end{aligned}$$

Here, the indices p, q, and r are primes.

To find the contribution of pairs (χ_1,χ_2) when one of the characters is non-principal, without loss of generality we assume that χ_1 is non-principal. This case contributes to

$$\ll \frac{1}{y}\sum_{p\le x}\tau_3(p-1)^2\tau(p-1)\sideset{}{^*}\sum_{\chi_1 (\mathrm{mod}\ p)}\frac{1}{\mathrm{ord}(\chi_1)}\left|\sum_{a\le y}\chi_1(a)\right|.$$

Splitting the sum into $\tau_3(p-1)^2\tau(p-1)\le \exp\left(\frac{c_2}{2}\sqrt{\log x}\right)$ and $\tau_3(p-1)^2\tau(p-1)> \exp\left(\frac{c_2}{2}\sqrt{\log x}\right)$, we see that the contribution of this case is, by Lemma 3.3,

$$\ll x\exp(-c_4\sqrt{\log x}),$$

where c_4 is an absolute positive constant.

The contribution of the case in which both characters χ_1 and χ_2 are principal is treated as

$$\begin{aligned}\sum_{p\le x}\sum_{\substack{s|p-1\\ t|p-1}}\sum_{\substack{q|\frac{p-1}{s}\\ r|\frac{p-1}{t}}}\frac{\phi\left(\frac{p-1}{s}\right)}{p-1}\frac{\phi\left(\frac{p-1}{t}\right)}{p-1}\left(1+O\left(\frac{1}{p}\right)\right)^2 &= \sum_{p\le x}\sum_{\substack{s|p-1\\ t|p-1}}\sum_{\substack{q|\frac{p-1}{s}\\ r|\frac{p-1}{t}}}\frac{\phi\left(\frac{p-1}{s}\right)}{p-1}\frac{\phi\left(\frac{p-1}{t}\right)}{p-1}\left(1+O\left(\frac{1}{p}\right)\right)^2\\ &= \sum_{p\le x}\frac{1}{(p-1)^2}\sum_{\substack{s|p-1\\ t|p-1}}\phi(s)\omega(s)\phi(t)\omega(t)\left(1+O\left(\frac{1}{p}\right)\right)^2\\ &= \sum_{p\le x}\frac{1}{(p-1)^2}\left(\sum_{s|p-1}\phi(s)\omega(s)\right)^2\left(1+O\left(\frac{1}{p}\right)\right)^2\\ &= \sum_{p\le x}\left(\omega(p-1)+O\left(\sum_{q|p-1}\frac{1}{q}\right)\right)^2\left(1+O\left(\frac{1}{p}\right)\right).\end{aligned}$$

By the Cauchy-Schwarz inequality and (18), the last expression is,

$$\begin{aligned}&= \sum_{p\le x}\omega(p-1)^2+O(\pi(x)\log\log x)\\ &= \pi(x)(\log\log x)^2+O(\pi(x)\log\log x).\end{aligned}$$

Therefore, we have (22) for $g(n)=\omega(n)$. For $g(n)=\Omega(n)$, we may use the estimates for $g(n)=\Omega(n)$ in Lemma 6.1. Then the proofs of (21) and (22) are complete. □

Also, by partial summation, the following estimates are immediate.

Corollary 6.2. *If $y > \exp((\alpha+\epsilon)\sqrt{\log x})$, then*

$$\mathfrak{A}(x) := \sum_{p \le x} \frac{\frac{1}{y}\sum_{a\le y} g(\ell_a(p))}{p} = \frac{1}{2}(\log\log x)^2 + O(\log\log x), \tag{23}$$

$$\mathfrak{B}(x)^2 := \sum_{p \le x} \frac{\left(\frac{1}{y}\sum_{a\le y} g(\ell_a(p))\right)^2}{p} = \frac{1}{3}(\log\log x)^3 + O((\log\log x)^2). \tag{24}$$

Here, $g(n) = \omega(n)$ or $\Omega(n)$.

7. Kubilius-Shapiro Theorem and Proof of Theorem 1.3

We say that an arithmetic function $f(n)$ is strongly additive if $f(mn) = f(m) + f(n)$ for any $(m,n) = 1$, and $f(p^a) = f(p)$ for any $a \ge 1$. The following result by Kubilius and Shapiro will be essential in this paper (see [E, Theorem 12.2]).

Lemma 7.1 (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,

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

We define a strongly additive arithmetic function by

$$F(n) := \frac{1}{y}\sum_{a\le y}\sum_{p\mid n}\Omega(\ell_a(p)).$$

As treated in [MS, (38)] and [EP, p. 348], we have for any $\epsilon > 0$,

$$\begin{aligned}\sum_{\substack{p\le x\\ |F(p)|>\epsilon\mathfrak{B}(x)}} \frac{F(p)^2}{p} &= \sum_{\substack{p\le x\\ |F(p)|>\epsilon\mathfrak{B}(x)}} \frac{\left(\frac{1}{y}\sum_{a\le y}\Omega(\ell_a(p))\right)^2}{p} \\ &\le \sum_{\substack{p\le x\\ |\Omega(p-1)|>\epsilon\mathfrak{B}(x)}} \frac{\Omega(p-1)^2}{p} = o(\mathfrak{B}(x)^2).\end{aligned}$$

Therefore, by Kubilius-Shapiro theorem, we have

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

In order to prove Theorem 1.3, we need to show that the four functions

$$F(n), \quad G(n) := \frac{1}{y}\sum_{a\le y}\sum_{p\mid n}\omega(\ell_a(p)), \quad \frac{1}{y}\sum_{a\le y}\Omega(\ell_a(n)), \quad \text{and} \quad \frac{1}{y}\sum_{a\le y}\omega(\ell_a(n))$$

are not very much different. We prove inequalities between the four functions without averaging and uniform in a.

Lemma 7.2. *For any $a \geq 1$, we have*
$$\sum_{p|n} \omega(\ell_a(p)) + O(\omega(n)) + O(\Omega(\phi(n)) - \omega(\phi(n))) \leq \omega(\ell_a(n))$$
$$\leq \Omega(\ell_a(n)) \leq \sum_{p|n} \Omega(\ell_a(p)) + O(\Omega(n) - \omega(n)).$$

Proof. The inequality in the middle is clear. The last inequality is by
$$\ell_a(n) = \underset{p^k||n}{\mathrm{LCM}} \ \ \ell_a(p^k),$$
which implies
$$\ell_a(n) | \prod_{p^k||n} \ell_a(p^k).$$
Note that $\ell_a(p^k) \leq \ell_a(p) + k - 1$ for any a and p. If $(a,p) \neq 1$, then $\ell_a(p^k) = \ell_a(p) = \ell_a(1) = 1$ due to the extended definition of $\ell_a(p)$. If $(a,p) = 1$, then $a^{\ell_a(p)} \equiv 1 \pmod{p}$. This gives $a^{p^{k-1}\ell_a(p)} \equiv 1 \pmod{p}$. It follows that $\ell_a(p^k) | p^{k-1}\ell_a(p)$. Thus, the claim follows. Then
$$\Omega(\ell_a(n)) \leq \sum_{p^k||n} \Omega(\ell_a(p^k)) \leq \sum_{p^k||n} (\Omega(\ell_a(p)) + k - 1) = \sum_{p|n} \Omega(\ell_a(p)) + \Omega(n) - \omega(n).$$
Thus, the third inequality follows.

For the first inequality, we use the following again
$$\ell_a(n) = \underset{p^k||n}{\mathrm{LCM}} \ \ \ell_a(p^k).$$
This shows that
$$\omega(\ell_a(n)) = \omega(\ell_a(\mathrm{rad}(n))) + O(\omega(n)) = \omega(\underset{p|n}{\mathrm{LCM}} \ \ \ell_a(p)) + O(\omega(n)).$$
Note that by $\ell_a(p) | p-1$, we have
$$\sum_{p|n} \omega(\ell_a(p)) - \omega(\underset{p|n}{\mathrm{LCM}} \ \ \ell_a(p)) = \sum_{\substack{q | \underset{p|n}{\mathrm{LCM}} \ \ell_a(p) \\ q | \ell_a(p) \text{ for } k \geq 2 \text{ primes } p|n}} (k-1) \leq \sum_{\substack{q | \underset{p|n}{\mathrm{LCM}} \ p-1 \\ q | p-1 \text{ for } k \geq 2 \text{ primes } p|n}} (k-1).$$
That is,
$$0 \leq \sum_{p|n} \omega(\ell_a(p)) - \omega(\underset{p|n}{\mathrm{LCM}} \ \ \ell_a(p)) \leq \sum_{p|n} \omega(p-1) - \omega(\lambda(\mathrm{rad}(n))) \leq \Omega(\phi(n)) - \omega(\phi(n)) + O(\omega(n)).$$
Here, $\lambda(n)$ is the Carmichael's lambda function and $\mathrm{rad}(n)$ is the largest square-free divisor of n. Thus,
$$\omega(\ell_a(n)) - \sum_{p|n} \omega(\ell_a(p)) = O(\Omega(\phi(n)) - \omega(\phi(n))) + O(\omega(n)).$$
This proves the first inequality. □

Lemma 7.3. *We have*
$$\sum_{p|n} (\Omega(\ell_a(p)) - \omega(\ell_a(p))) = O(\Omega(\phi(n)) - \omega(\phi(n))) + O(\omega(n)).$$

Proof. Note that
$$0 \leq \sum_{p|n} (\Omega(\ell_a(p)) - \omega(\ell_a(p))) = \sum_{p|n} \sum_{\substack{q^k || \ell_a(p) \\ k \geq 2}} (k-1) \leq \sum_{p|n} \sum_{\substack{q^\ell || p-1 \\ \ell \geq 2}} (\ell - 1) = \sum_{p|n} (\Omega(p-1) - \omega(p-1)).$$
We have
$$\sum_{p|n} \Omega(p-1) \leq \Omega(\phi(n))$$

and

$$\sum_{p|n}\omega(p-1)\geq\omega(\lambda(\mathrm{rad}(n)))=\omega(\phi(n))+O(\omega(n)).$$

Thus,

$$\sum_{p|n}(\Omega(p-1)-\omega(p-1))=O(\Omega(\phi(n))-\omega(\phi(n)))+O(\omega(n)).$$

□

As a consequence, the differences between any two members of the set

$$\left\{\Omega(\ell_a(n)),\omega(\ell_a(n)),\sum_{p|n}\Omega(\ell_a(p)),\sum_{p|n}\omega(\ell_a(p))\right\}$$

are, uniformly for a,

$$O(\Omega(\phi(n))-\omega(\phi(n)))+O(\Omega(n)).$$

Now, we are ready to prove Theorem 1.3.

Proof of Theorem 1.3. Applying the average over $a\leq y$, the differences between any two members of the set

$$\left\{\frac{1}{y}\sum_{a\leq y}\Omega(\ell_a(n)),\frac{1}{y}\sum_{a\leq y}\omega(\ell_a(n)),\frac{1}{y}\sum_{a\leq y}\sum_{p|n}\Omega(\ell_a(p)),\frac{1}{y}\sum_{a\leq y}\sum_{p|n}\omega(\ell_a(p))\right\}$$

are also

$$O(\Omega(\phi(n))-\omega(\phi(n)))+O(\Omega(n)).$$

By the Hardy-Ramanujan theorem [MV, Corollary 2.13], it is well-known that $\Omega(n)=O(\log\log x)$ for all but $o(x)$ integers $n\leq x$. By [EP, (3.5)], we have $\Omega(\phi(n))-\omega(\phi(n))=O((\log\log x)(\log\log\log\log x))$ for all but $o(x)$ integers $n\leq x$. Thus, except possibly for $o(x)$ integers $n\leq x$, we have

$$O(\Omega(\phi(n))-\omega(\phi(n)))+O(\Omega(n))=O((\log\log x)(\log\log\log\log x))=o((\log\log x)^{\frac{3}{2}}).$$

Therefore, we also have (7) for the functions

$$\frac{1}{y}\sum_{a\leq y}\Omega(\ell_a(n)),\quad\text{and}\quad\frac{1}{y}\sum_{a\leq y}\omega(\ell_a(n)).$$

This completes the proof of Theorem 1.3. □

8. Proof of Theorem 1.4

We prove that $\phi(n)\tau(n)/n$ can be written as a Dirichlet convolution identity. This identity is used in proving a result (see Lemma 8.5) similar to the Titchmarsh Divisor Problem.

Lemma 8.1. We have

$$\frac{\phi(n)}{n}\tau(n)=\sum_{d|n}\tau(d)f\left(\frac{n}{d}\right),\tag{25}$$

where

$$\sum_{n=1}^{\infty}\frac{f(n)}{n^s}=\prod_p\left(1-\frac{2}{p^{s+1}}+\frac{1}{p^{2s+1}}\right)$$

is absolutely convergent on $\Re(s)>0$.

Proof. We begin with
$$\sum_{n=1}^{\infty}\frac{\frac{\phi(n)}{n}\tau(n)}{n^s}=\sum_{n=1}^{\infty}\frac{\tau(n)}{n^s}\sum_{n=1}^{\infty}\frac{f(n)}{n^s}.$$
Then we have
$$\sum_{n=1}^{\infty}\frac{f(n)}{n^s}=\prod_p\left(1+\frac{\left(1-\frac{1}{p}\right)2}{p^s}+\frac{\left(1-\frac{1}{p}\right)3}{p^{2s}}+\cdots\right)\left(1-\frac{1}{p^s}\right)^2$$
$$=\prod_p\left(1-\frac{1}{p}\left(\frac{2}{p^s}-\frac{1}{p^{2s}}\right)\right)=\prod_p\left(1-\frac{2}{p^{s+1}}+\frac{1}{p^{2s+1}}\right).$$
This Dirichlet series is absolutely convergent on $\Re(s)>0$. □

The numbers $C_1(a,r)$ and $C_2(a,r)$ are defined in [F] as
$$C_1(a,r):=\frac{\zeta(2)\zeta(3)}{\zeta(6)}\prod_{p|a}\left(1-\frac{p}{p^2-p+1}\right)\prod_{p|r}\left(1+\frac{p-1}{p^2-p+1}\right),$$
$$C_2(a,r):=C_1(a,r)\left(\gamma-\sum_p\frac{\log p}{p^2-p+1}+\sum_{p|a}\frac{p^2\log p}{(p-1)(p^2-p+1)}-\sum_{p|r}\frac{(p-1)p\log p}{p^2-p+1}\right).$$
Here, γ is the Euler's constant. We write $C_1:=C_1(1,1)$. Denote by q' the largest positive square-free divisor of q. The following is Theorem 2.4 in [F].

Lemma 8.2 (Titchmarsh Divisor Problem-Fiorilli)**.** Let $1\le q\le x^{\lambda}$ with $\lambda<1/10$. Then we have for any $A>0$,

$$\sum_{\substack{p\le x\\ p\equiv 1(q)}}\tau\left(\frac{p-1}{q}\right)\log p=\frac{x}{q}\left[C_1(1,q)\log x+2C_2(1,q)+C_1(1,q)\log\frac{(q')^2}{eq}\right]+E_q(x)+O\left(\frac{x^{\frac{1}{2}+\epsilon}}{q}\right),\tag{26}$$

where
$$\sum_{q<x^{\lambda}}|E_q(x)|=O\left(\frac{x}{\log^A x}\right).$$

Applying this lemma, we prove the following that will play a central role in estimating error terms.

Lemma 8.3. Under the same assumptions as in Lemma 8.2, the term $E_q(x)$ also satisfies

$$\sum_{q<x^{\lambda}}\tau(q)|E_q(x)|=O\left(\frac{x}{\log^A x}\right).\tag{27}$$

Proof. Note that there is a fixed $N>0$ such that $|E_q(x)|\le\frac{x\log^N x}{q}$ and $\sum_{q\le x}\frac{\tau^2(q)}{q}\le\log^N x$. We split the sum into two parts: $\tau(q)<\log^{A+2N}x$ and $\tau(q)\ge\log^{A+2N}x$. The first part is treated by replacing A by $2A+2N$ in Lemma 8.2. The second part is bounded by
$$\sum_{q<x^{\lambda}}\frac{\tau^2(q)}{\log^{A+2N}x}|E_q(x)|\le\sum_{q<x^{\lambda}}\frac{x\tau^2(q)}{q\log^{A+N}x}\le\frac{x}{\log^A x}.$$
□

In the following lemma, we consider two convergent expressions K_1 and K_2 in double sums.

Lemma 8.4. The following double sums over positive integers u,d converge absolutely:

$$K_1=\sum_{u,d}\frac{f(u)}{d^2u}C_1(1,ud),\tag{28}$$

$$K_2 = \sum_{u,d} \frac{f(u)}{d^2 u} \left(2C_2(1, ud) + C_1(1, ud) \log \frac{((ud)')^2}{eud} \right). \tag{29}$$

Moreover, K_1 can be written as an Euler product,

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

Proof. From the definitions of $C_1(a, q)$ and $C_2(a, q)$ in [F, Section 3], we see that there is a fixed $N > 0$ such that $|C_1(1, q)| + |C_2(1, q)| = O(\log^N q)$. Thus, the double sums K_1 and K_2 converge absolutely. Let $C_1 = \frac{\zeta(2)\zeta(3)}{\zeta(6)}$. Also, if we write K_1 as Euler product, we have

$$\begin{aligned} K_1 = \sum_{d,u} \frac{f(u) C_1(1, du)}{d^2 u} &= \sum_q C_1(1, q) \sum_{du = q} \frac{f(u)}{d^2 u} \\ &= C_1 \prod_p \left[1 + \left(1 + \frac{p-1}{p^2 - p + 1} \right) \left[\left(1 - \frac{2}{p^2} + \frac{1}{p^3} \right) \left(1 - \frac{1}{p^2} \right)^{-1} - 1 \right] \right] \\ &= \prod_p \frac{p^3 - p + 1}{p^3 - p} = \prod_p \left(1 + \frac{1}{p^3 - p} \right). \end{aligned}$$

□

The following mean value theorem will be useful toward the proof of Theorem 1.4.

Lemma 8.5. *There are constants K_i's such that for any $A > 0$,*

$$\sum_{p \le x} \frac{\log p}{p - 1} \sum_{d | p-1} \tau(d) \phi(d) = K_1 x \log x + K_2 x + O\left(\frac{x}{\log^A x} \right). \tag{30}$$

The constant K_1 has an expression

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

Assuming the result of Lemma 8.5, the following corollary is proved by applying partial summation.

Corollary 8.1. Let K_1, K_2 be the constants in Lemma 8.1. Then we have for any $A > 0$,

$$\sum_{p \le x} \frac{1}{p - 1} \sum_{d | p-1} \tau(d) \phi(d) = K_1 x + (K_1 + K_2) \mathrm{Li}(x) + O\left(\frac{x}{\log^A x} \right). \tag{31}$$

Proof of Lemma 8.5. Interchanging the order of the sums, we have

$$\begin{aligned} \sum_{p \le x} \frac{\log p}{p - 1} \sum_{d | p-1} \tau(d) \phi(d) &= \sum_{p \le x} \frac{\log p}{p - 1} \sum_{d | p-1} \tau\left(\frac{p-1}{d} \right) \phi\left(\frac{p-1}{d} \right) \\ &= \sum_{d \le x-1} \sum_{\substack{p \le x \\ p \equiv 1 (d)}} \frac{\log p}{p - 1} \tau\left(\frac{p-1}{d} \right) \phi\left(\frac{p-1}{d} \right) \\ &= \sum_{d \le x-1} \frac{1}{d} \sum_{\substack{p \le x \\ p \equiv 1 (d)}} \frac{\phi\left(\frac{p-1}{d} \right)}{\frac{p-1}{d}} \tau\left(\frac{p-1}{d} \right) \log p. \end{aligned}$$

By Lemma 8.1, the sum is

$$= \sum_{d \le x-1} \frac{1}{d} \sum_{u \le \frac{x-1}{d}} f(u) \sum_{\substack{p \le x \\ p \equiv 1 (ud)}} \tau\left(\frac{p-1}{ud} \right) \log p.$$

By $\tau\left(\frac{p-1}{ud}\right)\log p \ll x^{\epsilon}$ and $du \le x-1$, we have

$$\sum_{\substack{p\le x\\ p\equiv 1 \pmod{ud}}} \tau\left(\frac{p-1}{ud}\right)\log p \ll \frac{x^{1+\epsilon}}{ud}.$$

Thus,

$$\sum_{\max(u,d)\ge x^{1/22}} \frac{|f(u)|}{d} \sum_{\substack{p\le x\\ p\equiv 1 (ud)}} \tau\left(\frac{p-1}{ud}\right)\log p \ll \sum_{\max(u,d)\ge x^{1/22}} \frac{|f(u)|x^{1+\epsilon}}{d^2u} \ll x^{21/22+\epsilon}.$$

We may truncate the sums over d and u. Then we apply Lemma 8.2 to treat the inner sum over p.

$$\begin{aligned}
&= \sum_{d<x^{1/22}} \sum_{u<x^{1/22}} \frac{f(u)}{d} \sum_{\substack{p\le x\\ p\equiv 1 (ud)}} \tau\left(\frac{p-1}{ud}\right)\log p + O(x^{21/22+\epsilon})\\
&= \sum_{\substack{d<x^{1/22}\\ u<x^{1/22}}} \frac{f(u)}{d}\frac{x}{ud}\left[C_1(1,ud)\log x + 2C_2(1,ud) + C_1(1,ud)\log\frac{((ud)')^2}{eud}\right]\\
&\quad + \sum_{\substack{d<x^{1/22}\\ u<x^{1/22}}} \frac{f(u)}{d}E_{ud}(x) + O\left(\sum_{\substack{d<x^{1/22}\\ u<x^{1/22}}} \frac{x^{\frac{1}{2}+\epsilon}}{ud}\right) + O(x^{21/22+\epsilon}).
\end{aligned}$$

By Lemma 8.3 and 8.4, we have

$$\begin{aligned}
&= x\log x\sum_{d,u}\frac{f(u)}{d^2u}C_1(1,ud) + x\sum_{d,u}\frac{f(u)}{d^2u}\left(2C_2(1,ud) + C_1(1,ud)\log\frac{((ud)')^2}{eud}\right)\\
&\quad + O\left(\frac{x}{\log^A x}\right) + O(x^{21/22+\epsilon})\\
&= K_1 x\log x + K_2 x + O\left(\frac{x}{\log^A x}\right).
\end{aligned}$$

□

A similar application of the above method yields an asymptotic formula of an independent interest. For any $A>1$ and an absolute constant K_4, we have

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

Now, we are ready to prove Theorem 1.4.

Proof of Theorem 1.4. The contribution of $a\le y$ for which $p|a$ and $p\le x$ is

$$\ll \frac{1}{y}\sum_{p\le x} 1\cdot\left(1+\frac{y}{p}\right) \ll \frac{x}{y\log x} + \log\log x.$$

Then

$$\begin{aligned}
y^{-1}\sum_{a\le y}\sum_{\substack{p\le x\\(a,p)=1}}\tau(\ell_a(p)) &= y^{-1}\sum_{a\le y}\sum_{\substack{p\le x\\(a,p)=1}}\sum_{d|\ell_a(p)}1\\
&= y^{-1}\sum_{a\le y}\sum_{p\le x}\sum_{w|p-1}\sum_{d|\frac{p-1}{w}}\sum_{\ell_a(p)=\frac{p-1}{w}}1\\
&= y^{-1}\sum_{p\le x}\sum_{\substack{w|p-1\\d|\frac{p-1}{w}}}\sum_{\chi(\mathrm{mod}\ p)}c_w(\chi)\sum_{a\le y}\chi(a).
\end{aligned}$$

The contribution of the principal characters modulo p is

$$\sum_{p\le x}\sum_{w|p-1}\frac{\phi\left(\frac{p-1}{w}\right)\tau\left(\frac{p-1}{w}\right)}{p-1}=\sum_{p\le x}\frac{\sum_{d|p-1}\phi(d)\tau(d)}{p-1},$$

which is $K_1x+(K_1+K_2)\mathrm{Li}(x)+O(x\log^{-B}x)$ by Corollary 8.1.

The contribution of non-principal characters to the sum is

$$\ll\frac{1}{y}\sum_{p\le x}\tau_3(p-1)\sideset{}{^*}\sum_{\chi(\mathrm{mod}\ p)}\frac{1}{\mathrm{ord}(\chi)}\left|\sum_{a\le y}\chi(a)\right|$$

which is $\ll x\exp(-c\sqrt{\log x})$ as we have seen in the proof of Lemma 6.2. Then the proof of Theorem 1.4 is complete. □

9. Further Developments

The method in this paper applies to several other results relying on Stephens' method. The result of Theorem 1.1 can be stated as a special case of [AF2, Theorem 1.4]. If we replace [AF2, Lemma 3.2] by Lemma 3.1-3.3, the result of [AF2, Theorem 1.4] holds true for $y>\exp((\alpha+\epsilon)\sqrt{\log x})$. If we replace [AF, Lemma 2.5] by Lemma 3.1-3.3, we may be able to determine a lower bound of c_1 in the results of [AF]. Moreover, the results of [PM] rely on [S1]. Thus, we may replace corresponding lemmas in [PM] to obtain an improved result. Another set of problems we can consider is on the multiplicative order of a modulo n, and primitive roots in $(\mathbb{Z}/n\mathbb{Z})^*$. These are studied in [L], [LP], and they rely on [S1]. The corresponding improvements of the results by using the idea of Lemma 3.1-3.3 will be carried on in an upcoming paper.

References

[AF] A. Akbary, A. T. Felix *On invariants of elliptic curves on average*, Acta Arithmetica, 168.1, (2015), pp. 31-70.

[AF2] A. Akbary, A. T. Felix, *On the average value of a function of the residual index*, Springer Proceedings in Mathematics & Statistics, Volume 251(2018), pp. 19-37.

[B] 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, pp. 1-35.

[Br] N. G. de Bruijn, *The Asymptotic Behavior of a Function Occuring in the Theory of Primes*, Journal of Indian Mathematical Society, New Series, 15(1951), pp. 25-32.

[C] R. D. Carmichael, *The Theory of Numbers*, Wiley (New York, 1914).

[BFI] E. Bombieri, J. Friedlander, H. Iwaniec, *Primes in Arithmetic Progressions to Large Moduli*, Acta Mathematica 156(1986), pp. 203-251.

[E] P. D. T. A. Elliott, *Probabilistic Number Theory II: Central Limit Theorems*, Springer 1980.

[EK] 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.

[EP] 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, pp. 343-352.

[F] D. Fiorilli, *On a Theorem of Bombieri, Friedlander and Iwaniec*, Canadian J. Math 64(2012), pp. 1019-1035.

[H] H. Halberstam, *On the distribution of additive number-theoretic functions (I, II, III)*, J. London Math. Soc. 30(1955), pp. 43-53; 31(1956), pp. 1-14; 31(1956), pp. 15-27.

[Ho] C. Hooley, *On Artin's Conjecture*, Journal für die Reine und Angewandte Mathematik, Volume 225, (1967) pp. 209-220.

[HT] A. Hildebrand, G. Tenenbaum, *Integers without Large Prime Factors*, Journal de Théorie des Nombres de Bordeaux, tome 5, no. 2 (1993), pp. 411-484.
[K1] S. Kim, *The Average Number of Divisors of the Euler Function*, Ramanujan Journal, May 2017, pp. 1-29.
[K2] S. Kim, *Average Results on the Order of a mod p*, Journal of Number Theory, Dec. 2016, pp. 353-368.
[L] S. Li, *An Improvement of Artin's Conjecture on Average for Composite Moduli*, Mathematika 51 (2004), pp. 97-109.
[LP] S. Li, C. Pomerance, *The Artin-Carmichael Primitive Root Problem on Average*, Mathematika 55(2009), pp. 13-28.
[LP2] F. Luca, C. Pomerance, *On the Average Number of Divisors of Euler Function*, Publ. Math. Debrecen, 70/1-2 (2007), pp. 125-148.
[PM] C. Pehlivan, L. Menici, *Average r-rank Artin Conjecture*, Acta Arithmetica 174 (2016), pp. 255-276.
[MS] M. R. Murty, F. Saidak, *Non-Abelian Generalizations of the Erdős-Kac Theorem*, Canad. J. Math. Vol. 56(2), 2004, pp. 356-372.
[MV] H. Montgomery, R. Vaughan, *Multiplicative Number Theory I, Classical Theory*, Cambridge University Press 2006.
[S1] P. J. Stephens, *An Average Result for Artin's Conjecture*, Mathematika, Volume 16, Issue 2, December 1969, pp. 178-188.
[S2] P. J. Stephens, *Prime Divisors of Second Order Linear Recurrences II*, Journal of Number Theory, Volume 8, Issue 3, August 1976, pp. 333-345.
[T] G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory*, Cambridge University Press 1995.