

AN IMPROVEMENT OF ARTIN'S CONJECTURE ON AVERAGE FOR COMPOSITE MODULI

SHUGUANG LI

1. Introduction

Let q be a natural number. When the multiplicative group $(\mathbb{Z}/q\mathbb{Z})^*$ is a cyclic group, its generators are called primitive roots. Note that the generators are also elements with the maximum order if $(\mathbb{Z}/q\mathbb{Z})^*$ is cyclic. Thus, when $(\mathbb{Z}/q\mathbb{Z})^*$ is not a cyclic group, we then call its element with the maximal possible order a primitive root, which was initially introduced by R. Carmichael [1].

Let a be an integer and x be any positive real number. In 1927, Artin conjectured that the number $P_a(x)$ of the primes up to x , for which a is a primitive root, is proportion to the number of primes up to x , namely $\pi(x)$. Although this conjecture has not been proved unconditionally, many results [3, 4, 6] have been achieved, favoring the conjecture from various perspectives. For a survey of Artin's conjecture, the reader may refer to Murty [12].

Among the unconditional results of Artin's conjecture is Stephens' theorem [14] on the average of $P_a(x)$ that is relevant to the work of this paper: if $y > \exp(4(\ln x \ln \ln x)^{1/2})$ then

$$(1) \quad \frac{1}{y} \sum_{a \leq y} P_a(x) = A \cdot \text{li } x + O\left(\frac{x}{\ln^D x}\right)$$

where $A = \prod_{\text{prime } p} (1 - \frac{1}{p(p-1)})$ and D is an arbitrary constant larger than 1. In obtaining this estimate, Stephens introduced a character sum to $P_a(x)$. Note that all moduli in $P_a(x)$ are primes and every non-principal character modulo a prime is a primitive character. It does not take too much effort for Stephens to apply results from large sieve to the character sum to achieve the above theorem. In the same paper, he also obtained an estimate of $\frac{1}{y} \sum_{a \leq y} (P_a(x) - A \cdot \text{li } x)^2$, which allows him to find an upper bound for the number of exceptions to the result in (1).

What would happen if the moduli are not restricted to primes? Let $N_a(x)$ be the number of moduli up to x for which a is a primitive root. In view of Artin's conjecture, one might conjecture that $N_a(x)$ is proportion to $[x]$, the number of natural numbers up

to x . On the contrary, this conjecture was proved wrong. In [8] the author proved that, for any $y \geq x$,

$$(2) \quad \underline{\lim}_{x \rightarrow \infty} \sup_{y \geq x} \frac{1}{xy} \sum_{a \leq y} N_a(x) = 0 \text{ and } \overline{\lim}_{x \rightarrow \infty} \inf_{y \geq x} \frac{1}{xy} \sum_{a \leq y} N_a(x) > 0.$$

Based on the results in (2), one may naturally guess that, for most integers a , the individual $N_a(x)/x$ should behave the same way as the average in (2). Namely,

$$\underline{\lim}_{x \rightarrow \infty} N_a(x)/x = 0, \text{ and } \overline{\lim}_{x \rightarrow \infty} N_a(x)/x > 0$$

for most of integers a . The first conjecture is proved in [9], free of any hypothesis for all integers a . The second conjecture is proved in [10] on assumption of GRH. The set of exceptional integers a to the second conjecture can also be found in [10].

In comparison with (1), the interval of a for averaging $N_a(x)$ in (2) is too large. The purpose of the paper is to show that (2) still holds for smaller values of y . Indeed, by introducing Dirichlet characters to $\sum_{a \leq y} N_a(x)$ and using the well-known inequality of Pólya-Vinogradov (see [13] and [16]), we can prove

THEOREM 1. *For any positive real numbers $x, y \geq 3$, we have*

$$(3) \quad \frac{1}{y} \sum_{a \leq y} N_a(x) = \sum_{n \leq x} \frac{R(n)}{n} + O \left(\frac{x^{3/2}}{y} \cdot \exp \left(\left(\frac{\ln x}{\ln \ln x} \right)^{1/2} \right) \right),$$

where $R(n)$ is the number of primitive roots modulo n within interval $[1, n]$.

Since the upper bound for the character sums in Pólya-Vinogradov inequality is attained very rarely [5], its application in Theorem 1 leaves a lot of room for more accurate estimation. With work in this direction, we are able to prove

THEOREM 2. *If $x \geq e^3$ and $y \geq \exp((\ln x)^{\frac{3}{4}})$, then*

$$(4) \quad \frac{1}{y} \sum_{a \leq y} N_a(x) = \sum_{n \leq x} \frac{R(n)}{n} + O \left(x \cdot \exp \left(-\frac{5}{16} (\ln x)^{\frac{1}{2}} \right) \right),$$

where $R(n)$ is the same as in Theorem 1. Moreover, $(\ln x)^{1/2}$ in the error term can be replaced by $(\ln y)^2 / \ln x$ if y is in the interval $[\exp((\ln x)^{\frac{3}{4}}), x^{\frac{1.01}{2}}]$.

It has been proved ([8]) that on an unbounded set of x we have $\sum_{n \leq x} \frac{R(n)}{n} \geq c \cdot x$ for some positive constant c , and on another unbounded set of x we have $\sum_{n \leq x} \frac{R(n)}{n} \leq o(x)$. Combining these results with Theorem 2, we can deduce

COROLLARY 3. *The statement in (2) holds for $y > \exp((\ln x)^{\frac{3}{4}})$.*

The main idea that leads to the proof of the two theorems is inspired from Stephens' method in proving (1). The author believes that the best lower bound for y , for which similar statement as in Theorem 2 holds, would be something like the one in Stephens' theorem in (1).

The author is grateful to Carl Pomerance for encouraging him to work on the problem and making valuable suggestions.

2. Involvement of Characters in Estimation of $N_a(x)$

In the following, let \mathbb{C} be the set of complex numbers and \mathbb{C}^* be the set of nonzero complex numbers. A homomorphism from Abelian group G to \mathbb{C}^* is called a character of G . Let q be any positive integer and χ be a Dirichlet character, which is a function χ from \mathbb{Z} to \mathbb{C} such that (i) $\chi(n+q) = \chi(n)$ for any integer n ; (ii) $\chi(n) \neq 0$ if $\gcd(n, q) = 1$ and $\chi(n) = 0$ if otherwise; (iii) $\chi(n \cdot m) = \chi(n) \cdot \chi(m)$ for any integers n and m . Due to its periodicity, χ induces a function $\bar{\chi}$ from $\mathbb{Z}/q\mathbb{Z}$ to \mathbb{C} such that

$$(5) \quad \bar{\chi} \circ \psi = \chi$$

where ψ is the natural homomorphism from ring \mathbb{Z} to $\mathbb{Z}/q\mathbb{Z}$. $\bar{\chi}$ is also a group character of $(\mathbb{Z}/q\mathbb{Z})^*$. Conversely each such group character $\bar{\chi}$ can be extended over $\mathbb{Z}/q\mathbb{Z}$ by defining $\bar{\chi}(\bar{a}) = 0$ for those residue classes \bar{a} where $\gcd(a, q) \neq 1$. Then, by equation (5), we obtain a Dirichlet character χ modulo q .

In this sense we will use the same notation for a Dirichlet character and its corresponding group character of $(\mathbb{Z}/q\mathbb{Z})^*$ although they are actually related by equation (5).

LEMMA 4. *Let χ be a character modulo q , and $c(\chi) = \frac{1}{\phi(q)} \sum'_b \chi(b)$ where the prime means that the sum is taken over all primitive roots between 1 and q modulo q . Then we have*

$$\sum_{\chi \bmod q} c(\chi) \cdot \chi(a) = \begin{cases} 1, & \text{if } a \text{ is a primitive root} \pmod{q} \\ 0, & \text{otherwise.} \end{cases}$$

Proof: By the definition of $c(\chi)$ we have

$$(6) \quad \sum_{\chi \bmod q} c(\chi) \cdot \chi(a) = \sum_{\chi \bmod q} \frac{1}{\phi(q)} \sum'_b \chi(a) \cdot \chi(b) = \sum'_b \frac{1}{\phi(q)} \sum_{\chi \bmod q} \chi(ab).$$

If a is not a primitive root then $ab \not\equiv 1 \pmod{q}$ for any primitive root b . If a is a primitive root then so is a^{-1} . Since $\sum_{\chi \bmod q} \chi(c) = 0$ if $c \not\equiv 1 \pmod{q}$ (see p.30 of [2]),

the only nontrivial contribution to the sum on the right side of (6) comes from the terms with $b = a^{-1}$, which is

$$\frac{1}{\phi(q)} \sum_{\chi \bmod q} \chi(a \cdot a^{-1}) = 1.$$

We have then proved the lemma.

LEMMA 5. *Let $N_a(x)$ be the number of moduli up to x for which a is a primitive root. Then, for any real numbers $x, y \geq 1$, we have*

$$(7) \quad \sum_{a \leq y} N_a(x) = y \cdot \sum_{n \leq x} \frac{R(n)}{n} + \sum_{n \leq x} \sum_{a \leq y} \sum_{\substack{\chi \bmod n \\ \chi \neq \chi_0}} c(\chi) \chi(a) + O(x \ln x),$$

where $R(n)$ is the number of primitive roots modulo n within the interval $[1, n]$, and χ_0 is the principal character modulo n .

Proof: Let $t_a(n)$ be a counting function of primitive roots which takes value 1 if a is a primitive root for n , and 0 if otherwise. By the definition of $N_a(x)$ and Lemma 4, $\sum_{a \leq y} N_a(x)$ can be written as

$$(8) \quad \begin{aligned} & \sum_{a \leq y} \sum_{n \leq x} t_a(n) = \sum_{n \leq x} \sum_{a \leq y} t_a(n) = \sum_{n \leq x} \sum_{a \leq y} \sum_{\chi \bmod n} c(\chi) \chi(a) \\ & = \sum_{n \leq x} \sum_{a \leq y} c(\chi_0) \chi_0(a) + \sum_{n \leq x} \sum_{a \leq y} \sum_{\substack{\chi \bmod n \\ \chi \neq \chi_0}} c(\chi) \chi(a). \end{aligned}$$

By the inclusion and exclusion principle, the number of positive integers up to y which are relatively prime to n is given by $[y] - \sum_{p|n} \left[\frac{y}{p} \right] + \sum_{p,q|n} \left[\frac{y}{p \cdot q} \right] - \dots$ or $[y] \frac{\phi(n)}{n} + O(2^{\omega(n)})$, where $\omega(n)$ is the number of distinct prime factors of integer n . Note that $c(\chi_0) = \frac{R(n)}{\phi(n)}$. We have

$$\begin{aligned} & \sum_{n \leq x} \sum_{a \leq y} c(\chi_0) \chi_0(a) = \sum_{n \leq x} \frac{R(n)}{\phi(n)} \sum_{\substack{a \leq y \\ \gcd(a,n)=1}} 1 \\ & = \sum_{n \leq x} \frac{R(n)}{\phi(n)} \left(\frac{\phi(n)}{n} y + O(2^{\omega(n)}) \right) = y \cdot \sum_{n \leq x} \frac{R(n)}{n} + O(x \ln x), \end{aligned}$$

where the average order of $2^{\omega(n)}$ in the last equation is a well-known result ([15]). We have proved the lemma.

3. Estimate of $c(\chi)$ and Proof of Theorem 1

In view of Lemma 5 a sharp bound of $c(\chi)$ for any non-principal character χ modulo q is critical for a good estimate of the error term. In [14], it is found that $|c(\chi)| \leq 1/\text{ord}(\chi)$ where $\text{ord}(\chi)$ denotes the order of χ . But when the moduli are not primes, this bound is not good enough.

Throughout this section, C_m represents a cyclic group of order m and χ is a character of a finite Abelian group. Any element of a finite Abelian group with the maximal order is called a primitive root of the group.

LEMMA 6. *Let G be a finite Abelian group and χ be a non-principal character of G . Then*

$$\sum_{b \in G} \chi(b) = 0.$$

Proof: See p. 254 of [7].

LEMMA 7. *Suppose that q is a prime and v is a natural number. Let χ be a character of cyclic group C_{q^v} . Let $C_{q^{v-1}}$ be the cyclic subgroup of C_{q^v} . Then*

$$\sum_{b \in C_{q^{v-1}}} \chi(b) = \begin{cases} 0, & \text{if } \text{ord}(\chi) > q, \\ q^{v-1}, & \text{if } \text{ord}(\chi) \leq q. \end{cases}$$

Proof: Let α be a generator of C_{q^v} , and $\eta = \chi(\alpha)$. Then $\eta^{q^v} = \chi(\alpha^{q^v}) = 1$. Thus the order of η , which is equal to order $\text{ord}(\chi)$, divides q^v . On the other hand, since α^q is a generator of the subgroup $C_{q^{v-1}}$, we have

$$\sum_{b \in C_{q^{v-1}}} \chi(b) = \sum_{0 \leq k < q^{v-1}} \chi(\alpha^{qk}) = \sum_{0 \leq k < q^{v-1}} \eta^{qk}.$$

If $\text{ord}(\chi) > q$, then $\eta^q \neq 1$ and the above sum is equal to

$$\frac{1 - \eta^{q^v}}{1 - \eta^q} = 0.$$

If $\text{ord}(\chi) \leq q$, then $\eta^{qk} = 1$ and the above sum is equal to q^{v-1} . We have proved the lemma.

Let q be a prime and G be a finite Abelian q -group, which means that the order of G is a power of q . By a well-known fact about Abelian groups, G can be written as

$$(9) \quad G = G_1 \otimes \cdots \otimes G_\Delta \otimes H,$$

where each of G_i is a cyclic subgroup of G of order q^v , and H has no cyclic subgroup of order q^v . Then it is well-known that any character χ of G can be factored as,

$$(10) \quad \chi = \chi_1 \cdots \chi_\Delta \cdot \chi_H$$

where χ_i and χ_H are the corresponding characters of G_i and H , respectively.

LEMMA 8. *Let q be a prime and G be a finite Abelian q -group for which (9) holds. Let χ be a character of G for which (10) holds. If χ is not the principal character, then*

$$\left| \sum_{\substack{\text{primitive} \\ \text{roots: } b \in G}} \chi(b) \right| = \begin{cases} |G|/q^\Delta, & \text{if each } \text{ord}(\chi_i) \leq q \text{ and } \chi_H = \chi_0, \\ 0, & \text{otherwise.} \end{cases}$$

If χ is the principal character, then

$$\left| \sum_{\substack{\text{primitive} \\ \text{roots: } b \in G}} \chi(b) \right| = |G|(1 - 1/q^\Delta).$$

Proof: If χ is not the principal character, by Lemma 6, we have

$$\sum_{\substack{\text{primitive} \\ \text{roots: } b \in G}} \chi(b) + \sum_{\substack{\text{non-primitive} \\ \text{roots: } b \in G}} \chi(b) = \sum_{b \in G} \chi(b) = 0.$$

Let s denote the second sum, and let G'_i be the cyclic subgroup of G_i of order $|G_i|/q$. Then

$$s = \sum_{b_i \in G'_i, b_H \in H} \chi_1(b_1) \cdots \chi_\Delta(b_\Delta) \chi_H(b_H) = \left[\prod_{i=1}^{\Delta} \left(\sum_{b \in G'_i} \chi_i(b) \right) \right] \cdot \left(\sum_{b \in H} \chi_H(b) \right).$$

By Lemma 7, $\sum_{b \in G'_i} \chi_i(b) = 0$ if $\text{ord} \chi_i > q$, and is equal to $|G_i|/q$ if $\text{ord}(\chi_i) \leq q$. By Lemma 6, $\sum_{b \in H} \chi_H(b) = 0$ if $\chi_H \neq \chi_0$, and is obviously $|H|$ if otherwise. Therefore, combining these facts with the above equation yields the first formula in the lemma.

If χ is the principal character, the above analysis still holds, which yields $s = |G|/q^\Delta$. On the other hand, $\sum_{b \in G} \chi(b) = |G|$. Thus, by the first equation of the proof,

$$\left| \sum_{\substack{\text{primitive} \\ \text{roots: } b \in G}} \chi(b) \right| = ||G| - s| = |G|(1 - 1/q^\Delta).$$

We have proved the lemma.

Let G and χ be the same as in Lemma 8. From the lemma, we have seen that the character sum has a non-trivial value if and only if $\text{ord}(\chi_i) \leq q$ for each i and χ_H is the principal character of H . We call such a character χ of G a **special character**.

Now let us turn our attention to Dirichlet characters. Let n be a nonzero integer. For each prime divisor q of $\phi(n)$, let G_q be the Sylow q -subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$. By a well-known result of group theory,

$$(11) \quad (\mathbb{Z}/n\mathbb{Z})^* \simeq \otimes_{q|\phi(n)} G_q.$$

Each character χ of $(\mathbb{Z}/n\mathbb{Z})^*$ can be factored as $\prod_{q|\phi(n)} \chi_q$, where χ_q is the corresponding character of G_q . If each such factor χ_q is a special character, then χ is called a **special character** of $(\mathbb{Z}/n\mathbb{Z})^*$. In other words, a special character is a character whose order is square-free and the factor χ_H defined in equation (10) for each χ_q is the principal character of H .

THEOREM 9. *Suppose that n is a nonzero integer and χ is a Dirichlet character modulo n . Let $\rho_n(d)$ denote the number of special characters modulo n of order d . If χ is not a special character, then $c(\chi) = 0$. If χ is a special character, then*

$$|c(\chi)| \leq \frac{1}{\rho_n(\text{ord}(\chi))}.$$

Proof: By the definition given in Lemma 4,

$$\phi(n) c(\chi) = \sum_{\substack{\text{primitive roots} \\ b \in (\mathbb{Z}/n\mathbb{Z})^*}} \chi(b).$$

With respect to the factorization of $(\mathbb{Z}/n\mathbb{Z})^*$ in (11), we can write $\chi = \prod_{q|\phi(n)} \chi_q$, where χ_q is a character of the Sylow q -subgroup G_q . Then $\chi(b) = \prod_{q|\phi(n)} \chi_q(b_q)$, where $b \rightarrow \prod_{q|\phi(n)} b_q$ is the isomorphism in (11). Note that b is a primitive root mod n if and only if each b_q is a primitive root in G_q . Thus,

$$\phi(n) c(\chi) = \sum_{\substack{\text{primitive roots} \\ b_q \in G_q, q|\phi(n)}} \prod_{q|\phi(n)} \chi_q(b_q) = \prod_{q|\phi(n)} \left(\sum_{\substack{\text{primitive roots} \\ b_q \in G_q}} \chi_q(b_q) \right).$$

If χ is not a special character, then one of its factors χ_q is not a special character of G_q . By Lemma 8, the corresponding factor in the factorization of $\phi(n) c(\chi)$ above is zero. Thus, $c(\chi) = 0$.

If χ is a special character, then so is each χ_q . Note that either $\chi_q = \chi_0$, the principal character of G_q , or $\text{ord}(\chi_q) = q$. By Lemma 8,

$$\sum_{\substack{\text{primitive} \\ \text{roots: } b_q \in G_q}} \chi_q(b_q) = \begin{cases} |G_q|/q^{\Delta_q(n)}, & \text{if } \text{ord}(\chi_q) = q, \\ |G_q|(1 - 1/q^{\Delta_q(n)}), & \text{if } \chi_q = \chi_0, \end{cases}$$

where $\Delta_q(n)$ is the subscript Δ in the factorization of $G = G_q$ in (9) (see [9] for another explanation of the function $\Delta_q(n)$). Therefore,

$$(12) \quad \phi(n) c(\chi) \leq \frac{\prod_{q|\phi(n)} |G_q|}{\prod_{\substack{q|\phi(n) \\ \text{ord}(\chi_q)=q}} q^{\Delta_q(n)}} = \frac{\phi(n)}{\prod_{\substack{q|\phi(n) \\ \text{ord}(\chi_q)=q}} q^{\Delta_q(n)}}.$$

Note that the denominator above is greater than the number of special characters of $(\mathbb{Z}/n\mathbb{Z})^*$ of order $\text{ord}(\chi)$, which is $\prod_{\substack{q|\phi(n) \\ \text{ord}(\chi_q)=q}} (q^{\Delta_q(n)} - 1)$. Therefore the inequality claimed in the theorem is true. We have proved the theorem.

Obviously, the denominator of (12) is greater than or equal to $\prod_{\substack{q|\phi(n) \\ \text{ord}(\chi_q)=q}} q = \text{ord}(\chi)$, if χ is a special character. Therefore, by (12) if χ is a special character and by Theorem 9 if χ is not a special character, we have the following corollary, which is used in the derivation of the major results in [14]. But it is not good enough for our derivation of Theorem 2.

COROLLARY 10. *Let χ be a character modulo n . Then*

$$|c(\chi)| \leq \frac{1}{\text{ord}(\chi)}.$$

Let n^* be a divisor of n . Let χ^* be a primitive character modulo n^* which induces χ modulo n . What we need for the deduction of Theorem 2 is the relation between $|c(\chi)|$ and $|c(\chi^*)|$. Complete understanding of this relation has yet to be clear. However, we find an alternative answer to the question in the next lemma.

If χ is a special character, then the number of the primitive characters χ^* modulo n^* , which induce special characters modulo n of the fixed order $\text{ord}(\chi)$, is less than or equal to $\rho_n(\text{ord}(\chi))$, the number of special characters modulo n with order $\text{ord}(\chi)$. Note that here $\text{ord}(\chi)$ is a squarefree integer and $|c(\chi)| \leq 1$. By Theorem 9 again, we have deduced the next lemma.

COROLLARY 11. *Let n^* be a divisor of n . For any primitive character χ^* modulo n^* , let χ be the induced character modulo n . Then, for any positive number $t \geq 1$, we*

have

$$\sum'_{\chi^* \bmod n^*} |c(\chi)|^t \leq \sum'_{\chi^* \bmod n^*} |c(\chi)| \leq \sum_{d|\phi(n^*)} |\mu(d)| = 2^{\omega(\phi(n^*))}$$

where the prime ' means that the sums are taken over primitive characters, and $\omega(\phi(n^*))$ is the number of distinct prime factors of $\phi(n^*)$.

We will end the section with a proof of Theorem 1.

LEMMA 12 (see [2, 13, 16]). *There exists an absolute constant c such that*

$$\left| \sum_{a \leq y} \chi(a) \right| \leq c\sqrt{n} \ln n$$

for any real number $y \geq 1$ and any non-principal character χ to the modulus n . Moreover, $c \leq 1$ if χ is a primitive character.

LEMMA 13 (see [11]). *Let $\tau(n)$ be the number of divisors of integer n . Then the estimate*

$$\sum_{x \leq n} \tau(\phi(n)) = x \cdot \exp \left(c(x) \cdot \left(\frac{\ln x}{\ln \ln x} \right)^{1/2} \cdot \left(1 + O \left(\frac{\ln x}{\ln \ln x} \right) \right) \right)$$

holds for large real numbers x where $c(x)$ is a number in the interval $[\frac{1}{8\sqrt{e^\gamma}}, \frac{1}{\sqrt{8e^\gamma}}]$, and γ is the Euler constant.

Proof of Theorem 1: Let E be the triple sum in Lemma 5. Obviously we have

$$|E| = \left| \sum_{n \leq x} \sum_{\substack{\chi \bmod n \\ \chi \neq \chi_0}} c(\chi) \sum_{a \leq y} \chi(a) \right| \leq \sum_{n \leq x} \sum_{\substack{\chi \bmod n \\ \chi \neq \chi_0}} |c(\chi)| \cdot \left| \sum_{a \leq y} \chi(a) \right|.$$

By Lemma 12, for some absolute constant c , we have

$$|E| \leq c \sum_{n \leq x} \sum_{\substack{\chi \bmod n \\ \chi \neq \chi_0}} |c(\chi)| \cdot n^{1/2} \ln n = c \sum_{n \leq x} n^{1/2} \ln n \sum_{\substack{\chi \bmod n \\ \chi \neq \chi_0}} |c(\chi)|.$$

Note that, from Theorem 9, $c(\chi) = 0$ if χ is not a special character modulo n , and $|c(\chi)| \leq 1/\rho_n(\text{ord}\chi)$ if χ is a special character modulo n . Also note that $\text{ord}\chi$ is a square-free divisor of $\phi(n)$ if χ is special. Thus

$$\sum_{\substack{\chi \bmod n \\ \chi \neq \chi_0}} |c(\chi)| \leq \sum_{d|\phi(n)} |\mu(d)| = 2^{\omega(\phi(n))},$$

where $\omega(n)$ is the number of distinct prime divisors of n , and

$$|E| \leq c \sum_{n \leq x} n^{1/2} \ln n \cdot 2^{\omega(\phi(n))} \leq c x^{1/2} \ln x \sum_{n \leq x} 2^{\omega(\phi(n))}.$$

By Lemma 13,

$$\sum_{n \leq x} 2^{\omega(\phi(n))} \ll x \cdot \exp\left(\frac{1}{\sqrt{8e^\gamma}} \left(\frac{\ln x}{\ln \ln x}\right)^{1/2}\right) \ll \frac{x}{\ln x} \cdot \exp\left(\left(\frac{\ln x}{\ln \ln x}\right)^{1/2}\right),$$

where the involved constants are absolute. Therefore,

$$|E| \ll x^{3/2} \cdot \exp\left(\left(\frac{\ln x}{\ln \ln x}\right)^{1/2}\right),$$

where the involved constant is absolute. We have then proved the theorem.

4. Proof of Theorem 2

LEMMA 14 (see [14]). *Let r be any natural number and x, y be positive real numbers.*

Then

$$\sum_{n \leq x} \sum'_{\chi \bmod n} \left| \sum_{a \leq y} \chi(a) \right|^{2r} \ll (x^2 + y^r) y^r \{\ln(ey^{r-1})\}^{r^2-1}$$

where \sum' means that the summation is over primitive characters only, and the involved constant is independent of r .

LEMMA 15. *Let $r \geq 2$ be any natural number. Let x, y be real numbers such that $x \geq 3$ and $y \geq 1$. If $\delta = \min\left\{r \frac{\ln y}{\ln x} - 1, \frac{2r}{r+2} \frac{\ln y}{\ln x}\right\}$ is in the interval $(0, 1)$, we have*

$$(13) \quad \sum_{n \leq x} \frac{1}{n} \sum'_{\chi \bmod n} \left| \sum_{a \leq y} \chi(a) \right|^{2r} \ll \frac{y^{2r}}{x^\delta} (\ln(ey^{r-1}))^{\max\{2r, r^2-1\}}$$

where \sum' means the same as in Lemma 14, and the involved constant is independent of r .

Proof: Note that if $n \leq 2$ the only character is the principal character. Thus

$$(14) \quad \begin{aligned} & \sum_{n \leq x} \frac{1}{n} \sum'_{\chi \bmod n} \left| \sum_{a \leq y} \chi(a) \right|^{2r} \\ &= \frac{1}{x} \sum_{n \leq x} \sum'_{\chi \bmod n} \left| \sum_{a \leq y} \chi(a) \right|^{2r} + \int_3^x \frac{1}{t^2} \sum_{n \leq t} \sum'_{\chi \bmod n} \left| \sum_{a \leq y} \chi(a) \right|^{2r} dt. \end{aligned}$$

By Lemma 14,

$$\frac{1}{x} \sum_{n \leq x} \sum'_{\chi \bmod n} \left| \sum_{a \leq y} \chi(a) \right|^{2r} \ll \left(x + \frac{y^r}{x} \right) y^r (\ln(ey^{r-1}))^{r^2-1}.$$

Let δ be a real number in $(0, 1)$. If $\delta \leq \frac{2r}{r+2} \cdot \frac{\ln y}{\ln x}$, then $\delta \ln x \leq \ln y^{r-1}$ provided $r \geq 2$. Also note that the characters below are primitive. Thus, the constant c in Lemma 12 can be taken as 1, and we have

$$\begin{aligned} & \int_3^{x^\delta} \frac{1}{t^2} \sum_{n \leq t} \sum'_{\chi \bmod n} \left| \sum_{a \leq y} \chi(a) \right|^{2r} dt \leq \int_3^{x^\delta} \frac{1}{t^2} \sum_{n \leq t} \sum'_{\chi \bmod n} n^r (\ln n)^{2r} dt \\ & \leq x^{\delta r} (\ln x^\delta)^{2r} \int_3^{x^\delta} \frac{1}{t^2} \sum_{n \leq t} n dt \leq x^{\delta(r+1)} (\delta \ln x)^{2r} \leq x^{\delta(r+1)} (\ln y^{r-1})^{2r}. \end{aligned}$$

By Lemma 14 again,

$$\begin{aligned} \int_{x^\delta}^x \frac{1}{t^2} \sum_{n \leq t} \sum'_{\chi \bmod n} \left| \sum_{a \leq y} \chi(a) \right|^{2r} dt & \ll \int_{x^\delta}^x \frac{1}{t^2} (t^2 + y^r) y^r (\ln(ey^{r-1}))^{r^2-1} dt \\ & \leq \left(x + \frac{y^r}{x^\delta} \right) y^r (\ln(ey^{r-1}))^{r^2-1}. \end{aligned}$$

Now let $\delta = \min \left\{ \frac{r \ln y}{\ln x} - 1, \frac{2r}{r+2} \cdot \frac{\ln y}{\ln x} \right\}$. Then we have $x \leq y^r/x^\delta$ and $x^{\delta(r+1)} \leq y^{2r}/x^\delta$. Therefore, if $0 < \delta < 1$, by combining the above estimates in (14), we have

$$\sum_{n \leq x} \frac{1}{n} \sum'_{\chi \bmod n} \left| \sum_{a \leq y} \chi(a) \right|^{2r} \ll \frac{y^{2r}}{x^\delta} (\ln(ey^{r-1}))^{\max\{2r, r^2-1\}}.$$

We have proved the lemma.

COROLLARY 16. *Let x, y, r and δ be the same as in Lemma 15. Then, for any natural number d such that $x/d, y/d \geq 1$, we have*

$$(15) \quad \sum_{n \leq x/d} \frac{1}{n} \sum'_{\chi \bmod n} \left| \sum_{a \leq y/d} \chi(a) \right|^{2r} \ll \frac{y^{2r}}{x^\delta} (\ln(ey^{r-1}))^{\max\{2r, r^2-1\}}$$

where \sum' means the same as in Lemma 14, and the involved constant is independent of r .

Proof: Suppose that $d \leq x$ and $d \leq y$. Obviously

$$\sum_{n \leq x/d} \frac{1}{n} \sum'_{\chi \bmod n} \left| \sum_{a \leq y/d} \chi(a) \right|^{2r} \leq \sum_{n \leq x} \frac{1}{n} \sum'_{\chi \bmod n} \left| \sum_{a \leq y/d} \chi(a) \right|^{2r},$$

which is, by Lemma 15,

$$\ll \frac{(y/d)^{2r}}{x^\delta} (\ln(e(y/d)^{r-1}))^{\max\{2r, r^2-1\}}$$

which in turn is less than or equal to the function on the right side of (15). Indeed the function on the right side of (15) is

$$\max\{y^r x, y^{2r(r+1)/(r+2)}\} (\ln(ey^{r-1}))^{\max\{2r, r^2-1\}}$$

which is increasing in y , so that its value at y is at least as big as its value at y/d . Therefore, we have proved the corollary.

Proof of Theorem 2: By Theorem 1 one can see that Theorem 2 is true for $y > x^{\frac{1}{2}} \exp(\ln^{\frac{1}{2}} x)$. Thus we only need to consider the case where $y \leq x^{1.01/2}$.

In view of Lemma 5 to prove Theorem 2 we only need to obtain a good estimate of

$$S = \sum_{n \leq x} \sum_{\substack{\chi \bmod n \\ \chi \neq \chi_0}} |c(\chi)| \cdot \left| \sum_{a \leq y} \chi(a) \right|.$$

Let χ^* be the primitive character modulo n^* which induces χ modulo n . Definitely $n^* | n$. Then

$$\sum_{a \leq y} \chi(a) = \sum_{n \leq y} \chi^*(n) \sum_{d | (n, n/n^*)} \mu(d) = \sum_{d | n/n^*} \chi^*(d) \mu(d) \sum_{a \leq y/d} \chi^*(a).$$

Also note that each χ is uniquely determined by χ^* , n^* and n . Thus

$$\begin{aligned} S &\leq \sum_{n \leq x} \sum_{\substack{\chi \bmod n \\ \chi \neq \chi_0}} |c(\chi)| \sum_{d | n/n^*} |\mu(d)| \cdot \left| \sum_{a \leq y/d} \chi^*(a) \right| \\ &= \sum_{n \leq x} \sum_{n^* | n} \sum'_{\chi^* \bmod n^*} |c(\chi)| \sum_{d | n/n^*} |\mu(d)| \cdot \left| \sum_{a \leq y/d} \chi^*(a) \right| \\ &= \sum_{d \leq x} |\mu(d)| \sum_{n^* \leq x/d} \sum_{\substack{n \leq x \\ d n^* | n}} \sum'_{\chi^* \bmod n^*} |c(\chi)| \cdot \left| \sum_{a \leq y/d} \chi^*(a) \right| \end{aligned}$$

where prime ' means that the sum is over the primitive characters modulo n^* . Using Holder's inequality and Corollary 11, we obtain

$$\begin{aligned} S^{2r} &\leq \left(\sum_{d \leq x} \sum_{n^* \leq \frac{x}{d}} \sum_{\substack{n \leq x \\ d n^* | n}} \sum'_{\chi^* \bmod n^*} |c(\chi)|^{\frac{2r}{2r-1}} \right)^{2r-1} \cdot \sum_{d \leq x} \sum_{n^* \leq \frac{x}{d}} \sum_{\substack{n \leq x \\ d n^* | n}} \sum'_{\chi^* \bmod n^*} \left| \sum_{a \leq \frac{y}{d}} \chi^*(a) \right|^{2r} \\ &\leq \left(\sum_{d \leq x} \sum_{n^* \leq x/d} \frac{x}{d n^*} 2^{\omega(\phi(n^*))} \right)^{2r-1} \cdot \sum_{d \leq x} \sum_{n^* \leq x/d} \frac{x}{d n^*} \sum'_{\chi^* \bmod n^*} \left| \sum_{a \leq y/d} \chi^*(a) \right|^{2r}. \end{aligned}$$

By Lemma 13,

$$\sum_{d \leq x} \sum_{n^* \leq x/d} \frac{x}{d n^*} 2^{\omega(\phi(n^*))} \ll x \sum_{d \leq x} \frac{1}{d} \ln x \exp \left(\frac{\left(\frac{\ln x}{\ln \ln x} \right)^{\frac{1}{2}}}{\sqrt{8e^\gamma}} \right) \ll x (\ln x)^2 \exp \left(\frac{\left(\frac{\ln x}{\ln \ln x} \right)^{\frac{1}{2}}}{\sqrt{8e^\gamma}} \right),$$

where γ is Euler's constant.

Assume that the conditions of Corollary 16 are satisfied. Then

$$\begin{aligned} \sum_{d \leq x} \sum_{n^* \leq x/d} \frac{x}{d n^*} \sum'_{\chi^* \bmod n^*} \left| \sum_{a \leq y/d} \chi^*(a) \right|^{2r} &\ll x \cdot \frac{y^{2r}}{x^\delta} (\ln(ey^{r-1}))^{\max\{2r, r^2-1\}} \cdot \sum_{d \leq x} \frac{1}{d} \\ &\ll x \cdot \frac{y^{2r}}{x^\delta} (\ln(ey^{r-1}))^{\max\{2r, r^2-1\}} \ln x, \end{aligned}$$

which, combined with the previous estimate, yields

$$S \ll x^{1-\frac{\delta}{2r}} y \cdot (\ln x)^2 \exp \left(\frac{2r-1}{2r\sqrt{8e^\gamma}} \left(\frac{\ln x}{\ln \ln x} \right)^{\frac{1}{2}} \right) (\ln(ey^{r-1}))^{\frac{\max\{2r, r^2-1\}}{2r}}$$

or

$$(16) \quad \frac{S}{xy} \ll x^{-\frac{\delta}{2r}} \cdot (\ln x)^2 \exp \left(\frac{2r-1}{2r\sqrt{8e^\gamma}} \left(\frac{\ln x}{\ln \ln x} \right)^{\frac{1}{2}} \right) (\ln(ey^{r-1}))^{\frac{\max\{2r, r^2-1\}}{2r}}.$$

Now let us take

$$r = \left\lfloor \frac{1.6 \ln x}{\ln y} \right\rfloor + 1.$$

Then $r \geq 4$ since $y \leq x^{1.01/2}$. Next we claim that

$$r \frac{\ln y}{\ln x} - 1 \geq \frac{2r}{r+2} \cdot \frac{\ln y}{\ln x},$$

which is equivalent to

$$(17) \quad \frac{r^2}{r+2} \geq \frac{\ln x}{\ln y}.$$

Indeed this inequality follows from the definition of r and the fact that $\ln x/\ln y \geq 2/1.01$. It can be verified first for $\ln x/\ln y$ in the interval $[2/1.01, 2.5)$ where $r = 4$. When $\ln x/\ln y \geq 2.5$, since $r^2/(r+2)$ is an increasing function and $r > 1.6 \ln x/\ln y$, the left-hand side of (17) is

$$> \frac{\left(\frac{1.6 \ln x}{\ln y}\right)^2}{\frac{1.6 \ln x}{\ln y} + 2} \geq \frac{\ln x}{\ln y}.$$

Then the number δ in Corollary 16 is $\frac{2r}{r+2} \cdot \frac{\ln y}{\ln x}$. Obviously $0 < \delta < 1$. Thus, we have cleared all the assumed conditions in the derivation of (16).

As $x^{-\delta/2r} = y^{-1/(r+2)}$, the logarithm of the right-hand side of (16)

$$(18) \quad -\frac{\ln y}{r+2} + 2 \ln \ln x + \frac{2r-1}{2r\sqrt{8e^\gamma}} \left(\frac{\ln x}{\ln \ln x}\right)^{\frac{1}{2}} + \frac{r^2-1}{2r} \ln \ln(ey^{r-1}).$$

The first term of (18) is less than or equal to $-(\ln y)^2/(3.03 \ln x)$. Indeed, this inequality follows from $r+2 \leq 3.03 \ln x/\ln y$, which can be verified for $\ln x/\ln y$ in the interval $[2/1.01, 2.5)$ where $r = 4$, and for $\ln x/\ln y \geq 2.5$ we have that $r+2 < 1.6 \ln x/\ln y + 3 \leq 2.8 \ln x/\ln y$. For $y \geq \exp((\ln x)^{3/4})$ the expression $(\ln y)^2/\ln x$ is at least $(\ln x)^{1/2}$. The second and third terms in (18) are clearly $o((\ln x)^{1/2})$, and so is the fourth for the stated range for y . By (16) and (18), we have

$$\frac{S}{x \cdot y} \ll \exp\left(-\frac{5}{16} \frac{(\ln y)^2}{\ln x}\right)$$

for all $x \geq e^3$ and y with $\exp((\ln x)^{\frac{3}{4}}) \leq y \leq x^{\frac{1.01}{2}}$. Thus, we have Theorem 2.

REFERENCES

- [1] R.D. CARMICHAEL, *The Theory of Numbers*, Wiley, New York, 1914.
- [2] H. DAVENPORT, *Multiplicative Number Theory*, Springer-Verlag, New York, 2000.
- [3] R. GUPTA AND M. RAM MURTY, A remark on Artin's conjecture, *Invent. Math.* **78** (1984), 127 – 130.
- [4] D.R. HEATH-BROWN, Artin's conjecture for primitive roots, *Quart. J. Math. Oxford* (2), **37**(1986), 27 – 38.
- [5] A. HILDEBRAND, Large Values of Character Sums, *J. Number Theory*, **29**(1988), 271 – 296.
- [6] C. HOOLEY, On Artin's conjecture, *J. reine angew. Math.* **225**(1967), 209 – 20.
- [7] K. IRELAND AND M. ROSEN, *A classical introduction to modern number theory*, 2nd ed., Springer-Verlag, New York, 1990.
- [8] S. LI, *Artin's conjecture on average for composite moduli*, *J. Number Theory* **84**(2000), 93 – 118.
- [9] S. LI, *On extending Artin's conjecture to composite moduli*, *Mathematika*, **46**(1999), 373 – 390.

- [10] S. LI AND C. POMERANCE, *On generalizing Artin's conjecture on primitive roots to composite moduli*, to appear in J. reine angew. Math.
- [11] F. LUCA AND C. POMERANCE, *On the average number of divisors of the Euler function*, preprint.
- [12] M.R. MURTY, *Artin's conjecture for primitive roots*, Math. Intelligencer **10** (1988), no. 4, 59 – 67.
- [13] G. PÓLYA, *Über die Verteilung der quadratischen Reste und Nichtreste*, Nachrichten Königl. Ges. Wiss. Göttingen (1918), pp. 30-36.
- [14] P.J. STEPHENS, *An average result for Artin's conjecture*, Mathematika **16**(1969), 178 – 188.
- [15] G. TENENBAUM, *Introduction to analytic and probabilistic number theory*, Cambridge University Press, Cambridge, 1995.
- [16] I.M. VINOGRADOV, *Über die Verteilung der quadratischen Reste und Nichtreste*, J. Soc. Phys. Math. Univ. Permi **2**(1919), pp. 1-14.