

THE ARTIN–CARMICHAEL PRIMITIVE ROOT PROBLEM ON AVERAGE

SHUGUANG LI AND CARL POMERANCE

1. INTRODUCTION

Let n be a natural number. It was known to Gauss that the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^*$ is cyclic if and only if n is not divisible by two different odd primes nor divisible by 4, except for $n = 4$ itself. In particular, this holds whenever n is prime. When $(\mathbb{Z}/n\mathbb{Z})^*$ is cyclic, a generator is called a primitive root. In general, let $\lambda(n)$ be the exponent of $(\mathbb{Z}/n\mathbb{Z})^*$, the maximal order of any element in the group. Following Carmichael [1], we broaden the definition of primitive root to an element of $(\mathbb{Z}/n\mathbb{Z})^*$ which has order $\lambda(n)$.

There are various natural questions associated with these concepts.

- (1) Let $R(n)$ denote the number of residues modulo n which are primitive roots for n . Thus, $R(n)/n$ is the proportion of residues modulo n which are primitive roots. What is $R(n)/n$ on average, and what is it on average for prime n ?
- (2) For a fixed integer a , let $N_a(x)$ denote the number of natural numbers $n \leq x$ for which a is a primitive root, and let $P_a(x)$ denote the number of such n which are prime. What is the asymptotic distribution of $N_a(x)$ and $P_a(x)$?
- (3) What is the average asymptotic behavior of $N_a(x)$ as a runs over a short interval, and what is it for $P_a(x)$?

We first review what is known for the prime case. If p is prime, the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic of order $p-1$, so it follows that $R(p) = \varphi(p-1)$, where φ is Euler's function. One has (see Stephens [13, Lemma 1])

$$(1) \quad \frac{1}{\pi(x)} \sum_{p \leq x} \frac{R(p)}{p} \sim A \quad \text{as } x \rightarrow \infty,$$

where

$$A = \prod_p \left(1 - \frac{1}{p(p-1)} \right) = 0.3739558136 \dots$$

C.P. was supported by NSF grant number DMS-0703850.

is known as Artin's constant. This suggests that typically we should have $P_a(x) \sim A\pi(x)$. It is easy to see though that for some choices of a this cannot be, namely for a a square or $a = -1$, since for each such a , there are at most 2 primes for which a is a primitive root. Artin's conjecture is the assertion that for all other values of a there are infinitely many primes for which a is a primitive root, and in fact, there is a positive rational c_a with $P_a(x) \sim c_a A\pi(x)$. This conjecture was proved by Hooley [2] under the assumption of the Generalized Riemann Hypothesis. For surveys, see [8], Moree [11] and Murty [12].

Concerning the third question, Stephens [13] has shown unconditionally that if $y > \exp(4(\log x \log \log x)^{1/2})$ then

$$(2) \quad \frac{1}{y} \sum_{1 \leq a \leq y} P_a(x) \sim A\pi(x) \quad \text{as } x \rightarrow \infty.$$

Turning to the composite case, the first author in [5] showed that $(1/x) \sum_{n \leq x} R(n)/n$ does *not* tend to a limit as $x \rightarrow \infty$. We have

$$x \geq \sum_{n \leq x} \frac{R(n)}{n} \gg \frac{x}{\log \log \log x}$$

and

$$\limsup_{x \rightarrow \infty} \frac{1}{x} \sum_{n \leq x} \frac{R(n)}{n} > 0, \quad \liminf_{x \rightarrow \infty} \frac{1}{x} \sum_{n \leq x} \frac{R(n)}{n} = 0.$$

Let $\mathcal{E}$ denote the set of integers a which are a power higher than the first power or a square times a member of $\{\pm 1, \pm 2\}$. It was shown by the first author in [4] that for $a \in \mathcal{E}$ we have $N_a(x) = o(x)$ and that for *every* integer a , we have $\liminf_{x \rightarrow \infty} N_a(x)/x = 0$. In [7] we showed that, under the assumption of the Generalized Riemann Hypothesis, for each integer $a \notin \mathcal{E}$ we have $\limsup_{x \rightarrow \infty} N_a(x)/x > 0$.

To complete our brief review of the literature, the first author showed in [6] that for $y \geq \exp((\log x)^{3/4})$,

$$(3) \quad \frac{1}{y} \sum_{1 \leq a \leq y} N_a(x) \sim \sum_{n \leq x} \frac{R(n)}{n} \quad \text{as } x \rightarrow \infty.$$

The goal of this paper is to improve the range for y in (3) to a range for y similar to that in (2). We use similar methods as have already been used on these problems. Let

$$L(x) = \exp((\log x \log \log x)^{1/2}).$$

We prove the following theorem.

Theorem 1. *For $y \geq L(x)^8$ we have*

$$\frac{1}{y} \sum_{1 \leq a \leq y} N_a(x) = \sum_{n \leq x} \frac{R(n)}{n} + O\left(\frac{x}{y^{1/7}}\right).$$

Further, for any fixed $\epsilon > 0$ and $L(x)^{2+\epsilon} \leq y \leq L(x)^8$,

$$\frac{1}{y} \sum_{1 \leq a \leq y} N_a(x) = \sum_{n \leq x} \frac{R(n)}{n} + O\left(\frac{xL(x)^{1/2+\epsilon/6}}{y^{1/4}} + \frac{x \log x}{y^{5/32}}\right).$$

In particular, we have (3) in the range $y \geq L(x)^{2+\epsilon}$.

We remark that our proof can be adapted to the case of $P_a(x)$ and so allows an improvement of (2) to the range $y \geq L(x)^{2+\epsilon}$.

2. PRELIMINARIES

Variables p, q will always denote primes.

For a positive integer n , we write $p^a \parallel n$ if $p^a \mid n$ and $p^{a+1} \nmid n$. In this case, we also write $v_p(n) = a$. The universal exponent function $\lambda(n)$ can be computed from the prime factorization of n as follows:

$$\lambda(n) = \text{lcm}\{\lambda(p^a) : p^a \parallel n\},$$

where $\lambda(p^a) = \varphi(p^a)$ unless $p = 2$, $a \geq 3$, in which case $\lambda(2^a) = \frac{1}{2}\varphi(2^a) = 2^{a-2}$. For each prime $q \mid \lambda(n)$ (which is equivalent to the condition $q \mid \varphi(n)$) let

$$\mathcal{D}_q(n) = \{p^a \parallel n : v_q(\lambda(p^a)) = v_q(\lambda(n))\}.$$

If $v_q(\lambda(n)) = v$, let $\Delta_q(n)$ denote the number of cyclic factors C_{q^v} in $(\mathbb{Z}/n\mathbb{Z})^*$, so that

$$\Delta_q(n) = \#\mathcal{D}_q(n),$$

except in the case $q = 2$ and $2^3 \in \mathcal{D}_2(n)$, when $\Delta_2(n) = 1 + \#\mathcal{D}_2(n)$. Then (see [5, 10]),

$$(4) \quad R(n) = \varphi(n) \prod_{q \mid \varphi(n)} (1 - q^{-\Delta_q(n)}).$$

Let $\text{rad}(m)$ denote the largest squarefree divisor of m . Let

$$E(n) = \{a \bmod n : a^{\lambda(n)/\text{rad}(\lambda(n))} \equiv 1 \pmod{n}\},$$

so that $E(n)$ is a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$. We say a character $\chi \bmod n$ is *elementary* if it is trivial on $E(n)$. Clearly the order of an elementary character is squarefree. For each squarefree number $h \mid \varphi(n)$, let $\rho_n(h)$

be the number of elementary characters mod n of order h . It is not hard to see that

$$(5) \quad \rho_n(h) = \prod_{q|h} (q^{\Delta_q(n)} - 1).$$

For a character χ mod n , let

$$c(\chi) = \frac{1}{\varphi(n)} \sum'_b \chi(b),$$

where the dash indicates that the sum is over primitive roots mod n in $[1, n]$. Further, let

$$\bar{c}(\chi) = \begin{cases} 1/\rho_n(\text{ord } \chi), & \text{if } \chi \text{ is elementary} \\ 0, & \text{if } \chi \text{ is not elementary.} \end{cases}$$

Proposition 2. *For a character χ mod n , we have $|c(\chi)| \leq \bar{c}(\chi)$.*

Proof. Various elements of the proof are in [6]; we give a self-contained proof here. To see that $c(\chi) = 0$ for χ not elementary, note that the primitive roots mod n comprise a union of some of the cosets of the subgroup $E(n)$ in $(\mathbb{Z}/n\mathbb{Z})^*$, so we can factor $\sum_{a \in E(n)} \chi(a)$ out of the character sum $\sum'_b \chi(b)$. This factor is 0 unless χ is trivial on $E(n)$, that is, $c(\chi) = 0$ for χ not elementary.

Suppose now that χ is elementary. For each prime $q \mid \varphi(n)$, let $S_q(n)$ be the q -Sylow subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$. This group has exponent $q^{v_q(\lambda(n))}$; let $R_q(n)$ denote the set of members with this order. Then a residue b mod n is a primitive root mod n if and only if it is of the form $\prod_{q \mid \varphi(n)} b_q$, where each $b_q \in R_q(n)$, and if it has such a representation, it is unique. Thus,

$$\varphi(n)c(\chi) = \sum'_{b \bmod n} \chi(b) = \prod_{q \mid \varphi(n)} \left(\sum_{b_q \in R_q(n)} \chi(b_q) \right).$$

This character sum is $\#R_q(n)$ if $q \nmid \text{ord } \chi$, since in this case χ acts as the trivial character on $S_q(n)$. Suppose $q \mid \text{ord } \chi$. Since $S_q(n) \setminus R_q(n) \subset E(n)$ and χ is elementary,

$$\begin{aligned} \sum_{b \in R_q(n)} \chi(b) &= \sum_{b \in S_q(n)} \chi(b) - \sum_{\substack{b \in S_q(n) \\ b \notin R_q(n)}} \chi(b) = 0 - \sum_{\substack{b \in S_q(n) \\ b \notin R_q(n)}} \chi(b) \\ &= -(\#S_q(n) - \#R_q(n)). \end{aligned}$$

We have $\#R_q(n) = \#S_q(n)(1 - q^{-\Delta_q(n)})$, so we conclude that

$$\sum_{b \in R_q(n)} \chi(b) = \begin{cases} -\#S_q(n)q^{-\Delta_q(n)}, & \text{if } q \mid \text{ord } \chi \\ \#S_q(n)(1 - q^{-\Delta_q(n)}), & \text{if } q \nmid \text{ord } \chi. \end{cases}$$

We thus have, where ω is the number of primes dividing $\text{ord } (\chi)$,

$$\begin{aligned} \varphi(n)c(\chi) &= \prod_{q \mid \text{ord } \chi} \frac{-\#S_q(n)}{q^{\Delta_q(n)}} \prod_{\substack{q \mid \varphi(n) \\ q \nmid \text{ord } \chi}} \#S_q(n) (1 - q^{-\Delta_q(n)}) \\ &= \frac{(-1)^\omega R(n)}{\prod_{q \mid \text{ord } \chi} (q^{\Delta_q(n)} - 1)} = \frac{(-1)^\omega R(n)}{\rho_n(\text{ord } (\chi))}, \end{aligned}$$

using (4) and (5). The proposition now follows since $R(n) \leq \varphi(n)$. $\square$

Proposition 3. *Suppose k, d are coprime positive integers and ψ is an elementary character mod kd that is induced by a character χ mod k . Each of the following holds:*

- (i) *For each $q \mid \text{ord } \psi$, we have $v_q(\lambda(k)) = v_q(\lambda(kd))$,*
- (ii) *χ is elementary,*
- (iii) *$\bar{c}(\chi) \geq |c(\psi)|$.*

Proof. Let $h = \text{ord } \psi = \text{ord } \chi$, let $q \mid h$, let $v = v_q(\lambda(k))$, and let $w = v_q(\lambda(kd))$. Clearly, $v \leq w$. Since χ has order h , there is some integer a with $\chi(a) \neq 1$ and $a^{q^{v'}} \equiv 1 \pmod{k}$ for some $v' \leq v$. Since k, d are coprime, there is an integer b with $b \equiv a \pmod{k}$ and $b \equiv 1 \pmod{d}$. Then

$$b^{q^{v'}} \equiv 1 \pmod{kd} \quad \text{and} \quad \psi(b) = \chi(a) \neq 1.$$

Since ψ is elementary, it follows that $b \notin E(kd)$, so that $v' > w - 1$. Thus we have $v \geq v' \geq w$, which completes the proof of (i).

Suppose χ is not elementary, so χ is not trivial on $E(k)$. This then implies that there is some $a \in E(k)$ with $\chi(a) \neq 1$. As above, there is some b with $b \equiv a \pmod{k}$ and $b \equiv 1 \pmod{d}$. Since $\lambda(k)/\text{rad}(\lambda(k))$ divides $\lambda(kd)/\text{rad}(\lambda(kd))$, it follows that $b \in E(kd)$. But $\psi(b) = \chi(a) \neq 1$, contradicting the assumption that ψ is elementary. This proves (ii).

Using (i) and k, d coprime we immediately have $\Delta_q(k) \leq \Delta_q(kd)$ for each $q \mid h$, so that (5) implies that $\rho_k(\text{ord } \chi) \leq \rho_{kd}(\text{ord } \psi)$. Thus, (iii) follows from (ii) and Proposition 2. $\square$

3. THE PROOF

Our starting point is a lemma from [6]. Let $X(n)$ denote the set of non-principal elementary characters mod n and let

$$S_{(x,y)} = \sum_{n \leq x} \sum_{\chi \in X(n)} c(\chi) \sum_{1 \leq a \leq y} \chi(a).$$

It is shown in [6] that

$$(6) \quad \sum_{1 \leq a \leq y} N_a(x) = y \sum_{n \leq x} \frac{R(n)}{n} + S_{(x,y)} + O(x \log x).$$

Thus, we would like to show that $|S_{(x,y)}|$ is small. A natural thought is to use character sum estimates to majorize the sum of $\chi(a)$, but to do this, it will be convenient to deal with primitive characters.

Let $\chi_{0,n}$ denote the principal character mod n and let $\sum^*$ denote a sum over non-principal primitive characters. We have

$$\begin{aligned} S_{(x,y)} &= \sum_{n \leq x} \sum_{k|n} \sum_{\substack{\chi \bmod k \\ \chi\chi_{0,n} \in X(n)}}^* c(\chi\chi_{0,n}) \sum_{a \leq y} \chi(a)\chi_{0,n}(a) \\ &= \sum_{n \leq x} \sum_{k|n} \sum_{\chi \bmod k}^* c(\chi\chi_{0,n}) \sum_{\substack{d|n \\ (d,k)=1}} \chi(d)\mu(d) \sum_{a \leq y/d} \chi(a), \end{aligned}$$

where we can drop the condition $\chi\chi_{0,n} \in X(n)$ since if $\chi\chi_{0,n}$ is not elementary, Proposition 2 implies $c(\chi\chi_{0,n}) = 0$. Thus,

$$\begin{aligned} |S_{(x,y)}| &\leq \sum_{d \leq x} |\mu(d)| \sum_{\substack{km \leq x/d \\ (k,d)=1}} \sum_{\chi \bmod k}^* |c(\chi\chi_{0,dkm})| \left| \sum_{a \leq y/d} \chi(a) \right| \\ (7) \quad &= \sum_{d \leq x} |\mu(d)| S_d, \end{aligned}$$

say. We have

$$\begin{aligned}
S_d &= \sum_{\substack{k \leq x/d \\ (k,d)=1}} \sum_{\substack{m_1 \leq x/dk \\ \text{rad}(m_1)|k}} \sum_{\substack{m_2 \leq x/dkm_1 \\ (m_2,k)=1}} \sum_{\chi \bmod k}^* |c(\chi\chi_{0,dkm_1m_2})| \left| \sum_{a \leq y/d} \chi(a) \right| \\
&\leq \sum_{\substack{k \leq x/d \\ (k,d)=1}} \sum_{\substack{m_1 \leq x/dk \\ \text{rad}(m_1)|k}} \sum_{\substack{m_2 \leq x/dkm_1 \\ (m_2,k)=1}} \sum_{\chi \bmod k}^* \bar{c}(\chi\chi_{0,km_1}) \left| \sum_{a \leq y/d} \chi(a) \right|, \\
(8) \quad &\leq \sum_{k \leq x/d} \sum_{\text{rad}(m)|k} \frac{x}{dkm} \sum_{\chi \bmod k}^* \bar{c}(\chi\chi_{0,km}) \left| \sum_{a \leq y/d} \chi(a) \right|,
\end{aligned}$$

where the first inequality follows from Propositions 2 and 3.

We now give an estimate that will be useful in the cases with d large. To do this, we trivially majorize the character sum $|\sum_{a \leq y/d} \chi(a)|$ with y/d , so that

$$S_d \leq \frac{xy}{d^2} \sum_{k \leq x/d} \frac{1}{k} \sum_{\text{rad}(m)|k} \frac{1}{m} \sum_{\chi \bmod k}^* \bar{c}(\chi\chi_{0,km}).$$

The sum over m and χ is estimated as follows.

Lemma 4. *For a positive integer k we have*

$$\sum_{\text{rad}(m)|k} \frac{1}{m} \sum_{\chi \bmod k}^* \bar{c}(\chi\chi_{0,km}) \leq \frac{k}{\varphi(k)} \tau(\varphi(k)),$$

where τ is the divisor function.

Proof. For each $h \mid \varphi(k)$, consider those primitive characters $\chi \bmod k$ of order h . The number of them for which $\chi\chi_{0,km}$ is an elementary character with modulus km is at most $\rho_{km}(h)$. Thus, the contribution to the inner sum for each h is at most 1, so the inner sum is majorized by $\tau(\varphi(k))$. Further the sum on m of $1/m$, which is an infinite sum, has an Euler product and is seen to be $k/\varphi(k)$. Thus, the lemma follows. $\square$

Using Lemma 4, we have

$$(9) \quad S_d \leq \frac{xy}{d^2} \sum_{k \leq x/d} \frac{1}{\varphi(k)} \tau(\varphi(k)).$$

We have from [9] that

$$(10) \quad \sum_{n \leq x} \tau(\varphi(n)) \ll x \exp(c(\log x / \log \log x)^{1/2})$$

for any fixed $c > \sqrt{8/e^\gamma} = 2.1193574\dots$. Using this result, the estimate $1/\varphi(k) \ll (\log \log x)/k$ for $k \leq x$, and partial summation, we get from (9) that

$$(11) \quad S_d \ll \frac{xy}{d^2} \exp(3(\log x / \log \log x)^{1/2}).$$

We will use this estimate when d is large.

For a positive integer k and positive reals w, z , let

$$\begin{aligned} F(k, z) &= \sum_{\text{rad}(m)|k} \frac{1}{m} \sum_{\chi \bmod k}^* \bar{c}(\chi \chi_{0,km}) \left| \sum_{a \leq z} \chi(a) \right|, \\ T(w, z) &= \sum_{k \leq w} F(k, z), \\ S(w, z) &= w \sum_{k \leq w} \frac{1}{k} F(k, z). \end{aligned}$$

Note that

$$(12) \quad S_d \leq S(x/d, y/d).$$

We now look to estimate $S(w, z)$, and to do this, we first estimate $T(w, z)$ so that a partial summation calculation will get us to $S(w, z)$.

Lemma 5. *For $w, z \geq 3$ and $z \geq L(w)^6$, we have uniformly that*

$$(13) \quad T(w, z) \ll wz^{13/16} L(w)^{1/4}.$$

Further, if $L(w)^8 \geq z \geq L(w)^2$, then as $w \rightarrow \infty$, we have

$$(14) \quad T(w, z) \leq wz^{3/4} L(w)^{1/2+o(1)}.$$

Proof. We first consider the case when $w \leq z^{3/2}$. We have by the Pólya–Vinogradov inequality (see [3, Theorem 12.5]),

$$T(w, z) \ll \sum_{k \leq w} k^{1/2} \log k \sum_{\text{rad}(m)|k} \frac{1}{m} \sum_{\chi \bmod k}^* \bar{c}(\chi \chi_{0,km}).$$

Using Lemma 4, we have

$$T(w, z) \ll \sum_{k \leq w} \frac{k^{3/2} \log k}{\varphi(k)} \tau(\varphi(k)) \leq w^{3/2} \log w \sum_{k \leq w} \frac{1}{\varphi(k)} \tau(\varphi(k)).$$

Thus, using the same argument that allowed us to deduce (11) from (9), we have

$$T(w, z) \ll w^{3/2} \exp(3(\log w / \log \log w)^{1/2}).$$

Since $w^{3/2} \leq wz^{3/4}$ when $w \leq z^{3/2}$, the lemma follows in this case.

Now assume that $w > z^{3/2}$. We use Hölder's inequality: let r be a positive integer, so that writing $1/m$ as $1/m^{(2r-1)/2r} \cdot 1/m^{1/2r}$,

$$(15) \quad T(w, z)^{2r} \leq A^{2r-1} \cdot B,$$

where

$$A = \sum_{\substack{k \leq w \\ \text{rad}(m)|k}} \frac{1}{m} \sum_{\chi \bmod k}^* \bar{c}(\chi \chi_{0,km})^{2r/(2r-1)},$$

$$B = \sum_{\substack{k \leq w \\ \text{rad}(m)|k}} \frac{1}{m} \sum_{\chi \bmod k}^* \left| \sum_{a \leq z} \chi(a) \right|^{2r} = \sum_{k \leq w} \frac{k}{\varphi(k)} \sum_{\chi \bmod k}^* \left| \sum_{a \leq z} \chi(a) \right|^{2r}.$$

Using $0 \leq \bar{c}(\chi \chi_{0,km}) \leq 1$, Lemma 4, and (10) we have

$$(16) \quad A \ll w \exp(3(\log w / \log \log w)^{1/2}).$$

To estimate B we use the large sieve, see [3, Theorem 7.13], and Lemmas 3 to 5 in [13], getting

$$B \ll (w^2 + z^r) z^r (r \log z)^{r^2}$$

uniformly for integers $r \geq 1$ and numbers $w \geq 3, z \geq 3$. We shall let

$$r = \lceil 2 \log w / \log z \rceil,$$

so that $w^2 \leq z^r$, which implies

$$B \ll z^{2r} (r \log z)^{r^2}.$$

Further, $r < 2 \log w / \log z + 1 < (8/3) \log w / \log z$, using $w > z^{3/2}$. Thus $r \log z < 3 \log w$. We conclude that

$$(17) \quad \begin{aligned} B^{1/2r} &\ll z(r \log z)^{r/2} < z \exp\left(\frac{r}{2} \log(3 \log w)\right) \\ &< z \exp\left(\frac{4}{3} \cdot \frac{\log w \log(3 \log w)}{\log z}\right). \end{aligned}$$

Since $r < (8/3) \log w / \log z$, we have $w^{1/2r} > z^{3/16}$, so that from (16), we have

$$A^{(2r-1)/2r} \ll \frac{w}{z^{3/16}} \exp(3(\log w / \log \log w)^{1/2}).$$

Using this estimate with (15) and (17), we have

$$T(w, z) \ll w z^{13/16} \exp\left(3 \left(\frac{\log w}{\log \log w}\right)^{1/2} + \frac{\log w \log(3 \log w)}{(3/4) \log z}\right),$$

and so the lemma in the range $z \geq L(w)^6$ follows.

If $z \leq L(w)^8$, then the above choice of r is $(2 + o(1)) \log w / \log z$, so that (16) implies that $A^{(2r-1)/2r} \leq w z^{-1/4} L(w)^{o(1)}$. Further, if $z \geq$

$L(w)^2$, the first part of (17) shows that $B^{1/2r} \leq zL(w)^{1/2+o(1)}$, so that the inequality $T(w, z) \leq wz^{3/4}L(w)^{1/2+o(1)}$ follows from (15). $\square$

We are now ready to complete the proof of the theorem. Using Lemma 5 and partial summation, we have that if $z \geq L(w)^6$, then

$$(18) \quad S(w, z) \ll w \log w \cdot z^{13/16} L(w)^{1/4}.$$

If $L(w)^8 \geq z \geq L(w)^2$, using $S(w, z) = T(w, z) + w \int_1^w u^{-2} T(u, z) du$, we distinguish the cases $L(u)^8 \leq z$ and $L(u)^8 > z$. In the first case, we use (13) and $L(u)^{1/4} \leq z^{1/32}$ to get an upper bound of order $\log w \cdot z^{27/32}$ for the integral. In the second case, we use (14) to get the upper bound $z^{3/4} L(w)^{1/2+o(1)}$ for the integral. So, for any fixed $\delta > 0$, when $L(w)^8 \geq z \geq L(w)^2$ we have

$$(19) \quad S(w, z) \ll wz^{3/4} L(w)^{1/2+\delta} + w \log w \cdot z^{27/32}.$$

Suppose first that $L(x)^8 \leq y \leq x$. For $d \leq y^{1/4}$, we have $y/d \geq y^{3/4} \geq L(x)^6 \geq L(x/d)^6$. Thus, from (12) and (18),

$$S_d \leq S(x/d, y/d) \ll \frac{xy \log x}{d^{29/16} y^{3/16}} L(x)^{1/4}.$$

Summing this for $d \leq y^{1/4}$ and (11) for $d > y^{1/4}$, and using (6) and (7), we have the theorem in the case that $y \geq L(x)^8$.

Now let $\epsilon > 0$ and assume that $L(x)^{2+\epsilon} \leq y \leq L(x)^8$. If $d \leq y/L(x)^{2+\epsilon/2}$, we have for large x that $L(x/d)^8 \geq L(x)^8/d \geq y/d \geq L(x)^{2+\epsilon/2} > L(x/d)^2$. Thus, by (12) and (19), we have

$$S_d \leq S(x/d, y/d) \ll \frac{xy}{d^{7/4} y^{1/4}} L(x)^{1/2+\delta} + \frac{xy \log x}{d^{59/32} y^{5/32}}.$$

We sum this for $d \leq y/L(x)^{2+\epsilon/2}$, add in the sum of the estimate in (11) for larger d , and get from (7) that

$$\frac{1}{y} S_{(x,y)} \ll \frac{x}{y^{1/4}} L(x)^{1/2+\delta} + \frac{x \log x}{y^{5/32}} + \frac{x}{y} L(x)^{2+\epsilon/2+\delta}.$$

We choose $\delta = \epsilon/6$ so that the first term dominates the third, and use (6) to complete the proof of the theorem.

REFERENCES

- [1] R.D. CARMICHAEL, *The Theory of Numbers*, Wiley, New York, 1914.
- [2] C. HOOLEY, *On Artin's conjecture*, J. Reine Angew. Math. **225** (1967), 209–220.
- [3] H. IWANIEC AND E. KOWALSKI, *Analytic Number Theory*, American Mathematical Society, Providence, 2004.
- [4] S. LI, *On extending Artin's conjecture to composite moduli*, Mathematika **46** (1999), 373–390.

- [5] S. LI, *Artin's conjecture on average for composite moduli*, J. Number Theory **84** (2000), 93–118.
- [6] S. LI, *An improvement of Artin's conjecture on average for composite moduli*, Mathematika **51** (2004), 97–109.
- [7] S. LI AND C. POMERANCE, *On generalizing Artin's conjecture on primitive roots to composite moduli*, J. Reine Angew. Math. **556** (2003), 205–224.
- [8] S. LI AND C. POMERANCE, *Primitive roots: a survey*, in Number Theoretic Methods — Future Trends, C. Jia and S. Kanemitsu, eds., Dev. Math. **8**, pp. 219–231, Kluwer Academic Publishers, Dordrecht, 2002.
- [9] F. LUCA AND C. POMERANCE, *On the average number of divisors of the Euler function*, Publ. Math. Debrecen **70** (2007), 125–148.
- [10] G. MARTIN, *The least prime primitive root and the shifted sieve*, Acta Arith. **80** (1997), 277–288.
- [11] P. MOREE, *Artin's primitive root conjecture — a survey*, ArXiv math.NT/0412262 (2004), 30 pp.
- [12] M.R. MURTY, *Artin's conjecture for primitive roots*, Math. Intelligencer **10** (1988), no. 4, 59–67.
- [13] P.J. STEPHENS, *An average result for Artin's conjecture*, Mathematika **16** (1969), 178–188.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF HAWAII AT HILO
E-mail address: `shuguang@hawaii.edu`

MATHEMATICS DEPARTMENT, DARTMOUTH COLLEGE
E-mail address: `carl.pomerance@dartmouth.edu`