THE ARTIN–CARMICHAEL PRIMITIVE ROOT PROBLEM ON AVERAGE

SHUGUANG LI AND CARL POMERANCE

Abstract. For a natural number n, let $\lambda(n)$ denote the order of the largest cyclic subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$. For a given integer a, let $N_a(x)$ denote the number of $n \le x$ coprime to a for which a has order $\lambda(n)$ in $(\mathbb{Z}/n\mathbb{Z})^*$. Let $R(n)$ denote the number of elements of $(\mathbb{Z}/n\mathbb{Z})^*$ with order $\lambda(n)$. It is natural to compare $N_a(x)$ with $\sum_{n\le x} R(n)/n$. In this paper we show that the average of $N_a(x)$ for $1 \le a \le y$ is indeed asymptotic to this sum, provided $y \ge \exp((2+\varepsilon)(\log x \log\log x)^{1/2})$, thus improving a theorem of the first author who had this for $y \ge \exp((\log x)^{3/4})$. The result is to be compared with a similar theorem of Stephens who considered the case of prime numbers n.

§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 four, 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 a 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 $n \le x$ 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 $p-1$, and so it follows that $R(p) = \varphi(p-1)$, where φ is Euler's function. One has (see Stephens [**13**, Lemma 1])

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

where

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

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 hold, namely, for a a square or $a = -1$, since for each such a there are at most two 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 Li and Pomerance [**7**], 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

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

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

$$x \ge \sum_{n\le x}\frac{R(n)}{n} \gg \frac{x}{\log\log\log x}$$

and

$$\limsup_{x\to\infty}\frac{1}{x}\sum_{n\le x}\frac{R(n)}{n} > 0, \qquad \liminf_{x\to\infty}\frac{1}{x}\sum_{n\le x}\frac{R(n)}{n} = 0.$$

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 $\liminf_{x\to\infty} N_a(x)/x = 0$. In [**8**] we showed that, under the assumption of the generalized Riemann hypothesis, for each integer $a \notin \mathcal{E}$ we have $\limsup_{x\to\infty} N_a(x)/x > 0$.

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

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

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 to those already used in these problems. Let

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

We prove the following theorem.

THEOREM 1. *For $y \ge L(x)^8$,*

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

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

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

In particular, (3) *holds in the range* $y \ge L(x)^{2+\varepsilon}$.

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 $y \ge L(x)^{2+\varepsilon}$.

§2. *Preliminaries.* Variables p, q 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:

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

where $\lambda(p^a) = \varphi(p^a)$ unless $p = 2$, $a \ge 3$, 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 $v_q(\lambda(n)) = v > 0$, 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**]),

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

Let $\operatorname{rad}(m)$ denote the largest square-free divisor of m. Let

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

so that $E(n)$ is a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$. We say that a character $\chi \bmod n$ is *elementary* if it is trivial on $E(n)$. Clearly the order of an elementary character is square-free. For each square-free 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

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

For a character $\chi \bmod n$, let

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

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

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

PROPOSITION 2. *If* χ mod n *is a character, then* $|c(\chi)| \le \bar{c}(\chi)$.

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 that we can factor $\sum_{a\in E(n)} \chi(a)$ out of the character sum $\sum_b' \chi(b)$. This factor is zero 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, then it is unique. Thus,

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

The inner character sum is $\#R_q(n)$ if $q \nmid \operatorname{ord}\chi$, since in this case χ acts as the trivial character on $S_q(n)$. Suppose that $q \mid \operatorname{ord}\chi$. Since $S_q(n)\backslash R_q(n) \subset E(n)$ 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 $\#R_q(n) = \#S_q(n)(1-q^{-\Delta_q(n)})$, and so we conclude that

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

Thus, using (4) and (5), we have

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

where ω is the number of primes dividing $\operatorname{ord}(\chi)$. The proposition now follows since $R(n) \le \varphi(n)$. □

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

(i) $v_q(\lambda(k)) = v_q(\lambda(kd))$ *for each* $q \mid \operatorname{ord} \psi$*;*
(ii) χ *is elementary;*
(iii) $\bar{c}(\chi) \geq |c(\psi)|$.

Proof. Let $h = \operatorname{ord} \psi = \operatorname{ord} \chi$, 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 arecoprime, 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 that χ is not elementary, so that 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 $\lambda(k)/\operatorname{rad}(\lambda(k))$ divides $\lambda(kd)/\operatorname{rad}(\lambda(kd))$, it follows that $b \in E(kd)$. However, $\psi(b) = \chi(a) \neq 1$, 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 $\rho_k(\operatorname{ord} \chi) \leq \rho_{kd}(\operatorname{ord} \psi)$. Thus, (iii) follows from (ii) and Proposition 2. □

§3. *The proof.* Our starting point is a lemma from [**6**]. Let $\mathrm{X}(n)$ denote the set of non-principal elementary characters mod n, and let

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

It is shown in [**6**] that

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

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

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

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

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

say.

We have

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

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 $|\sum_{a\le y/d} \chi(a)|$ with y/d, so that

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

The sum over m and χ is estimated as follows.

LEMMA 4. *If k is a positive integer, then*

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

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 $\rho_{km}(h)$. Hence, the contribution to the inner sum for each h is at most one, so that 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. □

Using Lemma 4, we have

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

We deduce from [**9**] that

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

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

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

We use this estimate when d is large.

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

$$F(k,z) = \sum_{\mathrm{rad}(m)|k}\frac{1}{m}\sideset{}{^*}\sum_{\chi \bmod k}\bar{c}(\chi\chi_{0,km})\left|\sum_{a\le z}\chi(a)\right|,$$

$$T(w,z) = \sum_{k\le w}F(k,z),$$

$$S(w,z) = w\sum_{k\le w}\frac{1}{k}F(k,z).$$

Note that

$$S_d \le S(x/d, y/d). \tag{12}$$

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 give us $S(w,z)$.

LEMMA 5. *For $w, z \ge 3$ and $z \ge L(w)^6$, uniformly,*

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

Further, if $L(w)^8 \ge z \ge L(w)^2$, then as $w \to \infty$,

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

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

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

Using Lemma 4, we have

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

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 $w^{3/2} \le wz^{3/4}$ when $w \le z^{3/2}$, 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 $1/m^{(2r-1)/2r} \cdot 1/m^{1/2r}$,

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

where

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

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

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

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

To estimate B we use the large sieve (see [**3**, Theorem 7.13]) and [**13**, Lemmas 3, 4 and 5], and obtain

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

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

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

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

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

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

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

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

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

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

If $z \le L(w)^8$, then the above choice of r is $(2+o(1))\log w/\log z$, so that (16) implies that $A^{(2r-1)/2r} \le wz^{-1/4}L(w)^{o(1)}$. Further, if $z \ge L(w)^2$, then the first part of (17) shows that $B^{1/2r} \le zL(w)^{1/2+o(1)}$, so that the inequality $T(w,z) \le wz^{3/4}L(w)^{1/2+o(1)}$ follows from (15). □

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

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

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

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

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

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

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

Now let $\varepsilon > 0$ and assume that $L(x)^{2+\varepsilon} \le y \le L(x)^8$. If $d \le y/L(x)^{2+\varepsilon/2}$, for large x we see that $L(x/d)^8 \ge L(x)^8/d \ge y/d \ge L(x)^{2+\varepsilon/2} > L(x/d)^2$. Thus, by (12) and (19) with $\delta = \varepsilon/6$, we have

$$S_d \le S(x/d, y/d) \ll \frac{xy}{d^{7/4} y^{1/4}} L(x)^{1/2+\varepsilon/6} + \frac{xy \log x}{d^{59/32} y^{5/32}}.$$

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

$$\frac{1}{y} S_{(x,y)} \ll \frac{x}{y^{1/4}} L(x)^{1/2+\varepsilon/6} + \frac{x \log x}{y^{5/32}} + \frac{x}{y} L(x)^{2+\varepsilon/2+\varepsilon/6}.$$

Note that the first term dominates the third in the given range for y. We now use (6) to complete the proof of the theorem.

Acknowledgement. The second author was supported by NSF grant number DMS-0703850.

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, RI, 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, Primitive roots: a survey. In *Number Theoretic Methods—Future Trends* (*Developments Mathematics* **8**) (eds. C. Jia and S. Kanemitsu) , Kluwer Academic (Dordrecht, 2002), 219–231.
8. S. Li and C. Pomerance, On generalizing Artin's conjecture on primitive roots to composite moduli. *J. Reine Angew. Math.* **556** (2003), 205–224.
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. *Preprint*, 2004, math.NT/0412262.
12. M. R. Murty, Artin's conjecture for primitive roots. *Math. Intelligencer* **10** (1988), 59–67.
13. P. J. Stephens, An average result for Artin's conjecture. *Mathematika* **16** (1969), 178–188.

Shuguang Li,
Department of Mathematics,
University of Hawaii at Hilo,
Hilo, HI 96720-4091, U.S.A.,
E-mail: shuguang@hawaii.edu

Carl Pomerance,
Mathematics Department,
Dartmouth College,
Hanover, NH 03755-3551,
U.S.A.
E-mail: carl.pomerance@dartmouth.edu

MSC (2000): *Primary*, 11N37; *Secondary*, 11A07.

Received on the 1st of December, 2008.
Accepted on the 19th of January, 2009.