ACTA ARITHMETICA
LXXX.3 (1997)

The least prime primitive root and the shifted sieve

by

Greg Martin (Ann Arbor, Mich.)

1. Introduction. If p is a prime, we define $g^*(p)$ to be the least prime that is a primitive root (mod p), and similarly for prime powers p^r. The problem of establishing a bound for $g^*(p)$ uniformly in p is quite difficult, comparable with establishing a uniform upper bound for the least prime in an arithmetic progression. Indeed, there do not exist any uniform upper bounds for $g^*(p)$ that improve upon the current bounds for the least prime in an arithmetic progression. However, much more can be said if we exclude a very small set of primes. The purpose of this paper is to improve existing bounds for $g^*(p)$ which hold for almost all primes p, and to establish analogous results for all composite moduli.

Elliott [2] had first given a bound for $g^*(p)$ for all but $O(Y^\varepsilon)$ primes p up to Y, of the form $g^*(p) \le (\log p)^{O_\varepsilon(\log_3 p)}$. (Here we have defined $\log_1 x = \max\{\log x, 1\}$ and $\log_n x = \max\{\log(\log_{n-1} x), 1\}$ for any integer $n \ge 2$.) This was subsequently improved by Nongkynrih [6] to $g^*(p) \le (\log p)^{O_\varepsilon(\log_3 p/\log_4 p)}$. We are able to establish the following bound. Write $\omega(n)$ for the number of distinct prime factors of n.

Theorem 1. *Let Y, ε, and η be positive real numbers with $\varepsilon \le 20/21$, and define $B = B(\varepsilon,\eta) = 3/\varepsilon + 5/4 + \eta$. The number of odd prime powers p^r not exceeding Y for which the estimate*

$$g^*(p^r) \ll_{\varepsilon,\eta} (\omega(p-1)^2 \log p)^B$$

fails is $O_{\varepsilon,\eta}(Y^\varepsilon)$.

Since $\omega(n) \ll \log n$ for all integers n, it is apparent that the bound for $g^*(p^r)$ given in Theorem 1 is no larger than a fixed (depending on ε and η) power of $\log p$. We see that this is an improvement over the existing bounds, where the exponent of $\log p$ tends to infinity with p. We remark that Theorem 1 may easily be extended to include all moduli which admit primitive roots, i.e., to include moduli of the form $2p^r$.

1991 *Mathematics Subject Classification*: Primary 11N69, 11N36.

To extend this type of result to composite moduli, we use the following definition. Given an integer $q \geq 2$, we say that a *λ-root* (mod q) is an integer, coprime to q, whose multiplicative order is maximal among all integers coprime to q. We see that the λ-root is an extension of the primitive root to all moduli, and we extend the notation $g^*(q)$ to mean the least prime λ-root (mod q).

THEOREM 2. *Let ε be a positive real number. For almost all integers $q \geq 2$, we have*

$$g^*(q) \ll_\varepsilon \omega(\phi(q))^{44/5+\varepsilon}(\log q)^{22/5}.$$

The approach to establishing these theorems is through Proposition 3 below, which gives a bound for $g^*(q)$ based on the assumption of a zero-free rectangle for Dirichlet L-functions (mod q). This is the same approach taken in earlier work on this subject; the improvement lies in the use of the "shifted sieve", a version of the linear sieve with very good error terms, rather than Brun's sieve.

For any integer n, let $s(n)$ denote the largest squarefree divisor of n. For any integer $q \geq 2$, let $E(q)$ denote the exponent of the group $\mathbb{Z}_q^\times$ of reduced residue classes (mod q), let $\Phi(q)$ be the group of Dirichlet characters (mod q), and define

$$\Phi_*(q) = \{\chi^{E(q)/s(\phi(q))} : \chi \in \Phi(q)\}.$$

Only the characters in $\Phi_*(q)$ are relevant to detecting λ-roots, as we show in Section 2. Let c_0 be the probability that a randomly chosen element of $\mathbb{Z}_q^\times$ is a λ-root. Also, given real numbers σ and T with $1/2 \leq \sigma < 1$ and $T > 0$, define $\mathcal{Q}(\sigma, T)$ to be the set of integers $q \geq 2$ such that, for some nonprincipal $\chi \in \Phi_*(q)$, the corresponding L-function $L(s,\chi)$ has a zero $\beta + i\gamma$ with $\beta > \sigma$ and $|\gamma| < T$.

PROPOSITION 3. *Let $q \geq 2$ be an integer and σ a real number satisfying $1/2 \leq \sigma < 1$, and set*

$$f(q,\sigma) = (\omega(\phi(q))^2 \log_1 \omega(\phi(q)) \cdot c_0^{-1} \log q)^{1/(1-\sigma)}.$$

If $q \notin \mathcal{Q}(\sigma, f(q,\sigma))$, then $g^*(q) \ll_\sigma f(q,\sigma)$.

We remark that $f(q,\sigma) \ll_{\sigma,\theta} q^\theta$ for every $\theta > 0$. We also remark that $c_0^{-1} \ll \log_1 \omega(\phi(q))$ (see Section 2) and that the generalized Riemann hypothesis implies that $\mathcal{Q}(1/2, T)$ is empty for every $T > 0$. Thus the following corollary of Proposition 3 is immediate.

COROLLARY 3.1. *If the generalized Riemann hypothesis holds for* (*certain*) *characters* (mod q), *then*

$$g^*(q) \ll (\omega(\phi(q)) \log_1 \omega(\phi(q)))^4 (\log q)^2.$$

In the case where q is a prime, this has already been shown by Shoup [7], improving an earlier result of Wang [8] in which $(\omega(\phi(q))\log_1\omega(\phi(q)))^4$ is replaced by $\omega(\phi(q))^6$. Although both authors state their bounds only for primitive roots, the bounds actually hold for prime primitive roots as well.

To deduce Theorems 1 and 2 from Proposition 3, we need bounds on the size of $\mathcal{Q}(\sigma,T)$. To this end, we define $Q(Y;\sigma,T)$ to be the number of elements of $\mathcal{Q}(\sigma,T)$ not exceeding Y, and $Q'(Y;\sigma,T)$ to be the number of elements of $\mathcal{Q}(\sigma,T)$ which are odd prime powers not exceeding Y. The following lemmas, when combined with Proposition 3, imply Theorems 1 and 2.

LEMMA 4. *Let Y, ε, η, and B be as in Theorem 1. There exists $\theta = \theta(\varepsilon,\eta) > 0$ such that*

$$Q'(Y;1-B^{-1},Y^{\theta}) \ll_{\varepsilon,\eta} Y^{\varepsilon}.$$

LEMMA 5. *We have $Q(Y;17/22,Y^{1/20}) = o(Y)$.*

Lemma 4 follows directly from existing zero-density estimates for Dirichlet L-functions, but Lemma 5 is somewhat more complicated due to the prevalence of imprimitive characters in $\Phi_*(q)$ for composite moduli q (see Section 4).

The author would like to express his gratitude to Hugh Montgomery for suggesting this problem and to thank him and Trevor Wooley for their guidance and support. The author would also like to thank Andrew Granville and Andrew Odlyzko for their comments regarding existing results related to this work. This material is based upon work supported under a National Science Foundation Graduate Research Fellowship.

2. Preliminaries. We begin by developing some notation and simple facts relating to the characters (mod q) which are relevant to detecting λ-roots. Let G be a finite abelian group with exponent E. For every prime l that divides E, let $\alpha(l)$ be the largest integer such that $l^{\alpha(l)}$ divides E. There exist integers $m(l)$ for which we can write

$$G \cong \Big(\bigoplus_{l\mid E}(\mathbb{Z}_{l^{\alpha(l)}})^{m(l)}\Big) \oplus H$$

for some subgroup H whose exponent divides $E/s(E)$. For each prime p dividing E, we define subgroups G_p of G by

$$G_p = (p\mathbb{Z}_{p^{\alpha(p)}})^{m(p)} \oplus \Big(\bigoplus_{\substack{l\mid E\\ l\neq p}}(\mathbb{Z}_{l^{\alpha(l)}})^{m(l)}\Big) \oplus H, \tag{1}$$

the set of all elements of G whose order divides E/p. We see that the index of G_p in G is $p^{m(p)}$. We extend this notation to all squarefree divisors d of

E by defining subgroups G_d by

$$G_d = \bigcap_{p\mid d} G_p,$$

and (abusing notation somewhat) we define $m(d)$ to be the real number which satisfies

$$d^{m(d)} = \prod_{p\mid d} p^{m(p)},$$

so that $d^{m(d)}$ is a multiplicative function of d. By convention, we let $G_1 = G$ and $m(1) = 1$. We note that $m(d) \geq 1$ for all squarefree divisors d of E, and that the index of G_d in G is $d^{m(d)}$.

Let $\gamma(g)$ be the characteristic function of elements of maximal order in G. Then, by definition (1) of the G_p, we have

$$\{g \in G : \gamma(g) = 1\} = G \setminus \bigcup_{p\mid E} G_p. \tag{2}$$

If we define $\nu(g)$ to be the product of all primes p dividing E such that $g \in G_p$ (or equivalently, the largest squarefree divisor d of E such that $g \in G_d$), then we see from equation (2) that for any $g \in G$, we have

$$\gamma(g) = \begin{cases} 1 & \text{if } \nu(g) = 1, \\ 0 & \text{if } \nu(g) > 1. \end{cases} \tag{3}$$

We may also detect these elements of maximal order using group characters. Let Φ be the group of homomorphisms from G into $\mathbb{C}$. For each squarefree d dividing E, define subgroups Φ_d of the character group Φ by

$$\Phi_d = \{\chi^{E/d} : \chi \in \Phi\}.$$

For convenience we write Φ_* for $\Phi_{s(E)}$. Let h_d be the characteristic function of G_d. By the standard properties of group characters, for any $g \in G$ we have

$$h_d(g) = \frac{1}{|\Phi_d|} \sum_{\chi \in \Phi_d} \chi(g). \tag{4}$$

By summing this over all $g \in G$ we see that $|\Phi_d| = |G|/|G_d| = d^{m(d)}$, and in fact we can treat this as the definition of the real numbers $m(d)$. Finally, we define c_0 to be the probability that a randomly chosen element of $\mathbb{Z}_q^\times$ is a λ-root. From equation (2) and the definition (1) of the G_p, we can easily calculate that

$$c_0 = \prod_{p\mid\phi(q)} \left(1 - \frac{1}{p^{m(p)}}\right).$$

We note in particular that $c_0^{-1} \leq \phi(q)/\phi(\phi(q)) \ll \log_1\omega(\phi(q))$.

In the course of applying the sieve, it will be important to understand the behavior of the sum $\psi_1(x,\chi)$ defined by

$$\psi_1(x,\chi) = \sum_{n<x} \chi(n)\Lambda(n)(x-n).$$

The following lemma provides the necessary bound, for the moduli q for which Proposition 3 will be established.

LEMMA 6. *Let $q \ge 2$ be an integer, and let x, σ, and T be real numbers satisfying $1/2 \le \sigma < 1$ and $1 \le x \ll T \ll q$. If $q \notin \mathcal{Q}(\sigma,T)$, then for all nonprincipal $\chi \in \Phi_*(q)$, we have*

$$\psi_1(x,\chi) \ll x^{1+\sigma}\log q.$$

Proof. We begin by writing

$$\psi_1(x,\chi) = \frac{-1}{2\pi i}\int_{2-i\infty}^{2+i\infty} \frac{L'}{L}(s,\chi)\frac{x^{s+1}}{s(s+1)}\,ds$$

and pulling the contour leftwards towards $\operatorname{Re} s = -\infty$ to see that

$$\psi_1(x,\chi) = -\sum_{\varrho} \frac{x^{\varrho+1}}{\varrho(\varrho+1)} + O(x\log x),$$

where the sum runs over all nontrivial zeros $\varrho = \beta + i\gamma$ of $L(s,\chi)$ (see for instance [1, Chapter 19]). Because q is not in $\mathcal{Q}(\sigma,T)$, every zero of $L(s,\chi)$ has either $\beta \le \sigma$ or $|\gamma| \ge T$, and thus we can write

$$\psi_1(x,\chi) \ll \sum_{\beta\le\sigma} \frac{x^{1+\beta}}{\gamma^2} + \sum_{|\gamma|\ge T} \frac{x^{1+\beta}}{\gamma^2} + x\log x.$$

However, the number of zeroes of $L(s,\chi)$ up to height T is $\ll T\log qT$, and so $\sum_{|\gamma|\ge T}\gamma^{-2} \ll T^{-1}\log qT$ by partial summation. Therefore

$$\psi_1(x,\chi) \ll x^{1+\sigma}\log q + x^2T^{-1}\log qT + x\log x.$$

Since $x \ll T \ll q$, the first term is dominant, and the lemma is established. ∎

3. The shifted sieve: Proof of Proposition 3. Let $\mathcal{A}$ be a finite sequence, ν a map from $\mathcal{A}$ to the positive integers, and w a function from $\mathcal{A}$ to the nonnegative reals. Let Υ be a squarefree integer, put

$$S(\mathcal{A},\Upsilon) = \sum_{\substack{a\in\mathcal{A}\\ (\nu(a),\Upsilon)=1}} w(a),$$

and, for all d dividing Υ, put

$$A_d = \sum_{\substack{a\in\mathcal{A}\\ d\mid\nu(a)}} w(a).$$

Lemma 7. *Suppose that X and R are positive numbers and $f(d)$ a multiplicative function such that for all d dividing Υ, we have $f(d) \ge d$ and*

$$\left| A_d - \frac{X}{f(d)} \right| \le R. \tag{5}$$

Then there exists an absolute positive constant C_1 such that

$$S(\mathcal{A}, \Upsilon) \ge \frac{C_1 X}{\log_1 \omega(\Upsilon)} \prod_{p\mid\Upsilon} \left(1 - \frac{1}{f(p)}\right) + O(R\omega(\Upsilon)^2).$$

Proof. Let p_j denote the jth prime, and put $z = p_{\omega(\Upsilon)}$ and $P = \prod_{p\le z} p$. Also let $\{\lambda_d^-\}$ be a sequence of real numbers such that $\lambda_1^- \le 1$ and, if we define $\sigma_n = \sum_{d\mid n} \lambda_d^-$, then $\sigma_n \le 0$ for all integers $n \ge 2$. We begin by citing the lower bound

$$S(\mathcal{A}, \Upsilon) \ge X \prod_{p\mid\Upsilon} \left(1 - \frac{1}{f(p)}\right) \sum_{d\mid P} \frac{\sigma_d}{\prod_{p\mid d}(p-1)} - R \sum_{d\mid P} |\lambda_d^-|. \tag{6}$$

This is a special case of the shifted sieve of Iwaniec [4, Lemma 1], where we have specified that $Q = \Upsilon$, $A = R$, $B = 1$, and $g(d) = d$ for all d dividing P, and that the correspondence l sends the smallest prime factor of Υ to p_1, the next smallest to p_2, and so on. We now take $\{\lambda_d^-\}$ to be Rosser's weights for the linear sieve, whose definition depends on a positive parameter y as follows. If d is not squarefree, define $\lambda_d^- = 0$. If $d = q_1 \ldots q_r$ for primes $q_1 > \ldots > q_r$, define

$$\lambda_d^- = \begin{cases} (-1)^r & \text{if } q_1 \ldots q_{2l-1} q_{2l}^3 < y \text{ for all } 0 \le l \le r/2, \\ 0 & \text{otherwise.} \end{cases}$$

We will need the following facts about the sequence $\{\lambda_d^-\}$ [4, Lemma 2]: if $4 \le z^2 \le y \le z^4$, then

$$\sum_{d\mid P} |\lambda_d^-| \ll y(\log y)^{-2}$$

and

$$\sum_{d\mid P} \frac{\sigma_d}{\prod_{p\mid d}(p-1)} = 2e^\gamma \frac{\log(s-1)}{s} + O\left(\frac{1}{\log y}\right), \tag{7}$$

where $s = (\log y)/(\log z)$. Applying this with $y = C_2 z^2$ for C_2 a positive constant gives us

$$\begin{aligned} 2e^\gamma \frac{\log(s-1)}{s} + O\left(\frac{1}{\log y}\right) &= \frac{e^\gamma \log C_2}{\log z}\left(1 + O\left(\frac{\log C_2}{\log z}\right)\right) + O\left(\frac{1}{\log z}\right) \\ &\ge \frac{C_1}{\log z} \end{aligned} \tag{8}$$

for some positive constant C_1, if C_2 and z are sufficiently large. With these estimates, the lower bound (6) becomes

$$S(\mathcal{A},\Upsilon) \geq \frac{C_1 X}{\log z} \prod_{p|\Upsilon} \left(1 - \frac{1}{f(p)}\right) + O\left(\frac{RC_2 z^2}{(\log z)^2}\right).$$

We note that C_2 is an absolute constant, since it depends only on the O-constant in equation (7), and thus C_1 is absolute as well, since it depends only on C_2 and the O-constants in equation (8). It remains only to note that $z \sim \omega(\Upsilon) \log_1 \omega(\Upsilon)$ to establish the lemma. ∎

We may now establish Proposition 3. Let $q \geq 2$ be an integer and $x > 1$ and $1/2 \leq \sigma < 1$ real numbers. We will apply Lemma 7 with $\mathcal{A}$ being the set of positive integers less than x. Let $\Upsilon = s(\phi(q))$, let $\nu(n)$ be defined as in Section 2 before equation (3), and let $w(n) = \Lambda(n)(x-n)$. From the relation (3), we see that

$$S(\mathcal{A},\Upsilon) = \sum_{n<x} \gamma(n)\Lambda(n)(x-n)$$

counts only prime powers which are λ-roots (mod q). Using the form (4) for h_d and the definition of the $\psi_1(x,\chi)$, we also have

$$\text{(9)} \quad A_d = \sum_{\substack{n<x \\ d|\nu(n)}} w(n) = \sum_{n<x} h_d(n) w(n)$$
$$= \frac{1}{|\Phi_d|} \sum_{\chi\in\Phi_d} \sum_{n<x} \chi(n) w(n) = \frac{1}{d^{m(d)}} \psi_1(x,\chi_0) + \frac{1}{|\Phi_d|} \sum_{\substack{\chi\in\Phi_d \\ \chi\neq\chi_0}} \psi_1(x,\chi).$$

If we write $\psi_1(x) = \sum_{n<x} \Lambda(n)(x-n)$, then

$$\psi_1(x) - \psi_1(x,\chi_0) = \sum_{\substack{n<x \\ (n,q)>1}} \Lambda(n)(x-n) \ll x \sum_{p|q} \sum_{\substack{r\geq 1 \\ p^r<x}} \log p \ll (x\log x)\log q,$$

since $\omega(q) \ll \log q$. Moreover, if we assume that $q \notin \mathcal{Q}(\sigma,x)$, then we may apply Lemma 6 (with $T = x$) to bound the terms in the last sum of equation (9); we obtain

$$A_d = \frac{1}{d^{m(d)}} \psi_1(x) + O(x^{1+\sigma} \log q).$$

Thus if we take $X = \psi_1(x)$ and $f(d) = d^{m(d)}$ for all d dividing $s(\phi(q))$, we see that we can take $R \ll x^{1+\sigma}\log q$. Applying Lemma 7, we see that

$$\begin{aligned} S(\mathcal{A},\Upsilon) &\ge \frac{C_1\psi_1(x)}{\log_1\omega(\phi(q))}c_0 + O((x^{1+\sigma}\log q)\omega(\phi(q))^2) \\ &= \frac{C_1\psi_1(x)}{\log_1\omega(\phi(q))}c_0(1+O(x^{-1+\sigma}(\omega(\phi(q))^2\log_1\omega(\phi(q)))c_0^{-1}\log q)) \\ &= \frac{C_1\psi_1(x)}{\log_1\omega(\phi(q))}c_0(1+O((x^{-1}f(q,\sigma))^{1-\sigma})), \end{aligned}$$

since the bound $\psi_1(x) \gg x^2$ follows from Chebyshev's bound for $\psi(x)$. Assuming that x exceeds a sufficiently large (in terms of σ) multiple of $f(q,\sigma)$, we obtain a positive lower bound for $S(\mathcal{A},\Upsilon)$. Therefore, there exists a prime power $p^r \ll_\sigma f(q,\sigma)$ which is a λ-root (mod q). But if p^r is a λ-root, we must have $(r,\phi(q))=1$, in which case p itself is also a λ-root which is $\ll_\sigma f(q,\sigma)$. This establishes the proposition.

4. Proof of Lemmas 4 and 5. To establish Lemma 4, we introduce the notation $\mathcal{Q}'(\sigma,T)$ to denote the subset of $\mathcal{Q}(\sigma,T)$ consisting of the odd prime powers, and we recall that $Q'(Y;\sigma,T)$ denotes the number of elements of $\mathcal{Q}'(\sigma,T)$ not exceeding Y. Given an odd prime power p^r, every character in $\Phi_*(p^r)$ is induced by a character (mod p^2) [5, Lemma 6]. The proof of this fact is similar to the proof that any primitive root (mod p^2) is also a primitive root (mod p^r) for every odd prime p and integer $r\ge 3$.

Consequently, for every prime power $p^r \in \mathcal{Q}'(\sigma,T)$, there is a character χ which is primitive to one of the moduli p or p^2 such that $L(s,\chi)$ has a zero $\beta+i\gamma$ with $\beta>\sigma$ and $|\gamma|<T$. On the other hand, every such character will account for $\ll \log Y$ prime powers in $\mathcal{Q}'(\sigma,T)$ which do not exceed Y, and so

$$Q'(Y;\sigma,T) \ll (\log Y)\sum_{q<Y}\ \sideset{}{^*}\sum_{\chi\,(\mathrm{mod}\,q)} N(\sigma,T,\chi), \tag{10}$$

where $N(\sigma,T,\chi)$ denotes the number of zeros $\beta+i\gamma$ of $L(s,\chi)$ satisfying $\beta>\sigma$ and $|\gamma|<T$, and $\sum^*$ denotes a summation over primitive characters only. Zhang [9] has established the following zero-density estimate for Dirichlet L-functions: for any real numbers Y, $\delta>0$ and $17/22\le\sigma\le 1$, we have

$$\sum_{q<Y}\ \sideset{}{^*}\sum_{\chi\,(\mathrm{mod}\,q)} N(\sigma,T,\chi) \ll_\delta (Y^2T)^{6(1-\sigma)/(5\sigma-1)+\delta}. \tag{11}$$

We apply this estimate with $T=Y^\theta$ and $\sigma = 1-B^{-1}$, where B is as in Theorem 1. Together with the bound (10), this gives us $Q'(Y;\sigma,T)\ll_{\varepsilon,\eta} Y^\varepsilon$, as long as $\delta=\delta(\varepsilon,\eta)$ and $\theta=\theta(\varepsilon,\eta)$ are small enough with respect to ε and η. This establishes Lemma 4.

Unfortunately, a given character can in general induce characters in $\Phi_*(q)$ for many more moduli q if we do not restrict to prime powers, and so we must work harder to establish Lemma 5. Given positive integers m and n such that m divides n, we say that n is an *admissible multiple* of m if there exists a character in $\Phi_*(n)$ which is induced by a primitive character (mod m).

LEMMA 8. *Let $q \geq 2$ be an integer, and set $t = \omega(q)$. Let $p_1, \ldots, p_t$ be the primes dividing q and $r_1, \ldots, r_t$ positive integers. Then for every admissible multiple nq of q, either*:

(i) *$p_i^{r_i}$ divides n for some $1 \leq i \leq t$; or*
(ii) *n is not divisible by any prime congruent to* $1 \pmod{\phi^2(q)p_1^{r_1}\ldots p_t^{r_t}}$.

Proof. We use parenthetical superscripts to indicate explicitly the modulus of a character, so that $\chi^{(q)}$ denotes a character (mod q), for example. To establish the lemma, it suffices to show that if (i) and (ii) both fail, then any character $\chi^{(q)}$ which induces an element $\chi_1^{(nq)}$ of $\Phi_*(nq)$ is in fact principal (hence imprimitive), contradicting the assumption that nq is an admissible multiple of q.

Assume the negations of (i) and (ii). Write $nq = n'q'$, where q' is the largest divisor of nq with $s(q') = s(q)$, so that q divides q' and $(n', q') = 1$. Then any character (mod nq) is the product of a character (mod n') and a character (mod q'). Since $\chi_1^{(nq)} \in \Phi_*(nq)$, we may write

$$\chi_1^{(nq)} = (\chi_2^{(n')}\chi_3^{(q')})^{E(nq)/s(E(nq))}$$

for some characters $\chi_2^{(n')}$ and $\chi_3^{(q')}$. Since $p_i^{r_i}$ does not divide n for any $1 \leq i \leq t$, we see from the definition of q' that $\phi(q')$ divides $\phi(q)p_1^{r_1-1}\ldots p_t^{r_t-1}$. On the other hand, n is divisible by a prime which is congruent to $1 \pmod{\phi^2(q)p_1^{r_1}\ldots p_t^{r_t}}$, and so $\phi^2(q)p_1^{r_1}\ldots p_t^{r_t}$ must divide $E(nq)$. These observations together imply that $\phi(q')$ divides $E(nq)/s(E(nq))$, and thus

$$(\chi_2^{(n')}\chi_3^{(q')})^{E(nq)/s(E(nq))} = (\chi_2^{(n')})^{E(nq)/s(E(nq))}\chi_0^{(q')},$$

where $\chi_0^{(q')}$ is the principal character (mod q'). We see that the character $\chi_1^{(nq)}$ induced by $\chi^{(q)}$ is also induced by a character (mod n'). But since $(q, n') = 1$, it must be the case that $\chi^{(q)}$ is principal. This establishes the lemma. ■

Let $A(x; q)$ be the number of admissible multiples of q not exceeding x.

LEMMA 9. *Let $\delta > 0$ be a real number and x, $y = y(x)$, and $z = z(x)$ real parameters satisfying x, y, $z > 1$ and*

$$z^3 y^{\log z} \ll (\log x)^{1-\delta}. \tag{12}$$

Then for all integers q with $2 \le q \le z$, we have

$$A(xq;q) \ll_\delta \frac{x\log z}{y} + \frac{x}{\exp((\log_2 x)/(z^3 y^{\log z}))}. \tag{13}$$

Proof. Set $t = \omega(q)$, and choose integers r_i such that

$$p_i^{r_i-1} \le y \le p_i^{r_i} \quad (1 \le i \le t). \tag{14}$$

By applying Lemma 8, we see that the number of admissible multiples nq of q with $n < x$ is bounded by

$$\sum_{i=1}^{t} \frac{x}{p_i^{r_i}} + \#\{n < x : p \mid n \Rightarrow p \not\equiv 1 \ (\mathrm{mod}\ \phi^2(q)p_1^{r_1}\ldots p_t^{r_t})\}. \tag{15}$$

In the first term, we use the estimate $t \le \log z$ for z sufficiently large, and the choice (14) of the r_i, to see that

$$\sum_{i=1}^{t} \frac{x}{p_i^{r_i}} \le \frac{x\log z}{y}. \tag{16}$$

We treat the second term using a simple upper bound sieve. Notice that by the choice (14) of the r_i, we have

$$\phi^2(q)p_1^{r_1}\ldots p_t^{r_t} \le q^2\Big(\prod_{i=1}^{t} yp_i\Big) \le q^2(y^t z) \le z^3 y^{\log z}. \tag{17}$$

The prime number theorem for arithmetic progressions states that given $\delta > 0$, we have

$$\psi(x;d,1) = \frac{x}{\phi(d)} + O_\delta(x\exp(-C_3(\log x)^{1/2}))$$

for some positive constant C_3, uniformly for all $d \ll (\log x)^{1-\delta}$ [1, equations (10)–(11) of Section 20]. By partial summation, this implies that

$$\sum_{\substack{p<x \\ p\equiv 1\ (\mathrm{mod}\ d)}} p^{-1} = \frac{\log_2 x}{\phi(d)} + O_\delta(1), \tag{18}$$

again uniformly for d in the above range, which includes $d = \phi^2(q)p_1^{r_1}\ldots p_t^{r_t}$ due to equation (17) and the restriction (12). The formula (18) allows us to apply an upper bound sieve from Halberstam–Richert [3, Corollary 2.3.1] to deduce that

$$\#\{n < x : p \mid n \Rightarrow p \not\equiv 1 \ (\mathrm{mod}\ \phi^2(q)p_1^{r_1}\ldots p_t^{r_t})\} \ll_\delta x(\log x)^{-1/\phi(\phi^2(q)p_1^{r_1}\ldots p_t^{r_t})}.$$

We rewrite this using the bound (17) as

$$\#\{n < x : p \mid n \Rightarrow p \not\equiv 1 \ (\mathrm{mod}\ \phi^2(q)p_1^{r_1}\ldots p_t^{r_t})\} \ll_\delta \frac{x}{\exp((\log_2 x)/(z^3 y^{\log z}))}.$$

Using this bound together with the bound (16) in equation (15) establishes the lemma. ∎

Define $\mathcal{R}(\sigma,T)$ to be the set of integers $q\ge 3$ such that, for some primitive character $\chi \pmod q$, the corresponding L-function $L(s,\chi)$ has a zero $\beta+i\gamma$ with $\beta>\sigma$ and $|\gamma|<T$.

LEMMA 10. *For all real $x>1$, we have*

$$\sum_{\substack{q<x\\ q\in\mathcal{R}(17/22,x^{1/20})}} 1 \ll x^{.997} \quad \textit{and} \quad \sum_{\substack{x<q\\ q\in\mathcal{R}(17/22,x^{1/20})}} q^{-1} \ll x^{-.003}. \tag{19}$$

Proof. The right-hand side of the zero-density estimate (11) is certainly an upper bound for the first sum in (19) as well. Taking $Y=x$, $T=x^{1/20}$, and $\theta=1/100$ in (11), we see that

$$\sum_{\substack{q<x\\ q\in\mathcal{R}(17/22,x^{1/20})}} 1 \ll x^{41861/42000},$$

and $41861/42000 < .997$. This establishes the first bound in (19), and the second bound follows directly by partial summation. ∎

We are now ready to prove Lemma 5. We note that every element of $\mathcal{Q}(\sigma,T)$ is an admissible multiple of some element of $\mathcal{R}(\sigma,T)$. Therefore,

$$Q(Y;\sigma,T)\le \sum_{\substack{q<Y\\ q\in\mathcal{R}(\sigma,T)}} A(Y;q). \tag{20}$$

For $q\le \log_3 Y$, we bound $A(Y;q)$ by applying Lemma 9 with $z=\log_3 Y$ and $y=(\log_2 Y)^{1/(2\log z)}$, which satisfy the condition (12) with any $\delta<1$. Of the two terms in equation (13), the first term is dominant, giving

$$A(Y;q)\le A(Yq;q)\ll \frac{Y\log_4 Y}{\exp((\log_3 Y)/(2\log_4 Y))}.$$

For the remaining values of q, we have the trivial bound $A(Y;q)\le Y/q$. Therefore equation (20) becomes

$$Q(Y;\sigma,T)\ll \sum_{q<\log_3 Y} \frac{Y\log_4 Y}{\exp((\log_3 Y)/(2\log_4 Y))} + \sum_{\substack{\log_3 Y\le q<Y\\ q\in\mathcal{R}(\sigma,T)}} \frac{Y}{q}.$$

Upon choosing $\sigma=17/22$ and $T=Y^{1/20}$, we apply Lemma 10 to the second sum to obtain

$$Q(Y;17/22,Y^{1/20})\ll \frac{Y\log_3 Y\log_4 Y}{\exp((\log_3 Y)/(2\log_4 Y))} + \frac{Y}{(\log_3 Y)^{.003}} = o(Y),$$

which establishes the lemma.

References

[1] H. Davenport, *Multiplicative Number Theory*, 2nd ed., Springer, New York, 1980.

[2] P. D. T. A. Elliott, *The distribution of primitive roots*, Canad. J. Math. 21 (1969), 822–841.

[3] H. Halberstam and H.-E. Richert, *Sieve Methods*, Academic Press, London, 1974.

[4] H. Iwaniec, *On the problem of Jacobsthal*, Demonstratio Math. 11 (1978), 225–231.

[5] G. Martin, *Uniform bounds for the least almost-prime primitive root*, submitted.

[6] A. Nongkynrih, *On prime primitive roots*, Acta Arith. 72 (1995), 45–53.

[7] V. Shoup, *Searching for primitive roots in finite fields*, Math. Comp. 58 (1992), 369–380.

[8] Y. Wang, *On the least primitive root of a prime*, Sci. Sinica 10 (1961), 1–14.

[9] W. P. Zhang, *On the density of zeros of the Dirichlet L-function*, Acta Math. Sinica 31 (1988), 326–331.

Department of Mathematics
University of Michigan
525 East University–2072 East Hall
Ann Arbor, Michigan 48109-1109
U.S.A.
E-mail: gerg@math.lsa.umich.edu

Received on 21.10.1996 (3064)