TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 246, December 1978

ON THE FIRST OCCURRENCE OF VALUES OF A CHARACTER

BY

G. KOLESNIK AND E. G. STRAUS[1]

ABSTRACT. Let χ be a character of order k (mod n), and let $g_m(\chi)$ be the smallest positive integer at which χ attains its $(m+1)$st nonzero value. We consider fixed k and large n and combine elementary group-theoretic considerations with the known results on character sums and sets of integers without large prime factors to obtain estimates for $g_m(\chi)$.

1. Introduction. Let χ be a character of order k (mod n), and let $g_m(\chi) = n^{1/\gamma_m(\chi)}$ be the least positive integer at which χ attains its $(m+1)$st nonzero value.

Even though we shall not need most of the information, it may be useful to give a brief review of some elementary facts about characters which can be found in most textbooks on the subject. The character group (mod n) is isomorphic to the multiplicative group $G(n)$ of reduced residue classes (mod n). If we write $n = 2^{\alpha}p_1^{\alpha_1}\cdots p_s^{\alpha_s}$; $\alpha \geqslant 0$, $\alpha_j > 0$ $(j = 1, \ldots, s)$ where p_j are odd primes, then, by the Chinese remainder theorem, $G(n)$ is the direct product of the groups $G(2^{\alpha})$, $G(p_j^{\alpha_j})$ $(j = 1, \ldots, s)$. Now $G(p_j^{\alpha_j})$ is cyclic of order $\varphi(p_j^{\alpha_j}) = p_j^{\alpha_j - 1}(p_j - 1)$ and $G(2^{\alpha}) = \{1\}$ if $\alpha = 0$, 1, while if $\alpha \geqslant 2$, then $G(2^{\alpha})$ is the direct product of a group of order 2 and a cyclic group of order $2^{\alpha-2}$. Thus there exists a character of order $k = 2^{\beta}q_1^{\beta_1}\cdots q_t^{\beta_t}$, where the q_j are odd primes, if and only if the following conditions are satisfied:

For every $j = 1, \ldots, t$ we have either

$$p_i \equiv 1 \left(\mathrm{mod}\ q_j^{\beta_j}\right) \quad \text{for some } i,$$

or

$$p_i = q_j \quad \text{and } \alpha_i > \beta_j \quad \text{for some } i,$$

and either

$$p_i \equiv 1 \ (\mathrm{mod}\ 2^{\beta}) \quad \text{for some } i,$$

Received by the editors August 16, 1976.

AMS (MOS) subject classifications (1970). Primary 10H35.

[1]Research of the first author was supported in part by a grant from ACEP, Program for Soviet Emigre Scholars. Research of the second author was supported in part by NSF Grant MPS 71-2884.

or

$$\beta = 0, \quad \text{or } \beta = 1 \text{ and } \alpha > 1, \quad \text{or } \beta > 1 \text{ and } \alpha > \beta + 1.$$

The group of nonzero values of a character of order k is the group of kth roots of unity. Also the character $\chi \pmod n$ of order $k = 2^{\beta}q_1^{\beta_1} \cdots q_t^{\beta_t}$ can be expressed uniquely as a product of characters $\chi_0, \chi_1, \ldots, \chi_t \pmod n$ of orders $2^{\beta}, q_1^{\beta_1}, \ldots, q_t^{\beta_t}$, respectively.

Throughout this paper the modulus n of the characters is assumed fixed and cube free (although some of the results could be extended to more general n). So we shall omit the notation (mod n). The symbol ε stands for a positive number which can be chosen arbitrarily small, although different uses of ε in the same statement may refer to unequal choices. Since $g_0(\chi) = 1$ ($\gamma_0(\chi) = \infty$) holds for all χ we use the symbol $g_m(\chi)$ in the following with the understanding that $m > 0$.

In §3 we use simple group theoretic facts to obtain estimates of $g_m(\chi)$ in terms of various values $g_l(\chi')$ with $l < m$ or ord $\chi' < k$. In §4, we use estimates for character sums and estimates on the number of integers without large prime divisors to get bounds for g_1 and apply these results to the result of §3 to obtain bounds for g_m which are useful for values of m which are small compared to k. Finally in §5 we illustrate a method of estimating the number of integers with few large prime factors to improve the estimates for g_m by carrying out some of the details in estimating g_2.

2. A group theoretic lemma. Let G be a group and S a subset of G. Define

$$S_l = \{s_1 s_2 \cdots s_l | s_i \in S\}, \qquad l = 1, 2, \ldots.$$

If $1 \in S$ and $S_0 = \{1\}$ then $S_0 \subset S_1 \subset S_2 \subset \ldots$.

2.1. THEOREM. *If $1 \in S$ and $|S_m| \leqslant m$, then S_m is a subgroup of G and $S_{m-1} = S_m = S_{m+1} = \cdots$.*

PROOF. The theorem is obvious when $m = 1$. Now assume the theorem true for $m - 1$. If $S_{m-1} \subsetneq S_m$, then $|S_{m-1}| \leqslant m - 1$ and therefore S_{m-1} is a subgroup. Hence $S_m = S_{m-1}S = S_{m-1}$ is a subgroup of G. We may thus assume that $S_{m-1} = S_m = S_{m-1}S$, which means that S_m is closed under multiplication and hence it is a subgroup of G.

Both hypotheses in Theorem 2.1 are necessary. If $1 \notin S$, then the result is false for $m = 1$; while if $S = \{1, a\}$, where a is an element of order $m + 2$, then $|S_m| = m + 1$ and S_m is not a group. It is convenient to state the following corollary.

2.2. COROLLARY. *If S is a set of generators of a group G of order m and S contains the identity, then $|S_l| > l$ for all $l < m$; and in particular, $S_{m-1} = G$.*

PROOF. If we had $|S_l| \leqslant l$ for some $l < m$ then, by Theorem 2.1, S_l would be the group generated by S, contrary to hypothesis.

3. Applications to values of characters. Let χ be a character of order k.

3.1. DEFINITION. Let $g_m = g_m(\chi)$ denote the least positive integer for which χ attains its $(m+1)$st nonzero value. Thus $g_0(\chi) = 1$ and $g_m(\chi)$ is the least positive integer with $\chi(g_m) \notin \{0, \chi(g_0), \ldots, \chi(g_{m-1})\}$.

Now Theorem 2.1 leads to the following:

3.2. LEMMA. *If x is a positive integer, $(x, n) = 1$ and all prime divisors of x lie in the interval $(1, g_m^{1/m})$, then $\chi(x)$ belongs to a subgroup of order $l \leqslant m$, $l|k$, of the group of kth roots of unity.*

PROOF. If we let $S = \{\chi(x) | (n, x) = 1, 0 < x < g_m^{1/m}\}$, then S satisfies the hypotheses of Theorem 2.1 and S_m is a subgroup contained in the set

$$T = \{\chi(x) | (n, x) = 1, 0 < x < g_m\}.$$

3.3. LEMMA. *Let l be the order of the subgroup defined in the proof of Lemma* 3.2.

(i) *We have $l = 1$ if and only if $g_m \leqslant g_1^m$.*

(ii) *If $1 < l \leqslant m$, define $\chi_1 = \chi^l$ as a character of order $k_1 = k/l$. If $l = m$, then $g_m(\chi) = g_1(\chi_1)$.*

(iii) *If $1 < l < m$, define*

$$m_t = \left[(m - l)/(t + 1)\right] + 1, \qquad t = 0, 1, \ldots, l - 1,$$

and obtain

$$g_m(\chi) \leqslant \min_{\substack{0 \leqslant t < l \\ m_t < k_1}} g_{m_t}(\chi_1)^{m/(m-t)}.$$

PROOF. Part (i) is obvious, since $\chi(x) = 1$ for $(x, n) = 1$, $0 < x < g_m^{1/m}$, implies $g_m^{1/m} \leqslant g_1$. Conversely, if $g_m^{1/m} \leqslant g_1$, then $S = \{1\} = S_m$ so that $l = 1$.

Part (ii) assumes that $l = m$. Thus $\chi(x)^l = 1$ for every $0 < x < g_m$, $(x, n) = 1$ and $\chi(g_m)^l \neq 1$. Hence g_m is the smallest positive integer x, $(x, n) = 1$, for which $\chi_1(x) \neq 1$.

To prove part (iii), we wish to estimate the number of values attained by χ_1 in the interval $[1, g_m(\chi)^{(m-t)/m})$. Assume that $\chi_1(x) = \zeta$ for some x with $(x, n) = 1$, $1 \leqslant x < g_m(\chi)^{(m-t)/m}$. Since the set of values $\chi(y)$ with $1 \leqslant y < g_m(\chi)^{1/m}$, $(n, y) = 1$ generates a group of order l, we have

$$\left|\{\chi(y_1 \cdots y_t) | 1 \leqslant y_1, \ldots, y_t < g_m(\chi)^{1/m}, (y_1 \cdots y_t, n) = 1\}\right| \geqslant t + 1$$

for all $t < l$ by Corollary 2.2. Thus $\chi(xy_1 \cdots y_t)$ attains at least $t + 1$ distinct values $\zeta_1, \ldots, \zeta_{t+1}$ with $\zeta_1^l = \cdots = \zeta_{t+1}^l = \zeta$, for $1 \leqslant y_1, \ldots, y_t < g_m(\chi)^{1/m}$ and hence for $1 \leqslant xy_1 \ldots y_t < g_m(\chi)$. In other words, to every nonzero value ζ attained by χ_1 in the interval $[1, g_m(\chi)^{(m-t)/m})$ there correspond at least $t + 1$ distinct values of χ, attained in the interval $[1, g_m(\chi))$, whose lth power is ζ. In addition we know from Theorem 2.1 that all l values

of the subgroup of lth roots of unity, that is the values $\chi(x)$ for which $\chi_1(x) = 1$, are attained in the interval $[1, g_m(\chi))$. Hence the number of distinct nonzero values of χ_1 in $[1, g_m(\chi)^{(m-t)/m})$ is at most $1 + (m - l)/(t + 1)$, that is

$$\left|\{\chi_1(x) | (x, n) = 1, 0 < x < g_m(\chi)^{(m-t)/m}\}\right| \leqslant \left[\frac{m-l}{t+1}\right] + 1 = m_t$$

for $0 \leqslant t \leqslant l - 1$. Hence $g_{m_t}(\chi_1) \geqslant g_m(\chi)^{(m-t)/m}$ for all these values of t whenever the sumbol $g_{m_t}(\chi_1)$ makes sense.

Lemma 3.3 enables us to get upper bounds for $g_m(\chi)$ in terms of $g_1(\chi^l)$ for the divisors l of k. If k is a prime, or generally when m is smaller than the least nontrivial divisor of k, then

$$g_m(\chi) \leqslant g_1(\chi)^m.$$

Now take $k = p^2$ where p is an odd prime. Then $g_m(\chi) \leqslant g_1(\chi)^m$ for $m < p$. For $p \leqslant m \leqslant 2p - 1$, we have either $l = 1$ and $g_m \leqslant g_1^m$ or $l = p$. In case $l = p$, choose $t = [m/2]$. Then

$$m_t = \left[\frac{m-p}{[m/2]+1}\right] + 1 = 1$$

and

$$g_m(\chi) \leqslant \max\left\{g_1(\chi)^m, g_1(\chi^p)^{m/(m-[m/2])}\right\} \leqslant \max\left\{g_1(\chi)^m, g_1(\chi^p)^2\right\}.$$

If $k > m \geqslant 2p$ and $l = p$ choose $t = p - 1$. Then $m_t = [m/p]$ and

$$g_m(\chi) \leqslant \max\left\{g_1(\chi)^m, g_{[m/p]}(\chi^p)^{m/(m-p+1)}\right\}.$$

But

$$g_{[m/p]}(\chi^p) \leqslant g_1(\chi^p)^{[m/p]} \leqslant g_1(\chi^p)^{m/p}$$

and therefore

$$g_m(\chi) \leqslant \max\left\{g_1(\chi)^m, g_1(\chi^p)^{m^2/p(m-p+1)}\right\}. \tag{3.4}$$

The computations get increasingly cumbersome as k has more factors. However, since, as we observed in the introduction, every χ can be expressed as a product of characters of prime power order, it is particularly useful to give the relations for $k = p^r$, p prime. This can be done by case divisions as above for the cases $r = 1, 2$. We omit the details.

Another upper bound for g_m for χ of arbitrary order k is obtained as follows.

Let l_1 be the order of the group generated by $\chi(g_1(\chi))$. Define $\chi_1 = \chi^{l_1}$ and let l_2 be the order of $\chi_1(g_1(\chi_1))$ and so on. In this manner we get divisors l_1, $l_2, \ldots, l_s$ of k so that $l_i > 1$ and $l_1 l_2 \cdots l_s = k$; and characters $\chi_i = \chi^{l_1 \cdots l_i}$ of order $k_i = k/l_1 \cdots l_i = l_{i+1} \cdots l_s$. The order of the group G_i generated by $\chi(g_1(\chi))$, $\chi(g_1(\chi_1))$, $\ldots$, $\chi(g_1(\chi_{i-1}))$ is $l_1 \cdots l_i$ as seen from the fact that

G_i/G_{i-1} is the cyclic group of order l_i generated by $\chi(g_1(\chi_{i-1}))G_{i-1}$, which is isomorphic to the group generated by $\chi_{i-1}(g_1(\chi_{i-1}))$. All values of G_i are attained by $\chi(x)$ with

$$1 \leqslant x \leqslant g_1(\chi)^{l_1-1} g_1(\chi_1)^{l_2-1} \cdots g_1(\chi_{i-1})^{l_i-1}.$$

The values $\chi(g_1(\chi)^{a_1} g_1(\chi_1)^{a_2} \cdots g_1(\chi_{i-1})^{a_i})$ are distinct elements of G_i for $0 \leqslant a_j < l_j$ and thus we have the following.

3.5. THEOREM. *There exist divisors $l_1, l_2, \ldots, l_s$ of k so that $l_i > 1$, $l_1 \cdots l_s = k$, $\chi_i = \chi^{l_1 \cdots l_i}$ and*

$$g_m(\chi) \leqslant g_1(\chi)^{a_1} g_1(\chi_1)^{a_2} \cdots g_1(\chi_{s-1})^{a_s}, \qquad 0 \leqslant a_i < l_i,$$

whenever

$$m \leqslant \Big|\big\{(b_1, \ldots, b_s) | 0 \leqslant b_i < l_i, g_1(\chi)^{b_1} \cdots g_1(\chi_{s-1})^{b_s} < g_1(\chi)^{a_1} \cdots g_1(\chi_{s-1})^{a_s}\big\}\Big|.$$

PROOF. We need only verify the assertion that

$$\chi(g_1(\chi)^{a_1} \cdots g_1(\chi_{i-1})^{a_i}) = \chi(g_1(\chi)^{b_1} \cdots g_1(\chi_{i-1})^{b_i}) \tag{3.6}$$

with $0 \leqslant a_j, b_j < l_j$ $(j = 1, \ldots, i)$ implies $a_j = b_j$ for $j = 1, \ldots, i$. We prove this by induction on i. For $i = 1$ we know that $\chi(g_1(\chi))$ is a root of unity of order l_1, and hence $\chi(g_1(\chi))^{a_1} = \chi(g_1(\chi))^{b_1}$ implies $a_1 \equiv b_1 \pmod{l_1}$, therefore $a_1 = b_1$ since $|a_1 - b_1| < l_1$. Now assume the statement true for $i - 1$ and raise both sides of (3.6) to the power $l_1 \cdots l_{i-1}$ to get

$$\chi_{i-1}(g_1(\chi_{i-1}))^{a_i} = \chi_{i-1}(g_1(\chi_{i-1}))^{b_i}$$

which implies $a_i \equiv b_i \pmod{l_i}$ and hence $a_i = b_i$, since $|a_i - b_i| < l_i$. Thus we can cancel the factor $\chi(g_1(\chi_{i-1}))^{a_i} = \chi(g_1(\chi_{i-1}))^{b_i}$ on both sides of (3.6) and get $a_j = b_j$ $(j = 1, \ldots, i)$ by the induction hypothesis.

4. Bounds in terms of powers of the modulus. Using the results on character sums due to D. A. Burgess [1] and K. Norton [4] which show that the different values of χ are equally distributed in relative short intervals, together with a simple sieve argument first used by Vinogradov [5], one can get bounds for $g_1(\chi)$, and thus for general $g_m(\chi)$ whose order is a fractional power of n. For details and further references see the monograph of K. Norton [3].

We need the following fact (compare [4, Theorem 7.24]).

4.1. LEMMA. *Let $N_m(h)$ be the number of integers x in $[1, h]$ for which $\chi(x) = \chi(g_m)$ where χ is a character of order k (mod n). Then*

$$N_m(h) = (\varphi(n)/kn)h + O(h^{1-1/r} n^{(r+1)/4r^2+\varepsilon}) \tag{4.2}$$

where r is an arbitrary positive integer, $\varepsilon > 0$, and the implied constant in O depends only on r and ε.

PROOF. Since Norton's proof in [4] refers to the case of power residues, we adapt the proof in [4] as suggested by the referee.

Let ζ be a kth root of unity; then

$$\frac{1}{k}\sum_{l=1}^{k}\zeta^l=\begin{cases}1 & \text{if } \zeta=1,\\ 0 & \text{if } \zeta\neq 1.\end{cases}$$

Hence

$$\frac{1}{k}\sum_{l=1}^{k}\chi^l(x)\bar{\chi}^l(g_m)=\begin{cases}1 & \text{if } \chi(x)=\chi(g_m),\\ 0 & \text{otherwise.}\end{cases}$$

Summing over $1\leqslant x\leqslant h$, we get

$$N_m(h)=\frac{1}{k}\sum_{l=1}^{k}\bar{\chi}^l(g_m)\sum_{1<x<h}\chi^l(x)$$

$$=\frac{1}{k}\left\{\sum_{1<x<h}\chi^k(x)+\sum_{l=1}^{k-1}\bar{\chi}^l(g_m)\sum_{1<x<h}\chi^l(x)\right\}. \tag{4.3}$$

Since χ^k is the principal character, we get by the method of Norton [4, p. 165] that

$$\sum_{1<x<h}\chi^k(x)=\frac{\varphi(n)}{n}\,h+O(n^{\varepsilon}).$$

We now use Theorem 2 of [1] which gives

$$\frac{1}{k}\left|\sum_{l=1}^{k-1}\bar{\chi}^l(g_m)\sum_{1<x<h}\chi^l(x)\right|\leqslant\frac{1}{k}\sum_{l=1}^{k-1}\left|\sum_{1<x<h}\chi^l(x)\right|$$

$$=\frac{1}{k}\sum_{l=1}^{k-1}O(h^{1-1/r}n^{(r+1)/4r^2+\varepsilon})=O(h^{1-1/r}n^{(r+1)/4r^2+\varepsilon}) \tag{4.4}$$

for any positive integer r (in case n is cube free as we assume throughout). Here the implied constant depends only on r and ε.

Combining (4.3) and (4.4) we have the desired result.

We also need the Dickman function.

4.5. DEFINITION. The *Dickman function* $\rho(\alpha)$ is defined for all nonnegative α by

$$\rho(\alpha)=1,\qquad 0\leqslant\alpha\leqslant 1,$$

$$\rho(\alpha)=\rho(N)-\int_N^{\alpha}\frac{\rho(\tau-1)}{\tau}\,d\tau,\qquad \begin{matrix}N<\alpha\leqslant N+1,\\ N=1,2,\cdots.\end{matrix}$$

The function $\rho(\alpha)$ is monotonically strictly decreasing for $1\leqslant\alpha<\infty$ with $\lim_{\alpha\to\infty}\rho(\alpha)=0$. It is therefore possible to define $\rho^{-1}(\zeta)$ for every $\zeta\in(0,1]$ as a number in $[1,\infty)$ (see [3, p. 3] for details).

Now let $N_n(x,y)$ be the number of integers prime to n in the interval $[1,x]$

which have no prime divisors $> y$. Then (see [3, (6.8)]) for $\alpha > 0$, $n \geqslant 3$ we have

$$N_n(x, x^{1/\alpha}) = \frac{\varphi(n)}{n}\ \rho(\alpha)x + O\left(\frac{(\log\log n)^2 x}{\log x} + n^{\varepsilon}(x^{1/\alpha} + x^{1-1/\alpha})\right) \tag{4.6}$$

where the implied constant depends only on α and ε.

We now write

$$g_m(\chi) = n^{1/\gamma_m(\chi)}, \qquad m = 1, \ldots, k-1.$$

In the following we assume k fixed. Then if $h = n^{1/4+\varepsilon}$, we can choose r such that the error term in (4.2) is small compared to the principal term. Thus

$$\gamma_m > 4 - \varepsilon \tag{4.7}$$

for all characters of order k provided n is sufficiently large.

Combining (4.2) and (4.6) we can prove the following (see [3, (1.7)]).

4.8. LEMMA. *For every ε there exists an $n(\varepsilon)$ such that $\gamma_1 \geqslant 4\rho^{-1}(1/k) - \varepsilon$ for all $n > n(\varepsilon, k)$.*

PROOF. Assume that there exists a $\delta > 0$ such that $\gamma_1 < 4\rho^{-1}(1/k) - \delta$ for infinitely many n and corresponding characters χ. Then choose $h = n^{1/4+\varepsilon}$, where ε is chosen so small that

$$g_1 = n^{1/\gamma_1} > h^{1/(\rho^{-1}(1/k)-\varepsilon)} + 1.$$

From (4.2) we get

$$N_0(h) = (\varphi(n)/kn)h(1 + o(1)). \tag{4.9}$$

From (4.6) we get

$$\begin{aligned} N_n(h, g_1 - 1) &> (\varphi(n)/n)\rho(\rho^{-1}(1/k) - \varepsilon)h(1 + o(1)) \\ &> (\varphi(n)/n)(1/k + \varepsilon)h(1 + o(1)), \end{aligned} \tag{4.10}$$

since ρ is a decreasing function. But every positive integer x which is prime to n and has all its prime factors $< g_1$ obviously satisfies $\chi(x) = 1$. Thus $N_0(h) \geqslant N_h(h, g_1 - 1)$, in contradiction to (4.9) and (4.10).

In order to apply Lemma 4.8 to the estimates of g_m which we obtained in §3, we observe the following.

4.11. LEMMA. *For all integers $k \geqslant 2$ and $1 \leqslant m < k$ we have*

$$(1/m)\rho_1^{-}(1/k) \leqslant \rho^{-1}(m/k).$$

PROOF. Set $f(x) = x\rho^{-1}(x/k)$. Then $f(x)$ is differentiable for all x in $0 < x < k$. For any x in this range, write $y = \rho^{-1}(x/k)$, so that $f(x) = ky\rho(y)$. Now, by Definition 4.3,

$$\frac{df}{dy} = k(\rho(y) + y\rho'(y)) = k(\rho(y) - \rho(y-1)) < 0$$

for all $y \in (1, \infty)$. Thus f is a decreasing function of y and hence an

increasing function of x, so that $f(1) \leqslant f(m)$.

If we combine Lemma 4.11 with Theorem 3.5 and write

$$g_1(\chi_i) = n^{1/\gamma_1(\chi_i)},$$

we find that for $i = 0, 1, \ldots, s-1$ and any ε, we have

$$\begin{aligned}\gamma_1(\chi_i) &> 4\rho^{-1}(1/k_i) - \varepsilon = 4\rho^{-1}((l_1 \cdots l_i)/k) - \varepsilon \\ &\geqslant (4/l_1 \cdots l_i)\rho^{-1}(1/k) - \varepsilon \qquad (4.12)\end{aligned}$$

for all large n.

4.13. THEOREM. *Let k be a fixed integer. For every ε, there exists an $n(\varepsilon, k)$ such that for every character χ of order k, we have*

$$\gamma_m(\chi) > (4/m)\rho^{-1}(1/k) - \varepsilon$$

for all $n > n(\varepsilon, k)$ and every integer $1 \leqslant m < k$.

PROOF. If $k = 1$ there is nothing to prove. If $k > 1$ define the divisors $l_1, \ldots, l_s$ and the characters $\chi_1, \ldots, \chi_{s-1}$ as in Theorem 3.5. We shall prove that for any ε there is an $n(\varepsilon, k)$ so that for all $n > n(\varepsilon, k)$ the number of solutions of the system

$$g_1^{a_1}(\chi)\, g_1^{a_2}(\chi_1) \cdots g_1^{a_s}(\chi_{s-1}) \leqslant \nu^m, \qquad 0 \leqslant a_i < l_i, \quad i = 1, \ldots, s, \quad (4.14)$$

where $\nu = n^{1/(4\rho^{-1}(1/k))+\varepsilon}$ is at least $m + 1$. Since χ attains distinct values at the integers on the left side of (4.14), this proves the theorem.

If we set $g_1(\chi_i) = \nu^{\beta_i}$, $g_1(\chi) = \nu^{\beta}$, then from Lemmas 4.8 and 4.11 it follows that $\beta \leqslant 1$, $\beta_i \leqslant l_1 \cdots l_i$. Now the number of solutions of (4.14) is equal to the number of solutions of

$$a_1\beta + a_2\beta_1 + \cdots + a_s\beta_{s-1} \leqslant m, \qquad 0 \leqslant a_i < l_i, \quad i = 1, \ldots, s, \quad (4.15)$$

and the number of such solutions can only decrease if the β, β_i are increased. It thus suffices to prove that the inequalities

$$\begin{aligned}a_1 + a_2 l_1 + a_3 l_1 l_2 + \cdots + a_s l_1 l_2 \cdots l_{s-1} &\leqslant m, \\ 0 \leqslant a_i < l_i, \quad i = 1, \ldots, s, \quad &(4.16)\end{aligned}$$

have $m + 1$ solutions. This is obvious from the fact that the expressions on the left of (4.16) represent all integers from 0 to $k - 1 = l_1 \cdots l_s - 1 \geqslant m$ in a unique manner as the a_i vary in the given ranges.

Note that Theorem 4.13 is useful only for m which are small compared to k since $\rho^{-1}(1/k)$ grows less rapidly than k. In fact (see [3, (3.24)]) we have $\rho^{-1}(1/k) << \log k/\log\log k$ for large k.

While we do not know how to improve the results in Theorem 4.13 without better information on the character sums which appear in the proof of Lemma 4.1, it is possible to get additional information for g_m of other characters in case $g_1(\chi)$ is comparatively large for some character χ.

4.17. COROLLARY. *Given characters χ_1 of order k_1 and χ_2 of order k_2. Assume that $g_m(\chi_2) < g_1(\chi_1)$. Then there exists an $n(\varepsilon, k)$ such that*

$$g_l(\chi_2) \leqslant n^{(l/4\rho^{-1}(1/k))+\varepsilon}, \qquad 1 \leqslant l \leqslant m,$$

where $k = [k_1, k_2]$ *and* $n \geqslant n(\varepsilon, k)$.

PROOF. Write $k_1 = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$, $k_2 = p_1^{\beta_1} \cdots p_s^{\beta_s}$ and set $k_1' = \prod_{\alpha_i \geqslant \beta_i} p_i^{\alpha_i}$, $k_2' = \prod_{\beta_i > \alpha_i} p_i^{\beta_i}$. Then the character

$$\chi = \chi_1^{k_1/k_1'} \chi_2^{k_2/k_2'}$$

has order $k = k_1'k_2' = [k_1, k_2]$.

Now assume that $g_1(\chi_1) > g_l(\chi_2)$. Then in the interval $[1, g_l(\chi_2))$ the character χ can assume at most l distinct nonzero values. Hence $g_l(\chi_2) \leqslant g_l(\chi)$. The corollary now follows from Theorem 4.13. It constitutes an improvement unless k_1 divides k_2.

5. More elaborate sieve arguments. We can improve the argument that led to the estimate of g_1 by way of (4.6) in a manner that was used by J. H. Jordan [2]. We illustrate the idea by estimating g_2.

5.1. DEFINITION. Let $N(x, y, z)$ be the number of integers in $[1, x]$ which have no prime factor $\geqslant y$ and at most one prime factor $\geqslant z$. Define $N_n(x, y, z)$ is an analogous manner, restricting attention to the integers which are relatively prime to n.

5.2. DEFINITION. $\rho(\alpha, \beta) = \rho(\beta) + \int_\alpha^\beta \rho(\beta - \beta/\tau)\, d\tau/\tau$, where $1 \leqslant \alpha \leqslant \beta < \infty$.

5.3. LEMMA. $N(x, x^{1/\alpha}, x^{1/\beta}) = \rho(\alpha, \beta)x + o(x)$, *where the constant implied in* $o(x)$ *depends only on* α, β.

PROOF. We have

$$\begin{aligned}
N(x, x^{1/\alpha}, x^{1/\beta}) &= N(x, x^{1/\beta}) + \sum_{x^{1/\beta} \leqslant p < x^{1/\alpha}} N\left[\left(\frac{x}{p}\right), x^{1/\beta}\right] \\
&= x\rho(\beta) + \sum_{x^{1/\beta} \leqslant p < x^{1/\alpha}} \frac{x}{p}\, \rho\left(\beta\, \frac{\log(x/p)}{\log x}\right) + o(x) \\
&= x\left(\rho(\beta) + \int_{x^{1/\beta}}^{x^{1/\alpha}} \rho\left(\beta \frac{\log(x/t)}{\log x}\right) \frac{dt}{t \log t} + o(1)\right) \\
&= x\left(\rho(\beta) + \int_\alpha^\beta \rho\left(\beta - \frac{\beta}{\tau}\right) \frac{d\tau}{\tau}\right) + o(x) \\
&= x\rho(\alpha, \beta) + o(x)
\end{aligned}$$

where we have substituted $t = x^{1/\tau}$ in the first integral.

We shall actually use a more specific lemma which we state without proof since the argument is entirely analogous to the one in [3] which leads to (4.6).

5.4. LEMMA. *If* $x > n^\delta$ *for a fixed* $\delta > 0$ *and* $\beta \geqslant \alpha \geqslant 1$, *then*

$$N_n(x, x^{1/\alpha}, x^{1/\beta}) = (\varphi(n)/n)\rho(\alpha, \beta)x(1 + o(1)).$$

Now we can express a bound for g_2.

5.5. THEOREM. *Let χ be a character of order k* (mod n), *and let $\gamma_1 = \gamma_1(\chi)$, $\gamma_2 = \gamma_2(\chi)$ be as in §4. Then for any ε and all large n, we have*

$$\rho(\gamma_2/4, \gamma_1/4) < 2/k + \varepsilon.$$

Since $\gamma_1/4 > \rho^{-1}(1/k) - \varepsilon$ for all large n and $\rho(\alpha, \beta)$ is a decreasing function of β for $1 \leqslant \alpha \leqslant \beta < \infty$, we get

$$\rho\big(\gamma_2/4, \rho^{-1}(1/k)\big) < 2/k + \varepsilon \tag{5.6}$$

for all large n.

PROOF. Choose $h = n^{1/4+\varepsilon}$. According to Lemma 4.1, the number of integers in $[1, h]$ for which χ has the value 1 or $\chi(g_1)$ is $(2\varphi(n)/kn)h(1 + o(1))$.

Now every integer x in $[1, h]$ with $(x, n) = 1$, which has no prime factor $\geqslant g_2$ and has at most one prime factor $\geqslant g_1$, obviously has $\chi(x) = 1$ or $\chi(x) = \chi(g_1)$. The number of such integers is

$$N(h, n^{1/\gamma_2}, n^{1/\gamma_1}) > N(h, h^{4/\gamma_2+\varepsilon}, h^{4/\gamma_1+\varepsilon}) > \frac{\varphi(n)}{n}\left(\rho\left(\frac{\gamma_2}{4}, \frac{\gamma_1}{4}\right) - \varepsilon\right)h.$$

Thus

$$\frac{2\varphi(n)}{kn}h > \frac{\varphi(n)}{n}\left(\rho\left(\frac{\gamma_2}{4}, \frac{\gamma_1}{4}\right) - \varepsilon\right)h$$

and the result follows.

It would not be difficult to extend these arguments to estimate g_m for larger values of m, but it would involve more case divisions.

REFERENCES

1. D. A. Burgess, *On character sums and L-series*. II, Proc. London Math. Soc. (3) **13** (1963), 524–536.

2. J. H. Jordan, *The distribution of cubic and quintic non-residues*, Pacific J. Math. **16** (1966), 77–85.

3. K. K. Norton, *Numbers with small prime factors and the least kth power non-residue*, Mem. Amer. Math. Soc. No. 106 (1971).

4. _____, *Upper bounds for k-th power coset representatives modulo n*, Acta. Arith. **15** (1969), 161–179.

5. I. M. Vinogradov, *On the bound of the least non-residue of nth powers*, Bull. Acad. Sci. USSR **20** (1926), 47–58 (Trans. Amer. Math. Soc. **29** (1927), 218–226).

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, LOS ANGELES, CALIFORNIA 90024 (Current address of E. G. Straus)

Current address (G. Kolesnik): Department of Mathematics, The University of Texas at Austin, RLM 8-100, Austin, Texas 78712