ACTA ARITHMETICA
LXXXV.1 (1998)

A character-sum estimate and applications

by

Karl K. Norton (Bangor, Me.)

1. Introduction. If χ is a Dirichlet character, we define

$$S_N(H,\chi)=\sum_{y=N+1}^{N+H}\chi(y) \tag{1.1}$$

for any integers N, H with $H\ge 1$. Our first objective is to obtain a conditional improvement of the following well-known result:

Theorem 1.2 (Burgess [8], [10]). *Let n, H be positive integers, let N be any integer, and let ε be any positive real number. Let χ be a nonprincipal Dirichlet character mod n. Then*

$$S_N(H,\chi)\ll_{\varepsilon,t} H^{1-1/t}n^{(t+1)/4t^2+\varepsilon} \tag{1.3}$$

for each of the values $t=1,2,3$ (the implied constant depends at most on ε and t). Furthermore, if n is cubefree, then (1.3) holds for every positive integer t.

Note that when $t=1$, (1.3) is a slightly weakened version of the Pólya–Vinogradov inequality (in which the factor n^{ε} can be replaced by $\log n$).

Theorem 1.2 has significant applications in number theory. For such applications, it is important that (1.3) be superior to the trivial inequality

$$|S_N(H,\chi)|\le H \tag{1.4}$$

in the widest possible range of H. For a given positive integer t, (1.3) is better than (1.4) if $H\ge n^{(t+1)/4t+\delta}$ for some fixed $\delta>0$, and otherwise (1.4) is better. In particular, (1.3) with $t=3$ is better than (1.4) whenever $H\ge n^{1/3+\delta}$, and (1.4) is better for every t if $H\le n^{1/4}$. In order to get nontrivial estimates from Theorem 1.2 in the range $n^{1/4}<H\le n^{1/3}$, we must assume $t>3$, which in turn requires the hypothesis that n be cubefree. We shall show that this latter hypothesis can be removed at the cost of

1991 *Mathematics Subject Classification*: Primary 11L40; Secondary 11N25, 11N56, 11N64.

an extra factor on the right-hand side of (1.3). We shall in fact obtain a new version of (1.3) which holds for any positive integers n, H, t and any nonprincipal χ mod n. This will lead to improved estimates in several related problems about the structure of the multiplicative group mod n.

Before stating our results, we need to specify some notation to be used throughout. The symbols n, k always represent positive integers, to be regarded as completely arbitrary unless further assumptions are stated. Also, y is any integer and p denotes any (positive) prime number. If a is a nonnegative integer, $p^a \parallel n$ means that $p^a \mid n$ and $p^{a+1} \nmid n$. We say n is *cubefree* if $p^3 \nmid n$ for every prime p. The symbols δ, ε represent any positive real numbers, and ε is not necessarily the same from one occurrence to the next. To avoid undue repetition in the statements of our theorems, we shall adopt the following convention throughout this paper:

(1.5) Any inequality involving ε is asserted to hold for every $\varepsilon > 0$.

The notations $O_{\delta,\varepsilon,\ldots}$ and $\ll_{\delta,\varepsilon,\ldots}$ imply constants depending at most on $\delta, \varepsilon, \ldots$, while O and $\ll$ without subscripts imply *absolute* constants. We use ϕ to denote Euler's function, and we define $\log_2 x = \log\log x$, $\log_r x = \log(\log_{r-1} x)$ for $r = 3, 4, \ldots$ We often write $x_1 \ldots x_m/y_1 \ldots y_n$ instead of $(x_1 \ldots x_m)(y_1 \ldots y_n)^{-1}$. $[x]$ denotes the greatest integer $\le x$. Empty sums mean 0, empty products 1. The term "character" means "Dirichlet character" throughout except in Lemma 3.6, where we refer to characters of a finite Abelian group. If χ is a character mod n, we write $\operatorname{ord}\chi$ for the order of χ (in the group of characters mod n).

Our new version of Theorem 1.2 reads as follows:

Theorem 1.6. *Let n, k, N, H be any integers with n, k, H positive. Let χ be a nonprincipal character mod n such that χ^k is principal. Then* (*recall* (1.5))

$$S_N(H,\chi) \ll_{\varepsilon,t} R_k(n)^{1/t} H^{1-1/t} n^{(t+1)/4t^2+\varepsilon} \tag{1.7}$$

for every positive integer t, where

$$R_k(n) = \min\{M(n)^{3/4}, Q(k)^{9/8}\} \tag{1.8}$$

and

$$M(n) = \prod_{p^a \parallel n,\, a \ge 3} p^a, \tag{1.9}$$

$$Q(k) = \prod_{p^a \parallel k,\, a \ge 2} p^a. \tag{1.10}$$

In particular,

$$S_N(H,\chi) \ll_\delta H n^{-\delta^2(1+2\delta)^{-1}} \quad \textit{if } H \ge R_k(n) n^{1/4+\delta} \textit{ and } \delta > 0. \tag{1.11}$$

Theorem 1.6 generalizes Theorem 1.2 when $t > 3$. The inequality (1.7) is of greatest interest when $Q(k)$ is of small or moderate size. For example, if k is bounded or squarefree, then (1.7) has the same strength as (1.3) with no restriction on n or t. In particular, it follows that (1.3) holds for all real-valued nonprincipal characters (the case $k = 2$) without restriction on n or t, a fact noted in a slightly weaker form by Burgess [7], p. 194, Corollary. When n is arbitrary and $R_k(n) \le n^{1/12-\alpha}$ for some fixed $\alpha > 0$, (1.11) shows that Theorem 1.6 gives a nontrivial estimate for $S_N(H,\chi)$ in a wider range of H than Theorem 1.2. On the other hand, it is not hard to see that Theorem 1.6 offers no advantage over the combination of (1.4) and Theorem 1.2 when $R_k(n) \ge n^{1/12}$.

Our first application of Theorem 1.6 is

Theorem 1.12. *Let χ be a nonprincipal character mod n. Let m, h be any integers with h positive, and suppose χ is constant on the set $\{y : m < y \le m+h \text{ and } (y,n) = 1\}$. Then $h \ll_\varepsilon n^{1/4+\varepsilon}$.*

This generalizes a theorem of Burgess [9], who obtained the estimate $h \ll p^{1/4}\log p$ when $n = p$ is prime. Theorem 1.12 also generalizes a result on consecutive power residues (or nonresidues) which was stated without proof by Norton [34], Theorem 4; a weaker version of that result was proved in [30], Theorem 3.15. See the remarks after the proof of Theorem 3.27 below.

The proof of Theorem 1.12 is a short, simple application of Theorem 1.6 (see §2). With more effort, Theorem 1.12 can be generalized considerably. Recall that $\operatorname{ord}\chi$ denotes the order of the character χ. If $\operatorname{ord}\chi = k$, it is a straightforward exercise to show that the set of nonzero values of χ is exactly the set of kth roots of unity. Our generalization of Theorem 1.12 reads as follows:

Theorem 1.13. *Let $K(q)$ be a real-valued function on the positive integers such that (recall (1.5))*

$$1 \le K(q) \ll_\varepsilon q^\varepsilon. \tag{1.14}$$

Let χ be a nonprincipal character mod n with $\operatorname{ord}\chi = k$. Let m, h be any integers with h positive, and suppose that χ assumes at most $\min\{k-1, K(n)\}$ distinct values on the set $\{y : m < y \le m+h \text{ and } (y,n) = 1\}$. Then $h \ll_\varepsilon n^{1/4+\varepsilon}$.

We shall prove this in §5. Some nontrivial bound on the number of values assumed by χ is necessary in Theorem 1.13, for if χ is a character mod p with $\operatorname{ord}\chi = p-1$, then χ assumes exactly h distinct values on the set $\{y : 0 < y \le h\}$ for any integer h with $1 \le h \le p-1$. It would be interesting to know whether the conclusion of Theorem 1.13 still holds if the assumption (1.14) is weakened somewhat.

In order to state further applications of Theorem 1.6, we must introduce some additional notation. For any positive integer n, let $C(n)$ denote the multiplicative group of residue classes mod n which are relatively prime to n. (For convenience in stating theorems about $C(n)$ and its subgroups, we shall generally ignore the distinction between a member $\{y : y \equiv b \pmod{n}\}$ of $C(n)$ and the integer b itself.) If E is any subgroup of $C(n)$, write

$$\nu = \nu(n; E) = [C(n) : E], \tag{1.15}$$

and let

$$1 = g_0(n; E) < g_1(n; E) < \ldots < g_{\nu-1}(n; E)$$

be the smallest positive representatives of the ν cosets of E in $C(n)$. Thus for $1 \le m \le \nu - 1$, $g_m = g_m(n; E)$ is the least positive integer relatively prime to n such that $g_m \notin \bigcup_{r=0}^{m-1} g_r E$.

A particularly interesting example of E is the subgroup

$$C_k(n) = \{z : z = x^k \text{ for some } x \in C(n)\}, \tag{1.16}$$

where k is a positive integer. In this case, we write

$$\nu(n; C_k(n)) = \nu_k(n). \tag{1.17}$$

When $\nu_k(n) > 1$, $g_1(n; C_k(n))$ exists and is the least positive kth power nonresidue mod n which is relatively prime to n. When p is prime, the estimation of the numbers $g_m(p; C_k(p))$ is a classical problem of great interest, particularly in the case $m = 1$. In a series of papers [29]–[34], the author generalized the classical methods for prime modulus to the case of an arbitrary modulus n, obtaining estimates for $g_m(n; C_k(n))$ and various related results on the distribution of power residues and nonresidues mod n. Using Theorem 1.6, we shall show in this paper how to strengthen several of those results, and we shall simultaneously generalize them by replacing $C_k(n)$ by an arbitrary subgroup E of $C(n)$. Bach [2] seems to be the only previous author to investigate the size of $g_m(n; E)$ when n and E are both arbitrary; however, he assumed the extended Riemann hypothesis and considered only the case $m = 1$.

To state here some of our main theorems, we need to introduce Dickman's function ϱ, defined recursively by

$$\varrho(\alpha) = \begin{cases} 1 & (0 \le \alpha \le 1), \\ \varrho(N) - \int_N^\alpha v^{-1} \varrho(v-1)\, dv & (N < \alpha \le N+1; \\ & \qquad N = 1, 2, \ldots). \end{cases} \tag{1.18}$$

The function $\varrho(\alpha)$ is positive, continuous, and strictly decreasing for $\alpha \ge 1$, and $\varrho(\alpha) \to 0$ as $\alpha \to +\infty$. (See [31], Lemma 4.7, or see [21], §2, where additional information and references are given.) Hence we can define a function $\alpha(w)$ by $\alpha(1) = 1$ and

$$\varrho(\alpha(w)) = w^{-1} \quad \text{for real } w > 1. \tag{1.19}$$

It follows that $\alpha(w)$ is strictly increasing for $w \geq 1$, and $\alpha(w) \to +\infty$ as $w \to +\infty$. (Estimates for $\alpha(w)$ and some numerical results are given at the end of §4.)

THEOREM 1.20. *Let w be any integer > 1. Let E be any subgroup of $C(n)$ with $\nu(n; E) \geq w$. Then* (*recall* (1.5))

$$g_1(n; E) \ll_{w,\varepsilon} n^{1/4\alpha(w)+\varepsilon}. \tag{1.21}$$

Taking $w = 2$, we get the universal estimate

$$g_1(n; E) \ll_{\varepsilon} n^{\beta+\varepsilon} \quad \text{whenever } E \neq C(n), \tag{1.22}$$

where

$$\beta = 1/4\alpha(2) = 1/4e^{1/2} = 0.15163\ldots \tag{1.23}$$

For the special case $E = C_k(n)$, the estimate (1.21) was stated without proof in Norton [34], Theorem 1. (The proof we had in mind at that time was different from the proof in this paper.) A somewhat less precise and less general result for $E = C_k(n)$ was proved in [31], Theorem 6.4. The latter result was a generalization of a theorem of Wang Yuan, who essentially obtained Theorem 1.20 for $n = p$ and $E = C_k(p)$, thus generalizing a theorem of Burgess for $n = p$ and $E = C_2(p)$ (for references and comments, see [31], pp. 4–7).

We can generalize Theorem 1.20 to the estimation of $g_m(n; E)$ when $1 < m < w \leq \nu(n; E)$, but the result (Theorem 4.23) is crude unless m is quite small compared to w. That result can be used, however, to obtain the following somewhat more satisfactory theorem:

THEOREM 1.24. *Let m be any positive integer, and let E be any subgroup of $C(n)$ with $\nu(n; E) > m$. Then*

$$g_m(n; E) \ll_{m,\varepsilon} n^{1/4+\varepsilon}. \tag{1.25}$$

For fixed $m \geq 2$, Theorem 1.24 gives our best universal upper bound for $g_m(n; E)$ (i.e., our best upper bound if we assume only that $g_m(n; E)$ exists). This theorem is significant only for bounded values of m, and in general, it sheds no light on the especially interesting case $m = \nu(n; E) - 1$. In the latter case, our methods do not yield good results unless $\nu = \nu(n; E)$ is a rather small function of n. Some such difficulty is to be expected, since trivially $g_m(n; E) \geq m + 1$ for $0 \leq m \leq \nu - 1$ (and $g_m(p; \{1\}) = m + 1$ for $0 \leq m \leq p - 2$). However, we can get the estimate

$$g_{\nu-1}(n; E) \ll_{k,\varepsilon} n^{1/4+\varepsilon} \quad \text{if } E \text{ contains } C_k(n) \tag{1.26}$$

(see Corollary 3.38 and the comments following it). We shall also prove the following uniform result when $\nu(n;E)$ is not too large (see Corollary 3.43 and the remark following it):

THEOREM 1.27. *Let $K(q)$ be a real-valued function on the positive integers such that* (1.14) *holds. Let E be any subgroup of $C(n)$ with $\nu = \nu(n;E) \le K(n)$. Then*

$$g_{\nu-1}(n;E) \ll_{\varepsilon} n^{1/4+\varepsilon}. \tag{1.28}$$

Our theorems yield new results on a problem considered by Kolesnik and Straus [25]. Let χ be a character mod n with $\operatorname{ord}\chi = k$. As we remarked before Theorem 1.13, χ assumes exactly k nonzero values (the kth roots of unity). As in [25], define $g_0 = g_0(\chi) = 1$, and for $1 \le m \le k-1$, let $g_m = g_m(\chi)$ be the least positive integer such that

$$\chi(g_m) \notin \{0, \chi(g_0), \chi(g_1), \ldots, \chi(g_{m-1})\}. \tag{1.29}$$

In other words, $g_m(\chi)$ is the least positive integer at which χ attains its $(m+1)$st nonzero value. Clearly

$$1 = g_0(\chi) < g_1(\chi) < \ldots < g_{k-1}(\chi) \le n.$$

Kolesnik and Straus obtained upper bounds for the numbers $g_m(\chi)$ under the assumptions that the modulus n is cubefree and $k = \operatorname{ord}\chi$ is bounded. We shall improve certain aspects of their work by eliminating these two assumptions. For example:

THEOREM 1.30. *Let w be any integer > 1. Let χ be a character mod n with* $\operatorname{ord}\chi = k \ge w$. *Then*

$$g_1(\chi) \ll_{w,\varepsilon} n^{1/4\alpha(w)+\varepsilon}, \tag{1.31}$$

where $\alpha(w)$ is defined by (1.19).

This may be compared with Lemma 4.8 of [25], where (1.31) is proved under the assumptions that n is cubefree and $k = w > 1$. Theorem 1.30 also improves Theorem 3.6 of Burthe [11], who obtained the case $w = 2$ of (1.31) under the assumption that $8 \nmid n$. (For arbitrary n, Burthe got a result like (1.31) with $w = 2$ and $1/4\alpha(w)$ replaced by $1/3\alpha(w)$.)

We shall prove Theorem 1.30 and give estimates for $g_m(\chi)$ when $m > 1$ in §5. See especially (5.7) and Corollary 5.14.

Our final main result is

THEOREM 1.32. *Let $G(n)$ be the least positive integer G such that $\{y : 1 \le y \le G$ and $(y,n) = 1\}$ generates $C(n)$. Then*

$$G(n) \ll_{\varepsilon} n^{\beta+\varepsilon}, \tag{1.33}$$

where β is defined by (1.23).

To prove this, let $n \geq 3$, and let E be the subgroup of $C(n)$ generated by $\{y : 1 \leq y < G(n) \text{ and } (y,n) = 1\}$. Then $E \neq C(n)$, and clearly $G(n) \notin E$. Hence $G(n) = g_1(n;E)$ and the result follows from (1.22).

In [11], Proposition 2.1, Burthe showed that for $n \geq 3$,

$$G(n) = \max\{g_1(\chi) : \chi \text{ nonprincipal mod } n\}. \tag{1.34}$$

Observe that (1.34) and Theorem 1.30 (with $w = 2$) yield another proof of Theorem 1.32. Burthe used (1.34) and a weaker version of Theorem 1.30 to get (1.33) when $8 \nmid n$, and he obtained the inequality $G(n) \ll_\varepsilon n^{4\beta/3+\varepsilon}$ for all n. Bach and Huelsbergen [3] had previously stated without proof the much weaker estimate

$$G(n) \ll n^{1/2}(\log n)\log_2 n.$$

Our upper bounds for the numbers $g_1(n;E)$ and $g_1(\chi)$ are much larger than bounds which can be obtained on the assumption of the extended Riemann hypothesis (ERH). Montgomery [28], Theorem 13.1, generalized work of Ankeny [1] by showing that

$$g_1(\chi) \ll (\log n)^2 \quad \text{on ERH} \tag{1.35}$$

for any nonprincipal character χ mod n. Bach [2] showed that

$$g_1(n;E) < 3(\log n)^2 \quad \text{on ERH} \tag{1.36}$$

if E is any subgroup of $C(n)$ with $E \neq C(n)$. (For remarks on related upper bounds, see [31], pp. 6–7, and [34], pp. 214–215, 218.) On the other hand, Elliott [14] obtained the unconditional lower bound

$$g_1(p;C_k(p)) > d_k \log p \tag{1.37}$$

for infinitely many primes $p \equiv 1 \pmod{k}$, where d_k is positive and depends only on k. (Elliott actually stated this result only for prime values of k but remarked to the author that it holds for any $k > 1$.) In the case $k = 2$, (1.37) was improved slightly but unconditionally by Graham and Ringrose [18], while Montgomery [28], Theorem 13.5 and p. 128, obtained a somewhat better result on ERH.

By (1.34) and (1.35), $G(n) \ll (\log n)^2$ for all $n \geq 2$ on ERH, and Pappalardi [35] has recently shown unconditionally that $G(p) \ll (\log p)^2$ for almost all primes p. Bach and Huelsbergen [3] gave a heuristic argument suggesting that the maximal order of $G(n)$ is about $(\log n)\log_2 n$. On the other hand, since $\nu(n;C_2(n)) = \nu_2(n) \geq 2$ for $n \geq 3$ (see the remarks at the beginning of §3), we have

$$G(n) \geq g_1(n;C_2(n)) \quad \text{for } n \geq 3, \tag{1.38}$$

for otherwise the integers y with $1 \leq y \leq G(n)$ and $(y,n) = 1$ would all be quadratic residues mod n and hence could not generate $C(n)$. Thus (1.37) and the improvements mentioned above lead to lower bounds for $G(p)$. (For further information on lower bounds for $G(n)$, see Burthe [11].) Moreover, (1.38) shows that any improvement in (1.33) would lead to a corresponding improvement in the long-standing estimate (1.22) for $g_1(n; C_2(n))$. Thus we expect that it will be difficult to improve Theorem 1.32.

My thanks to Dr. Ronald Burthe, Jr. for stimulating my interest in the problem of estimating $G(n)$. It was that stimulus which led to all of the developments in this paper.

2. Proofs of Theorems 1.6 and 1.12

LEMMA 2.1. *Suppose that n, q, m are positive integers with $n = qm$ and $(q,m) = 1$. If χ is a character mod n, then χ has a unique representation of the form $\chi = \theta\xi$, where θ is a character mod q and ξ is a character mod m. Also, χ is primitive if and only if θ and ξ are primitive.*

The proof of Lemma 2.1 is a straightforward exercise using the Chinese Remainder Theorem. For details, see [19], pp. 220–221. (Also see [19], pp. 217–224 for basic properties of conductors and primitive characters.)

In the remainder of this section, $S_N(H,\chi)$ is always defined by (1.1).

LEMMA 2.2. *Let χ be a primitive character mod n, where $n > 1$. Let N, H, t be any integers with H, t positive. Then*

$$S_N(H,\chi) \ll_{\varepsilon,t} M(n)^{3/4t} H^{1-1/t} n^{(t+1)/4t^2+\varepsilon}, \tag{2.3}$$

where $M(n)$ is defined by (1.9).

Proof. This lemma generalizes and strengthens a result of Burgess [7], Corollary to Theorem 1. We shall use his method of proof.

Write $M(n) = m$, and define

$$q = \prod_{p^a \| n,\, a \le 2} p^a,$$

so $n = qm$ and $(q,m) = 1$. First observe that if $H < m$, then

$$m^{3/4t} H^{1-1/t} n^{(t+1)/4t^2+\varepsilon} > m^{3/4t} H^{1-1/t} m^{1/4t} > H \ge |S_N(H,\chi)|.$$

Hence we may assume

$$H \ge m. \tag{2.4}$$

Also, if $m = n$, then (2.4) gives

$$m^{3/4t} H^{1-1/t} n^{(t+1)/4t^2+\varepsilon} > n \ge |S_N(H,\chi)|.$$

Hence we may assume $m < n$, so $q > 1$.

By Lemma 2.1, we can write $\chi = \theta\xi$, where θ is primitive mod q and ξ is primitive mod m. Observe that for each integer y, there is a unique integer w with $1 \le w \le m$ and $y \equiv -wq \pmod{m}$. If we use the notation

$\sum\{f(x) : P(x)\}$ for the summation of $f(x)$ over all x satisfying the condition $P(x)$ (a similar notation will be used below for certain products), it follows that

$$\begin{aligned}|S_N(H,\chi)| &= \Big|\sum_{w=1}^{m}\sum\{\theta(y)\xi(y) : N < y \le N+H,\ y \equiv -wq \pmod m\}\Big|\\ &\le \sum_{w=1}^{m}\Big|\sum\{\theta(y) : N < y \le N+H,\ y \equiv -wq \pmod m\}\Big|.\end{aligned}$$

Writing $y = zm - wq$, we get $\theta(y) = \theta(z)\theta(m)$, so

$$|S_N(H,\chi)| \le \sum_{w=1}^{m}\Big|\sum\{\theta(z) : (N+wq)/m < z \le (N+wq+H)/m\}\Big|.$$

Now apply Theorem 1.2 to the inner sum on the right, keeping in mind that q is cubefree. The number of integers z in the interval of summation is $< 2H/m$ by (2.4). Hence for any positive integer t,

$$\begin{aligned}S_N(H,\chi) &\ll_{\varepsilon,t} \sum_{w=1}^{m}(H/m)^{1-1/t}q^{(t+1)/4t^2+\varepsilon}\\ &= m^{1/t}H^{1-1/t}(n/m)^{(t+1)/4t^2+\varepsilon}. \ \blacksquare\end{aligned}$$

LEMMA 2.5. *Let χ be a nonprincipal character mod n with conductor d. Let N, H, t be any integers with H, t positive. Then*

$$S_N(H,\chi) \ll_{\varepsilon,t} 2^{\omega(n)}M(d)^{3/4t}H^{1-1/t}d^{(t+1)/4t^2+\varepsilon}, \tag{2.6}$$

where $\omega(n)$ is the number of distinct prime factors of n.

Proof. Let X be the primitive character mod d which induces χ. Define

$$f = \prod_{p\mid n,\, p\nmid d} p.$$

Then $\chi = \chi_0 X$, where χ_0 is the principal character mod f. Using the representation

$$\chi_0(y) = \sum_{h\mid (f,y)}\mu(h) = \sum_{h\mid f,\, h\mid y}\mu(h),$$

where μ is the Möbius function, we easily obtain

$$|S_N(H,\chi)| \le \sum_{h\mid f}\Big|\sum\{X(z) : N/h < z \le (N+H)/h\}\Big|.$$

We now apply Lemma 2.2 to the inner sum on the right and use the fact that $\sum_{h\mid f} 1 = 2^{\omega(f)} \le 2^{\omega(n)}$ to obtain (2.6). ■

In the special cases $t = 1, 2, 3$, the same method of proof with Theorem 1.2 in place of Lemma 2.2 shows that (2.6) holds without the factor $M(d)^{3/4t}$ on the right-hand side.

Before going further, we mention the simple fact that if n and q are any positive integers, then

$$n \mid q \quad \text{implies} \quad M(n) \mid M(q). \tag{2.7}$$

Since $2^{\omega(n)} \ll_\varepsilon n^\varepsilon$, it follows that for any nonprincipal χ mod n and any positive integer t, (2.6) implies (1.7) with $R_k(n)$ replaced by $M(n)^{3/4}$. It requires a little more work to obtain the full strength of Theorem 1.6.

Proof of Theorem 1.6. We need to introduce some notation. Write

$$n = p_1^{a_1} \ldots p_r^{a_r},$$

where $p_1, \ldots, p_r$ are primes with $p_1 < \ldots < p_r$ and a_j is a positive integer for each j. With reference to this factorization of n, write

$$k = p_1^{f_1} \ldots p_r^{f_r} k',$$

where each f_j is a nonnegative integer and k' is an integer with $(k', p_1 \ldots p_r) = 1$. For $1 \le j \le r$, define

$$\gamma_j = \begin{cases} \min\{a_j, f_j + 1\} & \text{if } p_j \text{ is odd}, \\ \min\{a_j, f_j + 2\} & \text{if } p_j = 2. \end{cases}$$

Also, let

$$\lambda = \lambda_k(n) = \begin{cases} 2 & \text{if } n \text{ is even and } k \text{ is odd}, \\ 1 & \text{otherwise}, \end{cases}$$

and define

$$n_k = \prod_{j=\lambda}^{r} p_j^{\gamma_j}. \tag{2.8}$$

(As always, an empty product means 1.)

Let d be the conductor of χ. We need the fact that

$$d \mid n_k. \tag{2.9}$$

This is the same as (3.18) of [32], where two proofs are given. (Some background is presented in [29]. Note that in both papers, ψ denotes a typical character mod n such that ψ^k is principal, and $K(\psi)$ is the conductor of ψ.) From (2.9) and (2.7), we get $M(d) \le M(n_k)$. Applying Lemma 2.5 and the inequalities $\omega(n) \le \omega(n_k) + 1$, $2^{\omega(m)} \ll_\varepsilon m^\varepsilon$, we obtain

$$S_N(H, \chi) \ll_{\varepsilon,t} M(n_k)^{3/4t} H^{1-1/t} n_k^{(t+1)/4t^2+\varepsilon} \tag{2.10}$$

for every positive integer t.

It is obvious that $n_k \mid n$, so

$$M(n_k) \mid M(n) \tag{2.11}$$

by (2.7). We shall complete the proof of (1.7) by showing that

$$M(n_k) \leq 8Q(k)^{3/2}. \tag{2.12}$$

To prove (2.12), first suppose that n is odd, or that n is even and k is odd. Then for each j with $\lambda \leq j \leq r$ and $\gamma_j \geq 3$, it follows that p_j is odd, $f_j \geq 2$, and $\gamma_j \leq f_j + 1 \leq (3/2)f_j$. Hence

$$M(n_k) \leq \prod\{p_j^{(3/2)f_j} : \lambda \leq j \leq r,\ f_j \geq 2\} \leq Q(k)^{3/2}.$$

Now suppose that n and k are both even, so $\lambda = 1$ and $p_1 = 2$. If $\gamma_1 < 3$, we obtain $M(n_k) \leq Q(k)^{3/2}$ as before. If $\gamma_1 = 3$, then

$$M(n_k) \leq 2^3 \prod\{p_j^{(3/2)f_j} : 2 \leq j \leq r,\ f_j \geq 2\} \leq 8Q(k)^{3/2}.$$

If $\gamma_1 \geq 4$, then $f_1 \geq 2$ and

$$M(n_k) \leq 2 \cdot 2^{(3/2)f_1} \prod\{p_j^{(3/2)f_j} : 2 \leq j \leq r,\ f_j \geq 2\} \leq 2Q(k)^{3/2}.$$

This completes the proof of (2.12), and (1.7) follows from (2.10), (2.11), and (2.12).

To prove (1.11), note that if $H \geq R_k(n)n^{1/4+\delta}$ for some $\delta > 0$, then (1.7) yields

$$S_N(H,\chi) \ll_{\varepsilon,t} Hn^{f(t)+\varepsilon},$$

where $f(t) = -\delta/t + 1/4t^2$. The function $f(x)$ increases for real $x \geq 1/2\delta$, so if we take $t = [1/2\delta] + 1$, we get

$$\begin{aligned} f(t) &\leq f(1/2\delta + 1) = -2\delta^2(1+2\delta)^{-1} + \delta^2(1+2\delta)^{-2} \\ &< (-\delta^2 - 2\delta^3)(1+2\delta)^{-2} = -\delta^2(1+2\delta)^{-1}, \end{aligned}$$

and (1.11) follows with an appropriate choice of $\varepsilon = \varepsilon(\delta)$. ■

Note that (2.10) is our most general estimate for $S_N(H,\chi)$ under the hypotheses of Theorem 1.6. Because of the complicated definition (2.8) of n_k, it seems preferable to have the simplified inequality (1.7) in place of (2.10).

As an application of Theorem 1.6, we have

Proof of Theorem 1.12. Let χ be a nonprincipal character mod n which is constant on $\{y : m < y \leq m+h \text{ and } (y,n) = 1\}$. Write $\operatorname{ord}\chi = k$, and define a character θ mod n as follows: choose a prime factor q of k and let $\theta = \chi^{k/q}$. Then θ has order q, and θ is constant on $\{y : m < y \leq m+h \text{ and } (y,n) = 1\}$. Hence $|S_m(h,\theta)| = S_m(h,\chi_0)$, where χ_0 is the principal character mod n. Now, the estimate

$$S_m(h,\chi_0) = n^{-1}\phi(n)h + O_\varepsilon(n^\varepsilon) \tag{2.13}$$

is easily obtained by using the representation for $\chi_0(y)$ given in the proof of Lemma 2.5 (see [29], (3.17)). On the other hand, Theorem 1.6 gives

$$S_m(h,\theta) \ll_{\varepsilon,t} h^{1-1/t} n^{(t+1)/4t^2+\varepsilon}$$

for every positive integer t. Comparing this inequality with (2.13) and choosing t as an appropriate function of ε, we get the result. ■

The use of Theorem 1.2 instead of Theorem 1.6 in the preceding proof would yield the weaker estimate $h \ll_\varepsilon n^{1/3+\varepsilon}$ (unless n is cubefree).

3. Distribution of integers in cosets of a subgroup of $C(n)$. Throughout this section, n and k denote any positive integers, and we use the notations $C(n)$, E, $\nu(n;E)$, $g_m(n;E)$, $C_k(n)$, $\nu_k(n)$ introduced after Theorem 1.13. Thus E denotes an arbitrary subgroup of $C(n)$, while $C_k(n)$ is the special subgroup defined by (1.16). In [29], p. 167, it was shown that for fixed k, the index $\nu_k(n) = [C(n) : C_k(n)]$ is a multiplicative function of n, and the following formulas were established:

$$\nu_k(p^a) = (k, \phi(p^a)) \quad \text{if } p \text{ is an odd prime and } a = 1,2,\ldots, \tag{3.1}$$

$$\nu_k(2) = 1, \qquad \nu_k(2^a) = (k,2)(k,2^{a-2}) \quad \text{for } a = 2,3,\ldots \tag{3.2}$$

It follows that

$$\nu_k(n) \le 2k^{\omega(n)}, \tag{3.3}$$

where $\omega(n)$ is the number of distinct prime factors of n. It is well known that $\omega(n) \ll (\log n)(\log_2 n)^{-1}$ for $n \ge 3$, so (3.3) implies

$$\nu_k(n) \ll_{k,\varepsilon} n^\varepsilon. \tag{3.4}$$

If k is an integer such that E contains $C_k(n)$, then clearly $\nu(n;E) \le \nu_k(n)$. Hence

$$\nu(n;E) \ll_{k,\varepsilon} n^\varepsilon \quad \text{if } E \text{ contains } C_k(n). \tag{3.5}$$

Our objective in this section is to study the distribution of members of cosets of E in intervals. We begin with the following lemma:

LEMMA 3.6. *Let G be a finite multiplicative Abelian group, and let G^* denote its character group. Let k be a positive integer, and write $G_k = \{z : z = x^k$ for some $x \in G\}$. If H is any subgroup of G, define*

$$H' = \{\theta \in G^* : \theta(x) = 1 \text{ for all } x \in H\} \tag{3.7}$$

(thus H' is a subgroup of G^*). For each $\theta \in H'$, define θ^* on G/H by $\theta^*(xH) = \theta(x)$. Then:

(3.8) *G is isomorphic to G^*;*

(3.9) *$H = \{x \in G : \theta(x) = 1$ for all $\theta \in H'\}$;*

(3.10) *the mapping $\theta \mapsto \theta^*$ is an isomorphism of H' onto $(G/H)^*$;*

(3.11) $$\sum_{x\in H}\theta(x)=\begin{cases}|H| & \text{if } \theta\in H',\\ 0 & \text{if } \theta\in G^*\setminus H';\end{cases}$$

(3.12) $$\sum_{\theta\in H'}\theta(x)=\begin{cases}[G:H] & \text{if } x\in H,\\ 0 & \text{if } x\in G\setminus H;\end{cases}$$

(3.13) *if* $\sigma=[G:H]$ *and* $x_1,\ldots,x_\sigma$ *are any representatives of the distinct cosets of* H *in* G, *then*
$$\sum_{j=1}^{\sigma}\theta(x_j)=\begin{cases}\sigma & \text{if } \theta \text{ is the principal character},\\ 0 & \text{if } \theta\in H' \text{ and } \theta \text{ is nonprincipal};\end{cases}$$

(3.14) $|H'|=[G:H]$;

(3.15) H *contains* G_k *if and only if* θ^k *is principal for each* $\theta\in H'$;

(3.16) *if* $[G:H]$ *divides* k, *then* H *contains* G_k.

Proof. The assertions (3.8) to (3.13) constitute Lemma 3.1 of [29]. The assertion (3.14) follows from (3.10) and (3.8). The result (3.15) is an obvious consequence of the elementary fact that if J and H are subgroups of G, then H contains J if and only if J' contains H' (the proof of this uses (3.9)). Finally, if $[G:H]$ divides k, then $|H'|$ divides k by (3.14), so θ^k is principal for each $\theta\in H'$, so H contains G_k by (3.15). ∎

LEMMA 3.17. *Write* $\nu(n;E)=\nu$, $g_s(n;E)=g_s$. *Let* s, m *be any integers with* $0\le s\le\nu-1$, *and let* h *be real with* $h\ge 1$. *Define* $N_s(n,E;m,m+h)$ *to be the number of integers* y *such that* $m<y\le m+h$ *and* $y\in g_sE$. *Then* (*recall* (1.1))

(3.18) $$N_s(n,E;m,m+h)=\nu^{-1}S_m([h],\chi_0)+\nu^{-1}\Delta_s(n,E;m,m+h),$$

where χ_0 *is the principal character mod* n,

(3.19) $$\Delta_s(n,E;m,m+h)=\sum_{\theta}{}'\,\overline{\theta}(g_s)S_m([h],\theta),$$

and

(3.20) $$\sum_{\theta}{}' \quad \text{means} \quad \sum_{\theta\in E',\,\theta\ne\chi_0}.$$

Furthermore,

(3.21) $$\sum_{s=0}^{\nu-1}\Delta_s(n,E;m,m+h)=0,$$

(3.22) $$\sum_{s=0}^{\nu-1}\{\Delta_s(n,E;m,m+h)\}^2=\nu\sum_{\theta}{}'\,|S_m([h],\theta)|^2.$$

Proof. Apply Lemma 3.6 with $G = C(n)$, $H = E$. By (3.14), $|E'| = [C(n) : E] = \nu$, and it follows from (3.12) that

$$\nu^{-1} \sum_{\theta\in E'} \theta(y)\overline{\theta}(g_s) = \begin{cases} 1 & \text{if } y \in g_s E, \\ 0 & \text{otherwise.} \end{cases}$$

Summing this formula over $m < y \le m+h$, we get (3.18). To get (3.21), simply observe that

$$\sum_{s=0}^{\nu-1} N_s(n, E; m, m+h) = S_m([h], \chi_0)$$

and apply (3.18). To prove (3.22), square both sides of (3.19) and sum over s to get

$$\begin{aligned}\sum_{s=0}^{\nu-1} &\{\Delta_s(n, E; m, m+h)\}^2 \\ &= \sum_{s=0}^{\nu-1} \sideset{}{'}\sum_{\theta_1,\theta_2} \sum_{1\le y_1,\, y_2\le h} (\overline{\theta}_1\theta_2)(g_s)\theta_1(m+y_1)\overline{\theta}_2(m+y_2).\end{aligned}$$

Now invert the order of summation and use (3.13) to get (3.22). ■

Theorem 3.23. *Write $\nu(n; E) = \nu$. Let s, m be any integers with $0 \le s \le \nu - 1$, and let h be real with $h \ge 1$. Then*

$$N_s(n, E; m, m+h) = (\nu n)^{-1}\phi(n)h + O_\varepsilon(h^{1-1/t} n^{(t+1)/4t^2+\varepsilon}) \tag{3.24}$$

for each of the values $t = 1, 2, 3$. If we assume also that k is a positive integer such that E contains $C_k(n)$, then

$$\begin{aligned} N_s&(n, E; m, m+h) \\ &= (\nu n)^{-1}\phi(n)h + O_{\varepsilon,t}(R_k(n)^{1/t} h^{1-1/t} n^{(t+1)/4t^2+\varepsilon}) \end{aligned} \tag{3.25}$$

for every positive integer t, where $R_k(n)$ is defined by (1.8).

Proof. To prove (3.24), we use (2.13) to estimate the first term on the right-hand side of (3.18), then estimate $\Delta_s(n, E; m, m+h)$ by applying Theorem 1.2 and (3.14) (with $G = C(n)$, $H = E$) to (3.19):

$$\begin{aligned}\Delta_s(n, E; m, m+h) &\ll_{\varepsilon,t} \sideset{}{'}\sum_{\theta} h^{1-1/t} n^{(t+1)/4t^2+\varepsilon} \\ &\ll_{\varepsilon,t} \nu h^{1-1/t} n^{(t+1)/4t^2+\varepsilon}\end{aligned}$$

for $t = 1, 2, 3$.

Now suppose that E contains $C_k(n)$. By (3.15), $\theta^k = \chi_0$ for each $\theta \in E'$. Using Theorem 1.6 instead of Theorem 1.2, we obtain (3.25) (for every positive integer t) in the same way as (3.24). ■

Theorem 3.23 is an appreciable improvement of Theorem 3.7 of Norton [30], which dealt only with the special case $E = C_k(n)$ (and which in turn strengthened and generalized a result of Jordan [23]). Note that for any subgroup E of $C(n)$, (3.16) shows that

$$\text{(3.26)} \qquad \textit{If } \nu = \nu(n; E) \textit{ divides } k, \textit{ then } E \textit{ contains } C_k(n).$$

In particular, E contains $C_\nu(n)$, so that (3.25) holds for every positive integer t if $R_k(n)$ is replaced by $R_\nu(n)$ (which does not exceed $\nu^{9/8}$ by Theorem 1.6).

THEOREM 3.27. *Let m, w be any integers with $1 \le w < \nu = \nu(n; E)$, and let $h \ge 1$ be real. Suppose that the set $\{y : m < y \le m + h$ and $(y, n) = 1\}$ is contained in the union of w distinct cosets of E in $C(n)$. Then*

$$\text{(3.28)} \qquad h \ll_\varepsilon \{\nu w(\nu - w)^{-1}\}^{t/2} n^{(t+1)/4t+\varepsilon} \quad \textit{for } t = 1, 2, 3.$$

If we assume also that k is a positive integer such that E contains $C_k(n)$, then

$$\text{(3.29)} \qquad h \ll_{\varepsilon,t} \{\nu w(\nu - w)^{-1}\}^{t/2} R_k(n) n^{(t+1)/4t+\varepsilon}$$

for every positive integer t. In particular,

$$\text{(3.30)} \qquad h \ll_{k,\varepsilon} n^{1/4+\varepsilon} \quad \textit{if } E \textit{ contains } C_k(n).$$

Proof. Let T be a set of w distinct indices such that $\{y : m < y \le m + h$ and $(y, n) = 1\}$ is contained in $\bigcup_{s \in T} g_s E$, where $g_s = g_s(n; E)$. Let $V = \{s : 0 \le s \le \nu - 1$ and $s \notin T\}$, and write $S_m([h], \chi_0) = B$, where χ_0 is the principal character mod n. If $s \in V$, then $N_s(n, E; m, m + h) = 0$, so by (3.18),

$$\text{(3.31)} \qquad B = -\Delta_s(n, E; m, m + h) \quad \text{for each } s \in V$$

and

$$\text{(3.32)} \qquad (\nu - w)B^2 = \sum_{s \in V} \{\Delta_s(n, E; m, m + h)\}^2.$$

Adding the identities (3.31) over all $s \in V$ and using (3.21), we get

$$(\nu - w)B = \sum_{s \in T} \Delta_s(n, E; m, m + h).$$

Applying the Cauchy–Schwarz inequality to this, we get

$$\text{(3.33)} \qquad (\nu - w)^2 B^2 \le w \sum_{s \in T} \{\Delta_s(n, E; m, m + h)\}^2.$$

A combination of (3.32) and (3.33) yields

$$(\nu - w)B^2 + w^{-1}(\nu - w)^2 B^2 \le \sum_{s=0}^{\nu-1} \{\Delta_s(n, E; m, m + h)\}^2,$$

and it follows from this and (3.22) (see (3.20)) that

$$B^2 \le w(\nu - w)^{-1} {\sum_\theta}' |S_m([h], \theta)|^2. \tag{3.34}$$

Applying Theorem 1.2 to (3.34) and using (3.14), we get

$$B \ll_{\varepsilon,t} \{\nu w(\nu - w)^{-1}\}^{1/2} h^{1-1/t} n^{(t+1)/4t^2+\varepsilon} \quad \text{for } t = 1, 2, 3.$$

By (2.13), $n^{-1}\phi(n)h = B + O_\varepsilon(n^\varepsilon)$, and since $n/\phi(n) \ll_\varepsilon n^\varepsilon$, we find that

$$h \ll_{\varepsilon,t} \{\nu w(\nu - w)^{-1}\}^{1/2} h^{1-1/t} n^{(t+1)/4t^2+\varepsilon} \quad \text{for } t = 1, 2, 3,$$

from which (3.28) follows. The estimate (3.29) is obtained in the same way from (3.34), (3.15), and (1.7).

Finally, observe that

$$\nu(\nu - w)^{-1} = 1 + w(\nu - w)^{-1} \le w + 1,$$

so (3.29) gives

$$h \ll_{\varepsilon,t} w^t R_k(n) n^{(t+1)/4t+\varepsilon} \quad (\text{if } E \text{ contains } C_k(n)) \tag{3.35}$$

for all positive integers t. Now apply (3.5), choose t appropriately as a function of ε, and observe that $R_k(n) \le k^{9/8}$ by (1.8) and (1.10). This gives (3.30). ■

In the special case $w = 1$, the conclusion of Theorem 3.27 can be improved, for (3.14) shows that there exists a nonprincipal character χ in E', and χ must be constant on $\{y : m < y \le m + h \text{ and } (y, n) = 1\}$. Hence $h \ll_\varepsilon n^{1/4+\varepsilon}$ by Theorem 1.12 (there is no need for the assumption that E contains $C_k(n)$). This result generalizes Theorem 4 of [34] (which was stated without proof) and strengthens Theorem 3.15 of [30].

As an example of the application of Theorem 3.27, suppose that $\nu = \nu(n; E) > 1$ and that $m < q$ are successive members of a given coset of E. Then the set $\{y : m < y < q \text{ and } (y, n) = 1\}$ is contained in the union of the remaining $\nu - 1$ distinct cosets of E, so by (3.28),

$$q - m \ll_\varepsilon \nu^t n^{(t+1)/4t+\varepsilon} \quad \text{for } t = 1, 2, 3, \tag{3.36}$$

and if E contains $C_k(n)$, (3.30) gives

$$q - m \ll_{k,\varepsilon} n^{1/4+\varepsilon}. \tag{3.37}$$

These inequalities generalize and strengthen Theorem 3.23 of [30], where the best unconditional estimate was $q - m \ll_{k,\varepsilon} n^{3/8+\varepsilon}$ when $E = C_k(n)$.

Similarly, Theorem 3.27 can be applied to the estimation of the coset representatives $g_m(n; E)$:

Corollary 3.38. *Let m be any integer with $1 \le m < \nu = \nu(n; E)$. Then*

$$g_m(n; E) \ll_\varepsilon m^t n^{(t+1)/4t+\varepsilon} \quad \textit{for } t = 1, 2, 3. \tag{3.39}$$

If k is a positive integer such that E contains $C_k(n)$, then

$$g_m(n;E) \ll_{m,\varepsilon} R_k(n)n^{1/4+\varepsilon} \tag{3.40}$$

and

$$g_{\nu-1}(n;E) \ll_{k,\varepsilon} n^{1/4+\varepsilon}. \tag{3.41}$$

Proof. Write $g_m(n;E) = g_m$. The set $\{y : 1 \le y < g_m \text{ and } (y,n) = 1\}$ is contained in the union of the cosets $g_0E, g_1E, \ldots, g_{m-1}E$. Thus (3.39) follows from (3.28) and the inequality $\nu(\nu - m)^{-1} \le m + 1$. Likewise, (3.40) follows from (3.29), and (3.41) is a consequence of (3.30). ■

Corollary 3.38 generalizes and strengthens Theorems 7.18 and 7.21 of Norton [29], where the best unconditional result was essentially $g_m(n; C_k(n)) \ll_{k,\varepsilon} n^{3/8+\varepsilon}$ for $1 \le m < \nu_k(n)$. Better results than (3.41) are known in some special cases. For example, when $n = p$ is prime, Jordan [24] (see also [22]) obtained

$$g_{\nu-1}(p; C_k(p)) \ll_{k,\varepsilon} p^{(1-d)/4+\varepsilon}. \tag{3.42}$$

Here $\nu = \nu_k(p) = (k, p-1)$ and $d = d(\nu)$ is a small positive function of ν defined in a complicated way. Certain generalizations of (3.42) to the case of arbitrary modulus n were given by Norton [29], Theorem 7.27; these required that n have a bounded number of distinct prime factors. More recently, Elliott [16], Theorem 1 (see also [15]) used a new method to obtain a result which implies (3.42) with a different (quite small) value of $d = d_1(\nu)$. See (5.9) below and the comments following it.

We shall show in §4 that the factor $R_k(n)$ in (3.40) can be omitted, and the assumption that E contains $C_k(n)$ is not needed for this improved version of (3.40). This is the content of Theorem 1.24.

If we assume that $\nu(n;E)$ is not very large, we can derive a version of Theorem 3.27 which is uniform in w and dispenses with the hypothesis that E contains $C_k(n)$:

COROLLARY 3.43. *Let $K(q)$ be a real-valued function on the positive integers such that* (1.14) *holds. Let E be any subgroup of $C(n)$ with $2 \le \nu = \nu(n;E) \le K(n)$. Let m, h be any integers with h positive*, *and suppose that the set $\{y : m < y \le m + h$ and $(y,n) = 1\}$ is contained in the union of $\nu - 1$ distinct cosets of E. Then $h \ll_\varepsilon n^{1/4+\varepsilon}$.*

Proof. By (3.26), E contains $C_\nu(n)$. Apply Theorem 3.27 with $w = \nu-1$ and $k = \nu$. By (3.29),

$$h \ll_{\varepsilon,t} \nu^t R_\nu(n) n^{(t+1)/4t+\varepsilon/4}$$

for all positive integers t. Now, $R_\nu(n) \le \nu^{9/8}$ by (1.8), and by assumption, $\nu \le K(n) \ll_{\varepsilon,t} n^{\varepsilon/4t}$. Hence

$$h \ll_{\varepsilon,t} n^{\varepsilon/4+(9/8)(\varepsilon/4t)+(t+1)/4t+\varepsilon/4}$$

for every positive integer t. If we choose $t = \max\{2, [1/\varepsilon] + 1\}$, we get the result. ■

Theorem 1.27 follows immediately from Corollary 3.43 if we take $m = 0$, $h = g_{\nu-1}(n; E) - 1$.

4. Proofs of Theorems 1.20 and 1.24. We continue to use the notation of §3. At this point, we have proved the estimates for $g_m(n; E)$ given by Corollary 3.38 and Theorem 1.27. Also, from the remark immediately following the proof of Theorem 3.27, Theorem 1.12 implies that $g_1(n; E) \ll_\varepsilon n^{1/4+\varepsilon}$ whenever $\nu(n; E) > 1$. We now seek to improve these results on $g_m(n; E)$ when m is bounded. For this purpose, we introduce the function $\Psi_n(x, z)$, defined to be the number of integers y such that $1 \le y \le x$, $(y, n) = 1$, and y has no prime factor greater than z (here x, z are real numbers with $x \ge 1$, $z \ge 1$). We shall need an asymptotic formula (or at least a sharp lower bound) for $\Psi_n(x, z)$.

A very large amount of research has been done on the estimation of $\Psi_1(x, z)$, but there have been relatively few papers on $\Psi_n(x, z)$ for $n > 1$. Norton [31] gave the first complete proofs of asymptotic formulas for $\Psi_n(x, z)$ when n is allowed to assume values which are rather large relative to x and z. Those formulas were applied in [31] to the estimation of $g_1(n; C_k(n))$ from above. Norton's formulas for $\Psi_n(x, z)$ were extended to asymptotic expansions and further improved by Hazlewood [20]. (Hazlewood used ideas of Levin and Faĭnleĭb [26], and he clarified and corrected some of their work in the process.) The next progress on $\Psi_n(x, z)$ was made much more recently by Fouvry and Tenenbaum [17], who used more difficult methods and considerably extended the range and precision of Norton's and Hazlewood's work. For further recent results on $\Psi_n(x, z)$, see Tenenbaum [36] and Xuan [37].

A survey of the research on $\Psi_n(x, z)$ up to 1970 (most of it dealing with the case $n = 1$) was given in [31]. For a very extensive survey of the literature since then, together with many proofs and a discussion of related problems, see Hildebrand and Tenenbaum [21].

While [17], [36], [37] contain refinements of Norton's and Hazlewood's work on $\Psi_n(x, z)$, those refinements are stated in such a way that they are inconvenient to use for our present purpose: the estimation of $g_m(n; E)$ for bounded m. Furthermore, we have no need for the extra precision and wider range of validity of the recent work on $\Psi_n(x, z)$, and the following rather simple formula (which follows immediately from [31], Theorem 5.48) is quite sufficient:

Lemma 4.1. *Let* $n \ge 3$, *and let* x, α, A *be real with* $x > e$, $1 \le \alpha \le A$. *Then* (*see* (1.5) *and* (1.18))

$$\Psi_n(x, x^{1/\alpha}) \\ = n^{-1}\phi(n)\varrho(\alpha)x + O_{\varepsilon,A}((\log_2 n)^2(x/\log x) + n^\varepsilon(x^{1/\alpha} + x^{1-1/\alpha})).$$

With this formula, we are in a position to prove the following preliminary estimates:

LEMMA 4.2. *Define the function $\alpha(w)$ by (1.19). Let m, w be any integers with $1 \le m < w$, and let E be any subgroup of $C(n)$ with $\nu = \nu(n; E) \ge w$. Write $g_s(n; E) = g_s$ for $0 \le s \le \nu - 1$, and suppose that $\{g_sE : 0 \le s \le m - 1\}$ is a subgroup of the quotient group $C(n)/E$. Then for each $\delta > 0$, we have*

$$g_m \ll_{w,\delta} n^{1/3\alpha(w/m)+\delta}. \tag{4.3}$$

If we assume also that k is a positive integer such that E contains $C_k(n)$, then for each $\delta > 0$,

$$g_m \ll_{w,\delta} R_k(n)n^{1/4\alpha(w/m)+\delta}. \tag{4.4}$$

Proof. It is clear that for each real $h \ge 1$, the set $\{y : 1 \le y \le h, (y, n) = 1$, and y has no prime factor $> g_m - 1\}$ is contained in the set

$$\bigcup_{s=0}^{m-1} \{y : 1 \le y \le h \text{ and } y \in g_sE\}.$$

Therefore,

$$\Psi_n(h, g_m - 1) \le \sum_{s=0}^{m-1} N_s(n, E; 0, h) \quad \text{for real } h \ge 1, \tag{4.5}$$

in the notation of Lemma 3.17. The idea of the proof is to take $h = (g_m-1)^\alpha$ for a suitable α, then compare the estimates of Lemma 4.1 and Theorem 3.23 via (4.5). While the proof is similar to the proof of [31], Theorem 6.4, we shall give it in full because of some additional complications.

It suffices to prove (4.3) and (4.4) under the assumption that

$$0 < \delta \le 1/2w. \tag{4.6}$$

By the definition (1.18),

$$\varrho(\alpha) = 1 - \log\alpha \quad \text{for } 1 \le \alpha \le 2, \tag{4.7}$$

and it follows from (1.19) that

$$\alpha(u) = \exp(1 - u^{-1}) \quad \text{for } 1 \le u \le (1 - \log 2)^{-1} = 3.25889\ldots \tag{4.8}$$

Since $\alpha(u)$ is strictly increasing for $u \ge 1$, we have

$$\alpha(w/m) \ge \alpha(w(w-1)^{-1}) = \exp(w^{-1}) > 1 + w^{-1}. \tag{4.9}$$

For the remainder of this proof, we hold δ fixed (subject to (4.6)), and we define

$$\alpha = \alpha(w/m) - \delta, \tag{4.10}$$

so

$$\alpha(w) > \alpha > 1 + (2w)^{-1} \tag{4.11}$$

by (4.6) and (4.9).

Since $\varrho(u)$ is positive and strictly decreasing for $u \geq 1$, we can apply [31], (4.10), to get

$$\gamma\varrho(\gamma) = \int\limits_{\gamma-1}^{\gamma} \varrho(z)\,dz \leq \varrho(\gamma - 1) \quad \text{for } \gamma \geq 1,$$

and by [31], (4.8), it follows that

$$\begin{aligned}\varrho(\beta) - \varrho(\gamma) &= \int\limits_{\beta}^{\gamma} z^{-1}\varrho(z-1)\,dz \geq (\gamma - \beta)\gamma^{-1}\varrho(\gamma - 1) \\ &\geq (\gamma - \beta)\varrho(\gamma) \quad \text{for } 1 \leq \beta \leq \gamma.\end{aligned} \tag{4.12}$$

Applying this with $\beta = \alpha,\ \gamma = \alpha(w/m)$, and using (4.10), we obtain

$$\varrho(\alpha) \geq mw^{-1}(1 + \delta). \tag{4.13}$$

For the remainder of this proof, we let $h = (g_m - 1)^{\alpha}$, and we assume $h > e$ (if $h \leq e$, there is nothing to prove). We can use Lemma 4.1 and the inequalities (4.11) and (4.13) to get the lower bound

$$\begin{aligned}\Psi_n(h, h^{1/\alpha}) &\geq n^{-1}\phi(n)hmw^{-1}(1+\delta) \\ &\quad + O_{\varepsilon,w}((\log_2 n)^2(h/\log h) + n^{\varepsilon}(h^{2w/(2w+1)} + h^{1-1/\alpha(w)})).\end{aligned} \tag{4.14}$$

Now if E contains $C_k(n)$ and t is any positive integer, we can use (3.25) and the hypothesis $\nu \geq w$ to get an upper bound for $N_s(n, E; 0, h)$ with main term $(wn)^{-1}\phi(n)h$ and the same error term as in (3.25). Adding these estimates for $N_s(n, E; 0, h)$, we get

$$\begin{aligned}&\sum_{s=0}^{m-1} N_s(n, E; 0, h) \\ &\quad \leq m(wn)^{-1}\phi(n)h + O_{\varepsilon,t}(mR_k(n)^{1/t}h^{1-1/t}n^{(t+1)/4t^2+\varepsilon}).\end{aligned} \tag{4.15}$$

Combining (4.5), (4.14), and (4.15), then subtracting $m(wn)^{-1}\phi(n)h$ from both sides and recalling that $m < w$ by hypothesis, we obtain

$$\begin{aligned}m(wn)^{-1}\phi(n)h\delta \ll_{\varepsilon,w,t} &(\log_2 n)^2(h/\log h) \\ &+ n^{\varepsilon}(h^{2w/(2w+1)} + h^{1-1/\alpha(w)}) \\ &+ R_k(n)^{1/t}h^{1-1/t}n^{(t+1)/4t^2+\varepsilon}\end{aligned} \tag{4.16}$$

if E contains $C_k(n)$ and t is any positive integer.

Likewise, if $t = 1, 2, 3$ and we drop the assumption that E contains $C_k(n)$, then (3.24), (4.5), and (4.14) show that (4.16) holds with the factor $R_k(n)^{1/t}$ replaced by 1.

Temporarily assuming that E contains $C_k(n)$, we multiply both sides of (4.16) by $wn(m\phi(n)h)^{-1}$ and apply the estimate $n/\phi(n) \ll \log_2 n$. This gives

$$\begin{aligned}(4.17)\qquad \delta &\ll_{\varepsilon,w,t} (\log_2 n)^3(\log h)^{-1} + n^{\varepsilon}(h^{-1/(2w+1)} + h^{-1/\alpha(w)})\\ &\quad + R_k(n)^{1/t}h^{-1/t}n^{(t+1)/4t^2+\varepsilon}\end{aligned}$$

for any positive integer t. Take $t = [1/\delta] + 1$, so

$$(4.18)\qquad 1/\delta < t < 3/2\delta,$$

and choose

$$\varepsilon = \min\left\{\frac{1}{8(2w+1)}, \frac{1}{8\alpha(w)}, \frac{\delta^2}{24}\right\}.$$

If $h > R_k(n)n^{1/4+\delta/2}$ and $n > A_1(w,\delta)$ (sufficiently large), we get a contradiction from (4.17) and (4.18). Hence either $n \le A_1(w,\delta)$ (in which case (4.4) is trivial) or $h \le R_k(n)n^{1/4+\delta/2}$ and we have

$$(4.19)\qquad g_m - 1 = h^{1/\alpha} \le R_k(n)^{1/\alpha}n^{(1/4+\delta/2)/\alpha}.$$

Since $\alpha > 1$ by (4.11), it follows from (4.9) and (4.10) that

$$\frac{1}{\alpha} = \frac{\alpha+\delta}{\alpha(w/m)\alpha} < \frac{1}{\alpha(w/m)} + \delta,$$

so

$$(1/4 + \delta/2)/\alpha < 1/4\alpha(w/m) + \delta$$

and (4.4) follows from (4.19).

The proof of (4.3) is similar: as we remarked above, if we drop the assumption that E contains $C_k(n)$, then (4.16) holds if $t = 3$ and $R_k(n)^{1/t}$ is replaced by 1. Keeping $t = 3$ and taking

$$\varepsilon = \min\left\{\frac{1}{6(2w+1)}, \frac{1}{6\alpha(w)}, \frac{\delta}{12}\right\},$$

we get a contradiction as before if $h > n^{1/3+\delta/2}$ and $n > A_2(w,\delta)$ (sufficiently large), and (4.3) follows. ■

LEMMA 4.20. *Write $g_s(n;E) = g_s$ for each s. Let m be any integer with $1 \le m \le \nu(n;E) - 1$. If $g_{m-1}^2 < g_m$, then $\{g_sE : 0 \le s \le m-1\}$ is a subgroup of $C(n)/E$.*

Proof. If t, u are integers with $0 \le t \le u \le m-1$, then $g_tg_u \le g_{m-1}^2$, so $(g_tE)(g_uE) = (g_tg_u)E$ is in the set $\{g_sE : 0 \le s \le m-1\}$. Hence the latter set is closed under multiplication. ■

From Lemma 4.2, we can derive the following more satisfactory result:

THEOREM 4.21. *Let m, w be any integers with $1 \le m < w$, and let E be any subgroup of $C(n)$ with $\nu = \nu(n; E) \ge w$. Write $g_s(n; E) = g_s$, and suppose that $\{g_s E : 0 \le s \le m-1\}$ is a subgroup of $C(n)/E$. Then*

$$g_m \ll_{w,\delta} n^{1/4\alpha(w/m)+\delta} \quad \textit{for each } \delta > 0. \tag{4.22}$$

Proof. Keeping m, w fixed, we first prove (4.22) when ν is sufficiently large. Since $\alpha(u) \to +\infty$ as $u \to +\infty$, we can choose $y = y(w)$ to be the smallest positive integer such that $\alpha(y) \ge (4/3)\alpha(w)$. Let $x = wy$, and observe that $\alpha(x/m) > \alpha(y) \ge (4/3)\alpha(w/m)$. Thus if $\nu \ge x$, it follows from (4.3) that

$$g_m \ll_{x,\delta} n^{1/3\alpha(x/m)+\delta} \ll_{w,\delta} n^{1/4\alpha(w/m)+\delta}$$

for each $\delta > 0$.

Now suppose that $\nu < x$. By (3.26), E contains $C_\nu(n)$, so (4.4) holds with $k = \nu$. By (1.8) and (1.10), $R_\nu(n) \le \nu^{9/8} < x^{9/8}$, and (4.22) follows. ∎

Only in the case $m = 1$ of Theorem 4.21 do we know without further hypotheses that $\{g_s E : 0 \le s \le m-1\}$ is a subgroup of $C(n)/E$. However, this is clearly enough to establish Theorem 1.20 (note that (1.22) and (1.23) then follow from (4.8)). We can also use Theorem 4.21 to prove the following more general result:

THEOREM 4.23. *Let m, w be any integers with $1 \le m < w$. Let E be any subgroup of $C(n)$ with $\nu(n; E) \ge w$. Then for each $\delta > 0$, we have*

$$g_m = g_m(n; E) \ll_{w,\delta} n^{2^{m-3}/\alpha(w)+\delta}. \tag{4.24}$$

Proof. Fix $\delta > 0$. By Theorem 4.21, there is a constant $c(w, \delta) \ge 1$ such that if $\{g_s E : 0 \le s \le m-1\}$ is a subgroup of $C(n)/E$, then

$$g_m \le c(w, \delta) n^{1/4\alpha(w/m)+\delta/2^w}. \tag{4.25}$$

In particular, (4.25) certainly holds for $m = 1$:

$$g_1 \le c(w, \delta) n^{1/4\alpha(w)+\delta/2^w} = F, \tag{4.26}$$

say. We shall now prove by induction on m (without assuming that $\{g_s E : 0 \le s \le m-1\}$ is a subgroup of $C(n)/E$) that

$$g_m \le F^{2^{m-1}} \tag{4.27}$$

for $1 \le m < w$. From this, (4.24) follows immediately.

If $m = 1$, (4.27) is the same as (4.26). Suppose that $2 \le m < w$ and that (4.27) holds with m replaced by $m - 1$. If $g_m \le g_{m-1}^2$, then we get (4.27) immediately. On the other hand, if $g_{m-1}^2 < g_m$, then $\{g_s E : 0 \le s \le m-1\}$

is a subgroup of $C(n)/E$ by Lemma 4.20, so (4.25) holds. To derive (4.27), take $\beta=\alpha(w/m)$ and $\gamma=\alpha(w)$ in (4.12) and simplify to get

$$\begin{aligned}\alpha(w)/\alpha(w/m)&\le m/\alpha(w/m)+1-1/\alpha(w/m)\\&\le m/\alpha(w/m)+m\{1-1/\alpha(w/m)\}=m\le 2^{m-1}.\ \blacksquare\end{aligned}$$

Proof of Theorem 1.24. As we remarked after (1.19), $\alpha(w)\to+\infty$ as $w\to+\infty$. Let $w=w(m)$ be the least integer such that $w>m$ and $2^{m-3}/\alpha(w)\le 1/4$. If $\nu=\nu(n;E)\ge w$, then the result follows from Theorem 4.23. Now suppose that $m<\nu<w$. By (3.26), E contains $C_\nu(n)$, and we can apply (3.40) and (1.8) to get

$$g_m(n;E)\ll_{m,\varepsilon}\nu^{9/8}n^{1/4+\varepsilon}\ll_{m,\varepsilon}n^{1/4+\varepsilon}.\ \blacksquare$$

Because the function $\alpha(w)$ plays an important role in our results, we summarize here some facts about this function of the real variable $w\ge 1$. As we mentioned after the definition (1.19), $\alpha(w)$ is strictly increasing. Using an asymptotic formula for $\log\varrho(\alpha)$ due to de Bruijn [5], (1.8) (see also [31], (3.24) or [21], Corollary 2.3), one can show that

$$(4.28)\qquad \alpha(w)=\frac{\log w}{\log_2 w}\left\{1+\frac{1}{\log_2 w}+o\left(\frac{1}{\log_2 w}\right)\right\}\quad\text{as } w\to+\infty.$$

Also, Buchštab [6] established a specific lower bound for $\varrho(\alpha)$ and used it to obtain the inequality

$$(4.29)\qquad \alpha(w)>(\log w)(\log_2 w+2)^{-1}>6\quad\text{for } w>e^{33}.$$

(See [31], pp. 11, 74 for remarks about a small correction of Buchštab's work needed to establish (4.29).)

By (4.8),

$$(4.30)\qquad \alpha(2)=e^{1/2}=1.64872\ldots,\qquad \alpha(3)=e^{2/3}=1.94773\ldots$$

It is harder to calculate $\alpha(w)$ when $w\ge 4$. Slightly refining a result of Davenport and Erdős [13], p. 256, Chamayou [12], p. 203, obtained

$$(4.31)\qquad \alpha(4)=2.12459\ldots,\qquad \alpha(5)=2.25710\ldots$$

Using Table 1 of Bellman and Kotkin [4] (see van de Lune and Wattel [27] for comments and corrections) and interpolating by use of the mean-value theorem for derivatives, one can do further computations of $\alpha(w)$. For example, we get these approximate values (correct to two decimal places):

$$(4.32)\qquad \alpha(6)=2.36,\qquad \alpha(7)=2.45,\qquad \alpha(8)=2.52.$$

We remarked above that for fixed $m\ge 2$, Theorem 1.24 gives our best universal upper bound for $g_m(n;E)$. Even in the case $m=2$, the application of Theorem 4.23 and (4.30) gives essentially nothing better than the inequality $g_2(n;E)\ll n^{0.257}$ when $\nu(n;E)=3$. However, Theorem 4.23 gives a better estimate for $g_2(n;E)$ than Theorem 1.24 if $\nu(n;E)\ge 4$. In any case, (4.28) shows that (4.24) is crude (even worse than trivial) unless m is very small compared to w.

5. Estimates for the Kolesnik–Straus numbers $g_m(\chi)$. Throughout this section, n and k are any positive integers as usual, and we assume

$$\chi \textit{ is a character mod } n \textit{ with } \operatorname{ord}\chi = k. \tag{5.1}$$

Recall that the numbers $g_m(\chi)$ $(0 \le m \le k-1)$ were defined just before Theorem 1.30.

LEMMA 5.2. *Assume* (5.1), *and let F be the subgroup of $C(n)$ defined by*

$$F = \{y \in C(n) : \chi(y) = 1\}. \tag{5.3}$$

Then

$$\nu(n; F) = k \tag{5.4}$$

and

$$g_m(\chi) = g_m(n; F) \quad \textit{for } 0 \le m \le k-1. \tag{5.5}$$

Proof. Observe that if y, z are members of $C(n)$, then

$$yF = zF \quad \text{if and only if} \quad \chi(y) = \chi(z). \tag{5.6}$$

It follows that the mapping $yF \mapsto \chi(y)$ is a well-defined one-to-one mapping of the quotient group $C(n)/F$ into the multiplicative group W_k of kth roots of unity, so $\nu(n; F) \le k$. On the other hand, the distinct characters $\chi, \chi^2, \ldots, \chi^k$ are all members of F' (see (3.7)), so by (3.14), $\nu(n; F) \ge k$. Thus (5.4) follows. (Alternatively, it is straightforward to show directly that the image of the homomorphism $\chi|C(n)$ is exactly W_k, so $C(n)/F$ is isomorphic to W_k by the first isomorphism theorem of group theory, and (5.4) follows.)

Using (5.6) and the definitions of $g_m(\chi)$ and $g_m(n; F)$, one can now prove (5.5) easily by strong induction on m. ■

Theorem 1.30 follows immediately from Lemma 5.2 and Theorem 1.20. Likewise, Lemma 5.2 and Theorem 1.24 yield

$$g_m(\chi) \ll_{m,\varepsilon} n^{1/4+\varepsilon} \quad \text{if (5.1) holds and } 0 \le m \le k-1. \tag{5.7}$$

Kolesnik and Straus [25], (4.7), obtained (5.7) in the special case when n is cubefree and $m = k-1$. (Note, however, that their result gives no information when k is large, whereas (5.7) is significant for bounded m regardless of the size of k.) They also used an elaborate and very ingenious method to show ([25], Theorem 4.13) that if (5.1) holds, then

$$g_m(\chi) \ll_{k,\varepsilon} n^{m/4\alpha(k)+\varepsilon} \quad \text{for } n \text{ cubefree, } 0 \le m \le k-1. \tag{5.8}$$

Note that the exponent in (5.8) is much smaller than the exponent in (4.24) with $w = k$. However, because of the slow growth of $\alpha(k)$ (see (4.28)), (5.8) is superior to (5.7) only when n is cubefree, k is bounded, and m is rather small compared to k. We shall not attempt to generalize (5.8) to the case of arbitrary n.

Elliott [15], [16] obtained a small improvement of (5.7) when $n = p$ is prime, $m = k - 1$, and (5.1) holds:

$$g_{k-1}(\chi) \ll_{k,\varepsilon} p^{1/4 - ck^{-19} + \varepsilon}, \tag{5.9}$$

where c is a positive absolute constant. As we remarked above, this implies a result of the type (3.42). To see this, let $p \equiv 1 \pmod{k}$. Since $C(p)$ and its character group are both cyclic, the same is true of $C_k(p)$ and $C_k(p)'$ (defined by (3.7)), and we have $|C_k(p)'| = \nu_k(p) = k$ by (3.14) and (3.1). Let χ be a generator of $C_k(p)'$. Then $C_k(p) = \{y \in C(p) : \chi(y) = 1\}$ by (3.9), so $g_m(p; C_k(p)) = g_m(\chi)$ for $0 \le m \le k - 1$ by (5.5), and (5.9) yields a version of (3.42).

A drawback to (5.8) and (5.9) is that they give no information when k is large. Likewise, (5.7) is uninformative when m is large. We can partially remedy these disadvantages by proving Theorem 1.13.

Proof of Theorem 1.13. Define $D = \{y : m < y \le m + h \text{ and } (y, n) = 1\}$, and let $w = \min\{k - 1, [K(n)]\}$. Let q be any integer such that

$$q \mid k \quad \text{and} \quad q > w. \tag{5.10}$$

Define $\theta = \chi^{k/q}$. Then $\operatorname{ord}\theta = q$, and θ assumes, say, s $(\le w)$ distinct values $\theta(y_1), \ldots, \theta(y_s)$ on D. Define $F = \{y \in C(n) : \theta(y) = 1\}$. By (5.4), $\nu(n; F) = q$. By (5.6), if $y \in D$, then $y \in y_j F$ for some j $(1 \le j \le s)$. Hence D is contained in the union of w distinct cosets of F in $C(n)$. Clearly F contains $C_q(n)$, so by (5.10) and (3.29),

$$h \ll_{\varepsilon,t} \{qw(q - w)^{-1}\}^{t/2} R_q(n) n^{(t+1)/4t + \varepsilon/4} \tag{5.11}$$

for every positive integer t. Applying the inequalities (1.8) and $q(q-w)^{-1} \le w + 1$, we get

$$h \ll_{\varepsilon,t} w^t Q(q)^{9/8} n^{(t+1)/4t + \varepsilon/4} \tag{5.12}$$

for every positive integer t, whenever (5.10) holds.

Next, we shall show that

(5.13) *There exists q such that* (5.10) *holds and* $Q(q) \le w^2$.

To see this, write $k = p_1^{a_1} \ldots p_r^{a_r}$, where $p_1 < \ldots < p_r$ are primes and $a_1, \ldots, a_r$ are positive integers. First suppose that $p_j^{a_j} > w$ for some j. Let c be the smallest integer such that $p_j^c > w$, and take $q = p_j^c$. Then (5.10) holds, and if $c = 1$, we have $Q(q) = 1$ by (1.10), while if $c \ge 2$, then (1.10) gives $Q(q) = q$, and we have $q \le wp_j \le w^2$. Now suppose that $p_j^{a_j} \le w$

for each $j = 1, \ldots, r$. Since $k > w$, there exists a smallest positive integer v such that $p_1^{a_1} \ldots p_v^{a_v} > w$. If we take $q = p_1^{a_1} \ldots p_v^{a_v}$, then (5.10) holds, and $Q(q) \le q \le w p_v^{a_v} \le w^2$. Thus (5.13) holds.

By (1.14), $w \ll_{\varepsilon,t} n^{\varepsilon/4t}$ for each positive integer t, and if we combine this inequality with (5.12) and (5.13), we get

$$h \ll_{\varepsilon,t} n^{\varepsilon/4+(9/4)(\varepsilon/4t)+(t+1)/4t+\varepsilon/4}$$

for $t = 1, 2, \ldots$ Choosing $t = \max\{3, [1/\varepsilon] + 1\}$, we obtain the result. ■

Applying Theorem 1.13 to the set $\{y : 0 < y \le g_m(\chi) - 1 \text{ and } (y, n) = 1\}$, we get

Corollary 5.14. *Assume* (5.1), *and let $K(q)$ be any function on the positive integers which satisfies* (1.14). *If m is any integer such that* $0 \le m \le \min\{k-1, K(n)\}$, *then* $g_m(\chi) \ll_\varepsilon n^{1/4+\varepsilon}$.

Corollary 5.14 generalizes (5.7) and compares favorably with (5.8) and (5.9).

In conclusion, we mention a result which follows from Montgomery [28], Theorem 13.2: if $n > 1$ and (5.1) holds, and if we assume the extended Riemann hypothesis, then $g_{k-1}(\chi) \ll k(\log n)^2$.

References

[1] N. C. Ankeny, *The least quadratic nonresidue*, Ann. of Math. 55 (1952), 65–72.

[2] E. Bach, *Explicit bounds for primality testing and related problems*, Math. Comp. 55 (1990), 355–380.

[3] E. Bach and L. Huelsbergen, *Statistical evidence for small generating sets*, ibid. 61 (1993), 69–82.

[4] R. Bellman and B. Kotkin, *On the numerical solution of a differential-difference equation arising in analytic number theory*, ibid. 16 (1962), 473–475.

[5] N. G. de Bruijn, *The asymptotic behaviour of a function occurring in the theory of primes*, J. Indian Math. Soc. (N.S.) 15 (1951), 25–32.

[6] A. A. Buchštab [A. A. Bukhshtab], *On those numbers in an arithmetic progression all prime factors of which are small in order of magnitude*, Dokl. Akad. Nauk SSSR (N.S.) 67 (1949), 5–8 (in Russian).

[7] D. A. Burgess, *On character sums and L-series*, Proc. London Math. Soc. (3) 12 (1962), 193–206.

[8] —, *On character sums and L-series. II*, ibid. 13 (1963), 524–536.

[9] —, *A note on the distribution of residues and non-residues*, J. London Math. Soc. 38 (1963), 253–256.

[10] —, *The character sum estimate with* $r = 3$, ibid. (2) 33 (1986), 219–226.

[11] R. J. Burthe, Jr., *Upper bounds for least witnesses and generating sets*, Acta Arith. 80 (1997), 311–326.

[12] J.-M.-F. Chamayou, *A probabilistic approach to a differential-difference equation arising in analytic number theory*, Math. Comp. 27 (1973), 197–203.

[13] H. Davenport and P. Erdős, *The distribution of quadratic and higher residues*, Publ. Math. Debrecen 2 (1952), 252–265.

[14] P. D. T. A. Elliott, *Some notes on kth power residues*, Acta Arith. 14 (1968), 153–162.

[15] —, *Extrapolating the mean-values of multiplicative functions*, Nederl. Akad. Wetensch. Proc. Ser. A 92 (1989), 409–420.

[16] —, *Some remarks about multiplicative functions of modulus* ≤ 1, in: Analytic Number Theory (Allerton Park, Ill., 1989), Progr. Math. 85, Birkhäuser Boston, Boston, Mass., 1990, 159–164.

[17] E. Fouvry et G. Tenenbaum, *Entiers sans grand facteur premier en progressions arithmétiques*, Proc. London Math. Soc. (3) 63 (1991), 449–494.

[18] S. W. Graham and C. J. Ringrose, *Lower bounds for least quadratic nonresidues*, in: Analytic Number Theory (Allerton Park, Ill., 1989), Progr. Math. 85, Birkhäuser Boston, Boston, Mass., 1990, 269–309.

[19] H. Hasse, *Vorlesungen über Zahlentheorie*, 2nd ed., Springer, Berlin, 1964.

[20] D. G. Hazlewood, *Sums over positive integers with few prime factors*, J. Number Theory 7 (1975), 189–207.

[21] A. Hildebrand and G. Tenenbaum, *Integers without large prime factors*, J. Théor. Nombres Bordeaux 5 (1993), 411–484.

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

[23] —, *The distribution of kth power residues and non-residues*, Proc. Amer. Math. Soc. 19 (1968), 678–680.

[24] —, *The distribution of kth power non-residues*, Duke Math. J. 37 (1970), 333–340.

[25] G. Kolesnik and E. G. Straus, *On the first occurrence of values of a character*, Trans. Amer. Math. Soc. 246 (1978), 385–394.

[26] B. V. Levin and A. S. Faĭnleĭb, *Application of some integral equations to problems of number theory*, Uspekhi Mat. Nauk 22 (1967), no. 3, 119–197 (in Russian); English transl.: Russian Math. Surveys 22 (1967), no. 3, 119–204.

[27] J. van de Lune and E. Wattel, *On the numerical solution of a differential-difference equation arising in analytic number theory*, Math. Comp. 23 (1969), 417–421.

[28] H. L. Montgomery, *Topics in Multiplicative Number Theory*, Lecture Notes in Math. 227, Springer, Berlin, 1971.

[29] K. K. Norton, *Upper bounds for kth power coset representatives modulo n*, Acta Arith. 15 (1969), 161–179.

[30] —, *On the distribution of kth power residues and non-residues modulo n*, J. Number Theory 1 (1969), 398–418.

[31] —, *Numbers with small prime factors, and the least kth power non-residue*, Mem. Amer. Math. Soc. 106 (1971).

[32] —, *On the distribution of power residues and non-residues*, J. Reine Angew. Math. 254 (1972), 188–203.

[33] —, *On character sums and power residues*, Trans. Amer. Math. Soc. 167 (1972), 203–226.

[34] —, *Bounds for sequences of consecutive power residues. I*, in: Analytic Number Theory, Proc. Sympos. Pure Math. 24, Amer. Math. Soc., Providence, R.I., 1973, 213–220.

[35] F. Pappalardi, *On minimal sets of generators for primitive roots*, Canad. Math. Bull. 38 (1995), 465–468.

[36] G. Tenenbaum, *Cribler les entiers sans grand facteur premier*, Philos. Trans. Roy. Soc. London Ser. A 345 (1993), 377–384.

[37] T. Z. Xuan, *Integers with no large prime factors*, Acta Arith. 69 (1995), 303–327.

94 Thornton Road
Bangor, Maine 04401-3336
U.S.A.

Received on 10.6.1997 (3200)