TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 167, May 1972

ON CHARACTER SUMS AND POWER RESIDUES

BY
KARL K. NORTON[1]

Abstract. Sharp estimates are given for a double sum involving Dirichlet characters. These are applied to the problem of estimating certain sums whose values give a measure of the average distance between successive power residues to an arbitrary modulus. A particularly good result of the latter type is obtained when the modulus is prime.

1. **Introduction.** Let n, h, w represent positive integers (throughout this section). Let χ be a Dirichlet (residue) character mod n, and define

$$S_w(n, h, \chi) = \sum_{x=1}^{n} \left| \sum_{l=1}^{h} \chi(x+l) \right|^{2w}. \tag{1.1}$$

For convenience, write $S_1(n, h, \chi) = S(n, h, \chi)$. In this paper, we obtain sharp upper bounds for $S(n, h, \chi)$ and apply the results to some problems on the differences of consecutive power residues mod n.

In a series of important papers, Burgess estimated the sums $S_w(n, h, \chi)$ for primitive characters χ and showed how to use the results to get inequalities for sums of the form

$$\sum_{l=1}^{h} \chi(x+l) \tag{1.2}$$

when χ is nonprincipal mod n. In [1] he carried out this process for the case in which $n=p$ is prime (and χ is nonprincipal mod p), obtaining

$$S_w(p, h, \chi) < (4w)^{w+1} p h^w + 2w p^{1/2} h^{2w} \tag{1.3}$$

and a bound for (1.2) which does not concern us here (the latter result was improved in [3]). In [2, Lemma 8] and [3, Lemma 8] Burgess generalized (1.3) by showing that if χ is primitive mod n, and if either $w=2$ or n is cubefree, then

$$S_w(n, h, \chi) = O_{w,\varepsilon}(n h^w + n^{1/2+\varepsilon} h^{2w}) \tag{1.4}$$

for each real $\varepsilon > 0$. (Throughout this paper, the notation $O_{\delta,\varepsilon,\ldots}$ indicates an

Received by the editors July 29, 1971.

AMS 1970 *subject classifications*. Primary 10G05, 10H35.

Key words and phrases. Dirichlet character, residue character, character sum, power residue.

(1) Part of this research was performed while the author was an ONR Postdoctoral Research Associate at the University of Michigan. Support was also received from the grant AF-AFOSR-69-1712.

implied constant depending at most on $\delta, \varepsilon, \ldots$, while O implies an absolute constant.) In [3, Theorem 2] he gave a corresponding estimate for the sum (1.2); here it was sufficient for χ to be nonprincipal mod n.

The inequalities (1.3) and (1.4) are powerful, and their proofs are deep. In the case $w=1$, better results can be obtained by much simpler methods. It has been known for some time that if χ is nonprincipal mod p (p prime), then

$$S(p, h, \chi) = ph - h^2 \quad \text{for } 1 \leqq h \leqq p, \tag{1.5}$$

and it follows from the periodicity of χ that

$$S(p, h, \chi) < ph \quad \text{for } h \geqq 1. \tag{1.6}$$

Easy proofs of (1.5) can be found in Vinogradov [20, pp. 125, 206–207] and in Davenport and Erdös [5, Lemma 1] (there is also a preliminary version of (1.3) in [5, Lemma 3]). It is natural to ask whether (1.6) still holds if p is replaced by an arbitrary positive integer n. It appears that little was known about this problem until quite recently, when Burgess showed that for each nonprincipal χ mod n and each real $\varepsilon > 0$,

$$S(n, h, \chi) \leqq nh\{d(n) \log n\}^2 = O_\varepsilon(n^{1+\varepsilon}h), \tag{1.7}$$

where $d(n)$ is the number of positive divisors of n. (His elementary proof is given in [17, pp. 410–413].) Our first objective in this paper is to improve (1.7) by showing that

$$S(n, h, \chi) < (9/8)nh \quad (\chi \text{ nonprincipal mod } n). \tag{1.8}$$

(We give a different sort of inequality in Theorem 3.52 which sometimes improves (1.8).) It is clear from (1.5) that the constant 9/8 cannot be replaced by a constant less than 1. Even when n is not prime, (1.8) is almost best possible. For example, we show that if $n \geqq 133$ is odd and χ is primitive mod n, then there are values of h for which $S(n, h, \chi) > (1/4)nh$. We conjecture that (1.8) holds with 1 in place of 9/8, but we can show this only in some special cases (e.g., when χ is primitive).

Our proof of (1.8) is elementary and virtually self-contained. However, it is rather complicated and depends on a method of Hooley [11], who estimated $S(n, h, \chi)$ when χ is principal mod n. (We shall also give a small improvement of Hooley's result; see Theorem 3.32.) In the important special case of primitive χ mod n ($n > 1$), Professor Patrick Gallagher has given a very simple and elegant proof that $S(n, h, \chi) < nh$. With his permission, we include this proof in §2.

In order to discuss the applications of these results on $S(n, h, \chi)$ to another problem, we must introduce some further notation. For positive integers n and k, let $C(n)$ denote the multiplicative group of residue classes (mod n) which are relatively prime to n, and let $C_k(n)$ denote the subgroup of kth powers. Write $\nu = \nu_k(n) = [C(n) : C_k(n)]$, and let $1 = g_0 < g_1 < \cdots < g_{\nu-1}$ be the smallest positive representatives of the ν cosets of $C_k(n)$, so $g_j = g_j(n, k)$. Let $\alpha = \alpha_k(n)$ be the cardinality of a coset $g_s C_k(n)$ (thus $\alpha = \varphi(n)/\nu$, where φ is Euler's function), and let

$h_0, h_1, \ldots, h_\alpha$ be the $\alpha+1$ smallest positive integers in this coset arranged in increasing order, so $h_j = h_j(n, k, s)$ and (if $n > 1$), $1 \leqq g_s = h_0 < h_1 < \cdots < h_{\alpha-1} < n < h_\alpha = n + h_0$. The values of the sum

$$\mathfrak{S}(n, \beta, k, s) = \sum_{j=1}^{\alpha} (h_j - h_{j-1})^\beta \qquad (\beta \text{ real}, \beta \geqq 1) \tag{1.9}$$

can be considered to measure the average size of the differences $h_j - h_{j-1}$. Since

$$\mathfrak{S}(n, 1, k, s) = n, \tag{1.10}$$

a simple application of Hölder's inequality (see [17, Theorem 3.32]) yields

$$\mathfrak{S}(n, \beta, k, s) \geqq n(n/\alpha)^{\beta-1} = \nu^{\beta-1} n\{n/\varphi(n)\}^{\beta-1} \qquad (\beta \geqq 1), \tag{1.11}$$

and this inequality will be fairly sharp if all of the numbers $h_j - h_{j-1}$ have approximately the same size.

We are interested in obtaining good upper bounds for $\mathfrak{S}(n, \beta, k, s)$; the significance of these will be easier to understand if we first state two facts about $\nu = \nu_k(n)$. An explicit formula for $\nu_k(n)$ was given in [16, Lemma 4.3]; from this it follows that

$$\nu = \nu_k(n) = O_{k,\varepsilon}(n^\varepsilon) \quad \text{for each } \varepsilon > 0. \tag{1.12}$$

On the other hand, it was shown in [17, Theorem 3.27] that for each $k \geqq 2$, there are infinitely many n such that

$$\nu_k(n) \geqq \exp\left\{\frac{(\log k)\log n}{\log\log n} + O_k\left(\frac{\log n}{(\log\log n)^2}\right)\right\}.$$

In [17] and [18] we obtained several upper estimates for $\mathfrak{S}(n, \beta, k, s)$. For example, we showed in [18, Theorem 5.7] that

$$\mathfrak{S}(n, \beta, k, s) = O_{\beta,\varepsilon}(\nu^{6\beta-6} n^{1+\varepsilon}) \tag{1.13}$$

for $0 \leqq s \leqq \nu - 1$, $\varepsilon > 0$, and $1 \leqq \beta \leqq 7/3$, while a weaker estimate was given for $\beta > 7/3$. Comparison with (1.12) and (1.11) shows that (1.13) is rather sharp, but it has a somewhat unsatisfactory vagueness, since it gives hardly any more information than the result

$$\mathfrak{S}(n, \beta, k, s) = O_{k,\beta,\varepsilon}(n^{1+\varepsilon}) \qquad (1 \leqq \beta \leqq 7/3), \tag{1.14}$$

which follows from (1.13) and (1.12). Our new results on $S(n, h, \chi)$ enable us to improve such inequalities in the range $1 \leqq \beta \leqq 2$. We can now show that

$$\mathfrak{S}(n, \beta, k, s) = O_\beta(\nu^{2\beta-2} n\{n/\varphi(n)\}^{2\beta-2}) \quad \text{for } 1 \leqq \beta < 2, 0 \leqq s \leqq \nu - 1, \tag{1.15}$$

and we can also get results of the type

$$\nu^2 n\{n/\varphi(n)\} \leqq \sum_{s=0}^{\nu-1} \mathfrak{S}(n, 2, k, s) = O(\nu^2 n\{n/\varphi(n)\} \log n) \tag{1.16}$$

for $n \geqq 2$.

The upper bound in (1.16) can be improved when $k=\nu=1$. In this case $\alpha=\varphi(n)$ and the numbers $h_0, \ldots, h_\alpha$ are the $\varphi(n)+1$ smallest positive integers relatively prime to n. The method which we use to obtain (1.16) also gives the result

$$(1.17) \qquad \mathfrak{S}(n, 2, 1, 0) = O\left(\frac{n^2}{\varphi(n)}\left\{1+\sum_{p\mid n} p^{-1}\log p\right\}\right) = O\left(\frac{n^2}{\varphi(n)}\log\log n\right)$$

for $n\geqq 3$, the sum in the middle running over the distinct prime factors of n. (1.17) was apparently first discovered by H. N. Shapiro and M. Hausman (their paper will probably appear in Comm. Pure Appl. Math.); it was rediscovered independently by R. C. Vaughan (unpublished) and (somewhat later) by the present author. For a brief discussion of its connections with a conjecture of Erdös and some work of Hooley, see the remarks after Theorem 4.22.

Our final result concerns $\mathfrak{S}(p, \beta, k, s)$, where p is prime. In this case, $\nu=\nu_k(p) =(k, p-1)$, and we showed in [17, Theorem 6.8] that

$$(1.18) \qquad \mathfrak{S}(p, \beta, k, s) = O_\beta(\nu^{2\beta-2}p) \quad \text{for } 1 \leqq \beta < 2, 0 \leqq s \leqq \nu-1,$$

with a somewhat weaker result for $\beta\geqq 2$ (see also [18, Theorem 5.15]). There is a gap between (1.11) and (1.18) involving a factor of $\nu^{\beta-1}$ (and, of course, a factor depending only on β). Since $\nu_k(p)\leqq k$, the lower and upper bounds here are virtually indistinguishable if k is bounded (and $1\leqq\beta<2$), but we can improve (1.18) in a way which is significant when k and ν are large. In §5, we show that if $0\leqq s\leqq\nu-1$, then

$$(1.19) \qquad \mathfrak{S}(p, \beta, k, s) = O_\beta(\nu^{\beta-1}p) \quad \text{for } 1 \leqq \beta < 2, p > (k\log k)^{16}.$$

This is best possible except for the constant factor and the restriction on p. The proof uses an idea of Gallagher given in §2, as well as one of Burgess's deep inequalities for character sums of the type (1.2) ([3, Theorem 1]; cf. also [4]). (Incidentally, this is the only point in the paper where we use a nonelementary method or result.) (1.11) and (1.19) suggest the possibility of an asymptotic formula of the following type (for $1\leqq\beta<2$, $0\leqq s\leqq\nu-1$):

$$\mathfrak{S}(p, \beta, k, s) \sim f(\beta, k, s)\nu^{\beta-1}p \quad \text{as } p\to+\infty.$$

Our methods do not seem strong enough to derive such a result.

A few remarks are in order concerning notation. The following symbols always represent integers: $d, h, k, l, m, n, q, s, w$. The letter p is reserved for prime numbers. When $n\geqq 2$ and we have occasion to refer to the prime factorization of n, we always write $n=p_1^{a_1}\cdots p_r^{a_r}$, where each $a_j\geqq 1$ and the primes $p_1, \ldots, p_r$ are distinct (but not necessarily listed in increasing order). φ denotes Euler's function, μ is the Möbius function, and $\omega(m)$ is the number of distinct prime factors of m. χ always denotes a Dirichlet character, χ_0 being the principal character to the modulus in question. An empty sum means 0, an empty product 1, and $[\beta]$ is the largest integer $\leqq\beta$. Other notation will be introduced as needed.

I wish to thank Professor Gallagher for his kind permission to include in §2 of this paper his method of estimating $S(n, h, \chi)$ when χ is primitive.

2. Gallagher's method.

(2.1) LEMMA. *Write* $e(t)=e^{2\pi it}$. *If* χ *is primitive* mod n, *then*

$$\sum_{x=1}^{n} \chi(x+l)\bar{\chi}(x+m) = \sum_{1 \leqq z \leqq n,(z,n)=1}^{n} e(z(l-m)/n). \tag{2.2}$$

Proof. Define

$$\tau(n, \chi) = \sum_{y=1}^{n} \chi(y)e(y/n). \tag{2.3}$$

Since χ is primitive, we have

$$|\tau(n, \chi)| = n^{1/2} \tag{2.4}$$

and

$$\sum_{y=1}^{n} \bar{\chi}(y)e(my/n) = \chi(m)\tau(n, \bar{\chi}) \tag{2.5}$$

for all m (see [14, Vol. I, pp. 483–486, 492–494]). By an obvious change of variable, the left-hand sum in (2.2) is

$$\sum_{y=1}^{n} \chi(y+l-m)\bar{\chi}(y) = \sum,$$

say. Now, (2.5) yields an expression for $\chi(y+l-m)$. Substituting this and inverting the order of summation, we get

$$\sum = \sum_{z=1}^{n} \bar{\chi}(z)e(z(l-m)/n)\left\{\frac{1}{\tau(n, \bar{\chi})} \sum_{y=1}^{n} \bar{\chi}(y)e(zy/n)\right\}.$$

By (2.5), the expression in braces is $\chi(z)$, and we get the right-hand side of (2.2). Q.E.D.

Our next result generalizes (1.5).

(2.6) THEOREM. *Suppose that* $n>1$, χ *is primitive* mod n, *and* $1 \leqq h \leqq n$. *Then*

$$S(n, h, \chi) = nh-h^2- \sum_{1<z<n,(z,n)>1} \frac{\sin^2(\pi zh/n)}{\sin^2(\pi z/n)}. \tag{2.7}$$

Proof. Taking $w=1$ in (1.1) and using Lemma 2.1, we get

$$\begin{aligned} S(n, h, \chi) &= \sum_{l,m=1}^{h} \sum_{x=1}^{n} \chi(x+l)\bar{\chi}(x+m) \\ &= \sum_{l,m=1}^{h} \sum_{z=1}^{n} e(z(l-m)/n) - \sum_{1 \leqq z \leqq n,(z,n)>1}^{n} \left| \sum_{l=1}^{h} e(zl/n) \right|^2 \\ &= nh-h^2- \sum_{1<z<n,(z,n)>1} \left| \sum_{l=1}^{h} e(zl/n) \right|^2. \end{aligned}$$

Q.E.D.

In particular, if $n>1$ and χ is primitive mod n, then

$$S(n, h, \chi) < nh \quad \text{for } h \geqq 1. \tag{2.8}$$

It was remarked by Gallagher that (2.8) can be used to obtain an inequality for $S(n, h, \chi)$ when χ is merely assumed to be nonprincipal mod n. Let K be the conductor of χ, let X be the primitive character mod K induced by χ, and let N be the product of the distinct primes dividing n but not K. By [18, (4.12)],

$$S(n, h, \chi) \leqq 2^{\omega(N)} nK^{-1} \sum_{c|N} c^{-1} \sum_{z=0}^{c-1} S(K, [(z+h)/c], X).$$

Applying (2.8) and using the elementary identity $\sum_{z=0}^{c-1} [(z+h)/c]=h$, we get

$$S(n, h, \chi) < nh2^{\omega(n)-\omega(K)} \prod_{p|n, p\nmid K} (1+p^{-1}). \tag{2.9}$$

This is a definite improvement on Burgess's inequality (1.7) but is still not as good as (1.8). A proof of (1.8) seems to require more complicated methods; these will be discussed in the next section.

3. **Estimation of $S(n, h, \chi)$ (χ arbitrary).** Unless stated otherwise, the results of this section apply to any character mod n (even the principal character). Our main objectives are Theorem 3.32 and Theorem 3.52.

(3.1) LEMMA. *Let $n\geqq 2$, $h\geqq 1$, and let χ be a character* mod n. *Write $n=p_1^{a_1}\cdots p_r^{a_r}$ and $\chi=\chi_1\cdots\chi_r$, where χ_j is a (uniquely determined) character* mod $p_j^{a_j}$ *for each j. Then $S(n, h, \chi)=\varphi(n)h+V(n, h)$, where*

$$V(n, h) = \sum_{l,m=1;l\neq m}^{h} \prod_{j=1}^{r} \sum_{x=1}^{p_j^{a_j}} \chi_j(x+l)\bar{\chi}_j(x+m).$$

Proof. We have

$$S(n, h, \chi) = \sum_{l=1}^{h} \sum_{x=1}^{n} |\chi(x+l)|^2 + \sum_{l,m=1;l\neq m}^{h} \sum_{x=1}^{n} \chi(x+l)\bar{\chi}(x+m).$$

The first double sum on the right equals $\varphi(n)h$. If $n=2$, the second double sum is clearly the same as $V(n, h)$, while if $n\geqq 3$, it can be written in the form

$$\sum_{l,m=1;l\neq m}^{h} \sum_{x=1}^{n} \chi((x+l)(x+m)^{\varphi(n)-1}).$$

The inner sum here can be factored as in the proof of [2, Lemma 7], and the result follows. Q.E.D.

For any integers n, m with n positive, we define Ramanujan's sum $c(n, m)$ as follows:

$$c(n, m) = \sum_{1\leqq k\leqq n,(k,n)=1}^{n} \exp(2\pi ikm/n).$$

(The usual notation is $c_n(m)$, but this would be typographically awkward below.)

We need two facts about $c(n, m)$:

(3.2) LEMMA. *We have*

$$c(nn', m) = c(n, m)c(n', m) \quad \text{if } (n, n') = 1, \tag{3.3}$$

$$c(n, m) = \frac{\mu(n/(n, m))\varphi(n)}{\varphi(n/(n, m))}. \tag{3.4}$$

Proof. See [10, Theorems 67, 272]. (The identity (3.4) is due to Hölder.)

(3.5) LEMMA. *Let χ be a character* mod p^a *with conductor p^b (where $a \geqq 1$, $0 \leqq b \leqq a$). Write*

$$\begin{aligned} \delta(p, q) &= 1-p^{-1} \quad \text{if } p|q, \\ &= 1-2p^{-1} \quad \text{if } p\nmid q, \end{aligned} \tag{3.6}$$

and let

$$Q = \sum_{x=1}^{p^a} \chi(x+l)\bar{\chi}(x+m).$$

If χ is nonprincipal, then

$$Q = p^{a-b}c(p^b, l-m). \tag{3.7}$$

If χ is principal, then

$$Q = p^{a-b}c(p^b, l-m)\delta(p, l-m). \tag{3.8}$$

Proof. If χ is nonprincipal, then χ can be regarded as a primitive character mod p^b and, by periodicity,

$$Q = p^{a-b} \sum_{x=1}^{p^b} \chi(x+l)\bar{\chi}(x+m).$$

(3.7) thus follows from (2.2) and the definition of $c(n, m)$. (A different proof of (3.7), due to Burgess, can be obtained easily from (3.4) and [17, Lemma 5.3].)

Now suppose that χ is principal, so $b=0$. Then clearly $p^a - Q$ is just the number of integers x such that $1 \leqq x \leqq p^a$ and $(x+l)(x+m) \equiv 0 \pmod{p}$, and (3.8) follows. Q.E.D.

It is convenient to define an auxiliary function $T(n, h, m)$ by

$$T(n, h, m) = \sum_{1 \leqq q \leqq h/m} (h-mq) \prod_{p|n} \delta(p, q) \tag{3.9}$$

for all positive integers n, h, m.

(3.10) LEMMA. *Let $n \geqq 2$, let χ be a character* mod n *with conductor K, and define*

$$N = N(n, K) = \prod_{p|n, p\nmid K} p. \tag{3.11}$$

If $V(n, h)$ is defined as in Lemma 3.1, *then*

$$V(n, h) = 2n \sum_{w|K} \mu(w) w^{-1} T(N, h, Kw^{-1}). \tag{3.12}$$

Proof. As in Lemma 3.1, write $n = p_1^{a_1} \cdots p_r^{a_r}$ and $\chi = \chi_1 \cdots \chi_r$, where χ_j is a character mod $p_j^{a_j}$. For convenience, let $K' = nK^{-1}$. Let s be the number of j for which χ_j is nonprincipal, so $0 \leqq s \leqq r$. Without loss of generality, we may assume that $\chi_1, \ldots, \chi_s$ are nonprincipal and $\chi_{s+1}, \ldots, \chi_r$ are principal. Let $p_j^{b_j}$ be the conductor of χ_j, so $b_j = 0$ for $j > s$, $K = p_1^{b_1} \cdots p_s^{b_s}$, and $N = p_{s+1} \cdots p_r$. By Lemma 3.5 and (3.3),

$$\prod_{j=1}^{r} \sum_{x=1}^{p_j^{a_j}} \chi_j(x+l)\bar{\chi}_j(x+m) = K' c(K, l-m) \prod_{p|N} \delta(p, l-m).$$

Substituting this result in the formula defining $V(n, h)$ and collecting terms for which $l-m$ has a fixed value, we get $V(n, h) = 2K' \sum_{t=1}^{h} c(K, t) B(t)$, where (temporarily) $B(t) = (h-t) \prod_{p|N} \delta(p, t)$. Collecting terms for which the greatest common divisor (K, t) has a fixed value and noting that $c(K, t) = c(K, (K, t))$ by (3.4), we obtain

$$V(n, h) = 2K' \sum_{d|K} c(K, d) \sum_{1 \leqq m \leqq h/d, (K/d, m) = 1} B(dm). \tag{3.13}$$

The inner sum in (3.13) is

$$\sum_{1 \leqq m \leqq h/d} B(dm) \sum_{v|(K/d), v|m} \mu(v) = \sum_{v|(K/d)} \mu(v) \sum_{1 \leqq q \leqq h/dv} B(dqv).$$

Since $(N, K) = 1$ by (3.11), it follows that if $p|N$ and $dv|K$, then $\delta(p, dqv) = \delta(p, q)$. Using (3.13) and (3.9), then grouping terms for which dv has a fixed value, we get

$$\begin{aligned} V(n, h) &= 2K' \sum_{d|K} c(K, d) \sum_{v|(K/d)} \mu(v) T(N, h, dv) \\ &= 2K' \sum_{w|K} T(N, h, w) \sum_{v|w} \mu(v) c(K, w/v). \end{aligned} \tag{3.14}$$

To evaluate the inner sum on the right, we use (3.4) and the well-known fact that

$$\text{If } g(m) \text{ is multiplicative, so is } G(m) = \sum_{t|m} g(t). \tag{3.15}$$

For w dividing K, we get

$$\begin{aligned} \sum_{v|w} \mu(v) c(K, w/v) &= \frac{\mu(K/w)\varphi(K)}{\varphi(K/w)} \sum_{v|w, (v, K/w) = 1} \frac{\mu^2(v)}{\varphi(v)} \\ &= \frac{\mu(K/w)\varphi(K)}{\varphi(K/w)} \prod_{p|w, p \nmid (K/w)} \frac{p}{p-1} = \mu(K/w) w. \end{aligned}$$

Substituting this result in (3.14), we obtain (3.12). Q.E.D.

In order to apply Lemma 3.10, we need to estimate the function $T(n, h, m)$ defined by (3.9). Bounds for similar functions were obtained by Erdös [8, p. 170]

(no proof was given) and by Hooley [11]. In the next lemma, we shall refine Hooley's method so as to obtain a certain identity for $T(n, h, m)$.

(3.16) LEMMA. *For each* $n \geqq 1$, *define*

$$n_0 = 1 \quad \text{if } n \text{ is odd}, \qquad = 2 \quad \text{if } n \text{ is even}; \tag{3.17}$$

$$n_1 = \prod_{p|n, p>2} p; \tag{3.18}$$

$$\xi(n) = \prod_{p|n, p>2} \frac{p}{p-2}. \tag{3.19}$$

For each real z, *write*

$$I(z) = \int_0^z ([y]-y+\tfrac{1}{2})\, dy. \tag{3.20}$$

Then for any positive integers n, h, m, *we have*

$$T(n, h, m) = \{\varphi(n)/n\}^2(h^2/2m) - \{\varphi(n)/n\}(h/2) + \{m/\xi(n)\} \sum_{t|n_1} \xi(t) I(h/n_0 mt). \tag{3.21}$$

Proof. It is convenient to introduce the function

$$\theta(n) = \prod_{p|n, p>2} \{1+(p-2)^{-1}\}. \tag{3.22}$$

Observe that the greatest common divisor of n and q has the property $(n, q)_1 = (n_1, q)$ for each q. With $\delta(p, q)$ defined by (3.6), it follows that

$$\prod_{p|n} \delta(p, q) = 0 \quad \text{if } n \text{ is even and } q \text{ is odd}, \qquad = \{n_0\xi(n)\}^{-1}\theta[(n_1, q)] \quad \text{otherwise}. \tag{3.23}$$

A combination of (3.23) and (3.9) yields

$$T(n, h, m) = \{n_0\xi(n)\}^{-1} \sum_{1 \leqq q \leqq h/n_0 m} (h - n_0 mq)\theta[(n_1, q)]. \tag{3.24}$$

Keeping n fixed, we define $F(x) = \sum_{1 \leqq q \leqq x} \theta[(n_1, q)]$ for real $x \geqq 0$. Clearly

$$\sum_{1 \leqq q \leqq h/m} (h - mq)\theta[(n_1, q)] = hF(h/m) - m \int_0^{h/m} x\, dF(x) = m \int_0^{h/m} F(x)\, dx \tag{3.25}$$

for any $m \geqq 1$. Now if n is odd and squarefree, then by (3.15),

$$\theta(n) = \prod_{p|n} \{1 + p^{-1}\xi(p)\} = \sum_{t|n} t^{-1}\xi(t).$$

Therefore,

$$F(x) = \sum_{1 \leqq q \leqq x} \sum_{t|n_1, t|q} t^{-1}\xi(t) = \sum_{t|n_1} t^{-1}\xi(t)[xt^{-1}],$$

so

$$\int_0^{h/m} F(x)\, dx = \sum_{t|n_1} \xi(t) \int_0^{h/mt} [y]\, dy = \sum_{t|n_1} \xi(t)\{(h^2/2m^2t^2) - (h/2mt) + I(h/mt)\}. \tag{3.26}$$

For the reader's convenience, we list here three identities which follow from (3.15) and which hold for each positive n:

$$\{n_0\xi(n)\}^{-1}\sum_{t|n_1} t^{-1}\xi(t) = n^{-1}\varphi(n), \tag{3.27}$$

$$\{n_0^2\xi(n)\}^{-1}\sum_{t|n_1} t^{-2}\xi(t) = n^{-2}\varphi^2(n), \tag{3.28}$$

$$\{\xi(n)\}^{-1}\sum_{t|n_1} \xi(t) = 2^{\omega(n)}n^{-1}\varphi(n). \tag{3.29}$$

We shall use these identities repeatedly.

The identity (3.21) follows from the results (3.24) to (3.28). Q.E.D.

We can now state an identity for $S(n, h, \chi)$.

(3.30) THEOREM. *Let n and h be positive integers. Let χ be a character* mod n *with conductor K, and define $N=N(n, K)$ by* (3.11). *Write*

$$E(\chi) = 1 \quad \text{if } \chi \text{ is principal,}$$
$$= 0 \quad \text{otherwise.}$$

Then (in the notation of Lemma 3.16)

$$S(n, h, \chi) = E(\chi)n^{-1}\varphi^2(n)h^2 + \{2nK/\xi(N)\}\sum_{t|N_1}\xi(t)\sum_{w|K}\mu(w)w^{-2}I(hw/N_0Kt). \tag{3.31}$$

Proof. (3.31) is obvious if $n=1$, since $S(1, h, \chi)=h^2$ and $I(h)=0$. If $n>1$, we combine (3.21) and (3.12), noting the identities

$$\sum_{w|K}\mu(w) = E(\chi), \qquad (NK)^{-1}\varphi(N)\varphi(K) = n^{-1}\varphi(n).$$

The result then follows from Lemma 3.1. Q.E.D.

Thus $S(n, h, \chi)$ depends only on n, h, and the conductor of χ.

(3.32) THEOREM. *Let n, h be positive integers, and let χ be a character* mod n. *If χ is principal, then*

$$0 \leqq S(n, h, \chi) - n^{-1}\varphi^2(n)h^2 \leqq \varphi(n)\min\{h, 2^{\omega(n)-2}\}. \tag{3.33}$$

If χ is nonprincipal, then

$$S(n, h, \chi) < (9/8)nh. \tag{3.34}$$

Proof. In order to apply Theorem 3.30, we begin with some simple facts about the integral $I(z)$ defined by (3.20). The integrand is periodic with period 1, and since $I(1)=0$, we can assert that

$$I(z) \text{ is periodic with period 1.} \tag{3.35}$$

Also,

$$I(z) = z/2 - z^2/2 \quad \text{for } 0 \leqq z \leqq 1, \tag{3.36}$$

and it follows that

$$0 \leqq I(z) \leqq \min\{(z-[z])/2, (1-(z-[z]))/2, \tfrac{1}{8}\} \qquad (z \geqq 0), \tag{3.37}$$

$$I(m) = 0, \quad I(m+\tfrac{1}{2}) = \tfrac{1}{8} \qquad (m = 0, 1, 2, \ldots). \tag{3.38}$$

Suppose now that χ is principal. We apply Theorem 3.30, taking $K=1$, $N=\prod_{p|n} p$, $N_0=n_0$, $N_1=n_1$. We get

$$S(n, h, \chi)-n^{-1}\varphi^2(n)h^2 = \{2n/\xi(n)\}\sum_{t|n_1} \xi(t)I(h/n_0t). \tag{3.39}$$

The left-hand inequality of (3.33) follows since $I(z)\geqq 0$. If we use the inequality $I(z)\leqq z/2$ and (3.27), we find that the right-hand side of (3.39) is $\leqq\varphi(n)h$, and it is also $\leqq\varphi(n)2^{\omega(n)-2}$ by (3.29) and the inequality $I(z)\leqq\frac{1}{8}$. This proves (3.33).

The proof of (3.34) is more delicate. We define

$$g(x) = g_K(x) = \sum_{w|K} \mu(w)w^{-2}I(w/x) \qquad (x \text{ real}, x > 0).$$

We seek a simple upper estimate for $g(x)$ to insert in (3.31). Using (3.36), we can write

$$g(x) = \sum_{w|K, w\leqq x} \mu(w)w^{-2}\{w/2x-w^2/2x^2\}+\sum_{w|K, w>x} \mu(w)w^{-2}I(w/x) = T_1+T_2, \tag{3.40}$$

say. Now,

$$2x^2T_1 = \sum_{w|K, w\leqq x} \mu(w)[x/w]+\sum_{w|K, w\leqq x} \mu(w)\{x/w-[x/w]-1\}. \tag{3.41}$$

The first sum on the right is

$$\sum_{w|K} \mu(w) \sum_{m\leqq x, w|m} 1 = \sum_{m\leqq x} \sum_{w|K, w|m} \mu(w) = \sum_{m\leqq x, (m,K)=1} 1.$$

If $x\geqq 1$, the second sum on the right of (3.41) does not exceed $x-[x]-1+\sum_{w|K, w\leqq x, \mu(w)=-1} 1$. But the sets $\{w : w\leqq x \text{ and } (w, K)=1\}$ and $\{w : w\leqq x, w|K, \text{ and } \mu(w)=-1\}$ are disjoint, so (3.41) yields

$$T_1 \leqq (2x^2)^{-1}(x-[x]-1+[x]) = (2x^2)^{-1}(x-1), \qquad x \geqq 1. \tag{3.42}$$

On the other hand, since $0\leqq I(z)\leqq\frac{1}{8}$ for all $z\geqq 0$, we have

$$T_2 \leqq \sum_{w|K, w>x, \mu(w)=1} (8w^2)^{-1} \leqq \tfrac{1}{16}\left\{\sum_{w>x} |\mu(w)|w^{-2}+\sum_{w>x} \mu(w)w^{-2}\right\}. \tag{3.43}$$

Clearly,

$$\sum_{w>x} |\mu(w)|w^{-2} \leqq \sum_{w>x} w^{-2}- \sum_{w>x, 4|w} w^{-2}- \sum_{w>x, 9|w} w^{-2}+ \sum_{w>x, 36|w} w^{-2}. \tag{3.44}$$

It is easy to see that for $x>0$,

$$\sum_{w>x} w^{-2} < x^{-2}+\int_x^{+\infty} t^{-2}\,dt = x^{-1}+x^{-2},$$

while

$$\sum_{w>x} w^{-2} \geqq \int_{x+1}^{+\infty} t^{-2}\,dt > x^{-1}-x^{-2}.$$

Thus (3.44) yields

$$\sum_{w>x} |\mu(w)|w^{-2} < 2/3x+4/x^2 \qquad (x \text{ real}, x > 0). \tag{3.45}$$

We could use (3.45) and the inequality

$$T_2 \leqq \tfrac{1}{8} \sum_{w>x} |\mu(w)|w^{-2}$$

to get (3.34) with the constant 9/8 replaced by 7/6. To obtain the better constant, we observe that Moser and MacLeod [15, p. 305] have given a fairly simple proof of the inequality

$$\left|\sum_{w>x} \mu(w)w^{-2}\right| \leqq 1/3x+8/3x^2 \qquad (x \text{ real}, x > 0). \tag{3.46}$$

They actually proved this only for $x \geqq 2$, but when $0<x<2$, it follows from the equation $\sum_{w=1}^{\infty} \mu(w)w^{-2}=6\pi^{-2}$.

Combining (3.43), (3.45), and (3.46), we obtain $T_2<1/16x+5/12x^2$, so that by (3.40) and (3.42),

$$g(x) < 9/16x \tag{3.47}$$

for $x \geqq 1$. (3.47) also holds for $0<x<1$, since the inequality $0 \leqq I(z) \leqq \frac{1}{8}$ gives

$$g(x) < \tfrac{1}{8} \sum_{w=1}^{\infty} |\mu(w)|w^{-2} < \tfrac{1}{4} \qquad (x \text{ real}, x > 0). \tag{3.48}$$

Taking $x=N_0Kt/h$ in (3.47), substituting the result in (3.31), and applying (3.27), we find that

$$S(n, h, \chi) < (9/8)nhN^{-1}\varphi(N) = (9/8)nh \prod_{p|n,\, p\nmid K} (1-p^{-1}). \qquad \text{Q.E.D.} \tag{3.49}$$

In this paragraph, let χ be nonprincipal mod n with conductor K. It seems reasonable to conjecture that $S(n, h, \chi)<nh$ for all $h \geqq 1$, but we are able to prove this only in some special cases. First, Theorem 2.6 shows that this result holds if χ is primitive. Second, if we start from the identity

$$\sum_{w \geqq 1, \mu(w)=1}^{\infty} w^{-2} = 21/2\pi^2, \tag{3.50}$$

then it is easy to verify that $\sum_{w>x, \mu(w)=1} w^{-2}<4x^{-2}$ for $1 \leqq x \leqq 12$, so that by (3.40), (3.42), (3.43), and (3.48), $g(x)<(2x)^{-1}$ for $0<x \leqq 12$. Taking $x=N_0Kt/h$ and using (3.31), we find that $S(n, h, \chi)<nh$ if $h \geqq KN/12$ (where N is defined by (3.11)). (This result can often be improved by using Theorem 3.52 below.) For our third example, we observe that by (3.43),

$$T_2 < (8x^2)^{-1} \sum_{w|K, \mu(w)=1} 1 = (8x^2)^{-1}2^{\omega(K)-1},$$

so that $g(x)<(2x)^{-1}$ if $\omega(K) \leqq 3$; hence $S(n, h, \chi)<nh$ if $\omega(K) \leqq 3$. Finally, if

$h \leqq N_0 K \prod_{p|K} p^{-1}$, then each of the numbers $I(hw/N_0Kt)$ in (3.31) can be calculated exactly by (3.36), and the result $S(n, h, \chi) = \varphi(n)h$ follows from (3.27). This last example suggests the possibility that $S(n, h, \chi) = O(\varphi(n)h)$, and indeed such a result was proved in [17, Lemma 5.10] for the case in which n is a prime power, but it does not hold in general. To see this, let p be the smallest prime factor of K, and suppose $h > NK/p$. If $t | N_1$ and $x = N_0Kt/h$, then $x \leqq NK/h < p$, so that the sum T_1 in (3.40) has only one term, namely that corresponding to $w = 1$. Thus $T_1 = (2x^2)^{-1}(x-1)$. Using (3.45) and (3.46), it is easy to show that $T_2 > -1/16x - 5/12x^2$, and by (3.40) and (3.31), we obtain

$$S(n, h, \chi) > (7/8)nhN^{-1}\varphi(N) - (11/6)nh^2K^{-1}N^{-2}\varphi^2(N)$$

for $h > NK/p$. In particular, let $n \geqq 133$ be odd, let χ be any primitive character mod n (such characters exist; see [16, §6]), and suppose that $n/3 < h \leqq 15n/44$. Then $S(n, h, \chi) > (1/4)nh$.

The inequalities given in (3.33) are also quite precise in some cases. Write

$$S = S(n, h, \chi) - n^{-1}\varphi^2(n)h^2 \qquad (\chi \text{ principal mod } n).$$

Hooley [11, p. 345] has shown that

$$S = \varphi(n)h + O(n^{-1}\varphi^2(n)h \log (2h)), \tag{3.51}$$

so that if we take

$$n = \prod_{p \leqq y} p \quad \text{and} \quad 1 \leqq h \leqq \log \log n,$$

we get

$$S = \varphi(n)h\left\{1 + O\left(\frac{\log \log \log n}{\log \log n}\right)\right\}$$

when y is large (see [10, Theorems 429, 414]). Thus $\varphi(n)h$ is a sharp upper bound for S in some cases; it is also superior to the upper bound given by (3.51). Finally, if n is even and h is an odd multiple of n_1 (defined by (3.18)), then (3.38) and (3.39) show that $S = \varphi(n)2^{\omega(n)-2}$. (This should be compared with (3.56) below.)

We can give another estimate for $S(n, h, \chi)$ which is interesting when χ has small conductor:

(3.52) THEOREM. *Let n, h be positive integers, and let χ be a nonprincipal character* mod n *with conductor K. Then*

$$S(n, h, \chi) < (21/8\pi^2)nK2^{\omega(n)-\omega(K)} \prod_{p|n, p\nmid K} (1-p^{-1}). \tag{3.53}$$

Proof. Since $0 \leqq I(z) \leqq \frac{1}{8}$ for all $z \geqq 0$, (3.31) yields

$$S(n, h, \chi) < \{2nK/\xi(N)\} \sum_{t|N_1} \xi(t) \sum_{w \geqq 1, \mu(w)=1}^{\infty} (8w^2)^{-1},$$

and the result follows from (3.50) and (3.29). Q.E.D.

There are cases in which (3.53) cannot be improved by more than a constant factor. For example, let n be even, and let χ be nonprincipal mod n with odd conductor K. Let h be an odd multiple of $KN_1 = K\prod_{p|n,p\nmid 2K} p$. Using (3.38) and (3.31), we get

$$S(n,h,\chi) > (3/2\pi^2)nK2^{\omega(n)-\omega(K)} \prod_{p|n,p\nmid K}(1-p^{-1})$$

in this special case.

If x and H are positive integers, then the formula

$$\sum_{h=1}^{H} I(h/x) = (H/12)(1-x^{-2}) \qquad \text{if } x|H \tag{3.54}$$

follows easily from (3.36) and the periodicity of $I(z)$. Taking $H=n$ and combining (3.54) and (3.31), we find that if χ is nonprincipal mod n with conductor K, then

$$\begin{aligned}\sum_{h=1}^{n} S(n,h,\chi) &= \frac{n^2K}{6}\,2^{\omega(n)-\omega(K)} \prod_{p|n,p\nmid K}(1-p^{-1}) \prod_{p|K}(1-p^{-2}) \\ &> \pi^{-2}n^2K2^{\omega(n)-\omega(K)} \prod_{p|n,p\nmid K}(1-p^{-1}).\end{aligned} \tag{3.55}$$

It is interesting to compare this with (3.53). There is an analogous result for the principal character χ_0 mod n:

$$\sum_{h=1}^{n} \{S(n,h,\chi_0) - n^{-1}\varphi^2(n)h^2\} = \frac{n\varphi(n)2^{\omega(n)}}{6}\left\{1-\frac{\varphi(n)}{n2^{\omega(n)}}\right\}. \tag{3.56}$$

4. **Applications.** In this section, we shall be concerned with the distribution of power residues, and in particular with the gaps between successive power residues. We shall use the notation given in the fifth paragraph of the introduction. Each result in this section holds for arbitrary positive integers n, k unless otherwise stated.

(4.1) LEMMA. *For $0 \leqq s \leqq \nu-1$ and integers m, h with $h \geqq 0$, let $N_s(m, m+h) = N_s(n, k; m, m+h)$ be the number of x satisfying $m+1 \leqq x \leqq m+h$ and $x \in g_sC_k(n)$. Write χ_0 for the principal character* mod n, *and let ψ denote the typical character* mod n *such that $\psi^k = \chi_0$. Then*

(4.2) *there are exactly $\nu = \nu_k(n)$ characters ψ* mod n,

and

$$N_s(m, m+h) = \nu^{-1}\{n^{-1}\varphi(n)h + R_n(m, m+h) + \Delta_s(m, m+h)\}, \tag{4.3}$$

where

$$\begin{aligned}R_n(m, m+h) &= \sum_{x=1}^{h} \chi_0(m+x) - n^{-1}\varphi(n)h \\ &= \sum_{d|n} \mu(d)\{[(m+h)/d] - (m+h)/d - [m/d] + m/d\},\end{aligned} \tag{4.4}$$

$$\Delta_s(m, m+h) = \sum_{\psi \neq \chi_0} \bar{\psi}(g_s) \sum_{x=1}^{h} \psi(m+x). \tag{4.5}$$

Furthermore,

$$|R_n(m, m+h)| < 2^{\omega(n)} = O_\varepsilon(n^\varepsilon) \quad \textit{for each } \varepsilon > 0, \tag{4.6}$$

$$\sum_{m=1}^{n} R_n^2(m, m+h) = S(n, h, \chi_0) - n^{-1}\varphi^2(n)h^2, \tag{4.7}$$

$$\sum_{s=0}^{\nu-1} \Delta_s(m, m+h) = 0, \tag{4.8}$$

$$\sum_{s=0}^{\nu-1} \Delta_s^2(m, m+h) = \nu \sum_{\psi \neq \chi_0} \left| \sum_{x=1}^{h} \psi(m+x) \right|^2. \tag{4.9}$$

Proof. (4.2) follows from [16, (3.5) and (3.3)]. The remaining facts (except for (4.7)) are proved in the same way as [16, Lemma 3.9]: as a consequence of some simple facts about characters of finite abelian groups, we obtain the identity

$$N_s(m, m+h) = \nu^{-1} \sum_{x=1}^{h} \chi_0(m+x) + \nu^{-1}\Delta_s(m, m+h), \tag{4.10}$$

and the rest follows easily. (4.7) is an elementary deduction from the first part of (4.4). Q.E.D.

We note in passing that by (4.7) and (3.56),

$$\max |R_n(m, m+h)| > \{2^{\omega(n)}\varphi(n)/12n\}^{1/2} \quad \text{for } n \geqq 2,$$

where the maximum is taken over all integer pairs m, h with $0 \leqq m \leqq n-1$, $1 \leqq h \leqq n$. Erdös [7, Theorem 3] gave a direct but rather tricky proof of the stronger result

$$\max_{1 \leqq h \leqq n} |R_n(0, h)| > \{2^{\omega(n)}\varphi(n)/12n\}^{1/2} \quad \text{for } n \geqq 2,$$

while Vijayaraghavan [19] showed that there are values of n and h with $\omega(n)$ arbitrarily large for which $|R_n(0, h)|$ almost attains the upper bound $2^{\omega(n)}$ given in (4.6).

Using (4.10) and (4.5), we get $n^{-1}\sum_{m=1}^{n} N_s(m, m+h) = (\nu n)^{-1}\varphi(n)h$. In other words, if h is fixed, then $(\nu n)^{-1}\varphi(n)h$ is the *average* of the periodic function $N_s(m, m+h)$ over one period. Define

$$G_s^{(w)}(n, k, h) = \sum_{m=1}^{n} \{N_s(m, m+h) - (\nu n)^{-1}\varphi(n)h\}^{2w} \tag{4.11}$$

for $w = 1, 2, \ldots$, and for typographical convenience, write $G_s^{(1)}(n, k, h) = G_s(n, k, h)$. In statistical terms, $n^{-1}G_s(n, k, h)$ is the *variance* of the numbers $N_s(m, m+h)$ $(1 \leqq m \leqq n)$, while $n^{-1}G_s^{(w)}(n, k, h)$ is their *central moment of order* $2w$. The basic idea of Hooley's method [11] (as adapted in [17] and [18]) is to estimate $\mathfrak{S}(n, \beta, k, s)$ in terms of $G_s^{(w)}(n, k, h)$. In this paper, we shall need only the special case $w = 1$; the result is as follows:

(4.12) LEMMA. *If β is real and $\geqq 1$, m is any positive integer, and $0 \leqq s \leqq \nu - 1$, then*

$$\mathfrak{S}(n, \beta, k, s) = O_\beta\left(m^{\beta-1}n + \left(\frac{\nu n}{\varphi(n)}\right)^2 m^{\beta-3} G_s(n, k, m) + \left(\frac{\nu n}{\varphi(n)}\right)^2 \sum_{l=m+1}^{M-1} l^{\beta-4} G_s(n, k, l)\right), \tag{4.13}$$

where

$$M = M(n, k, s) = \max\{h_j(n, k, s) - h_{j-1}(n, k, s) : 1 \leqq j \leqq \alpha = \varphi(n)/\nu\}. \tag{4.14}$$

Furthermore,

$$\sum_{s=0}^{\nu-1} G_s(n, k, h) = \nu^{-1}\left\{S(n, h, \chi_0) - n^{-1}\varphi^2(n)h^2 + \sum_{\psi \neq \chi_0} S(n, h, \psi)\right\}, \tag{4.15}$$

in the notation of Lemma 4.1.

Proof. (4.13) is obvious for $\beta = 1$ (see (1.10)). When $\beta > 1$, it follows from [17, Lemmas 4.5, 4.7]. To obtain (4.15), we substitute (4.3) in (4.11) and sum over s to get

$$\sum_{s=0}^{\nu-1} G_s(n, k, h) = \nu^{-1} \sum_{m=1}^{n} R_n^2(m, m+h) + 2\nu^{-2} \sum_{m=1}^{n} R_n(m, m+h) \sum_{s=0}^{\nu-1} \Delta_s(m, m+h) + \nu^{-2} \sum_{m=1}^{n} \sum_{s=0}^{\nu-1} \Delta_s^2(m, m+h).$$

By (4.8), the middle term on the right is 0. The proof of (4.15) is now completed by applying (4.7) and (4.9). Q.E.D.

(4.16) THEOREM. *For $1 \leqq \beta < 2$ and $0 \leqq s \leqq \nu - 1$,*

$$\mathfrak{S}(n, \beta, k, s) = O_\beta(\nu^{2\beta-2} n\{n/\varphi(n)\}^{2\beta-2}).$$

Proof. By (4.15), Theorem 3.32, and (4.2),

$$\sum_{s=0}^{\nu-1} G_s(n, k, h) = O(\nu^{-1}\varphi(n)h + (1-\nu^{-1})nh) = O(nh). \tag{4.17}$$

Using this as an estimate for $G_s(n, k, h)$ in (4.13), estimating the sum on the right of (4.13) by an integral (in the obvious way), and minimizing by taking $m = [\{\nu n/\varphi(n)\}^2] + 1$, we obtain the result. Q.E.D.

In the case $k = \nu = 1$, (4.17) yields the inequality $G_0(n, 1, h) = O(\varphi(n)h)$, and we get Hooley's result [11]

$$\mathfrak{S}(n, \beta, 1, 0) = O_\beta(n\{n/\varphi(n)\}^{\beta-1}), \qquad 1 \leqq \beta < 2,$$

which is best possible except for the constant. The same methods yield the estimates

$$\mathfrak{S}(n, 2, k, s) = O(\nu^2 n\{n/\varphi(n)\}^2 \log n) \qquad (0 \leqq s \leqq \nu - 1)$$

and

$$\mathfrak{S}(n, 2, 1, 0) = O((n^2/\varphi(n))\{1 + \log M(n, 1, 0)\}) = O((n^2/\varphi(n)) \log\log n).$$

(As remarked in [8] and [11], a sieve method can be used to get the estimate for $M(n, 1, 0)$.) However, these latter results can be improved a little by considering $\sum_{s=0}^{\nu-1} \mathfrak{S}(n, \beta, k, s)$. We proceed to this problem, considering first the case $1 \leqq \beta < 2$. Note that by (1.11),

$$\sum_{s=0}^{\nu-1} \mathfrak{S}(n, \beta, k, s) \geqq \nu^{\beta} n\{n/\varphi(n)\}^{\beta-1} \quad \text{for } \beta \geqq 1. \tag{4.18}$$

(4.19) THEOREM. *For* $1 \leqq \beta < 2$, $\sum_{s=0}^{\nu-1} \mathfrak{S}(n, \beta, k, s) = O_{\beta}(\nu^{\beta} n\{n/\varphi(n)\}^{2\beta-2})$.

Proof. Write

$$G(n, k, h) = \sum_{s=0}^{\nu-1} G_s(n, k, h). \tag{4.20}$$

Using (4.13) and the trivial inequality $M(n, k, s) \leqq n$, we get

$$\begin{aligned} &\sum_{s=0}^{\nu-1} \mathfrak{S}(n, \beta, k, s) \\ &\quad = O_{\beta}\left(\nu m^{\beta-1} n + \left(\frac{\nu n}{\varphi(n)}\right)^2 m^{\beta-3} G(n, k, m) + \left(\frac{\nu n}{\varphi(n)}\right)^2 \sum_{l=m+1}^{n} l^{\beta-4} G(n, k, l)\right) \end{aligned} \tag{4.21}$$

for any $\beta \geqq 1$ and any positive integer m. Combining (4.21) and (4.17), then taking $m = [\nu\{n/\varphi(n)\}^2] + 1$, we get the result. Q.E.D.

There is a very small gap between (4.18) and Theorem 4.19, but this gap seems difficult to close.

We could, of course, use the same methods when $\beta = 2$. The result would be $\sum_{s=0}^{\nu-1} \mathfrak{S}(n, 2, k, s) = O(\nu^2 n\{n/\varphi(n)\}^2 \log n)$ for $n \geqq 2$. We shall improve this slightly in the next theorem by using the identity (3.31) instead of the inequalities (3.33) and (3.34).

(4.22) THEOREM. *We have*

$$\sum_{s=0}^{\nu-1} \mathfrak{S}(n, 2, k, s) = O(\nu^2 n\{n/\varphi(n)\} \log n) \quad \textit{for } n \geqq 2, \tag{4.23}$$

and a better result for $k = \nu = 1$:

$$\mathfrak{S}(n, 2, 1, 0) = O\left(\frac{n^2}{\varphi(n)}\left\{1 + \sum_{p \mid n} p^{-1} \log p\right\}\right). \tag{4.24}$$

Proof. Define $G(n, k, h)$ by (4.20). We apply Lemma 4.12, taking $\beta = 2$ and $m = 1$, replacing $M - 1$ by n, and using the first part of (4.17) to estimate $G(n, k, 1)$. The result is

$$\sum_{s=0}^{\nu-1} \mathfrak{S}(n, 2, k, s) = O\left(\frac{\nu n^2}{\varphi(n)} + \frac{\nu(\nu-1)n^3}{\varphi^2(n)} + \left(\frac{\nu n}{\varphi(n)}\right)^2 \sum_{l=2}^{n} l^{-2} G(n, k, l)\right). \tag{4.25}$$

From (4.15) and Theorem 3.30, we can get an identity for $G(n, k, l)$, and inversion of the order of summation yields

$$\sum_{l=2}^{n} l^{-2}G(n,k,l) = 2n\nu^{-1}\sum_{\psi}\{K/\xi(N)\}\sum_{t|N_1}\xi(t)\sum_{w|K}\mu(w)w^{-2}\sum_{l=2}^{n} l^{-2}I(lw/N_0Kt), \tag{4.26}$$

where ψ runs through all characters mod n with the property that ψ^k is principal. It should be noted that in (4.26), the quantities K, N, N_1, N_0 all depend on ψ (cf. (3.11) and Lemma 3.16); in order to simplify the notation, we have not written $K(\psi)$, $N(n, K)$, etc.

Now if x is an integer and $1 \leqq x \leqq n$, then by (3.36) and (3.37),

$$\sum_{l=2}^{n} l^{-2}I(l/x) = \sum_{l=2}^{x} l^{-2}(l/2x - l^2/2x^2) + \sum_{l=x+1}^{n} O(l^{-2}) = (2x)^{-1}\log x + O(x^{-1}).$$

We use this estimate in (4.26), taking $x = N_0Kt/w$. We also use the obvious estimate $\sum_{w|K}|\mu(w)|w^{-1} = O(K/\varphi(K))$ and the identity

$$-\sum_{w|K}\mu(w)w^{-1}\log w = K^{-1}\varphi(K)\sum_{p|K}(p-1)^{-1}\log p,$$

which follows from logarithmic differentiation of the function $\sum_{w|K}\mu(w)w^{-s} = \prod_{p|K}(1-p^{-s})$. We obtain

$$\sum_{w|K}\mu(w)w^{-2}\sum_{l=2}^{n} l^{-2}I(lw/N_0Kt) = (2N_0K^2t)^{-1}\varphi(K)\left\{\log(Kt) + \sum_{p|K}(p-1)^{-1}\log p\right\} + O(\{t\varphi(K)\}^{-1}).$$

Next we multiply this quantity by $K\xi(t)/\xi(N)$ and sum over the divisors t of N_1, using the identity

$$\sum_{t|N_1}\xi(t)t^{-1}\log t = \left\{\sum_{t|N_1}\xi(t)t^{-1}\right\}\left\{\sum_{p|N_1}(p-1)^{-1}\log p\right\}$$

(a result of logarithmic differentiation), as well as the identities (3.27) and $(KN)^{-1}\varphi(K)\varphi(N) = n^{-1}\varphi(n)$. Substituting the result in (4.26) and using (4.2), we get

$$\sum_{l=2}^{n} l^{-2}G(n,k,l) = \nu^{-1}\varphi(n)\sum_{\psi}\log K + \varphi(n)\sum_{p|n}(p-1)^{-1}\log p + O\left(\nu^{-1}\varphi(n)\sum_{\psi}\{K/\varphi(K)\}^2\right).$$

Combining this with (4.25) and using the fact that $K/\varphi(K) = O(\log\log K)$ for $K \geqq 3$, we obtain

$$\sum_{s=0}^{\nu-1}\mathfrak{S}(n,2,k,s) = O\left(\frac{\nu n^2}{\varphi(n)}\left\{1 + \frac{(\nu-1)n}{\varphi(n)} + \sum_{\psi}\log K + \nu\sum_{p|n}p^{-1}\log p\right\}\right). \tag{4.27}$$

(4.23) follows from (4.27), (4.2), and the trivial estimates $\log K \leqq \log n$, $\sum_{p|n} p^{-1} \log p \leqq \log n$. Finally, if $k=\nu=1$, then $\sum_{\psi} \log K=0$ by (4.2), and (4.24) follows from (4.27). Q.E.D.

In the case $k=\nu=1$, we have $\alpha=\varphi(n)$, and $h_0, \ldots, h_\alpha$ are the $\varphi(n)+1$ smallest positive integers relatively prime to n. Erdös [6] conjectured that

$$\mathfrak{S}(n, 2, 1, 0) = O(n^2/\varphi(n)), \tag{4.28}$$

which would be best possible by (1.11). Hooley [11] obtained a best possible estimate for $\mathfrak{S}(n, \beta, 1, 0)$ when $1 \leqq \beta < 2$ (see our remarks after Theorem 4.16), and in [12], he obtained the asymptotic formula

$$\mathfrak{S}(n, \beta, 1, 0) \sim \Gamma(\beta+1) n\{n/\varphi(n)\}^{\beta-1} \qquad (0 \leqq \beta < 2), \tag{4.29}$$

which is valid if $n \to +\infty$ through a sequence of values such that $n/\varphi(n) \to +\infty$. (See his paper [13] for work on another related problem.) Hooley [11] was able to prove only a slightly weaker result for $\beta=2$, namely

$$\mathfrak{S}(n, 2, 1, 0) = O(n(\log\log n)^2) \quad \text{for } n \geqq 3, \tag{4.30}$$

and his proof of (4.30) required a sieve method to estimate

$$M(n, 1, 0) = \max\{h_j - h_{j-1} : 1 \leqq j \leqq \varphi(n)\}.$$

Contrary to an assertion of Erdös [9, p. 207], Hooley's method in [11] (as it stands) will not even prove

$$\mathfrak{S}(n, 2, 1, 0) = O((n^2/\varphi(n)) \log\log n) \quad \text{for } n \geqq 3. \tag{4.31}$$

In this context, the result (4.24) is interesting for several reasons. In the worst cases (e.g., when n is the product of all primes $\leqq x$ and x is large), it is no better than Hooley's estimate (4.30), but it usually gives more information. In the first place, (4.24) implies (4.31), since for $n \geqq 3$,

$$\sum_{p|n} p^{-1} \log p \leqq \sum_{p \leqq \log n} p^{-1} \log p + (\log n)^{-1} \sum_{p|n} \log p = \log\log n + O(1);$$

hence (4.24) implies (4.30) (and no sieve method is needed in proving (4.24), since a trivial estimate for $M(n, 1, 0)$ suffices). We can also deduce from (4.24) that if $f(n)$ is any real function tending to infinity with n, then

$$\text{the number of } n \leqq x \text{ with } \mathfrak{S}(n, 2, 1, 0) > (n^2/\varphi(n))f(n) \text{ is } o(x). \tag{4.32}$$

In other words, Erdös's conjecture (4.28) is "almost true for almost all n". (However, (4.24) is not strong enough to show that $\mathfrak{S}(n, 2, 1, 0) \leqq An^2/\varphi(n)$ for almost all n, where A is an absolute constant. For suppose that $c>0$, and let $q=q(c)$ be the smallest prime for which $\sum_{p \leqq q} p^{-1} \log p > c$. If n is divisible by the product $Q(c)$ of all primes $\leqq q$, then $F(n)=\sum_{p|n} p^{-1} \log p > c$, so that the number of $n \leqq x$ with $F(n) > c$ is at least $x/2Q(c)$ for large x.)

Another fact which follows easily from (4.24) is that

$$\sum_{n\leqq x} \mathfrak{S}(n, 2, 1, 0) = O(x^2) = O\left(\sum_{n\leqq x} \frac{n^2}{\varphi(n)}\right), \tag{4.33}$$

so that Erdös's conjecture is true "on the average". For another proof of (4.24), as well as derivations of (4.32) and (4.33), see the paper of Shapiro and Hausman referred to in the introduction.

5. **An estimate for** $\mathfrak{S}(p, \beta, k, s)$. In this section, we restrict ourselves to the case in which $n=p$ is prime. In this case, $\nu=\nu_k(p)=(k, p-1)$ (see [16, Lemma 4.2]). By Theorem 4.16, $\mathfrak{S}(p, \beta, k, s)=O_\beta(\nu^{2\beta-2}p)$ for $1\leqq\beta<2$, $0\leqq s\leqq\nu-1$, and Theorem 4.19 shows that for any p, k, β with $1\leqq\beta<2$, there is at least one $s=s(p, k, \beta)$ for which $\mathfrak{S}(p, \beta, k, s)=O_\beta(\nu^{\beta-1}p)$. By (1.11), this is best possible except for the constant. We shall now show how to obtain an inequality of this latter type for *each* s $(0\leqq s\leqq\nu-1)$, provided that p is larger than an appropriate function of k (or ν). We shall again rely on Lemma 4.12, so that it is essential to have a good estimate for the sum $G_s(p, k, h)$ defined by (4.11) (with $w=1$). To obtain such an estimate, we shall use a method very similar to that of §2, as well as a deep result of Burgess [3].

(5.1) LEMMA. *For any prime* p *and any positive integers* k, h, *we have*

$$\nu^2 G_s(p, k, h) = O\left(p+\sum_{\psi_1\neq\chi_0\neq\psi_2}\left|\sum_{x,y=1}^{h}\sum_{m=1}^{p}\psi_1(m+x)\bar{\psi}_2(m+y)\right|\right),$$

where $\nu=(k, p-1)$ *and* ψ_1, ψ_2 *run independently through the nonprincipal characters* χ mod p *such that* $\chi^k=\chi_0$ *is principal.*

Proof. By (4.11), (4.3), (4.6), and a trivial inequality,

$$\nu^2 G_s(p, k, h) \leqq 2\sum_{m=1}^{p}\left\{R_p^2(m, m+h)+\Delta_s^2(m, m+h)\right\} = O\left(p+\sum_{m=1}^{p}\Delta_s^2(m, m+h)\right).$$

The result now follows from (4.5). Q.E.D.

The next lemma is proved by Gallagher's method.

(5.2) LEMMA. *Let* χ, θ *be nonprincipal characters* mod p, *and define*

$$W_p(l, m, \chi, \theta) = \sum_{x=1}^{p}\chi(x+l)\bar{\theta}(x+m). \tag{5.3}$$

Then

$$\begin{aligned} W_p(l, m, \chi, \chi) &= p-1 \quad \text{if } p\mid(l-m), \\ &= -1 \quad \text{if } p\nmid(l-m). \end{aligned} \tag{5.4}$$

Furthermore,

$$W_p(l, m, \chi, \theta) = \frac{\tau(p, \bar{\theta})\tau(p, \bar{\chi}\theta)}{\tau(p, \bar{\chi})}(\chi\bar{\theta})(l-m) \quad \text{if } \chi \neq \theta, \tag{5.5}$$

where $\tau(p, \chi)$ *is defined by* (2.3).

Proof. As in the proof of Lemma 2.1,

$$\begin{aligned} W_p(l, m, \chi, \theta) &= \sum_{y=1}^{p} \chi(y+l-m)\bar{\theta}(y) \\ &= \{\tau(p, \bar{\chi})\}^{-1} \sum_{z=1}^{p} \bar{\chi}(z)e(z(l-m)/p)\theta(z)\tau(p, \bar{\theta}). \end{aligned}$$

(5.4) is now immediate, and (5.5) follows from (2.5). Q.E.D.

(5.6) LEMMA. *Let* p *be prime, and let* k, h, t *be any positive integers. Then*

$$\nu^2 G_s(p, k, h) = O(\nu ph + \nu^2 p^{1/2} h^2), \tag{5.7}$$

$$\nu^2 G_s(p, k, h) = O(\nu ph + \nu^2 h^{2-1/t} p^{(2t^2+t+1)/4t^2} \log p). \tag{5.8}$$

Furthermore, if $t \geqq 2$ *and* $1 \leqq h < p^{(2t+1)/4t}$, *then*

$$\nu^2 G_s(p, k, h) = O(\nu ph + \nu^2 h^{2-1/t} p^{(2t^2+t+1)/4t^2}). \tag{5.9}$$

Proof. Since $N_s(m, m+h+p) = N_s(m, m+h) + \nu^{-1}\varphi(p)$, it follows that $G_s(p, k, h)$ is periodic in h with period p. Thus we may assume throughout this proof that $1 \leqq h \leqq p$.

By Lemma 5.1 and (5.3),

$$\nu^2 G_s(p, k, h) = O\left(p + \sum_{\psi_1 \neq \chi_0 \neq \psi_2} \left| \sum_{x,y=1}^{h} W_p(x, y, \psi_1, \psi_2) \right| \right). \tag{5.10}$$

Now, (5.4) yields

$$\sum_{x,y=1}^{h} W_p(x, y, \psi_1, \psi_1) = ph - h^2 = O(ph) \quad \text{if } \psi_1 \neq \chi_0. \tag{5.11}$$

When $\psi_1 \neq \psi_2$ (and both characters are nonprincipal) it follows from (5.5) and (2.4) that

$$\begin{aligned} \left| \sum_{x,y=1}^{h} W_p(x, y, \psi_1, \psi_2) \right| &= p^{1/2} \left| \sum_{x,y=1}^{h} (\psi_1\bar{\psi}_2)(x-y) \right| \\ &\leqq 2p^{1/2} \left| \sum_{z=1}^{h-1} (\psi_1\bar{\psi}_2)(z) \sum_{v=z}^{h-1} 1 \right| \\ &\leqq 2p^{1/2} \sum_{v=1}^{h-1} \left| \sum_{z=1}^{v} (\psi_1\bar{\psi}_2)(z) \right|. \end{aligned} \tag{5.12}$$

Using the trivial estimate for the inner sum on the right, we get

$$\sum_{x,y=1}^{h} W_p(x, y, \psi_1, \psi_2) = O(p^{1/2}h^2) \quad \text{if } \chi_0 \neq \psi_1 \neq \psi_2 \neq \chi_0. \tag{5.13}$$

Also, Burgess [3, Theorem 1] has shown that if χ is nonprincipal mod p and h, t are positive integers, then

$$\sum_{l=1}^{h} \chi(x+l) = O(h^{1-1/t}p^{(t+1)/4t^2} \log p)$$

for any integer x (the implied constant is *absolute*). Applying this result to the inner sum on the right of (5.12), we get

$$\sum_{x,y=1}^{h} W_p(x, y, \psi_1, \psi_2) = O(h^{2-1/t}p^{(2t^2+t+1)/4t^2} \log p) \tag{5.14}$$

if $\chi_0 \neq \psi_1 \neq \psi_2 \neq \chi_0$. The result (5.7) follows from (5.10), (5.11), (5.13), and (4.2), while (5.8) is obtained similarly by the use of (5.14) instead of (5.13).

Burgess [4] also established the following result: if χ is nonprincipal mod p, t is any integer $\geqq 2$, and $1 \leqq h < p^{(2t+1)/4t}$, then

$$\sum_{l=1}^{h} \chi(l) = O(h^{1-1/t}p^{(t+1)/4t^2}).$$

(Note that this follows from the trivial estimate if $1 \leqq h \leqq p^{(t+1)/4t}$.) Hence (5.9) follows in the same way as the previous results. Q.E.D.

The results of Lemma 5.6 should be compared with the inequality

$$G_s(p, k, h) = O(ph), \tag{5.15}$$

which appears in [20, p. 207, Problem 10a(γ)] and was also proved in [17, p. 416]. This inequality (with Lemma 4.12) is sufficient to prove that $\mathfrak{S}(p, \beta, k, s) = O_\beta(\nu^{2\beta-2}p)$ for $1 \leqq \beta < 2$, but it will not yield the stronger result we seek.

(5.16) THEOREM. *Let p be prime, and let k be any positive integer. Suppose that $1 \leqq \beta < 2$, $0 \leqq s \leqq \nu - 1$, and $p > \nu^4$. Then*

$$\mathfrak{S}(p, \beta, k, s) = O_\beta(\nu^{\beta-1}p + \nu^{\max\{2,2\beta-1\}}p^{(3\beta+1)/8}(\log p)^2), \tag{5.17}$$

and in particular,

$$\mathfrak{S}(p, \beta, k, s) = O_\beta(\nu^{\beta-1}p) \quad \text{if } p > (\nu \log \nu)^{16}. \tag{5.18}$$

Proof. We can assume $\beta > 1$ by (1.10). We wish to combine the estimates (5.7) and (5.8) with Lemma 4.12. Preliminary investigations indicate that the best result of the type (5.18) can be obtained by taking $t = 2$ in (5.8); for simplicity, we shall do this from the outset. Note that if $t = 2$, then (5.7) is better than (5.8) roughly for $h \leqq p^{3/8}(\log p)^2 = H_1$, say. We shall also need the fact that there is an absolute constant A such that for $0 \leqq s \leqq \nu - 1$,

$$M = M(p, k, s) \leqq \min\{p, A\nu^2 p^{3/8}(\log p)^2\} = H_2, \tag{5.19}$$

say. For a proof of (5.19) see [18, Lemma 5.11]; the proof is a straightforward application of [3, Theorem 1] and the method of proof of [17, Theorem 3.23].

In (4.13), we use the estimate (5.7) when $l=m$ and when $m<l\leqq H_1$ (of course, we could have $m\geqq H_1$), and we use (5.8) with $t=2$ for $H_1<l\leqq M-1$ ($<H_2$). The resulting sums are estimated by integrals in the obvious way. Taking $m=\nu$ and using our assumptions $1<\beta<2$ and $p>\nu^4$ to simplify the result, we get

$$\mathfrak{S}(p,\beta,k,s) = O_\beta(\nu^{\beta-1}p+p^{(3\beta+1)/8}F),$$

where

$$\begin{aligned} F &= \nu^2(\log p)^{2\beta-2} && \text{if } 1<\beta<3/2,\\ &= \nu^2(\log p)^2 && \text{if } \beta=3/2,\\ &= \nu^{2\beta-1}(\log p)^{2\beta-2} && \text{if } 3/2<\beta<2. \end{aligned}$$

This yields (5.17), and (5.18) follows easily. Q.E.D.

In particular, the inequality of (5.18) holds whenever $p>(k\log k)^{16}$, since $\nu\leqq k$. Unfortunately, it does not seem easy to get the result with a much less restrictive condition on p, although we can make a trifling improvement on Theorem 5.16 when p and ν are both large. In fact, there is a positive absolute constant B such that if $1\leqq\beta<2$, $0\leqq s\leqq\nu-1$, and $p>B(\nu\log\nu)^8$, then

$$\mathfrak{S}(p,\beta,k,s) = O_\beta(\nu^{\beta-1}p+\nu^{\max\{2,2\beta-1\}}p^{(3\beta+1)/8}\log p), \tag{5.20}$$

and in particular,

$$\mathfrak{S}(p,\beta,k,s) = O_\beta(\nu^{\beta-1}p) \quad \text{if } p>B\nu^{16}(\log\nu)^8. \tag{5.21}$$

The proof is very similar to the preceding proof. We can assume $\beta>1$ and $\nu\geqq 2$. We use (5.9) instead of (5.8), again taking $t=2$. This time, we take $H_1=p^{3/8}$ and $H_2=A\nu^2p^{3/8}(\log p)^2$, where A is the constant of (5.19). If B is large enough, the assumption $p>B(\nu\log\nu)^8$ implies that $H_2\leqq p^{5/8}$, so that the condition for (5.9) is satisfied when $h<H_2$. We now proceed as before to get (5.20) and (5.21).

If we use the technique of Theorem 5.16 when $\beta=2$, we find that for $0\leqq s\leqq\nu-1$ and $p>\nu^4$,

$$\mathfrak{S}(p,2,k,s) = O(\nu p\log p+\nu^3p^{7/8}(\log p)^2). \tag{5.22}$$

When p is large relative to ν, this result is worse than the inequality

$$\mathfrak{S}(p,2,k,s) = O(\nu^6p), \tag{5.23}$$

which was proved in [17, Theorem 6.8] (note that (5.23) was improved under certain circumstances in [18, Theorem 5.15]). When p is not so large, (5.22) is of some interest. Similar techniques could be used for $\beta>2$, but here it seems better to use the methods of [18].

It appears to be difficult to extend these results to $\mathfrak{S}(n,\beta,k,s)$ when n is not prime. The reason is that Lemma 5.2 is hard to generalize to the case of composite modulus, since the characters we are dealing with need not be primitive. While the generalization may not be completely out of reach, the calculations involved seem extremely complicated.

REFERENCES

1. D. A. Burgess, *On character sums and primitive roots*, Proc. London Math. Soc. (3) **12** (1962), 179–192. MR **24** #A2569.

2. ———, *On character sums and L-series*, Proc. London Math. Soc. (3) **12** (1962), 193–206. MR **24** #A2570.

3. ———, *On character sums and L-series*. II, Proc. London Math. Soc. (3) **13** (1963), 524–536. MR **26** #6133.

4. ———, *A note on L-functions*, J. London Math. Soc. **39** (1964), 103–108. MR **28** #3973.

5. H. Davenport and P. Erdös, *The distribution of quadratic and higher residues*, Publ. Math. Debrecen **2** (1952), 252–265. MR **14**, 1063.

6. P. Erdös, *The difference of consecutive primes*, Duke Math. J. **6** (1940), 438–441. MR **1**, 292.

7. ———, *On the coefficients of the cyclotomic polynomial*, Bull. Amer. Math. Soc. **52** (1946), 179–184. MR **7**, 242.

8. ———, *On the integers relatively prime to n and on a number-theoretic function considered by Jacobsthal*, Math. Scand. **10** (1962), 163–170. MR **26** #3651.

9. ———, *Some recent advances and current problems in number theory*, Lectures on Modern Math., vol. 3, Wiley, New York, 1965, pp. 196–244. MR **31** #2191.

10. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 4th ed., Oxford Univ. Press, Oxford, 1960.

11. C. Hooley, *On the difference of consecutive numbers prime to n*, Acta Arith. **8** (1962/63), 343–347. MR **27** #5741.

12. ———, *On the difference between consecutive numbers prime to n*. II, Publ. Math. Debrecen **12** (1965), 39–49. MR **32** #4099.

13. ———, *On the difference between consecutive numbers prime to n*. III, Math. Z. **90** (1965), 355–364. MR **32** #1182.

14. E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen*, 2 Bände, 2nd ed., Chelsea, New York, 1953. MR **16**, 904.

15. L. Moser and R. A. MacLeod, *The error term for the squarefree integers*, Canad. Math. Bull. **9** (1966), 303–306. MR **34** #150.

16. K. K. Norton, *Upper bounds for kth power coset representatives modulo n*, Acta Arith. **15** (1968/69), 161–179. MR **39** #1419.

17. ———, *On the distribution of kth power residues and nonresidues modulo n*, J. Number Theory **1** (1969), 398–418. MR **40** #4223.

18. ———, *On the distribution of power residues and nonresidues*, J. Reine Angew. Math. (to appear).

19. T. Vijayaraghavan, *On a problem in elementary number theory*, J. Indian Math. Soc. **15** (1951), 51–56. MR **13**, 326.

20. I. M. Vinogradov, *Foundations of the theory of numbers*, GITTL, Moscow, 1949; English transl., *Elements of number theory*, Dover, New York, 1954. MR **12**, 10; MR **15**, 933.

INSTITUTE FOR ADVANCED STUDY, PRINCETON, NEW JERSEY 08540

Current address: Department of Mathematics, University of Colorado, Boulder, Colorado 80302