JOURNAL OF NUMBER THEORY 1, 398–418 (1969)

On the Distribution of *k*th Power Residues and Non-Residues Modulo *n*

KARL K. NORTON

Department of Mathematics, University of Colorado, Boulder, Colorado 80302

Communicated by P. T. Bateman

Received January 3, 1969

I. INTRODUCTION

Let n and k be positive integers with $n > 1$, let $C(n)$ denote the multiplicative group consisting of the residue classes mod n which are relatively prime to n, and let $C_k(n)$ denote the subgroup of kth powers. Write $v = v_k(n) = [C(n)\colon C_k(n)]$, and let

$$1 = g_0 < g_1 < \ldots < g_{v-1}$$

be the smallest positive representatives of the v cosets of $C_k(n)$. In a previous paper [*11*], we obtained various upper bounds for $g_m = g_m(n, k)$. Here we investigate the distribution of the members of $C(n)$ among the various cosets $g_s C_k(n)$, and we obtain information on the gaps between successive members of a given coset.

First we derive several asymptotic formulas for $N_s(h, H)$, the number of x satisfying $h+1 \leq x \leq H$ and $x \in g_s C_k(n)$, where h, H are integers with $0 \leq h < H$. Using one of Burgess's estimates for character sums ([*3*], Theorem 2), we find a result (Theorem 3.7) which generalizes and strengthens earlier theorems of Jordan [*10*] and the author ([*11*], Theorem 7.24). From this, we deduce various corollaries. For example, if $H-h \geq n^{(3/8)+\delta}$ for some $\delta > 0$, then

$$N_s(h, H) = (vn)^{-1} \varphi(n)(H-h)\{1 + O_{k,\delta}(n^{-\delta/3})\} \tag{1.1}$$

for $0 \leq s \leq v-1$, where φ is Euler's function. (Throughout this paper, the notation $O_{\delta,\varepsilon,\ldots}$ indicates an implied constant depending at most on $\delta, \varepsilon, \ldots$, while O implies an absolute constant.) Under a certain assumption about the prime factorizations of n and k, a result similar to (1.1) can be proved with the weaker hypothesis $H-h \geq n^{(1/4)+\delta}$ (see Theorem 3.11). This can be applied to strengthen considerably certain theorems of Rédei [*12*] and C. T. Whyburn [*13*] on the "densities" of the cosets $g_s C_k(p)$ in the interval $[1, p^{1/2}]$, where p is a large prime. (See the remarks after Theorem 3.11.)

Now consider an arbitrary but fixed coset $g_s C_k(n)$, let $\alpha = \varphi(n)/v$, and let $h_0 < h_1 < \ldots < h_\alpha$ be the $\alpha+1$ smallest positive members of this coset, so $h_\alpha = n+h_0$. We show that if $\delta > 0$ and $n^{(3/8)+\delta} \le j \le \alpha$, then

$$h_j = \frac{vnj}{\varphi(n)}\{1+O_{k,\delta}(n^{-\delta/3})\}, \tag{1.2}$$

and this result can sometimes be extended (see Theorem 3.19). (Note: we prove that $\alpha > n^{1-\varepsilon}$ for each $\varepsilon > 0$ and n sufficiently large, so (1.2) holds for "most" values of j if δ is small.) We then obtain results of the form

$$\max\{h_j - h_{j-1}: 1 \le j \le \alpha\} = O_{k,\delta}(n^{(3/8)+\delta}) \tag{1.3}$$

for each $\delta > 0$ (cf. Theorem 3.23), and we show that $h_j - h_{j-1} \le n^\delta$ for "most" values of j. In the other direction, we prove that for each $k \ge 2$, there are infinitely many n such that

$$\max\{h_j - h_{j-1}: 1 \le j \le \alpha\}$$
$$\ge \exp\left\{\frac{(\log k)\log n}{\log\log n} - \frac{(\log k)(\log\varphi(k)-1)\log n}{(\log\log n)^2} + O_k\left(\frac{\log n}{(\log\log n)^3}\right)\right\}. \tag{1.4}$$

We show that for $v > 1$, the maximum number of consecutive members of $C(n)$ in a given coset $g_s C_k(n)$ is $O_\varepsilon(n^{(3/8)+\varepsilon})$ (in some cases $O_\varepsilon(n^{(1/4)+\varepsilon})$) for each $\varepsilon > 0$, and in fact we obtain slightly sharper results (see Theorem 3.15). These results generalize a theorem of Burgess [4].

Finally, we examine the problem of estimating the sum

$$\mathfrak{S}(n,\beta) = \mathfrak{S}(n,\beta,k,s) = \sum_{j=1}^{\alpha}(h_j - h_{j-1})^\beta \tag{1.5}$$

for real $\beta \ge 1$. The values of this sum give a measure of the average "dispersion" of the members h_j of a given coset. It is easy to show that

$$\mathfrak{S}(n,\beta) \ge n^\beta \alpha^{1-\beta} \ge v^{\beta-1} n. \tag{1.6}$$

In the case $v = 1$, when $\alpha = \varphi(n)$ and $h_0, \ldots, h_\alpha$ are simply the $\varphi(n)+1$ smallest positive integers prime to n, Hooley has shown that

$$\mathfrak{S}(n,\beta) = O_\beta\left(n\left(\frac{n}{\varphi(n)}\right)^{\beta-1}\right) = O_\beta(n^\beta \alpha^{1-\beta})$$

for $1 \le \beta < 2$, while $\mathfrak{S}(n,2) = O(n(\log\log n)^2)$. (See [7]; cf. also [8], [9], and an earlier paper of Erdös [6].) For the case $v > 1$, we are unable to give a direct generalization of Hooley's method, but we do use some of his ideas. In addition, we use the following elegant character-sum estimate communicated to the author by Dr. D. A. Burgess:

$$\sum_{x=1}^{n} \left| \sum_{l=1}^{h} \chi(x+l) \right|^2 \leq nh\{d(n)\log n\}^2 = O_\varepsilon(n^{1+\varepsilon}h), \tag{1.7}$$

where χ is any non-principal residue character mod n, $h \geq 1$, and $d(n)$ is the number of positive divisors of n. Burgess's proof of (1.7) is given in Section V. (It was previously known ([5], pp. 253, 265) that when n is prime and $0 < h < n$, the sum (1.7) equals $nh-h^2$. This is easy to prove, but the proof of (1.7) is substantially harder for composite n.)

Our result is that for each $\varepsilon > 0$,

$$\mathfrak{S}(n,\beta) = \begin{cases} O_{k,\beta,\varepsilon}(n^{1+\varepsilon}) & \text{if} \quad 1 \leq \beta \leq 2 \\ O_{k,\beta,\varepsilon}(n^{\{(3\beta+2)/8\}+\varepsilon}) & \text{if} \quad \beta > 2. \end{cases} \tag{1.8}$$

The result for $\beta > 2$ can be improved in some cases (see Theorem 6.1), and various specific inequalities can be given when $1 \leq \beta \leq 2$. If $n = p$ is prime, we can use yet another result of Burgess ([1], Lemma 2) to improve (1.8) as follows:

$$\mathfrak{S}(p,\beta) = \begin{cases} O_{k,\beta}(p) & \text{if} \quad 1 \leq \beta < 3, \\ O_{k,\beta,\varepsilon}(p^{\{(\beta+1)/4\}+\varepsilon}) & \text{if} \quad \beta \geq 3. \end{cases} \tag{1.9}$$

II. Notation

Unless stated otherwise, small Latin letters other than e and i represent integers, and p always denotes a prime number. When we have occasion to refer to the prime factorization of n, we always write $n = p_1^{a_1} \ldots p_r^{a_r}$, where $p_1 < \ldots < p_r$ and $a_j \geq 1$ for all j. With reference to this factorization of n, we write $k = p_1^{f_1} \ldots p_r^{f_r} k'$, where $f_j \geq 0$ for all j and $(k', p_1 \ldots p_r) = 1$. We define

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

Also, let

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

The hypothesis that $\max\{\gamma_\lambda, \ldots, \gamma_r\} \leq 2$ is stated in many of our theorems. Note that this hypothesis holds if n is cubefree, or if $2 \nmid (n,k)$ and k is squarefree.

We write

$$n_k = \prod_{j=\lambda}^{r} p_j^{\gamma_j}, \qquad n_0 = \prod_{j=1}^{r} p_j.$$

It is easy to see that

$$n_k \leq \min\{n, 2kn_0\}, \qquad n_0 \leq 2n_k. \tag{2.1}$$

We shall generally write ν and g_j rather than $\nu_k(n)$ and $g_j(n, k)$, and we also write $\alpha = \alpha_k(n) = \varphi(n)/\nu$. We proved in ([*11*], Lemma 4.3) that

$$\nu = \prod_{j=\lambda}^{r} \{p_j^{\gamma_j - 1}(k, p_j - 1)\} \leq 2k^r. \tag{2.2}$$

φ denotes Euler's function, μ is the Möbius function, χ always denotes a residue character, and χ_0 is the principal character with respect to the modulus in question. ψ denotes a typical character mod n such that $\psi^k = \chi_0$. Taking $G = C(n)$, $H = C_k(n)$ in ([*11*], (3.5) and (3.3)), we get:

(2.3) *There are exactly* ν *characters* ψ.

$A_1, A_2, \ldots$ denote positive absolute constants, while $A_1(\delta, \varepsilon, \ldots), \ldots$ denote positive constants depending at most on $\delta, \varepsilon, \ldots$. A statement of the form "If $j \geq A_1$, then ..." means "If $j \geq A_1$ for some $A_1 > 0$, then ..." An empty sum means 0, an empty product 1, and $[\beta]$ is the largest integer $\leq \beta$.

III. Various Asymptotic Formulas

In the following lemma, all residue characters are to the modulus n. Recall that r is the number of distinct prime factors of n.

(3.1) Lemma. *For* $0 \leq s \leq \nu - 1$ *and integers* h, H *with* $0 \leq h < H$, *let* $N_s(h, H)$ *be the number of* x *satisfying* $h+1 \leq x \leq H$ and $x \in g_s C_k(n)$. *Then*

$$N_s(h, H) = \nu^{-1}\{n^{-1}\varphi(n)(H-h) + R_n(h, H) + \Delta_s(h, H)\}, \tag{3.2}$$

where

$$R_n(h, H) = \sum_{d \mid n} \mu(d)([H/d] - H/d - [h/d] + h/d) \tag{3.3}$$

and

$$\Delta_s(h, H) = \sum_{\psi \neq \chi_0} \bar{\psi}(g_s) \sum_{x=h+1}^{H} \psi(x). \tag{3.4}$$

Furthermore

$$|R_n(h, H)| < 2^r. \tag{3.5}$$

Proof. This follows easily from ([*11*], Lemma 3.9). Q.E.D.

(3.6) Lemma. *For each real* $\beta > 1$ *and* $\varepsilon > 0$, *we have*

$$\beta^r = O_{\beta, \varepsilon}(n_0^{\varepsilon}) = O_{\beta, \varepsilon}(n_k^{\varepsilon}).$$

In particular, $\nu = O_{k, \varepsilon}(n_0^{\varepsilon})$.

Proof. Let P_j be the jth prime ($P_1 = 2$). Clearly

$$\beta^r n_0^{-\varepsilon} = \beta^r \left(\prod_{j=1}^{r} p_j\right)^{-\varepsilon} \leq \prod_{j=1}^{r} (\beta P_j^{-\varepsilon}).$$

Let $j(\beta, \varepsilon)$ be the smallest $j \geq 1$ such that $P_j \geq \beta^{1/\varepsilon}$. It follows that

$$\beta^r n_0^{-\varepsilon} \leq \prod_{j=1}^{j(\beta,\varepsilon)-1} (\beta P_j^{-\varepsilon}) = A_1(\beta, \varepsilon).$$

The rest follows from (2.1) and (2.2). Q.E.D.

(3.7) THEOREM. *Let* $0 \leq s \leq v-1$, $0 \leq h < H$, $\varepsilon > 0$, *and let* t *be any positive integer. If* $t = 1$ *or* $t = 2$ *or* $\max\{\gamma_\lambda, \ldots, \gamma_r\} \leq 2$, *then*

$$N_s(h, H) = (vn)^{-1}\varphi(n)(H-h) + O_{\varepsilon,t}((H-h)^{1-1/t} n_k^{\{(t+1)/4t^2\}+\varepsilon}).$$

Proof. By (2.3), Lemma 3.1, and the Cauchy–Schwarz inequality,

$$N_s(h, H) - (vn)^{-1}\varphi(n)(H-h)| < v^{-1}\left\{2^r + \left|\sum_{\psi \neq \chi_0} \bar{\psi}(g_s) \sum_{x=h+1}^{H} \psi(x)\right|\right\}$$

$$\leq v^{-1}\left\{2^r + (v-1)^{1/2}\left(\sum_{\psi \neq \chi_0}\left|\sum_{x=h+1}^{H} \psi(x)\right|^2\right)^{1/2}\right\}. \quad (3.8)$$

From (3.8), it follows that if $v = 1$, we have

$$|N_s(h, H) - (vn)^{-1}\varphi(n)(H-h)| < 2^r. \quad (3.9)$$

Now suppose that $v > 1$. The sum on the right-hand side of (3.8) can then be estimated using the method of proof of ([*11*], Lemma 7.2) (some minor and obvious changes are required). The principal tool is ([*3*], Theorem 2). By this method, we obtain from (3.8) the inequality

$$\begin{aligned}|N_s(h, H) &- (vn)^{-1}\varphi(n)(H-h)| \\ &< v^{-1}\{2^r + A_2(\varepsilon, t)2^{3r/2} v(H-h)^{1-1/t} n_k^{\{(t+1)/4t^2\}+\varepsilon}\} \\ &\leq A_3(\varepsilon, t)2^{3r/2}(H-h)^{1-1/t} n_k^{\{(t+1)/4t^2\}+\varepsilon},\end{aligned} \quad (3.10)$$

provided $t = 1$ or $t = 2$ or $\max\{\gamma_\lambda, \ldots, \gamma_r\} \leq 2$ (in the latter case, there is no restriction on t). By (3.9), (3.10) also holds (for any t) when $v = 1$, and the theorem follows from (3.10) and Lemma 3.6. Q.E.D.

Theorem 3.7 has a number of interesting applications. First we prove (1.1) and another similar result.

(3.11) THEOREM. *Let* $0 \leq s \leq v-1$, $h \geq 0$.

(a). *If* $H - h \geq A_4(\delta)n^{(3/8)+\delta}$ *for some* $\delta > 0$, *then*

$$N_s(h, H) = (vn)^{-1}\varphi(n)(H-h)\{1 + O_{k,\delta}(n^{-\delta/3})\}. \quad (3.12)$$

(b). *Suppose* $\max\{\gamma_\lambda, \ldots, \gamma_r\} \leq 2$. *If* $H - h \geq A_5(\delta)n^{(1/4)+\delta}$ *for some* $\delta > 0$, *then*

$$N_s(h, H) = (vn)^{-1}\varphi(n)(H-h)\{1 + O_{k,\delta}(n^{-\delta_1})\}, \quad (3.13)$$

where

$$\delta_1 = \begin{cases} \delta^2/2 & \text{if } 0 < \delta < 1/6, \\ \delta/3 - 1/24 & \text{if } \delta \geq 1/6. \end{cases}$$

Proof. Clearly $n/\varphi(n) \le 2^r$. Hence by Lemma 3.6 and Theorem 3.7,

$$N_s(h,H) = (\nu n)^{-1}\varphi(n)(H-h)\{1+O_{k,\varepsilon,t}((H-h)^{-1/t} n_k^{\{(t+1)/4t^2\}+\varepsilon})\}, \tag{3.14}$$

provided $t = 1$ or $t = 2$ or $\max\{\gamma_\lambda, \ldots, \gamma_r\} \le 2$.

To prove (a), take $t = 2$ and $\varepsilon = \delta/6$ in (3.14), and use the inequality $n_k \le n$.

To prove (b), first suppose that $\delta \ge 1/6$. Then

$$H-h \ge A_5(\delta) n^{\{3/8\}+(\delta-\{1/8\})},$$

and (3.13) follows from (3.12). Now suppose that $0 < \delta < 1/6$. Since there is no restriction on t, we can take $t = [1/2\delta]+1$ and let

$$\varepsilon = -\delta^2/2 \quad -\delta^2+ \quad 2\delta^2/(1+2\delta),$$

so $\varepsilon > 0$. Since $n_k \le n$, the error term in braces in (3.14) is

$$O_{k,\delta}(n^{(\{1/4\}+\delta)(-1/t)+\{(t+1)/4t^2\}+\varepsilon}) = O_{k,\delta}(n^{-\delta^2/2}). \qquad \text{Q.E.D.}$$

To give an example of how Theorem 3.11 can be applied, let us suppose that n is a prime p with $p \equiv 1 \pmod{k}$, so $\nu = (k, p-1) = k$ by (2.2). Take $h = 0$ and $H = [p^{1/2}]$. By (3.12), the "density" $H^{-1}N_s(0, H)$ is $k^{-1}\{1+O_k(p^{-1/24})\}$. Using Theorem 3.7, we can even show that this density is $k^{-1}+O_\varepsilon(p^{(-1/16)+\varepsilon})$ for each $\varepsilon > 0$. For large p, these results are much stronger than certain theorems of Rédei [*12*] and Whyburn [*13*]; however, these authors used comparatively elementary methods.

Theorem 3.7 also yields the following generalization of a theorem of Burgess [*4*]:

(3.15) THEOREM. *Let $m_{k,s}(n)$ be the maximum number of consecutive members of $C(n)$ in the coset $g_s C_k(n)$, and let $\varepsilon > 0$. If $\nu > 1$, then*

$$\max\{m_{k,s}(n): 0 \le s \le \nu-1\} = O_\varepsilon(n_k^{(3/8)+\varepsilon}).$$

If $\nu > 1$ and $\max\{\gamma_\lambda, \ldots, \gamma_r\} \le 2$, then

$$\max\{m_{k,s}(n): 0 \le s \le \nu-1\} = O_\varepsilon(n_k^{(1/4)+\varepsilon}).$$

Proof. Let $\nu > 1$, and fix s $(0 \le s \le \nu-1)$. Let $0 \le h < H$, and suppose that for each x satisfying $h+1 \le x \le H$ and $(x, n) = 1$, we have $x \in g_s C_k(n)$. Then

$$N_s(h,H) = \sum_{\substack{x=h+1 \\ (x,n)=1}}^{H} 1. \tag{3.16}$$

We observe that the sum on the right is identical with $N_0(h, H)$ when $\nu = 1$, so by Lemma 3.1 and (2.3),

$$\sum_{\substack{x=h+1 \\ (x,n)=1}}^{H} 1 = n^{-1}\varphi(n)(H-h)+R_n(h,H).$$

By (3.5) and Lemma 3.6,

$$|R_n(h,H)| < 2^r = O_\varepsilon(n_k^\varepsilon).$$

Hence by (3.16) and Theorem 3.7,

$$(1-v^{-1})n^{-1}\varphi(n)(H-h) = O_{\varepsilon,t}((H-h)^{1-1/t}n_k^{\{(t+1)/4t^2\}+\varepsilon}),$$

if $t=1$ or $t=2$ or $\max\{\gamma_\lambda,\ldots,\gamma_r\} \le 2$, so

$$H-h = O_{\varepsilon,t}(n_k^{\{(t+1)/4t\}+\varepsilon t}).$$

Taking $t=2$, we get the first result. If $\max\{\gamma_\lambda,\ldots,\gamma_r\} \le 2$, we can take $t = [(4\varepsilon)^{-1/2}]+1$ to get the second result. Q.E.D.

Variants of Theorem 3.15 can be obtained by using the inequality (2.1) for n_k. In the special case when $n=p$ is prime (and $v=(k,p-1)>1$), Theorem 3.15 gives

$$\max\{m_{k,s}(p)\colon 0 \le s \le v-1\} = O_\varepsilon(p^{(1/4)+\varepsilon})$$

In [*4*], Burgess showed that the right-hand side could be replaced by $O(p^{1/4}\log p)$.

From now on, we consider the members of an arbitrary but fixed coset $g_s C_k(n)$. Let $\alpha = \alpha_k(n) = \varphi(n)/v$, and let $h_0, h_1, \ldots, h_\alpha$ be the $\alpha+1$ smallest positive members of $g_s C_k(n)$ arranged in increasing order, so

$$1 \le g_s = h_0 < h_1 < \ldots < h_{\alpha-1} < n < h_\alpha = n+h_0. \tag{3.17}$$

Using Lemma 3.6 and the well-known fact that $\varphi(n) \ge A_6(\varepsilon)n^{1-\varepsilon}$, we get

$$\alpha > A_7(k,\varepsilon)n^{1-\varepsilon} \tag{3.18}$$

for each $\varepsilon > 0$.

First we obtain two asymptotic formulas for h_j. Neither formula is proved valid for small values of j.

(3.19) THEOREM. *Let* $\delta > 0$.

(a). *If* $A_4(\delta)n^{(3/8)+\delta} \le j \le \alpha$, *then*

$$h_j = \frac{vnj}{\varphi(n)}\{1+O_{k,\delta}(n^{-\delta/3})\}.$$

(b). *If* $\max\{\gamma_\lambda,\ldots,\gamma_r\} \le 2$ *and* $A_5(\delta)n^{(1/4)+\delta} \le j \le \alpha$, *then*

$$h_j = \frac{vnj}{\varphi(n)}\{1+O_{k,\delta}(n^{-\delta_1})\},$$

where δ_1 *is defined as in Theorem* 3.11.

Proof. Trivially $h_j \ge j+1$, so if $j \ge A_4(\delta)n^{(3/8)+\delta}$, it follows from Theorem 3.11(a) that

$$j = N_s(0,h_j-1) = (vn)^{-1}\varphi(n)(h_j-1)\{1+O_{k,\delta}(n^{-\delta/3})\}.$$

Thus for $n > A_8(k, \delta)$, we have

$$h_j - 1 = \frac{vnj}{\varphi(n)} \{1 + O_{k,\delta}(n^{-\delta/3})\},$$

while if $1 < n \le A_8(k, \delta)$,

$$\left| \frac{\varphi(n)}{vnj}(h_j - 1) - 1 \right| \le h_j < 2n = O_{k,\delta}(n^{-\delta/3}).$$

Thus (a) follows, and (b) is proved similarly. Q.E.D.

We now study in detail the differences $h_j - h_{j-1}$. Our first result is trivial but interesting.

(3.20) THEOREM. *Let δ, ε be positive. Then $h_j - h_{j-1} \le n^\delta$ for all but $O_{k,\varepsilon}(\alpha^{1-\delta+\varepsilon})$ values of $j (1 \le j \le \alpha)$.*

Proof. (By (3.17), we have

$$\sum_{j=1}^{\alpha} (h_j - h_{j-1}) = n. \tag{3.21}$$

Let l be the number of values of j for which $h_j - h_{j-1} > n^\delta$. By (3.21), $n > ln^\delta$. By (3.18), there is a constant $A_9(k, \varepsilon) > 1$ such that $n \le A_9(k, \varepsilon)\alpha^{1+\varepsilon}$. Hence $l < A_9(k, \varepsilon)\alpha^{1-\delta+\varepsilon}$ for $\delta \le 1$, while $l = 0$ if $\delta > 1$. Q.E.D.

We remark that Theorem 3.20 can be improved slightly by using some of our later results. For example, using (1.8) with $\beta = 2$, we can show by the same method that $h_j - h_{j-1} \le n^\delta$ for all but $O_{k,\varepsilon}(\alpha^{1-2\delta+\varepsilon})$ values of j, and (1.9) allows a further improvement when n is prime.

After Theorem 3.20, it seems reasonable to conjecture that

$$\max \{h_j - h_{j-1} \colon 1 \le j \le \alpha\} = O_{k,\varepsilon}(n^\varepsilon) \tag{3.22}$$

for each $\varepsilon > 0$, but we are far from being able to prove this. The next two theorems show what we can prove in this connection.

(3.23) THEOREM. *For each $\varepsilon > 0$, we have*

$$\max \{h_j - h_{j-1} \colon 1 \le j \le \alpha\} = O_{k,\varepsilon}(n_0^{(3/8)+\varepsilon}),$$

and if $\max \{\gamma_\lambda, \ldots, \gamma_r\} \le 2$, *then*

$$\max \{h_j - h_{j-1} \colon 1 \le j \le \alpha\} = O_{k,\varepsilon}(n_0^{(1/4)+\varepsilon}).$$

Proof. We apply Theorem 3.7. If $t = 1$ or $t = 2$ or $\max \{\gamma_\lambda, \ldots, \gamma_r\} \le 2$, we get

$$N_s(h, H) \ge (vn)^{-1} \varphi(n)(H-h) - A_{10}(\varepsilon, t)(H-h)^{1-1/t} n_k^{\{(t+1)/4t^2\}+\varepsilon},$$

so $N_s(h, H) > 0$ provided that $H-h > A_{11}(\varepsilon, t)v^t n_k^{\{(t+1)/4t\}+\varepsilon t}$ (we have used Lemma 3.6 and the trivial inequality $n/\varphi(n) \leq 2^r$). Since $N_s(h_{j-1}, h_j-1) = 0$ for each j, we get

$$\max\{h_j-h_{j-1}: 1 \leq j \leq \alpha\} = O_{\varepsilon,t}(v^t n_k^{\{(t+1)/4t\}+\varepsilon t}). \tag{3.24}$$

The theorem now follows from (2.1) and Lemma 3.6. Q.E.D.

We note that $h_0 = g_s < (n+h_0)-h_{\alpha-1} = h_\alpha - h_{\alpha-1}$, so

$$h_0 = O_{k,\varepsilon}(n_0^{(3/8)+\varepsilon}) \tag{3.25}$$

for each $\varepsilon > 0$, and if $\max\{\gamma_\lambda, \ldots, \gamma_r\} \leq 2$, then

$$h_0 = O_{k,\varepsilon}(n_0^{(1/4)+\varepsilon}). \tag{3.26}$$

These results improve the inequalities (1.6) and (1.7) of [*11*] (in which n_0 was replaced by n).

It is also interesting to note that Theorem 3.23 can be improved in certain ways. For example, if we use a somewhat similar method of proof and the fact that $N_s(h_l, h_j) = j-l$, we find that if $0 \leq l < j \leq \alpha$ and $j-l = O_{k,\varepsilon}(n_0^{(3/8)+\varepsilon})$, then $h_j - h_l = O_{k,\varepsilon}(n_0^{(3/8)+2\varepsilon})$.

The following result partially complements Theorem 3.23:

(3.27) THEOREM. *For each $k \geq 2$, there are infinitely many n such that*

$$\max\{h_j-h_{j-1}: 1 \leq j \leq \alpha\}$$
$$\geq \exp\left\{\frac{(\log k)\log n}{\log\log n} - \frac{(\log k)(\log\varphi(k)-1)\log n}{(\log\log n)^2} + O_k\left(\frac{\log n}{(\log\log n)^3}\right)\right\}$$

for each coset $g_s C_k(n)$.

Proof. From (3.21), it follows that for any k and n,

$$\max\{h_j-h_{j-1}: 1 \leq j \leq \alpha\} \geq n/\alpha = vn/\varphi(n). \tag{3.28}$$

Let $k \geq 2$, let Q_j be the jth prime $\equiv 1 \pmod k$, and take $n = Q_1 \ldots Q_r$. By (2.2), we have

$$vn/\varphi(n) > v = k^r. \tag{3.29}$$

Using a strong form of the prime number theorem for arithmetic progressions, we get

$$\log n = \sum_{j=1}^{r} \log Q_j = \frac{Q_r}{\varphi(k)}\{1+O_k(e^{-c(\log Q_r)^{1/2}})\}, \tag{3.30}$$

where c is a positive absolute constant. From this it follows easily that $\log Q_r \geq A_{12}(k)\log\log n$, so by (3.30),

$$\log Q_r = \log\log n + \log\varphi(k) + O_k(e^{-c(k)(\log\log n)^{1/2}}), \tag{3.31}$$

where $c(k)$ is positive and depends only on k. By the prime number theorem,

$$r = \pi(Q_r; k, 1) = \frac{Q_r}{\varphi(k)}\left\{\frac{1}{\log Q_r} + \frac{1}{(\log Q_r)^2} + O_k\left(\frac{1}{(\log Q_r)^3}\right)\right\}.$$

Combining this with (3.31) and (3.29), we get the result from (3.28).

Q.E.D.

We now consider the sum $\mathfrak{S}(n, \beta) = \mathfrak{S}(n, \beta, k, s)$ defined in (1.5). Theorem 3.23 allows us to deduce easily the first two parts of

(3.32) THEOREM. *For any real $\beta \geq 1$ and $\varepsilon > 0$, we have:*

(a). $\mathfrak{S}(n, \beta) = O_{k,\beta,\varepsilon}(n^{\{(3\beta+5)/8\}+\varepsilon})$.

(b). *If* $\max\{\gamma_\lambda, \ldots, \gamma_r\} \leq 2$, *then* $\mathfrak{S}(n, \beta) = O_{k,\beta,\varepsilon}(n^{\{(\beta+3)/4\}+\varepsilon})$.

(c). $\mathfrak{S}(n, \beta) \geq n^\beta \alpha^{1-\beta} \geq v^{\beta-1} n$.

Proof. By (3.21), these results are all obvious when $\beta = 1$. Now assume $\beta > 1$. Then clearly

$$\mathfrak{S}(n, \beta) \leq \mathfrak{S}(n, 1) \max\{(h_j - h_{j-1})^{\beta-1} : 1 \leq j \leq \alpha\},$$

and (a), (b) follow from (3.21) and Theorem 3.23. To obtain (c), we use Hölder's inequality:

$$n = \sum_{j=1}^{\alpha} (h_j - h_{j-1}) \leq \left\{\sum_{j=1}^{\alpha} (h_j - h_{j-1})^\beta\right\}^{1/\beta} \left\{\sum_{j=1}^{\alpha} 1\right\}^{1-1/\beta}. \quad \text{Q.E.D.}$$

We remark that Theorem 3.32(c) may be almost best possible, since our conjecture (3.22) would yield $\mathfrak{S}(n, \beta) = O_{k,\beta,\varepsilon}(n^{1+\varepsilon})$ for any $\beta \geq 1$ and $\varepsilon > 0$.

The remainder of this paper is devoted to improving the upper estimates for $\mathfrak{S}(n, \beta)$ given in Theorem 3.32.

IV. THE SUM $\mathfrak{S}(n, \beta)$: PRELIMINARY LEMMAS

In this section, we use an adaptation of an ingenious method due to Hooley [7]. We continue to work with an arbitrary but fixed coset $g_s C_k(n)$, and we introduce some notation which will be used throughout the remainder of this paper. We define

$$M = \max\{h_j - h_{j-1} : 1 \leq j \leq \alpha\}, \tag{4.1}$$

and for each $l \geq 1$, we let T_l denote the number of j for which $h_j - h_{j-1} = l$ (so $T_l = 0$ for $l > M$). For $t = 0, 1$, let

$$S_l^{(t)} = T_l + 2^t T_{l+1} + 3^t T_{l+2} + \ldots. \tag{4.2}$$

Observe that

$$T_l = S_l^{(0)} - S_{l+1}^{(0)} \quad \text{for} \quad l \geq 1, \tag{4.3}$$

and

$$S_l^{(0)} = S_l^{(1)} - S_{l+1}^{(1)} \quad \text{for} \quad l \geq 1. \tag{4.4}$$

(4.5) LEMMA. *For any real $\beta > 1$ and any integer $m \geq 1$,*

$$\mathfrak{S}(n,\beta) \leq 2m^{\beta-1} n + \beta(m+1)^{\beta-1} S_{m+1}^{(1)} + \beta(\beta-1)\left(\frac{m+2}{m+1}\right) \sum_{l=m+2}^{M} S_l^{(1)} l^{\beta-2}.$$

Proof. We have

$$\begin{aligned}\mathfrak{S}(n,\beta) &= \sum_{j=1}^{\alpha} (h_j - h_{j-1})^\beta = \sum_{l=1}^{\infty} T_l l^\beta \\ &\leq m^{\beta-1} \sum_{l=1}^{m-1} T_l l + \sum_{l=m}^{\infty} T_l l^\beta \leq m^{\beta-1} n + \sum_{l=m}^{\infty} \{S_l^{(0)} - S_{l+1}^{(0)}\} l^\beta \\ &= m^{\beta-1} n + S_m^{(0)} m^\beta + \sum_{l=m+1}^{\infty} S_l^{(0)} \{l^\beta - (l-1)^\beta\} \\ &\leq m^{\beta-1} n + S_m^{(0)} m^\beta + \beta \sum_{l=m+1}^{\infty} S_l^{(0)} l^{\beta-1}.\end{aligned}$$

The last sum is

$$\sum_{l=m+1}^{\infty} \{S_l^{(1)} - S_{l+1}^{(1)}\} l^{\beta-1} = S_{m+1}^{(1)} (m+1)^{\beta-1} + \sum_{l=m+2}^{\infty} S_l^{(1)} \{l^{\beta-1} - (l-1)^{\beta-1}\}. \tag{4.6}$$

For $l \geq m+2$, we have

$$\begin{aligned} l^{\beta-1} - (l-1)^{\beta-1} &= (\beta-1) \int_{l-1}^{l} x^{\beta-2}\, dx \\ &\leq \begin{cases} (\beta-1)(l-1)^{\beta-2} \leq (\beta-1) l^{\beta-2} \left(\dfrac{m+2}{m+1}\right) & \text{if } 1 < \beta < 2, \\ (\beta-1) l^{\beta-2} \text{ if } \beta \geq 2. \end{cases}\end{aligned}$$

Combining our results, we get

$$\begin{aligned}\mathfrak{S}(n,\beta) \leq m^{\beta-1} n + S_m^{(0)} m^\beta + \beta S_{m+1}^{(1)} (m+1)^{\beta-1} \\ + \beta(\beta-1)\left(\frac{m+2}{m+1}\right) \sum_{l=m+2}^{\infty} S_l^{(1)} l^{\beta-2}.\end{aligned}$$

Finally, we note that $S_m^{(0)} = T_m + T_{m+1} + \ldots$ is the number of j for which $h_j - h_{j-1} \geq m$, so by (3.21), $n \geq m S_m^{(0)}$. Q.E.D.

We now need to estimate $S_l^{(1)}$ from above.

(4.7) LEMMA. *For $h \geq 1$, define*

$$G_s(n,h) = \sum_{m=1}^{n} \{N_s(m, m+h) - (\nu n)^{-1} \varphi(n) h\}^2. \tag{4.8}$$

Then for each $l \geq 2$, we have

$$S_l^{(1)} \leq \left\{\frac{vn}{\varphi(n)(l-1)}\right\}^2 G_s(n, l-1). \tag{4.9}$$

Proof. Fix $l \geq 2$, and take $h = l-1$ in (4.8). As a function of m, $N_s(m, m+l-1)$ is periodic with period n, so (since $n+h_0-1 = h_\alpha - 1$) we get

$$G_s(n, l-1) = \sum_{m=h_0}^{h_\alpha-1} \{N_s(m, m+l-1) - (vn)^{-1}\varphi(n)(l-1)\}^2. \tag{4.10}$$

We shall show that the number of m for which $h_0 \leq m \leq h_\alpha - 1$ and $N_s(m, m+l-1) = 0$ is at least $S_l^{(1)}$. (4.9) follows immediately from this fact and (4.10).

Since $S_l^{(1)} = 0$ for $l > M = \max\{h_j - h_{j-1} : 1 \leq j \leq \alpha\}$, we can assume $l \leq M$. For each q such that $l \leq q \leq M$, let B_q be the set of integers m of the form $m = h_{j-1} + t$, where $1 \leq j \leq \alpha$, $h_j - h_{j-1} = q$, and $0 \leq t \leq q - l$. B_q is contained in the union of the intervals $[h_{j-1}, h_j - 1]$ for which $h_j - h_{j-1} = q$, so the sets B_q are disjoint. Furthermore, if $m \in B_q$, then for some j, we have

$$h_{j-1} + 1 \leq m+1 \leq m+(l-1) \leq h_{j-1} + (q-l) + (l-1) = h_j - 1,$$

so $h_0 \leq m \leq h_\alpha - 1$ and $N_s(m, m+l-1) = 0$. Letting $|V|$ denote the number of elements in the set V, we clearly have $|B_q| = (q-l+1)T_q$, and hence the total number of m for which $h_0 \leq m \leq h_\alpha - 1$ and $N_s(m, m+l-1) = 0$ is

$$\geq \left|\bigcup_{q=l}^{M} B_q\right| = \sum_{q=l}^{M} (q-l+1)T_q = S_l^{(1)}. \qquad \text{Q.E.D.}$$

(4.11) LEMMA. *For each $h \geq 1$, we have*

$$G_s(n, h) \leq v^{-2}(2^r n^{1/2} + \{F_s(n, h)\}^{1/2})^2, \tag{4.12}$$

where

$$F_s(n, h) = \sum_{m=1}^{n} \Delta_s^2(m, m+h) \leq (v-1) \sum_{\psi \neq \chi_0} \sum_{m=1}^{n} \left|\sum_{x=1}^{h} \psi(m+x)\right|^2. \tag{4.13}$$

Proof. Applying Lemma 3.1 to (4.8) and using the Cauchy–Schwarz inequality, we get

$$\begin{aligned} G_s(n, h) &\leq v^{-2} \sum_{m=1}^{n} \{2^r + |\Delta_s(m, m+h)|\}^2 \\ &\leq v^{-2} \left\{2^{2r} n + 2^{r+1} n^{1/2} \times \left(\sum_{m=1}^{n} \Delta_s^2(m, m+h)\right)^{1/2} + \sum_{m=1}^{n} \Delta_s^2(m, m+h)\right\} \\ &= v^{-2}(2^r n^{1/2} + \{F_s(n, h)\}^{1/2})^2. \end{aligned}$$

By (3.4) and the Cauchy–Schwarz inequality,

$$\sum_{m=1}^{n} \Delta_s^2(m, m+h) \le \sum_{m=1}^{n} \left\{\sum_{\psi \ne \chi_0} 1\right\}\left\{\sum_{\psi \ne \chi_0} \left|\sum_{x=1}^{h} \psi(m+x)\right|^2\right\}$$
$$= (\nu-1) \sum_{\psi \ne \chi_0} \sum_{m=1}^{n} \left|\sum_{x=1}^{h} \psi(m+x)\right|^2,$$

where we have used (2.3). Q.E.D.

In order to apply Lemma 4.11, we need to estimate sums of the form

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

where χ is any non-principal residue character mod n. We shall do this in the next section.

V. Estimation of the Sum (1.7)

In this section, we shall consistently use the notation

$$\sum_{l_1, l_2=1}^{h}{}'$$

to mean summation over all pairs l_1, l_2 such that $1 \le l_1 \le h$, $1 \le l_2 \le h$, and $l_1 \ne l_2$.

(5.1) Lemma. *Let $n(= p_1^{a_1} \dots p_r^{a_r})$ and h be positive integers, and let χ be a non-principal character* mod n. *Write $\chi = \chi_1 \dots \chi_r$, where χ_j is a character* mod $p_j^{a_j}$ *for each j. Then*

$$\sum_{x=1}^{n} \left|\sum_{l=1}^{h} \chi(x+l)\right|^2 = h\varphi(n) + V(n, h),$$

where

$$V(n, h) = \sum_{l_1, l_2=1}^{h}{}' \prod_{j=1}^{r} \sum_{x=1}^{p_j^{a_j}} \chi_j(x+l_1)\bar{\chi}_j(x+l_2).$$

Proof. We have

$$\sum_{x=1}^{n} \left|\sum_{l=1}^{h} \chi(x+l)\right|^2 = \sum_{l=1}^{h} \sum_{x=1}^{n} |\chi(x+l)|^2 + \sum_{l_1, l_2=1}^{h}{}' \sum_{x=1}^{n} \chi(x+l_1)\bar{\chi}(x+l_2).$$

The first double sum on the right is just $h\varphi(n)$, while the second can be written in the form

$$\sum_{l_1, l_2=1}^{h}{}' \sum_{x=1}^{n} \chi((x+l_1)(x+l_2)^{\varphi(n)-1}).$$

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

(5.2) LEMMA. *Let χ be a non-principal character* mod p^a *with conductor* p^b. *Then* $\chi(1+mz) = 1$ *for all* z *if and only if* $p^b|m$.

Proof. Suppose that $\chi(1+mz) = 1$ for all z. Let p^c be the largest power of p dividing m, and let $y \equiv 1 \pmod{p^c}$. The congruence $1+mz \equiv y \pmod{p^a}$ can be solved for z, so $\chi(y) = 1$. Hence $p^b \le p^c$ and $p^b|m$. Q.E.D.

The next two lemmas are due to D. A. Burgess.

(5.3) LEMMA. *Let*

$$T = \sum_{x=1}^{p^a} \chi(x+l_1)\bar{\chi}(x+l_2),$$

where χ is a non-principal character mod p^a *with conductor* p^b, *and* $l_1 \neq l_2$. *Let p^c be the largest power of p dividing* $l_1 - l_2$. *Then*

$$T = \begin{cases} \varphi(p^a) & \text{if } \; c \ge b, \\ -p^{a-1} & \text{if } \; c = b-1, \\ 0 & \text{if } \; c \le b-2. \end{cases}$$

In particular,

$$|T| \le p^{a-b+\min\{b,c\}}.$$

(This inequality holds also when χ is principal.)

Proof. We have

$$T = \sum_{y=1}^{p^a} \chi(y+l_1-l_2)\bar{\chi}(y) = \sum_{\substack{z=1 \\ p \nmid z}}^{p^a} \chi(1+(l_1-l_2)z).$$

Hence if $p^b | l_1 - l_2$, it is clear that $T = \varphi(p^a)$.

Suppose from now on that $p^b \nmid l_1 - l_2$. We then have

$$T = \sum_{z=1}^{p^a} \chi(1+(l_1-l_2)z) - \sum_{\substack{z=1 \\ p \mid z}}^{p^a} \chi(1+(l_1-l_2)z) = T_1 - T_2,$$

say. Our first objective is to show that $T_1 = 0$. If $p \nmid l_1 - l_2$, this is clear, since then

$$T_1 = \sum_{y=1}^{p^a} \chi(y).$$

If $p | l_1 - l_2$, let H be the set of residue classes $y \pmod{p^a}$ such that $y \equiv 1+(l_1-l_2)z \pmod{p^a}$ for some z. It is well = known that for each $y \in H$, this congruence has exactly $(p^a, l_1 - l_2)$ solutions z. Hence

$$T_1 = (p^a, l_1 - l_2) \sum_{y \in H} \chi(y).$$

Now, H is obviously a subgroup of $C(p^a)$, and by Lemma 5.2, χ is not identically 1 on H. Hence $T_1 = 0$ (cf. [*11*], (3.6)).

Thus $T=-T_2$. If $p^{b-1}|l_1-l_2$, then clearly $T_2=p^{a-1}$. Suppose that $p^{b-1}\nmid l_1-l_2$, and let G be the set of residue classes $y \pmod{p^a}$ such that the congruence $y\equiv 1+(l_1-l_2)z \pmod{p^a}$ is satisfied by some z divisible by p. If $y\in G$, the number of such solutions $z \pmod{p^a}$ is the same as the number of solutions $w \pmod{p^{a-1}}$ of the congruence

$$(y-1)/p\equiv (l_1-l_2)w \pmod{p^{a-1}},$$

namely (p^{a-1}, l_1-l_2). Hence we obtain

$$T_2=(p^{a-1}, l_1-l_2)\sum_{y\in G}\chi(y).$$

Now, G is a subgroup of $C(p^a)$, and by Lemma 5.2, χ is not identically 1 on G. Hence $T_2=0$. Q.E.D.

(5.4) LEMMA. *Let χ be a non-principal character* mod n, *and let $h\geq 1$. Then*

$$\sum_{x=1}^{n}\left|\sum_{l=1}^{h}\chi(x+l)\right|^2\leq nh\{d(n)\log n\}^2=O_\varepsilon(n^{1+\varepsilon}h)$$

for each $\varepsilon>0$, where $d(n)$ is the number of positive divisors of n.

Proof. From Lemma 5.1, we get

$$|V(n,h)|\leq \sum_{l_1,l_2=1}^{h}{}' \prod_{j=1}^{r}\left|\sum_{x=1}^{p_j^{a_j}}\chi_j(x+l_1)\bar{\chi}_j(x+l_2)\right|,$$

where $\chi=\chi_1\ldots\chi_r$ and χ_j is a character mod $p_j^{a_j}$. Let $p_j^{b_j}$ be the conductor of χ_j, so the conductor of χ is $K=p_1^{b_1}\ldots p_r^{b_r}$. By Lemma 5.3,

$$|V(n,h)|\leq \sum_{l_1,l_2=1}^{h}{}' \prod_{j=1}^{r} p_j^{a_j-b_j+\min\{b_j,c_j\}},$$

where $c_j=c_j(l_1-l_2)$ is the largest c such that $p_j^c\,|\,l_1-l_2$. Write $K'=n/K=p_1^{a_1-b_1}\ldots p_r^{a_r-b_r}$. Then

$$|V(n,h)|\leq K'\sum_{l_1,l_2=1}^{h}{}' \prod_{j=1}^{r} p_j^{\min\{b_j,c_j\}} \tag{5.5}$$
$$=K'\sum_{l_1,l_2=1}^{h}{}'(K, l_1-l_2)\leq K'\sum_{t\,|\,K} tW(h,t),$$

where for each $t\geq 1$,

$$W(h,t)=\sum_{\substack{l_1,l_2=1\\ t\,|\,l_1-l_2}}^{h}{}' 1=2\sum_{\substack{l=1\\ t\,|\,l}}^{h-1}\sum_{\substack{1\leq l_1<l_2\leq h\\ l_2-l_1=l}}1$$
$$=2\sum_{1\leq m\leq h/t}(h-mt)=2[h/t]\{h-(t/2)[(h/t)+1]\}. \tag{5.6}$$

Writing $h/t=[h/t]+f$, we get

$$W(h,t)=(h^2/t)-h+tf(1-f)\leq h^2/t. \tag{5.7}$$

From (5.5), (5.7), and Lemma 5.1, it follows that

$$\sum_{x=1}^{n}\left|\sum_{l=1}^{h}\chi(x+l)\right|^2 \le nh\{1+(h/K)d(n)\}, \tag{5.8}$$

since $n = KK'$.

We now estimate the sum (5.8) in a different way. Let X be the primitive character mod K induced by χ (see [11], Lemma 5.1), and let χ^* be the principal character mod K', so $\chi(x) = X(x)\chi^*(x)$ for all x. The sum (5.8) becomes

$$\begin{aligned}\sum_{x=1}^{n}\left|\sum_{l=1}^{h}X(x+l)\chi^*(x+l)\right|^2 &= \sum_{x=1}^{n}\left|\sum_{\substack{u=x+1\\(u,K')=1}}^{x+h}X(u)\right|^2\\ &= \sum_{x=1}^{n}\left|\sum_{t\mid K'}\mu(t)\sum_{\substack{u=x+1\\ t\mid u}}^{x+h}X(u)\right|^2\\ &= \sum_{x=1}^{n}\left|\sum_{t\mid K'}\mu(t)X(t)\sum_{(x+1)/t\le v\le(x+h)/t}X(v)\right|^2\\ &\le \sum_{x=1}^{n}\left\{\sum_{t\mid K'}\left|\sum_{(x+1)/t\le v\le(x+h)/t}X(v)\right|\right\}^2.\end{aligned}$$

By the Pólya–Vinogradov inequality (cf. the proof of Lemma 5.3 in [11]), it follows that

$$\begin{aligned}\sum_{x=1}^{n}\left|\sum_{l=1}^{h}\chi(x+l)\right|^2 &\le \sum_{x=1}^{n}\left\{\sum_{t\mid K'}K^{1/2}\log K\right\}^2\\ &= nK\{d(K')\log K\}^2 \le nK\{d(n)\log n\}^2. \end{aligned}\tag{5.9}$$

The lemma now follows from (5.9) when $h > K$ and from (5.8) when $1 \le h \le K$. Q.E.D.

When n is a prime power, Lemma 5.4 can be replaced by a more precise result:

(5.10) LEMMA. *Let χ be a non-principal character* mod p^a, *and let $h \ge 1$. Then*

$$\sum_{x=1}^{p^a}\left|\sum_{l=1}^{h}\chi(x+l)\right|^2 \le \varphi(p^a)h,$$

with equality if $1 \le h \le p^{b-1}$, where p^b is the conductor of χ.

Proof. We can regard χ as a non-principal character mod p^b, and by periodicity, it suffices to prove the lemma when $1 \le h < p^b$.

After Lemma 5.1, we need information concerning the value of

$$V(p^a,h) = \sum_{l_1,l_2=1}^{h}{}' \sum_{x=1}^{p^a}\chi(x+l_1)\bar{\chi}(x+l_2).$$

By Lemma 5.3,

$$V(p^a, h) = \varphi(p^a)W(h, p^b) - p^{a-1}\{W(h, p^{b-1}) - W(h, p^b)\}$$
$$= p^a W(h, p^b) - p^{a-1} W(h, p^{b-1}),$$

where $W(h, t)$ is defined by (5.6). Write $h = yp^{b-1} + z$, where $0 \leq z < p^{b-1}$. Using the first part of (5.7) and our assumption that $1 \leq h < p^b$, we obtain

$$V(p^a, h) = -\varphi(p^a)h + p^a h - p^{a-b}h^2 - p^{a-1}z + p^{a-b}z^2.$$

Lemma 5.1 now yields

$$\sum_{x=1}^{p^a} \left| \sum_{l=1}^{h} \chi(x+l) \right|^2 = \varphi(p^a)h + p^{a-b}(h-z)\{p^{b-1} - (h+z)\},$$

and the rest follows easily. Q.E.D.

VI. Final Results on the Sum $\mathfrak{S}(n, \beta)$

We can now improve Theorem 3.32(a, b) as follows:

(6.1) Theorem. *Let β be real, $\beta \geq 1$. Then for each $\varepsilon > 0$, we have*

$$\mathfrak{S}(n, \beta) = \begin{cases} O_{\beta,\varepsilon}(v^{2\beta-2} n^{1+\varepsilon}) = O_{k,\beta,\varepsilon}(n^{1+\varepsilon}) \text{ if } 1 \leq \beta \leq 2, \\ O_{\beta,\varepsilon}(v^{2\beta-2} n^{\{(3\beta+2)/8\}+\varepsilon}) = O_{k,\beta,\varepsilon}(n^{\{(3\beta+2)/8\}+\varepsilon}) \text{ if } \beta > 2, \\ O_{k,\beta,\varepsilon}(n^{\{(\beta+2)/4\}+\varepsilon}) \text{ if } \beta > 2 \text{ and } \max\{\gamma_\lambda, \ldots, \gamma_r\} \leq 2. \end{cases} \quad (6.2)$$

Proof. By (4.13), Lemma 5.4, and (2.3),

$$F_s(n, h) = O_\varepsilon(v^2 n^{1+\varepsilon} h).$$

By (4.12) and Lemma 3.6,

$$G_s(n, h) = O_\varepsilon(n^{1+\varepsilon} h).$$

By (4.9),

$$S_l^{(1)} = O_\varepsilon(v^2 n^{1+\varepsilon} l^{-1}) \quad (6.3)$$

for $l \geq 2$.

By (3.21), (6.2) is trivial if $\beta = 1$. If $\beta > 1$ and m is any positive integer, then (6.3) and Lemma 4.5 yield

$$\mathfrak{S}(n, \beta) = O_{\beta,\varepsilon}\left(m^{\beta-1} n + v^2 n^{1+\varepsilon} m^{\beta-2} + v^2 n^{1+\varepsilon} \sum_{l=m+1}^{M} l^{\beta-3}\right). \quad (6.4)$$

First suppose that $1 < \beta < 2$. Then by (6.4),

$$\mathfrak{S}(n, \beta) = O_{\beta,\varepsilon}(m^{\beta-1} n + v^2 n^{1+\varepsilon} m^{\beta-2}),$$

and this can be approximately minimized by taking $v^2 n^\varepsilon < m \leq 2v^2 n^\varepsilon$. If $\beta = 2$, then (6.4) yields

$$\mathfrak{S}(n, 2) = O_\varepsilon(mn + v^2 n^{1+\varepsilon} + v^2 n^{1+\varepsilon} \log M)$$
$$= O_\varepsilon(v^2 n^{1+\varepsilon}),$$

if we take $m = 1$ and use the fact that $M \le n$. Thus the first part of (6.2) follows (if we use Lemma 3.6).

Now suppose that $\beta > 2$, and take $m = [v^2 n^\varepsilon]$. By (6.4),

$$\mathfrak{S}(n, \beta) = O_{\beta,\varepsilon}(v^{2\beta-2} n^{1+(\beta-1)\varepsilon} + v^2 n^{1+\varepsilon} M^{\beta-2}).$$

By (3.24), $M = O_\varepsilon(v^2 n^{(3/8)+\varepsilon})$, and we get the second part of (6.2). Finally, if $\max\{\gamma_\lambda, \ldots, \gamma_r\} \le 2$, then $M = O_{k,\varepsilon}(n^{(1/4)+\varepsilon})$ by Theorem 3.23, and the last part of (6.2) follows. Q.E.D.

Theorem 6.1 can be made more precise when $n = p^a$ by using Lemma 5.10 instead of Lemma 5.4. We shall give only the following interesting example:

(6.5) THEOREM.

$$\mathfrak{S}(p^a, 2) < 2p^a\left\{av^2\left(\frac{p}{p-1}\right)\log p + 4\right\}.$$

Proof. Taking $n = p^a$ in (3.3), we easily obtain $|R_n(h, H)| < 1$. Using this in the proof of Lemma 4.11, we can replace (4.12) by the inequality

$$G_s(p^a, h) \le v^{-2}\{p^{a/2} + F_s^{1/2}(p^a, h)\}^2,$$

where $F_s(p^a, h)$ is defined by (4.13). By Lemma 5.10 and (2.3), it follows that if $h \ge 2$,

$$\begin{aligned} G_s(p^a, h) &\le v^{-2}\{vp^{a/2}(1-p^{-1})^{1/2} h^{1/2} + p^{a/2}(1-h^{1/2}(1-p^{-1})^{1/2})\}^2 \\ &\le \varphi(p^a)h. \end{aligned}$$

By (4.9) and the proof of Lemma 4.5 (cf. (4.6)), it follows that for $m \ge 2$,

$$\begin{aligned} \mathfrak{S}(p^a, 2) &\le 2mp^a + 2S_{m+1}^{(1)}(m+1) + 2\sum_{l=m+2}^{M} S_l^{(1)} \\ &\le 2v^2 p^a(1-p^{-1})^{-1}\log M + 2p^a \\ &\qquad \times\{m - (\log m - 1 - m^{-1})v^2(1-p^{-1})^{-1}\}. \end{aligned} \tag{6.6}$$

Taking $m = 4$ and using the fact that $M \le p^a$, we get the result. Q.E.D.

If $v \ge 3$, we can take $m = v^2$ in (6.6) to get

$$\mathfrak{S}(p^a, 2) \le 2av^2\left(\frac{p}{p-1}\right)p^a \log p. \tag{6.7}$$

Theorems 6.1 and 6.5 can be further improved in the special case when $n = p$ is prime:

(6.8) THEOREM. *Let $\beta \ge 1$ be real. Then for each $\varepsilon > 0$, we have*

$$\mathfrak{S}(p, \beta) = \begin{cases} O_\beta(v^{2\beta-2}p) & \text{if } 1 \le \beta < 2, \\ O_\beta(v^{4+(\beta-1)[2/(3-\beta)]}p) & \text{if } 2 \le \beta < 3, \\ O_{k,\beta,\varepsilon}(p^{\{(\beta+1)/4\}+\varepsilon}) & \text{for } \beta \ge 3. \end{cases} \tag{6.9}$$

[*Note*: $v = v_k(p) = (k, p-1)$ *by* (2.2).]

Proof. We have $\mathfrak{S}(p, 1) = p$ by (3.21), so we assume from now on that $\beta > 1$. For any positive integers h, w, n, define

$$G_s^{(w)}(n, h) = \sum_{m=1}^{n} \{N_s(m, m+h) - (vn)^{-1}\varphi(n)h\}^{2w}.$$

The method of proof of Lemma 4.7 shows immediately that for each $l \geq 2$,

$$S_l^{(1)} \leq \left\{\frac{vn}{\varphi(n)(l-1)}\right\}^{2w} G_s^{(w)}(n, l-1). \tag{6.10}$$

For the remainder of this proof, let $n = p$ be prime. We must estimate $G_s^{(w)}(p, h)$ from above. By (3.3), $|R_p(m, m+h)| < 1$, so if we use (3.2) and Hölder's inequality in the form

$$1 + |x| \leq 2^{1-1/2w}(1 + |x|^{2w})^{1/2w},$$

we obtain

$$\{N_s(m, m+h) - (vp)^{-1}\varphi(p)h\}^{2w} \leq v^{-2w}2^{2w-1}\{1 + |\Delta_s(m, m+h)|^{2w}\}.$$

From (3.4), (2.3), and a similar application of Hölder's inequality, we get

$$|\Delta_s(m, m+h)|^{2w} \leq v^{2w-1} \sum_{\psi \neq \chi_0} \left|\sum_{x=m+1}^{m+h} \psi(x)\right|^{2w}.$$

It follows that

$$G_s^{(w)}(p, h) \leq v^{-2w}2^{2w-1}\left\{p + v^{2w-1} \sum_{\psi \neq \chi_0} \sum_{m=1}^{p} \left|\sum_{x=m+1}^{m+h} \psi(x)\right|^{2w}\right\}. \tag{6.11}$$

If $w = 1$, we can use Lemma 5.10 to obtain

$$G_s^{(1)}(p, h) = O(ph). \tag{6.12}$$

If $w > 1$, we use the following result of Burgess ([*1*], Lemma 2):

$$\sum_{m=1}^{p} \left|\sum_{x=m+1}^{m+h} \chi(x)\right|^{2w} < (4w)^{w+1}ph^w + 2wp^{1/2}h^{2w}, \tag{6.13}$$

where χ is any non-principal character mod p. Combining (6.13) with (6.11) and using (2.3), we get

$$G_s^{(w)}(p, h) = O_w(ph^w + p^{1/2}h^{2w}), \quad \text{if} \quad w \geq 2. \tag{6.14}$$

From (6.10) (with $n = p$) and (6.12), we get $S_l^{(1)} = O(v^2pl^{-1})$, and it follows easily that $\mathfrak{S}(p, \beta) = O_\beta(v^{2\beta-2}p)$ for $1 < \beta < 2$ (cf. the proof of Theorem 6.1).

For the remainder of this proof, we assume $w \geq 2$. From (6.10) and (6.14), we get

$$S_l^{(1)} = O_w(v^{2w}pl^{-w} + v^{2w}p^{1/2}), \quad \text{for} \quad l \geq 2. \tag{6.15}$$

If $1 \leq m \leq M = \max\{h_j - h_{j-1}: 1 \leq j \leq \alpha\}$, it follows from (6.15) and Lemma 4.5 that

$$\mathfrak{S}(p, \beta) = O_{\beta, w}\Bigg(m^{\beta-1}p + v^{2w}m^{\beta-1-w}p + v^{2w}p^{1/2}M^{\beta-1} + \\ + \sum_{l=m+2}^{M} v^{2w}pl^{\beta-2-w}\Bigg), \tag{6.16}$$

and this is an obvious consequence of Lemma 4.5 when $m > M$, since $S_l^{(1)} = 0$ for $l > M$. Estimating the sum on the extreme right of (6.16) in the obvious way and taking $m = v^2$, we obtain

$$\mathfrak{S}(p, \beta) = O_{\beta, w}(v^{2\beta-2} p + v^{2w} p^{1/2} M^{\beta-1} + v^{2w} pf(M)), \tag{6.17}$$

where

$$f(M) = \begin{cases} 0 & \text{if } \beta-2-w < -1, \\ \log M & \text{if } \beta-2-w = -1, \\ M^{\beta-1-w} & \text{if } \beta-2-w > -1. \end{cases}$$

Now by (3.24), we have

$$M = O_{\varepsilon, t}(v^t p^{((t+1)/4t)+\varepsilon t}) \tag{6.18}$$

for each integer $t \geq 1$ and each $\varepsilon > 0$. Inserting this estimate into (6.17) and recalling that $w \geq 2$, we find that

$$\mathfrak{S}(p, \beta) = O_{\beta, w, \varepsilon, t}(v^{2\beta-2} p + v^{2w+t(\beta-1)} p^{\{(\beta+1)/4\}+(\beta-1)(\{1/4t\}+\varepsilon t)}) \tag{6.19}$$

if $\beta-2-w \neq -1$. (6.19) holds also when $\beta-2-w = -1$. To prove this, we observe that $\log M = O_\delta(M^\delta)$ for each $\delta > 0$, take

$$\delta = (\beta-1)(\{1/4t\}+\varepsilon t)(\{1/4\}+\{1/4t\}+\varepsilon t)^{-1},$$

and use (6.17) and (6.18), noting that in this case $\beta = w+1 \geq 3$. Thus (6.19) holds whenever $\beta > 1$, $\varepsilon > 0$, $w \geq 2$, and $t \geq 1$.

It is now clear that there is no advantage in taking $w > 2$, so we let $w = 2$ in (6.19). If $\beta \geq 3$, we can take $t = [(1/2)\varepsilon^{-1/2}]+1$ to obtain

$$\mathfrak{S}(p, \beta) = O_{k, \beta, \varepsilon}(p^{\{(\beta+1)/4\}+\varepsilon}).$$

Finally, suppose $1 < \beta < 3$. We first choose the integer t as small as possible so that

$$\{(\beta+1)/4\}+\{(\beta-1)/4t\} < 1.$$

The correct value of t is

$$t = [(\beta-1)/(3-\beta)]+1 = [2/(3-\beta)].$$

With this value of t, we choose $\varepsilon = \varepsilon(\beta)$ so that

$$((\beta+1)/4)+(\beta-1)(\{1/4t\}+\varepsilon t) = 1.$$

From (6.19) (with $w = 2$), we get

$$\mathfrak{S}(p, \beta) = O_\beta(v^{2\beta-2} p + v^{4+(\beta-1)[2/(3-\beta)]} p). \qquad \text{Q.E.D.}$$

In conclusion, we note that Burgess ([2], Lemma 8 and [3], Lemma 8) obtained the following extension of (6.13) under the assumptions that n, h, and w are positive integers, $\varepsilon > 0$, χ is a *primitive* character mod n, and n is cubefree or $w = 2$:

$$\sum_{m=1}^{n} \left| \sum_{x=m+1}^{m+h} \chi(x) \right|^{2w} = O_{w, \varepsilon}(nh^w + n^{(1/2)+\varepsilon} h^{2w}). \tag{6.20}$$

It does not seem to be known whether such a result holds if χ is not primitive. If we knew that (6.20) held when $w = 2$, n is any positive integer, and χ is any non-principal character mod n, then we could obtain

$$\mathfrak{S}(n, \beta) = O_{k,\beta,\varepsilon}(n^{1+\varepsilon} + n^{(1/2)+\varepsilon} M^{\beta-1} + n^{1+\varepsilon} M^{\beta-3})$$

for $\beta \geq 1$, and this would lead to the following improvement of Theorem 6.1:

$$\mathfrak{S}(n, \beta) = \begin{cases} O_{k,\beta,\varepsilon}(n^{1+\varepsilon} + n^{\{(3\beta+1)/8\}+\varepsilon}) & \text{if } \beta \geq 1, \\ O_{k,\beta,\varepsilon}(n^{1+\varepsilon} + n^{\{(\beta+1)/4\}+\varepsilon}) & \text{if } \beta \geq 1 \text{ and} \\ & \max\{\gamma_\lambda, \ldots, \gamma_r\} \leq 2. \end{cases}$$

The method of proof would be similar to that of Theorem 6.8 (but slightly simpler).

Acknowledgment

I wish to thank Professor Wolfgang Schmidt for suggesting to me the problem of estimating the sum (1.5). I am also greatly indebted to Professor D. A. Burgess, who discovered the inequality (1.7) and generously permitted me to include his proof in this paper, thus enabling me to present Theorem 6.1 without restricting n to prime values.

References

1. Burgess, D. A. On character sums and primitive roots. *Proc. London Math. Soc.* (3) **12** (1962), 179–192.
2. Burgess, D. A. On character sums and L-series. *Proc. London Math. Soc.* (3) **12** (1962), 193–206.
3. Burgess, D. A. On character sums and L-series, II. *Proc. London Math. Soc.* (3) **13** (1963), 524–536.
4. Burgess, D. A. A note on the distribution of residues and non-residues. *J. London Math. Soc.* **38** (1963), 253–256.
5. Davenport, H. and Erdös, P. The distribution of quadratic and higher residues. *Pub. Math. Debrecen* **2** (1951–1952), 252–265.
6. Erdös, P. On the integers relatively prime to n and on a number-theoretic function considered by Jacobsthal. *Math. Scand.* **10** (1962), 163–170.
7. Hooley, C. On the difference of consecutive numbers prime to n. *Acta Arith.* **8** (1963), 343–347.
8. Hooley, C. On the difference between consecutive numbers prime to n: II. *Pub. Math. Debrecen* **12** (1965), 39–49.
9. Hooley, C. On the difference between consecutive numbers prime to n: III. *Math. Zeit.* **90** (1965), 355–364.
10. Jordan, J. H. The distribution of kth power residues and non-residues. *Proc. Amer. Math. Soc.* **19** (1968), 678–680.
11. Norton, K. K. Upper bounds for kth power coset representatives modulo n. *Acta Arith.* **15** (1968), 161–179.
12. Rédei, L. Über die Anzahl der Potenzreste mod p im Intervall 1, $\sqrt{p}$. *Nieuw Arch. Wisk.* (2) **23** (1950), 150–162.
13. Whyburn, C. T. The density of power residues and non-residues in sub-intervals of $[1, \sqrt{p}]$. *Acta Arith.* **14** (1968), 113–116.