Canad. Math. Bull. Vol. **30** (3), 1987

ON INCOMPLETE CHARACTER SUMS TO A PRIME-POWER MODULUS

BY
J. H. H. CHALK

ABSTRACT. Let χ denote a primitive character to a prime-power modulus $k = p^{\alpha}$. The expected estimate

$$\sum_{N+1 \leq n \leq N+H} \chi(n) \ll H^{1-r^{-1}} k^{(r^{-1}+r^{-2})/4} k^{\epsilon}$$

for the incomplete character sum has been established for $r = 1$ and 2 by D. A. Burgess and recently, he settled the case $r = 3$ for all primes $p > 3$, (cf. [2] for the proof and for references). Here, a short proof of the main inequality (Theorem 2) which leads to this result is presented; the argument being based upon my characterization in [3] of the solution-set of a related congruence.

1. Let[1] χ be a primitive character to a prime-power modulus $p^{\alpha}(p \geq 3,\ \alpha \geq 2)$,

$$(1) \qquad T_{n,r}(\boldsymbol{m}) = \sum_{\substack{0 \leq x \leq p^r \\ x \in S_n^0(f,g)}} \chi[F(x)],$$

where

$$(2) \qquad \boldsymbol{m} = (m_1, m_2, \ldots, m_6) \in \boldsymbol{Z}^6, \quad F(X)/g(X),$$

$$(3) \qquad f(X) = \prod_{1 \leq i \leq 3} (X + m_i), \quad g(X) = \prod_{3 < i \leq 6} (X + m_i),$$

$$(4) \qquad \left\{ \begin{array}{c} S_n(f,g) = \{x \in \boldsymbol{Z}: fg(x) \not\equiv 0(p), \quad J(f,g,x) \equiv 0(p^n)\}, \\ S_n^0(f,g) = \{x \in S_n(f,g): J'(f,g,x) \equiv 0(p)\} \end{array} , \right\}$$

and

$$(5) \qquad J(f,g,X) = f(X)g'(X) - f'(X)g(X).$$

In a recent letter, David Burgess wrote that he had established the estimate

$$(6) \qquad \sum_{\substack{m \in Z^6 \\ 0 < m_i \leq h}} |S_\alpha(\boldsymbol{m})| \leqslant h^3 p^{\alpha} (\alpha \log p)^4 \quad \text{for} \quad 0 < h \leq p^{\alpha/6},$$

Received by the editors May 8, 1985, and, in revised form, August 18, 1986.
AMS Subject Classification (1980): 10A10, 10G05.
Key words: Congruences, Character Sums.

[1] For notation and terminology, see [3]; in particular, "mod p^r is abbreviated to "(p^r)".

where

$$S_\alpha(\boldsymbol{m}) = \sum_{\substack{0 \le x < p^\alpha \\ fg(x) \not\equiv 0(p)}} \chi[F(x)]. \tag{7}$$

The connection between $S_\alpha(\boldsymbol{m})$ and $T_{n,r}(\boldsymbol{m})$ is given by an inequality of the form

$$|S_\alpha(\boldsymbol{m})| \le p^n |T_{n,r}(\boldsymbol{m})| + 4p^{\alpha/2}, \tag{8}$$

where

$$(n, r) = ((\alpha - \epsilon)/2, (\alpha + \epsilon)/2), \tag{9}$$

and $\epsilon = \epsilon(\alpha) = 0$ if α is even and $= -1$ if α is odd, (cf., Lemma 2 below). Our estimation of $S_\alpha(\boldsymbol{m})$ is entirely based upon that of $T_{n,r}(\boldsymbol{m})$, which in turn depends upon the fact (cf. [3], Theorem pp. 434–435) that $S_n(f, g)$ is a union of at most 4 arithmetic progressions. Thus, for fixed $\boldsymbol{m} \in \boldsymbol{Z}^6$ for which $S_n(f, g) \neq \emptyset$,

$$S_n(f, g) = \bigcup_{\tau, \sigma} A(\tau, \sigma) \tag{10}$$

where, for $m = n - \mu$, $\mu = \mathrm{ord}_p[f(X) - g(X)]$, and $[[\theta]] = -[-\theta]$,

$$A(\tau, \sigma) = \begin{cases} \{x \in \boldsymbol{Z}, x \equiv \tau(p^{m-\sigma})\}, & \text{if } 0 \le \sigma < [[m/2]] \\ \{x \in \boldsymbol{Z}, x \equiv \tau(p^\sigma)\}, & \text{if } \sigma = [[m/2]] \end{cases} \tag{11}$$

and[2] (τ, σ) takes on at least one and at most four values. For $\sigma \neq 0$,

$$(\tau, \sigma) = (t, \nu), (t + \nu z, \nu), (t_1, \nu_1), (t_1 + \nu_1 z_1, \nu_1) \tag{12}$$

which satisfy the conditions

(13) (i) $0 < \nu \le [[m/2]], 0 < \nu_1 \le [[m/2]]$

(14) (ii) $\begin{pmatrix} z \\ z_1 \end{pmatrix}$ is defined uniquely, $\begin{pmatrix} (p^{m-2\nu}) \\ (p^{m-2\nu_1}) \end{pmatrix}$ with $\begin{pmatrix} 3z + 2 \equiv 0(p) \\ 3z_1 + 2 \equiv 0(p) \end{pmatrix}$, respectively;

otherwise, $\nu = 0 \Rightarrow (\tau, \sigma) = (t, 0)$ and the case $\nu_1 = 0$ is anomalous in that $(\tau, \sigma) = (t_i, 0)$ with $i \le 2$ if $\nu \neq 0$ and $i \le 3$ if $\nu = 0$. We show, in Lemma 3, that $F(X)$ satisfies

$$F'(\tau) \equiv F''(\tau) \equiv 0(p^{\mu+\sigma}), F^{(r)}(\tau) \equiv 0(p^\mu), (r \ge 1), \tag{15}$$

for some pair (μ, σ) with $0 \le \mu < n$, $0 \le \sigma \le [[m/2]]$ and since $\tau \in A(\tau, \sigma) \subset S_n(f, g)$, trivially, it follows that

$$\boldsymbol{m} \in B(\mu, \mu + \sigma, h), \tag{16}$$

where

$$B(\mu, s, h) = \{\boldsymbol{m} \in \boldsymbol{Z}^6, 0 < m_i \le h \colon \exists x\, .F'(x) \equiv F''(x) \equiv 0(p^s), \tag{17}$$
$$F'''(x) \equiv 0(p^\mu), fg(x) \not\equiv 0(p)\}.$$

[2]It should be noted that the conditions above in the case $\sigma = 0$ are not explicitly stated in the theorem itself (see, however, part (ii), (a) for the case $\nu_1 = 0$).

Thus, by the decomposition of $S_n(f,g)$ in (10), and, since $A(\tau,\sigma) \subset S_n^0(f,g) \Rightarrow \mu + \sigma > 0$, it follows that

$$\sum_{\substack{m \in Z^6 \\ 0 < m_i \le h}} |T_{n,r}(\boldsymbol{m})| \tag{18}$$

cannot exceed the sum of at most four expressions of the type

$$\sum_{\substack{\mu,\sigma \\ 0 \le \mu < n \\ 0 \le \sigma \le [[m/2]] \\ \mu+\sigma > 0}} \; \sum_{m \in B(\mu,\mu+\sigma,h)} \left| \sum_{\substack{0 < x < p^r \\ x \in A(\tau,\sigma)}} \chi[F(x)] \right| \tag{19}$$

since (τ,σ) takes at most four values in (12). Now, by Burgess' recent work (cf. [2], Theorem 7), we have an upper bound to the cardinality of $B(\mu,s,h)$, which takes the shape

$$\# B(\mu,s,h) \le \kappa(s+1)^3 M(\mu,s,h), \tag{20}$$

where

$$M(\mu,s,h) = \frac{h^6}{p^{s+\mu/2}} + \frac{h^5}{p^{\mu/2}} + h^4 \tag{21}$$

and κ is a numerical constant $\le 6.2^7$. My contribution is a bound for the summand and this is stated in Theorem 1.

THEOREM 1. *For* $\mu + \sigma > 0$,

$$\left| \sum_{\substack{0 \le x < p^r \\ x \in A(\tau,\sigma)}} \chi[F(x)] \right| \le N_\alpha(\mu,\sigma,h), \tag{22}$$

where

$$N_\alpha(\mu,\sigma,h) = \begin{cases} p^{(\mu+\sigma+\epsilon)/2}, & \text{if} \quad 0 \le \sigma < [[m/2]], \\ 2p^{(n+\mu+2\epsilon)/3}, & \text{if} \quad \sigma = [[m/2]]. \end{cases} \tag{23}$$

By Lemma 5, we have

$$M(\mu,\mu+\sigma,h)N_\alpha(\mu,\sigma,h)p^n \le \begin{cases} 6h^3 p^{\alpha-\mu/6}, & \text{if} \quad \sigma < [[m/2]] \\ 6h^3 p^\alpha, & \text{if} \quad \sigma = [[m/2]]' \end{cases} \tag{24}$$

and this is the final ingredient for our version of Burgess' estimate in (6).

THEOREM 2.

$$\sum_{\substack{m \in Z^6 \\ 0 < m_i \le h}} |S_\alpha(\boldsymbol{m})| \le (24)^3(\alpha+3)^4 h^3 p^\alpha, \quad \text{if} \quad 0 < h \le p^{\alpha/6}. \tag{25}$$

2. **Proof of Theorem 2**. By (8), (9), (18), (19), we have

$$(26)\qquad \sum_{\substack{m \in Z^6 \\ 0 < m_i \le h}} |S_\alpha(m)| \le 4h^6 p^{\alpha/2} + 6! h^3 p^\alpha + 4p^n \sum_{\substack{\mu, \sigma \\ 0 \le \mu < n, \mu + \sigma > 0 \\ 0 \le \sigma \le [[m/2]]}} \# B(\mu, \mu + \sigma, h) N_\alpha(\mu, \sigma, h)$$

upon inserting the bounds in (20) and (22) into each of the sums of the type in (19), at most 4 in number, and noting that, for the special case $\mu = n$, the trivial bound p^α is sufficient when $f(X) \equiv g(X)(p^n)$, and the roots of f are merely a permutation of those of g, (as $h^3 \le p^n$). Now by (20), (21) and (24),

$$\begin{aligned}
(27)\quad p^n &\sum_{\substack{\mu, \sigma \\ 0 \le \mu \le n \\ 0 \le \sigma \le [[m/2]]}} \# B(\mu, \mu + \sigma, h) N_\alpha(\mu, \sigma, h) \\
&\le \kappa \sum_{\substack{\mu, \sigma \\ 0 \le \mu < n \\ 0 \le \sigma \le [[m/2]]}} (\mu + \sigma + 1)^3 M(\mu, \mu + \sigma, h) N_\alpha(\mu, \sigma, h) p^n \\
&\le 6\kappa h^3 p^\alpha \left\{ \sum_{\substack{0 \le \mu < n \\ 0 \le \sigma < [[m/2]]}} p^{-\mu/6} (\mu + \sigma + 1)^3 + \sum_{\substack{0 \le \mu < n \\ \sigma = [[m/2]]}} (\mu + \sigma + 1)^3 \right\} \\
&\le 6\kappa h^3 p^\alpha \left\{ \left[\sum_{0 \le \mu < n} \sum_{0 \le \sigma \le n} p^{-\mu/6} (n+1)^3 \right] + (n+1)^4 \right\} \\
&\le 6\kappa h^3 p^\alpha \left\{ 1 + \sum_{0 \le \mu < \infty} p^{-\mu/6} \right\} (n+1)^4 \\
&< 6^2 \kappa h^3 p^\alpha (n+1)^4 \\
&< 6^3 \cdot 2^3 (\alpha + 3)^4 h^3 p^\alpha.
\end{aligned}$$

Thus, the sum on the left of (26) does not exceed

$$[4 + 6! + 4.6^3.2^3(\alpha + 3)^4] h^3 p^\alpha \le 2^6 6^3 (\alpha + 3)^4 h^3 p^\alpha.$$

3. **The Auxiliary Lemmata**. In subsequent arguments, we shall need a finite form of the Taylor expansion of $F(x)$ or $F(a + x)$ and Lemma 1 provides the justification.

LEMMA 1. ($n \ge 2$). *Let* $k_n = p\phi(p^n) - 1$,

$$G(X) = f(X) g(X)^{k_n}, \; F(X) = f(X)/g(X).$$

Then

(i) for any x with $g(x) \not\equiv 0(p)$,

$$(28)\qquad G(x) \equiv F(x),\ G'(x) \equiv F'(x), \ldots, G^{(r)}(x) \equiv F^{(r)}(x), \ldots, (p^n),$$

and

$$\operatorname{ord}_p F^{(r)}(x)/r! \geq 0, \quad \textit{for all} \quad r.$$

(ii) If $g(a) \not\equiv 0(p)$, *then*

$$F(a + x) \equiv F(a) + \frac{F'(a)}{1!}x + \frac{F''(a)}{2!}x^2 + \cdots + \frac{F^{(1_n)}(a)}{1_n!}x^{1_n} \quad (p^n), \tag{29}$$

where $1_n \leq \deg G(X)$.

PROOF:

(i) Use induction on r, noting that

$$F^{(r)}(x) = \frac{f_r(x)}{g^r(x)}, \; G^{(r)}(x) \equiv f_r(x)g(x)^{k_n - r}(p^n)$$

for a suitable polynomial $f_r(x)$, and that $k_n \equiv -1(p^n)$.

(ii) Since $G(a + x) \equiv F(a + x)(p^n)$, and $G(a + x)$ is a polynomial in x, part (i) gives the result.

LEMMA 2.

$$|S_\alpha(\boldsymbol{m})| \leq 4p^{\alpha/2} + p^n |T_{n,r}(\boldsymbol{m})|. \tag{30}$$

PROOF. This is merely a refinement of Burgess' Lemma 2 and Lemma 4 ([1]) in which the non-singular solutions (p^r) of the congruence $F'(x) \equiv 0(p^r)$, at most 4 in number are separated and estimated crudely. Lemma 1 provides the justification in replacing his $f(x)g(x)^{\phi(p^n)-1}$ by $F(x) = f(x)/g(x)$.

LEMMA 3. $\operatorname{ord}_p F''(\tau) = \mu + \sigma$.

PROOF. If $F(X) = f(X)/g(X)$, then

$$-g^2(X)F'(X) = J(f,g,X)$$

and

$$-(g^2(X)F''(X) + 2g(X)g'(X)F'(X)) = J'(f,g,X)$$

Then, by our choice of $\tau \in A(\tau,\sigma) \subset S_n(f,g)$, we have $J(f,g,\tau) \equiv 0(p^n)$ and so

$$F'(\tau) \equiv 0(p^n), \quad \text{since} \quad g(\tau) \not\equiv 0(p).$$

If $\sigma = \nu$, then

$$J'(f,g,X) = J'(f + \lambda g,X) \equiv uJ'(f_1,g,X), \quad (p^n) \tag{31}$$

by the combinative invariance of J and J' and $f_1(x)$ is as defined in ([3], (19)). But

$$J'(f_1,g,X) = [w(X - t)^3 + v(X - t)^2]g''(X) - 2[3w(X - t) + v]g(X)$$

and on substituting $\tau = t$ and $\tau = t + vz$ for $v \neq 0$ and $\tau = t$ for $v = 0$ we have the required result (noting that $3z + 1 \equiv -1 \not\equiv 0(p)$ in the case $\tau = t + \nu z$). If $\sigma = \nu_1$, the argument is entirely similar, except that (31) is replaced by

$$J'(f_1, g, X) = J'(f_1, g + \lambda_1 f_1, X) \equiv u_1 J'(f_1, g_1, X), \quad (p^m) \tag{32}$$

where $u_1 \not\equiv 0(p)$ and $g_1(X)$ is as defined in ([3], (38)).

LEMMA 4. *Suppose* $l \geq 2$, $k \geq 2$ *and* $p > 3$. *Let*

$$f(X) = a_k X^k + \cdots + a_2 X^2 + a_1 X + a_0 \quad (a_i \in \mathbf{Z}, 0 \leq i \leq k),$$

where

$$(a_1, a_2, a_3, p) = 1, \quad p \mid a_r (r \geq 3). \tag{33}$$

If $\mu_1, \mu_2, \ldots, \mu_r$ *denote the distinct roots of the congruence*

$$f'(x) \equiv 0(p), \quad 0 \leq x < p \tag{34}$$

let $m_1, m_2, \ldots, m_r$ *denote their respective multiplicities and define*

$$m = m_1 + m_2 + \cdots + m_r, \quad M = \max(m_1, m_2, \ldots, m_r).$$

If

$$S(p^l, f) = \sum_{0 \leq x \leq p^l} e^{2\pi i f(x)/p^l}$$

then

$$|S(p^l, f)| \leq m p^{l\left[1 - \frac{1}{M+1}\right]},$$

where $m \leq k - 1$.

PROOF. See e.g. [4], pp. 40–41; also [5], Ch. 1, §5 with routine changes.[3]

LEMMA 5. *Let*

$$M(\mu, \mu + \sigma, h) = \frac{h^6}{p^{\sigma + 3\mu/2}} + \frac{h^5}{p^{\mu/2}} + h^4$$

Then

(i) $M(\mu, \mu + \sigma, h) \cdot p^{(\mu + \sigma + \epsilon)/2} \cdot p^n < 3h^3 p^\alpha p^{-\mu/6}$, if $0 \leq \sigma < \left[\left[\frac{m}{2}\right]\right]$

(ii) $M(\mu, \mu + [[m/2]], h) \cdot p^{(n + \mu + 2\epsilon)/3} p^n \leq 3h^3 p^\alpha$.

PROOF. (i) Since $n = (\alpha - \epsilon)/2$ and $\sigma < [[m/2]] \Rightarrow 2\sigma \leq n - \mu - 1$, we have $\max(2\sigma, \mu + \sigma) \leq \mu + 2\sigma \leq n - 1 = \alpha/2 - (1 + \epsilon/2)$. Then

$$(\mu + \sigma + \epsilon)/2 + n = (\alpha - \epsilon + \mu + \sigma + \epsilon)/2 = \alpha/2 + (\mu + \sigma)/2$$
$$\leq (\alpha/2 - \mu) + (\sigma + 3\mu/2)$$

[3]Alternatively, refer to my version (to appear in Mathematika).

https://doi.org/10.4153/CMB-1987-037-4 Published online by Cambridge University Press

and $h^6p^{\alpha/2} \leq h^3p^{\alpha}$. Similarly,

$$h^5p^{\alpha/2}p^{(\mu+\sigma)/2}p^{-\mu/2} \leq h^3p^{\alpha/3}p^{\alpha/2}p^{\sigma/2} < h^3p^{5\alpha/6}\cdot p^{\alpha/8}p^{-\mu/4} < h^3p^{\alpha}p^{-\mu/4}$$

and

$$h^4p^{(\alpha+\mu+\sigma)/2} < h^3p^{\alpha/6}p^{\alpha/2}\cdot p^{(\mu+\sigma)/2} = (h^3p^{\alpha}p^{-\mu/6})\cdot p^{(\mu+\sigma)/2-\alpha/3-\mu/6},$$

where

$$\alpha/3 > 2(\mu + 2\sigma)/3 \geq 2\mu/3 + \sigma/2 = \mu/6 + (\mu + \sigma)/2.$$

(ii) $\sigma = [[m/2]]$, $n = (\alpha - \epsilon)/2 \Rightarrow 2\sigma - (\alpha - \epsilon)/2 + \mu = 0$ or $1 \Rightarrow \sigma \geq \alpha/4 - \mu/2$. But, $(n + \mu + 2\epsilon)/3 + n = (2\alpha + \mu)/3$ and so

$$h^6p^{(2\alpha+\mu)/3}p^{-\left(\frac{3\mu}{2}+\sigma\right)} \leq h^3p^{7\alpha/6+\mu-\sigma},$$

where $7\alpha/6 - \mu - \sigma \leq 7\alpha/6 - \mu - (\alpha/4 - \mu/2) < \alpha$.

Similarly, $h^5p^{-\mu/2}p^{(2\alpha+\mu)/3} \leq h^3p^{\alpha/3}p^{2\alpha/3} = h^3p^{\alpha}$,

$$h^4p^{(2\alpha+\mu)/3} < h^3p^{\alpha/6}p^{2\alpha/3}p^{\mu/3} < h^3p^{\alpha},$$

since $\mu \leq n - 1 = (\alpha - \epsilon)/2 - 1 < \alpha/2$

3. **Proof of Theorem 1**. For convenience, we denote the sum in (22), by S_1 if $0 \leq \alpha < [[m/2]]$ and by S_2 if $\sigma = [[m/2]]$.

(i) Write $x = \tau + p^{m-\sigma}y$, where $0 \leq y < p^{\mu+\sigma+\epsilon}$; then

$$S_1 = \chi[F(\tau)] \sum_{0 \leq y < p^{\mu+\sigma+\epsilon}} \chi\left[1 + \frac{F_\tau(y) - F(\tau)}{F(\tau)}\right],$$

since $F(\tau) \not\equiv 0(p)$ where, by Lemma 2,

$$F_\tau(y) - F(\tau) = p^{m-\sigma}F'(\tau)y + \frac{p^{2(m-\sigma)}}{2!}F''(\tau)y^2 + \frac{p^{3(m-\sigma)}}{3!}F'''(\tau)y^3 + \cdots$$

$$\equiv p^{\alpha-(\mu+\sigma+\epsilon)}[a_1y + a_2y^2 + \cdots + a_ky^k], \quad (p^{\alpha})$$

and $\alpha - (\mu + \sigma + \epsilon) = 2n - \mu - \sigma > \alpha/2$, $k \leq \alpha/(m - \sigma) < \alpha$,

$$a_1 = \frac{F'(\tau)}{1!p^n}, \quad a_2 = \frac{F''(\tau)}{2!p^{\mu+\sigma}}, \quad a_3 = \frac{F''(\tau)}{3!p^{\mu}}p^{n-\mu-2\sigma}.$$

Moreover, $p^{\mu} | F^{(r)}(\tau)$ for $r \geq 1$ and, indeed we have

$$a_r = \frac{F^{(r)}(\tau)}{r!p^{\mu}}\cdot p^{w(r)}, \quad (r \geq 3),$$

where

$$\begin{aligned} w(r) &= r(m-\sigma) - (2n-\mu-\sigma) + \mu, \\ &= 3(m-\sigma) - (2n-2\mu-\sigma) + (r-3)(m-\sigma), \\ &= n-\mu-2\sigma + (r-3)(m-\sigma), \\ &= n-\mu-2\sigma + (r-3), \quad \text{since} \quad m > 2\sigma. \\ &> 0, \quad \text{for} \quad r \geq 3 \end{aligned}$$

Also, if $p^{\delta(r,p)} \| r!$, then

$$\delta(r,p) = \left[\frac{r}{p}\right] + \left[\frac{r}{p^2}\right] + \cdots < \frac{r}{p-1} \leq r-3, \quad \text{for} \quad r \geq 4, \quad p \geq 5,$$

and so

$$w(r) > n-\mu-2\sigma+\delta(r,p), \quad \text{for} \quad r \geq 4.$$

Hence

$$S_1 = \chi(F(\tau)) \sum_{0 \leq y < p^{\mu+\sigma+\epsilon}} e\left[\frac{c}{F(\tau)p^{\mu+\sigma+\epsilon}} G(y)\right),$$

since $\chi(1+p^\gamma) = e\left(\frac{c}{p^{\alpha-\gamma}}\right)$ if $\gamma \geq \alpha/2$, where $p \nmid c$, $e(x)$ denotes $e^{2\pi i x}$,

$$G(y) = a_1 y + a_2 y^2 + \cdots + a_k y^k,$$

$\text{ord}_p\, a_2 = 0$, by Lemma 4 and $p \mid a_r (3 \leq r \leq k)$. Now

$$G'(Y) \equiv a_1 + 2a_2 Y \quad (p)$$

and so, by Hua's inequality (Lemma 4) with $M = m = 1$,

$$|S_1| \leq p^{(\mu+\sigma+\epsilon)/2} \leq p^{(n+\mu)/3+\epsilon/2}$$

since $n > \mu + 2\sigma$.

(ii) Write $x = \tau + p^\sigma y$, where $0 \leq y < p^{n-\sigma+\epsilon}$ and

$$\sigma = [[m/2]] = \begin{cases} m/2, & \text{if } m \text{ even}, \\ (m+1)/2, & \text{if } m \text{ odd}. \end{cases}$$

Then, as in (i),

$$\begin{aligned} S_2 &= \sum_{0 \leq y < p^{n-\sigma+\epsilon}} \chi[F_\tau(y)] \\ &= \chi[F(\tau) \sum_{0 \leq y < p^{n-\sigma+\epsilon}} \chi\left[1 + \frac{F_\tau(y) - F(\tau)}{F(\tau)}\right], \end{aligned}$$

https://doi.org/10.4153/CMB-1987-037-4 Published online by Cambridge University Press

where

$$F_\tau(y) - F(\tau) \equiv \frac{p^\sigma}{1!}F'(\tau)y + \frac{p^{2\sigma}}{2!}F''(\tau)y^2 + \cdots + \frac{p^{k\sigma}}{k!}F^{(k)}(\tau)y^k. \quad (p^\alpha)$$

$$\equiv p^{\alpha-(n-\sigma+\epsilon)}[a_1y + a_2y^2 + \cdots + a_ky^k], \quad (p^\alpha)$$

and $\alpha - (n - \sigma + \epsilon) = 2n - (n - \sigma) > \alpha/2$, $k < \alpha/\sigma < \alpha$,

$$a_1 = \frac{F'(\tau)}{1!p^n}, \quad a_2 = \frac{F''(\tau)}{2!p^{n-\sigma}} = \frac{F''(\tau)}{2!p^{\mu+\sigma}}\cdot p^{2\sigma-m}$$

$$a_3 = \frac{F'''(\tau)}{3!p^{n-2\sigma}} = \frac{F'''(\tau)}{3!p^\mu}\cdot p^{2\sigma-m}, \quad a_4 = \frac{F^{(iv)}}{4!p^\mu}\cdot p^{3\sigma-m}$$

$$a_r = \frac{F^{(r)}(\tau)}{r!p^\mu}\cdot p^{w(r)}, \quad p^\mu | F^{(r)}(\tau), \quad (r \geq 1)$$

with $w(r) = r\sigma - (n + \sigma) + \mu = (r - 1)\sigma - m = (2\sigma - m) + (r - 3)\sigma$. Thus, for $r \geq 4$, we have $w(r) \geq 1 + \delta(r,p)$ with strict inequality if m is odd.

Hence

$$S_2 = \chi[F(\tau)] \sum_{0 \leq y < p^{n-\sigma+\epsilon}} e\left[\frac{c}{p^{n-\sigma+\epsilon}}G(y)\right],$$

where $G(y) = a_1y + a_2y^2 + \cdots + a_ky^k$ and

$$\operatorname{ord}_p a_2 = \begin{cases} 0 & \text{if } m \text{ is even} \\ 1 & \text{if } m \text{ is odd} \end{cases}, \quad p | a_r (4 \leq r \leq k).$$

Now, for m even,

$$G'(y) \equiv a_1 + 2a_2y + 3a_3y^2(p), \quad p \nmid 2a_2$$

and so, by Hua's inequality, with $M \leq 2$, $m \leq 2$

$$|S_2| \leq 2p^{(n-\sigma+\epsilon)(1-1/3)} = 2p^{(n+\mu+2\epsilon)/3}.$$

For m odd, when $2\sigma - m = 1$ and $p \| a_2$, $p | a_3$, we note that $S_2 = 0$ if $p \nmid a_1$; otherwise, if $p | a_1$, we have $p | G(Y)$ and

$$p^{-1}G'(y) \equiv a_1p^{-1} + 2a_2p^{-1}y + 3a_3p^{-1}y^2(p), \quad p \nmid 2\, a_2p^{-1}$$

and then, by Hua's inequality, with $f(X) = p^{-1}G(X)$, $M \leq 2$, $m \leq 2$,

$$|S_2| \leq 2p\cdot p^{(n-\sigma+\epsilon-1)(1-1/3)} = 2p^{(n+\mu+2\epsilon)/3}.$$

REFERENCES

1. D. A. Burgess, *On Character Sums and L-series*, Proc. London Math. Soc., (3), **12** (1962), pp. 193–206.

2. D. A. Burgess, *Estimation of Character Sums Modulo a Power of a prime*, *ibid* (3) **52** (1986), pp. 215–235.

3. J. H. H. Chalk, *On a Congruence related to Character Sums*, Canadian Math. Bull., **28**(4) (1985), pp. 431–439.

4. L.-K. Hua, *Enzyklopädie der Mat. Wissenschaften*, Band 1_2, Heft 13, Teil 1; B.13.

5. L.-K. Hua, *Additive Primzahltheorie*, (Teubner, Leipzig), 1959.

UNIVERSITY OF TORONTO,
TORONTO, ONT. M5S 1A1

https://doi.org/10.4153/CMB-1987-037-4 Published online by Cambridge University Press