Can. J. Math., Vol. XXXI, No. 3, 1979, pp. 476–487

MEAN VALUES OF CHARACTER SUMS

H. L. MONTGOMERY AND R. C. VAUGHAN

1. Introduction. For a non-principal Dirichlet character χ modulo q, let

$$M(\chi) = \max_N \left|\sum_1^N \chi(n)\right|.$$

The Pólya-Vingradov inequality asserts that $M(\chi) < q^{1/2}\log q$; see [**7**]. In the opposite direction it is a trivial consequence of Lemma 1 below and Parseval's identity that if χ is primitive modulo q, then

$$M(\chi) > q^{1/2}/\pi\sqrt{2}.$$

We show that on average the latter of these estimates is the more precise.

THEOREM 1. *For any real* $k > 0$,

$$\sum_{\chi\neq\chi_0} M(\chi)^{2k} \ll_k \phi(q)q^k$$

where the summation is over all non-principal characters modulo q.

THEOREM 2. *For any* $k > 0$,

$$\sum_{2<p\leqq P} \max_N \left|\sum_{n=1}^{N}\left(\frac{n}{p}\right)\right|^{2k} \ll_k \pi(P)P^k.$$

As an immediate consequence of the above for any fixed k we have the following:

COROLLARY. *Suppose that* $0 < \theta < 1$. *Then there is a constant* $C(\theta)$ *such that*
(*i*) *for at least* $\theta\phi(q)$ *of the non-principal characters modulo q we have*

$$M(\chi) \leqq C(\theta)q^{1/2}$$

and
(*ii*) *for at least* $\theta\pi(P)$ *of the prime numbers not exceeding P we have*

$$\max_N \left|\sum_{n=1}^{N}\left(\frac{n}{p}\right)\right| \leqq C(\theta)p^{1/2}.$$

The authors are happy to thank Professors D. A. Burgess, C. Hooley, and A. Selberg for their fruitful suggestions.

2. Lemmata. Our argument uses the Fourier expansion for character sums which was first given by Pólya [**8**] and which we state in the following form.

Received June 21, 1977. This research was supported by the Alfred P. Sloan Foundation and the Institute for Advanced Study.

LEMMA 1. *If χ is a primitive character modulo q, $q > 1$, then for real u and v with $u < v$ we have*

$$\sum_{uq<n\leqq vq} \chi(n) = \tau(\chi) \sum_{0<|h|\leqq H} \bar{\chi}(h) \frac{e(-hu) - e(-hv)}{2\pi i h} + O(1 + qH^{-1}\log q).$$

Here $\tau(\chi)$ is the Gaussian sum, and $|\tau(\chi)| = \sqrt{q}$.

We also require an estimate of Burgess [**2**] for character sums over short intervals.

LEMMA 2. *Let p be an odd prime number. Then for any real $u, v \geqq 1$,*

$$\sum_{u<n\leqq u+v} \left(\frac{n}{p}\right) \ll v^{1/2}p^{3/16} \log p.$$

In the proof of Theorem 1 we make use of the following well known identity which is immediate from the orthogonality of characters modulo q.

LEMMA 3. *Let the a_n be arbitrary complex numbers and $\sum_\chi$ denote a sum extended over all characters modulo q. Then, for any M, $N > 0$ we have*

$$\sum_\chi \left| \sum_{n=M+1}^{M+N} a_n \chi(n) \right|^2 = \phi(q) \sum_{\substack{h=1 \\ (h,q)=1}}^{q} \left| \sum_{n\equiv h(\mathrm{mod}\ q)} a_n \right|^2.$$

In Lemmas 6 and 9 we establish corresponding estimates for use in the proof of Theorem 2. In place of Lemmas 4–9 we could simply quote the weaker Lemmas 10 and 11 of Elliott [**3**]. However, we prove the stronger results because of the desirability of having basic tools in as sharp a form as possible. We begin by extending an estimate of L. K. Hua (see (7) of Bateman and Chowla [**1**]).

LEMMA 4. *If χ is a non-principal character modulo q and $\chi(-1) = 1$, then*

$$\sum_{n\leqq x} (x - n)\chi(n) \ll q^{1/2} \min (q, x).$$

Proof. Suppose first that χ is primitive modulo q. In Lemma 1 we take $u = 0$, integrate with respect to $t = vq$ from 0 to x, and let H tend to infinity. Then

$$\sum_{n\leqq x} (x - n)\chi(n) = (q\tau(\chi)/2\pi^2) \sum_{h=1}^{\infty} (\bar{\chi}(h)/h^2)(1 - \cos 2\pi hx/q) + O(x).$$

Since $1 - \cos \theta \ll \min (1, \theta^2)$ the first expression on the right is

$$\ll q^{3/2} \sum_{h=1}^{\infty} h^{-2} \min (1, h^2x^2q^{-2})$$
$$\ll \min (q^{3/2}, xq^{1/2}).$$

This deals with the case when χ is primitive. When χ is imprimitive, suppose that χ is induced by the primitive character χ^* modulo r, so that $q = rs$. Then

$$\begin{aligned}\sum_{n\leqq x}(x-n)\chi(n) &= \sum_{\substack{n\leqq x\\(n,s)=1}}(n-x)\chi^*(n)\\ &= \sum_{t\mid s}\mu(t)t\chi^*(t)\sum_{m\leqq x/t}((x/t)-m)\chi^*(m)\\ &\ll \sum_{t\mid s} t\min\left(r^{3/2},\frac{x}{t}r^{1/2}\right)\ll \min\,(q^{3/2}, xq^{1/2}).\end{aligned}$$

For the exposition of the following lemmas we introduce the summation convention $\sum_d{}'$ to denote a sum restricted to quadratic discriminants d, namely those integers, both positive and negative, that either lie in the residue class 1 modulo 4 and are square free or are of the form $4D$ where $D \equiv 2$ or 3 (mod 4) and D is square free. Associated with each such d is a primitive quadratic character, $\chi_d(n) = (d/n)$, the Kronecker symbol. Note that we include $d = 1$ as a quadratic discriminant.

LEMMA 5. *For arbitrary complex numbers c_d we have*

$$\begin{aligned}&\textstyle\sum_{n\leqq x}(x-n)\left|\sum'_{0<d\leqq D}c_d\chi_d(n)\right|^2\\ &= (x^2/2)\textstyle\sum'_{0<d\leqq D}|c_d|^2\phi(d)/d + O(x(\sum_{0<d\leqq D}|c_d|d^{1/2})^2).\end{aligned}$$

A similar conclusion also holds when we replace the d with $0 < d \leqq D$ by those with $-D \leqq d < 0$.

Proof. The left hand side is

$$S = \textstyle\sum'_{d_1,d_2}c_{d_1}\bar{c}_{d_2}\sum_{n\leqq x}(x-n)\chi_{d_1}\chi_{d_2}(n).$$

When $d_1 \neq d_2$, $\chi_{d_1}\chi_{d_2}$ is non-principal. Moreover $\chi_{d_1}\chi_{d_2}(-1) = 1$ since d_1 and d_2 have the same sign. Hence, by Lemma 4,

$$\begin{aligned}S &= \sum_{0<d\leqq D}{}' |c_d|^2\sum_{\substack{n\leqq x\\(n,d)=1}}(x-n) + 0\left(x\sum_{d_1\neq d_2}{}'|c_{d_1}c_{d_2}|d_1^{1/2}d_2^{1/2}\right)\\ &= \sum_{0<d\leqq D}{}'|c_d|^2\left(\tfrac{1}{2}x^2\frac{\phi(d)}{d}+0(x2^{\omega(d)})\right)+0\left(x\left(\sum_{0<d\leqq D}{}'|c_d|d^{1/2}\right)^2\right).\end{aligned}$$

Clearly the first error term is majorized by the second.

LEMMA 6. *Let the a_n be arbitrary complex numbers and write*

$$S = \sum_{2<p\leqq P}\left|\sum_{n=1}^{N}a_n\left(\frac{n}{p}\right)\right|^2.$$

Then

(1) $\quad S \ll P\sum_{s\leqq N}\mu(s)^2(\sum_m|a_{sm^2}|)^2 + (\sum_n|a_n|n^{1/2})^2$

and consequentially

(2) $\quad S \ll (P+N^2)\sum_{s\leqq N}\mu(s)^2(\sum_m|a_{sm^2}|)^2.$

Proof. For each integer n ($\neq 0$) we can write $4n$ uniquely in the form dr^2 where d is a quadratic discriminant. Let

$$c_d = \sum_{\substack{n=1 \\ 4n=dr^2}}^{N} a_n.$$

We have $(n/p) = (d/p)$ unless $p|r$. Hence

$$(3) \quad \sum_{n=1}^{N} a_n \left(\frac{n}{p}\right) = \sideset{}{'}\sum_{0<d\leqq 4N} c_d \left(\frac{d}{p}\right) + 0\left(\sum_{\substack{n=1 \\ p^2|n}}^{N} |a_n|\right).$$

The error term here is easily estimated in mean square by observing that

$$\sum_{p\leqq P} \left(\sum_{\substack{n=1 \\ p^2|n}}^{N} |a_n|\right)^2 \ll \sum_{m,n} |a_m a_n| \sum_{\substack{p \\ p^2|(m,n)}} 1 \ll \left(\sum_{n=1}^{N} |a_n| \log n\right)^2.$$

For the main term we use Lemma 5. Thus

$$\sum_{p\leqq P} \left| \sideset{}{'}\sum_{0<d\leqq 4N} c_d \left(\frac{d}{p}\right) \right|^2 \ll P \sum_{0<d\leqq 4N} |c_d|^2 + \left(\sideset{}{'}\sum_{0<d\leqq 4N} |c_d| d^{1/2}\right)^2$$
$$\ll P \sum_{k\leqq N} \mu(k)^2 \left(\sum_m |a_{km^2}|\right)^2 + \left(\sum_n |a_n| n^{1/2}\right)^2.$$

These estimates with (3) give (1). The second bound (2) follows from (1) by observing that Cauchy's inequality gives

$$\left(\sum\nolimits_n |a_n| n^{1/2}\right)^2 \leqq \left(\sum\nolimits_n n\right)\left(\sum\nolimits_n |a_n|^2\right) \leqq N^2 \sum\nolimits_k \mu(k)^2 \left(\sum\nolimits_m |a_{km^2}|\right)^2.$$

LEMMA 7. *Let f be a real-valued arithmetic function and put $g(n) = \sum_{k|n} f(k)$. Suppose that $f(n) = 0$ for all $n > y$ and $g(n) \geqq 0$ for all n. Then for any q we have*

$$(4) \quad 0 \leqq \sum_{\substack{n \\ (n,q)=1}} \frac{f(n)}{n} \leqq \frac{q}{\phi(q)} \sum_n \frac{f(n)}{n}.$$

A special case of this occurs in Hooley [**5**]. If $g(n) \leqq 0$ for all n, then the chain of inequalities (4) are reversed, as is easily seen by replacing f by $-f$.

Proof. Let $\mathscr{D}$ be the set of those integers none of whose prime factors exceed y, and let $\mathscr{D}(q) = \{k: k \in \mathscr{D}, (k, q) = 1\}$. Then

$$\sum_{\substack{n \\ (n,q)=1}} \frac{f(n)}{n} = \sum_{n\in\mathscr{D}(q)} \frac{f(n)}{n} = \sum_{n\in\mathscr{D}(q)} \frac{1}{n} \sum_{r|n} \mu(n/r) g(r)$$
$$= \sum_{m\in\mathscr{D}(q)} \frac{\mu(m)}{m} \sum_{r\in\mathscr{D}(q)} \frac{g(r)}{r}$$
$$(5) \quad = \left(\prod_{\substack{p\leqq y \\ p\nmid q}} \left(1 - \frac{1}{p}\right)\right) \sum_{r\in\mathscr{D}(q)} \frac{g(r)}{r}.$$

https://doi.org/10.4153/CJM-1979-053-2 Published online by Cambridge University Press

The left hand inequality in (4) is immediate on taking $q = 1$. The right hand one follows on observing that

$$\left(\prod_{\substack{p\leqq y\\ p\nmid q}}\left(1-\frac{1}{p}\right)\right)\sum_{r\in\mathscr{D}(q)}\frac{g(r)}{r}\leqq\frac{q}{\phi(q)}\left(\prod_{p\leqq y}\left(1-\frac{1}{p}\right)\right)\sum_{r\in\mathscr{D}}\frac{g(r)}{r}$$

and then applying (5) with $q = 1$.

LEMMA 8. *Let the real numbers λ_m be such that $\lambda_m = 0$ whenever $m > z$. Then for any q we have*

$$(6)\qquad \sum_{\substack{m,n\\ (mn,q)=1}}\frac{\lambda_m\lambda_n}{[m,n]}\leqq\frac{q}{\phi(q)}\sum_{m,n}\frac{\lambda_m\lambda_n}{[m,n]}.$$

Proof. Let

$$f(r) = \sum_{\substack{m,n\\ [m,n]=r}}\lambda_m\lambda_n.$$

Then $\sum_{r|s} f(r) = (\sum_{m|s}\lambda_m)^2 \geqq 0$. The desired conclusion is then obtained by appealing to Lemma 7 with $y = z^2$.

LEMMA 9. *Suppose that a_n $(n = 1, \ldots, N)$ are arbitrary complex numbers and $P \geqq N^2$. Then*

$$(7)\qquad \sum_{2<p\leqq P}\left|\sum_{n=1}^{N} a_n\left(\frac{n}{p}\right)\right|^2 \ll P\left(\log\frac{2P}{N^2}\right)^{-1}\sum_{s}\mu(s)^2\left(\sum_{m}|a_{sm^2}|\right)^2.$$

Proof. We show that when $P \geqq 4D^2$ we have

$$(8)\qquad \sum_{2<p\leqq P}\left|{\sum_{0<d\leqq D}}' c_d\left(\frac{d}{p}\right)\right|^2 \ll \frac{P}{\log\frac{P}{D^2}}{\sum_{d}}'|c_d|^2,$$

for then (7) follows in the same way that Lemma 6 was obtained from Lemma 5. Let

$$z = (4P/D^2)^{1/3}$$

and for m with $1 \leqq m \leqq z$ let λ_m be real with $\lambda_1 = 1$, while $\lambda_m = 0$ for $m > z$. Then $(\sum_{m|n}\lambda_m)^2 = 1$ whenever n is a prime number greater than z. Hence the left hand side of (8) is at most

$$\sum_{2<p\leqq z}\left|{\sum_{0<d\leqq D}}' c_d\left(\frac{d}{p}\right)\right|^2 + P^{-1}\sum_{0<k\leqq 2P}(2P-k)\left|{\sum_{0<d\leqq D}}' c_d\chi_d(k)\right|^2\left(\sum_{m|k}\lambda_m\right)^2.$$

By Lemma 6, the first term makes an acceptable contribution to (8). The second term is

$$P^{-1}\sum_{m,n}\lambda_m\lambda_n\sum_{\substack{0<k\leqq 2P\\ [m,n]\mid k}}(2P-k)\left|\sum_{0<d\leqq D}{}' c_d\chi_d(k)\right|^2$$

$$=P^{-1}\sum_{m,n}\lambda_m\lambda_n[m,n]\sum_{0<j\leqq 2P/[m,n]}\left(\frac{2P}{[m,n]}-j\right)$$
$$\times\left|\sum_{0<d\leqq D}{}' c_d\chi_d([m,n])\chi_d(j)\right|^2.$$

By Lemma 5 this is

$$2P\sum_{m,n}\frac{\lambda_m\lambda_n}{[m,n]}\sum_{\substack{d\\(mn,d)=1}}{}'|c_d|^2\frac{\phi(d)}{d}+O\left(\left(\sum_m|\lambda_m|\right)^2\left(\sum_d{}'|c_d|d^{1/2}\right)^2\right).$$

In the first term we take the sum over d outside, and apply Lemma 8. Thus the above is

$$\ll (P\textstyle\sum_{m,n}(\lambda_m\lambda_n/[m,n])+D^2(\sum_m|\lambda_m|)^2)\sum_d{}'|c_d|^2.$$

In Selberg's method it is well-known ([**4**, pp. 97-103]) that real numbers λ_m can be chosen such that $\lambda_1=1$, $\lambda_m=0$ $(m>z)$, $|\lambda_m|\leqq 1$ $(m\leqq z)$ and

$$\textstyle\sum_{m,n}\lambda_m\lambda_n/[m,n]\leqq 1/\log z.$$

This gives the desired result.

LEMMA 10. *Let k be a positive integer and y be a real number with $y\geqq 1$. Then*

(9) $$\textstyle\sum_{s=1}^{\infty}\left(\sum_{m=1}^{\infty}d_k(m^2s)\min(y^{-1},m^{-2}s^{-1})\right)^2\ll_k y^{-1}(\log 2y)^{2k^2+k-2}.$$

Here d_k is the k-th division function determined by the relation

$$\textstyle\sum d_k(n)n^{-s}=\zeta(s)^k.$$

Proof. Note that $d_k(ab)\leqq d_k(a)d_k(b)$, that

$$\textstyle\sum_{m\leqq x}d_k(m^2)\ll_k x(\log 2x)^{\frac{1}{2}(k^2+k-2)}$$

and that

(10) $$\textstyle\sum_{s\leqq x}d_k(s)^2\ll_k x(\log 2x)^{k^2-1}.$$

Then the left hand side of (9) is

$$\ll_k \textstyle\sum_s d_k(s)^2(\sum_m d_k(m^2)\min(y^{-1},m^{-2}s^{-1}))^2$$
$$\ll_k (\log 2y)^{k^2+k-2}\textstyle\sum_s d_k(s)^2s^{-1}\min(y^{-1},s^{-1})$$
$$\ll_k (\log 2y)^{2k^2+k-2}y^{-1}.$$

3. Proof of theorem 1. By Hölder's inequality we see that the assertion becomes stronger as k increases through real values. Hence it suffices to prove

https://doi.org/10.4153/CJM-1979-053-2 Published online by Cambridge University Press

the assertion for a sequence of k tending to infinity. We consider integral $k \geqq 2$. In the proof we allow implicit constants to depend on k. We shall show that for $q > 1$ we have

(11) $\sum_\chi^* M(\chi)^{2k} \ll \phi(q) q^k$

where $\sum^*$ denotes a sum over the primitive characters modulo q. The deduction of the theorem from this is straightforward. For let χ be a character modulo q, let χ^*, modulo r, be the primitive character which induces χ and let $s = q/r$. Then

$$\begin{aligned}\sum_{\chi \neq \chi_0} M(\chi)^{2k} &\ll \sum_{r|q, r>1} d(q/r)^{2k} \sum_{\chi \bmod r}^* M(\chi)^{2k} \\ &\ll \sum_{r|q} d(q/r)^{2k} r^k \phi(r) \\ &\ll q^k \phi(q) \sum_{s|q} d(s)^{2k}/s^k \\ &\ll q^k \phi(q).\end{aligned}$$

In order to deal with character sums of varying lengths we use a technique which is already found in the work of Menchov and Rademacher. Let

$$\mathscr{A} = \{a2^{-R}: a \in \mathbf{Z}, 0 \leqq a < 2^R\}$$

where R is an integer to be chosen later. For $\alpha \in \mathscr{A}$ we write $\alpha = \sum_1^R \epsilon_r 2^{-r}$ with $\epsilon_r = \epsilon_r(\alpha) = 0$ or 1. Let $\nu_1 = 0$, and for $r > 1$ let

$$\nu_r = \nu_r(\alpha) = 2^r \sum_1^{r-1} \epsilon_m 2^{-m}.$$

Then $\nu_r < 2^r$ and the interval $(0, \alpha]$ is a disjoint union of intervals $(\nu_r 2^{-r}, (\nu_r + \epsilon_r)2^{-r}]$, $1 \leqq r \leqq R$. Choose $N = N(\chi)$ so that $N \leqq q$ and $|\sum_1^N \chi(n)| = M(\chi)$. Then there is an $\alpha \in \mathscr{A}$ with $\alpha = \alpha(\chi)$ and such that $N \leqq \alpha q < N + q2^{-R}$. Hence

(12) $M(\chi) \leqq |\sum_{n \leqq \alpha q} \chi(n)| + q2^{-R}.$

We take $R = [\frac{1}{2}(\log q)/\log 2]$. Thus to prove (11) it suffices to show that

(13) $\sum_\chi^* |\sum_{n \leqq \alpha q} \chi(n)|^{2k} \ll \phi(q) q^k$

(where, of course, $\alpha = \alpha(\chi)$ is as above).

By Hölder's inequality

$$|\sum_{n \leqq \alpha q} \chi(n)|^{2k} = |\sum_{r=1}^R \sum_{\nu_r 2^{-r} q < n \leqq (\nu_r + \epsilon_r) 2^{-r} q} \chi(n)|^{2k}$$

(14) $\leqq (\sum_r r^{-2k/(2k-1)})(\sum_r r^{2k} |\sum_{\nu_r 2^{-r} q < n \leqq (\nu_r + \epsilon_r) 2^{-r} q} \chi(n)|^{2k}).$

Now χ is primitive, so by Lemma 1

$$\sum_{\nu_r 2^{-r} q < n \leqq (\nu_r + \epsilon_r) 2^{-r} q} \chi(n) \ll q^{1/2}(|\sum_{0<h \leqq H} \chi(h) e(h\nu_r/2^r) a(h)| + |\sum_{0<h\leqq H} \bar{\chi}(h) e(h\nu_r/2^r) a(h)|) + 1 + qH^{-1} \log q,$$

where

(15) $a(h) = a(h, r) = (1/h)(e(h/2^r) - 1) \ll \min(2^{-r}, h^{-1}).$

Thus, by (14),

$$\sum_\chi^* |\sum_{n\leqq\alpha q}\chi(n)|^{2k} \ll \sum_\chi^* \sum_r r^{2k}(q^k|\sum_{0<h\leqq H}\chi(h)e(h\nu r/2^r)a(h)|^{2k} + 1 + (qH^{-1}\log q)^{2k}).$$

The last two terms contribute

$$\ll \phi(q)R^{2k+1}(1 + (qH^{-1}\log q)^{2k}).$$

This is acceptable provided that $H = q^{\frac{1}{2}}(\log q)^3$.

In order to obviate the dependence of ν_r on χ we sum over all possible ν. We make no further use of the χ being primitive so we also permit χ to run over all characters modulo q. Therefore, to establish (13) it suffices to show that

$$(16)\quad \sum_\chi \sum_{r=1}^{R} \sum_{\nu=0}^{2^r-1} r^{2k}\left|\sum_{0<h\leqq H}\chi(h)e(h\nu 2^{-r})a(h)\right|^{2k} \ll \phi(q).$$

We now write

$$(17)\quad (\sum_{0<h\leqq H}\chi(h)e(h\nu 2^{-r})a(h))^k = \sum_{h\leqq H^k}\chi(h)b(h),$$

where, by (15),

$$(18)\quad b(h) = b_k(h; r, \nu) \ll d_k(h)\min(2^{-kr}, h^{-1}).$$

Thus, by Lemma 3,

$$\sum_\chi |\sum_{h\leqq H^k}\chi(h)b(h)|^2 \ll \phi(q) \sum_{h=1}^{q}[\sum_{m=0}^{qk} d_k(h+mq) \times \min(2^{-kr}, (h+mq)^{-1})]^2.$$

For $m \leqq q^k$ we have $d_k(h+mq) \ll q^\epsilon$. On considering separately the cases $m = 0$ and $m > 0$ we obtain

$$\sum_\chi |\sum_{h\leqq H^k}\chi(h)b(h)|^2 \ll \phi(q) \sum_{h=1}^{q} d_k(h)^2\min(2^{-2kr}, h^{-2}) + \phi(q) \sum_{h=1}^{q}(q^{-1+\epsilon}\sum_{m=1}^{qk} 1/m)^2 \ll \phi(q)2^{-kr}r^{k^2-1} + q^{3\epsilon}$$

in view of (10). We have assumed that $k \geqq 2$ and we have chosen R so that $2^R \geqq q^{1/2}$. Thus the left hand side of (16) is

$$\ll \sum_{r=1}^{R} r^{2k}2^r(\phi(q)2^{-kr}r^{k^2-1} + q^{3\epsilon})$$
$$\ll \phi(q) + q^{4\epsilon}2^R$$
$$\ll \phi(q)$$

as required.

4. Proof of theorem 2. We proceed as in the proof of Theorem 1, but we require several new ideas to compensate for the weakness of Lemma 6. We define $\mathscr{A}$ as before. Then, for a given $N = N(p)$ there is an $\alpha = \alpha(p)$ such

https://doi.org/10.4153/CJM-1979-053-2 Published online by Cambridge University Press

that $N \leqq \alpha p < N + p2^{-R}$. Thus

$$\max_N \left| \sum_{n=1}^{N} \left(\frac{n}{p}\right) \right| \leqq \left| \sum_{n \leqq \alpha p} \left(\frac{n}{p}\right) \right| + \left| \sum_{N(p) < n \leqq \alpha p} \left(\frac{n}{p}\right) \right|.$$

By Lemma 2 the last term is $\ll p^{11/16} 2^{-\frac{1}{2}R} \log p$. If R is chosen so that

$$P^{3/8}(\log P)^2 \leqq 2^R < 2P^{3/8}(\log P)^2,$$

then this is $\ll p^{1/2}$ whenever $p \leqq P$. Thus it suffices to show that for $\alpha \in \mathscr{A}$, $\alpha = \alpha(p)$ we have

$$\sum_{p \leqq P} \left| \sum_{n \leqq \alpha p} \left(\frac{n}{p}\right) \right|^{2k} \ll \pi(P) P^k.$$

As in the proof of Theorem 1 we define $\nu_r = \nu_r(p)$, $\epsilon_r = \epsilon_r(p)$, and appeal to Lemma 1 with $H = P^{1/2} (\log P)^3$. Corresponding to (16) we now have to show that

$$(19) \quad \sum_{2 < p \leqq P} \sum_{r=1}^{R} r^{2k} \sum_{\nu=0}^{2^r - 1} \left| \sum_{0 < h \leqq H} \left(\frac{h}{p}\right) e\left(\frac{h\nu}{2^r}\right) a(h) \right|^{2k} \ll \pi(P).$$

Here $a(h) = a(h, r)$ is given by (15), and we note the trivial bound

$$(20) \quad \sum_{0 < h \leqq H} \left(\frac{h}{p}\right) e\left(\frac{h\nu}{2^r}\right) a(h) \ll \sum_{0 < h \leqq H} h^{-1} \ll \log P.$$

In (19) we first consider the contribution from those h which are relatively large, say $H(r) < h \leqq H$, where $H(r)$ is to be defined. We apply (20) to $2k - 2$ of the $2k$ factors. Hence this range of h contributes to (19) an amount

$$(21) \quad \ll (\log P)^{4k-2} \sum_{r=1}^{R} \sum_{\nu=0}^{2^r - 1} \sum_{2 < p \leqq P} \left| \sum_{H(r) < h \leqq H} \left(\frac{h}{p}\right) e\left(\frac{h\nu}{2^r}\right) a(h) \right|^2.$$

By (2) of Lemma 6 we see that the sum over p is

$$\ll (P + H^2) \textstyle\sum_{s \leqq H} \left(\sum_{m, sm^2 > H(r)} |a(sm^2)|\right)^2$$
$$\ll H^2 \textstyle\sum_s \left(\sum_{m, sm^2 > H(r)} s^{-1} m^{-2}\right)^2.$$

By Lemma 10 with $y = H(r)$, $k = 1$, this is

$$\ll H^2 H(r)^{-1} \log H$$
$$\ll H(r)^{-1} P (\log P)^7.$$

We take

$$(22) \quad H(r) = 2^r (\log P)^{4k+7}.$$

Then the expression in (21) is $\ll \pi(P)$.

When $h \leqq H(r)$ we distinguish two cases, $r \leqq R_1$ and $R_1 < r \leqq R$ where R_1 is chosen below. We first of all consider the contribution to (19) when $r \leqq R_1$ and $h \leqq H(r)$. Clearly (17) holds with H replaced by $H(r)$, $\chi(h)$ by (h/p), and

https://doi.org/10.4153/CJM-1979-053-2 Published online by Cambridge University Press

then (18) holds. If, say,

(23) $H(r)^k \leqq P^{1/3}$.

Then by (18) and Lemma 9 we have

$$\sum_{2<p\leqq P} \left| \sum_{0<h\leqq H(r)} \left(\frac{h}{p}\right) e\left(\frac{h\nu}{2^r}\right) a(h) \right|^{2k} \ll \pi(P) \sum_{s=1}^{\infty} \left(\sum_{m=1}^{\infty} d_k(sm^2) \min(2^{-kr}, s^{-1}m^{-2}) \right)^2.$$

By Lemma 10 this is

$$\ll \pi(P) 2^{-kr} r^{2k^2+k-2}.$$

Summing over ν and r we obtain a total contribution in this case of an amount $\ll \pi(P)$ to (19) (since $k \geqq 2$). We determine R_1 so that $H(r)$, defined by (22), satisfies (23) whenever $r \leqq R_1$. The choice

(24) $R_1 = [(1/4k)(\log P)/\log 2]$

suffices.

We finally consider the terms in (19) with $h \leqq H(r)$, $R_1 < r \leqq R$. We apply (20) to $2k - 4$ of the $2k$ factors. Thus we have to show that

(25) $$(\log P)^{4k-4} \sum_{R_1<r\leqq R} \sum_{2<p\leqq P} \sum_{\nu=0}^{2^r-1} \left| \sum_{0<h\leqq H(r)} \left(\frac{h}{p}\right) e\left(\frac{h\nu}{2^r}\right) a(h) \right|^4 \ll \pi(P).$$

We now make use of the cancellation produced by the factor $e(h\nu 2^{-r})$ as ν varies. Multiplying out the fourth power and taking the sum over ν inside, we find that

$$\sum_{\nu=0}^{2^r-1} \left| \sum_{0<h\leqq H(r)} \left(\frac{h}{p}\right) e\left(\frac{h\nu}{2^r}\right) a(h) \right|^4 = 2^r \sum_{t=1}^{2^r} \left| \sum_{0<h\leqq H(r)^2} \left(\frac{h}{p}\right) c(h; r, t) \right|^2,$$

where

$$c(h; r, t) = \sum_{h_1, h_2} a(h_1) a(h_2),$$

where the sum is constrained by the conditions

$$h_1, h_2 \leqq H(r);\ h_1 h_2 = h;\ h_1 + h_2 \equiv t \pmod{2^r}.$$

Then, by (1),

$$\sum_{2<p\leqq P} \sum_{\nu=0}^{2^r-1} \left| \sum_{0<h\leqq H(r)} \left(\frac{h}{p}\right) e\left(\frac{h\nu}{2^r}\right) a(h) \right|^4$$
$$\ll 2^r P \sum_{t=1}^{2^r} \sum_{\substack{h,h' \\ hh'=\square}} |c(h; r, t) c(h'; r, t)|$$
$$+ 2^r \sum_{t=1}^{2^r} \left(\sum_{0<h\leqq H(r)^2} |c(h; r, t)| h^{1/2} \right)^2 = T_1 + T_2,$$

https://doi.org/10.4153/CJM-1979-053-2 Published online by Cambridge University Press

say. In T_1 we observe that

$$\sum_{t=1}^{2r} \sum_{hh'=\square} |c(h; r, t)c(h'; r, t)| \leqq \sum_{h_1h_2h_3h_4=\square} |a(h_1) \ldots a(h_4)| \ll \sum_s \left(\sum_m d(m^2 s) \min (2^{-2r}, m^{-2}s^{-1})\right)^2.$$

By Lemma 10 this is $\ll 2^{-2r}r^8$. Thus

(26) $T_1 \ll P2^{-r}r^8.$

As for T_2, we have

$$\sum_{0<h\leqq H(r)^2} |c(h; r, t)|h^{\frac{1}{2}} \ll \sum_{0<h_1\leqq H(r)} h_1^{-1/2} \sum h_2^{-1/2},$$

where in the sum over h_2 we have

$$0 < h_2 \leqq H(r) \text{ and } h_2 \equiv t - h_1 \pmod{2^r}.$$

Since $H(r) \geqq 2^r$, the inner sum is $\ll H(r)^{1/2}2^{-r}$. Thus the above is $\ll H(r)2^{-r}$, whence

(27) $T_2 \ll H(r)^2.$

To establish (25) we note that by (22), (24), (26) and (27),

$$(\log P)^{4k-4} \sum_{R_1<r\leqq R}(T_1 + T_2) \ll P(\log P)^{4k-4} \sum_{r>R_1} 2^{-r}r^8 + (\log P)^{12k+10}\, 2^{2R} \ll \pi(P).$$

The principal difficulty in this proof is to give a satisfactory estimate for T_2. In fact there are two other ways in which one might proceed. A. I. Vinogradov [**9**] has sharpened Lemma 2 in such a way that we could take 2^R to be about $P^{1/4+\epsilon}$ in size. Then we could dispense with the cancellation produced by $e(h\nu 2^{-r})$, and replace (27) by the more immediate estimate $T_2 \ll 2^r H(r)^2 \times (\log P)^2$. Alternatively, instead of appealing to Lemma 6 we could use the more complicated bound of Jutila [**6**, Lemma 3]. This would give $T_2 \ll P^{1/2+\epsilon}2^r$, which is acceptable.

References

1. P. T. Bateman and S. Chowla, *Averages of character sums*, Proc. Amer. Math. Soc. *1* (1950), 781–787.

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

3. P. D. T. A. Elliott, *On the mean value of f(p)*, Proc. London Math. Soc. (3) *21* (1970), 28–96.

4. H. Halberstam and H.-E. Richert, *Sieve methods* (Academic Press, London, 1974).

5. C. Hooley, *On the Brun-Titchmarsh theorem*, J. Reine Angew. Math. *255* (1972), 60–79.

6. M. Jutila, *On mean values of Dirichlet polynomials with real characters*, Acta Arithmetica *27* (1975), 191–198.

7. H. L. Montgomery and R. C. Vaughan, *Exponential sums with multiplicative coefficients*, Inventiones Math. *43* (1977), 69–82.

8. G. Pólya, *Über die Verteilung der quadratishen Reste und Nichtreste,* Göttinger Nachrichten, 1918, 21–29.

9. A. I. Vinogradov, *On the symmetry property for sums with Dirichlet characters,* Izv. Akad. Nauk UzSSR. Ser. Fiz.-Mat. Nauk, 1965, no. 1, 21–27.

Institute for Advanced Study,
Princeton, New Jersey;
Imperial College,
London, England