PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 119, Number 2, October 1993

ESTIMATES FOR CHARACTER SUMS

J. FRIEDLANDER AND H. IWANIEC

(Communicated by William W. Adams)

ABSTRACT. We give a number of estimates for character sums

$$\sum_{a\in\mathscr{A}}\sum_{b\in\mathscr{B}}\chi(a+b)$$

for rather general sets $\mathscr{A}$, $\mathscr{B}$. These give, in particular, a modified proof of the inequalities of Pólya-Vinogradov and of Burgess, which displays the latter as a generalization of the former.

1. INTRODUCTION

Let p be prime and let χ denote a nonprincipal character $(\bmod\, p)$. In this paper we prove a number of estimates for character sums of the form

$$\sum_{a\in\mathscr{A}}\sum_{b\in\mathscr{B}}\chi(a+b), \tag{1}$$

where $\mathscr{A}$ and $\mathscr{B}$ are finite sets of integers, say with cardinality $|\mathscr{A}|$ and $|\mathscr{B}|$. We learned about this problem from H. L. Montgomery and from E. Bombieri, to whom it was suggested by Fan Chung. The techniques we use are simpler than, but bear resemblance to, those that we used in [FI] and thus have been influenced by work of Vinogradov, Burgess, and Karatsuba. In §2 we record some estimates for complete character sums that will be required in our proofs.

The most important special case of the sums (1) is

$$S_\chi=\sum_{M<a<M+A}\chi(a).$$

The first fundamental bound given for S_χ was the Pólya-Vinogradov Theorem [P, V]:

Theorem 1. *We have* $S_\chi \ll p^{1/2}\log p$.

In §3 we give a proof of this estimate, which is somewhat different than earlier proofs. It also generalizes to sums (1) of special type. We say that the set $\mathscr{D}$ of integers is A-spaced modulo p if $|(d_1-d_2) \bmod p|>A$ whenever $d_1\neq d_2$ in $\mathscr{D}$. The argument we give in §3 yields

Received by the editors May 2, 1991 and, in revised form, February 14, 1992.
1991 *Mathematics Subject Classification*. Primary 11L40.

Theorem 1′. *If $\mathscr{D}$ has cardinality $|\mathscr{D}|$ and is A-spaced modulo p, then*

$$\sum_{M<a<M+A}\ \sum_{d\in\mathscr{D}} \chi(a+d) \ll (|\mathscr{D}|p)^{1/2}\log p.$$

In §4 we give a proof of the Burgess estimate [B2]:

Theorem 2. *For any integer $r \geq 1$, and any $\varepsilon > 0$ we have*

$$S_\chi \ll A^{1-1/r}p^{(r+1)/4r^2+\varepsilon}, \tag{2}$$

where the implied constant depends on r and ε.

As with Theorem 1 our proof is somewhat different than the earlier proofs and it can be generalized as above to

Theorem 2′. *Let $\mathscr{D}$ be A-spaced modulo p and assume $\mathscr{D}$ lies in an interval of length D with $AD < p^{1+1/2r}$. Then*

$$\sum_{M<a<M+A}\ \sum_{d\in\mathscr{D}} \chi(a+d) \ll |\mathscr{D}|^{1-1/2r}A^{1-1/r}p^{(r+1)/4r^2+\varepsilon}.$$

Burgess [B2] actually gives the estimate (2) with p^ε replaced by $\log p$. In §4 we also give an elementary combinatorial lemma, which allows us to replace p^ε by the slightly weaker factor $(\log p)^{1+1/2r}$. We note that the use of this lemma in conjunction with the earlier proof of Iwaniec [F] leads, in case $r \geq 2$, to $(\log p)^{1/2r}$ slightly improving both of the above.

In §5 we consider a rather general sum of type (1). We suppose that we have two sequences $\mathscr{A} \subset (M, M+A)$ and $\mathscr{B} \subset (N, N+B)$ of cardinality $|\mathscr{A}|$ and $|\mathscr{B}|$ respectively.

Theorem 3. *Suppose $AB \leq p$ and $B \leq A$. For $r \geq 1$ an integer and $\varepsilon > 0$, we have*

$$\sum_{a\in\mathscr{A}}\sum_{b\in\mathscr{B}} \chi(a+b) \ll A^{1/2}|\mathscr{A}|^{1/2}|\mathscr{B}|\left(\frac{(A+p^{1/2r}B)B}{A^2|\mathscr{B}|^2}\right)^{1/4r} p^{1/8r+\varepsilon} + |\mathscr{A}|^{1/2}|\mathscr{B}|^{1/2}(A+p^{1/2r}B)^{1/2}, \tag{3}$$

the implied constant depending on r and ε.

We remark that our method applies more generally giving the following result.

Theorem 3′. *Let λ_a and μ_b be bounded. Then, under the conditions of Theorem 3, the estimate* (3) *holds also for the weighted sum*

$$\sum_{a\in\mathscr{A}}\sum_{b\in\mathscr{B}} \lambda_a\mu_b\chi(a+b).$$

Let S denote the sum on the left-hand side of (3). The following corollaries of Theorem 3 are immediate.

Corollary 1. *Suppose $\mathscr{A} = \mathscr{B}$ and $A \ll p^{1/2}$. Then*

$$S \ll A^{1/2}|\mathscr{A}|^{3/2-1/2r}p^{(r+1)/8r^2+\varepsilon} + A^{1/2}|\mathscr{A}|p^{1/4r}.$$

Moreover, if for some $r \geq 2$, $|\mathscr{A}| > A^{r/(r+1)}p^{1/4r+\varepsilon}$ then, with some $\delta = \delta(\varepsilon, r) > 0$, we have

$$S \ll |\mathscr{A}|^2p^{-\delta}. \tag{4}$$

In particular, (4) holds whenever we have

$$|\mathscr{A}| > p^{11/24+\varepsilon}. \tag{5}$$

Corollary 2. *Suppose $p^\varepsilon \le B \le A$ and $p^{1/2+\varepsilon} < AB \le p$. Then, for some $\delta = \delta(\varepsilon) > 0$, for all sets $\mathscr{A}$, $\mathscr{B}$ contained in intervals of length A, B and satisfying $|\mathscr{A}| > Ap^{-\delta}$, $|\mathscr{B}| > Bp^{-\delta}$, we have $S \ll |\mathscr{A}|\,|\mathscr{B}|p^{-\delta}$, where the implied constant depends only on ε.*

We also have the following corollary of Theorem 3′.

Corollary 3. *Let ψ be an additive character. Suppose $p^{1/4+\varepsilon} < N < p^{1/2}$. We then have*

$$\sum_{M<n<M+N} \chi(n)\psi(n) \ll Np^{-\delta},$$

with some $\delta = \delta(\varepsilon) > 0$, the implied constant depending on ε only.

Proof. The sum is equal to

$$\begin{aligned} K^{-1} & \sum_{\substack{M<n<M+N \\ 0\le k<K}} \chi(n+k)\psi(n+k) + O(K) \\ &= K^{-1} \sum_{\substack{M<n<M+N \\ 0\le k<K}} \chi(n+k)\psi(n)\psi(k) + O(K) \\ &\ll K^{-1}NKp^{-\delta} + K \ll Np^{-\delta} \end{aligned}$$

on taking $K = Np^{-\delta}$.

2. Complete character sums

We require the following estimates, which, as is well known, follow from the work of Weil, see [B1].

Let χ be a nonprincipal character $\bmod p$ of order k, let $r \ge 1$ be an integer, and let $\mathbf{c} = (c_1, \dots, c_r)$, $\mathbf{c}' = (c_1', \dots, c_r')$ be r-tuples of integers such that the rational function $P_{\mathbf{c}}(u)/P_{\mathbf{c}'}(u)$ is not a kth power modulo p, where $P_{\mathbf{c}}$ is the polynomial given by $P_{\mathbf{c}}(u) = (u+c_1)\cdots(u+c_r)$, and similarly for $P_{\mathbf{c}'}$.

Then we have

$$\sum_{u (\bmod p)} \chi(P_{\mathbf{c}}(u))\overline{\chi}(P_{\mathbf{c}'}(u)) \ll p^{1/2} \tag{6}$$

and

$$\sum_{u (\bmod p)} \chi(P_{\mathbf{c}}(u)P_{\mathbf{c}}(u-1))\overline{\chi}(P_{\mathbf{c}'}(u)P_{\mathbf{c}'}(u-1)) \ll p^{1/2} \tag{7}$$

where the implied constants may depend only on r.

We shall use the latter estimate in our proof of Theorem 3 and (as is customarily the case) we shall use (6) in the proof of the Burgess estimate. For $r = 1$, the sum in (6) is the Jacobsthal sum and is bounded; we use this elementary fact in our proof of the Pólya-Vinogradov estimate.

3. The Pólya-Vinogradov estimate

In this section we prove Theorem 1; the modification to Theorem 1′ is immediate. We can assume that $2 \le A < p/2$ and that M and A are integers.

Put

$$f(x) = \min(x - M, 1, M + A - x)$$

in the interval $[M, M+A]$ and $f(x) = 0$ elsewhere. Let g denote the Fourier transform of f,

$$g(y) = \int_{-\infty}^{\infty} f(x)e(-yx)\,dx,$$

so that, on integrating by parts, we have $|g(y)| \le \min(A, |\pi y|^{-1}, (\pi y)^{-2})$, whence

$$\int |g(y)|dy \ll \log A.$$

We obtain

$$\begin{aligned} S_\chi &= \sum_a f(a)\chi(a) = A^{-1} \sum_{M-A<a<M+A} \sum_{1\le b\le A} f(a+b)\chi(a+b) \\ &= A^{-1}\int_{-\infty}^{\infty} g(y) \sum_{M-A<a<M+A} e(ay) \sum_{1\le b\le A} e(by)\chi(a+b)\,dy \\ &\ll A^{-1}(\log p) \sum_{M-A<a<M+A} \left|\sum_{1\le b\le A} e(by)\chi(a+b)\right| \end{aligned}$$

for some $y \in \mathbb{R}$. By Cauchy's inequality we obtain

$$\begin{aligned} S_\chi^2 &\ll (\log p)^2 A^{-1} \sum_{u \bmod p} \left|\sum_{1\le b\le A} e(by)\chi(u+b)\right|^2 \\ &\ll (\log p)^2 A^{-1} \sum_{1\le b_1, b_2\le A} \left|\sum_{u \bmod p} \chi(u+b_1)\overline{\chi}(u+b_2)\right|. \end{aligned}$$

For $b_1 \ne b_2$ the inner sum is bounded and so this is

$$\ll (\log p)^2 A^{-1}(Ap + A^2) \ll p(\log p)^2.$$

Remark. Without any special effort this method gives

$$|S_\chi| \le (1 + o(1))(2/\pi)p^{1/2}\log A.$$

We do not know to what extent this could be improved. The best known values of this constant are given in [H].

4. The Burgess estimate

Here too we just prove Theorem 2; the extension to Theorem 2′ is immediate.

We can assume that $A < p^{1/2+1/4r}$ because otherwise the result follows from Theorem 1. Let $BC = A$. We obtain

$$\begin{aligned} S_\chi &\ll A^{-1} \sum_{M-A<a<M+A} \sum_{1\le b\le B} \left|\sum_{1\le c\le C} f(a+bc)\chi(a+bc)\right| \\ &\le A^{-1} \sum_{M-A<a<M+A} \sum_{1\le b\le B} \int_{-\infty}^{\infty} \frac{1}{b}\left|g\left(\frac{y}{b}\right)\right| \left|\sum_{1\le c\le C} e(cy)\chi(a\overline{b}+c)\right| dy. \end{aligned}$$

We have $|g(y/b)|/b \le \min(A, |y|^{-1}, By^{-2}) = h(y)$, say, and

$$\int_{-\infty}^{\infty} h(y)\,dy \ll \log p;$$

hence,

$$S_\chi \ll A^{-1}(\log p) \sum_{u \bmod p} \nu(u) \left| \sum_{1 \le c \le C} e(cy)\chi(u+c) \right|$$

for some $y \in \mathbb{R}$, where $\nu(u) = \#\{a, b : M - A < a \le M + A,\ 1 \le b \le B,$ $a \equiv bu \bmod p\}$.

We have $\sum_u \nu(u) = 2AB$ and

$$\sum_u \nu^2(u) \ll ABp^\varepsilon \tag{8}$$

provided $AB < p$, which we henceforth assume. Now by Hölder's inequality we obtain

$$S_\chi \ll A^{-1}(\log p) \left(\sum_u \nu(u)\right)^{1-1/r} \left(\sum_u \nu^2(u)\right)^{1/2r} \left(\sum_u \left|\sum_c\right|^{2r}\right)^{1/2r}. \tag{9}$$

By (6) this is

$$\ll A^{-1}(AB)^{1-1/2r}(pC^r + p^{1/2}C^{2r})^{1/2r}p^\varepsilon.$$

We choose $C = p^{1/2r}$ and $B = Ap^{-1/2r}$ giving Theorem 2.

The following lemma (which we proved some years ago and was referred to in [F]) allows the replacement in (8) of p^ε by $\log p$. This in turn gives Theorem 2 with p^ε replaced by $(\log p)^{1+1/2r}$ and, if we use instead the earlier method of Iwaniec [F] (but using Hölder's inequality as in (9) above), gives Theorem 2, for $r \ge 2$, with p^ε replaced by $(\log p)^{1/2r}$.

The method of proof used here for Theorem 2 differs from that in [F] in that an inductive argument there has been rendered unnecessary by the introduction of the smoothing function f. As here, the earlier method can be used to give an estimate of the form $S_\chi \ll p^{1/2+o(1)}$, but we were not able to use it to prove Theorem 1. It is curious that the current method works slightly better for the Pólya-Vinogradov estimate and slightly worse for the Burgess estimate.

Lemma. *Let* $1 \le A \le H$, $2AH < q$, *and*

$$S = \#\left\{ (a_1, a_2, n_1, n_2) \,\middle|\, \begin{array}{l} 1 \le a_1 \le A,\ N < n_1 \le N + H \\ 1 \le a_2 \le A,\ N < n_2 \le N + H \\ a_2 n_1 \equiv a_1 n_2 \ (\bmod q) \end{array} \right\}.$$

Then $S \ll AH \log q$.

Proof. Let $I = (N, N + H]$ and, for $j \in \mathbb{Z}$, let

$$I_j = ((a_2 N - jq)/a_1, (a_2(N + H) - jq)/a_1].$$

Since $AH < \frac{1}{2}q$, it follows that, for given (a_1, a_2), the intervals I_j are pairwise disjoint and that $I \cap I_j$ is nonempty for at most one value $j = j_0 = j_0(a_1, a_2)$. Given a_1, a_2 all quadruples satisfy $n_2 \in I \cap I_j$ for some j and hence $n_2 \in$

$I \cap I_{j_0}$. Once n_2 is also given then n_1 is determined by $a_2 n_1 - a_1 n_2 = j_0 q$. Finally note that for given a_1, a_2 we have (since j_0 is determined) $a_1 n_2 \equiv j_0 q \pmod{a_2}$ so that n_2 lies in at most one residue class $\varepsilon = \varepsilon(a_1, a_2)$ modulo $a_2/(a_1, a_2)$. Thus

$$S \le \sum_{a_1 \le A} \sum_{a_2 \le A} \sum_{\substack{n_2 \in I \cap I_{j_0} \\ n_2 \equiv \varepsilon \ (\mathrm{mod}(a_2/(a_1, a_2)))}} 1 = \sum_{a_1 \le a_2} + \sum_{a_2 < a_1} = S_1 + S_2,$$

say. Now

$$\begin{aligned} S_1 &\le \sum_{a_2 \le A} + \sum_{a_1 \le a_2} \sum_{\substack{n_2 \in I \\ n_2 \equiv \varepsilon (\mathrm{mod}\,(a_2/(a_1, a_2)))}} 1 \\ &\le H \sum_{a_2 \le A} \frac{1}{a_2} \sum_{\delta | a_2} \delta \sum_{\substack{a_1 \le a_2 \\ a_1 \equiv 0 \ (\mathrm{mod}\ \delta)}} 1 + O(A^2) \\ &\le H \sum_{a_2 \le A} \tau(a_2) + O(A^2) \ll AH \log q. \end{aligned}$$

Similarly

$$\begin{aligned} S_2 &\le \sum_{a_1 \le A} \sum_{a_2 \le a_1} \sum_{\substack{n_2 \in I_{j_0} \\ n_2 \equiv \varepsilon (\mathrm{mod}\,(a_2/(a_1, a_2)))}} 1 \\ &\le H \sum_{a_1 \le A} \frac{1}{a_1} \sum_{\delta | a_1} \delta \sum_{\substack{a_2 \le a_1 \\ a_2 \equiv 0 \ (\mathrm{mod}\ \delta)}} 1 + O(A^2), \end{aligned}$$

and this is the same sum that occurred in the estimation of S_1 but with the roles of a_1 and a_2 reversed. This completes the proof.

Remark. Without the assumptions $A \le H$, $2AH < q$, the result becomes

$$S \ll A(1 + q^{-1}AH)(H \log 2A + A).$$

5. A general result

In this section we prove Theorem 3. We can assume $A > p^{1/2r}$, since otherwise the result is trivial. Let S denote the sum to be estimated. By Cauchy's inequality we get

$$\begin{aligned} |S|^2 &\le |\mathscr{A}| \sum_a f(a) \left| \sum_{b \in \mathscr{B}} \chi(a+b) \right|^2 \\ &\le |\mathscr{A}| \sum_{b_1 \ne b_2} \sum_a f(a) \chi(a + b_1) \overline{\chi}(a + b_2) + A |\mathscr{A}|\, |\mathscr{B}|, \end{aligned}$$

where here we have kept the conditions $b_i \in \mathscr{B}$ but enlarged the sum over a to run over all integers. Denote $b = b_1 - b_2$ and make a shift $a \mapsto a - b_1 + bc$

with $0 \le c < C = [AB^{-1}]$. We get

$$\begin{aligned} |S|^2 &\le |\mathscr{A}|C^{-1} \sum_{|a-M-N|<2A} \sum_{b_1 \ne b_2} \left| \sum_c f(a-b_1+bc)\chi(a\bar{b}+c)\bar{\chi}(a\bar{b}+c-1) \right| \\ &\quad + A|\mathscr{A}|\,|\mathscr{B}| \\ &\ll (\log p)|\mathscr{A}|C^{-1} \sum_a \sum_{b_1 \ne b_2} \left| \sum_c e(cy)\chi(a\bar{b}+c)\bar{\chi}(a\bar{b}+c-1) \right| + A|\mathscr{A}|\,|\mathscr{B}| \\ &= (\log p)|\mathscr{A}|C^{-1} \sum_{u \bmod p} \nu(u) \left| \sum_c e(cy)\chi(u+c)\bar{\chi}(u+c-1) \right| + A|\mathscr{A}|\,|\mathscr{B}|, \end{aligned}$$

where $y \in \mathbb{R}$ and $\nu(u)$ is the number of solutions to $a\bar{b} \equiv u \bmod p$ in a and $b = b_1 - b_2$ with $|a - M - N| < 2A$, $b_1 \ne b_2 \in \mathscr{B}$. We have $\sum_u(\nu) \ll A|\mathscr{B}|^2$ and

$$\sum_u \nu^2(u) \ll AB|\mathscr{B}|^2 p^\varepsilon \tag{10}$$

since $AB \le p$. Hence by (7) and Hölder's inequality we get

$$\begin{aligned} |S|^2 &\ll p^\varepsilon |\mathscr{A}|C^{-1}(A|\mathscr{B}|^2)^{1-1/r}(AB|\mathscr{B}|^2)^{1/2r}(pC^r + p^{1/2}C^{2r})^{1/2r} + A|\mathscr{A}|\,|\mathscr{B}| \\ &\ll p^\varepsilon |\mathscr{A}|A^{1-1/2r}B^{1/2r}|\mathscr{B}|^{2-1/r}\left[p^{1/2r}\left(\frac{B}{A}\right)^{1/2} + p^{1/4r}\right] + A|\mathscr{A}|\,|\mathscr{B}|, \end{aligned}$$

whence

$$|S| \ll |\mathscr{A}|^{1/2}|\mathscr{B}|^{1-1/2r}A^{1/4-1/4r}B^{1/4r}(A+p^{1/2r}B)^{1/4}p^{1/8r+\varepsilon} + (A|\mathscr{A}|\,|\mathscr{B}|)^{1/2}. \tag{11}$$

Next we shall refine (11) by a subdivision argument. We divide the interval $[N, N+B]$ into K disjoint subintervals $I_1, \dots, I_K$ of equal length BK^{-1}. Let $\mathscr{B}_j = \mathscr{B} \cap I_j$. We apply (11) for each $\mathscr{B}_j$ separately and add the results. We have

$$\sum |\mathscr{B}_j|^{1-1/4r} \le |\mathscr{B}|^{1-1/4r}K^{1/4r}$$

and

$$\sum |\mathscr{B}_j|^{1/2} \le |\mathscr{B}|^{1/2}K^{1/2}.$$

This gives

$$\begin{aligned} |S| &\ll |\mathscr{A}|^{1/2}|\mathscr{B}|^{1-1/2r}A^{1/4-1/4r}B^{1/4r}K^{1/4r}(A + p^{1/2r}BK^{-1})^{1/4}p^{1/8r+\varepsilon} \\ &\quad + (A|\mathscr{A}|\,|\mathscr{B}|K)^{1/2} \end{aligned}$$

for any K with $1 \le K \le B$. We choose $K = \max(1, A^{-1}Bp^{1/2r})$ getting (3).

Remark. If the sums $a + b$ are not too large, that is, if $M + N \ll A$, then (10) can be improved to $\ll A|\mathscr{B}|^3 p^\varepsilon$. This leads to an improvement of Theorem 3. For example, in (5) the exponent $\frac{11}{24}$ can be replaced by $\frac{9}{20}$.

Note. After writing the first draft of this paper we learned of a paper of Dobrowolski and Williams [DW], which, in particular, gives a proof of the Pólya-Vinogradov inequality using ideas similar to those given here in §3.

Acknowledgment

This work was supported in part by grants from NSERC and NSF and was done while the authors were participating in the number theory programme at the Institute for Advanced Study, Princeton, New Jersey.

References

[B1] D. A. Burgess, *On character sums and primitive roots*, Proc. London Math. Soc. (3) **12** (1962), 179–192.

[B2] ——, *On character sums and L-series*. II, Proc. London Math. Soc. (3) **13** (1963), 524–536.

[DW] E. Dobrowolski and K. S. Williams, *An upper bound for the sum* $\sum_{n=a+1}^{a+H} f(n)$ *for a certain class of functions* f, Proc. Amer. Math. Soc. **114** (1992), 29–35.

[F] J. Friedlander, *Primes in arithmetic progressions and related topics*, Analytic Number Theory and Diophantine Problems (Proc. Conf. Oklahoma State Univ. 1984) (Adolphson, Conrey, Ghosh, and Yager, eds.), Birkhäuser, Boston, PM, 70, 1987, pp. 125–134.

[FI] J. Friedlander and H. Iwaniec, *Incomplete Kloosterman sums and a divisor problem*, Ann. of Math. (2) **121** (1985), 319–350.

[H] A. Hildebrand, *Large values of character sums*, J. Number Theory **29** (1988), 271–296.

[P] G. Pólya, *Über die Verteilung der quadratischen Reste und Nichtreste*, Königl. Ges. Wiss. Göttingen Nachr. (1918), 21–29.

[V] I. M. Vinogradov, *On the distribution of power residues and non-residues*, J. Phys. Math. Soc. Perm Univ. **1** (1918), 94–98; *Selected works*, Springer, Berlin, 1985, pp. 53–56.

Department of Mathematics, University of Toronto, Ontario, Canada M5S 1A1
E-mail address: frdlndr@math.toronto.edu

Department of Mathematics, Rutgers University, New Brunswick, New Jersey 08903
E-mail address: iwaniec@math.rutgers.edu