CHARACTER SUMS AND PRIMITIVE ROOTS IN FINITE FIELDS

by **H. Davenport** (Cambridge, England) and **D. J. Lewis** (Ann Arbor, U. S. A.)

1. Let p be a prime and let χ be a non-principal character modulo p. It was proved independently by Pólya and Vinogradov that

$$\sum_{x=N+1}^{N+H} \chi(x) = O(p^{\frac{1}{2}} \log p) \tag{1}$$

for any N and H, where the implied constant is absolute. This inequality, though exceedingly valuable, fails to give any information if $H < p^{\frac{1}{2}} \log p$, and it was not until recently that a result applicable to a range of smaller values of H was found, namely by Burgess (*). He proved that, for any positive integer r, we have

$$\sum_{x=N+1}^{N+H} \chi(x) = O(H^{\frac{r}{r+1}} p^{\frac{1}{4r}} \log p), \tag{2}$$

where the implied constant is again absolute. This gives a non-trivial estimate for the character sum if $H > p^{\frac{1}{4}+\delta}$ for any fixed $\delta > 0$. Using an argument due to Vinogradov, Burgess deduced from (2) that, subject to the last mentioned condition on H, any interval $N < x \leqslant N + H$ contains asymptotically its due proportion of primitive roots to the modulus p.

(*) «On character sums and primitive roots», *Proc. London Math. Soc.*, (3), 12 (1962), 179-192.

The object of the present paper is to investigate how far these results can be extended to the finite field («Galois field») of p^n elements. This field, which we shall denote by $[p^n]$, has a basis of n elements $\omega_1, \ldots, \omega_n$ relative to the mod p field, and the elements of $[p^n]$ are representable uniquely as

$$\xi = x_1\omega_1 + \cdots + x_n\omega_n, \tag{3}$$

with the x_j in $[p]$. We shall give the x_j rational integral values satisfying $0 \leqslant x_j < p$, and we shall identify the element ξ of $[p^n]$ with the integer point $(x_1, \ldots, x_n)$.

Let $\mathfrak{B}$ be a box in n dimensional space, defined by

$$N_j < x_j \leqslant N_j + H_j \qquad (j = 1, \ldots, n), \tag{4}$$

where the N_j and H_j are integers, satisfying

$$0 \leqslant N_j < N_j + H_j < p \qquad (j = 1, \ldots, n). \tag{5}$$

The Pólya-Vinogradov inequality (1) extends almost immediately to the field $[p^n]$, in the following form:

THEOREM 1. *Let χ be any non-principal character of the multiplicative group formed by the non-zero elements of $[p^n]$. Then*

$$\Big|\sum_{\xi\in\mathfrak{B}}\chi(\xi)\Big| < \big(p^{\frac{1}{2}}(\log p + 1)\big)^n. \tag{6}$$

In this result we do not have to suppose that p is large.

We obtain also an extension of Burgess's inequality (2), but in this case the result becomes less effective as n gets larger. We suppose for simplicity that $H_1 = H_2 = \cdots = H_n = H$, so that the box $\mathfrak{B}$ in (4) becomes a cube $\mathfrak{k}$. We prove:

THEOREM 2. *For any $\delta > 0$ there exists $\delta_1(\delta) > 0$ and $p_1(\delta)$ such that, if*

$$H > p^{\frac{n}{2(n+1)}+\delta} \qquad \textit{and} \qquad p > p_1(\delta), \tag{7}$$

then

$$\Big|\sum_{\xi\in\mathfrak{k}}\chi(\xi)\Big| < (p^{-\delta_1}H)^n. \tag{8}$$

It will be seen that if $n = 1$ the exponent of p in (7) is still $\frac{1}{4} + \delta$, but that as n increases the exponent approaches $\frac{1}{2}$. The reason for this weakening in the result lies in the fact that the parameter q used in Burgess's method (see § 4)

has to be a rational integer and cannot (as far as we can see) be given values in $[p^n]$. It would be possible to replace (8) by an explicit estimate of the form (2), but then the proof would be more complicated.

By the same argument as that used by Burgess (*loc. cit.* § 6) it follows that, *subject to* (7), *the number of primitive roots of* $[p^n]$ *falling in the cube* $\mathfrak{K}$ *is*

$$\frac{\varphi(p^n-1)}{p^n-1}H^n(1+O(p^{-n\delta_1})). \tag{9}$$

We omit the proof. The conclusion may be compared with a result of Davenport (*) which states that for any n there exists $p_0(n)$ such that if $p > p_0(n)$ there is a primitive root of $[p^n]$ of the form $\vartheta + x$, where ϑ is a generating element of $[p^n]$ and $0 \leqslant x < p$.

2. PROOF OF THEOREM 1. Let $e_p(m) = e^{2\pi i m/p}$ for any integer m, and let

$$e(\xi) = e_p(S(\xi))$$

for any ξ in $[p^n]$, where S denotes the trace of an element of $[p^n]$ relative to $[p]$. Let

$$\tau(\chi) = \sum_{\xi \in [p^n]} \chi(\xi) e(\xi),$$

where we make the convention that $\chi(0) = 0$. It is known (Davenport, *loc. cit.*) that $|\tau(\chi)| = p^{\frac{1}{2}n}$ for any non-principal χ.

For any $\lambda \neq 0$ in $[p^n]$ we have

$$\sum_{\xi} \chi(\xi) e(\lambda\xi) = \sum_{\eta} \chi(\lambda^{-1}\eta) e(\eta) = \bar{\chi}(\lambda)\tau(\chi).$$

Hence

$$\chi(\lambda) = \frac{1}{\tau(\bar{\chi})} \sum_{\zeta} \bar{\chi}(\zeta) e(\lambda\zeta),$$

and this continues to hold when $\lambda = 0$. Thus

$$\sum_{\xi \in \mathfrak{B}} \chi(\xi) = \frac{1}{\tau(\bar{\chi})} \sum_{\zeta} \bar{\chi}(\zeta) \sum_{\xi \in \mathfrak{B}} e(\xi\zeta).$$

Now

$$\sum_{\xi \in \mathfrak{B}} e(\xi\zeta) = \sum_{x_1=N_1+1}^{N_1+H_1} \cdots \sum_{x_n=N_n+1}^{N_n+H_n} e_p(S(\zeta(x_1\omega_1 + \cdots + x_n\omega_n)))$$

$$= \prod_{j=1}^{n} \left\{ \sum_{x_j=N_j+1}^{N_j+H_j} e_p(S(\zeta\omega_j)x_j) \right\}.$$

(*) « On primitive roots in finite fields », *Quarterly J. of Math.*, 8 (1937), 308-312.

We have

$$\left|\sum_{x=N+1}^{N+H} e_p(mx)\right| \leqslant \min\left(H, \frac{p}{2\|m\|_p}\right),$$

for any integer m, where $\|m\|_p$ denotes the absolutely least residue of m modulo p. Hence

$$\left|\sum_{\xi\in\mathfrak{B}} \chi(\xi)\right| \leqslant p^{-\frac{1}{2}n} \sum_{\zeta\neq 0} \left\{\prod_{j=1}^{n} \min\left(H_j, \frac{1}{2} p \|S(\zeta\omega_j)\|_p^{-1}\right)\right\}.$$

For any $t_1, \ldots, t_n$ in $[p]$, not all 0, there is just one ζ for which

$$S(\zeta\omega_1) = t_1, \ldots, S(\zeta\omega_n) = t_n.$$

Hence, if $H = \max H_j$,

$$\begin{aligned}\left|\sum_{\xi\in\mathfrak{B}} \chi(\xi)\right| &\leqslant p^{-\frac{1}{2}n}\left(\sum_{t=0}^{p-1} \min\left(H, \frac{1}{2} p \|t\|_p^{-1}\right)\right)^n \\ &\leqslant p^{-\frac{1}{2}n}\left(H + \sum_{1\leq t\leq \frac{1}{2}p} \frac{p}{2t} + \sum_{\frac{1}{2}p<t<p} \frac{p}{2(p-t)}\right)^n \\ &< p^{-\frac{1}{2}n}(p + p\log p)^n.\end{aligned}$$

This proves Theorem 1.

3. LEMMA 1. *Let χ be a non-principal character of $[p^n]$ of order k, where $k|p^n - 1$. Let $B(\xi)$ be a polynomial of the form*

$$B(\xi) = (\xi - \beta_1)^{a_1} \cdots (\xi - \beta_t)^{a_t},$$

where $\beta_1, \ldots, \beta_t$ are distinct elements of $[p^n]$ and $0 < a_j < k$ and

$$a_1 + \cdots + a_t \equiv 0 \pmod{k}.$$

Then

$$\left|\sum_{\xi\in[p^n]} \chi(B(\xi))\right| \leqslant (t-2)p^{\frac{1}{2}n} + 1.$$

PROOF. This is a consequence of Weil's proof of the analogue of the Riemann hypothesis for congruence ζ-functions, the deduction being the same as for Burgess's Lemma 1.

LEMMA 2. *Let r be any positive integer and suppose $0 < h < p$. Let*

$$S_h(\mathfrak{N}) = \sum_{\xi\in\mathfrak{N}} \chi(\xi), \tag{10}$$

where $\mathfrak{N} = (N_1, \ldots, N_n)$ *and* $\mathfrak{k}$ *is the cube* (4) *with* $H_j = h$. *Then*

$$\sum_{x_1=0}^{p-1} \cdots \sum_{x_n=0}^{p-1} |S_h(\mathfrak{x})|^{2r} < (4r)^{r+1} p^n h^{nr} + 2r p^{\frac{1}{2}n} h^{2nr}.$$

PROOF. This is a straightforward extension of Burgess's Lemma 2, based on Lemma 1.

4. PROOF OF THEOREM 2. We have to prove that $S_H(\mathfrak{N})$, defined in (10), satisfies (8). We assume the contrary, namely that

$$|S_H(\mathfrak{N})| \geqslant (p^{-\delta_1} H)^n, \tag{11}$$

and reach a contradiction if δ_1 is suitably chosen in terms of δ. Comparison of (11) with Theorem 1 gives

$$H < p^{\frac{1}{2}+\delta_1}(\log p + 1), \tag{12}$$

and as an inequality for H in the opposite sense we have, of course, the hypothesis (7).

Let q be a prime less than H, and divide the points $\xi = x_1\omega_1 + \cdots + x_n\omega_n$ in the cube $\mathfrak{k} = \mathfrak{k}_H(\mathfrak{N})$ into sets according to the residue classes to which $x_1, \ldots, x_n$ belong modulo q. If $x_j \equiv -t_j p \pmod q$, we put

$$x_j = -t_j p + q z_j,$$

and have

$$\chi(\xi) = \chi(q)\chi(\zeta), \quad \text{where} \quad \zeta = z_1\omega_1 + \cdots + z_n\omega_n.$$

Hence

$$S_H(\mathfrak{N}) = \chi(q) \sum_{t} \sum_{\zeta \in \vartheta(q,t)} \chi(\zeta), \tag{13}$$

where in the outer sum t runs through n complete sets of residues modulo q, and in the inner sum ζ runs through the integer points $(z_1, \ldots, z_n)$ in the box

$$\vartheta(q, t): \frac{N_j + t_j p}{q} < z_j \leqslant \frac{N_j + t_j p + H}{q} \qquad (j = 1, \ldots, n).$$

Two of these boxes with the same q cannot overlap, since $z_1, \ldots, z_n$ determine $t_1, \ldots, t_n$ uniquely. If two boxes $\vartheta(q_1, \mathfrak{t}^{(1)})$ and $\vartheta(q_2, \mathfrak{t}^{(2)})$ overlap, where $q_1 < q_2$, we find that

$$|p(t_j^{(1)} q_2 - t_j^{(2)} q_1) + N_j(q_2 - q_1)| < H q_2 \qquad (j = 1, \ldots, n).$$

Assuming that $Hq_2 < \frac{1}{2}p$, the above inequality implies that for given q_1 and q_2 there is at most one possibility for $t^{(1)}$ and $t^{(2)}$

Let q run through all primes in the interval

$$p^{-\delta_2} H < q < 2p^{-\delta_2} H, \tag{14}$$

where $\delta_2 > 0$ will be chosen later. The number Q of primes q satisfies

$$C_1 H p^{-\delta_2} (\log p)^{-1} < Q < C_2 H p^{-\delta_2} (\log p)^{-1}, \tag{15}$$

where C_1, C_2 are positive absolute constants. The condition $Hq_2 < \frac{1}{2}p$ occurring above is satisfied, by (14) and (12), provided

$$\delta_2 > 3\delta_1 \tag{16}$$

and provided $p > p_2(\delta_1)$.

For each q there are at most $Q - 1$ points t for which the box $\mathfrak{H}(q, t)$ can overlap any other box $\mathfrak{H}(q', t')$. Denote the set of remaining points t, after these are excluded, by $T(q)$. Then (13) and (11) imply that

$$(p^{-\delta_1} H)^n \leqslant \sum_{t \in T(q)} \Big| \sum_{\zeta \in \mathfrak{H}(q,t)} \chi(\zeta) \Big| + Q(p^{\delta_2} + 1)^n,$$

since the number of integer values for each z_j in $\mathfrak{H}(q, t)$ is at most $p^{\delta_2} + 1$. We now suppose that $n \geqslant 2$, since the result of Theorem 2 is already known when $n = 1$. Since $Q < H$ and since H satisfies (7), the last term on the right above is small compared with the term on the left, provided δ_1 and δ_2 are small. Hence

$$\sum_{t \in T(q)} \Big| \sum_{\zeta \in \mathfrak{H}(q,t)} \chi(\zeta) \Big| > \tfrac{1}{2}(p^{-\delta_1} H)^n.$$

Summing over q, we obtain

$$\sum_q \sum_{t \in T(q)} \Big| \sum_{\zeta \in \mathfrak{H}(q,t)} \chi(\zeta) \Big| > \tfrac{1}{2}(p^{-\delta_1} H)^n Q.$$

The boxes $\mathfrak{H}(q, t)$ in this sum are disjoint, and their number is

$$M \leqslant \sum_q q^n < Q(2p^{-\delta_2} H)^n. \tag{17}$$

We can rewrite the previous inequality as

$$\sum_{m=1}^{M} \Big| \sum_{\zeta \in I_m} \chi(\zeta) \Big| > \tfrac{1}{2}(p^{-\delta_1} H)^n Q, \tag{18}$$

where the boxes I_m are disjoint and each of them has sides $\leqslant p^{\delta_2} + 1$.

Let $h = [p^{\delta_1}]$ and let J denote the cube $0 < x_j \leqslant h$. Then, for any box I of sides $\leqslant p^{\delta_2} + 1$ and any η in J, we have

$$\Big|\sum_{\zeta \in I} \chi(\zeta) - \sum_{\zeta \in I} \chi(\zeta + \eta)\Big| \leqslant 2nh(p^{\delta_2} + 1)^{n-1}.$$

Hence

$$\Big|\sum_{\zeta \in I} \chi(\zeta) - h^{-n} \sum_{\eta \in J} \sum_{\zeta \in I} \chi(\zeta + \eta)\Big| \leqslant 2nh(p^{\delta_2} + 1)^{n-1}.$$

Applying this to all the I_m in (18), we obtain

$$\sum_{m=1}^{M} \sum_{\zeta \in I_m} |S_h(\zeta)| > h^n \Big\{\frac{1}{2}(Hp^{-\delta_1})^n Q - 2nh(p^{\delta_2} + 1)^{n-1} M\Big\}.$$

In view of (17) we find that

$$2nh(p^{\delta_2} + 1)^{n-1} M < \frac{1}{4}(Hp^{-\delta_1})^n Q$$

provided $\delta_2 = 2n\delta_1 + \delta_3$. This condition supersedes (16). Hence

$$\sum_{m=1}^{M} \sum_{\zeta \in I_m} |S_h(\zeta)| > \frac{1}{4}(hHp^{-\delta_1})^n Q. \tag{19}$$

The total number of values of ζ (all distinct) in the sum on the left of (19) is

$$U \leqslant M(p^{\delta_2} + 1)^n \leqslant Q(4H)^n,$$

by (17). If r is any positive integer, it follows from Lemma 2 and Hölder's inequality that

$$\sum_{m=1}^{M} \sum_{\zeta \in I_m} |S_h(\zeta)| \leqslant U^{1-\frac{1}{2r}} \Big\{(4r)^{r+1} p^n h^{nr} + 2rp^{\frac{1}{2}n} h^{2nr}\Big\}^{\frac{1}{2r}}.$$

Comparison with (19) gives

$$H^n Q < 4^{2r+(2r-1)n} p^{2nr\delta_1} \Big\{(4r)^{r+1} p^n h^{-nr} + 2rp^{\frac{1}{2}n}\Big\}.$$

Take $r = [\delta_3^{-1} + 1]$, which ensures that $h^r > p^{\frac{1}{2}}$. Then, using (15) we obtain

$$C_1 H^{n+1} < 4^{2r+(2r-1)n} p^{2nr\delta_1 + o_2} (\log p)(4r)^{r+2} p^{\frac{1}{2}n}.$$

By (7) this implies

$$C_1 p^{(n+1)\delta} < 4^{2r+(2r-1)n} (4r)^{r+2} p^{2nr\delta_1 + \delta_2} (\log p).$$

First choose $\delta_3 = \delta$; this determines r. Since $\delta_2 = 2n\delta_1 + \delta_3$, the last inequality implies

$$p^{n\delta} < (C_3(r))^n p^{2nr\delta_1 + 2n\delta_1}.$$

This is false if we choose $\delta_1 = \frac{1}{8}\delta^2$, provided $p > p_3(\delta)$. Thus we have obtained a contradiction for a suitable choice of δ_1 depending only on δ, and this establishes Theorem 2.

Cambridge and Ann Arbor, May 1963.