Pacific Journal of Mathematics

SOME AVERAGES OF CHARACTER SUMS

HERBERT WALUM

Vol. 16, No. 1 November 1966

PACIFIC JOURNAL OF MATHEMATICS
Vol. 16, No. 1, 1966

SOME AVERAGES OF CHARACTER SUMS

H. WALUM

Let χ and ψ be nonprincipal characters mod p. Let f be a polynomial mod p and let $a_1, \cdots, a_p$ be complex constants. We will assume $a_j = a_k$ for $j \equiv k(p)$, and thus have a_n defined for all n. Define

$$S = \sum_r a_r \chi(f(r)) \tag{1}$$

and

$$J_n(c) = \sum_r \psi(r)\chi(r^n - c)\ , \tag{2}$$

where the variables of summation run through a complete system of residues mod p.

The averages in question are

$$A_1 = \sum_{a=1}^{p-1} | J_n(a) |^2 \tag{3}$$

and

$$A_2 = \Sigma | S |^2\ , \tag{4}$$

where the sum in (4) is over the coefficients mod p of certain fixed powers of the variables in f. Exact formulae for A_1 will be obtained in all cases, and for A_2 in an extensive class of cases.

Specifically, the following theorems are true.

THEOREM I. *Let $f(r) = yr^{m_1} + xr^{m_2} + g(r)$ and assume $(m_2 - m_1, p-1) = 1$. Let the sum in* (4) *be over all x and y* mod p. *If g has a nonzero constant term and neither m_1 nor m_2 is zero, then*

$$A_2 = p(p-1)\sum_{r=1}^{p-1} | a_r |^2 + p^2 | a_0 |^2\ . \tag{5}$$

Otherwise,

$$A_2 = p(p-1)\sum_{r=1}^{p-1} | a_r |^2\ . \tag{6}$$

THEOREM II. *Let $d = (n, p-1)$, $\psi(t) = e^{2\pi i (r \operatorname{ind}(t)/s)}$, where, naturally, $s \mid (p-1)$, $(r, s) = 1$ and $g^{\operatorname{ind}(t)} \equiv t(p)$ for g a primitive root* mod p. *If $ds \nmid (p-1)$, then $A_1 = 0$. If $ds \mid (p-1)$ and $\psi\chi^n$ is nonprincipal, then $A_1 = p(p-1)d$. If $ds \mid (p-1)$ and $\psi\chi^n$ is principal, then $A_1 = p(p-1)(d-1) - (p-1)$.*

The following is an immediate consequence of the first theorem.

Received November 21, 1963 and in revised form June 16, 1964. Research done under the auspices of the National Science Foundation.

THEOREM III. *Let f be as in Theorem I, and assume* $|a_r| = 1$, $r = 1, \cdots, p$. *Then there exist x_0, y_0, x_1 and y_1 depending on χ, such that the S, as in* (1), *for x_0 and y_0 satisfies* $|S| < \sqrt{p}$ *and the S, for x_1 and y_1, satisfies* $\sqrt{(p-2)} < |S|$.

Proof of Theorem II. Our principal device is the fact that a function which is periodic mod p has a unique expansion by means of the characters mod p [2]. That is if $h(r) = h(s)$ for $r \equiv s(p)$, then for $n \not\equiv 0(p)$

$$h(n) = \sum_\theta b_\theta \theta(n) , \tag{7}$$

where θ runs through the characters mod p. b_θ is given by

$$(p-1)b_\theta = \sum_r h(r)\bar{\theta}(r) . \tag{8}$$

Regarding $J_n(c)$ as a periodic function mod p of c, and expanding $J_n(c)$ in the form (7), we obtain, by standard methods,

$$J_n(c) = \sum_{\rho^n = \psi\chi^n} \pi(\bar{\rho}, \chi)\rho(c) \tag{9}$$

where $\pi(\alpha, \beta)$ is a Jacobi sum [1]

$$\pi(\alpha, \beta) = \sum_r \alpha(r)\beta(1-r) . \tag{10}$$

The sum in (9) is over all characters ρ which satisfy the indicated condition.

The expansion (7) has a Parseval identity

$$\sum_{t=1}^{p-1} |h(t)|^2 = (p-1) \sum_\theta |a_\theta|^2 . \tag{11}$$

Thus we can evaluate A_1 by means of (11) and (9) when we know the value of $|\pi(\alpha, \beta)|^2$. Now [1] $|\pi(\alpha, \beta)|^2 = p$ when $\alpha \neq \varepsilon$, $\beta \neq \varepsilon$ and $\alpha\beta \neq \varepsilon$, where ε is the principal character. If $\alpha = \varepsilon$ or $\beta = \varepsilon$, then $|\pi(\alpha, \beta)|^2 = 1$. If $\alpha\beta = \varepsilon$ with $\alpha \neq \varepsilon$ or $\beta \neq \varepsilon$, then $|\pi(\alpha, \beta)|^2 = p$. By hypothesis, χ is nonprincipal. Thus $|\pi(\bar{\rho}, \chi)|^2$ is p unless $\bar{\rho} = \varepsilon$ or $\bar{\rho}\chi = \varepsilon$. If $\bar{\rho} = \varepsilon$, then $\bar{\rho} = \varepsilon$ and $\psi\chi^n$ is principal. If $\bar{\rho}\chi = \varepsilon$, then $\rho = \chi$ and $\rho^n = \psi\chi^n$ implies $\psi = \varepsilon$ which is excluded by hypothesis. Let N be the number of solutions of $\rho^n = \psi\chi^n$. If $\psi\chi^n$ is nonprincipal then $|\pi(\bar{\rho}, \chi)|^2 = p$ for all N of the ρ and $A_1 = p(p-1)N$. If $\psi\chi^n$ is principal, then $|\pi(\bar{\rho}, \chi)|^2 = p$ for $N-1$ of the ρ and $|\pi(\bar{\rho}, \chi)|^2 = 1$ for $\rho = \varepsilon$. Thus, in this case, $A_1 = (p-1)(p(N-1)+1) = Np(p-1)^2$.

N, the number of solutions of $\rho^n = \psi\chi^n$, is the number of solutions of $\sigma^n = \psi$. It is a standard lemma from the theory of cyclic groups of order k that $a^n = b$ has (n, k) or 0 solutions according to whether or not order $b \mid k/(n, k)$. Also, N is the number of solutions of $x^n = \psi(g)$, for x, in $(p-1)-st$ roots of unity. From either description of N, it follows that $N = d$ or $N = 0$ according as $ds \mid (p-1)$ or $ds \nmid (p-1)$, and the theorem follows.

Proof of Theorem I. Referring to the hypotheses of Theorem I,

$$|S|^2 = \sum_{r,s} a_r \bar{a}_s \chi(yr^{m_1} + xr^{m_2} + g(r))\bar{\chi}(ys^{m_1} + xs^{m_2} + g(s))$$

and thus,

$$A_2 = \Sigma a_r \bar{a}_s \Sigma \chi(yr^{m_1} + xr^{m_2} + g(r))\chi(ys^{m_1} + xs^{m_2} + g(s)) = T_1 + T_2 . \tag{12}$$

T_1 is the sum of the terms in (12) such that $r \not\equiv 0$ and $s \not\equiv 0$. T_2 is the sum of the terms in (12) such that $r \equiv 0$ or $s \equiv 0$. T_1 can be witten

$$T_1 = \sum_{r \not\equiv 0, s} a_r \bar{a}_s \chi^{m_1}(r/s) A(r^{m_2-m_1}, r^{-m_1}g(r); s^{m_2-m_1}, s^{-m_1}g(s)) \tag{13}$$

where

$$A(a, b; c, d) = \sum_{y+cx+d \not\equiv 0} \chi\left(\frac{y + ax + b}{y + cx + d}\right) .$$

Now,

$$A(a, b; c, d) = \sum_{x} \sum_{y \not\equiv 0} \chi\left(\frac{y + x(a-c) + (b-d)}{y}\right) .$$

Except when $(a-c)x + (b-d) \equiv 0(p)$,

$$\sum_{y \not\equiv 0} \chi\left(\frac{y + (a-c)x + (b-d)}{y}\right) = -1 .$$

Also, $(a-c)x + (b-d) \equiv 0(p)$ when $x \equiv ((b-d)/(a-c))(p)$ or when $a \equiv c$ and $b \equiv d$. Thus, if $a \not\equiv c$ or $b \not\equiv d$, then

$$A(a, b; c, d) = -(p-1) + p - 1 = 0 .$$

If $a \equiv c$ and $b \equiv d$, then

$$A(a, b; c, d) = p(p-1) .$$

In view of this (13) becomes the sum over all r and s such that $r \not\equiv 0 \not\equiv s$ and $r^{m_2-m_1} = s^{m_2-m_1}$, $r^{-m_1}g(r) = s^{-m_1}g(s)$. Since $(m_2 - m_1, p-1) = 1$, we have $r \equiv s$. Thus the sum in (13) is over those r and s such that $r \not\equiv 0 \not\equiv s$ and $r \equiv s$. Thus

$$T_1 = p(p-1) \sum_{r=1}^{p-1} |a_r|^2 .$$

Now

$$T_2 = \sum_{r \not\equiv 0} a_r \bar{a}_0 \sum_{x,y} \chi(yr^{m_1} + xr^{m_2} + g(r))\bar{\chi}(g(0)) + \sum_{s \not\equiv 0} a_0 \bar{a}_s \sum_{x,y} \chi(g(0))\bar{\chi}(ys^{m_1} + xs^{m_2} + g(s)) + |a_0|^2 \sum_{x\ y} \chi(g(0))\bar{\chi}(g(0)) = p^2 |a_0|^2 |\chi(g(0))|^2 , \tag{14}$$

except when $m_1 = 0$ or $m_2 = 0$.

Thus, if $g(0) \equiv 0$,

$$A_2 = p(p-1) \sum_{r \not\equiv 0} |a_r|^2$$

and if $g(0) \not\equiv 0$, then

$$A_2 = p(p-1) \sum_{r \not\equiv 0} |a_r|^2 + p^2 |a_0|^2 ,$$

when $m_1 = 0$ or $m_2 = 0$, then $\chi(g(0))$ in (14) must be changed to $\chi(y + g(0))$ or $\chi(x + g(0))$, and A_2 is given by (6).

References

1. H. Davenport, and H. Hasse, *Die Nullstellen der Kongruenzzetafunktionen in* gewissen zyklischen Fallen, Journal für Math. (Crelle) **172** (1934), S. 151–182.

2. M. J. Delsarte, *Essai sur l'application de la theorie des fonctions periodiques a l'rithmetique*, Annales Scientifiques L'Ecole Normale Superieure, series 3, **62** (1945), 185–204.

Ohio State University

Printed in Japan by International Academic Printing Co., Ltd., Tokyo Japan

Pacific Journal of Mathematics
Vol. 16, No. 1 November, 1966