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.