ON GAUSSIAN SUMS

BY S. CHOWLA

UNIVERSITY OF COLORADO, BOULDER

Communicated by Deane Montgomery, May 15, 1962

1. Let χ denote a nonprincipal character (mod p), where p is an odd prime. Denote by χ_0 the principal character. I made the following

Conjecture: It is known that

$$\tau(\chi) = \sum_{1}^{p-1} \chi(n)\, e^{2n\pi i/p} = \sqrt{p}\, \epsilon(\chi)$$

where $|\epsilon(\chi)| = 1$; $\epsilon(\chi) =$ *is a root of unity only when* $\chi^2 = \chi_0$.

In this paper, I prove the conjecture. In the special case when $(p - 1)/2$ is also a prime a proof was recently given by Straus, Peck, and me, by a method whose power in other directions we hope to investigate later.

For a recent study of Jacobi and Gaussian sums, I would like to refer to a paper of A. Weil "Jacobi sums as Grössencharactere" in *Trans. Amer. Math. Soc.*, 1952. My thanks are due to A. Selberg for a stimulating conversation on the subject of this paper.

2. Let k be the least positive integer such that $\chi^k = \chi_0$. Then we have $p - 1 = qk$, where q is an integer. Write $\tau(\chi)$ in the form

$$T_1(\omega, \zeta) = \sum_{m=0}^{k-1} \omega^m S_m,$$

where

$$\omega = e^{\frac{2\pi i b}{k}}, \quad (b, k) = 1, \quad S_m = \sum_{t=1}^{q} \zeta^{g^{tk+m}}$$

and g denotes a primitive root (mod p); $\zeta = e^{2\pi i/p}$. We operate in the field $R(e^{2\pi i/w})$ where $w = 4\,pk$. We write $\theta = e^{2\pi i/w}$ and note that the automorphisms of $R(\theta)$ are given by $\theta \to \theta^h$ where $0 < h < w$, $(h, w) = 1$.

3. Suppose that $\epsilon(\chi)$ is a root of unity. Since $\tau^k(\chi)$ lies in $R(\omega)$ (Hasse, *Vorlesungen über Zahlentheorie*, Springer Verlag, pp. 440–450), it is easy to see that our theorem is true for k odd > 1. Hence suppose k even. Since $\tau^k(\chi)$ lies in $R(\omega)$, we easily see that if $\epsilon(\chi)$ is a root of unity, we must have

$$\epsilon(\chi) = i^m e^{\frac{2\pi i c}{k}}.$$

Thus our supposition gives

$$T_1(\omega, \zeta) = \sum_{m=0}^{k-1} \omega^m S_m = \sqrt{p}\, i^m \omega^a. \tag{1}$$

Write
$$T_h = T_1(\omega^h, \zeta^h) = \sum_{0}^{k-1} \omega^{mh} S_{m+\text{ind } h},$$

where h is prime to $4\,pk$. Thus,

$$T_h = \omega^{-h \text{ ind } h} T_1(\omega^h, \zeta) = \pm\sqrt{p} i^{mh} \omega^{ah}. \tag{2}$$

Thus, from (1) and (2), we see that if $h = 1 \pmod{k}$, then

$$\omega^{-h \text{ ind } h} \sqrt{p} i^m \omega^a = \pm\sqrt{p} i^{mh} \omega^{ah}. \tag{3}$$

Let
$$h = 2vk + 1 \quad (1 \leqslant v \leqslant p,\ 2vk + 1 \not\equiv 0 \pmod{p})). \tag{4}$$

We can choose v so that ind $h = k - 1$, for example. Then (3) and (4) give

$$\omega = \pm 1. \tag{5}$$

Thus, $k = 2$ and we have proved the

THEOREM. *If $\chi \neq \chi_0$ and $\tau(\chi) = \sqrt{p}\epsilon(\chi)$, then $\epsilon(\chi)$ is not a root of unity unless* $\chi^2 = \chi_0$.

A different solution has also been obtained by L. J. Mordell and L. G. Peck.

The author wishes to dedicate this article to Professor HANS RADEMACHER.