62. *On Certain Generalized Gaussian Sums*

By Michio OZEKI
Department of Mathematics, Nagasaki University

(Communicated by Shokichi IYANAGA, M. J. A., May 12, 1982)

§1. **Statement of the main result.** Let p be a fixed prime different from 2, and $\varepsilon_1, \varepsilon_2, \varepsilon_3$ be integers which are prime to p. We denote the diagonal matrix of degree m with diagonal elements $\alpha_1, \alpha_2, \cdots, \alpha_m$ by

$$\langle\alpha_1\rangle \perp \langle\alpha_2\rangle \perp \cdots \perp \langle\alpha_m\rangle.$$

Let $S=\langle 1\rangle \perp \langle 1\rangle \perp \cdots \perp \langle 1\rangle \perp \langle\varepsilon_1\rangle$ be a diagonal matrix of degree $m \geqq 4$, and put

$$T=\langle\varepsilon_2 p^r\rangle \perp \langle\varepsilon_3 p^s\rangle$$

where r, s are non negative integers such that $r \leqq s$.

Let $q=p^a$ be a sufficiently large power of p and $M_{m,2}(Z)$ be the set of $m\times 2$ rational integral matrices, then the quantity $A_q(S, T)$ is defined to be the number of the solutions X in $M_{m,2}(Z)$, which are different mod q one from another, of the matrix equation

$$(1) \qquad {}^tXSX \equiv T \pmod{q},$$

where ${}^tX$ is the transposed of X. There is a formula which expresses $A_q(S, T)$ as a kind of exponential sum, so called generalized Gaussian sum. (For details the reader is referred to [1] or [8].) Let $\omega_a\langle x\rangle$ be a function of a real variable x defined by

$$\omega_a\langle x\rangle=\exp(2\pi i x/q).$$

Let $B=(b_{ij})$ be the binary symmetric square matrix with coefficients in Z, and C be an element of $M_{m,2}(Z)$. By $B(q)$ we understand that the quantities b_{11}, $2b_{12}$ and b_{22} run independently modulo q and by $C\ (\mathrm{mod}\ q)$ we understand that the coefficients of C run independently modulo q. Then the formula mentioned above reads

$$(2) \qquad q^3 A_q(S, T)=\sum_{\substack{B(q)\\ C\,(\mathrm{mod}\,q)}} \omega_a\langle \mathrm{tr}\,\{({}^tCSC-T)B\}\rangle,$$

where tr is the trace of the matrix. Let G be the ordinary Gaussian sum $G=\sum_{x \bmod p}\exp(2\pi i x^2/p)$ and $(*/p)$ be the Legendre's symbol, then our main results are given by the two theorems.

Theorem 1. *Let the notations be as above. If* $q=p^a$, $a\geqq s+1$, $m\equiv 1\ (\mathrm{mod}\ 2)$ *and* $m \geqq 5$, *then* $A_q(S, T)$ *are given by*

$$A_q(S, T)=q^{2m-3}(1-p^{1-m})\left\{\sum_{\mu=0}^{(r-1)/2} p^{(4-m)\mu}+\left(\frac{-\varepsilon_2\varepsilon_3}{p}\right)p^{(s+r)(3-m)/2}\sum_{\mu=0}^{(r-1)/2} p^{(m-2)\mu}\right\}$$

$$\text{if} \quad s\geqq r \quad \text{and} \quad s\equiv r\equiv 1 \pmod{2},$$