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 $C \pmod{q}$ 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* $q = p^a$, $a \geqq s+1$, $m \equiv 1 \pmod 2$ *and* $m \geqq 5$, *then* $A_q(S, T)$ *are given by*

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

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

$$=q^{2m-3}(1-p^{1-m})\left\{\sum_{\mu=0}^{(r-1)/2} p^{(4-m)\mu}+\left(\frac{-\varepsilon_1\varepsilon_3}{p}\right)G^{m+1}p^{(s+r+1)(3-m)/2-2}\sum_{\mu=0}^{(r-1)/2} p^{(m-2)\mu}\right\}$$

if $s\geqq r+1$ *and* $s\equiv 0,\ r\equiv 1 \pmod 2$,

$$=q^{2m-3}(1-p^{1-m})\left\{\sum_{\mu=0}^{r/2} p^{(4-m)\mu}+p^{2r+3-(r+2)m/2}\sum_{\mu=0}^{(s-r-3)/2} p^{(3-m)\mu}\right.$$
$$+\left(\frac{-\varepsilon_1\varepsilon_2}{p}\right)G^{m+1}p^{3r+1-(r+1)m}\left[\sum_{\mu=0}^{r/2} p^{(m-2)\mu}\right]\left[\sum_{\mu=0}^{(s-r-1)/2} p^{(3-m)\mu}\right]$$
$$\left.-\left(\frac{-\varepsilon_1\varepsilon_2}{p}\right)G^{m+1}p^{3r+1-(r+1)m}\left[\sum_{\mu=0}^{r/2-1} p^{(m-2)\mu}\right]\left[\sum_{\mu=0}^{(s-r-3)/2} p^{(3-m)\mu}\right]\right\}$$

if $s\geqq r+1$ *and* $s\equiv 1,\ r\equiv 0 \pmod 2$,

$$=q^{2m-3}(1-p^{1-m})\left\{\sum_{\mu=0}^{r/2} p^{(4-m)\mu}+\left(\frac{-\varepsilon_1\varepsilon_2}{p}\right)G^{m+1}p^{2r+1-(r+2)m/2}\sum_{\mu=0}^{(s-r-2)/2} p^{(3-m)\mu}\right.$$
$$+p^{3r+3-(r+1)m}\left[\sum_{\mu=0}^{r/2} p^{(m-2)\mu}\right]\left[\sum_{\mu=0}^{(s-r-2)/2} p^{(3-m)\mu}\right]$$
$$\left.-p^{3r+3-(r+1)m}\left[\sum_{\mu=0}^{r/2-1} p^{(m-2)\mu}\right]\left[\sum_{\mu=0}^{(s-r-4)/2} p^{(3-m)\mu}\right]\right\}$$

if $s\geqq r$ *and* $s\equiv r\equiv 0 \pmod 2$,

where in the above formulas we should understand that the sum vanishes if the upper bound of the summation is negative. For example,

$$\sum_{\mu=0}^{(s-r-2)/2} p^{(3-m)\mu}=0 \qquad \text{if } s-r-2<0.$$

Theorem 2. *We put* $\alpha=(\varepsilon_1/p)G^m p^{-m}$ *and* $\beta=(-\varepsilon_2\varepsilon_3/p)$. *If* $q=p^a$, $a\geqq s+1$, $m\equiv 0 \pmod 2$ *and* $m\geqq 4$, *then* $A_q(S,T)$ *are given by*

$$A_q(S,T)=q^{2m-3}(1-\alpha)(1+\alpha\beta p)\left\{(1-\alpha\beta p)p^{(r-1)(4-m)/2}\right.$$
$$+(1-\alpha\beta p)\sum_{\lambda=0}^{(r-3)/2} p^{(4-m)\lambda}\left[\sum_{\mu=0}^{r-1-2\lambda} p^{(3-m)\mu}\right]$$
$$+\alpha p^2(1-\alpha\beta p)\sum_{\lambda=0}^{(r-3)/2} p^{(4-m)\lambda}\left[\sum_{\mu=0}^{r-2-2\lambda} p^{(3-m)\mu}\right]$$
$$+\alpha p^{(r-1)(3-m)+2}(1+\alpha p)\left[\sum_{\mu=0}^{(r-1)/2} p^{(m-2)\mu}\right]\left[\sum_{\mu=0}^{(s-r)/2} p^{(3-m)\mu}\right]$$
$$\left.-\beta p^{r(3-m)}(1+\alpha p)\left[\sum_{\mu=0}^{(r-1)/2} p^{(m-2)\mu}\right]\left[\sum_{\mu=0}^{(s-r-2)/2} p^{(3-m)\mu}\right]\right\}$$

if $s\geqq r$ *and* $s\equiv r\equiv 1 \pmod 2$,

$$=q^{2m-3}(1-\alpha)(1-\alpha^2p^2)\left\{p^{(r-1)(4-m)/2}+\sum_{\lambda=0}^{(r-3)/2} p^{(4-m)\lambda}\left[\sum_{\mu=0}^{r-1-2\lambda} p^{(3-m)\mu}\right]\right.$$
$$+\alpha p^2\sum_{\lambda=0}^{(r-3)/2} p^{(4-m)\lambda}\left[\sum_{\mu=0}^{r-2-2\lambda} p^{(3-m)\mu}\right]$$
$$\left.+\left[p^{r(3-m)}+\alpha p^{(r-1)(3-m)+2}\right]\left[\sum_{\mu=0}^{(r-1)/2} p^{(m-2)\mu}\right]\left[\sum_{\mu=0}^{(s-r-1)/2} p^{(3-m)\mu}\right]\right\}$$

if $s\geqq r+1$ *and* $s\equiv 0,\ r\equiv 1 \pmod 2$,

$$=q^{2m-3}(1-\alpha)(1-\alpha^2p^2)\left\{(1+\alpha p^2)\sum_{\mu=0}^{(r-2)/2} p^{(4-m)\mu}\right.$$

$$+p^{3-m}\sum_{\lambda=0}^{(r-2)/2} p^{(6-2m)\lambda}\left[\sum_{\mu=0}^{r/2-1-\lambda} p^{(4-m)\mu}\right]$$

$$+(p^{6-2m}+\alpha p^{5-m}+\alpha p^{8-2m})\sum_{\lambda=0}^{r/2-2} p^{(6-2m)\lambda}\left[\sum_{\mu=0}^{r/2-2-\lambda} p^{(4-m)\mu}\right]$$

$$+\left[\sum_{\mu=0}^{(s-r-1)/2} p^{(3-m)\mu}\right]\left[p^{r(3-m)}\sum_{\mu=0}^{r/2} p^{(m-2)\mu}+\alpha p^{(r-1)(3-m)+2}\sum_{\mu=0}^{r/2-1} p^{(m-2)\mu}\right]\Bigg\}$$

if $s\geqq r+1$ *and* $s\equiv 1,\ r\equiv 0 \pmod 2$,

$$=q^{2m-3}(1-\alpha)(1+\alpha\beta p)\Bigg\{(1-\alpha\beta p)(1+\alpha p^2)\sum_{\mu=0}^{(r-2)/2} p^{(4-m)\mu}$$

$$+p^{3-m}(1-\alpha\beta p)\sum_{\lambda=0}^{(r-2)/2} p^{(6-2m)\lambda}\left[\sum_{\mu=0}^{r/2-1-\lambda} p^{(4-m)\mu}\right]$$

$$+(1-\alpha\beta p)(p^{6-2m}+\alpha p^{5-m}+\alpha p^{8-2m})\sum_{\lambda=0}^{r/2-2} p^{(6-2m)\lambda}\left[\sum_{\mu=0}^{r/2-2-\lambda} p^{(4-m)\mu}\right]$$

$$+\alpha p^{(r-1)(3-m)+2}\left[\sum_{\mu=0}^{(s-r)/2} p^{(3-m)\mu}\right]\left[\alpha p\sum_{\mu=0}^{r/2} p^{(m-2)\mu}+\sum_{\mu=0}^{(r-2)/2} p^{(m-2)\mu}\right]$$

$$-\beta p^{r(3-m)}\left[\sum_{\mu=0}^{(s-r-2)/2} p^{(3-m)\mu}\right]\left[\alpha p\sum_{\mu=0}^{r/2} p^{(m-2)\mu}+\sum_{\mu=0}^{(r-2)/2} p^{(m-2)\mu}\right]\Bigg\}$$

if $s\geqq r$ *and* $s\equiv r\equiv 0 \pmod 2$,

where in the above formulas the sum vanishes if the upper bound of the summation is negative.

§ 2. **Applications.** Theorem 1 can be applied to derive explicit formulas for the Fourier coefficients $A_k(T)$ of Siegel-Eisenstein series of degree 3 and of weight (k is even) for the ternary primitive T. With the aids of the present work we are preparing a table of those values $A_k(T)$ in the range where $2\leqq \det(2T)\leqq 100$ and $4\leqq k\leqq 24$ ([4]). Theorem 2 will serve to give explicit formulas for Eisenstein series of degree 2 and of even weight k for the general binary T. Concerning this, there is a table by Resnikoff and Saldanã [5] which gives mainly the values of $A_4(T)$, the Fourier coefficients of Eisenstein series of degree 2 and of weight 4, for many primitive T's and for a few imprimitive T's. For the further arithmetical investigations of Siegel modular forms of degree 2, it would be desirable to enlarge the above table of Resnikoff and Saldanã. Theorem 2 is useful for this purpose.

References

[1] H. Braun: Über die Zerlegung quadratischer Formen in Quadrate. Crelle J., Bd. 178, pp. 34–64 (1938).

[2] H. Maass: Die Fourierkoeffizienten der Eisensteinreihen zweiten Grades. Dan. Vid. Selsk., **34** (1964).

[3] ——: Über die Fourierkoeffizienten der Eisensteinreihen zweiten Grades. ibid., **38** (1972).

[4] M. Ozeki and T. Washio: A table of Fourier coefficients of Eisenstein series of degree 3 (in preparation).

[5] H. L. Resnikoff and R. L. Saldaña: Some properties of Fourier coefficients of Eisenstein series of degree two. Crelle J., Bd. 265, pp. 90–109 (1974).

[6] C. L. Siegel: Über die analytische Theorie der quadratischen Formen 1. Ann. of Math., **36**, 527–606 (1935).
[7] ——: Einführung in die Theorie der Modulfunktionen n-ten Grades. Math. Ann., **116**, 617–657 (1939).
[8] ——: Lectures on the Analytic Theory of Quadratic Forms. Princeton University, Revised Edition (1949).