A. V. MALYSHEV

Let

1960

SovietRxiv

Abstract

Full Text

A. V. MALYSHEV

ON GAUSS SUMS AND KLOOSTERMAN SUMS

(Presented by Academician I. M. Vinogradov on 9 IV 1960)

Let

$$f = f(x_1, \dots, x_n) = \sum_{\alpha,\beta=1}^{n} a_{\alpha\beta} x_\alpha x_\beta$$

be an integral quadratic form, so that $a_{\alpha\alpha}$ $(\alpha = 1, \dots, n)$ and $a_{\alpha\beta} + a_{\beta\alpha} = 2a_{\alpha\beta}$ $(\alpha, \beta = 1, \dots, n;\ \alpha \neq \beta)$ are integers; let

$$l = l(x_1, \dots, x_n) = \sum_{\alpha=1}^{n} c_\alpha x_\alpha$$

be an integral linear form; let q and g be positive integers, and let $b_1, \dots, b_n$ be integers. The sum

$$S_{g;\,b_1,\dots,b_n}(f, l; q) = \frac{1}{g^n} \sum_{x_1,\dots,x_n=0}^{q-1} \exp\left[2\pi i \, \frac{f(gx_1 + b_1, \dots, gx_n + b_n) + l(gx_1 + b_1, \dots, gx_n + b_n)}{q}\right] \tag{1}$$

will be called an **inhomogeneous multiple Gauss sum modulo** g. These sums find application in the arithmetic of quadratic forms. If $g = 1$, $b_1 = \dots = b_n = 0$, then we have an inhomogeneous multiple Gauss sum over a complete system of residues

$$S(f, l; q) = S_{1,0,\dots,0}(f, l; q) = \sum_{x_1,\dots,x_n=0}^{q-1} \exp\left[2\pi i \, \frac{f(x_1, \dots, x_n) + l(x_1, \dots, x_n)}{q}\right]. \tag{2}$$

If, moreover, $l = 0$, then we have the homogeneous multiple Gauss sum

$$S(f; q) = S(f, 0; q) = \sum_{x_1,\dots,x_n=0}^{q-1} \exp\left[2\pi i \, \frac{f(x_1, \dots, x_n)}{q}\right]. \tag{3}$$

If $n = 1,\ f = ax^2$, then (3) turns into the ordinary Gauss sum

$$S(a; q) = S(ax^2; q).$$

The sums $S(a; q)$ were already studied by Gauss ([1]). The original theory of the sums (3), given by Weber ([2]), was later substantially simplified by Minkowski ([3]). Weber ([2]) and Kloosterman ([4]) considered special cases of the sums (2). Here we give formulas that make it possible to compute Gauss sums in their most general form (1).

Theorem 1. 1) If g is a complete system of residues $(x_1, \dots, x_n) \pmod q$, $(b'_1, \dots, b'_n) \equiv (b_1, \dots, b_n) \pmod{\text{g.c.d.}(g, q)}$, then

$$S_{g;\, b_1, \dots, b_n}(f, l; q) =$$

$$= \frac{1}{g^n} \sum_{(x_1, \dots, x_n) \in B} \exp\left[2\pi i\, \frac{f(gx_1 + b'_1, \dots, gx_n + b'_n) + l(gx_1 + b'_1, \dots, gx_n + b'_n)}{q}\right].$$

2) If $g = g_1 g_2$, $\text{g.c.d.}(g_2, q_1) = 1$, then

$$S_{g;\, b_1, \dots, b_n}(f, l; q) = \frac{1}{g_2^n} S_{g_1;\, b_1, \dots, b_n}(f, l; q).$$

3) If $\gcd(a, q) = 1$, then

$$S_{g;\, b_1, \dots, b_n}(a^2 f, al; q) = S_{g;\, ab_1, \dots, ab_n}(f, l; q).$$

4) If $d \mid q$, $d \mid f$, then

$$S_{g;\, b_1, \dots, b_n}(f, l; q) = \begin{cases} d^n S_{g;\, b_1, \dots, b_n}\left(\frac{f}{d}, \frac{l}{d}; \frac{q}{d}\right), & \text{if } d \mid l, \\ 0, & \text{if } d \nmid gl. \end{cases}$$

5) Let $q = q_1 q_2 \cdots q_k$, where the positive integers $q_1, \dots, q_k$ are pairwise coprime; $Q_1 = q/q_1, \dots, Q_k = q/q_k$. Then*

$$S_{g;\, b_1, \dots, b_n}(f, l; q) = g^{n(k-1)} \prod_{\alpha=1}^{k} S_{g;\, b_1, \dots, b_n}\left(Q_\alpha^{-1 \,(\text{mod } q_\alpha)} f, Q_\alpha^{-1 \,(\text{mod } q_\alpha)} l; q_\alpha\right).$$

6) If, under an integral substitution whose determinant is relatively prime to q, the forms f, l and the vector $(b_1, \dots, b_n)$ are transformed respectively into the forms f', l' and the vector $(b'_1, \dots, b'_n)$, then

$$S_{g;\,b_1,\dots,b_n}(f,l;q)=S_{g;\,b'_1,\dots,b'_n}(f',l';q).$$

7) Let

$$f(x_1,\dots,x_n)=\sum_{\alpha=1}^{k}f_\alpha(x_{\alpha_1},\dots,x_{\alpha n_\alpha}),\quad l(x_1,\dots,x_n)=\sum_{\alpha=1}^{k}l_\alpha(x_{\alpha_1},\dots,x_{\alpha n_\alpha}),$$

where $\{1,\dots,n\}$ is the union of pairwise disjoint sets of indices $\{(\alpha 1),\dots,(\alpha n_\alpha)\}$ $(\alpha=1,\dots,k)$. Then

$$S_{g;\,b_1,\dots,b_n}(f,l;q)=\prod_{\alpha=1}^{k}S_{g;\,b_1,\dots,b_{\alpha n_\alpha}}(f_\alpha,l_\alpha;q).$$

The following known proposition holds ([5]).

Remark. Let

$$q=\prod_{p\mid q}p^{t(p)}$$

be the factorization of the positive integer q into distinct prime factors p. Every integral quadratic form f is equivalent to a form f_1 for which, for every prime number $p\mid q$,

$$f_1\equiv\varphi^{(p)}=\sum_{\alpha=1}^{s(p)}p^{e_\alpha(p)}\varphi_\alpha^{(p)}\pmod{p^{t(p)}},\tag{4}$$

where

$$-1\le e_1(p)<e_2(p)<\dots<e_{s(p)}(p)<t(p);$$

$\varphi_1^{(p)},\dots,\varphi_{s(p)}^{(p)}$ are forms with integral matrices whose variables are pairwise disjoint; the determinants $d_1(p),\dots,d_{s(p)}(p)$ of these forms are relatively prime to p.

We additionally define: $n_\alpha(p)$ to be the number of variables of the form $\varphi_\alpha^{(p)}$ $(\alpha=1,\dots,s(p))$;

$$n(p)=\sum_{\alpha=1}^{s(p)}n_\alpha p,\quad 0\le n(p)\le n;$$

$\sigma(\varphi_\alpha^{(2)}) = 1$, if $2 \nmid \varphi_\alpha^{(2)}$;

$$\sigma(\varphi_\alpha^{(2)}) = 2, \quad \text{if } 2 \mid \varphi_\alpha^{(2)};$$

$$\varphi_{s(p)+1}^{(p)} = f_1 - \varphi^{(p)}; \quad n_{s(p)+1}(p) = n - n(p); \quad e_{s(p)+1} = t(p).$$

Theorem 2. Let

$$q = \prod_{p|q} p^{t(p)} = 2^{t(2)} q_1$$

be the factorization of the positive integer q into distinct prime factors p; q_1 is odd; $t(2) \geq 0$; $t(p) > 0$, if $p \neq 2$. Let the integral quadratic form f in n variables, for every $p \mid q$, be equivalent $(\mathrm{mod}\, p^{t(p)})$ to a form $\varphi^{(p)}$ of the form (4). Then $S(f;q) = 0$, if $\sigma(\varphi_{s(2)}^{(2)}) = 1$ and $e_{s(2)}(2) + 1 = t(2)$. In the opposite case

$$S(f;q) = (-1)^{\frac{q_1-1}{2}\sum_{\alpha=1}^{s(2)} \sigma\left(\varphi_\alpha^{(2)}\right) \frac{(-1)^{n_\alpha(2)(n_\alpha(2)+1)/2} d_\alpha(2)-1}{2}} \times$$

---

* By $a^{-1} (\mathrm{mod} m)$ we denote the number $a_1 (\mathrm{mod} m)$ for which $a_1 a \equiv 1 \pmod{m}$.

$$\times i^{\left(\frac{q_1-1}{2}\right)^2 \sum_{\alpha=1}^{s(2)} n_\alpha(2)\, s(2)} \prod_{\alpha=1}^{s(2)} \{-c_2(\varphi_\alpha^{(2)})\}^{\sigma(\varphi_\alpha{}^{(2)})} \times$$

$$\times \prod_{\alpha=1}^{s(2)} \left(\frac{2}{d_\alpha(2)}\right)^{t(2)-e_\alpha(2)-\sigma(\varphi_\alpha^{(2)})+1} \times \prod_{p|q_1} \prod_{\alpha=1}^{s(p)} \left(\frac{d_\alpha(p)}{p}\right)^{t(p)-e_\alpha(p)} \times$$

$$\times i^{\sum_{\alpha=1}^{s(2)} \sigma(\varphi_\alpha^{(2)})^2 \left(\frac{d_\alpha(2)-1}{2}\right)^2} \times \prod_{p|q_1} \left(\frac{2}{p}\right)^{t(2)\sum_{\alpha=1}^{s(p)} n_\alpha(p)(t(p)-e_\alpha(p))+t(p)\sum_{\alpha=1}^{s(2)} n_\alpha(2)(t(2)-e_\alpha(2))} \times$$

$$\times \prod_{\substack{p|q_1,\ p'|q_1 \\ p\neq p'}} \left(\frac{p'}{p}\right)^{t(p')\sum_{\alpha=1}^{s(p)} n_\alpha(p)(t(p)-e_\alpha(p))} \times$$

$$\times i^{\sum_{p|q_1} \left(\frac{p-1}{2}\right)^2 \sum_{\alpha=1}^{s(p)} n_\alpha(p)(t(p)-e_\alpha(p))^2} \times \left(\frac{1+i}{\sqrt{2}}\right)^{\sum_{\alpha=1}^{s(2)} n_\alpha(2)(2-\sigma(\varphi_\alpha^{(2)}))} \times$$

$$\times (2q)^{\frac{n}{2}} \times 2^{\frac{1}{2}(n-n(2))(t(2)-1)+\frac{1}{2}\sum_{\alpha=1}^{s(2)} n_\alpha(2)e_\alpha(2)} \times$$

$$\times \prod_{p|q_1} p^{\frac{1}{2}(n-n(p))t(p)+\frac{1}{2}\sum_{\alpha=1}^{s(p)} n_\alpha(p)e_\alpha(p)}, \tag{5}$$

where $c_2(\varphi)$ is the Hasse invariant ([5]).

Theorem 3. Let

$$q = \prod_{p|q} p^{t(p)} = 2^{t(2)} q_1; \qquad t(2) \geq 0; \qquad t(p) > 0,$$

if p is an odd prime; $Q(p) = \dfrac{q}{p^{t(p)}}$. Let the integral quadratic form $f = f(x_1, \dots, x_n) = f_1$ satisfy congruence (4) for all primes $p \mid q$. Let

$$l = l(x_1, \dots, x_n) = \sum_{\beta=1}^{n} c_\beta x_\beta$$

be an integral linear form;

$$l = \sum_{\alpha=1}^{s(p)+1} l_\alpha^{(p)},$$

where the variables of the forms $l_\alpha^{(p)}$ coincide with the variables of the quadratic form $\varphi_\alpha^{(p)}$. Let

$$\tau_\alpha(p) = \begin{cases} 1, & \text{if } p^{e_\alpha(p)} \mid l_\alpha^{(p)}, \\ 0, & \text{if } p^{e_\alpha(p)} \nmid l_\alpha^{(p)}; \end{cases} \qquad (p \neq 2)$$

$$\tau_\alpha(2)=\begin{cases}2, & \text{if } \alpha=s(2),\ \sigma(\varphi_\alpha^{(2)})=1,\ t(2)=e_\alpha^{(2)}+1,\ 2^{e_\alpha(2)}\mid l_s^{(2)},\ \text{and all}\\ & \text{coefficients of the linear form } 2^{-e_\alpha(2)}l_\alpha^{(2)} \text{ are odd;}\\ 1, & \text{if } (s(2)+1-\alpha)\sigma(\varphi_\alpha^{(2)})(t(2)-e_\alpha(2))>1 \text{ and } 2^{e_\alpha(2)+1}\mid l_\alpha^{(2)},\\ & \text{if } \alpha=s(2)+1 \text{ and } 2^{e_\alpha(2)}\mid l_\alpha^{(2)};\\ 0, & \text{if } 2^{e_\alpha(2)+1}\nmid l_\alpha^{(2)};\ \text{if } \alpha=s(2),\ \sigma(\varphi_\alpha^{(2)})=1,\ t(2)=e_\alpha(2)+1\\ & \text{and } 2^{e_\alpha(2)}\nmid l_\alpha^{(2)};\ \text{if } \alpha=s(2),\ \sigma(\varphi_\alpha^{(2)})=1,\ t(2)=e_\alpha(2)+1,\\ & 2^{e_\alpha(2)}\mid l_\alpha^{(2)} \text{ and not all coefficients of the form } 2^{-e_\alpha(2)}l_\alpha^{(2)} \text{ are odd;}\\ & \text{if } \alpha=s(2)+1 \text{ and } 2^{e_\alpha(2)}\nmid l_\alpha^{(2)};\end{cases}$$

$(p>q;\ \alpha=1,\dots,s(p)+1)$. Then

$$S(f,l;q)=\frac{\prod\limits_{p<q}\prod\limits_{\alpha=1}^{s(p)+1}\tau_\alpha(p)^{n_\alpha(p)}}{2^{2n}}\times S(f_1;4q)\times$$
$$\times\exp\left[-\frac{2\pi i}{4q}\sum_{p<q}Q(p)^{-1\ (\mathrm{mod}\ p^{t(p)+1+(-1)^p})}\times Q(p)\times 2^{1+(-1)^p+1}\times\right.$$
$$\left.\times\left\{2^{1+(-1)^p+1}\prod_{\alpha=1}^{s(p)}d_\alpha(p)\right\}^{-1\ (\mathrm{mod}\ p^{t(p)+1+(-1)^p})}\times p^{\sum_{\alpha=1}^{s(p)}n_\alpha(p)e_\alpha(p)}\times\bar\varphi^{(p)}(c_1,\dots,c_n(p))\right],\tag{6}$$

where $\bar\varphi^{(p)}$ is a form algebraically reciprocal to $\varphi^{(p)}=\varphi^{(p)}(x_1,\dots,x_n(p))$;
$f_1=4f-\left(4-4^{2-\tau s(2)^{(2)}}\right)2^{es(2)^{(2)}}\varphi_{s(2)}^{(2)}$.

The sums (1) reduce to sums (2)

$$S_{g;b_1,\dots,b_n}(f,l;q)=\frac{1}{g^n}\exp\left[2\pi i\,\frac{f(b_1,\dots,b_n)+l(b_1,\dots,b_n)}{q}\right]S(g^2f,gL;q),\tag{7}$$

where

$$L=L(x_1,\dots,x_n)=l(x_1,\dots,x_n)+2f(b_1,\dots,b_n;x_1,\dots,x_n)$$
$$=\sum_{\alpha=1}^{n}\left(c_\alpha+2\sum_{\beta=1}^{n}a_{\alpha\beta}b_\beta\right)x_\alpha.$$

The formulas given above, together with estimates for Kloosterman sums ([4,6,7]), allow us to obtain the following useful proposition, which is a generalization and refinement of Kloosterman' s lemma ([4]):

Theorem 4. Let $f = f(x_1, \dots, x_n)$ be an integral quadratic form with determinant d; let $g > 0$, $B_1, \dots, B_n$, $C_1, \dots, C_n$, m, $q > 0$, Q_1, Q_2 be integers; let

$$l_h = l_h(x_1, \dots, x_n) = \sum_{\alpha=1}^{n} (hgB_\alpha + C_\alpha)x_\alpha.$$

Then

$$\left| \sum_{Q_1 \le h^{-1} \pmod q \le Q_2}{}' S(hg^2 f, l_h; q) \exp\left[-2\pi i \frac{mh}{q}\right] \right| <$$

$$< \chi_\varepsilon q^{\frac{n+1}{2}+\varepsilon} \left\{\text{g. c. d.}(2^{n+2}dg^2m - w, q)\right\}^{\frac{1}{2}} \left\{\text{g. c. d.}(2^{3n}d^3g^{2n+4}, q^{n+2})\right\}^{\frac{1}{2}}; \quad (8)$$

here the summation on the left is over all residues h of a reduced residue system $(\mathrm{mod}\, q)$ satisfying the condition $*$ $Q_1 \le h^{-1} (\mathrm{mod}\, q) \le Q_2 (\mathrm{mod}\, q)$; w is an integer depending only on f, g and $B_1, \dots, B_n$; $\varepsilon > 0$ is arbitrarily small; $\chi_\varepsilon > 0$ is a constant depending only on n and ε; $w = 0$ if $B_1 = \cdots = B_n = 0$.

Leningrad Branch
of the V. A. Steklov Mathematical Institute
Academy of Sciences of the USSR

Received
6 IV 1960

REFERENCES

1. K. F. Gauss, *Tr. po teorii chisel*, Moscow, 1959, p. 594.
2. H. Weber, *J. reine u. angew. Math.*, **74**, 14 (1872).
3. H. Minkowski, *Gesammelte Abhandlungen*, 1, Leipzig, 1911, S. 3.
4. H. D. Kloosterman, *Acta Math.*, **49**, 407 (1926).
5. B. W. Jones, *The Arithmetic Theory of Quadratic Forms*, 1950.
6. H. Salié, *Math. Zs.*, **34**, 91 (1931).
7. A. Weil, *Proc. Nat. Acad. USA*, **34**, 204 (1948).

* We say that $Q_1 \le z \le Q_2 \pmod q$, if there is $z_1 \equiv z \pmod q$ for which $Q_1 \le z_1 \le Q_2$.

Note: Figure translations are in progress. See original paper for figures.

Source: Math-Net.Ru and CyberLeninka. Machine translation. Verify with the original.