# ON THE REPRESENTATION OF INTEGERS BY POSITIVE QUADRATIC FORMS WITH FOUR AND MORE VARIABLES

Let

1960

SovietRxiv

## Abstract

## Full Text

## MATHEMATICS

**A. V. MALYSHEV**

# ON THE REPRESENTATION OF INTEGERS BY POSITIVE QUADRATIC FORMS WITH FOUR AND MORE VARIABLES

*(Presented by Academician I. M. Vinogradov, 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 positive quadratic form, where $a_{\alpha\alpha}$ $(\alpha = 1, \dots, n)$ and $a_{\alpha\beta} + a_{\beta\alpha} = 2a_{\alpha\beta}$ $(\alpha, \beta = 1, \dots, n;\ \alpha \neq \beta)$ are integers; $n \geq 4$; $\det f \equiv \det(a_{\alpha\beta}) = d$. Let $m$ be a positive integer; in the $n$-dimensional Euclidean space $\{x_1, \dots, x_n\}$ consider the ellipsoid $f(x_1, \dots, x_n) = m$. Let $\Omega = \Omega_{f,m}$ be a region on the surface of this ellipsoid; by the $f$-elliptic angle $\omega = \omega_f(\Omega)$ of the region $\Omega$ we shall mean the ordinary $n$-dimensional solid angle under which, from the origin, one sees the region $\Omega'$ obtained from $\Omega$ by means of such a linear transformation as reduces the form $f$ to $f_0 = x_1^2 + \cdots + x_n^2$.

Suppose, in addition, that integers $g > 0$ and $b_1, \dots, b_n$ are given. Denote by $R_{g;b_1,\dots,b_n}(\Omega_{f,m})$ the number of all integral points $(x_1, \dots, x_n)$ lying in the elliptical region $\Omega_{f,m}$ and congruent to $(b_1, \dots, b_n)$ modulo $g$; by $r_{g;b_1,\dots,b_n}(\Omega_{f,m})$ denote the number of all such points with the additional condition $\gcd(x_1, \dots, x_n) = 1$. If $\Omega_{f,m}$ coincides with the surface of the entire ellipsoid $f(x_1, \dots, x_n) = m$, then

$$R_{g;b_1,\dots,b_n}(\Omega_{f,m}) = R_{g;b_1,\dots,b_n}(f; m)$$

and

$$r_{g;b_1,\dots,b_n}(\Omega_{f,m}) = r_{g;b_1,\dots,b_n}(f; m)$$

are, respectively, the number of all integral and of all integral primitive representations $(x_1, \dots, x_n)$ of the number $m$ by the form $f$ with the additional condition

$$(x_1, \dots, x_n) \equiv (b_1, \dots, b_n) \pmod{g}.$$

If, moreover, $g = 1$, then

$$R_{g;b_1,\dots,b_n}(f; m) = R(f; m)$$

and

$$r_{g;b_1,\dots,b_n}(f;m) = r(f;m)$$

are, respectively, the number of all integral and the number of all integral primitive representations of the number $m$ by the form $f$.

In this note, developing the results of ([1,2]), asymptotic formulas are obtained and investigated for

$$R_{g;b_1,\dots,b_n}(\Omega_{f,m}) \quad \text{and} \quad r_{g;b_1,\dots,b_n}(\Omega_{f,m}).$$

Let

$$H_{g;b_1,\dots,b_n}(f;m) = \sum_{q=1}^{\infty} \left\{ \sum_{h \pmod q}{}' q^{-n} S_{g;b_1,\dots,b_n}(hf;q) e^{-2\pi i \frac{mh}{q}} \right\} \tag{1}$$

be the singular series; here $S_{g;b_1,\dots,b_n}(f;q)$ is the generalized Gauss sum defined and studied in ([3]); the summation

$$\sum_{h \pmod q}{}'$$

is taken over a reduced system of residues (mod $q$). The absolute convergence of the infinite series (1) for $n \geq 4$ follows from Theorem 4 of the note ([3]). As usual, the singular series

$$H_{g;b_1,\dots,b_n}(f;m)$$

can be represented in the form of an infinite product over prime numbers. The factors of this infinite product, by means of the formulas of ([3]), can be expressed in finite form.

through the joint arithmetic invariants of the form $f$ and of the residue class $(b_1,\dots,b_n) \pmod g$. We do not give the formulas, because of their bulkiness.

Let $p$ be a prime number. We introduce the quantities $u_p, \tau_p, w_p, T_p, S_p$.

1) $p^{u_p} \parallel g$.

2) To define $\tau_p$ and $w_p$, we distinguish two cases: $p > 2$ and $p = 2$.

a) $p > 2$. Let

$$f(x_1,\dots,x_n) \equiv \sum_{\beta=1}^{n} a_\beta^{(p)} p^{\varepsilon_\beta{}^{(p)}} x_\beta^2 \pmod{p^t},$$

where $\varepsilon_\beta^{(p)} \geq 0$, $a_1^{(p)},\dots,a_n^{(p)}$ are relatively prime to $p$; let $(b_1,\dots,b_n) \equiv (b_1^{(p)},\dots,b_n^{(p)}) \pmod{p^{u_p}}$, where $b_\alpha^{(p)} = 0$ if $b_\alpha \equiv 0 \pmod{p^{u_p}}$; let $p^{v_\alpha{}^{(p)}} \parallel b_\alpha^{(p)}$ $(\alpha = 1,\dots,n$; if $b_\alpha^{(p)} = 0$, then $v_\alpha^{(p)} = \infty)$; by definition

$$\tau_p = \min_{\alpha}\{u_p + v_\alpha^{(p)} + \varepsilon_\alpha^{(p)}\},$$

$$p^{w_p} \parallel (m - f(b_1^{(p)}, \dots, b_n^{(p)})).$$

b) $p = 2$. Let

$$f(x_1, \dots, x_n) = \sum_{\beta=1}^{n'} a_\beta 2^{\varepsilon_\beta{}^{(1)}} x_\beta^2 + \sum_{\gamma=1}^{n''} 2^{\varepsilon_\gamma{}^{(2)}} \psi_\gamma(y_\gamma, z_\gamma) \pmod{2^t},$$

where $n' + 2n'' = n$; $\varepsilon_\beta^{(1)} \geq 0$, $\varepsilon_\gamma^{(2)} \geq -1$; $a_1, \dots, a_{n'}$ are odd; $\psi_\gamma(y_\gamma, z_\gamma) = 2a'_\gamma y_\gamma^2 + 2a''_\gamma y_\gamma z_\gamma + 2a'''_\gamma z_\gamma^2$; $a'_\gamma, a''_\gamma, a'''_\gamma$ are integers; $a''_\gamma$ is odd ($\gamma = 1, \dots, n''$); let $(b_1, \dots, b_n) \equiv (b_1^{(2)}, \dots, b_n^{(2)}) \pmod{2^{u_2}}$, where $b_\alpha^{(2)} = 0$ if $b_\alpha \equiv 0 \pmod{2^{u_2}}$; let $2^{v_\alpha{}^{(2)}} \parallel b_\alpha^{(2)}$; we put

$$\tau' = \min_{\alpha \leq n,\ v_\alpha^{(2)} \neq u_2 - 1} \{u_2 + v_\alpha^{(2)} + \varepsilon_\alpha^{(1)} + 1\}$$

(if there are no such $\alpha$, we assume that $\tau' = \infty$);

$$\tau'' = \min_{\alpha \leq n',\ v_\alpha^{(2)} = u_2 + 1} \{u_2 + v_\alpha^{(2)} + \varepsilon_\alpha^{(1)} + 2\};$$

$$\tau''' = \min_{\alpha > n'} \{u_2 + v_\alpha^{(2)} + \varepsilon^{(2)}_{\left[\frac{\alpha - n' + 1}{2}\right]} + 1\}; \qquad \tau_2 = \min\{\tau', \tau'', \tau'''\};$$

we define

$$2^{w_2} \parallel (m - f(b_1^{(2)}, \dots, b_n^{(2)})).$$

3) Finally, we put

$$T_p = \min\{w_p + 1 + 1 + (-1)^p, \tau_p\}, \qquad S_p = \max\{T_p, u_p\}.$$

To the quadratic form $f$ we associate the set $\mathfrak{P}_f$ of exceptional (herabsetzende) prime numbers (for their definition see (4)). If $p \in \mathfrak{P}_f$, then $n = 4$ and $p \backslash 2^{n+1} d$.

**Theorem 1.** *If for every prime number $p \backslash 2^{n+1} dg$ the system of congruences*

$$\begin{aligned} f(x_1, \dots, x_n) &\equiv m \pmod{p^{S_p}}, \\ (x_1, \dots, x_n) &\equiv (b_1, \dots, b_n) \pmod{p^{u_p}}, \end{aligned} \tag{2}$$

then

$$H_{g;b_1,\dots,b_n}(f;m) \geqslant \chi_\varepsilon d^{-\frac{1}{2}(n-1)} g^{-(n-1)} m^{-\varepsilon} \prod_{p\in\mathfrak{P}_f} p^{-(\frac{1}{2}n-1)}\tau_p, \tag{3}$$

where $\varepsilon > 0$ is arbitrary, $\chi_\varepsilon > 0$ is a constant depending only on $\varepsilon$. In the contrary case

$$H_{g;b_1,\dots,b_n}(f;m) = 0. \tag{4}$$

**Theorem 2.** There is the asymptotic formula

$$R_{g;b_1,\dots,b_n}(f;m) = \frac{\pi^{\frac{n}{2}} m^{\frac{n}{2}-1}}{d^{\frac{1}{2}}\Gamma(n/2)} H_{g;b_1,\dots,b_n}(f;m) + O\Big(d^{\frac{n}{4}+\frac{3}{2}} g^{\frac{3}{2}n+2} m^{\frac{n}{4}-\frac{1}{4}+\varepsilon}\Big), \tag{5}$$

where the constants occurring in $O$ depend only on $n$ and $\varepsilon > 0$. Moreover, if for all primes $p > 2^{n+1}dg$ the system of congruences (2) is solvable* and if, for some fixed $\theta > 0$,

$$d^{\frac{3}{4}n+\frac{3}{2}} g^{\frac{3}{2}n+1} \prod_{p\in\mathfrak{P}_f} p^{(\frac{1}{2}n-1)}\tau_p = O\Big(m^{\frac{n}{4}-\frac{3}{4}-\theta}\Big), \tag{6}$$

where the constants occurring in $O$ depend only on $n$ and $\theta$, then as $m \to \infty$ the remainder term in formula (5) is infinitesimal in comparison with the main term.

**Theorem 3.** Let $\Omega_{f,m}$ be a convex domain on the surface of the ellipsoid $f(x_1, \dots, x_n) = m$ with $f$-elliptic solid angle $\omega$. Then

$$R_{g;b_1,\dots,b_n}(\Omega_{f,m}) = \frac{\omega}{\omega_0} \frac{\pi^{\frac{n}{2}} m^{\frac{n}{2}-1}}{d^{\frac{1}{2}}\Gamma(n/2)} H_{g;b_1,\dots,b_n}(f;m) +$$

$$+ O\Big(d^{\frac{n}{4}+\frac{5}{2}} g^{\frac{3}{2}n+7} m^{\frac{n}{2}-1-\frac{n-3}{4(3n-2)}+\varepsilon}\Big), \tag{7}$$

where

$$\omega_0 = \frac{2\pi^{\frac{n}{2}}}{\Gamma(n/2)};$$

the constants occurring in $O$ depend only on $n$ and $\varepsilon > 0$. Moreover, if for all primes $p > 2^{n+1}dg$ the system of congruences (2) is solvable and if, for $\theta > 0$,

$$\omega^{-1} d^{\frac{3n}{4}+\frac{3}{2}} g^{\frac{5}{2}n+4} \prod_{p\in\mathfrak{P}_f} p^{(\frac{1}{2}n-1)}\tau_p = O\Big(m^{\frac{n-3}{4(3n-2)}-\theta}\Big), \tag{8}$$

where the constants occurring in $O$ depend only on $n$ and $\theta$, then as $m \to \infty$ the remainder term in formula (7) is infinitesimal in comparison with the main term.

It is also possible to obtain the asymptotic formula (7) for nonconvex domains $\Omega_{f,m}$, assuming, however, that as $m$ varies their shape does not change (then the constants occurring in $O$ will depend on the shape of the domain $\Omega_{f,m}$).

The asymptotic formulas (5) and (7) can be obtained by refining the arguments in ([1],[2]); here Theorem 4 of the note ([3]) is used essentially. The concluding parts of Theorems 2 and 3 are derived from the estimate (3).

From Theorem 3 one may derive:

---

* In the contrary case, obviously, $R_{g;b_1,\dots,b_n}(f;m) = 0$.

**Theorem 4.** Let $\Omega_{f,m}$ be a convex domain on the surface of the ellipsoid $f(x_1,\dots,x_n) = m$ with $f$-elliptic solid angle $\omega$. Then

$$r_{g;b_1,\dots,b_n}(\Omega_{f,m}) = \frac{\omega}{\omega_0}\frac{\pi^{n/2}m^{n/2-1}}{d^{1/2}\Gamma(n/2)}G_{g;b_1,\dots,b_n}(f;m)+O\Big(d^{n/4+5/2}g^{3n/2+7}m^{n/2-1-\frac{n-3}{4(3n-2)}+\varepsilon}\Big), \tag{9}$$

where

$$G_{g;b_1,\dots,b_n}(f;m) = \sum_{\substack{\delta^2|m\\ \gcd(\delta,g)=1}} \frac{\mu(\delta)}{\delta^{n-2}}\, H_{g;b_1\delta^{-1}(\bmod g),\dots,b_n\delta^{-1}(\bmod g)}\Big(f;\frac{m}{\delta^2}\Big)$$

is a primitive singular series*; the constants entering the $O$-term depend only on $n$ and $\varepsilon > 0$. Moreover, if for all primes $p > 2^{n+1}dg$ the system of congruences (2) is primitively solvable $(\bmod p)$** and if, for $\theta > 0$,

$$\omega^{-1}d^{7n/4+3/2}g^{7n/2+5} = O\Big(m^{\frac{n-3}{4(3n-2)}-\theta}\Big), \tag{10}$$

where the constants entering the $O$-term depend only on $n$ and $\theta$, then as $m \to \infty$ the remainder term in formula (9) is infinitely small in comparison with the main term.

**Theorem 5.** Let $\gcd(m,g,2d) = 1$. Then, under the conditions of Theorem 4,

$$r_{g;b_1,\dots,b_n}(\Omega_{f,m}) \sim \frac{\omega}{\omega_0}\,\frac{1}{\nu_g(f,m)}\,r(f;m), \tag{11}$$

where $\nu_g(f,m)$ is the number of primitive $(\bmod g)$ solutions of the congruence

$$f(x_1, \dots, x_n) \equiv m \pmod{g}. \tag{12}$$

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

Received
6 IV 1960

## REFERENCES

1. A. V. Malyshev, DAN, **114**, 25 (1957).
2. A. V. Malyshev, Izv. AN SSSR, ser. matem., **23**, 337 (1959).
3. A. V. Malyshev, DAN, **133**, No. 5 (1960).
4. V. A. Tartakovskii, Izv. AN SSSR, Otd. fiz.-matem., **111**, 165 (1929).

* By $a^{-1}(\mathrm{mod} g)$ we denote the number $a_1(\mathrm{mod} g)$ for which $aa_1 \equiv 1 \pmod{g}$.

** Otherwise, obviously, $r_{g;b_1,\dots,b_n}(\Omega_{f,m}) = 0$.

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