Proceedings of the Steklov Institute of Mathematics, Vol. 218, 1997, pp. 243–256.
Translated from Trudy Matematicheskogo Instituta imeni V. A. Steklova, Vol. 218, 1997, pp. 248–261.

Representation of Numbers by Quadratic Forms

L. A. Kogan

Received February, 1997

INTRODUCTION

We consider briefly the history of the problem. (For more details, see monographs and reviews by Cassells [7], Rankin [28], Malyshev [17], Fomenko [20], and Kogan [10]).

Gauss, Jacobi, Dirichlet, Kronecker, Eisenstein, Liouville, Hermite, Smith, Minkowski, Nazimov, Uspenskii, Mordell, Hardy, Schoenberg, Mass, Kloosterman, Venkov, Linnik, Val'fish, Andrianov, Lomadze, Kogan, Fomenko, Vepkhvadze, Gogishwili, Tashpulatov, Abdullaev, and other researches have obtained (by various methods) the formulas for the amounts of representations of numbres by specific quadratic forms.

These formulas have been obtained in the following forms.

Let

$$M[n = Q(x) = Q(x_1, \dots, x_k)] = \rho(n) + \psi(n), \tag{1}$$

where $M[n = Q]$ is the number of representations of the positive integer n by the integral positive qudratic form Q, $k \geq 3$, $\rho(n)$ is the principal term in formula (1), $\psi(n)$ is an additional term.

(a) $\psi(n) \equiv 0$. Formulas of this form were obtained by Gauss, Jacobi, Kronecker, Minkowski, Venkov, Linnik, and others.

The examples are the following: the Gaussian theorem on three squares, Jacobi's formulas for the four, six, and eight squares.

The questions concerning the existence of these formulas were considered by Hardy, Rankin, the author, Gogishvili, and Lomadze.

(b) The additional term is a linear combination of expressions of the form

$$\sum_{n=ax^2+bxy+cy^2} \varphi(x, y),$$

where $\varphi(x, y)$ is the simplest numerical function.

Functions of this kind were obtained by Liouville, Uspenskii, Val'fish, the author, Lomadze, Andrianov, Vepkhvadze, and others.

The questions concerning the existence of formulas of this kind were studied by the author.

(c) *Formulas of the Bulygin–Mordell type.* For $k \geq 4$, the additional term is a linear combination of the expressions

$$\sum_{m=Q_i(x_1,\dots,x_l)} \varphi_i(x_1, \dots, x_l),$$

where φ_i is the simplest numerical function, Q_i is a qudratic form, and $l \leq k$.

Formulas of this kind were obtained by Bulygin, Mordell, Lomadze, the author, Vepkhvadze, and others.

(d) *Formulas of the Kloosterman type.*

$\psi(n)$ is equal to the coefficient of z^n ($z = e^{i\pi\tau}$, $\operatorname{Im}\tau > 0$) in the series expansion in the powers of z of products of certain Jacobi theta-functions or theta-functions with characteristics (in some cases, we can encounter products of the theta-functions in fractional degrees).

Formulas of this kind were obtained by Kloosterman, Lomadze, the author, Vepkhvadze, Tashpulatov, and others.

(e) *Formulas of the Liouville type* for quadratic forms with an odd number of variables.

$\psi(n)$ is a linear combination of expressions of the form $\sum_{n=ax^2} f(x)$, where $f(x)$ is a certain simplest numerical function.

Formulas this form were obtained by the author, Lomadze, Poll, Ross, and others.

(f) *Formulas of the Weil type.*

$\psi(p)$ is a linear combination of expressions of the form

$$\sum_{x=0}^{p-1} \left(\frac{x^3 + Ax + B}{p} \right).$$

Formulas of this kind were obtained by Andrianov, the author, Abdullaev, and others.

The questions concerning the existence of forms of this kind were studied by the author.

In 1967, Academician Yu. V. Linnik, in the private communication with the author posed the following question: is the number of classes of primitive positive quadratic forms of the Liouville type finite or not?

In [8, 9, 11, 10], the author have stated a conjecture that the classes of primitive quadratic forms of the Lioville and Weil type were finite. This conjecture was also formulated by Malyshev in the overview [17].

Analyzing the methods and formulas obtained by the above-mentioned authors, the author gave in [10] the definitions of quadratic forms of the Jacobi, Liouville, Weil, and Bulygin–Mordell type on the basis of the modern theory of modular forms and algebraic geometry.

The general definitions made it possible to pose the problem of the limits of the existence of formulas of the indicated types and the algorithm for obtaining them, and also to connect the solutions of the indicated problems with the modern theory of modular forms, the results of Vinogradov [3] and Burgess [22] on the distribution of quadratic nonresidues, Weil's conjecture [31], the generalized Weil conjecture [12], Mumford's problem [18], and the results by Eichler [23] on the representability of modular forms in the form of generalized theta-series.

The author constructed in [10] a method for determining the limits of existence of formulas of the Jacobi type, of the Liouville type, and of the Weil type. By this method, the author proved the theorems (see [10, 13, 14]) on the finiteness of the number of classes of quadratic forms with four and more variables. Using the method of the author [10], Tashpulatov proved in [13] the theorems on the finiteness of classes of quadratic forms of the Jacobi type and of the Liouville type for ternary quadratic forms.

By the method of [10], some results obtained by the author were generalized to quadratic forms with congruent conditions by Tashpulatov and Kulmatov [14].

Generalizing the results of Lomadze in his doctoral dissertation, Vepkhvadze [2] used the generalized theta-functions with characteristics for the investigation of the quadratic forms $Q(x_1, \dots, x_k)$. The author announced in [15, 26] that, when generalizing his methods, he also used generalized theta-functions with characteristics to study the quadratic forms

$$Q(x_1, \dots, x_k), \quad k > 2, \quad (x_1, \dots, x_k) \equiv (b_1, \dots, b_k) \bmod g, \tag{2}$$

The author gave the general definition of quadratic forms of the Liouville type with the aid of these functions for the quadratic forms (2) and proved the theorems on the finiteness of classes of quadratic forms of the Liouville type defined by the theta-functions with characteristics for the quadratic forms (2) of the Jacobi, Liouville, and Weil type.

These theorems generalize a part of the results of the author presented in the monographs by Cassels [7], Rankin [28], in overviews by Malyshev [17] and by Fomenko [20], and in the four mononographs by the author [10], by the author and Tashpulatov, and in other works [13, 14, 19]. These theorems will be proved in this paper.

1. SOME DEFINITIONS AND AUXILIARY RESULTS

Definition 1 (see, e.g., [25, 27]). Let Γ be the modular group, i.e., the group of all linear permutations $\tau_1 = \frac{a\tau+b}{c\tau+d}$, where $ad - bc = 1$. Suppose also that $\Gamma_0(N)$ denotes the subgroup of the group Γ whose permutation satisfies the congruence $C \equiv 0 \pmod N$. Then an analytic function $\mathcal{F}(\tau)$ is the entire modular form of dimension r which is adjoined to the subgroup $\Gamma_0(N)$ if it satisfies the following conditions:

(1) $\mathcal{F}(\tau)$ is regular and single-valued in the upper half-plane,

(2) for each permutation of the group $\Gamma_0(N)$, we have

$$\mathcal{F}\left(\frac{a\tau+b}{c\tau+d}\right) = \mathcal{E}(d)(c\tau+d)^r\mathcal{F}(\tau), \qquad |\mathcal{E}(d)| = 1,$$

(3) in a neigbourhood of $\tau = \infty$, we have the expansion

$$\mathcal{F}(\tau) = \sum_{m=0}^{\infty} C_m e^{\frac{2\pi i m}{N}\tau};$$

(4) in a neighborhood of $\tau = -\frac{d}{c}$ $(c \neq 0,\ (c,d) = 1)$ we have the expansion

$$(c\tau+d)^r\mathcal{F}(\tau) = \sum_{m=0}^{\infty} C'_m e^{2\pi i \frac{m}{n}\frac{a\tau+b}{c\tau+d}}.$$

In a similar way, we can define the modular form adjoined to the subgroup $\Gamma(N)$, where $\Gamma(N)$ denotes the subgroup of the group Γ whose permutations satisfy the congruence $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod N$.

Lemma 1 (see [21, 29]). *Let*

$$\vartheta(\tau, Q, P_l, \eta) = \sum_{\substack{x_1,\dots,x_{2k}=-\infty \\ x_i \equiv \eta_i \ (\mathrm{mod}\ N)\ (i=1,2,\dots,2k)}}^{\infty} P_l(x_1,\dots,x_{2k}) \exp\left(2\pi i\tau \frac{Q(x_1,\dots,x_{2k})}{N^2}\right), \tag{3}$$

$Q(x_1,\dots,x_{2k})$ *be an integral positive quadratic form of degree* N, $P_l(x_1,\dots,x_{2k})$ *be a solid spherical function of the order* l *with respect to the quadratic form* Q, η_i *be integers satisfying the condition*

$$\frac{\partial}{\partial x_i} Q(x_1,\dots,x_{2k})\Bigg|_{\substack{x_1=\eta_1 \\ \vdots \\ x_{2k}=\eta_{2k}}} \equiv 0 \pmod N, \qquad \eta = (\eta_1,\dots,\eta_{2k}),$$

and let $\left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)$ *be a unimodular matrix. Then*

$$\frac{\vartheta\left(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}, Q, P_l, \eta\right)}{(\gamma\tau+\delta)^{k+l}} = \mathcal{E}(d)e^{2\pi i\alpha\beta Q(\eta)}\vartheta(\tau, Q, P_l, \alpha\eta)$$

for $\left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right) \in \Gamma_0(N)$, *where* $\mathcal{E}(d)$ *is a real character* $\bmod N$ *satisfying the condition*

$$\mathcal{E}(-1) = (-1)^k, \qquad \mathcal{E}(n) = \left(\frac{\Delta}{n}\right), \quad \Delta = 0, 1 \pmod 4,$$

Δ *is the discriminant of the quadratic form* Q.

In particular, setting $\left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right) \in \Gamma'(N)$, we have

$$\frac{\vartheta\left(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}, Q, P_l, \eta\right)}{(\gamma\tau+\delta)^{k+l}} = \vartheta(\tau, Q, P_l, \eta),$$

where $\Gamma(N) = \Gamma'(N)/\{\pm I\}$, $I = \left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right)$.

(Series (3) for $P_l = 1$ can be represented as the sum $E(\tau) + \psi(\tau)$ of the Eisenstein series and a parabolic form.)

Thus, $\vartheta(\tau, Q, P_l, \eta)$ is a modular form of weight $k+l$ which is adjoined to the group $\Gamma'(N)$. For $l = 0$, we set $P_0 = 1$, and in the case $P_0 = 1$ and $\eta = (0, \dots, 0)$, we set

$$\vartheta(\tau, Q, P_l, \eta) = \vartheta(\tau, Q) = \sum_{x_1,\dots,x_{2k}=-\infty}^{\infty} e^{2\pi i\tau Q(x_1,\dots,x_{2k})} = \sum_{m=0}^{\infty} M[m = Q]e^{2\pi i\tau m},$$

where $M[m = Q]$ is the number of representations of a natural number by the form Q, i.e., the number of solutions to the undefined equation $m = \frac{1}{2}x'Ax$. It follows from Lemma 1 that

$$\vartheta(\tau, Q, 1, \eta) = \vartheta(\tau, Q, \eta) = \sum_{\substack{x\\ x\equiv\eta \pmod N\\ A\eta\equiv 0 \pmod N}} e^{\pi i\tau\frac{x'Ax}{N^2}} = \sum_x e^{\pi i\tau\left(x'+\frac{\eta'}{N}\right)A\left(x+\frac{\eta}{N}\right)}$$

$$= \sum_{m=0}^{\infty} M[2Nmt = (Nx'+\eta')A(Nx+\eta)]e^{\frac{2\pi itm\tau}{N}}, \qquad t = \left(N, \frac{\eta'A\eta}{2N}\right),$$

$$\vartheta(\tau, Q, \eta) = \sum_{m=0}^{\infty} r(Q, m, \eta)e^{\frac{2\pi itm\tau}{N}}, \qquad t = \left(N, \frac{\eta'A\eta}{2N}\right),$$

$$M[2Nmt = (Nx'+\eta')A_Q(Nx+\eta)] = r(Q, m, \eta).$$

Consider the function

$$M[m = Q(x_1, \dots, x_{2k})], \quad x \equiv b \pmod g, \quad b = \begin{pmatrix} b_1\\ \vdots\\ b_{2k}\end{pmatrix}, \quad g = \begin{pmatrix} g_1\\ \vdots\\ g_{2k}\end{pmatrix},$$

where b_i, g_i are integers.

Let $\eta = gN_Q \times b$.

Consider the quadratic form R with the matrix $A_R = g^2 Aa$.

The step N_R of the form R is equal to $g^2 N_Q$, $A_R \times \eta \equiv 0 \pmod{N_R}$.

We have

$$M[m = Q(x_1, \dots, x_{2k}), x \equiv b \,(\operatorname{mod} g)] = M[2mN_R^2 = (\eta' + N_R x')A_R(\eta + N_R x)] = r(R, m, \eta)$$

since

$$t = \left(\frac{\eta' A_R \eta}{2N_R}, N_R\right) = \left(N_R \frac{b' A_Q b}{2}, N_R\right) = N_R.$$

Thus,

$$\begin{aligned}\vartheta(\tau, R, \eta) &= \sum_{\substack{x \equiv \eta \,(\operatorname{mod} N_R) \\ R\eta \equiv 0 \,(\operatorname{mod} N_R)}} e^{\pi i \tau \frac{x' R x}{N_R^2}} = \sum_{m=0}^{\infty} r(R, m, \eta) e^{\frac{2\pi i t m \tau}{N_R}} \\ &= \sum_{m=0}^{\infty} M[m = Q(x_1, \dots, x_{2k}), x \equiv b \,(\operatorname{mod} g)] e^{\frac{2\pi i t m \tau}{N_R}} \\ &= \sum_{m=0}^{\infty} M[m = Q(x_1, \dots, x_{2k}), x \equiv b \,(\operatorname{mod} g)] e^{2\pi i m \tau}.\end{aligned}$$

Thus, we find from Lemma 1 that the following assertion is valid:

Lemma 2. *The function*

$$\vartheta(\tau, Q, b, g) = \sum_{m=0}^{\infty} M[m = Q(x_1, \dots, x_{2k}), x \equiv b \,(\operatorname{mod} g)]$$

is a modular form adjoined to the group $\Gamma'(N_R)$; $N_R = g^2 N_Q$.

Following Hecke [24, 25], we decompose the theta-series $\vartheta(\tau, R, \eta)$ into the sum of the Eisenstein series and a parabolic form, i.e.,

$$\vartheta(\tau, Q, b, g) = \vartheta(\tau, R, \eta) = \sum_{m=0}^{\infty} M[m = Q(x_1, \dots, x_{2k}), x \equiv b \,(\operatorname{mod} g)] e^{2\pi i \tau} = E(\tau) + \psi(\tau).$$

The Eisenstein series corresponding to the positive quadratic form

$$Q = \frac{1}{2} \sum_{i,k=1}^{n} a_{i,k} x_i x_k$$

with the matrix $A = (a_{ik})$ and discriminant $\Delta = (-1)^{[n/2]} \det A$ is defined in the following way:

$$E(\tau, Q) = 1 + \frac{e^{\pi i n/4}}{|\Delta|^{1/2}} \sum_{q=1}^{\infty} \sum_{h=1}^{\infty} \frac{\mathcal{S}(Qh, q)}{q^{n/2}(q\tau - h)^{n/2}},$$

where

$$\mathcal{S}(Qh,q)=\sum_{x_1,\ldots,x_n=1}^{q} e^{\frac{2\pi iQh}{q}}$$

is the Gauss sum.

Let

$$E(\tau,z,Q,b,g)=\delta+e^{\pi in/4}g^{-n/2}|\Delta|^{-1/2}\sum_{q=1}^{\infty}\sum_{h=-\infty}^{\infty}\frac{\mathcal{S}(Qh,q,b,g)}{q^{n/2}(q\tau-h)^{n/2}(g\tau-h)^{z}}, \tag{4}$$

$$\delta=\begin{cases}1, & b_i\equiv 0 \pmod g,\ i=1,\ldots,n,\\ 0 & \text{otherwise,}\end{cases}$$

$$\mathcal{S}=(Qh,q,b,g)=\sum_{\substack{x \bmod gq\\ x\equiv b \pmod g}} e^{\frac{2\pi iQh}{gq}}$$

be the Gauss sum.

Function (4) converges absolutely for $\operatorname{Re} z>2-\frac{n}{2}$.

Van der Blij [23] showed that in the case $n>4$ the following result was valid:

Lemma 3. *The Fourier coefficients of the function*

$$E(\tau,0,Q,b,g)=E(\tau,z,Q,b,g)\big|_{z=0}$$

constitute a singular Hardy–Littlewood series[1] *corresponding to the function*

$$M[m=Q(x_1,\ldots,x_n),x\equiv b \pmod g].$$

Lemma 4 (see [25, p. 62]). *The step and the discriminant of the quadratic form $Q(x)$ have the same simple divisors.*

For the given step N and the number $2k$ of variables, there is only a finite number of discriminants of positive definite quadratic integer-valued forms $Q(x)$. They are divisors of N^{2k}.

Lemma 5 (see [16, pp. 58– 59]). *Let $\rho_n(m)$ be the sum of the singular Hardy–Littlewood series corresponding to the quadratic form $Q(x_1,\ldots,x_n)$ for $(x_1,\ldots,x_n)\equiv(b_1,\ldots,b_n) \pmod g$. Then*[2]

$$\rho_n(m,Q)=\frac{\pi^{nm^{n/2-1}/2}}{d^{1/2}\Gamma(N)}H_g,\qquad b_1,\ldots,b_n(Q,m),\ H_g,\qquad b_1,\ldots,b_n(Q,m)=\prod_p\chi(p).$$

According to the results of [16], we set

$$f(x_1,\ldots,x_n)=\sum_{\alpha=1}^{s}p^{l_\alpha}\varphi_\alpha=\sum_{\beta=1}^{n}a_\beta p_\beta x_\beta^2 \pmod{p^{l_s+1}},$$

[1] The definition of these series and formulas for their computation are given in the paper by A. V. Malyshev [16].
[2] The formulas for $\chi(p)$ will be written in the sequel; for the definition of $\Gamma(n)$ see, e.g., [4].

for an odd p, where a_β are integers, $(a_\beta, p) = 1$, $0 \le l_1 \le \dots \le l_s$; $\varphi_1, \dots, \varphi_s$ are proper integral forms with pairwise disjoint variables; the number of their variables is $n_1 = n(\varphi_1), \dots, n_s = n(\varphi_s)$, $n_1 + n_2 + \dots + n_s = n$; their determinants are relatively prime to p; $a_1, \dots, a_n$ are integers which are relatively prime to p; $\varepsilon_1 \ge 0, \dots, \varepsilon_n \ge 0$.

Let $p^{\nu_1} \parallel b, \dots, p^{\nu_n} \parallel b_n$; moreover, if $b_\alpha \equiv 0 \pmod{p^u}$, then we assume that $b_\alpha = 0$, $\nu_\alpha = \infty$ $(\alpha = 1, 2, \dots, n)$; $\tau = \min(u + \nu_\alpha + \varepsilon_\alpha)$ (if $b_1 \equiv \dots \equiv b_n \equiv 0 \pmod{p^u}$, then $\tau = \infty$). We denote $p^w \parallel [m - f(b_1, \dots, b_n)]$, and if $w \ne \infty$, i.e., if $[m \ne f(b_1, \dots, b_n)]$, then $\{m - f(b_1, \dots, b_n)\} = p^w m_1$. The following assertions hold true.

Lemma 6 (it follows from [16, Remark 3, pp. 59–60]). *Let $p \mid dg$, $w = 0$. Then $\chi_p = 1$ if $\tau = 0$,*

$$\chi_p = \begin{cases} 1 - p^{-n_1/2}\left(\dfrac{d_1}{p}\right) i^{\left(\frac{p-1}{2}\right)^2 n_1} & n_1 \equiv 0 \pmod 2 \\[2ex] 1 + \left(\dfrac{-m_1}{p}\right)^{\frac{1-n_1}{2}} \left(\dfrac{d_1}{p}\right) i^{\left(\frac{p-1}{2}\right)^2 (n_1+1)} & n_1 \equiv 1 \pmod 2 \end{cases}$$

if $\tau > 0$.

Lemma 7 (it follows from the results of [16]). *Let g be positive integers, $m = 2^w m_1 + Q(b_1, \dots, b_n)$, $w = 0$. Then*

$$|\chi_2| < c_1, \qquad |\chi_2| < 13 \quad \textit{for } g = 1.$$

Lemma 8 (see [1]). *Let Q be a quadratic form in the field $\mathcal{F}_p$ ($\mathcal{F}_p$ is the field of residues* mod p) *of rank ≥ 2 (p is an odd prime), and let $a \not\equiv 0 \pmod p$. Then the congruence $Q \equiv a \pmod p$ is solvable.*

Lemma 9 (see [16, p. 63]). *Let p be an odd prime which does not divide dg, $p^w \parallel m$, $m = p^w m_1$. Then denoting*

$$\delta = \begin{cases} \left(\dfrac{(-1)^{n/2}}{p}\right) & \textit{if } n \textit{ is even} \\[2ex] \left(\dfrac{(-1)^{(n-1)/2} d m_1}{p}\right) & \textit{if } n \textit{ is odd,} \end{cases}$$

we have

$$\chi(p) = \begin{cases} \left(1 - \dfrac{\delta}{p^{n/2}}\right)\left(1 + \dfrac{\delta}{p^{2(n/2-1)}} + \dots + \dfrac{\delta^w}{p^{w(n/2-1)}}\right) & \textit{if } n \textit{ is even} \\[2ex] \left(1 - \dfrac{1}{p^{n-1}}\right)\left(1 + \dfrac{1}{p^{n-2}} + \dfrac{1}{p^{2(n-2)}} + \dots + \dfrac{1}{p^{\frac{w-1}{2}(n-2)}}\right) & \textit{if } n \textit{ and } w \textit{ are odd} \\[2ex] \left(1 - \dfrac{1}{p^{n-1}}\right)\left(1 + \dfrac{1}{p^{n-2}} + \dots \right. \\[2ex] \qquad \left. + \dfrac{1}{p^{(w/2-1)(n-2)}} + \dfrac{1}{p^{\frac{w}{2}(n-2)}\left(1 - \delta/p^{(n-1)/2}\right)}\right) & \textit{if } n \textit{ is odd and } w \textit{ is even.}^3 \end{cases}$$

[3]For $w = 0$, all terms in the second brackets of the last sum, except for the last one, are zero.

Hence

$$\prod_p \chi(p) < 2^\sigma \prod_p \left(1 + \frac{1}{p^2}\right) < c_\varepsilon m^\varepsilon.$$

Here σ is the number of different prime divisors of m and p does not divide $2^{n+1}dg$.

Lemma 10 (see [16, p. 71]). *Let*

$$T_p = \min\{\omega_p + 1 + 1 + (-1)^p, \tau_p\}.$$

If the congruence

$$Q(p^{u_p}\varphi_1 + b_1, \ldots, p^{u_p}\varphi_n + b_n) \equiv m \pmod{p^{T_p}}$$

is solvable, then $\chi(p) > 0$; *otherwise,* $\chi(p) = 0$.

Lemma 11 (see, e.g., [5]). *The necessary conditions for solvability of the congruence* $x^2 \equiv a \pmod m$; $m = 2^\alpha p_1^\alpha \cdots p_k^{\alpha_k}$, $(a, m) = 1$, *are the following*:

$$a \equiv 1 \pmod 4 \text{ for } \alpha = 2, \quad a \equiv 1 \pmod \alpha \text{ for } \alpha \geq 3, \quad \left(\frac{a}{p_1}\right) = 1, \ \ldots, \ \left(\frac{a}{p_k}\right) = 1.$$

Lemma 12 (see [1]). *A natural number can be represented by a certain primitive binary quadratic form of the discriminant D if and only if there exist integers $s > 0, a > 0, b$, and c such that*

$$m = as^2, \qquad b^2 - 4ac = D, \qquad (a, b, c) = 1, \qquad -a \leq b \leq a.$$

Furthermore, let D be the discriminant of a quadratic field. A natural number $m = as^2$, where a is free of the square, can be represented by a certain binary primitive form of the discriminant D if and only if the congruence $x^2 \equiv D \pmod{4a}$ is solvable.

Lemma 13 (see [3]). *Let Δ be a square-free number > 1; a and b be two relatively prime numbers, and, moreover, $(b, \Delta) = 1$, x be any integer, c, d be any real numbers, $c < d$, and let t be an odd number which is relatively prime to Δ. Then*

$$\left|\sum_{x>c}^{x \leq d} \left(\frac{a + bx}{\Delta t^2}\right)\right| < 2^k \sqrt{\Delta} \ln \Delta,$$

where k is the number of different prime divisors of the number t which do not divide b.

Lemma 13′ (see [3]). *Let*

$$(t, 2D) = 1, \qquad D = \mathcal{E} 2^n \Delta, \quad \mathcal{E} = \pm 1,$$

where D is an integer which is not the square of an integer, n is an integer, and Δ is odd positive number. Then, for any c, d, $c < d$,

$$\sum_{\eta<c}^{\eta<d} \left(\frac{Dt^2}{\eta}\right) < u,$$

where

$$u = \begin{cases} 2^{k+2}\sqrt{|D|} & \text{if } \Delta \text{ is not a square} \\ 2^{k_0+2} & \text{if } \Delta \text{ is a square,} \end{cases}$$

k is the number of different prime divisors of the number t, k_0 is the number of different prime divisors of the number Δ.

Lemma 14 (it is well known). *Let α be a real positive number, and let $A(\alpha, p_1, \dots, p_k)$ be the number of positive integers that do not exceed α and are not divisible by any of the prime numbers $p_1, \dots, p_k$. Then*

$$A(\alpha, p_1, \dots, p_k) = [\alpha] - \left[\frac{\alpha}{p_1}\right] - \dots - \left[\frac{\alpha}{p_k}\right] + \left[\frac{\alpha}{p_1 p_2}\right] + \dots + \left[\frac{\alpha}{p_k p_{k+1}}\right]$$
$$- \left[\frac{\alpha}{p_1 p_2 p_3}\right] - \dots - \left[\frac{\alpha}{p_{k-2} p_{k-1} p_k}\right] + \dots + (-1)^k \left[\frac{\alpha}{p_1 p_2 \cdots p_k}\right].$$

Lemma 15 (see [4]). *Let $\tau(n)$ be the number of positive divisors of the number n, and let ε be a sufficiently small positive number. Then we have*

$$\tau(n) \le \left(\frac{2}{\varepsilon \ln 2}\right)^{2^{1/\varepsilon}} n^{\varepsilon}.$$

Let σ be the number of different prime divisors of the number n, and let $0 < \varepsilon < 1$. Then

$$2^{\sigma} < 2^{2^{1/\varepsilon}} n^{\varepsilon}.$$

Definition 2. Let

$$\vartheta_{gh}(\tau, P_\nu, Q) = \sum_{x \equiv g \pmod N} (-1)^{\frac{h' A(x-g)}{(-1)^{N^2}}} P_\nu(x) e^{\frac{\pi i \tau x' A x}{N^2}},$$

$Ag \equiv 0 \pmod N$, $Ah \equiv 0 \pmod N$, N be the step of the quadratic form Q, and P_ν be the spherical function of order ν corresponding to the positive quadratic form Q.

ϑ_{gh} is the *generalized theta-function with characteristics g, h.*

The modular properties of this function were studied by Schoenberg [29], Shimura [30], and Vepkhvadze [2].

We shall now give the general definitions of quadratic forms of the Liouville type, and, in particular, of the Gauss–Jacobi forms.

Let

$$Q(x) = Q(x_1, \dots, x_k) = \frac{1}{2} \sum_{i,j=1}^{k} x_i x_j = \frac{1}{2} x' A x \tag{5}$$

be an integer-valued form of k variables, where $x = \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix}$, $x' = (x_1, \dots, x_k)$ and $(x_1, \dots, x_k) \equiv (b_1, \dots, b_k) \bmod g$,

$$\sum_{x \equiv b \pmod g} e^{2\pi i \tau Q(x)} = \sum_{x \equiv b \pmod g} e^{\pi i \tau x' A x} = E(\tau, Q) + \theta(\tau). \tag{6}$$

Here τ is a complex variable with $\operatorname{Im} \tau > 0$, $E(\tau)$ is an Eisenstein series, and $\theta(\tau)$ is a parabolic form.

Definition 3. If $\theta(\tau) = 0$ in (6), then the quadratic form (5) is called a form of the *Gauss–Jacobi type.*

Definition 4. If, in (6), for $k \geq 4$ and even k, $\theta(\tau)$ can be represented as a finite linear combination of generalized (binary) theta-functions with characteristics

$$\vartheta_{gh}(\tau, a, P_\nu, Q_i) = \sum_{x \equiv a_i \,(\mathrm{mod}\, N_i)} (-1)^{\frac{h' A_i (x-a)}{N_i^2}} P_\nu(x+g) e^{\pi i \tau (x+g)' A_i (x+g)}, \tag{7}$$

where A_i is the matrix of the quadratic form Q_i, $Q_i = \frac{1}{2} x' A x$, $A_i a_i \equiv 0 \,(\mathrm{mod}\, N_i)$, $A_i 2 g_i \equiv 0 \,(\mathrm{mod}\, N_i)$, $a_i = \binom{a_{i,1}}{a_{i,2}}$, $g_i = \binom{g_{i,1}}{g_{i,2}}$, $P_{k-1,i}(x)$ is the spherical function of order $(k-1)$ with respect to the quadratic form $\frac{1}{2} x' A x$, A_i is a second-order matrix, $x = \binom{x_1}{x_2}$, $x' = (x_1, x_2)$, then the quadratic form (5) is called a *form of the Liouville type.*

Definition 4′. If in

$$\sum_{x \equiv b \,(\mathrm{mod}\, g)} e^{\pi i \tau x' A x} - \sum_m \rho_{gh}(m) e^{2\pi i \tau m} = \theta(\tau), \tag{8}$$

for $k \geq 4$ and even k, $\theta(\tau)$ can be represented as a finite linear combination of generalized (binary) theta-functions with characteristics (7), then the quadratic form (5) is called a *form of the Liouville type*, and the formula for the number of its representations, which follows from (8), is also called a *formula of the Liouville type*; ρ_{gh} is the sum of the singular Hardy–Littlewood series corresponding to the series

$$\sum_{x \equiv e \,(\mathrm{mod}\, g)} e^{\pi i \tau x' A x}.$$

2. FINITENESS OF THE NUMBER OF CLASSES OF PRIMITIVE QUADRATIC FORMS OF THE LIOUVILLE TYPE

The aim that we persue in the sequel is to construct a number m satisfying the following conditions:

(a) $0 < \rho_n(m) < 1$ for $d > C$, $C = \mathrm{const} > 0$;

(b) $m N_{Ri}^2 (N_{Ri} | N_R)$ cannot be represented in the form

$$m N_{Ri}^2 = \frac{1}{2} (x+g)' A_{Ri} (x+g),$$

where $\frac{1}{2} x' A_{Ri} x$ is a quadratic form with matrix $A_{Ri} = g_i^2 A a$, $N_R = g^2 N a$, N_{Ri} runs over all divisors of N.

Taking into account that $M[m = Q(x_1, \ldots, x_n), x \equiv b \,(\mathrm{mod}\, g)]$ is an integer, we deduce from (a), (b), and the definition of quadratic forms of the Liouville type the theorem on the finiteness of quadratic form of the Liouville type.

We assume, for defineteness, that the rank of the quadratic form Q over $\mathcal{F}_{p_1}, \ldots, \mathcal{F}_{p_t}$ is equal to 1 and that this rank is greater than or equal to 2 over $\mathcal{F}_{p_{t+1}}, \ldots, \mathcal{F}_{p_k}$ (provided that they exist) (the rank of Q over $\mathcal{F}_{p_i}$, $i = 1, 2, \ldots, k$, cannot be zero since it is assumed that the quadratic form Q is primitive).

B, B_i are absolute constants ($i = 1, 2, \ldots$), B_δ is a constant dependent only on δ, and β, β_1, β_2 is a given sequence of numbers ± 1.

By the results of [16] (Remarks 4 and 5, pp. 65–71), we can choose m_1 belonging to a given primitive arithmetic progression $8k+l \pmod 8$ such that $x(2) \neq 0$ for a given m_1. (We say that m_1 satisfies condition (E).)

According to Lemma 5, we assume that $m = Q(b_1, \dots, b_n) + m_1$, $(m_1, p) = 1$ for $P \mid 2dg$, i.e., $w = 0$.

Consider the expression

$$N = \frac{1}{2} \sum_{\substack{T/2+Q(b_1,\dots,b_n) \le x \le T+Q(b_1,\dots,b_n) \\ x \text{ is odd}}} \left\{ 1 - \left(\frac{\beta' 2^\nu \times 4}{x} \right) \right\}, \qquad \nu = 0 \text{ or } 1,$$

$$T = 2^s \times 2^{k+1} \times 8.5 \prod_{i=1}^{k} \left(1 - \frac{1}{p_i} \right)^{-1}, \qquad Q(b_1, \dots, b_n) = q_1^{\delta_1} \cdots q_s^{\delta_s},$$

N is the number of odd x satisfying the condition

$$\left(\frac{\beta' 2^\nu \times 4}{x} \right) = \beta, \qquad (x, Q) = 1, \tag{9}$$

$$x \in \left[\frac{T}{2} + Q(b_1, \dots, b_n), T + Q(b_1, \dots, b_n) \right], \qquad N = \frac{T}{4} + \frac{\theta}{4}, \quad |\theta| < 1.$$

We denote by R the numbers satisfying condition (9). Let $m = m_2 R = Q + m_1$, $(m_2, R) = 1$. The amount of $m_2 R = Q + m_1 \equiv 0 \pmod{R^2}$ which are less than $Q + BT$ is $< (Q+BT)/R^2$.

Consider now the expression

$$N = \frac{1}{2^t} \sum_{\substack{1 \le x \le x BT_2 \\ x = m_1 = m_2 R - Q}} \left\{ \left(1 + \beta_1 \left(\frac{x}{p_1 \Phi_1^2} \right) \right) \cdots \left(1 + \beta_t \left(\frac{x}{p_t \Phi_t^2} \right) \right) \right\},$$

where x satisfies condition (E), $(x, 2p_1, \dots, p_k) = 1$.

N is the amount of numbers in the closed interval $[1, BT]$ satisfying the condition

$$\left(\frac{x}{p_1} \right) = \beta_1, \quad \dots, \quad \left(\frac{x}{p_t} \right) = \beta_t, \qquad (x + Q, R^2) = 1,$$

$$N = \frac{BT + Q - l}{8} \prod_{i=1}^{k} \left(1 - \frac{1}{p_i} \right) + \theta \times 2^{2k+1} \sqrt{p_1 \cdots p_t} \, \ln(p_1 \cdots p_t) + \theta_1 \tau_1 \left(\prod_{i=1}^{k} p_i \right)$$
$$+ \theta_2 \frac{BT + Q}{\left(2^{2k+1} \times 2^s \times 8.5 \prod_{i=1}^{k} (1 - 1/p_i)^{-1} \right)^2}, \qquad \Phi_i = \frac{p_1 \cdots p_k}{p_i}.$$

By the choice of m_1 and R, we obtain the following result.

Theorem 1. *Let $d = 2^\alpha p_1^{2\alpha_1} \cdots p_k^{2\alpha_k}$ be the determinant of the positive quadratic form $Q(x_1, \dots, x_n)$, and let n be even.*

We assume, for definiteness, that the rank of the quadratic form Q over $\mathcal{F}_{p_1}, \dots, \mathcal{F}_{p_t}$ is equal to 1 and this rank is greater than or equal to 2 over $\mathcal{F}_{p_{t+1},\dots,\mathcal{F}_{p_k}}$ (provided that they exist). ($\mathcal{F}_{p_i}$ is the residue field modulo p_i.)

We denote $m = m_2R = Q(b_1, \dots, b_{2n}) + L$. *There exist* m *and* L *satisfying the following conditions*:

I. L *satisfies condition* (E).

II. m *contains a prime number* q *of odd degree satisfying the condition*

$$\left(\frac{\beta \times 2^\nu \times 4}{q}\right) = -1, \qquad \text{where } \nu \text{ is an integer}, \quad \nu \geq 0.$$

III. $\left(\dfrac{L}{p_1}\right) = \beta_1, \dots, \left(\dfrac{L}{p_t}\right) = \beta_t$.

IV. $L < B \times 5 \times 8 \times 2^{2k+1}(p_1 \cdots p_t)^{1/2} \ln^2(p_1 \cdots p_t)$.

V.

$$m = Q(b_1, \dots, b_n) + L < Q + B \times 5 \times 8 \times 2^{2k+1}(p_1 \cdots p_t)^{1/2} \ln^2(p_1 \cdots p_t),$$

$$0 < \rho(m, Q) < c_2 \frac{\pi^{n/2}\big(Q + 5 \times 8 \times 2^{2k+1}(p_1 \cdots p_t)^{1/2} \ln^2(p_1 \cdots p_t)\big)^{n/2-1}}{\big(2^{r_1} p_1^{2\alpha_1} \cdots p_t^{2\alpha_t}\big)^{1/2} \big(p_{t+1}^{2\alpha_{t+1}} \cdots p_k^{2\alpha_k}\big)^{1/2} \Gamma(n/2)} 2^k (Q + L)^{\varepsilon_1} g^{\varepsilon_2}, \quad (10)$$

$$2\alpha_i \geq n - 1, \quad 1 \leq i \leq t.$$

We deduce from (10) that $0 < \rho_n(L) \leq 1$ $(n \geq 4)$ for sufficiently large d and sufficiently small ε_2',

$$Q(b_1, \dots, b_n) < \frac{\Gamma(n/2)^{2/(n-2)-\varepsilon}}{\pi^{n(n-2)/4}} d^{1/(n-2)-\varepsilon_2'}, \qquad g < c_2' d. \quad (11)$$

Consider the function

$$M\Big[m = m_2R = Q + L = \frac{1}{2} x' A_i x, \ x \equiv b \ (\operatorname{mod} g)\Big],$$

where $\frac{1}{2} x' A_i x$ is a quadratic form of step N_i, $N_i \mid N$.

By Lemmas 11 and 12 and by Theorem 1,

$$M\Big[m = m_2R = Q + L = \frac{1}{2} x' A_i x\Big] = 0. \quad (12)$$

Taking into account (11), (12), and the fact that $M[m = \frac{1}{2} x' A x, \ x \equiv b \ (\operatorname{mod} g)]$ is an integer, we deduce the following results:

Theorem 2. *Assume that* $Q = \frac{1}{2} x' A x$ *is an integer-valued primitive positive quadratic form of* n *variables with determinant* $d = 2^r \Delta_1^2$ (Δ_1 *is odd*, $r \geq 0$ *is an integer*), $n \geq 4$; n *is even*, x *is a column vector*, x' *is a row vector*, $b' = (b_1, \dots, b_n)$, $b_1, \dots, b_n$ *are integers, and* g *is a natural number. Then there exists* $c(n)$ *such that for* $d > c(n)$, *we have*

$$Q(b_1, \dots, b_n) < \frac{\Gamma(n/2)^{2/(n-2)-\varepsilon}}{\pi^{n(n-2)/4}} d^{1/(n-2)-\varepsilon_2'}$$

($\varepsilon > 0$, $\varepsilon_2' > 0$ *are sufficiently small numbers*), $g < c_2' d$ (c_2 *is an absolute constant*), *and there are no Liouville forms among* Q *for* $x' \equiv b'$ (mod g).

Theorem 3. *The number of classes of primitive positive quadratic forms* $Q(x_1, \ldots, x_n) = \frac{1}{2}x'Ax$, $n \geq 4$, *where* n *is any fixed even number with determinant* $d = 2^r \Delta_1^2$ (Δ_1 *is odd*), $x' \equiv b' \pmod g$, *of the Liouville type is finite for*

$$Q(b_1, \ldots, b_n) < \frac{\Gamma(n/2)^{2/(n-2)-\varepsilon}}{\pi^{n(n-2)/4}} d^{1/(n-2)-\varepsilon_1'}, \qquad g < c_2' d.$$

Other theorems of the author on the finiteness of quadratic forms of the Liouville type with any definition can be similarly generalized. In this case, it is necessary to apply the results of the papers on the distribution of quadratic nonresiduals by Vinogradov [3] and Burgess [22].

The final results on the finiteness of quadratic forms of the Liouville type follow from Vinogradov's conjecture on the minimal quadratic nonresidual [6].

REFERENCES

1. Borevich, Z. I. and Shafarevich, I. R., *Teoriya chisel* (Number Theory), 2nd ed., Moscow: Nauka, 1972.
2. Vepkhvadze, T. V., *Predstavlenie chisel polozhitel'nymi kvadratichnymi formami i svyazannye s nim voprosy iz analiticheskoi arifmetiki kvadratichnykh form* (Representation of Numbers by Positive Quadratic Forms and Related Problems From Analytic Geometry of Quadratic Forms), Abstract of D. Sc. Dissertation, Tbilisi, 1993.
3. Vinogradov, I. M., *Izbrannye trudy* (Selected Works), Moscow: Akad. Nauk SSSR, 1952.
4. Vinogradov, I. M., *Metod trigonometricheskikh summ v teorii chisel* (Method of Trigonometrical Sums in Number Theory), Moscow: Nauka, 1971.
5. Vinogradov, I. M., *Osnovy teorii chisel* (Fundamentals of Number Theory), Moscow: Nauka, 1972.
6. Gel'fond, A. O. and Linnik, Yu. V., *Elementarnye metody v analiticheskoi teorii chisel* (Elementary Methods in Analytic Number Theory), Moscow, 1962.
7. Cassels, J., *Rational Quadratic Forms*, London: Academic Press, 1978.
8. Kogan, L. A., Theory of Modular Forms and the Problem of Finding Formulas for the Amount of Representations of Numbers by Positive Quadratic Forms, *Dokl. Akad. Nauk SSSR*, 1968, vol. 182, no. 2, pp. 259–261.
9. Kogan, L. A., Liouville Formulas and Parabolic Forms Generated by Generalized Binary Theta-Series, *Lit. Mat. Sb.*, 1968, vol. 9, no. 3.
10. Kogan, L. A., *O predstavlenii tselykh chisel polozhitel'no opredelennymi kvadratichnymi formami* (On the Representation of Integers by Positive Definite Quadratic Forms), Tashkent: Fan, 1971.
11. Kogan, L. A., Vinogradov's Conjecture on the Least Quadratic Nonresidue and Representation of Numbers by Quadratic Forms, *Dokl. Akad. Nauk SSSR*, 1971, vol. 198, no. 6, pp. 1263–1264.
12. Kogan, L. A., Elliptic Curves and Modular Forms, *Dokl. Akad. Nauk SSSR*, 1972, vol. 204, no. 3, pp. 275–278.
13. Kogan, L. A., Tashpulatov, B. T., and Faisiev, S. R., *Predstavlenie chisel kvadratichnymi formami* (Representation of Numbers by Quadratic Forms), Tashkent: Fan, 1980.
14. Kogan, L. A., Tashpulatov, B. T., and Dusumbetov, A. D., *Predstavlenie chisel kvadratichnymi formami* (Representation of Numbers by Quadratic Forms), Tashkent: Fan, 1989.
15. Kogan, L. A., Generalized Theta-Functions with Characteristics and Representation of Numbers by Quadratic Forms, in: *International Conference "Sovremennye problemy teorii chisel i ee prilozheniya"* (Modern Problems of Number Theory and its Applications), Abstract of Reports, Tula, 1996.
16. Malyshev, A. V., On Representation of Integers by Positive Quadratic Forms, *Trudy Mat. Inst. Akad. Nauk SSSR*, 1962, vol. 65.
17. Malyshev, A. V., On Formulas for the Amount of Representations of Numbers by Positive Quadratic Forms, in: *Aktual'nye problemy analiticheskoi teorii chisel* (Actual Problems of Analytic Number Theory), Minsk: Nauka i tekhnika, 1974.
18. Mumford, D., *Lektsii o teta-funktsiyakh* (Lectures on Theta-Functions), Moscow: Mir, 1988.
19. Tashpulatov, B. T. and Kogan, L. A., *Predstavlenie chisel kvadratichnymi formami* (Representation of Numbers by Quadratic Forms), Tashkent: Fan, 1993.
20. Fomenko, O. M., Applications of Modular Form Theory to Number Theory, in: *Itogi Nauki i Tekhniki. Algebra. Topologiya. Geometriya*, Moscow: VINITI, 1977, vol. 15.
21. Blij, F. van der, On the Theory of Quadratic Forms, *Ann. Math.*, 1940, vol. 50, pp. 875–883.

22. Burgess, D., The Distributions of Quadratic Residues and Nonresidues, *Mathematika*, 1957, vol. 4, no. 8, p. 2.
23. Eichler, M., Quadratische Formen und Modulfunctionen, *Acta Arith.*, 1958, vol. 4, pp. 217–239.
24. Hecke, E., Theorie Eisensteinischen Reichen höhrer Stufe und ihre Anbendung auf funktionen Theorie und Arithmetik, *Abh. Math. Sem. Univ. Hamburg*, 1927, vol. 5, pp. 199–224.
25. Hecke, E., *Analitische Arithmetik der positiven quadratischen Formen*, Kobenhaven, 1940.
26. Kogan, L. A., Representation of Numbers by Quadratic Forms in Connection with the Theory of Modular Forms, in: *Proc. Int. Conf. on Diophantine Analysis and its Applications in Honour of Acad. Sprindzuk*, Minsk, 1996, p. 15.
27. Ogg, A. P., *Modular Forms and Dirichlet Series*, New York: Benjamin, 1969.
28. Rankin, R. A., *Modular Forms and Functions*, Cambridge: Cambridge Univ. Press, 1977.
29. Schoenberg, B., Das Verhalten von nehrfachen Thetureihen bei Modulsubstitutionen, *Math. Ann.*, 1939, vol. 116, pp. 511–523.
30. Shimura, C., On Modular Form of Half-Integral Weight, *Ann. Math.*, 1973, vol. 97, pp. 440–481.
31. Weil, A., Über die Bestimung Dirichletscher Reihen durch Funktionalgleichungen, *Math. Ann.*, 1967, vol. 168, pp. 149–156.

Translated by S. Vakhromeev