

## ON TYPES OF SOLUTIONS OF THE LAGRANGE PROBLEM

L. N. Kurtova and N. N. Mot'kina

UDC 511.51

**Abstract.** In this paper, we present an analysis of some cases where a positive integer cannot be represented by a diagonal quadratic form with four integer variables.

**Keywords and phrases:** quadratic form, trigonometric sum, Gauss sum, comparison, Kloosterman sum, asymptotic formula.

**AMS Subject Classification:** 11D09

**1. Introduction.** In the literature on number theory, many problems are known about representing a natural number in the form of sums of various kinds. One of them is the Lagrange problem (1770) that any positive integer can be represented as the sum of no more than four squares of natural numbers:

$$l_1^2 + l_2^2 + l_3^2 + l_4^2 = N.$$

Before this problem, P. Fermat, L. Euler, and other mathematicians studied quadratic forms of a particular form. J. Lagrange established an exact relationship between the problem of representing numbers by quadratic forms and solvability of the corresponding quadratic congruence.

C. F. Gauss and then L. Dirichlet, continuing studies of Euler, created the theory of representation of natural numbers by quadratic forms. Gauss introduced sums (called now *Gauss sums*)

$$S(q, a, b) = \sum_{1 \leq l \leq q} e^{2\pi i(al^2 + bl)/q},$$

which were first examples of trigonometric sums, and showed their usefulness in many problems of number theory.

In 1926, H. Kloosterman generalized the Lagrange problem (see [4]) and considered the problem on representation of a positive natural number in the form of a diagonal quadratic form depending on four integer variables (the Kloosterman problem):

$$n = ax^2 + by^2 + cz^2 + dt^2. \quad (1)$$

For the number of solutions  $r(n)$  of Eq. (1), he obtained the asymptotic formula

$$r(n) = \frac{\pi^2}{\sqrt{abcd}} n S(n) + O(n^{17/18+\varepsilon}),$$

where

$$S(n) = \sum_{q=1}^{\infty} \frac{1}{q^4} \sum_{\substack{l=1 \\ (l,q)=1}}^q e^{-2\pi i nl/q} S(q, al, 0) S(q, bl, 0) S(q, cl, 0) S(q, dl, 0). \quad (2)$$

Moreover, in [4] some examples were considered in which the number of representations is equal to zero. Their proofs were based on the congruence theory and were absent in some cases. The question of the representation of an even number was considered by Kloosterman in more detail than the cases with an odd prime  $p$  involved in the decomposition of  $n$ .

---

Translated from *Itogi Nauki i Tekhniki, Seriya Sovremennaya Matematika i Ee Prilozheniya. Tematicheskie Obzory*, Vol. 166, Proceedings of the IV International Scientific Conference "Actual Problems of Applied Mathematics," Kabardino-Balkar Republic, Nalchik, Elbrus Region, May 22–26, 2018. Part II, 2019.

Application of exact formulas for Gauss and Ramanujan sums (see [1–3, 5]) allows one to consider in more detail cases for odd prime  $p$  for which Eq. (1) has no solutions; here  $a, b, c, d$ , and  $n$  are positive integers.

**2. Main results.** Let  $p$  be an odd prime number and  $a, b, c, d$ , and  $n$  be positive integers.

**Theorem 1.** *The equation  $n = ax^2 + by^2 + cz^2 + dt^2$  has no solutions in the following cases:*

- 1.1. *if  $n$  and  $p$  are coprime and the coefficients  $a, b, c$ , and  $d$  are divisible by  $p$ ;*
- 1.2. *if  $n$  and  $p$  are coprime, three coefficients of the quadratic form  $ax^2 + by^2 + cz^2 + dt^2$  are divisible by  $p$ , and the product of the fourth coefficient by  $n$  is a quadratic nonresidue modulo  $p$ .*

**Theorem 2.** *Let*

$$a = p^{\alpha_1} a_1, \quad (a_1, p) = 1, \quad b = p^{\beta_1} b_1, \quad (b_1, p) = 1, \\ (c, p) = 1, \quad (d, p) = 1, \quad n = p^{\eta_1} n_1, \quad (n_1, p) = 1.$$

*The equation  $n = ax^2 + by^2 + cz^2 + dt^2$  has no solutions in the following cases:*

- 2.1. *if  $\eta_1 < \alpha_1 \leq \beta_1$ ,  $\eta_1$  is an odd number, and  $(-cd)$  is a quadratic nonresidue modulo  $p$ ;*
- 2.2. *if  $\eta_1 = \alpha_1 < \beta_1$ ,  $\eta_1$  is an odd number, and  $a_1 n_1$  and  $(-cd)$  are quadratic nonresidues modulo  $p$ ;*
- 2.3. *if  $\alpha_1 < \eta_1 < \beta_1$ ,  $\alpha_1$  and  $\eta_1$  are odd numbers, and  $a_1 n_1$  and  $(-cd)$  are quadratic nonresidues modulo  $p$ .*

**Theorem 3.** *Let*

$$a = p^{\alpha_1} a_1, \quad (a_1, p) = 1, \quad b = p^{\beta_1} b_1, \quad (b_1, p) = 1, \\ c = p^{\gamma_1} c_1, \quad (c_1, p) = 1, \quad (d, p) = 1, \quad n = p^{\eta_1} n_1, \quad (n_1, p) = 1.$$

*The equation  $n = ax^2 + by^2 + cz^2 + dt^2$  has no solutions in the following cases:*

- 3.1. *if  $\eta_1 < \alpha_1 \leq \beta_1 \leq \gamma_1$  and  $\eta_1$  is an odd number;*
- 3.2. *if  $\eta_1 < \alpha_1 \leq \beta_1 \leq \gamma_1$ ,  $\eta_1$  is an even number, and  $dn_1$  is a quadratic nonresidue modulo  $p$ ;*
- 3.3. *if  $\eta_1 = \alpha_1 < \beta_1 \leq \gamma_1$ ,  $\eta_1$  is an odd number, and  $a_1 n_1$  is a quadratic nonresidue modulo  $p$ ;*
- 3.4. *if  $\alpha_1 < \eta_1 < \beta_1 \leq \gamma_1$ ,  $\eta_1$  is an odd number,  $\alpha_1$  is an even number, and  $(-a_1 d)$  is a quadratic nonresidue modulo  $p$ ;*
- 3.5. *if  $\alpha_1 < \eta_1 < \beta_1 \leq \gamma_1$ ,  $\alpha_1$  is an odd number, and*

$$\left( \frac{d}{p^{\eta_1+1}} \right) \left( \frac{a_1}{p^{\eta_1}} \right) \left( \frac{n_1}{p} \right) = -1;$$

- 3.6. *if  $\alpha_1 < \eta_1 = \beta_1 < \gamma_1$ ,  $\eta_1$  is an odd number,  $\alpha_1$  is an even number, and  $(-a_1 d)$  and  $b_1 n_1$  are quadratic nonresidues modulo  $p$ ;*
- 3.7. *if  $\alpha_1 \leq \beta_1 < \eta_1 < \gamma_1$ ,  $\eta_1$  is an even number,  $\alpha_1$  is an odd number,  $\beta_1$  is an odd number, and  $(-a_1 b_1)$  and  $dn_1$  are quadratic nonresidues modulo  $p$ ;*
- 3.8. *if  $\alpha_1 \leq \beta_1 < \eta_1 < \gamma_1$ ,  $\eta_1$  is an odd number,  $\alpha_1$  is an odd number,  $\beta_1$  is an even number, and  $(-b_1 d)$  and  $a_1 n_1$  are quadratic nonresidues modulo  $p$ ;*
- 3.9. *if  $\alpha_1 \leq \beta_1 < \eta_1 < \gamma_1$ ,  $\eta_1$  is an odd number,  $\alpha_1$  is an even number,  $\beta_1$  is an odd number, and  $(-a_1 d)$  and  $b_1 n_1$  are quadratic nonresidues modulo  $p$ .*

Note that Kloosterman proved Theorem 1 in [4] by using the congruence theory. The cases 2.1 and 2.2 were not proved in [4]. The assertion 2.3 and Theorem 3 are new (they were not considered by Kloosterman).

We present a detailed proof of Theorem 1; Theorems 2 and 3 can be proved similarly. We will need the following assertions; their proofs can be found in [5].

### 3. Auxiliary lemmas.

**Lemma 1** (equalities for the Gauss sum).

1. If  $(q_1, q_2) = 1$ , then

$$S(q_1 q_2, u, 0) = S(q_1, u q_2, 0) S(q_2, u q_1, 0).$$

2. If  $(q, 2u) = 1$ , then

$$S(q, u, 0) = \left(\frac{u}{q}\right) S(q, 1, 0),$$

where  $\left(\frac{u}{q}\right)$  is the Jacobi symbol,

$$S(q, 1, 0) = \begin{cases} \sqrt{q} \text{ if } q \equiv 1 \pmod{4}, \\ i\sqrt{q} \text{ if } q \equiv 3 \pmod{4} \end{cases} = i^{(q-1)^2/4} \sqrt{q}.$$

3. If  $(q, u) = n$ , then

$$S(q, u, 0) = n S\left(\frac{q}{n}, \frac{u}{n}, 0\right).$$

**Lemma 2** (equalities for the Ramanujan sum). Let

$$K(q, u) = \sum_{\substack{1 \leq l \leq q \\ (l, q) = 1}} e^{2\pi i u l / q}$$

is the Ramanujan sum. The following assertions hold.

1.  $K(q, -u) = K(q, u)$ .

2. For  $(q_1, q_2) = 1$ , the equality

$$K(q_1 q_2, u) = K(q_1, u_1) K(q_2, u_2)$$

holds, where  $u_1$  and  $u_2$  are defined modulo  $q_1$  and  $q_2$ , respectively, by the congruence

$$u_1 q_2 + u_2 q_1 \equiv u \pmod{q_1 q_2}.$$

3. Let  $(u, p) = 1$ , and  $\alpha > 1$ . Then

$$K(p, u) = -1, \quad K(p^\alpha, u) = 0.$$

4. Let  $u = p^\alpha u_1$ ,  $(u_1, p) = 1$ ,  $\alpha > 1$ , and  $s > 1$ . Then

$$K(p^\alpha, u) = p^{\alpha-1}(p-1), \quad K(p^{\alpha+1}, u) = -p^\alpha, \quad K(p^{\alpha+s}, u) = 0.$$

**Lemma 3** (equalities for the generalized Ramanujan sum). Let  $p$  be an odd prime number and

$$K_p(p^\alpha, u) = \sum_{\substack{l=1 \\ (l, p^\alpha)=1}}^{p^\alpha} \left(\frac{l}{p}\right) e^{2\pi i u l / p^\alpha}$$

is the generalized Ramanujan sum. The following assertions hold.

1. Let  $(u, p) = 1$ ,  $\alpha > 1$ . Then

$$K_p(p, u) = S(p, u, 0), \quad K_p(p^\alpha, u) = 0.$$

2. Let  $u = p^\alpha u_1$ ,  $(u_1, p) = 1$ ,  $\alpha > 1$ , and  $s > 1$ . Then

$$K_p(p^\alpha, u) = 0, \quad K_p(p^{\alpha+1}, u) = p^\alpha S(p, u_1, 0), \quad K_p(p^{\alpha+s}, u) = 0.$$

**4. Proof of Theorem 1.** For the singular series  $S(n)$  of the asymptotic formula (2), we consider the function

$$\Phi(q) = \frac{1}{q^4} \sum_{\substack{l=1 \\ (l,q)=1}}^q e^{-2\pi i n l / q} S(q, al, 0) S(q, bl, 0) S(q, cl, 0) S(q, dl, 0).$$

We show that it is multiplicative. Let  $q = q_1 q_2$ ,  $(q_1, q_2) = 1$ , and  $l = l_1 q_2 + l_2 q_1$ ; then the assertion 1.1 of Lemma 1 implies that

$$S(q, al, 0) = S(q_1 q_2, al_1 q_2 + al_2 q_1, 0) = S(q_1, al_1 q_2^2, 0) S(q_2, al_2 q_1^2, 0).$$

We take into account the equality

$$S(q_1, al_1 q_2^2, 0) = \sum_{1 \leq j \leq q_1} e^{2\pi i a l_1 q_2^2 j^2 / q_1} = \sum_{q_2 \leq j_1 \leq q_1 q_2} e^{2\pi i a l_1 j_1^2 / q_1} = S(q_1, al_1, 0).$$

Then

$$S(q, al, 0) = S(q_1, al_1, 0) S(q_2, al_2, 0).$$

Similar arguments are also valid for other sums  $S(q, bl, 0)$ ,  $S(q, cl, 0)$ , and  $S(q, dl, 0)$ . Moreover, the assertion 2.2 of Lemma 2 implies that

$$\sum_{\substack{l=1 \\ (l, q_1 q_2)=1}}^{q_1 q_2} e^{-2\pi i n l / (q_1 q_2)} = \sum_{\substack{l_1=1 \\ (l_1, q_1)=1}}^{q_1} e^{-2\pi i n l_1 / q_1} \sum_{\substack{l_2=1 \\ (l_2, q_2)=1}}^{q_2} e^{-2\pi i n l_2 / q_2}.$$

Therefore,

$$\begin{aligned} \Phi(q_1 q_2) &= \frac{1}{q_1^4} \sum_{\substack{l_1=1 \\ (l_1, q_1)=1}}^{q_1} e^{-2\pi i n l_1 / q_1} S(q_1, al_1, 0) S(q_1, bl_1, 0) S(q_1, cl_1, 0) S(q_1, dl_1, 0) \\ &\quad \times \frac{1}{q_2^4} \sum_{\substack{l_2=1 \\ (l_2, q_2)=1}}^{q_2} e^{-2\pi i n l_2 / q_2} S(q_2, al_2, 0) S(q_2, bl_2, 0) S(q_2, cl_2, 0) S(q_2, dl_2, 0). \end{aligned}$$

Thus,  $\Phi(q_1 q_2) = \Phi(q_1) \Phi(q_2)$ , i.e., the multiplicativity is proved.

Due to the property of multiplicative functions, we obtain the representation of the singular series in the product form:

$$\sum_{q=1}^{+\infty} \Phi(q) = \prod_{p|q} (1 + \Phi(p) + \Phi(p^2) + \dots).$$

We obtain exact formulas for various products for odd prime  $p$ ,  $(n, p) = 1$ .

*4.1. Case where  $a, b, c, d$ , and  $n$  are coprime with  $p$ .* Let

$$(a, p) = 1, \quad (b, p) = 1, \quad (c, p) = 1, \quad (d, p) = 1, \quad (n, p) = 1.$$

Then for the product of Gauss sums (Lemma 1, assertion 1.2) we obtain the formula

$$S(p^\alpha, al, 0) S(p^\alpha, bl, 0) S(p^\alpha, cl, 0) S(p^\alpha, dl, 0) = \left( \frac{abcd}{p^\alpha} \right) p^{2\alpha}.$$

Therefore,

$$\Phi(p^\alpha) = \left( \frac{abcd}{p^\alpha} \right) \frac{1}{p^{2\alpha}} K(p^\alpha, -n).$$

Using Eq. 3 from Lemma 3.2, we obtain

$$\Phi(p) = - \left( \frac{abcd}{p} \right) \frac{1}{p^2}, \quad \Phi(p^\alpha) = 0, \quad \alpha > 1.$$

We obtain the first factor in the representation of the singular series in the product form:

$$\prod_{\substack{p: (a,p)=1, \\ (b,p)=1, (c,p)=1, \\ (d,p)=1, (n,p)=1}} \left( 1 - \left( \frac{abcd}{p} \right) \frac{1}{p^2} \right).$$

Note that for  $(a, p) = 1$ ,  $(b, p) = 1$ ,  $(c, p) = 1$ ,  $(d, p) = 1$ ,  $n = p^\alpha n_1$ ,  $(n_1, p) = 1$ , and  $\alpha > 1$ , formulas for the product of Gauss sum are similar:

$$\Phi(p^\alpha) = \left( \frac{abcd}{p^\alpha} \right) \frac{1}{p^{2\alpha}} K(p^\alpha, -n).$$

The formulas for the Ramanujan sum are diverse. Using Eq. 4 from Lemma 2, we obtain

$$\begin{aligned} \Phi(p^k) &= \left( \frac{abcd}{p^k} \right) \frac{p-1}{p^{k+1}}, \quad k = 1, 2, \dots, \alpha, \\ \Phi(p^{\alpha+1}) &= - \left( \frac{abcd}{p^{\alpha+1}} \right) \frac{1}{p^{\alpha+2}}, \quad \Phi(p^{\alpha+s}) = 0, \quad s > 1. \end{aligned}$$

We obtain the second factor in the representation of the singular series in the product form:

$$\prod_{\substack{p \\ (a,p)=1, (b,p)=1, \\ (c,p)=1, (d,p)=1 \\ n=p^\alpha n_1, \alpha > 1, \\ (n_1,p)=1}} \left( 1 + \left( \frac{abcd}{p} \right) \frac{p-1}{p^2} + \left( \frac{abcd}{p^2} \right) \frac{p-1}{p^3} + \dots + \left( \frac{abcd}{p^\alpha} \right) \frac{p-1}{p^{\alpha+1}} - \left( \frac{abcd}{p^{\alpha+1}} \right) \frac{1}{p^{\alpha+2}} \right).$$

As a result, for  $(a; p) = (b; p) = (c; p) = (d; p) = 1$ ,  $n = p^\alpha n_1$ ,  $(n_1, p) = 1$ , and  $\alpha \geq 1$  we have

$$\prod_{\substack{p \\ (a,p)=1, (b,p)=1, \\ (c,p)=1, (d,p)=1, \\ n=p^\alpha n_1, \alpha \geq 1, \\ (n_1,p)=1}} \left( 1 - \left( \frac{abcd}{p} \right) \frac{1}{p^2} \right) \left( 1 + \left( \frac{abcd}{p} \right) \frac{1}{p} + \left( \frac{abcd}{p^2} \right) \frac{1}{p^2} + \dots + \left( \frac{abcd}{p^\alpha} \right) \frac{1}{p^\alpha} \right).$$

If  $abcd$  is a quadratic residue modulo  $p$ , then

$$\begin{aligned} 1 - \left( \frac{abcd}{p} \right) \frac{1}{p^2} &= 1 - \frac{1}{p^2} > 3/4, \\ \left( 1 + \left( \frac{abcd}{p} \right) \frac{1}{p} + \left( \frac{abcd}{p^2} \right) \frac{1}{p^2} + \dots + \left( \frac{abcd}{p^\alpha} \right) \frac{1}{p^\alpha} \right) &= \frac{p^{\alpha+1} - 1}{p^\alpha(p-1)} > 1. \end{aligned}$$

If  $abcd$  is a quadratic nonresidue modulo  $p$ , then

$$\begin{aligned} 1 - \left( \frac{abcd}{p} \right) \frac{1}{p^2} &= 1 + \frac{1}{p^2} > 1, \\ \left( 1 + \left( \frac{abcd}{p} \right) \frac{1}{p} + \left( \frac{abcd}{p^2} \right) \frac{1}{p^2} + \dots + \left( \frac{abcd}{p^\alpha} \right) \frac{1}{p^\alpha} \right) &= \frac{p^{\alpha+1} - (-1)^{\alpha+1}}{p^\alpha(p+1)} > \frac{1}{2}. \end{aligned}$$

4.2. Case where one of the coefficients  $a, b, c,$  and  $d$  is divisible by  $p, (n, p) = 1.$  Let

$$a = p^{\alpha_1} a_1, \quad (a_1, p) = 1, \quad (b, p) = 1, \quad (c, p) = 1, \quad (d, p) = 1, \quad (n, p) = 1.$$

We find  $\Phi(p)$ :

$$\Phi(p) = \frac{1}{p^3} \left( \frac{bcd}{p} \right) S^3(p, 1, 0) \sum_{\substack{l=1 \\ (l,p)=1}}^p \left( \frac{l}{p} \right) e^{-2\pi i n l / p}.$$

Using Lemma 3 (assertion 3.1), we obtain

$$\Phi(p) = \frac{1}{p^3} \left( \frac{-bcdn}{p} \right) S^4(p, 1, 0) = \frac{1}{p} \left( \frac{-bcdn}{p} \right).$$

Let  $1 < \alpha \leq \alpha_1.$  Then

$$\Phi(p^\alpha) = \frac{1}{p^{3\alpha}} \left( \frac{bcd}{p^\alpha} \right) S^3(p^\alpha, 1, 0) \sum_{\substack{l=1 \\ (l,p^\alpha)=1}}^{p^\alpha} \left( \frac{l}{p^\alpha} \right) e^{-2\pi i n l / p^\alpha}.$$

If  $\alpha$  is even, then

$$\sum_{\substack{l=1 \\ (l,p^\alpha)=1}}^{p^\alpha} \left( \frac{l}{p^\alpha} \right) e^{-2\pi i n l / p^\alpha} = K(p^\alpha, -n) = 0$$

by Lemma 2 on the Ramanujan sum (assertion 2.3). If  $\alpha$  is odd, then

$$\sum_{\substack{l=1 \\ (l,p^\alpha)=1}}^{p^\alpha} \left( \frac{l}{p^\alpha} \right) e^{-2\pi i n l / p^\alpha} = K_p(p^\alpha, -n) = 0$$

by Lemma 3 on the generalized Ramanujan sum (assertion 3.1). Then  $\Phi(p^\alpha) = 0.$

Let  $\alpha > \alpha_1 \geq 1.$  In this case,

$$\Phi(p^\alpha) = p^{\alpha_1 - 4\alpha} \left( \frac{bcd}{p^\alpha} \right) \left( \frac{a_1}{p^{\alpha - \alpha_1}} \right) S^3(p^\alpha, 1, 0) S(p^{\alpha - \alpha_1}, 1, 0) \sum_{\substack{l=1 \\ (l,p^\alpha)=1}}^{p^\alpha} \left( \frac{l}{p^{2\alpha - \alpha_1}} \right) e^{-2\pi i n l / p^\alpha}.$$

We have

$$\sum_{\substack{l=1 \\ (l,p^\alpha)=1}}^{p^\alpha} \left( \frac{l}{p^{2\alpha - \alpha_1}} \right) e^{-2\pi i n l / p^\alpha} = 0$$

for even  $\alpha_1$  due to Lemma 2 (assertion 2.3) and for odd  $\alpha_1$  due to Lemma 3 (assertion 3.1). Then  $\Phi(p^\alpha) = 0.$

We obtain the following factor:

$$\prod_p \left( 1 + \left( \frac{-bcdn}{p} \right) \frac{1}{p} \right).$$

$a=p^{\alpha_1} a_1, (a_1,p)=1,$   
 $(b,p)=1, (c,p)=1,$   
 $(d,p)=1, (n,p)=1$

The expression in the brackets is greater than 1 if  $(-bcdn)$  is a quadratic residue modulo  $p$  and is greater than  $1/2$  and tends to 1 as  $p$  increases if  $(-bcdn/p) = -1.$

4.3. Case where two coefficients are divisible by  $p$ ,  $(n, p) = 1$ . Let

$$a = p^{\alpha_1} a_1, \quad (a_1, p) = 1, \quad b = p^{\beta_1} b_1, \quad (b_1, p) = 1, \quad (c, p) = 1, \quad (d, p) = 1, \quad (n, p) = 1.$$

We have

$$\Phi(p) = \frac{1}{p^2} \left( \frac{cd}{p} \right) S^2(p, 1, 0) \sum_{\substack{l=1 \\ (l,p)=1}}^p e^{-2\pi i n l / p} = - \left( \frac{-cd}{p} \right) \frac{1}{p}.$$

Let  $\min(\alpha_1, \beta_1) = \alpha_1$ .

4.3.1. For  $1 < \alpha \leq \alpha_1$ , taking into account the assertion 2.3 of Lemma 2, we have

$$\Phi(p^\alpha) = \frac{1}{p^{2\alpha}} \left( \frac{cd}{p^\alpha} \right) S^2(p^\alpha, 1, 0) \sum_{\substack{l=1 \\ (l,p^\alpha)=1}}^{p^\alpha} e^{-2\pi i n l / p^\alpha} = 0.$$

4.3.2. For  $\alpha_1 < \alpha \leq \beta_1$ ,

$$\Phi(p^\alpha) = p^{\alpha_1 - 4\alpha} \left( \frac{cd}{p^\alpha} \right) \left( \frac{a_1}{p^{\alpha - \alpha_1}} \right) S^2(p^\alpha, 1, 0) S(p^{\alpha - \alpha_1}, 1, 0) \sum_{\substack{l=1 \\ (l,p^\alpha)=1}}^{p^\alpha} \left( \frac{l}{p^{\alpha - \alpha_1}} \right) e^{-2\pi i n l / p^\alpha}.$$

The Ramanujan sum

$$\sum_{\substack{l=1 \\ (l,p^\alpha)=1}}^{p^\alpha} \left( \frac{l}{p^{\alpha - \alpha_1}} \right) e^{-2\pi i n l / p^\alpha}$$

is equal to zero. For even  $\alpha - \alpha_1$  this follows from the assertion 2.3 of Lemma 2, for odd—from the assertion 3.1 of Lemma 3. Therefore,  $\Phi(p^\alpha) = 0$ .

4.3.3. For  $\alpha_1 \leq \beta_1 < \alpha$ ,

$$\begin{aligned} \Phi(p^\alpha) &= p^{\alpha_1 + \beta_1 - 4\alpha} \left( \frac{cd}{p^\alpha} \right) \left( \frac{a_1}{p^{\alpha - \alpha_1}} \right) \left( \frac{b_1}{p^{\alpha - \beta_1}} \right) \\ &\quad \times S^2(p^\alpha, 1, 0) S(p^{\alpha - \alpha_1}, 1, 0) S(p^{\alpha - \beta_1}, 1, 0) \sum_{\substack{l=1 \\ (l,p^\alpha)=1}}^{p^\alpha} \left( \frac{l}{p^{2\alpha - \alpha_1 - \beta_1}} \right) e^{-2\pi i n l / p^\alpha}. \end{aligned}$$

As in the case (2), we have  $\Phi(p^\alpha) = 0$ . We obtain the factor

$$\prod_p \left( 1 - \left( \frac{-cd}{p} \right) \frac{1}{p} \right).$$

$$\begin{aligned} &a = p^{\alpha_1} a_1, \quad (a_1, p) = 1, \\ &b = p^{\beta_1} b_1, \quad (b_1, p) = 1, \\ &(c, p) = 1, \quad (d, p) = 1, \quad (n, p) = 1 \end{aligned}$$

The expression in the brackets is greater than  $1/2$  if  $(-cd)$  is a quadratic residue modulo  $p$  and is greater than  $1$  and tends to  $1$  as  $p$  increases if  $(-cd/p) = -1$ .

4.4. Case where three coefficients are divisible by  $p$ ,  $(n, p) = 1$ . Let

$$\begin{aligned} a &= p^{\alpha_1} a_1, \quad (a_1, p) = 1, \quad b = p^{\beta_1} b_1, \quad (b_1, p) = 1, \\ c &= p^{\gamma_1} c_1, \quad (c_1, p) = 1, \quad (d, p) = 1, \quad (n, p) = 1. \end{aligned}$$

We find  $\Phi(p)$ :

$$\Phi(p) = \frac{1}{p} \left( \frac{d}{p} \right) S(p, 1, 0) \sum_{\substack{l=1 \\ (l,p)=1}}^p \left( \frac{l}{p} \right) e^{-2\pi i n l / p}.$$

Using the assertion 3.1 of Lemma 3, we obtain

$$\Phi(p) = \frac{1}{p} \left( \frac{-dn}{p} \right) S^2(p, 1, 0) = \left( \frac{dn}{p} \right).$$

Let  $\alpha_1 \leq \beta_1 \leq \gamma_1$ . From the assertion 2.3 of Lemma 2 and the assertion 3.1 of Lemma 3 we obtain  $\Phi(p^\alpha) = 0$ . We have the following factor:

$$\prod_{\substack{p \\ a=p^{\alpha_1}a_1, (a_1,p)=1, \\ b=p^{\beta_1}b_1, (b_1,p)=1, \\ c=p^{\gamma_1}c_1, (c,p)=1, \\ (d,p)=1, (n,p)=1}} \left( 1 + \left( \frac{dn}{p} \right) \right).$$

The expression in the brackets vanishes in the case where  $dn$  is a quadratic nonresidue modulo  $p$  and it is equal to 2 if  $dn$  is a quadratic residue modulo  $p$ .

4.5. *Case where all coefficients are divisible by  $p$ ,  $(n, p) = 1$ .* Equation (1) has no solutions.

Thus, we have proved Theorem 1.

Theorems 2 and 3 are proved similarly. For calculating exact formulas for the function  $\Phi(p^\alpha)$ , the assertions 2.4 of Lemma 2 and 3.2 of Lemma 3 are used.

## REFERENCES

1. T. Estermann, "On Kloosterman's sum," *Mathematica*, **8**, 83–86 (1961).
2. T. Estermann, "A new application of the Hardy–Littlewood–Kloosterman method," *Proc. London Math. Soc.*, **12**, 425–444 (1962).
3. Hua Loo-Keng, *Introduction to Number Theory*, Springer-Verlag, Berlin–Heidelberg–New York (1982).
4. Kloosterman H. D., "On the representation of number in the form," *Acta Math.*, **49**, 407–464 (1926).
5. A. V. Malyshev, "On representation of integer numbers by positive quadratic forms," *Tr. Mat. Inst. Steklova*, **65**, 3–212 (1962).

L. N. Kurtova

Belgorod State National Research University, Belgorod, Russia

E-mail: kurtova@bsu.edu.ru

N. N. Mot'kina

Belgorod State National Research University, Belgorod, Russia

E-mail: motkina@bsu.edu.ru