ЧЕБЫШЕВСКИЙ СБОРНИК
Том 26. Выпуск 1.

УДК 511 DOI 10.22405/2226-8383-2025-26-1-62-75

Об асимптотиках представлений пары целых чисел суммой квадратов и линейной формой с конгруэнциальным условием специального вида

У. М. Пачев, А. Х. Кодзоков, М. М. Исакова, М. С. Нирова

Пачев Урусби Мухамедович — доктор физико-математических наук, профессор, Кабардино-Балкарский государственный университет им. Х. М. Бербекова (г. Нальчик).
e-mail: urusbi@rambler.ru
Кодзоков Азамат Хасанович — Кабардино-Балкарский государственный университет им. Х. М. Бербекова (г. Нальчик).
e-mail: Kodzoko@mail.ru
Исакова Мариана Малиловна — кандидат физико-математических наук, доцент, Кабардино-Балкарский государственный университет им. Х. М. Бербекова (г. Нальчик).
e-mail: isakova2206@mail.ru
Нирова Марина Сефовна — кандидат физико-математических наук, доцент, Кабардино-Балкарский государственный университет им. Х. М. Бербекова (г. Нальчик).
e-mail: nirova_m@mail.ru

Аннотация

В работе получены асимптотические формулы с остаточным членом для числа представлений пары целых чисел m и n соответственно суммой квадратов и линейной формой от $s \geqslant 5$ переменных, причём каждое решение такой диофантовой системы удовлетворяет конгруэнциальному условию специального вида, связанному определенным образом с линейной формой. Асимптотика с остаточным членом для числа решений такой диофантовой системы выводится при $N \to \infty$, где $N = \Delta m - n^2$, при этом Δ равняется сумме квадратов коэффициентов линейной формы.

Кроме того, получены двусторонние оценки снизу и сверху для особого ряда исследуемой диофантовой системы, опираясь при верхней оценке на формулы для числа решений сравнения второй степени $x_1^2 + \ldots + x_s^2 \equiv a \pmod{p^k}$, где p — простое число, a — целое число, k — натуральное число.

Настоящая работа является продолжением ранее проведенного исследования, относящегося к случаю чётного числа переменных.

Ключевые слова: сумма квадратов, линейная форма, диофантова система, конгруэнциальное условие, число решений квадратного сравнения, асимптотическая формула, особый ряд диофантовой системы.

Библиография: 23 названия.

Для цитирования:
Пачев, У. М., Кодзоков, А. Х., Исакова, М. М., Нирова, М. С. Об асимптотиках представлений пары целых чисел суммой квадратов и линейной формой с конгруэнтным условием специального вида // Чебышевский сборник, 2025, т. 26, вып. 1, с. 62–75.

CHEBYSHEVSKII SBORNIK
Vol. 26. No. 1.

UDC 511 DOI 10.22405/2226-8383-2025-26-1-62-75

On the asymptotics of representations by a sum of a pair of integers by a sum and a linear form with a congruential condition of a special form

U. M. Pachev, A. Kh. Kodzokov, M. M. Isakova, M. S. Nirova

Pachev Urusbi Mukhamedovich — doctor of physical and mathematical sciences, professor, Berbekov Kabardino-Balkarian State University (Nalchik).
e-mail: urusbi@rambler.ru
Azamat Khasanovich Kodzokov — Berbekov Kabardino-Balkarian State University (Nalchik).
e-mail: Kodzoko@mail.ru
Mariana Malilovna Isakova — candidate of physical and mathematical sciences, assistant professor, Berbekov Kabardino-Balkarian State University (Nalchik). *e-mail: isakova2206@mail.ru*
Marina Sefovna Nirova — candidate of physical and mathematical sciences, assistant professor, Berbekov Kabardino-Balkarian State University (Nalchik).
e-mail: nirova_m@mail.ru

Abstract

In the work, asymptotic formulas with a remainder term are obtained for the number of representations of a pair of integers m and n, respectively, as a sum of $s \geqslant 5$ variables, and each solution of such a Diophantine system satisfies the congruential a condition of a special type, associated in a certain way with a linear form.

Asymptotic formulas with a remainder term for the number of solutions of such a Diophantine system are derived for $N \to \infty$, where $N = \Delta m - n^2$ and Δ equals the sum of the squares on the coefficients on the linear form.

In addition, two-sided lower and upper bounds are obtained for a special series of Diophantine system under study based on the upper bound based on formulas for the number of solutions of a congruence of the second degree modulo the power $x_1^2 + \ldots + x_s^2 \equiv a \pmod{p^k}$ of the prime number, where a is natural number.

This work is a continuation of a previous study, relating to the case of an even number of variables.

Keywords: sum of squares, linear form, Diophantine system, congruential condition, number of solutions to quadratic congruence, estimates of a special series.

Bibliography: 23 titles.

For citation:
Pachev, U. M., Kodzokov, A. Kh., Isakova, M. M., Nirova, M. S. 2025, “On the asymptotics of representations by a sum of a pair of integers by a sum and a linear form with a congruential condition of a special form”, *Chebyshevskii sbornik*, vol. 26, no. 1, pp. 62–75.

1. Введение

Мы рассматриваем вопрос об асимптотике числа решений $r_{g;l_1,\ldots,l_s}(m,n)$ диофантовой системы

$$\begin{cases} x_1^2 + \ldots + x_s^2 = m, \\ l_1x_1 + \ldots + l_sx_s = n, \\ (x_1, \ldots, x_s) \equiv (l_1, \ldots, l_s) \pmod{g}, \end{cases} \tag{1}$$

где $s \geqslant 5$; $m > 0$, n — целые числа; $l_1x_1 + \ldots + l_sx_s$ — целочисленная линейная форма; g — натуральное число.

Особенностью системы (1) является то, что значения неизвестных сравнимы по данному модулю g с коэффициентами линейной формы. Выбор такой диофантовой системы представляет интерес тем, что для неё удаётся более точно исследовать её особый ряд.

Говоря об истоках направления, связанного с вопросом о числе решений систем диофантовых уравнений, следует отметить, что первое исследование по асимптотическому подсчёту числа решений систем из двух диофантовых уравнений “варингтовского типа” (по имени английского математика 18$^{\text{го}}$ века Варинга) было проведено в 1929 г. И. М. Виноградовым (см. [1, 2]) для системы вида

$$\begin{gathered} x_1^m + \ldots + x_r^m = M, \\ x_1^n + \ldots + x_r^n = N \end{gathered}$$

в целых положительных числах $x_1, \ldots, x_r$. Пользуясь методом И. М. Виноградова исследование было продолжено его учеником К. К. Марджанишвили [3] в случае систем с несколькими уравнениями варингтовского типа, при этом в неё уже входило также одно линейное уравнение.

В дальнейшем проводились также исследования по точным (не асимптотическим) формулам для числа решений $r_s(m,n)$ диофантовой системы

$$\begin{cases} x_1^2 + \ldots + x_s^2 = m, \\ x_1 + \ldots + x_s = n \end{cases} \tag{2}$$

в случаях $3 \leqslant s \leqslant 8$ такими авторами как Г. Полл [4, 5], Н. Клоостерман [6], Н. де-Брейн [7], P. Bronkhorst [8], ван-дер Блей [9], Г. А. Ломадзе [10].

Но как оказалось (см. Воронецкий А. Б. и Малышев А. В. [11]) при $s \geqslant 9$ невозможно получить точные формулы для числа решений $r_s(m,n)$ в том смысле, что величина $r_s(m,n)$ может отличной от особого ряда для указанной диофантовой системы (2) (относительно особого ряда, входящего в формулу для числа решений диофантовых уравнений см. напр. [12, 13]).

Ввиду этого представляет дальнейший интерес вопрос о получении асимптотических формул для числа решений $r_s(m,n)$ при $s \geqslant 9$ для диофантовых систем (1) и (2).

Асимптотическая формула для $r_s(m,n)$ при $sn - m^2 \to \infty$ была получена А. З. Вальфиш [14].

В дальнейшем эти исследования были продолжены А. А. Вальфиш [15] для диофантовых систем более общего вида, в которых сумма квадратов из [14] была заменена произвольной целочисленной положительной квадратичной формой.

В последнее время У. М. Пачевым и Л. А. Халиловой [16] получено обобщение результатов статьи [15], рассмотрев диофантову систему

$$\begin{cases} f(x_1, \ldots, x_s) = m, \\ l(x_1, \ldots, x_s) = n, \\ (x_1, \ldots, x_s) \equiv (l_1, \ldots, l_s) \pmod g \end{cases}$$

с конгруэнциальным условием, где f — целочисленная положительная квадратичная форма, $l(x_1, \ldots, x_s)$ — целочисленная линейная форма (при $g = 1$ как частный случай получаются основные результаты [15]). В следующей работе [17] проводилось исследование числа решений системы (1), связанное с верхней оценкой её особого ряда в случае чётного числа неизвестных.

Опираясь на теорему 2 работы [16] и на соответствующие вспомогательные результаты для числа решений квадратных сравнений по модулю степени простого числа из [17, 18] (леммы 1–5), получаем асимптотику числа решений системы (1) вместе с оценками её особого ряда.

2. Сведение исходной системы к системе без конгруэнтного условия

Исходная диофантова система (1) может быть сведена к тому её частному случаю, когда нет конгруэнтного условия

$$(x_1, \ldots, x_s) \equiv (l_1, \ldots, l_s) \pmod g.$$

Лемма 1. *Если*

$$m - 2n + \sum_{i=1}^{s} l_i^2 \equiv 0 \pmod{g^2} \quad \text{и} \quad n - \sum_{i=1}^{s} l_i^2 \equiv 0 \pmod g,$$

то система (1) *сводится к системе*

$$\begin{cases} y_1^2 + \ldots + y_s^2 = a, \\ l_1 y_1 + \ldots + l_s y_s = b, \end{cases}$$

где

$$a = \frac{m - 2n + \sum\limits_{i=1}^{s} l_i^2}{g^2}, \quad b = \frac{n - \sum\limits_{i=1}^{s} l_i^2}{g}.$$

Доказательство. Из сравнения $(x_1, \ldots, x_s) \equiv (l_1, \ldots, l_s) \pmod g$ имеем $x_i \equiv l_i \pmod g$, $i = 1, \ldots, s$, откуда $x_i = l_i + g y_i$ $(i = 1, \ldots, s)$, где $y_1, \ldots, y_s$ принимают целые значения. Подставляя выражения для x_i в оба уравнения системы (1), будем иметь систему

$$\begin{cases} g^2 \sum\limits_{i=1}^{s} y_i^2 + 2g \sum\limits_{i=1}^{s} l_i y_i + \sum\limits_{i=1}^{s} l_i^2 = m, \\ g \sum\limits_{i=1}^{s} l_i y_i + \sum\limits_{i=1}^{s} l_i^2 = n. \end{cases}$$

Преобразуя теперь первое уравнение этой системы с помощью второго уравнения получаем диофантову систему

$$\begin{cases} y_1^2 + \ldots + y_s^2 = a, \\ l_1 y_1 + \ldots + l_s y_s = b, \end{cases} \tag{3}$$

где

$$a = \frac{m - 2n + \sum\limits_{i=1}^{s} l_i^2}{g^2}, \quad b = \frac{n - \sum\limits_{i=1}^{s} l_i^2}{g},$$

ч. т. д. □

Замечание. *Ясно, что системы* (1) *и* (3) *равносильны в том смысле, что между их решениями существует взаимно однозначное соответствие. При этом a и b должны быть целыми числами. Если же хотя бы одно из чисел a и b не является целым, система* (1) *не имеет решений в целых числах. Согласно [14, 15], асимптотику числа решений полученной системы* (3) *мы будем рассматривать при $N = \Delta a - b^2 \to \infty$, где $\Delta = l_1^2 + \ldots + l_s^2$.*

3. Леммы о числе решений сравнений для суммы квадратов

Для формулировок дальнейших используемых вспомогательных утверждений нужны следующие понятия (см. [18]).

Определение 1. *Пусть F_q — произвольное конечное поле. Определим целочисленную функцию $v(x)$ на поле F_q с условием*

$$v(c) = \begin{cases} -1, & \text{если } c \in F_q^*, \\ q-1, & \text{если } c = 0, \end{cases}$$

где F_q^* — мультипликативная группа поля F_q.

Определение 2. *Пусть F_q — конечное поле нечётной характеристики и пусть на его мультипликативной группе F_q^* задана вещественнозначная функция η такая, что $\eta(c) = 1$ для элементов c, таких что являющихся квадратами некоторых элементов группы F_q^* и $\eta(c) = -1$ для всех остальных элементов $c \in F_q^*$. Такая функция $\eta(c)$ называется квадратичным характером поля F_q.*

Замечание. *В случае $q = p$, где p — простое число, квадратичный характер поля F_q есть символ Лежандра, т. е.*

$$\left(\frac{c}{p}\right) = \begin{cases} 1, & \text{если } c \text{ — квадратичный вычет } \mathrm{mod} p, \\ -1, & \text{если } c \text{ — квадратичный невычет } \mathrm{mod} p. \end{cases}$$

Ввиду мультипликативности квадратичного характера $\eta(c)$ поля F_q полезно доопределить его на всём поле, полагая $\eta(0) = 0$.

Лемма 2. *Пусть f — невырожденная квадратичная форма от чётного числа s переменных над полем F_q, где q — нечётно. Тогда для любого $b \in F_q$ число решений уравнения $f(x_1, \ldots, x_s) = b$ в F_q равно*

$$q^{s-1} + v(b)q^{\frac{s-2}{2}}\eta((-1)^{\frac{s}{2}} \det f),$$

где η — квадратичный характер поля F_q.

Доказательство даётся в [18].

Переходим теперь к рассмотрению вспомогательных результатов о числе решений сравнений для суммы квадратов от s неизвестных по модулю p^k, где p — простое число, используемых при верхней оценке особых рядов диофантовой системы из леммы 1.

Лемма 3. *Пусть $N_s(a\mathrm{mod}p)$ — число решений сравнения $x_1^2 + \ldots + x_s^2 \equiv a \pmod p$ от чётного числа s неизвестных, где p — простое число; a — целое число. Тогда*

1. $N_s\,(u\mathrm{mod}p) = p^{s-1}\left(1 - h^{\frac{s}{2}}\right)$, *где* $p \nmid u$;

2. $N_s\,(0) = N_s\,(u) + p^s h^{\frac{s}{2}}$,

где $h = \left(\frac{-1}{p}\right) \cdot p^{-1}$.

Доказательство. Воспользуемся леммой 2, положив в ней $f = x_1^2 + \ldots + x_s^2$; $q = p$ и $b = u$, где $p \nmid u$. Тогда по лемме 2 имеем

$$N_s(u \pmod p) = p^{s-1} + v(u)p^{\frac{s-2}{2}}\eta((-1)^{\frac{s}{2}} \det f).$$

Так как $v(u) = -1$ и $\det f = 1$ и η — символ Лежандра, то

$$\begin{aligned} N_s(u\mathrm{mod}p) &= p^{s-1} - p^{\frac{s}{2}-1}\eta((-1)^{\frac{s}{2}}) = \\ &= p^{s-1} - p^{\frac{s}{2}-1}\left(\frac{(-1)^{\frac{s}{2}}}{p}\right) = p^{s-1} - p^{\frac{s}{2}-1}h^{\frac{s}{2}} = \\ &= p^{s-1}\left(1 - h^{\frac{s}{2}}\right). \end{aligned}$$

2) Случай $N_s(0 \bmod p)$. По лемме 2 при $b=0$ имеем

$$\begin{aligned}
N_s(0 \bmod p) &= p^{s-1} + v(0)p^{\frac{s}{2}-1}\eta((-1)^{\frac{s}{2}}) = \\
&= p^{s-1} + (p-1)p^{\frac{s}{2}-1}\left(\frac{-1}{p}\right)^{\frac{s}{2}} = \\
&= p^{s-1} + (p-1)p^{\frac{s}{2}-1}p^{\frac{s}{2}}\left(\frac{-1}{p}\right)^{\frac{s}{2}}\frac{1}{p^{\frac{s}{2}}} = \\
&= p^{s-1} + (p-1)p^{s-1}h^{\frac{s}{2}} = \\
&= p^{s-1}\left(1-h^{\frac{s}{2}}\right) + p^s h^{\frac{s}{2}} = \\
&= N_s(u \bmod p) + p^s h^{\frac{s}{2}}
\end{aligned}$$

(см. п. 1), ч. т. д. $\square$

Следующий вспомогательный результат о числе решений квадратного сравнения по модулю p^k, где p — простое число приводится в [19], где его доказательство строится по схеме разбора трёх случаев, но мы дадим более подробное изложение.

Лемма 4. *Если $0 \leqslant v < k$, то число $N_s(p^v u \bmod p^k)$ решений сравнения*

$$x_1^2 + \ldots + x_s^2 \equiv p^v u \pmod{p^k} \qquad (*)$$

при чётном s равно

$$p^{(s-1)k}\left(1-h^{\frac{s}{2}}\right)\left(1+ph^{\frac{s}{2}}+p^2h^{2\frac{s}{2}}+\ldots+p^v h^{v\frac{s}{2}}\right),$$

где $h=(-1)^{\frac{p-1}{2}}\cdot p^{-1}$.

Доказательство. Случай 1. Если $v=0$, то число решений $N_s(u \bmod p^k)$ сравнения $(*)$ равно

$$p^{(s-1)(k-1)}N_s(u),$$

где $N_s(u)$ есть число решений сравнения $x_1^2+\ldots+x_s^2 \equiv u \pmod{p^k}$, где $p \nmid u$.

Действительно, пусть $(\xi_1,\ldots,\xi_s) \pmod p$ есть любое решение сравнения $\xi_1^2+\ldots+\xi_s^2 \equiv u \pmod p$, где $p \nmid u$. Такое решение поднимается в точности до $p^{(s-1)(k-1)}$ решений по модулю p^k. Имеем следующее представление решений сравнения $(*)$:

$$\begin{aligned}
&\xi_1 = h_0^{(1)} + h_1^{(1)}p + h_2^{(1)}p^2 + \ldots + h_{k-1}^{(1)}p^{k-1},\\
&\xi_2 = h_0^{(2)} + h_1^{(2)}p + h_2^{(2)}p^2 + \ldots + h_{k-1}^{(2)}p^{k-1},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&\xi_s = h_0^{(s)} + h_1^{(s)}p + h_2^{(s)}p^2 + \ldots + h_{k-1}^{(s)}p^{k-1},
\end{aligned}$$

где $0 \leqslant h_i^{(j)} < p$; $0 \leqslant i \leqslant k-1$; $1 \leqslant j \leqslant s$, которые позволяют осуществить поднятие решений сравнения $x_1^2+\ldots+x_s^2 \equiv u \pmod p$ до решения такого сравнения по модулю p^k. Но тогда по комбинаторному правилу произведения получаем, что число решений сравнения $x_1^2+\ldots+x_s^2 \equiv u \pmod{p^k}$ равно $N_s\left(u \bmod p^k\right) = p^{(s-1)(k-1)}N_s(u)$, при этом учитывается, что значение неизвестного x_s определено однозначно по соответствующим значениям остальных неизвестных.

Случай 2. Пусть теперь $v>1$. Тогда сравнение $\xi_1^2+\ldots+\xi_s^2 \equiv p^v u \equiv 0 \pmod p$ как и в случае 1 может иметь решения, для которых не все ξ_i делятся на p. Общее число таких решений равно $N_s(0)-1$, при этом нулевое решение рассматриваемого сравнения не засчитывается поскольку все значения неизвестных нулевого решения делятся на p, чем и обусловлено вычитание из $N_s(0)$ числа 1. Тогда согласно рассуждениям случая 1 число решений сравнения $(*)$, в которых не все неизвестные x_i делятся на p, по комбинаторному правилу произведения будет равно

$$p^{(s-1)(k-1)}(N_s(0)-1).$$

Случай 3. Если $v \geqslant 2$, то сравнение $(*)$ может иметь решения, для которых все x_i делятся на p, т. е. $x_i = py_i$, и значит, сравнение $(*)$ принимает вид

$$p^2\left(y_1^2+\ldots+y_s^2\right) \equiv p^v u \pmod{p^k},$$

откуда

$$y_1^2+\ldots+y_s^2 \equiv p^{v-2} u \pmod{p^{k-2}}.$$

Учитывая теперь, что лемма 3 даёт базу индукции при $v=0$, а рассмотренные выше случаи позволяют осуществить шаг индукции, то индукцией по v получаем сформулированный результат, ч. т. д. $\square$

В последнее время было продолжено исследование по асимптотике числа решений диофантовой системы (1) в оставшемся случае нечётного числа неизвестных. С этой целью получен следующий вспомогательный результат о числе решений квадратного сравнения

$$x_1^2+\ldots+x_s^2 \equiv p^v u \pmod{p^k},$$

где s — нечётное число; p — простое число; $p \nmid u$.

Лемма 5. *Если $0 \leqslant v < k$, то для числа решений $N_s\left(p^v u \pmod{p^k}\right)$ решений сравнения $x_1^2+\ldots+x_s^2 \equiv p^v u \pmod{p^k}$ при нечётном s и $p \nmid u$ справедлива оценка сверху*

$$N_s\left(p^v u \pmod{p^k}\right) \leqslant$$
$$\leqslant p^{(s-1)k}\left(1-h^{\frac{s-1}{2}}\right)\left(1+ph^{\frac{s-1}{2}}+p^2h^{2\frac{s-1}{2}}+\ldots+p^{v'}h^{v'\frac{s-1}{2}}\right),$$

где $0 \leqslant v' < k$, $p \nmid u$; $p^v u - x_s^2 = p^{v'}u'$; $v' = \max\limits_{0\leqslant x_s<p^k} \operatorname{ord}_p(p^v u - x_s^2)$; ord_p — порядок целого числа относительно простого числа p, $h = (-1)^{\frac{p-1}{2}}p^{-1}$.

Доказательство. Представим рассматриваемое сравнение в следующем виде

$$x_1^2+\ldots+x_{s-1}^2 \equiv p^v u - x_s^2 \pmod{p^k}.$$

Обозначим $p^v u - x_s^2 = p^{v'}u'$, где $0 \leqslant v' < k$ и $p \nmid u'$,

$$v' = \max_{0\leqslant x_s<p^k} \operatorname{ord}_p\left(p^v u - x_s^2\right),$$

где $\operatorname{ord}_p \alpha$ — порядок целого числа α относительно простого числа p. Тогда имеем

$$N_s\left(p^v u \pmod{p^k}\right) \leqslant \sum_{0\leqslant x_s<p^k} N_{s-1}\left((p^v u - x_s^2) \pmod{p^k}\right) \leqslant$$
$$\leqslant \sum_{0\leqslant x_s<p^k} N_{s-1}\left(p^{v'}u' \pmod{p^k}\right) \leqslant \sum_{0\leqslant x_s<p^k-1} N_{s-1}\left(p^{v'}u' \pmod{p^k}\right) =$$
$$= p^k N_{s-1}\left(p^{v'}u' \pmod{p^k}\right).$$

Применяя теперь ввиду чётности числа $s-1$ лемму 4, получим

$$N_s(p^{v'}u' \pmod{p^k}) \leqslant$$
$$\leqslant p^k\cdot p^{(s-2)k}\left(1-h^{\frac{s-1}{2}}\right)\left(1+ph^{\frac{s-1}{2}}+p^2h^{2\frac{s-1}{2}}+\ldots+p^{v'}h^{v'\frac{s-1}{2}}\right)=$$
$$=p^{(s-1)k}\left(1-h^{\frac{s-1}{2}}\right)\left(1+ph^{\frac{s-1}{2}}+p^2h^{2\frac{s-1}{2}}+\ldots+p^{v'}h^{v'\frac{s-1}{2}}\right),$$

ч. т. д. □

Замечание. *Как отмечается в [19] в случае сравнения* $x_1^2+\ldots+x_n^2\equiv a \pmod p$ *по нечётному простому модулю* p *число его решений вычислялось в работе Зигеля [20, с. 344] с помощью остроумного соображения о гауссовых суммах.*

4. Результаты об асимптотике числа решений диофантовой системы специального вида

В асимптотических формулах в главном члене для числа решений диофантовых систем уравнений второй степени с несколькими неизвестными при применении кругового метода появляется важная арифметическая функция, называемая особым рядом.

Для диофантовой системы (1) обозначим такой ряд через

$$H_{g;l_1,\ldots,l_s}(f,m;l,n),$$

где f — квадратичная форма, l — линейная форма. В силу леммы 1 такой ряд может быть записан ещё в следующем виде $H_{g;l_1,\ldots,l_s}(a,b)$, где a и b зависят от m и n, при этом $f=x_1^2+\ldots+x_s^2$. Нужный нам особый ряд определяется равенством

$$H_{g;l_1,\ldots,l_s}(a,b)=\prod_p \chi_p(a,b),$$

где

$$a=\frac{m-2n+\sum_{i=1}^s l_i}{g^2},\quad b=\frac{n-\sum_{i=1}^s l_i^2}{g};\quad \chi_p(a,b)=\lim_{t\to\infty}p^{-(s-2)t}\rho(p^t;a,b);$$

$\rho(p^t;a,b)$ — число решений системы сравнений

$$\begin{cases} x_1^2+\ldots+x_s^2\equiv a \pmod{p^t},\\ l_1x_1+\ldots+l_sx_s\equiv b \pmod{p^t},\end{cases}\tag{4}$$

произведение берётся по всем простым числам p.

Лемма 6. *Пусть* $r_{g;l_1,\ldots,l_s}(f,m;l,n)$ *— число целочисленных решений диофантовой системы*

$$\begin{cases} f(x_1,\ldots,x_s)=m,\\ l(x_1,\ldots,x_s)=n,\\ (x_1,\ldots,x_s)\equiv(l_1,\ldots,l_s) \pmod g,\end{cases}$$

где f *— положительная целочисленная квадратичная форма.*

Тогда при $N\to\infty$

$$r_{g;l_1,\ldots,l_s}(f,m;l,n)=\frac{\pi^{\frac{s-1}{2}}N^{s-3}}{(g^{s-1}\Delta)^{\frac{s}{2}-1}\Gamma\left(\frac{s-1}{2}\right)}\cdot H_{g;l_1,\ldots,l_s}(F,m_1;l,n_1)+O\left(\Delta^{2s-\frac{5}{4}+\frac{\varepsilon}{2}}N^{\frac{s-2}{4}+\varepsilon}\right),$$

где $N=\frac{m_1\Delta-gn_1^2D}{g}$; $F=gf(x_1,\ldots,x_s)+l(x_1,\ldots,x_s)$; $m_1=\frac{m-f(b_1,\ldots,b_s)}{g^2}$; $n_1=\frac{n-l(b_1,\ldots,b_s)}{g}$; $\Delta=\overline{f}(l_1,\ldots,l_s)$, $\overline{f}$ *— алгебраически взаимная форме* f; Γ *— гамма-функция;* $\varepsilon>0$ *— сколь*

угодно малое число;
$H_{g;l_1,\ldots,l_s}(F, m_1; l, n_1)$ — *особый ряд заданной диофантовой системы.*

Доказательство этого результата см. в [16].

Опираясь на вышеизложенные вспомогательные факты получаем следующие результаты о числе решений диофантовой системы (1).

Теорема 1. *Для числа решений $r_{g;l_1,\ldots,l_s}(m,n)$ диофантовой системы*

$$\begin{cases} x_1^2 + \ldots + x_s^2 = m, \\ l_1x_1 + \ldots + l_sx_s = n, \\ (x_1, \ldots, x_s) \equiv (l_1, \ldots, l_s) \pmod{g}, \end{cases}$$

при $N \to \infty$ справедлива формула

$$r_{g;l_1,\ldots,l_s}(m,n) = \frac{\pi^{\frac{s-1}{2}} N^{\frac{s-3}{2}}}{(g^{s-1}\Delta)^{\frac{s}{2}-1}\Gamma\left(\frac{s-1}{2}\right)} \cdot H_{g;l_1,\ldots,l_s}(a,b) + O\left(g^{s-1}N^{\frac{s-2}{4}+\varepsilon}\right),$$

где $N = \Delta a - b^2 \to \infty$; $\Delta = l_1^2 + \ldots + l_s^2$.

$$H_{g;l_1,\ldots,l_s}(a,b) = \prod_p \lim_{t\to\infty} \frac{\rho(p^t; a, b)}{p^{(s-2)t}},$$

где $\rho(p^t; a, b)$ — число решений системы сравнений

$$\begin{cases} x_1^2 + \ldots + x_s^2 \equiv a \pmod{p^t}, \\ l_1x_1 + \ldots + l_sx_s \equiv b \pmod{p^t}, \end{cases}$$

произведение берётся по всем простым числам p; $a = \frac{m-2n+\sum_{i=1}^s l_i^2}{g^2}$; $b = \frac{n-\sum_{i=1}^s l_i^2}{g}$.

Доказательство основано на леммах 1 и 6.

Отметим, что этот результат содержится в [17], но здесь он представлен в улучшенной формулировке.

С целью получения более точной информации о числе решений диофантовой системы (1) будем рассматривать двусторонние оценки снизу и сверху особого ряда, входящего в главный член асимптотической формулы для этой системы.

Сначала рассмотрим оценку снизу для особого ряда. Для этого воспользуемся теоремой Е. В. Подсыпанина [21] о сингулярном (особом) ряде в задаче представления системы целых чисел суммой форм одной и той же степени $d \geqslant 1$ от s переменных.

Поскольку результат работы [21] об особом ряде относится только к однородным уравнениям с одной и той же степенью d, то он не может быть непосредственно применён к нашему случаю диофантовой системы, состоящей из двух уравнений второй и первой степени.

В связи с этим наряду с системой сравнений (4) рассмотрим также систему сравнений вида

$$\begin{cases} y_1^2 + \ldots + y_s^2 \equiv a \pmod{p^t}, \\ (l_1y_1 + \ldots + l_sy_s)^2 \equiv b^2 \pmod{p^t}. \end{cases} \tag{5}$$

При этом заметим, что число решений $\rho(p^t; a, b^2)$ системы (5) в 2 раза больше числа решений системы сравнений (4), т. е.

$$\rho(p^t; a, b^2) = 2\rho(p^t; a, b),$$

откуда

$$\rho(p^t; a, b) = \frac{1}{2}\rho(p^t; a, b^2). \tag{6}$$

В нашем случае в обозначениях работы [21] имеем

$$\tau = 2; \quad k = 1;\ 2.$$

$$\begin{cases} \phi^{(1)}(x_1, \ldots, x_s) = x_1^2 + \ldots + x_s^2 = n_1 = a, \\ \phi^{(2)}(x_1, \ldots, x_s) = (l_1x_1 + \ldots + l_sx_s)^2 = n_2 = b^2. \end{cases} \tag{7}$$

Сформулируем результат работы [21].

Теорема (Подсыпанин). *Пусть существует целое число $\delta \geqslant 0$ и индексы $j_1, \ldots, j_r$, для которых разрешима система сравнений*

$$\Phi^{(k)}(x_1, \ldots, x_s) \equiv n_k \pmod{p^{2\tau+2\delta+1}} \quad (k = 1, \ldots, r)$$

при условии

$$p^\delta \parallel \Delta_{j_1,\ldots,j_r}(x_1, \ldots, x_s)\,.$$

Тогда

$$H_p(n_1, \ldots, n_r) \geqslant p^{-(2\tau+2\delta+1)(s-r)}.$$

В этой теореме используются следующие обозначения:

$$\Phi_j^{(k)}(\overline{x}) = \sum_{j_2,\ldots,j_d=1}^{s} \varphi_{j,j_2,\ldots,j_d}^{(k)} x_{j_2} \cdot \ldots \cdot x_{j_d} \quad (j = 1, \ldots, s),$$

$$\Delta_{j_1,\ldots,j_r}(\overline{x}) = \det\left(\Phi_{j_g}^{(k)}(\overline{x})\right)_{g,k=1}^{r},$$

$p^\tau \parallel d$ — наивысшая степень простого числа p, делящая число d.

Как обычно, особый ряд $H(n_1, \ldots, n_r)$ диофантовой системы представляется в виде бесконечного произведения по всем простым числам, т. е.

$$H(n_1, \ldots, n_r) = \prod_p H_p(n_1, \ldots, n_r)\,.$$

Тогда в силу теоремы Подсыпанина имеем неравенство

$$H_p(n_1, \ldots, n_r) \geqslant p^{-(2\tau+2\delta+1)(s-r)}.$$

В нашем случае двух уравнений имеем

$$H_p\left(a, b^2\right) \geqslant p^{-(2\tau+2\delta+1)(s-2)}.$$

Но учитывая конгруэнтное условие решений системы, следуя А. В. Малышеву [12], используем также и другое обозначение особого ряда через $H_{g;l_1,\ldots,l_s}(a, b)$ в случае нашей диофантовой задачи. Следуя опять работам [12, 21] в силу (6) и (7) получаем

$$H_{g;l_1,\ldots,l_s}(a,b) \geqslant \frac{1}{2} H_{g;l_1,\ldots,l_s}(a,b^2) \geqslant \frac{1}{2}\prod_p H_p(a,b^2) \geqslant \frac{1}{2}\prod_p p^{-(2\tau+2\delta+1)(s-2)} \gg 1.$$

При этом ещё учитывается одно замечание в [21], относящееся к работе Берча [22], о том, что существует p_0, для которого

$$\prod_{p \geqslant p_0} H_p(n_1, \ldots, n_r) \gg 1.$$

Таким образом, имеет место следующий вспомогательный результат, относящийся к нижней оценке особого ряда диофантовой системы (1).

Лемма 7. *Для особого ряда $H_{g;l_1,\ldots,l_s}(m,n)$ диофантовой системы* (1) *имеет место оценка снизу $H_{g;l_1,\ldots,l_s}(m,n) \gg 1$, т. е. $H_{g;l_1,\ldots,l_s}(m,n) > 0$.*

Более точную информацию о числе решений диофантовой системы (1) в случае чётного числа s переменных даёт следующая

Теорема 2. *Для числа решений диофантовой системы* (1) *при чётном s и $N \to \infty$ имеет место формула*

$$r_{g;l_1,\ldots,l_s}(m,n) = \frac{\pi^{\frac{s-1}{2}} N^{\frac{s-3}{2}}}{(g^{s-1}\Delta)^{\frac{s}{2}-1}\Gamma\left(\frac{s-1}{2}\right)} \cdot H_{g;l_1,\ldots,l_s}(a,b) + O\left(g^{s-1}N^{\frac{s}{4}-\frac{1}{2}+\varepsilon}\right),$$

где

$$1 \leqslant H_{g;l_1,\ldots,l_s}(a,b) < \prod_p \left(1 - h^{\frac{s}{2}}\right)\left(1 + ph^{\frac{s}{2}} + p^2h^s + \ldots + p^v h^{v\frac{h}{2}}\right),$$

где $a = p^v$, $p \nmid u$; $h = (-1)^{\frac{p-1}{2}} \cdot \frac{1}{p}$; $a = \frac{m-2n+\sum_{i=1}^{s} l_i^2}{g^2}$; $b = \frac{n-\sum_{i=1}^{s} l_i^2}{g}$.

Доказательство основано на результатах лемм 1, 4, 6 и теоремы 1.

Аналогичный результат о числе решений диофантовой системы (1) в случае нечётного числа s переменных даёт следующая

Теорема 3. *Для числа решений диофантовой системы* (1) *при нечётном s и $N \to \infty$ имеет место формула*

$$r_{g;l_1,\ldots,l_s}(m,n) = \frac{\pi^{\frac{s-1}{2}} N^{\frac{s-3}{2}}}{(g^{s-1}\Delta)^{\frac{s}{2}-1}\Gamma\left(\frac{s-1}{2}\right)} \cdot H_{g;l_1,\ldots,l_s}(a,b) + O\left(g^{s-1}N^{\frac{s}{4}-\frac{1}{2}+\varepsilon}\right),$$

$$1 \ll H_{g;l_1,\ldots,l_s}(a,b) < \left(1 - h^{\frac{s-1}{2}}\right)\left(1 + ph^{\frac{s-1}{2}} + p^2h^{2\frac{s-1}{2}} + \ldots + p^{v'}h^{v'\frac{s-1}{2}}\right),$$

где $0 \leqslant v' < k$, $p \nmid u$, $p^v u - x_s^2 = p^{v'}u'$; $v' = \max_{0 \leqslant x_s < p^k} \operatorname{ord}_p\left(p^v - x_s^2\right)$; ord_p — порядок целого числа относительно простого числа p; $h = (-1)^{\frac{p-1}{2}} \cdot \frac{1}{p}$.

Доказательство опирается на результаты лемм 1, 5, 6 и теоремы 1.

5. Заключение

Полученные результаты можно обобщить на диофантовы системы, содержащие более одного линейного уравнения. Представляет также интерес перенесение проведенного исследования на случай суммы квадратов с линейной частью (при этом предполагается возможность использования результатов работ [15, 16, 23]). Интересно также исследовать особые ряды для диофантовых систем с диагональной квадратичной формой и линейной формой, удовлетворяющих конгруэнциальному условию.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Виноградов И. М. Об одном классе совокупных диофантовых уравнений // Изв. АН СССР, 1929. С. 355-376.

2. Виноградов И. М. Избранные труды. Изд-во АН СССР. — М., 1952. С. 151-168.

3. Марджанишвили К. К. Об одновременном представлении n чисел суммами полных первых, вторых, ..., n-х степеней // Изв. АН СССР, сер. матем. 1 (1937), С. 609-631.

4. Pall G. Simultaneous quadratic and linear representations. Quart. J. Math. 2 (1931). P. 136-143.

5. Pall G. Simultaneous representations in a quadratic and linear form // Duke Math. J. S. (1941). P. 173-180.

6. Kloosterman H. Simultane Darstellung zweier ganzen Zahlen al seiner Samme von ganzen Zahlen und deren Quadrat–Summe. Math. Ann. 118 (1942). S. 319-364.

7. de Bruijn N. G. Over het a antal oplossingen van het stelsel $x_1^2+x_2^2+x_3^2=n$, $x_1+x_2+x_3=m$, Nieuw. Arch. Wisk (2)22 (1943), S. 53-56.

8. Bronkhorst P. Over het a antal oplossingen van het stelsel Diophatische Vergelijkinder $x_1^2+\ldots+x_s^2=n$, $x_1+\ldots+x_s=m$ vor $s=6$ en $s=8$. Diss. Groningen, 1943.

9. Van der Blij. On the theory of simultaneous linear and quadratic representation I–II, Proc. Kon. Acad. V. Wet. 50 (1947), 31-48.

10. Ломадзе Г. А. Об одновременном представлении двух целых чисел суммами целых чисел и их квадратов // Труды Тбилисского матем. ин-та. 18 (1950). С. 153-181,

11. Воронецкий А. Б., Малышев А. В. Об одновременном представлении пары чисел суммами целых чисел и их квадратов // Тр. МИАН СССР, 142 (1976). С. 122-134,

12. Малышев А. В. О представлении целых чисел положительными квадратичными формами // Труды МИАН СССР, Т. 65 (1962), С. 3-212.

13. Малышев А. В. О формулах для количества представлений чисел положительными квадратичными формами // Актуальные проблемы аналитической теории чисел. Минск : Наука и техника, 1974.

14. Вальфиш А. З. О представлении чисел суммами квадратов. Асимптотические Формулы // Успехи матем. наук. 7 (1952), № 6, С. 97-178,

15. Walfisz A. A. Über die simultane Darstellung zweier ganzen Zahlen durch quadratische und lineare Formen // Acta Arithmetica XXXV (1979). S. 289-301.

16. Пачев У. М., Халилова Л. А. Об асимптотике числа представлений пары целых чисел квадратичной и линейной формами с конгруэнциальным условием // Матем. заметки. Т. 111, вып. 5 (2022). С. 726-737.

17. Urusbi Pachev, Rezuan Dokhov, Asamat Kodzokov. On Diophantine Systems with Sum of Squares and Linear Forms Satisfying a Congruential Condition of a Special Form // Current Problems of Applied Mathematics and Computer Systems, 2024, pp. 3-10.

18. Лидл Р., Нидеррайтер Г. Конечные поля. Т. 1. — М. : "Мир". (1988).

19. Милнор Дж., Хьюзмоллер Д. Симметрические билинейные формы. — М. : "Наука". (1986).

20. Siegel C. L. Gesammelte Abhandlungen, I. — Berlin; Heidelberg; Springer–Verlag, 1966, S. 326-405.

21. Подсыпанин Е. В. О сингулярном ряде в задаче представления системы чисел системой форм // Зап. научн. сем. ЛОМИ Т. 50 (1975), С. 130-136.

22. Birch B. J. Forms in many variables. Proc. Roy. Soc., 1962, A. 265, pp. 245-263,

23. Watson G. L. Quadratische Diophantine equations. Phil. Trans. Roy. Soc London A 253, pp. 227-254.

REFERENCES

1. Vinogradov, I. M. 1929. “On one class of aggregate Diophantine equations”, *Izv. Academy of Sciences of the USSR*, pp. 355–376.

2. Vinogradov, I. M. 1952, “Selected works”, *Publishing house of the USSR Academy of Sciences*, pp. 151–168.

3. Marjanishvilli, K. K. 1937, “On the simultaneous representation of complete first second, $\dots$, n-th degrees”, *Izv. AN SSSR, ser. Mat.*, 4, pp. 609–634.

4. Pall, G. 1931, “Simultaneous quadratic and linear representations”, *Quart. J. Math.*, 2, pp. 136–143.

5. Pall, G. 1941, “Simultaneous representations in a quadratic and linear form”, *Duke Math. J. S.*, pp. 173–180.

6. Kloosterman, H. 1942, “Simultane Darstellung zweier ganzen Zahlen al seiner Samme von ganzen Zahlen und deren Quadrat–Summe”, *Math. Ann.*, 118, pp. 319–364.

7. de Bruijn, N. G. 1943, “Over het a antal oplossingen van het stelsel $x_1^2 + x_2^2 + x_3^2 = n$, $x_1 + x_2 + x_3 = m$”, *Nieuw. Arch. Wisk*, (2)22, pp. 53–56.

8. Bronkhorst, P. 1943 “Over het a antal oplossingen van het stelsel Diophatische Vergelijkinder $x_1^2 + \ldots + x_s^2 = n$, $x_1 + \ldots + x_s = m$ vor $s = 6$ en $s = 8$”, *Diss. Groningen.*

9. Van der Blij. 1947, “On the theory of simultaneous linear and quadratic representation I–II”, *Proc. Kon. Acad. V. Wet.*, 50, pp. 31–48.

10. Lomadze, G.A, 1950, “On the simultaneous representation of two integers by sums of integers and their squares”, *Proceedings of the Tbilisi Mathematical Institute*, 18, pp. 153–181.

11. Voronetsky, A. B., Malyshev A. V. 1976, “On the simultaneous representation of a pair of numbers by sums of integers and their squares”, *Proceedings of the Steklov Mathematical Institute of the USSR*, 142, pp. 122–134.

12. Malyshev, A. V. 1962, “On the representation of integers by positive quadratic forms”, *Proceedings of the Steklov Mathematical Institute of the USSR*, V. 65, pp. 3–212.

13. Malyshev, A. V. 1974, “On formulas for the number of representations of numbers by positive quadratic forms”, *Actual problems of analytical number theory. Minsk. Science and Technology.*

14. Valfish, A. Z. 1952, “On the representation of squares. Asymptotic formulas”, *Uspekhi Matematicheskikh Nauk*, 7, № . 6, pp. 97–178.

15. Walfisz, A. A. 1979, “Über die simultane Darstellung zweier ganzen Zahlen durch quadratische und lineare Formen”, *Acta Arithmetica XXXV*, pp. 289–301.

16. Pachev, U. M., Khalilova L, A. 2022, “On the asymptotics on the number of representations of a pair of integers by quadratic and linear forms with a congruent condition”, *Mathematical notes*, Vol. 111, Iss. 5, pp. 726–737.

17. Urusbi Pachev, Rezuan Dokhov, Asamat Kodzokov. 2024, “On Diophantine Systems with Sum of Squares and Linear Forms Satisfying a Congruential Condition of a Special Form”, *Current Problems of Applied Mathematics and Computer Systems*, pp. 3–10.

18. Lidl, R., Niederreiter G. 1988, “Finite fields”, *M.:Mir*, Vol. 1.

19. Mulnor, J., Huesmoller D, 1986, “Symmetric bilinear forms”, *M.:Science*.

20. Siegel, C. L. 1966, “Gesammelte Abhandlungen, I”, *Berlin; Heidelberg; Springer–Verlag*, pp. 326–405.

21. Podsypanin, E. V. 1975, “On the singular series in the problem of representing a system of numbers by a system”, *Notes of scientific seminars LOMI*, V. 50, pp. 130–136.

22. Birch, B. J. 1962, “Forms in many variables”, *Proc. Roy. Soc. A.*, 265, pp. 245–263,

23. Watson, G. L. “Quadratische Diophantine equations”, *Phil. Trans. Roy. Soc. London A.*, 253, pp. 227–254.

Получено: 27.11.2024
Принято в печать: 10.03.2025