



H. Al-Assad, A generalisation of Legendre's three-square theorem, *Chebyshevskii Sb.*, 2024, Volume 25, Issue 1, 127–137

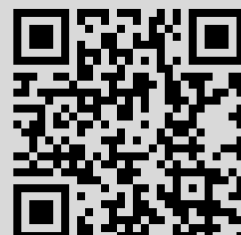
DOI: 10.22405/2226-8383-2024-25-1-127-137

Use of the all-Russian mathematical portal Math-Net.Ru implies that you have read and agreed to these terms of use
<http://www.mathnet.ru/eng/agreement>

Download details:

IP: 44.220.255.141

November 5, 2024, 03:17:28



ЧЕБЫШЕВСКИЙ СБОРНИК

Том 25. Выпуск 1.

УДК 511

DOI 10.22405/2226-8383-2024-25-1-127-137

Обобщение теоремы Лежандра о трёх квадратах

Х. Аль-Ассад

Хафез Аль-Ассад — Московский государственный университет им. М. В. Ломоносова (г. Москва).

e-mail: 1hbrh0@gmail.com

Аннотация

В данной работе представлено обобщение теоремы Лежандра о трех квадратах на представления двух натуральных чисел в виде сумм трех квадратов, для которых имеется общий квадрат.

Ключевые слова: Теорема Лежандра о трёх квадратах, принцип Хассе для систем двух квадратичных форм.

Библиография: 8 названий.

Для цитирования:

Х. Аль-Ассад. Обобщение теоремы Лежандра о трёх квадратах // Чебышевский сборник, 2024, т. 25, вып. 1, с. 127–137.

CHEBYSHEVSKII SBORNIK

Vol. 25. No. 1.

UDC 511

DOI 10.22405/2226-8383-2024-25-1-127-137

A generalisation of Legendre's three-square theorem

H. Al-Assad

Hafez Al-Assad — Lomonosov Moscow State University (Moscow).

e-mail: 1hbrh0@gmail.com

Abstract

In this paper a generalisation of Legendre's three-square theorem to representations of two positive integers as sums of three squares for which the first square of each representation is the same is presented.

Keywords: Legendre's three-square theorem, Hasse's Principle for systems of two quadratic forms.

Bibliography: 8 titles.

For citation:

H. Al-Assad, 2024, "A generalisation of Legendre's three-square theorem", *Chebyshevskii sbornik*, vol. 25, no. 1, pp. 127–137.

1. Введение и постановка задачи

Основной результат этой работы, теорема 2, приведенная ниже, был предложен с помощью компьютерных расчетов, выполненных Али Дибом (dib_a@spbstu.ru), Высшая школа управления кибер-физическими системами, Институт компьютерных наук и кибербезопасности, Санкт-Петербургский политехнический университет Петра Великого (СПбПУ).

Проблема представления целого положительного числа в виде суммы трёх целых квадратов решается следующей теоремой Лежандра ([2], ст. 47).

ТЕОРЕМА 1. (ЛЕЖАНДР) Пусть m — целое положительное число. Уравнение

$$m = x^2 + y^2 + z^2$$

имеет решение в $x, y, z \in \mathbb{Z}$ если и только если m удовлетворяет условию

$$m \neq 4^a(8b + 7); a, b \in \mathbb{Z}, a, b \geq 0.$$

Мы обобщим этот классический результат, рассматривая представления двух натуральных чисел в виде сумм трех квадратов, так что эти два представления имели общий квадрат.

Т.е. мы рассматриваем решения системы

$$\begin{aligned} m &= a^2 + b_1^2 + c_1^2, \\ m' &= a^2 + b_2^2 + c_2^2 \end{aligned} \quad (1)$$

в целых числах a, b_1, b_2, c_1, c_2 .

Для удобства будем называть целые числа, представимые в виде суммы трёх квадратов, Лежандровыми.

Кроме того, мы заключаем следующее полезное соглашение: мы говорим, что две пары целых чисел (m_1, m'_1) и (m_2, m'_2) сравнимы по модулю целого числа n , если либо

$$m_1 \equiv m_2 \pmod{n}, \quad m'_1 \equiv m'_2 \pmod{n},$$

или

$$m_1 \equiv m'_2 \pmod{n}, \quad m'_1 \equiv m_2 \pmod{n}.$$

Наш основной результат - следующая теорема.

ТЕОРЕМА 2. Пусть $m, m' \in \mathbb{Z}$ — пара Лежандровых положительных целых чисел. Система

$$\begin{aligned} q^2 m &= a^2 + b_1^2 + c_1^2, \\ q^2 m' &= a^2 + b_2^2 + c_2^2 \end{aligned} \quad (2)$$

имеет решение в положительных q, a, b_1, b_2, c_1, c_2 тогда и только тогда, когда пара (m, m') не сравнима с $(0, 3)$ или $(3, 4)$ по модулю 8 и не сравнима ни с одной из пар

$$\begin{aligned} &(0, 3 \cdot 2^{k-3}), \\ &(0, 3 \cdot 2^{k-2}), \\ &(0, 7 \cdot 2^{k-3}), \\ &(2^{k-3}, 3 \cdot 2^{k-2}), \\ &(5 \cdot 2^{k-3}, 3 \cdot 2^{k-2}) \end{aligned}$$

по модулю 2^k , для любого четного целого $k \geq 4$.

Более того, существует решение системы (2) такое, что q нечетно и взаимно просто с a .

План доказательства следующий.

Рассматриваем систему (1) в рациональных числах a, b_1, b_2, c_1, c_2 .

Сначала мы покажем, что для любой пары (m, m') , система (1) имеет нетривиальное решение в кольце $\mathbb{Z}/p\mathbb{Z}$ для любого простого числа p .

Потом мы покажем, что для любой пары (m, m') , система (1) имеет нетривиальное решение в кольце $\mathbb{Z}/p^k\mathbb{Z}$ для любого нечетного простого числа p и любого целого числа $k > 1$.

Затем мы покажем, что если $v_2(\gcd(m, m')) \leq 1$, то система (1) имеет нетривиальное решение в кольце $\mathbb{Z}/2^k\mathbb{Z}$ для любого целого числа $k > 1$ тогда и только тогда, тогда пара (m, m') удовлетворяет условиям теоремы 2.

Из этого получим условия нетривиальной разрешимости системы (1) в p -адических полях \mathbb{Q}_p при $v_2(\gcd(m, m')) \leq 1$, и, поскольку разрешимость в \mathbb{R} очевидна, мы используем форму локально-глобального принципа Хассе ([5], ст. 22, теорема 3.2) для перехода к решениям системы (1) в \mathbb{Q} , при $v_2(\gcd(m, m')) \leq 1$.

После этого, мы используем теорему Давенпорта-Касселса ([2], ст. 46) для перехода от решений системы (1) к решениям системы (2), при $v_2(\gcd(m, m')) \leq 1$.

Наконец, воспользуемся леммой для перехода от решений системы (2) в случай, когда $v_2(\gcd(m, m')) \leq 1$ к решениям системы (2) в общем случае.

2. Задача по модулю простого числа

Пусть p — некоторое простое число. Мы рассматриваем систему

$$\begin{aligned} t^2 + x^2 + y^2 &\equiv m \pmod{p}, \\ t^2 + z^2 + w^2 &\equiv m' \pmod{p}, \end{aligned} \quad (3)$$

в $t, x, y, z, w \in \mathbb{Z}/p\mathbb{Z}$.

Покажем, что (3) разрешимо для всех m, m' .

Разрешимость (3) в случае $p = 2$ тривиальна, а 0 нетривиально представляется как $0 \equiv 1+1 \pmod{2}$. Поэтому предположим, что $p > 2$.

ЛЕММА 1. Если $m \not\equiv 0 \pmod{p}$, то сравнение

$$x^2 + y^2 \equiv m \pmod{p} \quad (4)$$

разрешима.

ДОКАЗАТЕЛЬСТВО. Если m — квадратичный вычет по модулю p , то можно взять $y = 0$. Предположим, что m — квадратичный невычет.

Пусть $Q_1 = \{q_i\}_{i=1}^{\frac{p-1}{2}}$ — множество квадратичных вычетов по модулю p .

Покажем, что множество $Q_2 = \{q_i + 1\}_{i=1}^{\frac{p-1}{2}}$ содержит хотя бы один квадратичный невычет.

Действительно, если Q_2 не содержит квадратичных невычетов, то $Q_2 = Q_1$, и мы можем рассматривать элементы Q_2 как перестановку элементов Q_1 .

Рассмотрим цикл перестановки, содержащей элемент q_1

$$q_{i+1} \equiv q_i + 1, \quad 1 \leq i \leq k-1, \quad q_1 \equiv q_k + 1,$$

для некоторого $1 \leq k \leq \frac{p-1}{2}$.

Однако это дает, что

$$q_1 \equiv q_k + 1 \equiv q_{k-1} + 2 \equiv \dots \equiv q_1 + k \implies k \equiv 0 \pmod{p},$$

что является противоречием.

Следовательно, множество Q_2 содержит некоторый квадратичный невычет r , скажем с

$$r = q + 1 = \tilde{r}^2 + 1, \quad (5)$$

для некоторого \tilde{r} .

Пусть g — примитивный корень по модулю p . Поскольку m и r — квадратичные невычеты, мы можем написать

$$m \equiv g^{2a+1}, \quad r \equiv g^{2b+1}, \quad (6)$$

для некоторых $0 \leq a, b \leq \frac{p-3}{2}$.

Из (5) и (6) мы видим, что

$$m \equiv rg^{2(a-b)} \equiv \tilde{r}^2 g^{2(a-b)} + g^{2(a-b)} \equiv x^2 + y^2.$$

□

Теперь докажем основной результат данного раздела.

ТЕОРЕМА 3. Система (3) разрешима для всех m, m' .

ДОКАЗАТЕЛЬСТВО. Если $m, m' \not\equiv 0 \pmod{p}$, то берем $t = 0$, и теорема следует из леммы 1.

Если, скажем, $m' \equiv 0$, то берем $t \neq 0$ такой, что $t^2 \not\equiv m$, и теорема опять следует из леммы 1. □

3. Задача по модулю степени нечетного простого числа

Пусть p — нечетное простое число, а $k \geq 2$ — целое число. Мы рассматриваем систему

$$\begin{aligned} t^2 + x^2 + y^2 &\equiv m \pmod{p^k}, \\ t^2 + z^2 + w^2 &\equiv m' \pmod{p^k}, \end{aligned} \quad (7)$$

в $t, x, y, z, w \in \mathbb{Z}/p^k\mathbb{Z}$.

Покажем, что (7) разрешимо для всех m, m' .

ТЕОРЕМА 4. Система (7) разрешима для всех m, m' .

ДОКАЗАТЕЛЬСТВО. Будем действовать индукцией по k . Случай $k = 1$ доказанно в теореме 3.

Предположим сначала, что $m, m' \not\equiv 0 \pmod{p}$. Доказательство теоремы 3 показало, что в этом случае при $k = 1$ система (7) разрешима при $t = 0$.

По индукции мы предполагаем, что это верно по модулю p^{k-1} , так что

$$x^2 + y^2 \equiv m \pmod{p^{k-1}} \implies x^2 + y^2 \equiv m + rp^{k-1} \pmod{p^k}; \quad 0 \leq r \leq p-1, \quad (8)$$

где, поскольку $m \not\equiv 0 \pmod{p}$, мы можем считать, что $x \not\equiv 0 \pmod{p}$.

Следовательно, пусть \tilde{r} — единственное решение сравнения

$$2x\tilde{r} \equiv -r \pmod{p}.$$

Тогда согласно (8) имеем

$$(x + \tilde{r}p^{k-1})^2 + y^2 \equiv x^2 + y^2 + 2x\tilde{r}p^{k-1} \equiv m \pmod{p^k},$$

что завершает индукцию в этом случае и показывает, как и при доказательстве теоремы 3, что система (7) разрешима с $t = 0$, если $m, m' \not\equiv 0 \pmod{p}$.

Предположим теперь, что $m \not\equiv 0 \pmod{p}$, $m' \equiv 0 \pmod{p}$. Мы выбираем любой $t \not\equiv 0 \pmod{p}$ такой, что $t^2 \not\equiv m \pmod{p}$, и рассматриваем эквивалентную систему

$$\begin{aligned}x^2 + y^2 &\equiv m - t^2 \pmod{p^k}, \\z^2 + w^2 &\equiv m' - t^2 \pmod{p^k},\end{aligned}\tag{9}$$

в x, y, z, w .

По определению t мы знаем, что

$$m' - t^2 \not\equiv 0 \pmod{p}, \quad m - t^2 \not\equiv 0 \pmod{p}$$

и, таким образом, решение (9) сводится к предыдущему случаю.

Наконец, доказательство случая $m, m' \equiv 0 \pmod{p}$ полностью аналогично доказательству предыдущего случая, надо только выбирать любое $t \not\equiv 0 \pmod{p}$. \square

4. Задача по модулю степени 2

Пусть $k \geq 1$ — целое число. Мы рассматриваем систему

$$\begin{aligned}t^2 + x^2 + y^2 &\equiv m \pmod{2^k}, \\t^2 + z^2 + w^2 &\equiv m' \pmod{2^k},\end{aligned}\tag{10}$$

в $t, x, y, z, w \in \mathbb{Z}/2^k\mathbb{Z}$.

В этом разделе мы будем предполагать, что m, m' — Лежандровы целые числа, и что $v_2(\gcd(m, m')) \leq 1$.

Случай $k = 1$ тривиален (он был рассмотрен в начале раздела 2), и нетрудно видеть, что при $k = 2$ система (10) разрешима для всех (m, m') , не сравнимых с $(0, 3)$ по модулю 4.

В дальнейшем мы будем обозначать m_0 и m_1 соответствующие приведения m и m' по модулю 2^{k-1} и будем рассматривать приведение (10) по модулю 2^{k-1} :

$$\begin{aligned}t^2 + x^2 + y^2 &\equiv m_0 \pmod{2^{k-1}}, \\t^2 + z^2 + w^2 &\equiv m_1 \pmod{2^{k-1}}.\end{aligned}\tag{11}$$

Если (11) имеет решение, то можем записать (10) в виде

$$\begin{aligned}t^2 + x^2 + y^2 &\equiv m_0 + r2^{k-1} \pmod{2^k}, \\t^2 + z^2 + w^2 &\equiv m_1 + s2^{k-1} \pmod{2^k},\end{aligned}\tag{12}$$

где $r, s \in \{0, 1\}$.

Всего существует четыре возможных пар (r, s) , и основная идея, лежащая в основе данного раздела, заключается в том, что решение (11) дает решение (12) ровно для одной пары (r, s) , и мы хотим использовать это решение (12) для перехода к соответствующим решениям (12) для трех оставшихся пар (r, s) .

При необходимости, сделав замена переменных

$$m_0 \rightarrow m_0 + 2^{k-1}, \quad m_1 \rightarrow m_1 + 2^{k-1},$$

можно считать, что данное решение всегда имеет $r = s = 0$.

Для любой компоненты u с

$$v_2(u) < \frac{k-3}{2},\tag{13}$$

замена переменных

$$u' = u + 2^{k-v_2(u)-2}$$

дает

$$u'^2 \equiv u^2 + 2^{k-1} \pmod{2^k}.$$

Кроме того, если

$$k \text{ нечетно, } v_2(u) > \frac{k-3}{2}, \quad (14)$$

тогда замена переменных

$$u' = u + 2^{\frac{k-1}{2}}$$

дает

$$u'^2 \equiv u^2 + 2^{k-1} \pmod{2^k}.$$

Компоненты, удовлетворяющие (13) или (14), мы называем поднимаемыми компонентами.

Решение (12) назовем применимым, если хотя бы одна из t, x, y и одна из t, z, w поднимаемы, а если t поднимаемый, то существует еще один поднимаемый компонент, кроме t .

Определим для поднимаемого вычета u

$$\psi(u) = \begin{cases} k - v_2(u) - 2 & \text{если } u \text{ удовлетворяет (13),} \\ \frac{k-1}{2} & \text{если } u \text{ удовлетворяет (14).} \end{cases}$$

ПРЕДЛОЖЕНИЕ 1. Если существует применимое решение (12) для $r = s = 0$, то существует решение (12) для любой пары $(r, s) \in J$.

ДОКАЗАТЕЛЬСТВО. Если $u_0, u_1 \in \{t, x, y, z, w\}$ — разные поднимаемые компоненты данного решения (12), то замена переменных

$$u'_0 = u_0 + \epsilon_0 2^{\psi(u_0)}, u'_1 = u_1 + \epsilon_1 2^{\psi(u_1)}, \quad (15)$$

гдк ϵ_0, ϵ_1 означают либо 0, либо 1, если фиксировать остальные компоненты, как легко видеть, дает решения (12) для различных пар $(r, s) \in J$ при вариациях значений $\epsilon_0, \epsilon_1 \in \{0, 1\}$.
□

ЛЕММА 2. Если t, t' нечетны, то (10) разрешимо.

ДОКАЗАТЕЛЬСТВО. Мы индуктивно покажем, что существует решение (10) с нечетными x и z и, следовательно, поднимаемыми.

При $k = 3$ это можно проверить вычислительно.

Предположим, что это справедливо для $k-1$, так что (11), а значит, и (12), имеют решение с x и z нечетными.

Замена переменных в (15) при $u_0 = x, u_1 = z$ дает решения (12) для остальных пар $(r, s) \in J$, а u'_0, u'_1 остаются нечетными для всех значений ϵ_0, ϵ_1 . □

ПРЕДЛОЖЕНИЕ 2. Пусть $k \geq 3$. Нечетный вычет $u \in \mathbb{Z}/2^k\mathbb{Z}$ является квадратичным вычетом тогда и только тогда, когда $u \equiv 1 \pmod{8}$.

ДОКАЗАТЕЛЬСТВО. Обратное утверждение очевидное из того факта, что 1 — единственный нечетный квадратичный вычет по модулю 8.

Для прямого утверждения, мы знаем, что u может быть выражен однозначно как

$$u \equiv (-1)^{\frac{u-1}{2}} 5^{h(u)}; \quad 0 \leq h(u) < 2^{k-2}.$$

Следовательно, несложно увидеть, что u является квадратичным вычетом тогда и только тогда, когда $\frac{u-1}{2}$ и $h(u)$ четны, что дает ровно $2^{k-3} = \frac{2^k}{8}$ квадратичных вычетов, и с учетом обратной импликации отсюда следует, что любой $u \equiv 1 \pmod{8}$ является квадратичным вычетом.

□

Предложение 3. *Если существует решение (12) при $r = s = 0$ с хотя одним из x, y, z, w нечётным, то существует решение (12) для любой пары $(r, s) \in J$.*

Доказательство. Без ограничения общности предположим, что x нечетно. Это позволяет перейти к решению (12) при $r = 1$ при фиксировании s , применив замену переменных в (15) с $u_0 = z$, без u_1 .

Следовательно, нам достаточно найти решения уравнения (12) для $s = 1$, поскольку мы можем перейти между решениям для $r = 0$ и $r = 1$, сохраняя при этом s фиксированным, как было только что показано.

Если бы одно из t, z, w было поднимаемым, то у нас было бы применимое решение, и предложение следует из предложения 1.

Поэтому предположим, что ни один из t, z, w не поднимается. Рассматриваем два случая.

Случай 1. k четно:

Тогда $t^2, z^2, w^2 \in \{0, 2^{k-2}\}$ и, следовательно, $m_1 \in \{0, 2^{k-2}, 2^{k-1}, 3 \cdot 2^{k-2}\}$, что дает

$$m_1 + 2^{k-1} \in \{0, 2^{k-2}, 2^{k-1}, 3 \cdot 2^{k-2}\}.$$

Следовательно, мы всегда можем взять $t^2 = 0$ или $t^2 = 2^{k-2}$ в представлении $m_1 + 2^{k-1}$, и, таким образом, решение (12) для $s = 1$ всегда можно найти либо взяв $z' = z$, если $t^2 = 0$, либо

$$z'^2 \equiv z^2 - 2^{k-2} \pmod{2^k}$$

если $t^2 = 2^{k-2}$, что возможно по предложению 2, поскольку имеем $z^2 - 2^{k-2} \equiv z^2 \equiv 1 \pmod{8}$, так как $k \geq 5$ и z нечетно.

Случай 2. k нечетно:

Тогда $t^2 = z^2 = w^2 = 2^{k-3}$, и поэтому $m_1 = 3 \cdot 2^{k-3}$, что дает $m_1 + 2^{k-1} \equiv 7 \cdot 2^{k-1}$.

Поскольку k нечетно, мы видим, что $m_1 + 2^{k-1}$ не является Лежандровым, и поэтому $s = 1$ не может быть. □

Сформулируем и докажем основной результат данного раздела.

ТЕОРЕМА 5. *Пусть m, m' — Лежандровые целые числа, и что $v_2(\gcd(m, m')) \leq 1$.*

Тогда система (10) разрешима если и только если (m, m') не сравнима с $(0, 3)$ или $(3, 4)$ по модулю 8, и не сравнима ни с одной из $(0, 6), (0, 14), (2, 12), (10, 12)$ по модулю 16.

Доказательство. При $k = 3, 4$ это можно проверить непосредственным вычислением.

Предположим, что $k \geq 5$.

Докажем теорему по индукции. Предположим, что (10) разрешимо для $k - 1$, так что нам дано решение (14), которое, не ограничивая общности, можно считать с $r = s = 0$.

Если данное решение поднимается, то теорема следует из предложения 1.

Предположим, что данное решение не является поднимаемым. Если один из x, y, z, w был нечетным, то теорема следует из предложения 3.

Если все x, y, z, w четные, а t нечетно, то m и m' оба нечетны, и теорема следует из леммы 2.

Если бы все t, x, y, z, w были четными, то мы имели бы $v_2(\gcd(m, m')) \geq 2$, что противоречит условиям теоремы. □

5. Доказательство основного результата

Доказательство теоремы 2 займет весь данный раздел.

Сначала докажем третье утверждение теоремы 2. Допустим, что нам дано решение системы (2) такое, что q четно. Тогда $q^2 \equiv 0 \pmod{4}$, а приведение (2) по модулю 4 показывает, что a, b_1, b_2, c_1, c_2 обязательно четны, поэтому мы можем разделить все члены обоих уравнений в (2) на 4. Повторяя этот процесс, мы видим, что если (2) имеет решение, то q можно предположить нечетным. Это доказывает третье утверждение теоремы 2.

Рассмотрим систему двух диагональных квадратичных форм с целыми коэффициентами

$$\begin{aligned} mu^2 - t^2 - x^2 - y^2 &= 0, \\ m'u^2 - t^2 - z^2 - w^2 &= 0. \end{aligned} \quad (16)$$

Если m и m' оба рациональные квадраты, то (16) имеет нетривиальное решение

$$u = 1, x = \sqrt{m}, z = \sqrt{m'}, t = y = w = 0,$$

и поэтому в дальнейшем мы предполагаем, что хотя бы один из m и m' не является рациональным квадратом.

В разделах 2,3,4 мы рассматривали разрешимость системы (16) в кольцах $\mathbb{Z}/p^k\mathbb{Z}$ для всех простых p и целых чисел $k \geq 1$, при условии, что $v_2(\gcd(m, m')) \leq 1$.

Для перехода к пересечениям в p -адических полях \mathbb{Q}_p воспользуемся следующей простой леммой ([2], ст. 14, предложение 6).

ЛЕММА 3. Пусть $f_i \in \mathbb{Z}_p[X_1, \dots, X_h]$ — однородные многочлены с целыми p -адическими коэффициентами, и пусть $f_{i,k} \in (\mathbb{Z}/p^k\mathbb{Z})[X_1, \dots, X_h]$ обозначают их приведения по модулю p^k . Тогда f_i имеют общий нетривиальный нуль в $(\mathbb{Q}_p)^h$ тогда и только тогда, когда $f_{i,k}$ имеют общий примитивный нуль в $(\mathbb{Z}/p^k\mathbb{Z})^h$ для всех $k > 1$.

Чтобы убедиться, что лемма 3 применима к нашему случаю, рассмотрим приведение системы (16) по модулю p^k .

Если p — нечетное простое число, то теорема 4 показала, что система (16) имеет нетривиальное решение в $\mathbb{Z}/p^k\mathbb{Z}$ для всех пар (m, m') , и существует такое решение содержащее примитивный элемент из $\mathbb{Z}/p^k\mathbb{Z}$.

Если $p = 2$, то из предположения, что $v_2(\gcd(m, m')) \leq 1$, следует, что хотя бы одно из m и m' не сравнимо с 0 по модулю 2^k при $k > 1$, а теорема 5 показывает, что (16) разрешимо в $\mathbb{Z}/2^k\mathbb{Z}$ для всех таких пар (m, m') , не сравнимых с исключениями из теоремы 2 (или, что то же самое, исключениями из самой теоремы 5). Такие пары (m, m') обладают тем свойством, что хотя бы одно из m и m' предполагается ненулевым в $\mathbb{Z}/2^k\mathbb{Z}$, мы всегда можем взять $u = 1$ при решении (16) в $\mathbb{Z}/2^k\mathbb{Z}$, и это, очевидно, дает примитивное решение.

Таким образом, мы показали, что для пар, не сравнимых с исключениями из теоремы 2, система (16) имеет нетривиальные решения во всех p -адических полях \mathbb{Q}_p , при условии, что $v_2(\gcd(m, m')) \leq 1$.

Система (16), очевидно, нетривиально разрешима в \mathbb{R} .

Теперь нам нужен механизм перехода от решений во всех пополнениях \mathbb{Q} , а именно p -адических полях \mathbb{Q}_p и \mathbb{R} , к решениям в самом \mathbb{Q} .

Для этого воспользуемся следующим результатом Коллио-Телена, Корэ и Сансука ([5], ст. 22, теорема 3.2).

ТЕОРЕМА 6. Пусть \mathbb{K} — числовое поле и ϕ, ϕ_1, ϕ_2 — невырожденные бинарные квадратичные формы с коэффициентами из \mathbb{K} .

Рассмотрим трехмерное \mathbb{K} -многообразие V в проективном пространстве $\mathbb{P}_{\mathbb{K}}^5$, заданное пересечением двух квадратичных уравнений

$$\phi(u_1, v_1) = \phi_1(x, y), \quad \phi(u_2, v_2) = \phi_2(x, y).$$

Предположим, что ϕ_1 или ϕ_2 анизотропны. Тогда если V имеет \mathbb{K}_p -ую точку для каждого пополнения \mathbb{K}_p поля \mathbb{K} , то V имеет \mathbb{K} -ую точку.

Взяв $\mathbb{K} = \mathbb{Q}$ и

$$\phi(u, v) = u^2 + v^2, \quad \phi_1(x, y) = mx^2 - y^2, \quad \phi_2(x, y) = m'x^2 - y^2,$$

мы видим, поскольку в начале данного раздела предполагалось, что хотя бы один из m и m' не является рациональным квадратом, то один из ϕ_1 и ϕ_2 анизотропен.

Следовательно, теорема применима, и мы видим, что (16) имеет нетривиальное рациональное решение, при $v_2(\gcd(m, m')) \leq 1$.

Если $u = 0$ в рациональном решении (16) в \mathbb{Q} , то $t = x = y = z = w = 0$, что является тривиальным решением, и поэтому существует решение системы (16) в \mathbb{Q} с $u \neq 0$. Взяв такое решение и умножив (16) на u^{-2} , получим

$$m = \frac{a^2}{q^2} + \frac{a_1^2}{q_1^2} + \frac{a_2^2}{q_2^2}, \quad m' = \frac{a^2}{q^2} + \frac{a_3^2}{q_3^2} + \frac{a_4^2}{q_4^2},$$

где $a, q, a_i, q_i \in \mathbb{Z}$, при этом можно предположить, что $\gcd(a, q) = 1$, и это все можно записать как

$$q^2m - a^2 = \frac{q^2a_1^2}{q_1^2} + \frac{q^2a_2^2}{q_2^2}, \quad q^2m' - a^2 = \frac{q^2a_3^2}{q_3^2} + \frac{q^2a_4^2}{q_4^2}.$$

Следовательно, целые числа $q^2m - a^2$ и $q^2m' - a^2$ представляются в виде суммы двух рациональных квадратов.

Чтобы показать, что $q^2m - a^2$ и $q^2m' - a^2$ представляются в виде суммы двух целых квадратов, нам нужно одно следствие теоремы Давенпорта-Касселса ([2], ст. 46), которая мы сейчас сформулируем.

ТЕОРЕМА 7. (ДАВЕНПОРТ-КАССЕЛС) Пусть f — положительно определенная квадратичная форма от h переменных с целыми коэффициентами.

Предположим, что для любого $(y_1, \dots, y_h) \in \mathbb{Q}^h$ существует $(x_1, \dots, x_h) \in \mathbb{Z}^h$ такое, что

$$f(\vec{x} - \vec{y}) < 1.$$

Тогда любое целое число, представимое f в \mathbb{Q} , представимо f в \mathbb{Z} .

ЛЕММА 4. Если целое число представляется в виде суммы двух рациональных квадратов, то оно представляется в виде суммы двух целых квадратов.

Лемма непосредственно следует из применения теоремы Давенпорта-Касселса с

$$f(\vec{v}) = v_1^2 + v_2^2, \quad x_i = \|y_i\|,$$

где $\|y_i\|$ обозначает ближайшее целое число к y_i .

Таким образом, применяя лемму мы видим, что $q^2m - a^2$ и $q^2m' - a^2$ оба представляются как сумма двух целых квадратов, что дает (2):

$$q^2m - a^2 = b_1^2 + c_1^2, \quad q^2m' - a^2 = b_2^2 + c_2^2,$$

что доказывает первое утверждение теоремы 2, при условии, что $v_2(\gcd(m, m')) \leq 1$.

Более того, поскольку $\gcd(a, q) = 1$, это доказывает второе утверждение теоремы 2, при условии, что $v_2(\gcd(m, m')) \leq 1$.

Это завершает доказательство теоремы 2 при условии, что $v_2(\gcd(m, m')) \leq 1$.

Для доказательства первого утверждения теоремы 2 в общем случае, воспользуемся следующей леммой.

ЛЕММА 5. Пусть $m, m' \in \mathbb{Z}$ такие, что $4 \mid \gcd(m, m')$. Тогда (2) разрешимо для (m, m') тогда и только тогда, когда оно разрешимо для $(\frac{m}{4}, \frac{m'}{4})$.

ДОКАЗАТЕЛЬСТВО. Предположим, что нам дано решение (2) для (m, m') . Тогда приведение обоих уравнений (2) по модулю 4 показывает, что a, b_1, b_2, c_1, c_2 четные, и поэтому мы можем разделить все члены обоих уравнений в (2) на 4, и получим

$$q^2 \left(\frac{m}{4} \right) = \left(\frac{a}{2} \right)^2 + \left(\frac{b_1}{2} \right)^2 + \left(\frac{c_1}{2} \right)^2,$$

$$q^2 \left(\frac{m'}{4} \right) = \left(\frac{a}{2} \right)^2 + \left(\frac{b_2}{2} \right)^2 + \left(\frac{c_2}{2} \right)^2,$$

что является решением (2) для $(\frac{m}{4}, \frac{m'}{4})$.

Наоборот, если нам дано решение (2) для $(\frac{m}{4}, \frac{m'}{4})$, то умножение всех слагаемых на 4 дает

$$q^2 m = (2a)^2 + (2b_1)^2 + (2c_1)^2,$$

$$q^2 m' = (2a)^2 + (2b_2)^2 + (2c_2)^2,$$

что является решением уравнения (2) для (m, m') . \square

Из утверждения теоремы 2 легко видеть, что исключения для любого четного $k \geq 6$ являются образцами исключений $k - 2$ при умножении на 4. При $k = 4$ все исключения из теоремы 2 входят в теорему 5. Следовательно, лемма 5 показывает, что доказательство первого утверждения теоремы 2 при условии, что $v_2(\gcd(m, m')) \leq 1$, эквивалентно общему случаю.

Для второго утверждения теоремы 2, по лемме 5 можно предположить, что дано решение (2) для $(\frac{m}{4}, \frac{m'}{4})$ с $\gcd(a, q) = 1$, и по третьему утверждению теоремы 2, доказанному в общем случае в начале данного раздела, можно считать, что q нечетно. Доказательство леммы 5 показало, что соответствующее решение (2) для (m, m') есть $(q, 2a, 2b_1, 2b_2, 2c_1, 2c_2)$, и очевидно, что $\gcd(q, 2a) = \gcd(q, a) = 1$. Это завершает доказательство теоремы 2 в общем случае.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Anthony Knapp. Advanced Algebra // Birkhäuser Boston, 2006.
2. Jean-Pierre Serre, A Course in Arithmetic // Springer Verlag, New York 1973.
3. В. Н. Чубариков. Обобщенная формула бинома Ньютона и формулы суммирования // Чебышевский сборник, 2020, т.00, с.1–18.
4. J.-L. Colliot-Thélène, J.-J. Sansuc, Sir Peter Swinnerton-Dyer. Intersections of two quadrics and Châtelet surfaces // J. für die reine und angew Math. I, Bd. 373(1987) 37-107; II Bd. 374(1987) 72-168.
5. Colliot-Thélène, Jean-Louis, and Coray, D. Descente et principe de Hasse pour certaines variétés rationnelles // Journal für die reine und angewandte Mathematik 320 (1980): 150-191.
6. Per Salberger On the arithmetic of intersections of two quadrics containing a conic, 2023, arXiv:2305.02109v1 [math.NT].
7. Виноградов И. М. Основы теории чисел // М.: Физ.-мат.лит. 1983.
8. Боревиц З.И., Шафаревич И.Р. Теория Чисел // Москва, 1964.

REFERENCES

1. Anthony, Knapp, 2006. “Advanced Algebra”, *Birkhäuser Boston*.
2. Jean-Pierre, Serre, 1973. “A Course in Arithmetic”, *Springer Verlag, New York*.
3. Chubarikov, V. N., 2020. “A generalized Binomial theorem and a summation formulae”, *Chebyshevskii Sbornik*, Vol.21, Iss. 4, pp. 1–18.
4. Colliot-Thélène, J.-L., Sansuc, J.-J., Sir Peter Swinnerton-Dyer, 1987. “Intersections of two quadrics and Châtelet surfaces”, *J. für die reine und angew. Math. I, Bd.*, 373, pp. 37–107; *II Bd.*, 374, pp. 72–168.
5. Colliot-Thélène, Jean-Louis, and Coray, D., 1980. “Descente et principe de Hasse pour certaines variétés rationnelles”, *Journal für die reine und angewandte Mathematik*, 320, pp. 150–191.
6. Per Salberger, 2023. “On the arithmetic of intersections of two quadrics containing a conic”, arXiv:2305.02109v1 [math.NT].
7. Vinogradov, I. M., 1983. “Foundations of Number Theory”, *M.: Fiz.-Mat.lit.*.
8. Borevich, Z. I., Shafarevich, I. R., 1964. “Theory of Numbers”, *M: Moscow*.

Получено: 18.12.2023

Принято в печать: 21.03.2024