МИНИСТЕРСТВО ВЫСШЕГО И СРЕДНЕГО СПЕЦИАЛЬНОГО ОБРАЗОВАНИЯ РЕСПУБЛИКИ УЗБЕКИСТАН

САМАРКАНДСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ АЛИШЕРА НАВОИ

Механико-математический факультет

5400100 – математическое направление

Буляева Мафтуна

МЕТОДЫ ГЕОМЕТРИИ ЧИСЕЛ ДЛЯ РЕШЕНИЯ ДИОФАНТОВЫХ УРАВНЕНИЙ

(выпускная квалификационная работа)

Разрешение на защиту:

Декан факультета: **проф.А.Солеев**

Зав.кафедры: **доц.Х.Х.Рузимурадов**

Научный руководитель: **доц.Х.Х.Рузимурадов**

М.П.

Самарканд-2012

Содержание

Введение

Постановка задачи: Выпускная квалификационная работа посвящена одному из разделов теории чисел – теории диофантовых уравнений, их решению методами геометрии чисел. Рассмотрение диофантовых уравнений частного вида с целыми и рациональными решениями – наиболее важная часть данной работы. Все рассматриваемые уравнения являются классическими и каждое из них играло важную роль в историческом развитии этой области теории чисел.

Актуальность темы: Стандартная задача из элементарной алгебры обычно приводится к системе из двух уравнений с тремя неизвестными. Четкая перспектива периода формирования диофантовых уравнений представлена А.Вейлем, С.Ленгом, И.Виноградовым, и т.д. В настоящее время диофантовы уравнения продолжают изучаться, при этом полная теория разработана лишь для линейных уравнений.

Цели и задачи: В работе изучаются следующие задачи:

- Представление любого натурального числа в виде суммы квадратов целых чисел.
- Изучение основных теорем геометрии чисел.
- Рассмотрение диофантовых уравнений частного вида с целыми и рациональными решениями – наиболее важная часть данной работы
- Применение изученной теории к решению диофантовых уравнений

Научное значение: Одним из центральных в теории диофантовых уравнений является вопрос о том, когда число решений конечно, и о нахождении в этом случае эффективной границы для координат решений. Вопрос об эффективности удалось решить лишь для частного вида. Поэтому

всякое представление решения диофантовых уравнений эффективно имеет научное значение.

Научно-исследовательские методы: В работе используются методы алгебры и геометрии чисел, методы решения сравнений, методы решения уравнений.

Практическое значение работы: Методы решения диофантовых уравнений и их эффективность связаны с вопросами представления чисел в виде суммы двух, трех и четырех квадратов целых чисел. Результаты, приведенные в работе могут найти применение в различных задачах геометрии чисел, теории чисел.

Содержание работы: Работа состоит из введения, трех глав, семи параграфов, заключения и списка использованной литературы, содержащий 5 наименований.

Во введении обосновывается тема, дается обзор литературы, формулируются цели и задачи и краткое содержание темы работы.

В первой главе даны основы геометрии чисел: решетки, подрешетки и их базисы, а также основные теоремы геометрии чисел.

Во второй главе описываются квадратичные формы и их связь с решетками.

Третья глава представляет самостоятельную часть работы, изучаются диофантовы уравнения. В этой главе, на основании изученной теории, решены следующие задачи:

1) Решено неопределенное уравнение

$$x^2 - 21x + 110 = 13y$$

Решением уравнения будут системы

$$\begin{cases} x_1 = 10 + 13t \\ y_1 = 13t^2 - t \end{cases}$$

$$\begin{cases} x_2 = 11 + 13t \\ y_2 = 13t^2 + t \end{cases}$$

2) Доказано, что уравнение неразрешимо в целых числах.

3) Решить в целых числах уравнение

$$4x - 9y + 13z = 7$$

Для этого уравнения получим решения

$$z = 7 - 4x' - 3y', \Rightarrow$$

$$y = 16x' + 13y' - 28, \Rightarrow$$

$$x = 49x' + 39y' - 84,$$

где x' и y' – произвольные целые числа.

4) Решено в рациональных числах уравнение

Решением уравнения является целое число -3 .

ГЛАВА I. Основы геометрии чисел

§ I.1. Решетки, подрешетки и их базисы

Геометрия чисел сформировалась с выходом основополагающей монографии Г. Минковского в 1896 году, где подмечалось то обстоятельство, что некоторые предложения почти очевидны при рассмотрении фигур в $n-$ мерном евклидовом пространстве.

Основной и типичной задачей геометрии чисел является задача об арифметическом минимуме $M(F)$ некоторой действительной функции

$$F(x) = F(x_1, x_2, \dots, x_n)$$

При этом под $m(F)-$ понимается точная граница значения функции $F(x)$; когда x пробегает все целые точки, удовлетворяющие некоторому дополнительному условию (например $x \neq 0$).

Геометрия чисел базируется на теореме Минковского о выпуклом теле, которая дает связь между «геометрическими» свойствами – выпуклостью, симметричностью, объемом и «арифметическими свойствами» - существованием во множестве целой точки.

В этой работе будут изложены теоремы о разрешимости диофантовых уравнений в целых числах, доказанные при помощи теоремы Минковского о выпуклом теле.

Векторы $n-$мерного пространства R^n будем записывать столбцом, т.е.

$$X^T = (x_1, ..., x_n).$$

1. Множество $\Lambda : AZ^n \ (\det A \neq 0)$ будем называть решеткой , где $A-$невырожденная матрица, . Если $A = I$, то решетка называется главной и записывается $\Lambda_0 : Z^n$, т.е., главная решетка совпадает с множеством целочисленных векторов из R^n.

   Величина $d(\Lambda) = |\det A|$ называется объемом решетки Λ.

Лемма 1. Все автоморфизмы множества Z^n совпадает с множеством целочисленных унимодулярных матриц, т.е. $EZ^n = Z^n$, тогда и только тогда, когда E - целочисленная унимодулярная матрица.

Доказательство. Покажем, что если

$$EZ^n = Z^n, \qquad \text{(I.1.1)}$$

то E - целочисленная унимодулярная матрица, и обратное, если E - целочисленная унимодулярная матрица, то выполняется условие (I.1.1).

Пусть выполняется условие (I.1.1) и элемент $e_{ij} \in E$ не целое число. Возьмем вектор $z \in Z^n$, у которого $i-$ой координатой является 1, а остальные координаты нули. Тогда j-ая координата вектора $z_1 = EZ$ есть элемент e_{ij}, поэтому $z \notin Z^n$. Это противоречит тому, что $EZ^n = Z^n$. Следовательно, E-целочисленная матрица.

Далее, можем считать, что $\det E \neq 0$. В противном случае множество $EZ^n = Z^n$ не имело бы n-линейно независимых точек, т.е. все точки множества $EZ^n = Z^n$ лежали бы в пространстве размерности меньшей чем n, что невозможно.

Из равенства $EZ^n = Z^n$ вытекает $Z^n = E^{-1}Z^n$. Отсюда, по только что доказанному, матрица E^{-1} также целочисленная. Из целочисленности матриц E и E^{-1} следует, что $E-$ унимодулярная матрица.

Обратное, пусть E -целочисленная унимодулярная матрица, тогда $EZ^n \subseteq Z^n$, отсюда следует, что $\eta = f(\xi)$. Когда E пробегает все целочисленные унимодулярные матрицы, то E^{-1} также пробегает все целочисленные унимодулярные матрицы, поэтому $EZ^n = Z^n$.

Теорема 1. Пусть в $n-$ мерном пространстве R^n задана решетка $\Lambda: AZ^n$, где $A-$ матричный базис решетки. Для того, чтобы матрица A' была базисом решетки Λ необходимо и достаточно, чтобы существовала целочисленная унимодулярная матрица E, что $A' = AE$.

Доказательство. *Необходимость*.

Рассмотрим два множества, которые совпадают: $A'Z^n$ и AZ^n. Если на эти два множества подействуем матрицей A^{-1} слева, то получим множества $A^{-1}A'Z^n$ и Z^n. Эти множества совпадают, поэтому по лемме I матрица $A^{-1}A^1 = E-$ целочисленная и унимодулярная, т.е. $A' = AE$.

Достаточность.

Рассмотрим множество $A'Z^n = AEZ^n$, где $E-$ унимодулярная, целочисленная матрица. По лемме 1: $EZ^n = Z^n$, следовательно $A'Z^n = AEZ^n = AZ^n$. Теорема доказана.

Решетку Λ можно записать в виде:

$$\Lambda: \left(a_1 z_1 + a_2 z_2 + ... + a_n z_n \;\middle|\; a_i \in Z,\ i = 1,2,...,n\right),$$

$z_1,...,z_n$ – столбцы матрицы A, т.е.

$$A=(Z_1,Z_2,...,Z_n)$$

2. Если каждая точка решетки $M: BZ^n$, $d(M)\neq 0$ является тоже точкой решетки Λ, т.е. $M\subset\Lambda$, то M называется подрешеткой решетки Λ.

Теперь сформулируем и докажем теорему, которая связывает базисы решетки Λ с базисом ее подрешетки.

Теорема II. Для того, чтобы множество M было подрешеткой решетки $\Lambda: AZ^n$ необходимо и достаточно существование целочисленной матрицы B $(\det B\neq 0)$ такой, что $M: ABZ^n$.

Доказательство. *Достаточность*.

Возьмем произвольный элемент Y из M, т.е. $Y_1=AB_x=Ax_2\in\Lambda$, где $x\in Z^n$, $x_2=Bx_1\in Z^n$, $B-$ целочисленная матрица, следовательно $M\subset\Lambda$

Необходимость. Пусть $M\subset\Lambda-$ решетка, тогда M имеет вид: $M: CZ^n$, где $C-$ базис решетки M.

Каждый столбец матрицы C рассмотрим как $n-$ мерный вектор, т.е. $C=(Y_1,Y_2,...,Y_n)$.

Из определения M следует, что $Y_1,Y_2,...,Y_n\in\Lambda$. Тогда из определения Λ следует существование векторов $Y_1,Y_2,...,Y_n\in\Lambda$, таких, что имеют место равенства:

$$\begin{cases} Ax_1 = Y_1 \\ Ax_2 = Y_2 \\ \vdots \\ Ax_n = Y_n \end{cases} \quad \text{или} \quad A(x_1, x_2, ..., x_n) = (Y_1, Y_2, ..., Y_n)$$

т.е. $AB = C$, где $C -$ целочисленная матрица, следовательно, $M : AB Z^n$. Теорема доказана.

3. Целое число

$$Y = \frac{d(M)}{d(\Lambda)} = \frac{(\det A)(\det B)}{(\det A)} = |\det\ B|$$

называется индексом подрешетки M в решетке Λ.

§ I.2. Основные теоремы геометрии чисел

Определение. Точечное множество T называется компактным, если любая последовательность точек $X_i \in T$ содержит последовательность

$$Y_s = X_{rs} \quad (z_1 < z_2 < \cdots)$$

сходящуюся к пределу в T.

$$\lim_{s\to\infty} Y_s = Y' \in T$$

Говорят, что последовательность векторов $X_r \ (r = 1,2,...)$ сводятся к вектору X, если $\lim(X_2 - X_1) = 0$ в обычном смысле.

Теорема 1. (Блихфельдт) Пусть m – натуральное число, Λ – решетка с определителем $d(\Lambda)$, а T – точечное множество объема $V(T)$ (допускается случай $V(T) = \infty$). Предположим, что либо

$$V(T) > md(\Lambda) \qquad (1)$$

либо компактно и

$$V(T) = md(\Lambda) \qquad (2)$$

тогда найдутся $m+1$ таких различных точек $x_1, x_2, ..., x_{m+1} \in T$, что все разности $x_i - x_j$ содержатся в Λ.

Доказательство. Пусть $b_1, b_2, ..., b_n$ – произвольный базис решетки Λ, а P – обобщенный параллелепипед, т.е. множество точек вида:

$$Y_1 b_1 + Y_2 b_2 + \ldots + Y_n b_n \quad \left(0 \le Y_j < 1,\ 1 \le j \le n\right)$$

Тогда объем P равен:

$$V(P) = \left(\det(b_1, b_2, \ldots, b_n)\right) d(\Lambda) \qquad (3)$$

Каждую точку Z пространства можно представить в виде:

$$Z = u + v, \text{ где } u \in \Lambda,\ v \in P$$

причем это представление однозначно, ибо точки решетки имеют вид:

$$Y_1 b_1 + Y_2 b_2 + \ldots + Y_n b_n$$

при целых $Y_1, Y_2, \ldots, Y_n$.

Пусть $u \in \Lambda$, через $R(u)$ будем обозначать множество точек v с условием

$$v \in P, \quad v + u \in T.$$

Очевидно, что для объемов $V(R(u))$ этих множеств справедливо равенство:

$$\sum_{u \in \Lambda} V\{R(u)\} = V(T) \qquad (4)$$

Предположим теперь, что выполнено первое условие, а именно

$$V(T) > md(\Lambda)$$

Тогда из равенства (4) вытекает следующее неравенство:

$$\sum_{u \in \Lambda} V\{R(u)\} > md(\Lambda) = mV(P)$$

Ввиду того, что все множества $R(u)$ содержатся в P должна найтись по крайней мере одна точка $v_0 \in P$ принадлежащая $m+1$ множествам вида: $R(u)$. Скажем $v_0 \in P(u_j), \quad (1 \le j \le m+1)$, где u_j различные точки. Тогда по определению $R(u)$ точки $z_j = v_0 + u_j$ находятся в T, причем

$$z_i - z_j = u_j - u_i \begin{cases} \in \Lambda \\ \neq 0 \ (i \neq j) \end{cases}$$

Этим доказан первый случай теоремы.

Предположим теперь, что выполнено второе условие. Пусть $\varepsilon_r \ (1 \le z < \infty)$ последовательность чисел, причем $\lim \varepsilon_k = 0$. Для каждого z множество $(1+\varepsilon_r)T$ точек $(1+\varepsilon_r)z$, где $z \in T$ имеет очевидно объем

$$(1+\varepsilon_r)^n V(T) > V(T) = md(\Lambda).$$

Следовательно, в силу только что доказанного, найдутся такие точки

$$z_{ir} \in (1+\varepsilon_r)T \quad (1 \le j \le m+1)$$

что скажем

$$u(i, j) = z_{ir} - z_{jr} \begin{cases} \in \Lambda \\ \neq 0 \quad (j \neq i) \end{cases} \qquad (5)$$

Выделив подходящим образом из заданной последовательности подпоследовательности (которые обозначим теми же индексами), мы можем, не ограничивая общности, предполагать, что все пределы $\lim\limits_{\varepsilon \to \infty} z_{jr} = z_j \quad (1 \le j \le m+1)$ существуют. Здесь z_{jr} – подпоследовательность, отвечающие выбранным последовательностям ε_r.

Так как предполагается, что $T-$ компактно, то точки z_j находятся в T. Тогда в силу равенства (5)

$$z_i^1 - z_j^1 = \lim_{\varepsilon \to \infty} u_r(i, j)$$

Но точки $u_r(i, j) \in \Lambda$. Это значит, что начиная с некоторого места точки $u_r(i, j)$ не зависят от ε, т.е. $u_r(i, j) = u'(i, j)$.

Таким образом, мы разобрали второй случай теоремы. Теорема полностью доказана.

Теорема 2. (обобщенная теорема Минковского) Пусть $S-$симметрическое множество с объемом $V(S)$ и $\Lambda-$решетка с определителем $d(\Lambda)$. Если $V(S) \geq d(\Lambda)$, то множество $S+S$ содержит точки решетки Λ, кроме начала.

Доказательство. По условию теоремы $V(S) \geq d(\Lambda)$, тогда по теореме Блихфельдта множество S содержит пару различных точек $z_1, z_2 \in S$, т.к. $S-$симметрическое множество, то вместе с z_2 множество S содержит и $-z_2$, поэтому, по определению суммы $S+S$ точка $z_1 - z_2$ принадлежит $S+S$. Теорема доказана.

Теорема 3. (теорема Минковского о выпуклом теле).

Пусть $S-$симметрическое относительно начала координат выпуклое точечное множество с объемом $V(S)$ (возможно бесконечное). Пусть $m-$целое число, а $V-$решетка с определителем $d(V)$. Пусть $V(S) > mz^n d(\Lambda)$, либо $S-$компактное множество и $V(S) = mz^n d(\Lambda)$,

тогда S содержит по крайней мере m пар различных точек $\pm u_j \ (1 \le j \le m+1)$ решетки Λ, не совпадающих с 0.

Доказательство. Применим теорему Блихфельдта к множеству $\frac{1}{2}S$, состоящую из точек $\frac{1}{2}z$, где $\in S$. Ее объем будет равен $\frac{1}{2^n}V(S)$. Тогда найдутся $m+1$ различных точек $\frac{1}{2}z_j \in \frac{1}{2}S, \quad (1 \le j \le m+1)$, что

$$\frac{1}{2}z_i - z_j \begin{cases} \in \Lambda \\ \neq 0 \quad (j \neq i) \end{cases}$$

Упорядочим вещественные точки, считая $z_1 > z_2 > \ldots$

Если первая, отличная от нуля координата точки $z_1 - z_2$ положительна не умаляя общности, можно считать, что

$$z_1 > z_2 > \ldots > z_{m+1}$$

Положим

$$u_j = \frac{1}{2}z_j - \frac{1}{2}z_{m+1}$$

Тогда, очевидно, что все точки $0, \pm u_1, \pm u_2, \ldots, \pm u_n$ различны. Но $-z_{m+1} \in S$, т.к. $z_{m+1} \in S$ и множество S симметрично. Следовательно, $u_j = \frac{1}{2}(-z_j) + \frac{1}{2}(-z_{m+1}) \in S$, в силу выпуклости S. Теорема полностью доказана.

Из этой теоремы непосредственно следует

Теорема 4. Если $S-$ произвольное множество, а T выпуклое и центрально – симметрическое множество, причем:

$$T \subset \bigcup_{k=1}^{\infty} \frac{1}{k} S = \overline{S},$$

то множество S содержит точку (отличную от начала) любой точки Λ с определителем $d(\Lambda) = 2^{-n} V(T)$.

Доказательство. Для множества T все условия предыдущей теоремы выполняются, поэтому множество T содержит точку решетки Λ, отличную от начала, т.е. $0 \neq z \in \Lambda$ и $z \in T$. По условию теоремы $T \subset S$, значит $z \in S$.

Из этого следует, что

$$z \in \frac{1}{2} S \qquad (6)$$

Если $k = 1$, то теорема доказана, если $k \neq 1$, то из (6) следует, что $k\,z \in S$. Ясно, что $k\,z$ является точкой решетки, т.к. $z \in \Lambda$. Теорема доказана.

Теорема Минковского (о линейных формах).

Пусть задана система линейных форм:

$$\begin{cases} f_1(x) = a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \\ f_2(x) = a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ f_n(x) = a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n \end{cases}$$

и пусть $0 < \left|\det\left(a_{ij}\right)\right| \le c_1 c_2 \ldots c_n$, где $\det\left(a_{ij}\right)$ – определитель системы, $c_1 c_2 \ldots c_n$ любое положительное число. Тогда существует целое число при котором будет выполнено:

$$f_1(x_0) \le c_1$$
$$f_2(x_0) \le c_2$$
$$\ldots\ldots\ldots\ldots$$
$$f_n(x_0) \le c_n$$

Доказательство. Рассмотрим решетку $\Lambda : AZ^n$, где A матрица системы

$$A = \left(a_{ij}\right) = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n1} & a_{n2} & a_{n3} & \cdots & a_{nn} \end{pmatrix}$$

Множество AZ^n имеет вид

$$\Lambda : AZ^n = \left\{ \begin{pmatrix} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n \end{pmatrix} \right\} = \left\{ \begin{pmatrix} f_1(x) \\ f_2(x) \\ \ldots\ldots \\ \ldots\ldots \\ \ldots\ldots \\ f_n(x) \end{pmatrix} \right\}$$

Рассмотрим множество вида

$$P(c_1c_2\cdots c_n):\left\{\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}\right\}\ |y_1|\le c_1\cdots|y_n|\le c_n$$

Это множество выпукло и симметрично.

$$V(P(c_1c_2\cdots c_n))=2^n c_1c_2\cdots c_n\ge 2^n|\det A|=2^n\det A$$

Следовательно, по теореме Минковского о выпуклом теле множество $P(c_1c_2\cdots c_n)$ содержит некоторую точку из решетки $\Lambda: Ax_0,\ \ x_0\neq 0$, что

$$|f_1(x_0)|\le c_1$$
$$|f_2(x_0)|\le c_2$$
$$\cdots\cdots\cdots\cdots$$
$$|f_n(x_0)|\le c_n$$

Теорема доказана.

Глава II. Квадратичные формы и их связь с решетками

§.II.1. Квадратичные формы

Квадратичная форма от n переменных имеет вид

$$f_n(x)=\sum_{1\le i\le j\le n} b_{ij}\,x_i x_j=(x_1,x_2,...,x_n)B\begin{pmatrix}x_1\\x_2\\\vdots\\x_n\end{pmatrix},\ \text{где,}$$

$$B=(b_{ij})=\begin{pmatrix}b_{11}&b_{12}&\cdots&b_{1n}\\b_{21}&b_{22}&\cdots&b_{2n}\\\cdots&\cdots&\cdots&\cdots\\b_{n1}&b_{n2}&\cdots&b_{nn}\end{pmatrix}$$

$b_{ij}=b_{ji}$, т.е. матрица B симметрическая $\left(B^T=B\right)$, $X^T=(x_1,x_2,...,x_n)$.

Формула бинарной квадратичной формы (от двух переменных) запишется в виде

$$f_2(x)=b_{11}x_1^2+2b_{12}x_1x_2+b_{22}x_2^2$$

Определение 1. Форму $f(x)$ называют определенной, если при всех значениях переменной она не меняет знак, т.е. всегда положительна или всегда отрицательна.

Квадратичная форма решетки запишется в виде:

$$f(\Lambda) = f_1^2(x) + f_2^2(x) + \ldots + f_n^2(x) = (AX)^T AX = X^T A^T AX ,$$

где

$$R^n \supset \Lambda : AZ^n = \begin{pmatrix} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n \end{pmatrix} = \left\{ \begin{pmatrix} f_1(x) \\ f_2(x) \\ \vdots \\ f_n(x) \end{pmatrix} \right\}$$

§ II.2. Связь квадратичных форм с решетками

Определение 1. Множество $G \subset R^n$ называется симметричным (относительно начала), если вместе с точкой x оно содержит и точку $-x$.

Определение 2. Множество $G:\{x:+y:\}$, где $x:, y:$независимо друг от друга пробегают соответственно элементы множеств G_1 и G_2, называется суммой двух множеств G_1 и G_2, записываются в виде:

$G = G_1 + G_2$

Лемма 1. Если G_1 и G_2 – симметричные множества, то $G_1 + G_2$ также симметричные множества.

Доказательство. Рассмотрим множество

$G = G_1 + G_2 : \{x:+y:\}$

где $G:\{x:\};\ G\{y:\}$

Пусть $z = x_1 + y_1 \in G$,

где $x_1 \in G,\ y_1 \in G$. Так как множества G_1 и G_2 симметричны, то $-x_1 \in G,\ -y_1 \in G$, тогда по определению суммы имеем

$(-x_1) + (-y_1) = -z \in G$. Лемма доказана.

Определение 3. Множество $G \subset R^n$ называется выпуклым, если для любых точек $x_1, x_2 \in G$ и любого числа $\lambda (0 \le \lambda \le 1)$ выполняется

$\lambda x_1 + (1-\lambda)x_2 \in G$.

Лемма 2. Если G_1, G_2 – выпуклые множества, $G_1 + G_2$ также выпуклое множество.

Доказательство. Предположим противное. Пусть $G_1 + G_2$ – не выпуклое множество, т.е. существуют такие точки Z_1 и Z_2 из $G_1 + G_2$, что для некоторого числа $\lambda (0 \le \lambda \le 1)$ имеет место соотношение:

$$\lambda Z_1 + (1-\lambda) Z_2 \notin G_1 + G_2$$

По определению суммы множеств G_1 и G_2 имеем

$$Z_1 = x_1 + y_1 Z_2 = x_2 + y_2,$$

где $x_1, x_2 \in G_1$, $y_1, y_2 \in G_2$.

Так как G_1 и G_2 – выпуклое множество, то

$$\lambda x_1 + (1-\lambda) x_2 \in G_1 \text{ и } \lambda y_1 + (1-\lambda) y_2 \in G_2.$$

Отсюда и из определения 2 вытекает, что

$$\lambda Z_1 + (1-\lambda) Z_2 = \lambda x_1 + (1-\lambda) x_2 + \lambda y_1 + (1-\lambda) y_2 \in G_1 + G_2$$

А это противоречит нашему предположению, следовательно $G_1 + G_2$ выпукло.

Определение 4. Множество $T:\{\bar{x}:\}$ будем называть подобным множеству $S:\{y:\}$ и писать $T \tilde{} S$, если существует такое вещественное число $\lambda > 0$ и точка $Z \in R^n$, что

$$T = Z + \lambda S.$$

Теорема 1. Если выпуклые подобные множества $T:\{\bar{x}:\}$ и $S:\{y:\}$ имеют объемы $V(T)$ и $V(S)$, то имеет место соотношение:

$$V(T+S)=(1+\lambda)^n V(S)=\left(\frac{1}{\lambda}+1\right)^n V(T)$$

Определение 5. Две точки $Y_1, Y_2 \in R^n$ назовем сравнимыми по модулю Λ и запишем $Y_1 \equiv Y_2(\Lambda)$, если их разность $Y_1 - Y_2 \in \Lambda$.

Глава III. Диофантовы уравнения

§ III.1. Основные понятия

Диофантовыми уравнениями называют уравнение, которое должно быть решено в целых числах.

Ни одна из областей теории чисел не сталкивается с такими трудностями, как теория диофантовых уравнений. С помощью различных искусственных приемов установлено много результатов, связанных с отдельными уравнениями вида $x^2 + y^2 = n$, $x^2 - Ny^2 = 1$ и т.д. , но весьма затруднительным является объединить эти результаты в общую теорию. Иногда удается создать общую теорию, связанную с найденным решением, разумно объясняющую возникновение этого решения и показывающую, насколько найденное решение можно обобщить. Но внутренние трудности предмета настолько велики, что область применения такой теории обычно очень ограничена. Если получается развить достаточно глубокую теорию диофантовых уравнений специального вида, например, теорию квадратичных форм, то такая теория выделяется как самостоятельная.

Существует несколько диофантовых уравнений, допускающие элементарное исследование, где возможно указаны общие теории, связанные с этими уравнениями. Например, уравнение

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

Это уравнение интересовало греческих математиков в связи с Теоремой Пифагора, и его общее решение дал Евклид:

После разделения уравнение на z^2, получим

$$\left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1$$

Эта задача сводится к нахождению решения в рациональных X и Y, где $X=\frac{x}{z}$, $Y=\frac{y}{z}$, т.е. $X^2+Y^2=1$

$Y^2=1-X^2=(1-X)(1+X)$

$(1+X)^2$

Поделив его на , получим $\left(\frac{Y}{1+X}\right)^2=\frac{1-X}{1+X}$

Теперь если заменить $\left(\frac{Y}{1+X}\right)^2=t$, то ,то X и Y будут рациональными функциями от t: $X=\frac{1-t^2}{1+t^2}$, $Y=\frac{2t}{1+t^2}$

О решении неопределенных уравнений.

Диофантовым уравнением называется алгебраическое уравнение с двумя или более неизвестными с целыми коэффициентами, решение которых ищется в целых или рациональных числах.

Например, уравнение имеет решение $x=7, y=4$; вообще же его решениями служат целые числа вида $x=7+5n, \quad y=4+3n$.

В настоящее время сведения из задач решения неопределенных уравнений формулируется так: пусть дано m многочленов от n переменных, $m<n, \quad f_1(x_1,x_2,\dots,x_n),\dots,f_m(x_1,x_2,\dots,x_n)$ с коэффициентами из некоторого поля K. требуется найти множество $M(K)$ всех рациональных решений системы

$$\begin{cases} f_1(x_1,x_2,\dots,x_n)=0 \\ \dots\dots\dots\dots\dots\dots\dots \\ f_m(x_1,x_2,\dots,x_n)=0 \end{cases} \qquad (1)$$

и определить его алгебраическую структуру. При этом решение $(x_1^{(0)}, \ldots, x_n^{(0)})$ называется рациональным, если все $x_i^{(0)} \in K$.

Множество $M(K)$, разумеется, зависит от поля K . Так, уравнение $x^2 + y^2 = 3$ не имеет ни одного рационального решения в поле Q рациональных чисел, но имеет бесконечно много решений в поле $Q(\sqrt{3})$, т.е. в множестве чисел вида $a + b\sqrt{3}$, где a и $b -$ рациональные числа.

Наиболее важным для теории чисел являются случаи когда 1) $K = Q$, где $Q -$ поле рациональных чисел, или 2) K есть поле вычетов по простому модулю p .

Диофант рассматривал первый из этих случаев. В дальнейшем будем всегда считать, что $K = Q$. Ограничимся рассмотрением только этих задач Диофанта, которые сводятся к одному уравнению с двумя неизвестными, т.е. к случаю $m = 1, \quad n = 2$;

$$f(x, y) = 0 \ .$$

Это уравнение определяет на плоскости R^2 алгебраическую кривую Γ . Рациональное решение (2) будем называть рациональной точкой кривой Γ . В дальнейшем нередко будем прибегать к языку геометрии, хотя Диофант нигде его не применяет. Однако геометрический язык стал в настоящее время столь неотъемлемой частью математического мышления, что многие факты будет легче понять и объяснить с его помощью.

Прежде всего необходимо дать какую-нибудь классификацию уравнений (2) или, что то же, алгебраических кривых. Наиболее естественной и ранее всего возникшей является классификация их по порядкам. Порядком кривой (2) называется максимальный порядок членов многочлена $f(x, y)$, где под порядком членов понимается сумма степеней при x и y .

Геометрический смысл этого понятия в том, что прямая пересекается с кривой порядка n ровно в n точках. При подсчете точек надо, разумеется, учитывать кратность точек пересечении, и также комплексные и «бесконечно удаленные» (см. далее) точки. Так, например, окружность $x^2+y^2=1$ и прямая $x+y=2$ пересекаются в двух комплексных точках, а гипербола $x^2-y^2=1$ и прямая $y=x-$ в двух бесконечно удаленных точках, та же гипербола с прямой $x=1$ имеет одну общую точку кратности 2.

Однако, для целей диофантова анализа (такое название получила область математики, выросшая из задач решения неопределенных уравнений; впрочем, теперь ее чаще называют диофантовой геометрией) классификация по порядкам оказалась слишком грубой.

Например, пусть дана окружность (см. рис.1.) с: $x^2+y^2=1$ и любая прямая с рациональными коэффициентами, например, $L:\ y=0$. Покажем, что рациональные точки этой окружности и прямой можно поставить во взаимно однозначное соответствие.

Это можно сделать, например, так: закрепим точку $A(0,-1)$ окружности и поставим в соответствие каждой рациональной точке B прямой L точку B_1 окружности C, лежащую на пересечении C и прямой AB. То, что координаты точки B' будут рациональными, предоставим аналогичное доказательство у Диофанта.

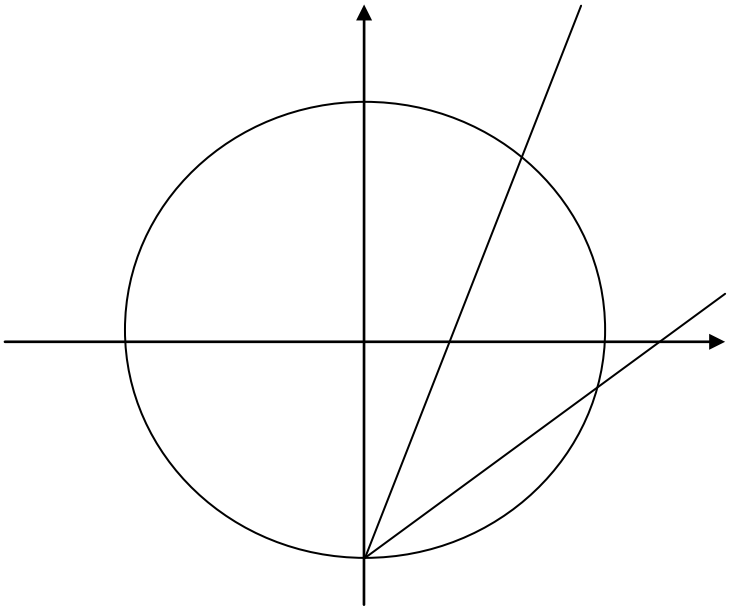

Рис.1.

Очевидно, что такое же соответствие можно установить между рациональными точками любого канонического сечения, если на нем лежит хотя бы одна рациональная точка, и рациональной прямой.

Мы видим, что с точки зрения диофанотова анализа окружность C и прямая L неотличимы; множества их рациональных решений эквивалентны. И это несмотря на то, что порядки обоих кривых различны.

Более тонкой является классификация алгебраических кривых по родам, которая была введена только в XIX веке Абелем и Риманом. Эта классификация учитывает число особых точек кривой Γ.

Будем считать, что в уравнении (2) кривой Γ многочлен $f(x,y)$ неприводим над полем рациональных чисел, т.е. он не раскладывается в произведение многочленов с рациональными коэффициентами. Как известно, уравнение касательной к кривой Γ в точке $P(x_0,y_0)$ будет

$$Y - y_0 = k(x - x_0),$$

где

$$k = \frac{f_x'(x_0, y_0)}{f_y'(x_0, y_0)}.$$

Если в точке P производная f_x' или f_y' отлична от нуля, то угловой коэффициент k касательной имеет вполне определенное значение (если $f_x'(x_0, y_0) \neq 0$, а $f_y'(x_0, y_0) = 0$, то $k = \infty$ и касательная в P будет вертикальной).

Если в точке P обе частные производные обращаются в нуль,

$$f_x'(x_0, y_0) = 0 \text{ , и } f_y'(x_0, y_0) = 0 \text{ ,}$$

то точка P называется особой.

Например, у кривой $y^2 = x^2 + x^3$ точка $(0,0)$ будет особой, т.к. в ней $f_x' = -2x - 3x^2$ и $f_y' = 2y$ обращаются в нуль.

Наиболее простым из диофантовых уравнений является неопределенное уравнение первой степени с двумя неизвестными, имеющий вид

$ax + by = c$, где a, b и $c -$ заданные целые числа.

Если $(a, b) = 1$, то уравнение имеет целые решения, которые в общем виде записываются так :

$$x = x_1 + bt \qquad y = y_1 - at$$

или при отрицательном b удобно брать:

$$x = x_1 - bt \qquad y = y_1 + at$$

В этих формулах решения x_1 и y_1-пара частных целых значений x и y, удовлетворяющих уравнению, и $t -$ произвольное целое число.

Если $(a,b)=d>1$ и c не делится на $d.$ то уравнение не имеет решений в целых числах.

В теории неопределенных уравнений первой степени известны несколько способов отыскания пары частных значений неизвестных, удовлетворяющих уравнению.

При помощи сравнений, например, эта пара частных значений находится так: исходя из уравнения $ax+by=c$, записывается сравнение $ax\equiv c(mod\ b)$, где b берется со знаком плюс, значение x , удовлетворяющее сравнению,

берется в качестве x_1, а значение обычно находится непосредственно после подстановки в него найденного значения x_1.

§III.2. Методы геометрии чисел для решения диофантовых уравнений

Теорема Лагранжа о четырех квадратах.

Теорема: Всякое натуральное m может быть представлено в виде суммы четырех квадратов целых чисел

$$m=u_1^2+u_2^2+u_3^2+u_4^2 \qquad (*)$$

Ясно, что достаточно доказать существование представления (*) лишь для бесквадратных чисел.

Воспользуемся следующей леммой для доказательства теоремы:

Лемма: Для любого простого p найдутся такие целые a_p и b_p такие, что

$a_p^2 + b_p^2 + 1 \equiv 0 (mod\ p)$

Доказательство: Если $p = 2$, то $a_p = 1$, $b_p = 0$.

Пусть p простое нечетное число. Очевидно, что числа

(1)

попарно не сравнимы между собой по модулю p . Отсюда вытекает, что и числа

$$-1, -1^2 - 1, -1 - 2^2, -1 - \left(\frac{p-1}{2}\right)^2 \qquad (2)$$

так же попарно не сравнимы между собой по модулю p .

Суммарное количество чисел, принадлежащих этим двум последовательностям равно $p + 1$, что превышает общее количество классов вычетов по модулю p . Значит, среди них, взятых в совокупности , есть по меньшей мере два числа, сравнимые между собой по модулю p .

Значит, при некоторых a_p и b_p

$$a_p^2 \equiv -1 - b_p^2 (mod\ p). \qquad (3)$$

что и требуется установить.

Пусть $m = p_1 p_2 \dots p_g$ где $p_i, i = 1,2, \dots, g$ различные простые числа.

Рассмотрим решетку целых точек $\bar{U} = (U_1, U_2, U_3, U_4)$ координаты которых удовлетворяют сравнений

$U_1 \equiv a_{p_i} U_3 + b_{p_i} U_4 (mod\ p_i)$

$$U_2 \equiv a_{p_i} U_3 - b_{p_i} U_4 (mod\ p_i) \qquad (4)$$

$i = 1,2, \ldots, g$.Эти точки образуют решетку, объем основного параллелепипеда которой d(Λ) подчинен оценке

$$d(\Lambda) \le p_1^2 p_2^2 \ldots p_g^2$$

Введем в рассмотрение четырехмерный шар

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 < 2m$$

Его объем равен

И эти неравенства очевидны

Значит по теореме Минковского о выпуклом теле найдется решение системы сравнений (*), отличное от нулевого решения (0, 0, 0, 0) такое, что

(5)

Но в силу (3) и (4)

$$U_1^2 + U_2^2 + U_3^2 + U_4^2 \equiv \left(a_{p_i}^2 + b_{p_i}^2 + 1\right) U_3^2 + \left(a_{p_i}^2 + b_{p_i}^2 + 1\right) U_4^2 \equiv 0 (mod\ p_i),$$

$i = 1,2, \ldots, g$

Отсюда следует, что

$$u_1^2 + u_2^2 + u_3^2 + u_4^2 \equiv 0 (mod\ m).$$

Это сравнение вместе с неравенством (5) и доказывает , что

$$m = u_1^2 + u_2^2 + u_3^2 + u_4^2$$

Представление числа в виде суммы трех квадратов

Вопрос о том, каким условиям должно удовлетворять натуральное число n, для того, чтобы его возможно было представить в виде суммы трех квадратов целых чисел, был решен Гауссом, который установил следующий результат.

Теорема. Натуральное число n представимо в виде суммы трех квадратов целых чисел тогда и только тогда, когда оно не имеет вид

(1)

где k и l целые неотрицательные числа.

Доказательство. Необходимость.

Предположим, что существует такое натуральное число вида с $l \geq 0$ и $k \geq 0,$ которое является суммой трех квадратов. Пусть n наименьшее число такого вида:

$n = a^2 + b^2 + c^2.$

Если среди чисел a, b, c есть хотя бы одно нечетное , тогда сумма

$a^2 + b^2 + c^2$ имеет вид , что не согласуется с предполагаемой формой числа n. Если среди чисел a, b, c два нечетны, а третье четное, то $a^2 + b^2 + c^2$ имеет вид – опять не подходит. Если все числа a, b, c нечетны, то их сумма имеет вид , а это противоречит предположению. Итак, все a, b, c должны быть четными

$a = 2a_1, \quad b = 2b_1, \quad c = 2c_1,$

где $a_1 \cdot b_1 \cdot c_1$ некоторые целые числа.

Значит $\frac{n}{4} = 4^{b-1}(8k+7) = a_1^2 + b_1^2 + c_1^2.$

Но это противоречит предположению, что n наименьшее число вида (1) , представимо в виде суммы трех квадратов.

Достаточность. Итак, n не имеет вида . Докажем, что n представляется в виде суммы трех квадратов целых чисел. Всякое натуральное число n можно записать в виде $n = n' n^{(\llbracket' \rrbracket^2}$.

где n' - бесквадратное число, называющееся бесквадратной частью числа n . Очевидно, что если n' представляется в виде суммы трех квадратов, то и n представляется в таком виде. С другой стороны, если n не имеет вида , то и n' не имеет вида .

В самом деле, предположим, что

$$n' = 4^l(8k+7)$$

Так как n' бесквадратное число, то $l' = 0$. т.е.

$$n' = 8k' + 7 \ .$$

Пусть $n'' = 2^{l''}(4k''+1)$, тогда $n^{(\llbracket' \rrbracket^2} = 4^{l''}(8k''+1)$

и значит , $n = n^{n^{(\llbracket' \rrbracket^2}} = 4^l(8k+7)$ в противоречие с предположением.

Итак, можно предположить, что n бесквадратное число и

$n \not\equiv 7(mod\ 8)$

1) Сначала докажем теорему для случая $n \equiv 3(mod\ 8)$:

Пусть каноническое разложение числа n имеет вид

$$n = p_1 p_2 \dots p_r \ ,$$

где $p_1, p_2, \dots, p_r$ различные простые числа.

По каждому из модулей $p_j, j = 1,2, \dots, r$. возьмем какой либо класс вычетов b_j такой, что

$$\left(\frac{b_j}{p_j}\right) = +1$$

Так как $(p_j, 2) = 1$, то существуют числа a_j $(j = 1,2, \dots, r)$. которые удовлетворяют сравнению

$$b_j \equiv -2a_j \pmod{P_j}, \qquad j = 1,2, \dots, r.$$

Заметим, что $(a_j, p_j) = 1$. Поскольку числа $p_1 p_2 \dots p_r$ попарно взаимнопростые, то найдется такой класс вычетов A по модулю ,что

$$A \equiv 1 \pmod 4$$

$$A \equiv a_j \pmod{p_j}$$

$(j = 1,2, \dots, r)$.

Так как $(a_j, p_j) = 1$, то $(A, 4n) = 1$

Обратимся к следующей классической теореме Дирихле:

Теорема: Пусть A и B взаимно простые натуральные числа. В арифметической прогрессии

$$Bx + A, x = 0, 1, 2, \dots$$

содержится бесконечное количество простых чисел.

Возьмем простое число q, принадлежащее прогрессии

$$q = 4nx + A$$

Тогда

$$q \equiv 1 \pmod 4$$

и $$q \equiv a_j (mod\ p_j), j = 1, 2, 3, \ldots, r.$$

и тем самым $$-2q \equiv b_j (mod\ p_j), j = 1, 2, 3, \ldots, r.$$

Мы доказали, что существует простое число q ,которое обладает следующими свойствами

$$q \equiv 1 (mod\ 4) \quad (1)$$

И $$\left(\frac{-2q}{p_j}\right) = 1, j = 1, 2, 3, \ldots, r \quad (2)$$

Из свойства (2) мы получаем

$$1 = \prod_{j=1}^{r}\left(\frac{-2q}{p_j}\right)\prod_{j=1}^{r}\left(\frac{-2}{p_j}\right)\left(\frac{q}{p_j}\right) = \left(\frac{-2}{n}\right)\prod_{j=1}^{r}\left(\frac{q}{p_j}\right)$$

Так как $q \equiv 1 (mod\ 4)$, то по закону взаимности мы заключаем

$$\left(\frac{q}{p_j}\right) = \left(\frac{p_j}{q}\right)$$

Далее,

Так как

$n \equiv 3 (mod\ 8)$, то $\left(\frac{-2}{n}\right) = 1$

и значит,

Так как

$q \equiv 1 (mod\ 4)$, то $\left(\frac{-1}{q}\right) = 1$.

то $\left(\frac{-n}{q}\right) = 1$

и мы получаем $\left(\frac{-n}{q}\right) = 1$.

Согласно определению символа Лежандра $\left(\frac{-n}{q}\right)$ существует решение b сравнения

$$b \equiv -n (mod\ q). \qquad (4)$$

Мы можем предполагать, что b есть число нечетное: если мы встретимся с четным b ,то нечетное число $b+q$ также удовлетворяет сравнению (4). Сравнение (4) запишем в виде равенства

$$b^2 - qh_1 = -n \qquad (4`)$$

Рассматривая это равенство по модулю 4, мы получаем в силу условия

$$n \equiv 3 (mod\ 4)$$

$$1 - h_1 \equiv 1 (mod\ 4),$$

откуда следует, что , т.е $h_1 = 4h$

где h целое число. Значит,

$$b^2 - 4qh = -n \qquad (4``)$$

Вернемся к свойству (2). На основании общей теоремы элементарной теории чисел , т.к сравнения

$x^2 \equiv -2q \left(mod\ p_j\right)$, $j = 1,2,,\ldots,r.$

разрешимы, то разрешимо и сравнение

$$x^2 \equiv -2q(mod\ n).$$

Так как q и n взаимно просты, то и x взаимно просто с n .Обозначим через t решение сравнения

$$tx \equiv 1(mod\ n)$$

Мы видим, что разрешимо сравнение

$$t^2 \equiv \frac{-1}{2q}(mod\ n) \qquad (5)$$

Где число $\frac{-1}{2q} = z$ обозначает решение сравнения

$$-2qz \equiv 1(mod\ n).$$

Перейдем к теоремам о решении неравенств в целых числах.

В трехмерном евклидовом пространстве , координаты которого будем обозначать символом R,S,T рассмотрим открытый шар с центром в начале координат (т.е в точке, у которой $R = S = T = 0$) радиуса $\sqrt{2n}$:

$$R^2 + S^2 + T^2 < 2n \qquad (6)$$

Объем шара (6) равен

Далее рассмотрим решету

$$R = 2tq + tby + nz$$

$$S = \sqrt{2q}x + \frac{b}{\sqrt{2q}} \qquad (7)$$

$$T = \frac{\sqrt{n}}{2q} y \quad .$$

Здесь x , y , z пробегают всевозможные числа. Объем основного параллелепипеда решетки, равный абсолютной величине определителя системы линейных форм (7). Легко видеть, что этот объем равен $n^{3/2}$.

Шар (6) выпуклое, центрально симметричное тело с центром в точке $R = 0, \quad S = 0, T = 0.$

Поскольку

то между объемом шара (6) и объемом основного параллелепипеда решетки (7) имеет неравенство

По теореме Минковского о выпуклом теле найдутся три целых числа $x_1\ y_1\ z_1$ по крайней мере одно из которых не равно нулю, такое, что соответствующие им из формулам (7) числа $R_1.S_1.T_1$ удовлетворяют неравенствам

$$R_1^2 + S_1^2 + T_1^2 < 2n$$

Из формул (7) видно, что R_1 есть целое число. Далее,

$$R_1^2 + S_1^2 + T_1^2 = R_1^2 + \left(\sqrt{2q}x_1 + \frac{b}{\sqrt{2q}}y_1\right)^2 + \left(\frac{\sqrt{n}}{2q}y_1\right)^2 = R_1^2 + \frac{1}{2q}(2qx_1 + by_1)^2 + \frac{n}{2q}y_1^2 = R_1^2 + 2(qx$$

(8)

Таким образом, $R_1^2 + S_1^2 + T_1^2$ есть целое число.

Далее,

$$R_1^2 + S_1^2 + T_1^2 = (2tx_1 + tby_1 + nz_1)^2 + \left(\sqrt{2q}x_1 + \frac{b}{\sqrt{2q}}y_1\right)^2 + \left(\frac{\sqrt{n}}{2q}y_1\right)^2.$$

откуда следует, что

$$R_1^2 + S_1^2 + T_1^2 \equiv t^2(2qx_1 + by_1)^2 + \frac{1}{2q}(2qx_1 + by_1)^2 (mod\ n)$$

в силу сравнения (5)

$$R_1^2 + S_1^2 + T_1^2 \equiv 0 (mod\ n) \qquad (9)$$

Обозначим

$$v = qx_1^2 + bx_1y_1 + ky_1^2 \qquad (10)$$

Из формул (8) видно, что v целое положительное число, $v = \frac{S_1^2 + T_1}{2}$

Из сравнения (9) вытекает, что

$$[n \mid (R]_1^2 + 2v\ )$$

Из неравенства (6) следует, что

$$R_1^2 + 2v < 2n.$$

Далее,

$$R_1^2 + 2v = R_1^2 + S_1^2 + T_1^2 > 0\ .$$

ибо $R_1.S_1.T_1$ определяются через ненулевую систему значений $x_1\ y_1\ z_1$ с помощью невырожденного преобразования (7) . Итак,

и $n \mid (R_1 1^1 2 + 2v).$

Значит

$$n = R_1^2 + 2v \qquad (11)$$

Докажем теперь, что если нечетный простой делитель p числа v входит в каноническое разложение числа v в четной степени, то тогда обязательно

$p \equiv 1 (mod\ 4)$

Итак, пусть $P^{2s+1} \| v$, то есть $P^{2s+1} | v$, но $p^{2s+2} \nmid v$.

Если p не делит n ,то так как $p | (R_1 1^{\dagger} 2 - n)$, то $\left(\frac{n}{p}\right) = 1$ (12).

Из формул (10) и (4``) имеем

(13)

Пусть $p = q$ тогда из формулы (4``) получаем $\left(\frac{-n}{p}\right) = 1$.

Если $p \neq q$, то тогда по формуле (13)

$p^{2s+1} \downarrow\downarrow (l^2 + ny_1^2)$, где $l = 2qx_1 + by_1$.

Пусть $p^{\dagger}\lambda | y \downarrow 1$. Если $s < \lambda$, то мы пришли к противоречию

$$p \| \left(\frac{l}{p^s}\right)^2 + n\left(\frac{p^\alpha}{p^s}\right)^2 \left(\frac{y_1}{p^\alpha}\right)^2.$$

Значит $s \geq \alpha$. Но тогда

$$n\left(\frac{y_1}{p^\alpha}\right)^2 + \left(\frac{l}{p^s}\right)^2 \equiv 0 (mod\ p)$$

и в силу $\left(\frac{y_1}{p^\alpha}, p\right) = 1$ и $(n, p) = 1$ мы видим, что разрешимо сравнение

$$N^2 + n \equiv 0 (mod\ p)$$

то есть $\left(\frac{-n}{p}\right)=1$.Итак, в случае $p \nmid n$ - $\left(\frac{-n}{p}\right)=1$ что вместе с формулой (12) дает, что $\left(\frac{-1}{p}\right)=1$ или

$p \equiv 1(mod\ 4)$.

Пусть теперь $p|v$ и $p|n$ тогда по формуле (11) $p|R_1 1$ и по формуле (13) $p|(2qx_1 1 + by_1 1)$.

Формулы (11) и (13) дают

$$R_1^2 + \frac{1}{2q}\left((2qx_1 + by_1)^2 + ny_1^2\right) = n \qquad (14)$$

Поскольку n бесквадратное число, то деля обе части последнего равенства на p , получим

или $y_1^2 \equiv 2q(mod\ p)$, то есть , что в сочетании с (12) дает $\left(\frac{-1}{p}\right)=1$, то есть снова

$$p \equiv 1(mod\ 4)\ .$$

Таким образом, мы доказали, что всякое нечетное простое число, входящее в v , обязательно имеет вид . Таким же свойством обладает и число . Но это свойство является необходимым и достаточным условием для того, чтобы число представлялось в виде суммы двух квадратов целых чисел. Значит,

И в сочетании с формулой (11) получаем

$$n = R_1^2 + x^2 + y^2\ .$$

Теорема доказана для случая, когда $n \equiv 3(mod\ 8)$.

2) Разберем теперь случай, когда

$$n \equiv 1 (mod\ 8)\ ,\ n \equiv 5 (mod\ 8)\ , n \equiv 2 (mod\ 8)\ , n \equiv 6 (mod\ 8)$$

Первые два случая будем называть нечетными, а два последних четными. В случае четном число n четно, положим $n = 2n^{'}$, здесь число $n^{'}$, в силу предположения о бесквадратности n , уже нечетно.

На основании теоремы Дирихле об арифметической прогрессии можно построить простое число q такое, что для всех простых нечетных делителей $p_1, p_2, \dots, p_r$ числа n выполняются соотношения

$$\left(\frac{-q}{p_j}\right) = +1, \qquad j = 1, 2, 3, \dots, r$$

и кроме того

когда $n = 1 (mod\ 8)$ $q \equiv 1 (mod\ 4)$

когда $q \equiv 1 (mod\ 4)$

когда $n = 2 (mod\ 8)$ $q \equiv 1 (mod\ 8)$

и тем самым $\left(\frac{-2}{q}\right) = (-1)^{\frac{n^2-1}{2}}$

когда $n = 6 (mod\ 8)$ $q \equiv 5 (mod\ 8)$

и тем самым .

Мы имеем в нечетных случаях

$$1 = \left(\frac{pq}{n}\right) = \left(\frac{n}{p}\right) = \left(\frac{p}{n}\right) = \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = \left(\frac{q}{n}\right) .$$

А в четных случаях

отсюда следует

Таким образом, сравнение

$b^2 \equiv -n(mod\ q)$

в обоих случаях имеет решение, положим

$$b^2 + n = -qh\ .$$

Далее, как в случае 1) мы убеждаемся в том, что существует t, удовлетворяющее сравнениям

$t^2 \equiv -\frac{1}{q}(mod\ p_j), j = 1, 2, 3 \ldots\ldots, r$

можно предположить t нечетным, или четное t можно заменить на число

$t + p_1, p_2, \ldots, p_r.$

Рассматривают точечную решетку

$R = tqx + tby + nz$

$S = \sqrt{q}x + \frac{b}{\sqrt{q}}y$

$T = \frac{\sqrt{n}}{q}y,$

и шар $R^2 + S^2 + T^2 < 2n\ .$

Применение леммы Минковского о выпуклом теле позволяет провести и в случаях $n \equiv 1,5,2,6 (mod\ 8)$ те же рассуждения, что и в случае $n \equiv 3 (mod\ 8)$ и тем самым доказать теорему в полном объеме.

Числа вида

$\frac{n(n+1)}{2}$ называют иногда треугольными, ибо такими числами выражается количество точек в треугольных кучках.

Следствие. Всякое натуральное число есть сумма не более трех треугольных чисел.

В самом деле, всякое натуральное число формы есть сумма трех квадратов, которые очевидным образом, являются нечетными числами

,

где a, b, c неотрицательные числа.

Следовательно,

$$k = \frac{a(a+1)}{2} + \frac{b(b+1)}{2} + \frac{c(c+1)}{2} = t_a + t_b + t_c$$

что и требовалось доказать

Решение диофантовых уравнений с двумя неизвестными.

1) Если 2 числа представимы в виде $n_1 = x_1^2 + dy_1^2$, $n_2 = x_2^2 + dy_2^2$, тогда и произведение их представимо в виде

$$n = x^2 + dy^2$$

Доказательство:

$$n_1 n_2 = (x_1^2 + dy_1^2)(x_2^2 + dy_2^2) = (x_1 x_2)^2 + dy_1^2 x_2^2 + dx_1^2 y_2^2 + d^2 (y_1 y_2)^2 = (x_1 x_2 + dy_1 y_2)^2 - 2dx_$$

.

2) Пусть $\left(-\frac{m}{p}\right)=1$, тогда при любом простом нечетном p и $m=1,2,3,7$ уравнение $x^2+my^2=p$ разрешимо в целых числах.

Доказательство:

Рассмотрим решетку вида $R^2 \ni \Lambda:\begin{pmatrix}\sqrt[2]{m} & 0\\ z & p\end{pmatrix}\begin{pmatrix}x\\ y\end{pmatrix}=\left\{\begin{pmatrix}\sqrt[2]{m}\,x\\ zx+py\end{pmatrix}\right\}$

Запишем квадратичную форму

$$f(\Lambda)=mx^2+z^2x^2+p^2y^2+2zxpy=x^2(m+z)+p^2y^2+2zxpy=KA$$

По условию теоремы нам известно, что $z^2+m\equiv 0(mod\ p),\Rightarrow f(\Lambda)$ всегда делится на p .

Мы имеем $d(\Lambda)=\sqrt[2]{m}\,p,\Rightarrow$ по теореме Минковского при $m=1,2$ в круге

$$S:\left\{\begin{pmatrix}y_1\\ y_2\end{pmatrix}/_{y_1^2+y_2^2<2p}\right\}$$

площади $V(S)=2\pi p>4\sqrt[2]{m}\,p$ найдется такая точка

$\Lambda\ni\left(zx_0^{\sqrt[2]{m}x_0}+py_0\right)$,отличная от начала, что

$$mx_0^2+(zx_0+py_0)^2<2p,\Rightarrow\ mx_0^2+(zx_0+py_0)^2=p$$

При $m=3,7$ в круге

$$S:\left\{\begin{pmatrix}y_1\\ y_2\end{pmatrix}/_{y_1^2+y_2^2<4p}\right\}$$

площади $V(S)=4\pi p>4\sqrt[2]{m}\,p$ найдется такая точка

$\Lambda\ni\left(\begin{pmatrix}\sqrt[2]{m} & x_0\\ z & y_0\end{pmatrix}+py_0\right)$, отличная от начала, что

$mx_0^2+(zx_0+py_0)^2<4p$.

Рассмотрим случай для $m = 3$:

1) $3x_0^2 + (zx_0 + py_0)^2 = p$,т.к делится на p и .

2) $3x_0^2 + (zx_0 + py_0)^2 = 2p$

при x_0 четном

$3x_0^2 \equiv 0(mod\ 4)$, $(zx_0 + py_0) \equiv 0(mod\ 4)$,

а при x_0 нечетном

$x_0^2 \equiv 1(mod\ 4)$, $3 \equiv -1(mod\ 4), \Rightarrow\ 3x_0^2 \equiv -1(mod\ 4)$

$(zx_0 + py_0)^2 \equiv 1(mod\ 4) \Rightarrow$,$3x_0^2 + (zx_0 + py_0)^2 \equiv 0(mod\ 4)$, что невозможно при условии $mx_0^2 + (zx_0 + py_0)^2 < 4p.$

3) $3x_0^2 + (zx_0 + py_0)^2 = 3p$

Разделив обе части на 3, получим

$x_0^2 + \frac{1}{3(zx_0 + py_0)}^2 = p$, такое же, как в первом случае.

Теперь рассмотрим случай при m=7:

$7x_0^2 + (zx_0 + py_0)^2 = p$

1) т.к $f(1)$ делится на p .

$7x_0^2 + (zx_0 + py_0)^2 = 2p$

2) здесь также как при $m = 3$.

3) $7x_0^2 + (zx_0 + py_0)^2 = 3p$ левая часть не делится на 3, следовательно уравнение $x^2 + my^2 = p$ разрешимо в целых числах.

§3. Приложение изученной теории к решению задач

1) Решить неопределенное уравнение

$x^2 - 21x + 110 = 13y$

Рассмотрим сравнение

$x^2 - 21x + 110 \equiv 0(mod\ 13)$ или приведем его к виду

$$x^2 - 8x + 6 \equiv 0(mod\ 13)$$

$x^2 - 8x + 16 \equiv 10(mod\ 13)$

$x^2 - 8x + 16 \equiv 36(mod\ 13)$

$(x-4)^2 \equiv 36(mod\ 13)$

Откуда $x - 4 = \mp 6 + 13t$, т.е

$x_1 = 10 + 13t$

$x_2 = 11 + 13t$

Подставив x_1, x_2 в уравнение получим

$y_1 = 13t^2 - t$

$y_2 = 13t^2 + t$

Решением уравнения будут системы

$$\begin{cases} x_1 = 10 + 13t \\ y_1 = 13t^2 - t \end{cases}$$

$$\begin{cases} x_2 = 11 + 13t \\ y_2 = 13t^2 + t \end{cases}$$

2) Доказать, что уравнение неразрешимо в целых числах.

Рассмотрим сравнение или $5x^2 \equiv 7 (mod\ 11)$

или также $5x^2 \equiv 40 (mod\ 11)$

Сократив на 5 сравнение, т.к (5,11)=1, 5 и 11 взаимнопростые, получим

$x^2 \equiv 8 (mod\ 11)$

Проверяя вычеты по модулю 11, можем убедиться, что все значения x являются квадратичными невычетами 8 по модулю 11, следовательно уравнение неразрешимо в целых числах.

3) Решить в целых числах уравнение

$$4x - 9y + 13z = 7$$

Разделив с остатком -9 на 4, получим -9=4(-3)+3.

Представим исходное уравнение в виде

После замены $x' = x - 3y$ это уравнение запишется в виде

Теперь , учитывая , что $13 = 3 \cdot 4 + 1$, преобразуем уравнение

Заменим $y + 4z = y'$ и запишем

Из этого уравнения получим решения

$z = 7 - 4x' - 3y', \Rightarrow$

$$y = 16x' + 13y' - 28, \Rightarrow$$

$x = 49x' + 39y' - 84,$

где x' и y' – произвольные целые числа.

4) Решить в рациональных числах уравнение

Решение:

Свободный член уравнения имеет следующие делители:

$\pm 1, \pm 3, \pm 7, \pm 21$

Выпишем также положительные делители старшего коэффициента:

$1, 2$

Следовательно, для рационального корня уравнения получаем следующие возможные значения:

$\pm 1, \pm 3, \pm 7, \pm 21, \pm {}^{1}/_{2}, \pm {}^{3}/_{2}, \pm {}^{7}/_{2}, \pm {}^{21}/_{2}$

Подстановкой в исходное уравнение этих чисел убеждаемся, что у этого множества только -3 и ${}^{1}/_{2}$ являются корнями уравнения. Так как -3 целое

число, то уравнение

разрешимо в целых числах.

ЗАКЛЮЧЕНИЕ

Рассмотрение диофантовых уравнений частного вида с целыми и рациональными решениями – наиболее важная часть данной работы. Все рассматриваемые уравнения являются классическими и каждое из них играло важную роль в историческом развитии этой области теории чисел.

Самостоятельная часть работы посвящена решению диофантовых уравнений. На основании изученной теории решены следующие задачи:

1) Решено неопределенное уравнение

$$x^2 - 21x + 110 = 13y$$

Решением уравнения будут системы

$$\begin{cases} x_1 = 10 + 13t \\ y_1 = 13t^2 - t \end{cases}$$

$$\begin{cases} x_2 = 11 + 13t \\ y_2 = 13t^2 + t \end{cases}$$

2) Доказано, что уравнение неразрешимо в целых числах.

3) Решить в целых числах уравнение

$$4x - 9y + 13z = 7$$

Для этого уравнения получим решения

$$z = 7 - 4x' - 3y', \Rightarrow$$

$$y = 16x' + 13y' - 28, \Rightarrow$$

$$x = 49x' + 39y' - 84,$$

где x' и y' – произвольные целые числа.

4) Решено в рациональных числах уравнение

Решением уравнения является целое число -3 .

Одним из центральных в теории диофантовых уравнений является вопрос о том, когда число решений конечно, и о нахождении в этом случае эффективной границы для координат решений. Вопрос об эффективности удалось решить лишь для частного вида. Поэтому всякое представление решения диофантовых уравнений эффективно имеет научное значение.

Список использованной литературы

1. И. А Каримов. Мировой финансовый кризис; пути и меры по его преодолению в условиях Узбекистана. Ташкент, 2009.
2. Г. Дэвенпорт. Высшая арифметика. Введение в теорию чисел. «Наука» Москва.1965 г.
3. З. И. Боревич, И. Р. Шафаревич. Теория чисел. Высшая математика онлайн, vmate.ru, 2012.
4. А. А. Бухштаб. Теория чисел. Высшая математика онлайн, vmate.ru, 2012.
5. И. М. Виноградов. Основы теории чисел. Москва 1965г.
6. Дж. В. С. Касселс. Введение в геометрию чисел. Москва.1965г.
7. Дж. В. С. Касселс. Введение в теорию диофантовых приближений. Москва. 1961г.
8. С. Ленг. Введение в теорию диофантовых приближений. Москва. 1970 г.

9. Интернет-сайт: www.mathnet.ru
10. Интернет-сайт : wwww.exponenta.ru