ЧЕБЫШЕВСКИЙ СБОРНИК
Том 17 Выпуск 3

УДК 517.36

ОТ ДИОФАНТОВЫХ ПРИБЛИЖЕНИЙ ДО ДИОФАНТОВЫХ УРАВНЕНИЙ

А. Д. Брюно (г. Москва)

Аннотация

Пусть в вещественном n-мерном пространстве $\mathbb{R}^n = \{X\}$ задано m однородных вещественных форм $f_i(X)$, $i = 1, \dots, m$, $2 \leqslant m \leqslant n$. Выпуклая оболочка множества значений $G(X) = (|f_1(X)|, \dots, |f_m(X)|) \in \mathbb{R}^m_+$ для целочисленных $X \in \mathbb{Z}^n$ во многих случаях является выпуклым многогранным множеством, граница которого для $||X|| < \text{const}$ вычисляется с помощью стандартной программы. Точки $X \in \mathbb{Z}^n$, для которых значения $G(X)$ лежат на этой границе, названы граничными. Они являются наилучшими диофантовыми приближениями для корневых множеств указанных форм. Их вычисление даёт глобальное обобщение цепной дроби. Для $n = 3$ обобщить цепную дробь безуспешно пытались Эйлер, Якоби, Дирихле, Эрмит, Пуанкаре, Гурвиц, Клейн, Минковский, Брун, Арнольд и многие другие.

Пусть $p(\xi)$ — целый неприводимый в $\mathbb{Q}$ многочлен степени n и λ — его корень. Набор основных единиц кольца $\mathbb{Z}[\lambda]$ можно вычислить по граничным точкам некоторой совокупности линейных и квадратичных форм, построенных по корням многочлена $p(\xi)$. До сих пор эти единицы вычислялись только для $n = 2$ (с помощью обычных цепных дробей) и $n = 3$ (с помощью алгоритмов Вороного). Каждая единица определяет автоморфизм граничных точек в $\mathbb{R}^n$ и автоморфизм их образов в $\mathbb{R}^m_+$. В логарифмической проекции $\mathbb{R}^m_+$ на $\mathbb{R}^{m-1}$ можно найти фундаментальную область для группы вторых автоморфизмов, соответствующих единицам.

С помощью этих конструкций можно находить целочисленные решения диофантовых уравнений специального вида. Аналогично вычисляются все указанные объекты для других колец поля $\mathbb{Q}(\lambda)$. Приведены примеры.

Наш подход обобщает цепную дробь, позволяет вычислить наилучшие совместные приближения, основные единицы алгебраических колец поля $\mathbb{Q}(\lambda)$ и все решения некоторого класса диофантовых уравнений для любого n.

Ключевые слова: обобщение цепной дроби, диофантовы приближения, набор основных единиц, фундаментальная область, диофантово уравнение.

Библиография: 16 названий.

FROM DIOPHANTINE APPROXIMATIONS TO DIOPHANTINE EQUATIONS

A. D. Bruno (Moscow)

Abstract

Let in the real n-dimensional space $\mathbb{R}^n = \{X\}$ be given m real homogeneous forms $f_i(X)$, $i = 1, \dots, m$, $2 \leqslant m \leqslant n$. The convex hull of the set of points $G(X) = (|f_1(X)|, \dots, |f_m(X)|)$ for integer $X \in \mathbb{Z}^n$ in many cases is a convex polyhedral set. Its boundary for $||X|| < \text{const}$ can be computed by means of the standard program. The points $X \in \mathbb{Z}^n$ are called boundary points if $G(X)$ lay on the boundary. They correspond to the best Diophantine approximations X for the given forms. That gives the global generalization of the continued fraction. For $n = 3$

Euler, Jacobi, Dirichlet, Hermite, Poincaré, Hurwitz, Klein, Minkowski, Brun, Arnold and a lot of others tried to generalize the continued fraction, but without a succes.

Let $p(\xi)$ be an integer real irreducible in $\mathbb{Q}$ polynomial of the order n and λ be its root. The set of fundamental units of the ring $\mathbb{Z}[\lambda]$ can be computed using boundary points of some set of linear and quadratic forms, constructed by means of the roots of the polynomial $p(\xi)$. Similary one can compute a set of fundamental units of other rings of the field $\mathbb{Q}(\lambda)$. Up today such sets of fundamental units were computed only for $n = 2$ (using usual continued fractions) and $n = 3$ (using the Voronoi algorithms).

Our approach generalizes the continued fraction, gives the best rational simultaneous approximations, fundamental units of algebraic rings of the field $\mathbb{Q}(\lambda)$ and all solutions of a certain class of Diophantine equations for any n.

Keywords: generalization of continued fraction, Diophantine approximations, set of fundamental units, fundamental domain, Diophantine equation.

Bibliography: 16 titles.

1. Цепная дробь

Пусть α_0 и α_1 — натуральные числа. Для нахождения их наибольшего общего делителя используется алгоритм Евклида последовательного деления с остатком:

$$\alpha_0 = a_0\alpha_1 + \alpha_2, \quad \alpha_1 = a_1\alpha_2 + \alpha_3, \quad \alpha_2 = a_2\alpha_3 + \alpha_4, \dots$$

где натуральные числа $a_0, a_1, a_2, \dots$ суть неполные частные. Это алгоритм разложения числа $\alpha = \alpha_0/\alpha_1$ в правильную цепную дробь [1], и он применим к любым вещественным числам α. При этом $a_0 = [\alpha]$, где $[\alpha]$ — целая часть числа α, $a_1 = [1/(\alpha - a_0)]$, ..., т. е.

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots}}, \tag{1}$$

и

$$\begin{pmatrix}\alpha_{k+1}\\ \alpha_{k+2}\end{pmatrix} = \begin{pmatrix}0 & 1\\ 1 & -a_k\end{pmatrix}\begin{pmatrix}\alpha_k\\ \alpha_{k+1}\end{pmatrix}, \quad a_k = [\alpha_k/\alpha_{k+1}].$$

Если разложение (1) оборвать на a_k и свернуть эту оборванную цепную дробь в рациональное число p_k/q_k, то получается **подходящая дробь**, которая даёт наилучшее рациональное приближение к числу α. При этом

$$\begin{pmatrix}p_k & p_{k-1}\\ q_k & q_{k-1}\end{pmatrix} = \begin{pmatrix}p_{k-1} & p_{k-2}\\ q_{k-1} & q_{k-2}\end{pmatrix}\begin{pmatrix}a_k & 1\\ 1 & 0\end{pmatrix},$$
$$\begin{pmatrix}a_k & 1\\ 1 & 0\end{pmatrix}^{-1} = \begin{pmatrix}0 & 1\\ 1 & -a_k\end{pmatrix}, \quad \det\begin{pmatrix}p_k & p_{k-1}\\ q_k & q_{k-1}\end{pmatrix} = \pm 1,$$

т.е. векторы (α_k, α_{k+1}) и (p_k, q_k) принадлежат сопряжённым плоскостям, и пара векторов (p_k, q_k), (p_{k-1}, q_{k-1}) может служить базисом в одной из них. Лагранж [1, § 10] доказал, что для квадратичных иррациональностей α разложение в цепную дробь периодично (и обратно), то есть последовательность неполных частных $a_0, a_1, a_2, a_3, \dots$, начиная с какого-то номера состоит из повторяющегося отрезка $a_k, a_{k+1}, \dots, a_{k+t}$.

Итак, разложение числа в цепную дробь: просто; дает наилучшие рациональные приближения к числу; конечно для рационального числа; периодично для квадратичных иррациональностей [1, § 10]; устроено как для почти всех чисел [1, гл. III] для кубических иррациональностей [2]. Кроме того, оно обладает ещё рядом замечательных свойств.

2. Глобальное обобщение цепной дроби и наилучшие диофантовы приближения

Обобщить цепную дробь для векторов безуспешно пытались Эйлер, Якоби, Дирихле, Эрмит, Пуанкаре, Гурвиц, Клейн, Минковский, Брун, Арнольд и многие другие [3, 4], [5, п. 1.2]. Только пошаговые алгоритмы Вороного [6] безотказны, но сложны.

В [5, 7, 8] предложено следующее обобщение цепной дроби.

Пусть в n-мерном вещественном пространстве $\mathbb{R}^n$ с координатами $X = (x_1, \dots, x_n)$ заданы m однородных вещественных форм (т. е. многочленов от переменных) $f_1(X), \dots, f_m(X)$, $2 \leqslant \leqslant m \leqslant n$.

Модули $g_i(X) = |f_i(X)|$ форм $f_i(X)$, $i = 1, \dots, m$, задают отображение $G(X) = (g_1(X), \dots, g_m(X))$ пространства $\mathbb{R}^n$ в положительный ортант $\mathbf{S} \stackrel{\text{def}}{=} \mathbb{R}^m_+$ в m-мерном пространстве $\mathbb{R}^m$ с координатами $S = (s_1, \dots, s_m)$: $s_i = g_i(X) = |f_i(X)|$, $i = 1, \dots, m$. При этом целочисленная решётка $\mathbb{Z}^n \subset \mathbb{R}^n$ отображается в некоторое множество $\mathbf{Z} \subset \mathbf{S}$. Замыкание выпуклой оболочки $\mathbf{H}$ множества $\mathbf{Z}\backslash 0$ является выпуклым множеством. Все целочисленные точки $X \in \mathbb{Z}^n\backslash 0$, отображающиеся на границу $\partial\mathbf{H}$ множества $\mathbf{H}$, назовём **граничными**.

Задача 1. *Найти все граничные точки X.*

Решение задачи 1. В дальнейшем ограничимся случаями, когда выпуклое множество $\mathbf{H}$ является многогранным, т.е. его граница $\partial\mathbf{H}$ состоит из вершин, рёбер, граней различных размерностей и не содержит непрерывных «кривых» частей. В этих случаях граница $\partial\mathbf{H}$ вычисляется с помощью стандартных программ для вычисления выпуклых многограных оболочек [9, 10]. Это и даёт алгоритмическое обобщение цепной дроби на любую размерность. Примеры см. в [5].

В частности, это даёт возможность вычислить наилучшие совместные рациональные приближения q_1/q_0, ..., q_m/q_0 к вещественным числам $\beta_1, \dots, \beta_m$, где $q_0, q_1, \dots, q_m \in \mathbb{Z}$ и $f_i(q_0, q_i) = q_0\beta_i - q_i$, $i = 1, \dots, m$. Здесь $m = m$ и $n = m + 1$.

Пример 1. *Пусть $f_1 = x_1\alpha - x_2$, $f_2 = x_1$, где $\alpha \in \mathbb{R}$, $\alpha > 0$. Здесь $n = m = 2$. Каждой вершине ломаной $\partial\mathbf{H}$ с $x_1 = p$, $x_2 = q \in \mathbb{Z}_+$ соответствует подходящая дробь q/p цепной дроби числа α. Эта точка (x_1, x_2) является граничной. Но, вообще говоря, не каждой подходящей дроби s/r, $r, s \in \mathbb{Z}_+$ цепной дроби числа α соответствует вершина $x_1 = r$, $x_2 = s$ ломаной $\partial\mathbf{H}$.*

Гипотеза. *Если все $f_1, \dots, f_m$ суть линейные и квадратичные формы, то граница $\partial\mathbf{H}$ не имеет непрерывных кривых участков, т. е. является многогранной.*

Более того, до сих пор неизвестно ни одного набора форм $f_1, \dots, f_m$, для которого граница $\partial\mathbf{H}$ не была бы многогранной.

3. Основные единицы кольца $\mathbb{Z}[\lambda]$

Пусть дан целый неприводимый в $\mathbb{Q}$ вещественный многочлен

$$p(\xi) = \xi^n + b_1\xi^{n-1} + \dots + b_{n-1}\xi + b_n \tag{2}$$

с целыми коэффициентами b_i, т. е. он не разлагается в произведение двух нетривиальных многочленов с коэффициентами из $\mathbb{Q}$. Ему соответствует кольцо $\mathbb{Z}[\lambda]$ чисел вида

$$\xi(X) = x_1 + x_2\lambda + \dots + x_n\lambda^{n-1} \tag{3}$$

с целыми коэффициентами x_i, где λ — корень многочлена (2) и $X = (x_1, \ldots, x_n) \in \mathbb{Z}^n$. Каждому числу (3) соответствует квадратная матрица $D(\xi) = (d_{ij})$:

$$\lambda^i \xi(X) = \sum_{j=0}^{n-1} d_{ij} \lambda^j, \quad i = 0, 1, \ldots, n-1.$$

Определитель $\det D(\xi)$ называется нормой числа (3) и обозначается $N(\xi)$. Норма произведения чисел равна произведению их норм: $N(\xi_1 \cdot \xi_2) = N(\xi_1) \cdot N(\xi_2)$. Те числа (3), у которых норма $N(\xi) = \pm 1$, называются единицами [11, гл. II]. В дальнейшем предполагаем, что среди корней многочлена $p(\xi)$ нет единиц. Существует такой набор единиц $\Sigma = (\varepsilon_1, \ldots, \varepsilon_r)$, что всякая единица $\varepsilon \in \mathbb{Z}[\lambda]$ однозначно представляется в виде

$$\varepsilon = \pm \varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r}, \tag{4}$$

где a_i — целые числа. Эти единицы $\varepsilon_1, \ldots, \varepsilon_r$ называются основными.

Задача 2. *Для фиксированного многочлена* (2) *найти набор основных единиц кольца* $\mathbb{Z}[\lambda]$.

Решение задачи 2. Пусть неприводимый в $\mathbb{Q}$ многочлен (2) имеет l вещественных корней λ_1, …, λ_l и k пар комплексно сопряжённых корней λ_{l+1}, …, λ_{l+k}, $\bar{\lambda}_{l+1}$, …, $\bar{\lambda}_{l+k}$, $l + 2k = n$. Здесь $l \geqslant 0$, $k \geqslant 0$. Рассмотрим $m = k + l$ форм

$$f_i(X) = \langle L_i, X \rangle, \quad i = 1, \ldots, l,$$
$$f_{l+j}(X) = \langle K_{l+j}, X \rangle \left\langle \bar{K}_{l+j}, X \right\rangle, \quad j = 1, \ldots, k,$$

где

$$L_i = \left(1, \lambda_i, \lambda_i^2, \ldots, \lambda_i^{n-1}\right), \quad \langle L_i, X \rangle = x_1 + \lambda_i x_2 + \ldots + \lambda_i^{n-1} x_n,$$
$$K_{l+j} = \left(1, \lambda_{l+j}, \lambda_{l+j}^2, \ldots, \lambda_{l+j}^{n-1}\right), \quad \bar{K}_{l+j} = \left(1, \bar{\lambda}_{l+j}, \bar{\lambda}_{l+j}^2, \ldots, \bar{\lambda}_{l+j}^{n-1}\right).$$

По теореме Дирихле [11, гл. II, § 4, п. 3] для многочлена (2) число основных единиц $r = k+l-1$. Далее предполагаем, что $m = k + l \geqslant 2$. Ибо, если $k + l \leqslant 1$, то $r \leqslant 0$ и по теореме Дирихле основные единицы отсутствуют.

Теорема 1 ([11, гл. II, § 1, п. 2]). *Для чисел* (3) *с* $X = (x_1, \ldots, x_n) \in \mathbb{R}^n$

$$N(\xi) = f(X) \stackrel{\text{def}}{=} f_1(X) \ldots f_m(X). \tag{5}$$

Поэтому для всех единиц вида (3)

$$f(X) = \pm 1 \text{ и } g(X) \stackrel{\text{def}}{=} |f(X)| = 1. \tag{6}$$

Пусть $\check{\mathbb{Z}}^n$ — множество точек $X \in \mathbb{Z}^n$ со свойством (6). Рассмотрим для него (т. е. для $X \in \check{\mathbb{Z}}^n$) конструкции раздела 1: множество $\check{\mathbf{Z}}$ значений

$$G(X) = (g_1(X), \ldots, g_m(X)) \subset \mathbf{S} = \mathbb{R}_+^m,$$

где $g_i(X) = |f_i(X)|$, $i = 1, \ldots, m$, выпуклую оболочку $\check{\mathbf{H}}$ множества $\check{\mathbf{Z}}$ и её границу $\partial\check{\mathbf{H}}$. Граница $\partial\check{\mathbf{H}}$ имеет размерность $m - 1 = r$, не имеет кривых участков и состоит из вершин, рёбер и граней.

Теорема 2. *Все грани границы $\partial\check{\mathbf{H}}$ являются симплексами, а значение $G_0 = (1, 1, \ldots, 1)$ является её вершиной.*

Пусть Δ — некоторая $(m-1)$-мерная грань границы $\partial\check{\mathbf{H}}$, содержащая вершину $G_0 = (1, 1, \ldots, 1)$, а $R_1, \ldots, R_{m-1}$ — её рёбра, содержащие G_0.

Теорема 3. *Пусть G_i — вторая вершина ребра R_i, отличная от вершины G_0, $i = 1, \ldots, m-1$. Числа (3), у которых $G(X) = G_i$, $i = 1, \ldots, m-1$, образуют набор основных единиц кольца $\mathbb{Z}[\lambda]$.*

Следовательно, для вычисления основных единиц надо на некотором ограниченном множестве $||X|| < \text{const}$, $X \in \check{\mathbb{Z}}^n$ вычислить кусок границы $\partial\check{\mathbf{H}}$, содержащий $(m-1)$-мерную грань Δ.

Каждому числу (3) соответствует матрица

$$T(\xi) = x_1 E + x_2 B + \ldots + x_n B^{n-1},$$

где E — единичная, а B — это матрица, сопровождающая многочлен (2):

$$B = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ -b_n & -b_{n-1} & -b_{n-2} & \cdots & -b_2 & -b_1 \end{pmatrix}.$$

Если число (3) является единицей, то матрица $T(\xi)$ унимодулярна и линейное преобразование $X^* = T(\xi)X$ в $\mathbb{R}^n$ является автоморфизмом множества $\mathbf{H}$ и индуцирует автоморфизм

$$s_i^* = g_i(X) s_i, \quad i = 1, \ldots, m, \tag{7}$$

множества $\check{\mathbf{H}}$ в $\mathbf{S} = \mathbb{R}^m_+$. Следовательно, каждой единице ε соответствует период $T(\varepsilon)$ обобщённой цепной дроби. Количество независимых периодов равно $m-1$. Это — обобщение теоремы Лагранжа [1, § 10], доказанной для $n = l = 2$, $k = 0$, т. е. $m = k + l = 2$.

4. Фундаментальная область

В поле $\mathbb{Q}(\lambda)$ всякая целая степень $t \geqslant n$ числа ξ из (3) однозначно записывается в виде многочлена от λ степени $n-1$, ибо

$$\lambda^n = -\left(b_n + b_{n-1}\lambda + \ldots + b_1\lambda^{n-1}\right).$$

Поэтому отношение двух многочленов от λ однозначно записывается в виде многочлена от λ степени $n-1$.

Теорема 4. *Пусть $X = (x_1, \ldots, x_n)$, $Y = (y_1, \ldots, y_n)$, $Z = (z_1, \ldots, z_n) \in \mathbb{Q}^n$ и $\xi(X)\cdot\xi(Y) = \xi(Z)$, тогда $f_i(X) \cdot f_i(Y) = f_i(Z)$, $i = 1, \ldots, m$.*

Следствие 1. *В условиях теоремы 4 $g_i(X) \cdot g_i(Y) = g_i(Z)$, $i = 1, \ldots, m$.*

Логарифмическая замена

$$h_i(X) = \ln g_i(X), \quad i = 1, ..., m, \quad H \stackrel{\text{def}}{=} (h_1, \ldots, h_m)$$

взаимно однозначно переводит $\mathbf{S} = \mathbb{R}^m_+$ в $\mathbb{R}^m$. При этом $(m-1)$-мерная граница $\partial\mathbf{H}$ многогранного множества $\mathbf{H}$ переходит в $(m-1)$-мерную поверхность, которая взаимно однозначно проектируется на $\mathbb{R}^{m-1} = \{H'\}$, где $H' \stackrel{\text{def}}{=} (h_1, \ldots, h_{m-1})$.

На $\mathbb{R}^{m-1}$ автоморфизм (7) принимает вид

$$h_i^* = \ln g_i(X) + h_i, \quad i = 1, \ldots, m-1, \tag{8}$$

т. е. является параллельным переносом. Единицы кольца $\mathbb{Z}[\lambda]$ образуют абелеву группу по умножению. По теореме 4 их логарифмы H образуют абелеву группу по сложению. В $\mathbb{R}^{m-1}$ имеется фундаментальная область $\mathcal{F}$ относительно сдвигов (8) этой группы. Пусть m-мерные векторы G_i, $i = 1, \ldots, m-1$, соответствующие основным единицам теоремы 3, имеют вид $G_i = (g_{1i}, \ldots, g_{mi})$. Положим

$$\Gamma_i = (\ln g_{1i}, \ldots, \ln g_{m-1,i}), \quad i = 1, \ldots, m-1. \tag{9}$$

Теорема 5. *В $\mathbb{R}^{m-1}$ фундаментальная область относительно сдвигов* (8), (9) *— это $(m-1)$-мерный «куб»*

$$\mathcal{F} = \left\{ H' = \mu_1\Gamma_1 + \ldots + \mu_{m-1}\Gamma_{m-1},\ 0 \leqslant \mu_i \leqslant 1,\ i = 1, \ldots, m-1 \right\}. \tag{10}$$

При вычислении границы выпуклой оболочки некоторого множества точек трудности возрастают вместе с ростом количества точек. Чтобы уменьшить эти трудности можно вычисления разбить на следующие 6 шагов.

Шаг 1. Сначала в кольце $\mathbb{Z}[\lambda]$ находим все единицы с $X \in \mathbb{Z}^n$ из области $||X|| < \text{const}$, вычисляя значения $g(X)$ в этих X.

Шаг 2. Затем на множестве единиц $\{\check{X}\}$ надо вычислить границу $\partial\check{\mathbf{H}}$ их выпуклой оболочки $\check{\mathbf{H}}$.

Шаг 3. По теореме 3 из $\partial\check{\mathbf{H}}$ выделяем набор основных единиц, представленных в $\mathbf{S}$ вершинами $G_1, \ldots, G_{m-1}$.

Шаг 4. По теореме 5 находим фундаментальную область (10).

Шаг 5. Теперь выпуклая оболочка значений $G(X)$ с $\xi(X) \in \mathbb{Z}[\lambda]$ вычисляется только по тем X, у которых $H'(X)$ попадают в фундаментальную область (10) и её близкую окрестность.

Шаг 6. По этой части границы $\partial\mathbf{H}$ восстанавливается вся граница $\partial\mathbf{H}$ с помощью периодов G_i, $i = 1, \ldots, m-1$, соответствующих основным единицам, или с помощью сдвигов (8).

5. Диофантовы уравнения

Многочлену $p(\xi)$ степени n из (2) соответствует форма $f(X)$ из (5) степени n от n переменных $X = (x_1, \ldots, x_n)$. Её коэффициенты являются многочленами от коэффициентов b_i многочлена (2). Так, при $n = 2$

$$f(X) = x_1^2 - b_1x_1x_2 + b_2x_2^2,$$

при $n = 3$

$$f(X) = x_1^3 - b_1x_1^2x_2 + b_2x_1x_2^2 - b_3x_2^3 + \left(b_1^2 - 2b_2\right)x_1^2x_3 + (3b_3 - b_1b_2)x_1x_2x_3 - \\ - b_1b_2x_2^2x_3 + \left(b_2^2 - 2b_1b_3\right)x_1x_3^2 - b_2b_3x_2x_3^2 + b_3^2x_3^3.$$

Для любого n при $x_3 = \ldots = x_n = 0$ имеем

$$f(X) = x_1^n - b_1 x_1^{n-1} x_2 + b_2 x_1^{n-2} x_2^2 - \ldots$$
$$\ldots + (-1)^{n-1} b_{n-1} x_1 x_2^{n-1} + (-1)^n b_n x_2^n.$$

Задача 3. *Для заданного многочлена* (2) *найти все решения* (3) *с* $\xi \in \mathbb{Z}[\lambda]$ *уравнения*

$$f(X) = \beta, \tag{11}$$

где число β *рационально,* $\beta \neq \pm 1$.

Решение задачи 3.

Теорема 6 ([11, гл. II, § 5, теорема 1]). *Все решения* (3) *с* $\xi \in \mathbb{Z}[\lambda]$ *уравнения* (11) *имеют вид*

$$\xi = \xi_j^0 \varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r}, \quad j = 1, \ldots, J, \tag{12}$$

где $\xi_1^0, \ldots, \xi_J^0$ *— конечное множество выделенных решений и* $a_1, \ldots, a_r$ *— любые целые числа. Если выделенных решений* ξ_j^0 *нет, то уравнение* (11) *не имеет решений.*

Далее даётся набросок конструктивного доказательства этой теоремы, позволяющий вычислять соответствующие постоянные и выделенные решения $\xi_1^0, \ldots, \xi_J^0$.

Согласно предыдущим разделам находим набор основных единиц $\Sigma = (\varepsilon_1, \ldots, \varepsilon_{m-1})$ кольца $\mathbb{Z}[\lambda]$ и по ним строим фундаментальную область $\mathcal{F}$ в координатах $H' \stackrel{\text{def}}{=} (h_1, \ldots, h_{m-1})$.

Лемма 1. *Для всех точек* $X \in \mathbb{R}^n$, *у которых логарифмические проекции*

$$H' = (h_1, \ldots, h_{m-1})$$

лежат в фундаментальной области $\mathcal{F}$, *справедливы оценки*

$$\mu_i \leqslant g_i(X) \leqslant \nu_i, \quad i = 1, \ldots, m-1, \tag{13}$$

где $0 < \mu_i < \nu_i$ *— вещественные числа.*

Лемма 2. *Для всех точек* X, *у которых* $H' \in \mathcal{F}$ *и выполнено равенство* $g(X) = |\beta|$, *справедливы оценки*

$$\mu_m \leqslant g_m(X) \leqslant \nu_m, \tag{14}$$

где $0 < \mu_m < \nu_m$ *— вещественные числа.*

Нижние оценки в (13) нужны для получения верхней оценки в (14).

Поскольку $\langle K, X \rangle = \langle \Re K, X \rangle + i \langle \Im K, X \rangle$, то

$$\langle K, X \rangle \left\langle \bar{K}, X \right\rangle = \langle \Re K, X \rangle^2 + \langle \Im K, X \rangle^2 .$$

Лемма 3. *Если*

$$\gamma \stackrel{\text{def}}{=} \det (\Lambda_1, \ldots, \Lambda_l, \Re K_{l+1}, \Im K_{l+1}, \ldots, \Re K_{l+k}, \Im K_{l+k}) \neq 0, \tag{15}$$

то области в $\mathbb{R}^n$, *где выполнены неравенства* (13) *и* (14), *ограничены.*

Поскольку

$$\gamma = \frac{1}{(-2i)^k} \det\left(\Lambda_1, \ldots, \Lambda_l, K_{l+1}, \bar{K}_{l+1}, \ldots, K_{l+k}, \bar{K}_{l+k}\right),$$

и последний определитель отличается от определителя Вандермонда W ненулевым множителем, а $W = \prod\limits_{1<i<j}^{n} (\lambda_i - \lambda_j)$, то условие (15) эквивалентно условию, что у многочлена (2) нет кратных корней. Но это так по условию, что многочлен (2) неприводим в $\mathbb{Q}$.

Неравенства (13), (14) выделяют в $\mathbb{R}^n$ всего 2^m ограниченных областей вида

$$\mu_i \leqslant \varkappa_i f_i(X) \leqslant \nu_i, \quad \varkappa_i = \pm 1, \quad i = 1, \ldots, m.$$

В каждой из них количество целочисленных точек $X \in \mathbb{Z}^n$ конечно. В каждой из этих точек можно вычислить $f(X)$ и отобрать те X_i, в которых выполнено уравнение (11). Наконец, среди этих точек X_i оставляем только те $X_1^0, \ldots, X_J^0$, для которых отношения $\xi(X_i^0)/\xi(X_j^0)$ по $j \neq i$ не лежат в $\mathbb{Z}[\lambda]$. Тогда $\xi_j^0 = \xi(X_j^0)$, $j = 1, \ldots, J$, являются выделенными решениями уравнения (11) и все решения этого уравнения имеют вид (12).

6. Обобщения

6.1. Единицы с положительной нормой

Для единицы ε норма $N(\varepsilon) = \pm 1$. Иногда нужны только единицы, у которых норма положительна. Чтобы при чётном n найти базисный набор таких (квазиосновных) единиц $\widehat{\Sigma} = (\hat{\varepsilon}_1, \ldots, \hat{\varepsilon}_{m-1})$, надо в описанной процедуре раздела 3 оставлять только те точки $X \in \check{\mathbb{Z}}^n$, для которых $f(X) = +1$, и по ним указанным выше способом выделить мультипликативный базис. При нечётном n всякой единице ε соответствует единица ε' с $N(\varepsilon') = 1$: это либо ε, либо $-\varepsilon$, т. е. в записи (3) X заменяется на $-X$.

6.2. Произвольный порядок

Согласно [11, гл. II,§ 2] полный модуль в поле $\mathbb{Q}(\lambda)$, содержащий число 1 и являющийся кольцом, называется **порядком** поля $\mathbb{Q}(\lambda)$. Очевидно, что кольцо $\mathbb{Z}[\lambda]$ является порядком поля $\mathbb{Q}(\lambda)$. Но в этом поле могут быть и другие порядки. Например, если в записи (3) все x_2 — чётные, то получим подкольцо кольца $\mathbb{Z}[\lambda]$. Все результаты разделов 3–5, доказанные для порядка $\mathbb{Z}[\lambda]$, справедливы для любого порядка Ω поля $\mathbb{Q}(\lambda)$. Пусть $\omega_1, \ldots, \omega_n$ — базис порядка Ω, т. е. все числа $\alpha \in \Omega$ имеют вид

$$\alpha = y_1\omega_1 + y_2\omega_2 + \ldots + y_n\omega_n, \quad y_i \in \mathbb{Z}. \tag{16}$$

При записи этих чисел в виде (3) коэффициенты x_i могут быть рациональными числами.

Отметим отличия, возникающие для произвольного порядка Ω. Единицы (3) этого порядка могут иметь рациональные коэффициенты x_i. Существует такой набор единиц $\varepsilon_1, \ldots, \varepsilon_r \in \Omega$, что все единицы поля имеют вид (4). Назовём эти единицы основными. Для них справедливы все конструкции и теоремы разделов 3–5. Только матрица периода $T(\varepsilon)$ может иметь рациональные элементы, но $\det T(\varepsilon) = N(\varepsilon) = \pm 1$. Поэтому для отыскания основных единиц порядка надо вычислять $f(X)$ на решётке чисел (16), записанных в виде (3) с рациональными x_i. Дальнейшие вычисления такие же, как для кольца $\mathbb{Z}[\lambda]$. Мультипликативный базис единиц с положительной нормой образует набор квазиосновных единиц $\widehat{\Sigma} = (\hat{\varepsilon}_1, \ldots, \hat{\varepsilon}_{m-1})$ с положительной нормой. Здесь также можно найти фундаментальные области $\mathcal{F}$ и $\widehat{\mathcal{F}}$, соответствующие наборам Σ и $\widehat{\Sigma}$.

6.3. Максимальный порядок

В поле $\mathbb{Q}(\lambda)$ имеется максимальный порядок $\widetilde{\Omega}$. Его базис $\tilde{\omega}_1, \dots, \tilde{\omega}_r$ называется фундаментальным, о его вычислении см. [11, гл. II, § 2]. Всё сказанное для порядка $\mathbb{Z}[\lambda]$ справедливо и для максимального порядка. В частности, он имеет набор основных единиц $\Sigma = (\varepsilon_1, \dots, \varepsilon_r)$, набор квазиосновных единиц $\widehat{\Sigma} = (\widehat{\varepsilon}_1, \dots, \widehat{\varepsilon}_r)$ с положительными нормами и соответствующие им фундаментальные области $\mathcal{F}$ и $\widehat{\mathcal{F}}$.

7. Пример 2

Пусть $p(\xi) = \xi^2 - 5$. Тогда $n = 2$, а корни многочлена $p(\xi)$ суть $\lambda = \pm\sqrt{5} \approx \pm 2.23605$. Поэтому $k = 0, l = 2, m = k+l = 2$ и $r = m-1 = 1$. Основная единица максимального порядка $\widetilde{\Omega}$ есть $\varepsilon = (1+\lambda)/2 \approx 1.61803$, т. е. в записи (3) $x_1 = x_2 = 1/2$. Поскольку $N(X) = x_1^2 - 5x_2^2$, то $N(\varepsilon) = -1$ и квазиосновная единица максимального порядка $\widetilde{\Omega}$ есть $\hat{\varepsilon} = \varepsilon^2 = (3+\lambda)/2 \approx 2.61803$. Основная единица кольца $\mathbb{Z}[\lambda]$ есть $\varepsilon^3 = 2 + \lambda \approx 4.23605$ с нормой $N\left(\varepsilon^3\right) = -1$. Наконец, квазиосновная единица этого кольца есть $\hat{\varepsilon} = \varepsilon^6 = 9 + 4\lambda \approx 17.94421$.

Уравнение (11) здесь имеет вид $x_1^2 - 5x_2^2 = \beta$. Положим $\beta = 4$ и найдем все целочисленные решения (x_1, x_2) уравнения

$$x_1^2 - 5x_2^2 = 4, \tag{17}$$

т. е. $\xi(x_1, x_2) = x_1 + x_2\sqrt{5} \in \mathbb{Z}\left[\sqrt{5}\right]$. Ограничимся решениями $x_1, x_2 \geqslant 0$, остальные решения получаются изменением знаков. Поэтому наша основная единица — это $\hat{\varepsilon} = \varepsilon^6 = 9 + 4\sqrt{5} \approx 17.94421 < 18$. Фундаментальная область $\widehat{\mathcal{F}}$ в координатах x_1, x_2 — это

$$1 \leqslant f_1 \stackrel{\text{def}}{=} x_1 + x_2\sqrt{5} \leqslant \hat{\varepsilon} < 18. \tag{18}$$

На кривой (17) над $\widehat{\mathcal{F}}$ выполнены неравенства $4/\hat{\varepsilon} \leqslant f_2 \stackrel{\text{def}}{=} x_1 - x_2\sqrt{5} \leqslant 4$, т. е.

$$\frac{2}{9} \leqslant x_1 - x_2\sqrt{5} \leqslant 4. \tag{19}$$

На плоскости $(x_1, x_2) \in \mathbb{R}^2$ неравенства (18), (19) выделяют четырёхугольник, ограниченный прямыми $f_1 = 1$, $f_1 = 18$, $f_2 = 2/9$, $f_2 = 4$ и показанный на рис. 2.

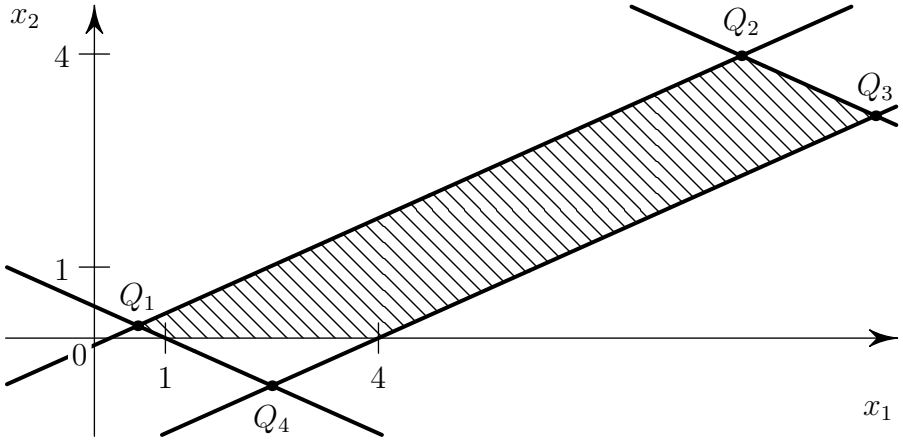

Рис. 2: Область в $\mathbb{R}^2$, где содержатся все выделенные решения ξ_i^0, показана штриховкой.

Вершины этого четырёхугольника суть

$$\begin{aligned} Q_1 &= \left(\frac{1}{2}+\frac{1}{9}, \frac{1}{2\sqrt{5}}-\frac{1}{9\sqrt{5}}\right) && \approx(0.61111,\ 0.17392),\\ Q_2 &= \left(9+\frac{1}{9}, \frac{9}{\sqrt{5}}-\frac{1}{9\sqrt{5}}\right) && \approx(9.11111,\ 3.97524),\\ Q_3 &= \left(11, \frac{7}{\sqrt{5}}\right) && \approx(11, 3.13051),\\ Q_4 &= \left(\frac{5}{2}, -\frac{3\sqrt{5}}{10}\right) && \approx(2.5, -0.67082). \end{aligned}$$

Теперь для каждого целого $x_2 : 0 \leqslant x_2 \leqslant 3$, переберём все целые $x_1 : 1 \leqslant x_1 < 11$ и выберем среди таких точек (x_1, x_2) решения уравнения (17). Получаем точки $(2,0)$, $(3,1)$, $(7,3)$. Поскольку отношения $\left(3+\sqrt{5}\right)/2$, $\left(7+3\sqrt{5}\right)/2$, $\dfrac{7+3\sqrt{5}}{3+\sqrt{5}} = \dfrac{3+\sqrt{5}}{2}$ не лежат в $\mathbb{Z}\left[\sqrt{5}\right]$, то получим три выделенных решения $\xi_1^0 = 2$, $\xi_2^0 = 3+\sqrt{5}$, $\xi_3^0 = 7+3\sqrt{5}$. По теореме 6 все решения с $x_1, x_2 \geqslant 0$ имеют вид

$$\xi = \xi_i^0 \left(9+4\sqrt{5}\right)^a, \quad i = 1,2,3, \quad 0 \leqslant a \in \mathbb{Z}.$$

8. Пример 3

Пусть $p(\xi) = \xi^3 - 7\xi - 2$, все его корни вещественны:

$$\lambda_1 \approx -2.489288, \quad \lambda_2 \approx -0.289168, \quad \lambda_3 \approx 2.778457.$$

Здесь $n = m = l = 3$, $k = 0$, $r = m - 1 = 2$. Фундаментальный базис максимального порядка $\widetilde{\Omega}$ есть $1, \lambda, \left(\lambda+\lambda^2\right)/2$. Вычисления проведём в 6 шагов раздела 4.

Шаг 1. Вычисляя значения $g(Y)$ на точках $\xi = y_1 + y_2\lambda + y_3\left(\lambda+\lambda^2\right)/2$ с целыми y_i, находим единицы $\varepsilon_i = (y_1, y_2, y_3)$: $\varepsilon_1 = (0,0,1)$, $\varepsilon_2 = (1,2,2)$, $\varepsilon_3 = (-2,0,1)$, $\varepsilon_4 = (-10,-2,3)$, $\varepsilon_5 = (5,2,-2)$, $\varepsilon_6 = (0,2,-1)$.

Шаг 2. Вычисляем выпуклую оболочку соответствующих точек $G_0, G_i = G(Y)$ и получаем у неё 6 двумерных граней. Их логарифмические проекции на плоскость h_1, h_2 показаны на рис. 3. На нём логарифмические проекции рёбер показаны прямыми отрезками, хотя они являются криволинейными. Заметим, что $\varepsilon_{i+3} = \varepsilon_i^{-1}$, $i = 1,2,3$.

Шаг 3. Здесь любая пара ε_i и $\varepsilon_j \neq \varepsilon_i^{\pm 1}$ $(i,j = 1,\ldots,6)$ образует набор фундаментальных единиц.

Шаг 4. Для пары ε_1, ε_3 фундаментальная область $\mathcal{F}$ — четырёхугольник с вершинами $0, \varepsilon_1, \varepsilon_2, \varepsilon_3$.

Шаг 5. Логарифмическая проекция границы выпуклой оболочки значений $G(Y)$ по $Y \in \mathbb{Z}^3$ с $H'(Y) \in \mathcal{F}$ показана на рис. 4.

Тут имеются две новые вершины: $\delta_1 = (0,1,1)$ и $\delta_2 = (1,1,1)$. На них $g(Y) = 2$. Имеется четырёхугольная грань с вершинами $0, \delta_1, \varepsilon_2, \delta_2$.

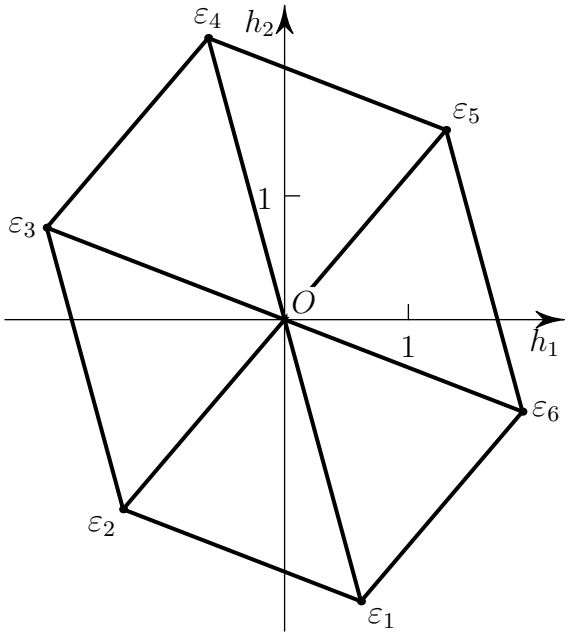

Рис. 3: Логарифмическая проекция вершин, рёбер и граней многогранника $\partial\widetilde{\mathbf{H}}$. Показаны проекции единиц, близкие к нулю. Проекции рёбер выпрямлены.

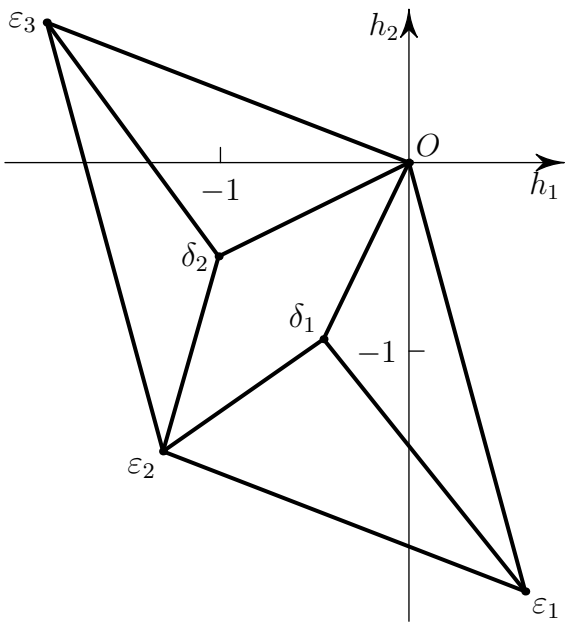

Рис. 4: Логарифмическая проекция многогранника $\partial\mathbf{H}$ на фундаментальную область.

Шаг 6. Сдвигая фундаментальную область рис. 4 на целочисленные линейные комбинации логарифмов известных единиц, получаем схематическую проекцию всего многогранника $\partial\mathbf{H}$ на плоскость h_1, h_2, показанную на рис. 5. На рис. 6 показана точная логарифмическая проекция многогранника $\partial\mathbf{H}$ на плоскость h_1, h_2; проекции рёбер криволинейны. Отрезки в ромбах — это ошибки: их не должно быть. Этот рисунок взят из [5], куда он попал из [12].

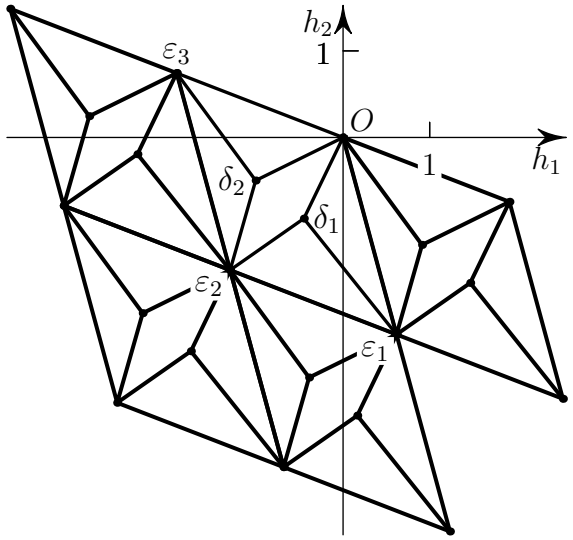

Рис. 5: Логарифмическая проекция многогранника $\partial\mathbf{H}$ на часть плоскости h_1, h_2.

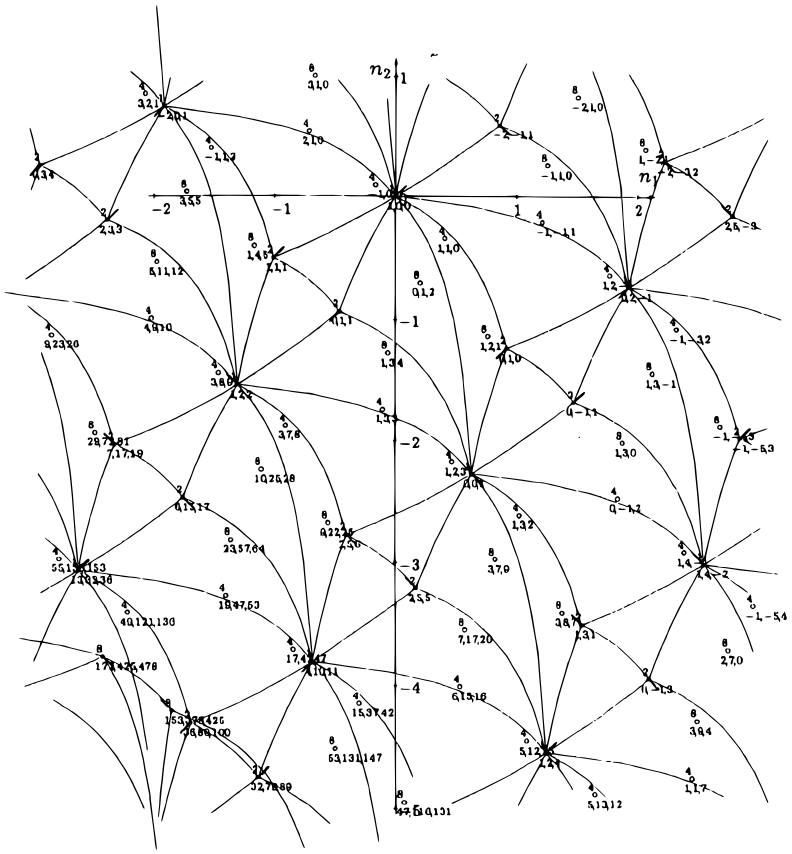

Рис. 6: Аналог рис. 5 с точными проекциями рёбер. Рёбра, разделяющие ромбы на треугольники, ошибочны.

Этот пример взят у Вороного [6, § 59, пример]. Там найдены две пары основных единиц $\varepsilon_2, \varepsilon_3$ и $\varepsilon_2, \varepsilon_4$, но нет аналогов наших рисунков. На самом деле, в этом примере граница $\partial\mathbf{H}$ вычисляется сразу как выпуклая оболочка значений $G(Y)$ по $Y \in \mathbb{Z}^3$, ибо размерность задачи $n = 3$ невелика. Но здесь показано разбиение на шаги, которое может быть полезным при больших размерностях n и m.

9. Предшественники

Для $n = 2$, $k = 0$, $l = 2$, когда $m = 2$ и $r = 1$, т. е. для вещественных квадратичных полей способ вычисления основной единицы максимального порядка $\widetilde{\Omega}$, основанный на разложении в цепную дробь, описан в книге [11, гл. II, § 7]. В конце этой книги в табл. 1 приведены значения основных единиц $\varepsilon > 1$ максимальных порядков полей $\mathbb{Q}\left(\sqrt{d}\right)$ для $2 \leqslant d \leqslant 101$, $d \in \mathbb{Z}$.

Для $n = 3$, $m = 2$ $(r = 1)$ и $n = 3$, $m = 3$ $(r = 2)$ основные единицы максимальных порядков вычислял Вороной [6] с помощью своего пошагового обобщения цепной дроби. В [3, 5, 13] вычислены многоугольники и многогранники $\partial\mathbf{H}$.

Для $n = 4$, $k = 2$, $l = 0$, т. е. $m = 2$ $(r = 1)$, Парусников [14] вычислил единицы максимальных порядков полей $\mathbb{Q}(\lambda)$ для 41 многочлена (2) с помощью пошагового алгоритма, основанного на выпуклом многоугольнике. Но большинство найденных им единиц не являются основными, а являются лишь их целыми степенями.

Предварительные версии этой статьи — это препринт [15] и статья [16].

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Хинчин А. Я. Цепные дроби. 3-е изд. М.: Физматгиз, 1961.

2. Брюно А. Д. Разложения алгебраических чисел в цепные дроби // Журнал вычислительной матем. и матем. физики. 1964. Т. 4, № 2. С. 211–221.

3. Bruno A. D. New generalizations of continued fraction. I // Functiones et Approximatio. 2010. vol. 43, no. 1. Pp. 55–104.

4. Bruno A. D. On geometric methods in works by V. I. Arnold and V. V. Kozlov. Preprint of arXiv, No 1401.6320.

5. Брюно А. Д. Универсальное обобщение алгоритма цепной дроби // Чебышевский сборник (Тула), 2015, том 16, выпуск 2. С. 35–65.

6. Вороной Г. Ф. Об одном обобщении алгорифма непрерывных дробей. Варшава: Из-во Варш. Ун-та, 1896. Также: Собр. соч. в 3-х томах. Киев: Из-во АН УССР, 1952. Т. 1. С. 197–391.

7. Брюно А. Д. Структура многомерных диофантовых приближений// ДАН, 2010. Т. 433, № 5. С. 587–589.

8. Bruno A. D. Structure of the best diophantine approximations and multidimensional generalizations of the continued fraction // Чебышевский сборник (Тула), 2010. том 11, вып. 1. С. 68–73.

9. Fukuda K. Exact algorithms and software in optimization and polyhedral computation // Proceed. ISSAC'08 of XXI International Symposium on Symbolic and Algebraic Computations, ACM NY, USA, 2008. Pp. 333–334.

10. Barber C. B., Dobkin D. P., Huhdanpaa H. T. The Quickhull algorithm for convex hulls // ACM Trans. on Mathematical Software, 22(4):469–483, Dec. 1996, http://www.qhull.org.

11. Боревич З. И., Шафаревич И. Р. Теория чисел. 2-е изд. М.: Наука, 1972.

12. Брюно А. Д., Парусников В. И. Многогранники модулей троек линейных форм // Препринты ИПМ им. М. В. Келдыша. 2003. № 93. 20 с.
URL: http://library.keldysh.ru/preprint.asp?id=2003-93

13. Брюно А. Д. Обобщения цепной дроби // Чебышевский сборник (Тула), 2006, том 7, вып. 3. С. 4–71.

14. Парусников В. И. Четырёхмерное обобщение алгоритма цепных дробей // Препринты ИПМ им. М. В. Келдыша. 2011. № 78. 16 с. URL: http://library.keldysh.ru/preprint.asp?id=2011-78.

15. Брюно А. Д. От диофантовых приближений к диофантовым уравнениям // Препринты ИПМ им. М. В. Келдыша. 2016. № 1. 20 с. URL: http://library.keldysh.ru/preprint.asp?id=2016-1

16. Брюно А. Д. Вычисление наилучших диофантовых приближений и основных единиц алгебраических полей // ДАН, 2016. Т. 468, № 1. С. 7–11.

REFERENCES

1. Khinchin, A. Ya. 1963, *Continued fractions*, Noordhoff, Groningen.

2. Bruno, A. D. 1964, "The expansion of algebraic numbers into continued fractions", *USSR Comp. Math. Math. Phys.*, Vol. 4, no. 2, Pp. 1–15.

3. Bruno, A. D. 2010, "New generalizations of continued fraction. I", *Functiones et Approximatio.* vol. 43, no. 1. Pp. 55–104.

4. Bruno, A. D. 2014, *On geometric methods in works by V. I. Arnold and V. V. Kozlov*, Preprint of arXiv, No 1401.6320.

5. Bruno, A. D. 2015, "Universal generalization of the continued fraction algorithm", *Chebyshevsky sbornik*, vol. 16, no. 2, pp. 35–65.

6. Voronoi, G. F. 1896, *On Generalization of the Algorithm of Continued Fraction*, Warsawa University.

7. Bruno, A. D. 2010, "The structure of multidimensional Diophantine approximations", *Doklady Mathematics*, vol. 82, no. 1. Pp. 587–589.

8. Bruno, A. D. 2010, "Structure of the best diophantine approximations and multidimensional generalizations of the continued fraction", *Chebyshevsky sbornik*, vol. 11, no. 1, pp. 68–73.

9. Fukuda, K. 2008, "Exact algorithms and software in optimization and polyhedral computation", *Proceed. ISSAC'08 of XXI International Symposium on Symbolic and Algebraic Computations*, ACM NY, USA, Pp. 333–334.

10. Barber, C. B. & Dobkin, D. P. & Huhdanpaa, H. T. 1996, "The Quickhull algorithm for convex hulls", *ACM Trans. on Mathematical Software*, 22(4):469–483, http://www.qhull.org.

11. Borevich, ZI & Shafarevich, IR 1966, *Number Theory*, Academic Press.

12. Bruno, A. D. & Parusnikov, V. I. 2003, "Polyhedra of absolute values for triple of linear forms", *Preprint no. 93 of the Keldysh Inst. of Applied Math.*, Moscow. URL: http://library.keldysh.ru/preprint.asp?id=2003-93.

13. Bruno, A. D. 2006, "Generalization of continued fraction", *Chebyshevsky sbornik*, vol. 7, no. 3, pp. 4–71.

14. Parusnikov, V. I. 2011, "4-dimensional generalization of the continued fractions", *Preprint no. 78 of the Keldysh Inst. of Applied Math.*, Moscow. URL: http://library.keldysh.ru/preprint.asp?id=2011-78.

15. Bruno, A. D. 2016, "From Diophantine approximations to Diophantine equations", *Preprint no. 1 of the Keldysh Inst. of Applied Math.*, Moscow. URL: http://library.keldysh.ru/preprint.asp?id=2016-1

16. Bruno, A. D. 2016, "Computation of the best Diophantine approximations and the fundamental units of the algebraic fields", *Doklady Mathematics*, vol. 93, no. 3. Pp. 243–247.

Институт прикладной математики им. М. В. Келдыша РАН.
Получено 5.05.2016 г.
Принято в печать 12.09.2016 г.