М. А. Всемирнов

ДИОФАНТОВЫ ПРЕДСТАВЛЕНИЯ ЛИНЕЙНЫХ РЕКУРРЕНТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ. II

1. Введение

В настоящей статье мы продолжаем исследование вопроса о прямых методах построения диофантовых представлений линейных рекуррентных последовательностей, поставленного в [2, Открытый вопрос 2.3]. Мотивировку и подробную постановку задачи, можно найти в работе автора [3]. Историю вопроса см. в [12, гл. 2]. Большинство результатов данного цикла работ было анонсировано автором в [2, 4, 5].

Напомним основные определения, конструкции и результаты работы [3], которые потребуются в дальнейшем.

Определение. *Множество n-ок целых чисел $\mathcal{M}$ называется диофантовым, если существует многочлен $P(y_1, \dots, y_n, x_1, \dots, x_m)$ с целыми коэффициентами такой, что*

$$\langle a_1, \dots, a_n\rangle \in \mathcal{M} \Longleftrightarrow \exists x_1 \in \mathbf{N} \dots$$
$$\dots \exists x_m \in \mathbf{N}\ [P(a_1, \dots, a_n, x_1, \dots, x_m) = 0]. \qquad (1)$$

Эквивалентность (1) *называется диофантовым представлением множества $\mathcal{M}$.*

Замечание. В фундаментальной работе Ю. В. Матиясевича [11] было доказано, что теоретико-числовое понятие диофантова множества совпадает с понятием рекурсивно-перечислимого множества. См. также [12].

Традиционно, в задачах построения диофантовых представлений речь идет о множествах n-ок *натуральных* чисел. В данном случае более естественно рассматривать множества целочисленных n-ок, поскольку элементы произвольной линейной рекуррентной последовательности могут быть как положительными,

Работа выполнена при поддержке ISSEP (гранты a96-1965 и a97-2261).

так и отрицательными. По этой же причине иногда будет удобно рассматривать $\mathbf{Z}$-диофантовы представления, т.е. представления, аналогичные (1), но в которых переменные $x_1, x_2, \ldots, x_m$ принимают целочисленные значения.

Хорошо известно, что понятия диофантова множества и $\mathbf{Z}$-диофантова множества совпадают (см., например, [12, §1.3]), точнее, по диофантову представлению множества мы можем построить его $\mathbf{Z}$-диофантово представление и наоборот. Эта же техника позволяет показать, что если множество $\mathcal{M} \subset \mathbf{Z}^n$ диофантово, то множества n-ок натуральных чисел $\mathcal{M}' = \{\langle a_1, \ldots, a_n\rangle \in \mathbf{N}^n : \exists \langle b_1, \ldots, b_n\rangle \in \mathcal{M}\ [a_1 = |b_1|, \ldots, a_n = |b_n|]\}$ и $\mathcal{M}'' = \mathcal{M} \cap \mathbf{N}^n$ также являются диофантовыми.

В дальнейшем, чтобы избежать громоздких формул, мы не будем явно преобразовывать $\mathbf{Z}$-диофантовы представления в диофантовы. По этой же причине, мы будем рассматривать системы диофантовых уравнений. При необходимости такие системы могут быть свернуты в одно диофантово уравнение. Кроме того, мы будем использовать простейшие отношения, такие как делимость или неравенства, диофантовость которых очевидна.

2. Рекуррентные последовательности и их свойства

Пусть последовательность a_n определена рекуррентным соотношением k-го порядка (т.е. каждый последующий элемент представляется в виде линейной комбинации k элементов, непосредственно предшествующих ему)

$$a_{n+k} = b_{k-1}a_{n+k-1} + \ldots + b_0 a_n, \tag{2}$$

и начальными условиями

$$a_0 = 1, \quad a_{-1} = a_{-2} = \ldots = a_{-k+1} = 0. \tag{3}$$

Коэффициенты рекуррентного соотношения b_i – целые числа. Кроме того, мы накладываем дополнительное ограничение

$$b_0 = \pm 1, \tag{4}$$

Это ограничение позволяет доопределить данную последовательность для всех отрицательных n на основании соотношения

$$a_n = (a_{n+k} - b_{k-1}a_{n+k-1} - \ldots b_1 a_{n+1})/b_0. \tag{5}$$

При этом мы получим бесконечную в обе стороны *целозначную* последовательность. В дальнейшем мы ограничимся только такими последовательностями.

Далее мы будем рассматривать наиболее интересный для приложений случай, когда многочлен

$$f(\lambda) = t^k - b_{k-1}t^{k-1} - \ldots - b_1 t - b_0 \tag{6}$$

неприводим над полем $\mathbf{Q}$. Как мы увидим далее, во всех интересующих нас случаях условие неприводимости многочлена f можно будет выразить с помощью системы диофантовых уравнений относительно $b_0,\ b_1, \ldots, b_{k-1}$.

Под диофантовым представлением линейной рекуррентной последовательности (2)–(3) мы будем понимать диофантово представление множества

$$\mathcal{M} = \{\langle u, n\rangle \mid u = a_n\}. \tag{7}$$

Отметим один тривиальный случай. А именно, если многочлен f, определенный согласно (6), является l-ым многочленом деления круга, то рассматриваемая последовательность будет периодичной с периодом не больше l. Действительно, хорошо известно, что если многочлен f имеет k различных корней $\lambda_{(1)} = \lambda, \lambda_{(2)}, \ldots, \lambda_{(k)}$, то найдутся коэффициенты c_j, $j = 1, \ldots, k$, такие, что

$$a_n = \sum_{j=1}^{k} c_j \lambda_{(j)}^n.$$

Так как в рассматриваемом случае все $\lambda_{(j)}$ есть корни из 1, то заключаем, что последовательность a_n периодична. А для периодической последовательности (при фиксированных $b_0, b_1, \ldots, b_{k-1}$) задача построения ее диофантова представления тривиальна. Поэтому далее мы не рассматриваем этот случай и предполагаем, что f не является многочленом деления круга.

Напомним основную техническую конструкцию, введенную в [3]. Рассмотрим квадратные матрицы порядка k (ниже E обозначает единичную матрицу):

$$B = \begin{pmatrix} 0 & 0 & \dots & 0 & b_0 \\ 1 & 0 & \dots & 0 & b_1 \\ 0 & 1 & \dots & 0 & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & b_{k-1} \end{pmatrix} \tag{8}$$

$$A(x_0, x_1, \dots, x_{k-1}) = \sum_{l=0}^{k-1} x_l \left(B^l - \sum_{j=1}^{l} b_{k-j} B^{l-j} \right) =$$

$$= x_0 E + x_1(B - b_{k-1}E) + \dots + x_{k-1}(B^{k-1} - b_{k-1}B^{k-2} - \dots - b_1 E), \tag{9}$$

$$A^*(n) = A(a_n, a_{n-1}, \dots, a_{n-k+1}). \tag{10}$$

Определим однородный многочлен k-й степени от k переменных:

$$F_B(x_0, x_1, \dots, x_{k-1}) = \det A(x_0, x_1, \dots, x_{k-1}). \tag{11}$$

Как было показано в [3],

$$F_B(a_n, a_{n-1}, \dots, a_{n-k+1}) = \det B^n = \pm 1,$$

$$F_B(-a_n, -a_{n-1}, \dots, -a_{n-k+1}) = \det(-B)^n = \pm 1. \tag{12}$$

Естественно возникает вопрос о том, когда эти соотношения полностью характеризуют рассматриваемую последовательность. Дадим следующее определение.

Определение (см. [3]). *Будем говорить, что соотношение*

$$F_B(x_0, x_1, \dots, x_{k-1}) = \pm 1 \tag{13}$$

является характеристическим для последовательности (2)–(3)*, если все удовлетворяющие ему целочисленные наборы* $\langle x_0, x_1, \dots, x_{k-1} \rangle$ *исчерпываются следующими двумя сериями:*

$$\langle x_0, x_1, \dots, x_{k-1} \rangle = \langle a_n, a_{n-1}, \dots, a_{n-k+1} \rangle,$$

$$\langle x_0, x_1, \dots, x_{k-1} \rangle = \langle -a_n, -a_{n-1}, \dots, -a_{n-k+1} \rangle.$$

Описание всех последовательностей (2)–(3) (иными словами, всех наборов коэффициентов $b_0, b_1, \dots, b_{k-1}$), для которых соотношение (13) является характеристическим, будет первым шагом на пути построения диофантовых представлений множества

(7). Действительно, если для данного набора $b_0, b_1, \dots, b_{k-1}$ соотношение (13) является характеристическим для последовательности (2)–(3), то нетрудно указать $\mathbf{Z}$-диофантово представление множества

$$\mathcal{M}_1 = \{u \in \mathbf{Z} \mid \exists n \in \mathbf{Z}\ [u = a_n \vee u = -a_n]\}.$$

А именно,

$$x \in \mathcal{M}_1 \Longleftrightarrow \exists x_1 \in \mathbf{Z} \dots \exists x_{k-1} \in \mathbf{Z}\ [F_B^2(x, x_1, \dots, x_{k-1}) - 1 = 0].$$

3. Общая схема

Как показано в [3, 5], задача описания последовательностей, для которых соотношение (13) является характеристическим, тесно связана со свойствами единиц (обратимых элементов) в кольцах целых алгебраических чисел.

Пусть λ – корень многочлена f, определенного согласно (6). В частности, так как мы предполагаем, что f неприводим над полем $\mathbf{Q}$, то $\mathbf{Q}(\lambda)$ является расширением поля $\mathbf{Q}$ степени k, $[\mathbf{Q}(\lambda) : \mathbf{Q}] = k$. Пусть $(\mathbf{Z}[\lambda])^*$ обозначает, как обычно, мультипликативную группу единиц порядка $\mathbf{Z}[\lambda]$. В частности, так как $b_0 = \pm 1$, то

$$\langle \pm\lambda^n : n \in \mathbf{Z}\rangle \subseteq (\mathbf{Z}[\lambda])^*.$$

Нам потребуется следующее представление степеней λ, полученное в [3, тождество (18)]:

Лемма 1.

$$\lambda^n = a_n + a_{n-1}(\lambda - b_{k-1}) + \dots + a_{n-k+1}(\lambda^{k-1} - b_{k-1}\lambda^{k-2} - \dots - b_1). \quad (14)$$

Лемма 2. *Равенство* (13) *имеет место для целых* $x_0, x_1, \dots, x_{k-1}$ *тогда и только тогда, когда число*

$$x_0 + x_1(\lambda - b_{k-1}) + \dots + x_{k-1}(\lambda^{k-1} - b_{k-1}\lambda^{k-2} - \dots - b_1)$$

обратимо в $\mathbf{Z}[\lambda]$.

Это условие потребуется в дальнейшем.

Заметим, что отображение $T : \mathbf{Q}(\lambda) \to M_k(\mathbf{Q})$, заданное следующим образом

$$T(x_0 + x_1(\lambda - b_{k-1}) + \dots + x_{k-1}(\lambda^{k-1} - b_{k-1}\lambda^{k-2} - \dots - b_1)) =$$
$$= A(x_0, x_1, \dots, x_{k-1}),$$

является вложением поля $\mathbf{Q}(\lambda)$ в кольцо матриц $M_k(\mathbf{Q})$. В действительности, для $\mu \in \mathbf{Q}(\lambda)$ матрица $T(\mu)$ есть матрица оператора умножения на μ в базисе $\langle 1, \lambda, \lambda^2, \dots, \lambda^{k-1}\rangle$. В частности, $T(\lambda) = B$. Учитывая определение гомоморфизма T и многочлена F_B, отметим, что лемма 2 является переформулировкой следствия к лемме 2 из [3].

Теорема 1. *Рассмотрим последовательность a_n, определенную согласно* (2)–(3). *Пусть многочлен f, определенный согласно* (6), *неприводим над полем* $\mathbf{Q}$, *и пусть λ – корень f Определим многочлен F_B цепочкой равенств* (8), (9), (11). *Для того, чтобы* (13) *было характеристическим для последовательности a_n, необходимо и достаточно, чтобы*

$$(\mathbf{Z}[\lambda])^* = \langle \pm\lambda^n : n \in \mathbf{Z}\rangle. \tag{15}$$

Замечание. В [3] этот результат не формулировался в явном виде, а был получен как промежуточный шаг в доказательстве основного результата [3] (см. доказательство теоремы 1 из [3] и, в частности, равенство (9) из указанной работы).

В действительности, в [3, доказательство теоремы 1] условие (13) было переформулировано в терминах алгебраических единиц:

Из теоремы 1 следует, что если (13) является характеристическим, то свободный ранг группы $(\mathbf{Z}[\lambda])^*$ не превосходит 1. Комбинируя этот результат с теоремой Дирихле (см. [1, гл. II, §4, теорема 5]), описывающей структуру группы единиц в произвольном порядке алгебраических чисел, получаем следующее следствие.

Следствие 1. *Для того, чтобы* (13) *было характеристическим, необходимо, чтобы выполнялось одно из следующих условий:*

1. *$k = 2$;*
2. *$k = 3$ и многочлен f имеет в точности один вещественный корень;*
3. *$k = 4$ и многочлен f не имеет вещественных корней.*

Следует отметить, что следствие 1 дает лишь необходимые, но не достаточные условия. Последовательности, для которых выполнено одно из условий, перечисленных в следствии, но соотношение (13) не является характеристическим, мы будем называть исключительными. Соответствующие примеры будут приведены далее. Кроме того, в данной работе будут явно указаны все исключительные последовательности второго и третьего порядка. Для таких последовательностей группа $\langle \pm\lambda^n : n \in \mathbf{Z} \rangle$ уже не совпадает с $(\mathbf{Z}[\lambda])^*$, а является ее подгруппой конечного индекса. Это позволяет дополнить уравнение (13) до характеристической системы уравнений.

Итак, для описания исключительных последовательностей нам необходимо найти все обратимые элементы λ в кольцах целых алгебраических чисел такие, что свободный ранг группы $(\mathbf{Z}[\lambda])^*$ равен 1, но не выполнено равенство (15).

4. Последовательности второго порядка

Последовательности второго порядка исследовались в работах [10, 14, 6]; см. также [2, гл. II]. Мы рассмотрим этот случай, поскольку наш метод отличается от применявшихся ранее. Кроме того, этот случай естественным образом укладывается в общую схему и позволяет продемонстрировать основные идеи метода на простом примере.

Укажем ограничения на коэффициенты b_0, b_1. Напомним, что мы рассматриваем лишь последовательности с $b_0 = \pm 1$ и неприводимым над $\mathbf{Q}$ многочленом

$$f(\lambda) = t^2 - b_1 t - b_0. \tag{16}$$

Как отмечено выше (см. §2), мы не будем рассматривать тривиальный случай периодических последовательностей. Для того, чтобы исключить этот случай, для последовательностей второго порядка с неприводимым многочленом f мы должны дополнительно потребовать, чтобы корни f были вещественными, т.е. его дискриминант

$$b_1^2 + 4b_0 \geqslant 0. \tag{17}$$

Многочлен f неприводим тогда и только тогда, когда

$$b_1^2 + 4b_0 \quad \text{не есть полный квадрат.} \tag{18}$$

Нетрудно видеть, что условия (4), (17) и (18) равносильны следующей системе условий:

$$b_0 = \pm 1, \quad b_1 \neq 0, \quad b_1^2 + 4b_0 > 0.$$

Лемма 3. *Пусть* $k = 2$, $c_0 = \pm 1$, $c_1 \in \mathbf{Z}$, $c_1 \neq 0$, $c_1^2 + 4c_0 > 0$. *Пусть* μ *удовлетворяет уравнению*

$$\mu^2 - c_1\mu - c_0 = 0 \tag{19}$$

и $\lambda = \mu^n$ *или* $\lambda = -\mu^n$ *для некоторого целого* n. *Для того, чтобы* $\mu \in \mathbf{Z}[\lambda]$ *необходимо и достаточно, чтобы выполнялось одно из следующих условий:*

(i) $|n| = 1$.

(ii) $|n| = 2$, $|c_1| = 1$, $c_0 = 1$.

Доказательство. Необходимость. Заметим, что $\lambda \in \mathbf{Z}[\mu]$. Поэтому, если $\mu \in \mathbf{Z}[\lambda]$, то

$$\mathbf{Z}[\mu] = \mathbf{Z}[\lambda].$$

В частности, $\langle 1, \mu \rangle$ и $\langle 1, \lambda \rangle$ будут базисами одного и того же модуля. Следовательно, дискриминанты $D(1, \mu)$ и $D(1, \lambda)$ этих базисов совпадают (см., например, [1, гл. 2, §2, п. 5]).

Пусть

$$\lambda = x\mu + y. \tag{20}$$

Тогда $D(1, \lambda) = x^2 D(1, \mu)$ и, значит, $x = \pm 1$.

Для нормы ччисла λ имеем $N(\lambda) = N(x\mu + y) = x^2 N(\mu) + xy\mathrm{Tr}\,(\mu) + y^2 = -c_0 x^2 + c_1 xy + y^2$. С другой стороны, $N(\lambda) = N(\pm\mu^n) = N(\mu^n) = (N(\mu))^n = (-c_0)^n$. Следовательно,

$$-c_0 x^2 + c_1 xy + y^2 = (-c_0)^n.$$

Рассмотрим возможные случаи.

Случай 1: $c_0 = -1$. Так как $x = \pm 1$, то $c_1 xy + y^2 = 0$, т.е. либо $y = 0$, либо $y = -xc_1$. Если $y = 0$, то $\lambda = x\mu = \pm\mu$, т.е. $n = 1$. Если $y = -xc_1$, то согласно (19) и (20) имеем $\lambda = x(\mu - c_1) = xc_0\mu^{-1} = \mp\mu^{-1}$, т.е. $n = -1$.

Случай 2: $c_0 = 1$, n нечетно. Так как $x = \pm 1$, то мы вновь приходим к равенству $c_1 xy + y^2 = 0$. Аналогично случаю 1 это дает допустимые значения $n = \pm 1$.

Случай 3: $c_0 = 1$, n четно. Тогда $c_1 xy + y^2 = (-c_0)^n + c_0 x^2 = 2$. Учитывая, что x, y, c_1 – целые, приведем все возможные варианты в таблице 1. Кроме того, в таблице приведен $g_\mu(t)$ (минимальный многочлен для μ), а также указаны соответствующие значения λ и n.

Таблица 1

y	x	c_1	$g_\mu(t)$	λ	n
2	1	-1	t^2+t-1	$\mu+2=\mu^{-2}$	-2
2	-1	1	t^2-t-1	$-\mu+2=\mu^{-2}$	-2
-2	1	1	t^2-t-1	$\mu-2=-\mu^{-2}$	-2
-2	-1	-1	t^2+t-1	$-\mu-2=-\mu^{-2}$	-2
1	1	1	t^2-t-1	$\mu+1=\mu^2$	2
1	-1	-1	t^2+t-1	$-\mu+1=\mu^2$	2
-1	1	-1	t^2+t-1	$\mu-1=-\mu^2$	2
-1	-1	1	t^2-t-1	$-\mu-1=-\mu^2$	2

Как видно из таблицы 1, в этом случае $|n|=2$, $|c_1|=1$. Необходимость доказана.

Достаточность. Достаточность условия (i) очевидна, так как μ – обратимый элемент кольца $\mathbf{Z}[\mu]$. Достаточность условия (ii) проверяется непосредственно (см. значения λ в таблице 1). Лемма доказана.

Если μ – корень уравнения $\mu^2-\mu-1=0$, то минимальным многочленом для чисел $\lambda=\mu^2$ и $\lambda=\mu^{-2}$ будет $\lambda^2-3\lambda+1$, а минимальным многочленом для чисел $\lambda=-\mu^2$ и $\lambda=-\mu^{-2}$ будет $\lambda^2+3\lambda+1$. Эти же многочлены получаются, если рассмотреть μ, удовлетворяющее уравнению $\mu^2+\mu-1=0$, и $\lambda=\pm\mu^2$, $\lambda=\pm\mu^{-2}$.

Теорема 2. *Пусть $k=2$, $b_0=\pm1$, $b_1\in\mathbf{Z}$, $b_1\neq0$, $b_1^2+4b_0>0$.*

- *Если $b_0=-1$, $b_1=\pm3$, то $[(\mathbf{Z}[\lambda])^*:\langle\pm\lambda^n\mid n\in\mathbf{Z}\rangle]=2$.*
- *Во всех остальных случаях $(\mathbf{Z}[\lambda])^*=\langle\pm\lambda^n\mid n\in\mathbf{Z}\rangle$.*

Доказательство. Непосредственно следует из леммы 3.

Теорема 3. *Пусть $k=2$, $b_0=\pm1$, $b_1\in\mathbf{Z}$, $b_1\neq0$, $b_1^2+4b_0>0$. Для того, чтобы соотношение* (13) *было характеристическим для последовательности* (2)–(3), *необходимо и достаточно, чтобы*

$$\langle b_0,b_1\rangle\notin\{\langle-1,3\rangle,\langle-1,-3\rangle\}.$$

Доказательство. Следует из теорем 1 и 2.

Замечание 1. Рассмотрим подробнее исключительные наборы $\langle b_0,b_1\rangle$ из теоремы 3.

Прежде всего заметим, что для последовательностей второго порядка при $b_0 = -1$ более тщательный анализ равенства (12) приводит к соотношению

$$F_B(-a_n, -a_{n-1}) = F_B(a_n, a_{n-1}) = (\det B)^n = 1^n = 1.$$

Пусть $b_0 = -1$, $b_1 = 3$ и $\lambda^2 - 3\lambda + 1 = 0$. В этом случае

$$F_B(x_0, x_1) = x_0^2 - 3x_0x_1 + x_1^2.$$

В качестве фундаментальной единицы кольца $\mathbf{Z}[\lambda]$ можно взять $\mu = \lambda - 1$. При этом $\lambda = \mu^2$. Из леммы 2 следует, что лишние решения уравнения (13) соответствуют числам $\pm\mu^{2n+1}$. А именно, все лишние решения исчерпываются парами $\langle y_n, z_n\rangle$, $\langle -y_n, -z_n\rangle$, где y_n и z_n определяются из равенства $\mu^{2n+1} = y_n + z_n(\lambda - b_1)$. Заметим, что $\mu^{2n+1} = \mu\lambda^n = (\lambda - 1)\lambda^n = \lambda^{n+1} - \lambda^n$. Представим λ^{n+1} и λ^n согласно лемме 1. Тогда

$$\mu^{2n+1} = a_{n+1} - a_n + (a_n - a_{n-1})(\lambda - b_1),$$

т.е. $y_n = a_{n+1} - a_n$, $z_n = a_n - a_{n-1}$. Учитывая рекуррентное соотношение (2) при $b_1 = 3$, получим, что $y_n = 2a_n - a_{n-1}$. Непосредственное вычисление показывает, что

$$F_B(y_n, z_n) = F_B(-y_n, -z_n) = -F_B(a_n, a_{n-1}) = -1.$$

Таким образом, в этом случае в качестве характеристического соотношения для рассматриваемой последовательности вместо (13) можно взять

$$F_B(x_0, x_1) = 1. \tag{21}$$

Аналогичные рассуждения показывают, что в случае $b_0 = -1$, $b_1 = -3$ в качестве характеристического соотношения можно взять (21).

Замечание 2. Пусть $b_0 = -1$, $|b_1| \neq 3$ и $b_1^2 + 4b_0 > 0$. Согласно теоремам 1 и 2, в этом случае уравнение (13) является характеристическим, т.е. не имеет лишних решений. Но как и в замечании 1 для $b_0 = -1$ имеем $F_B(-a_n, -a_{n-1}) = F_B(a_n, a_{n-1}) = 1$. Значит, уравнение

$$F_B(x_0, x_1) = -1$$

не имеет решения в целых числах, и вместо (13) можно рассматривать более простое характеристическое соотношение (21).

5. Последовательности третьего порядка

Укажем ограничения на коэффициенты b_i в случае последовательностей третьего порядка. Согласно следствию 1 к теореме 1, для того, чтобы соотношение (13) было характеристическим для последовательностей третьего порядка, необходимо, чтобы многочлен f, определенный согласно (6) при $k = 3$, имел в точности один вещественный корень. Хорошо известно (см., например, [8, §26]), что наличие у кубического многочлена f ровно одного вещественного корня равносильно тому, что его дискриминант отрицателен:

$$D = b_1^2 b_2^2 + 4b_1^3 - 4b_0 b_2^3 - 27b_0^2 - 18b_0 b_1 b_2 < 0. \tag{22}$$

Выделим среди таких многочленов приводимые над полем $\mathbf{Q}$. Так как $b_0 = \pm 1$, то вещественный корень f равен 1 или -1, а комплексные корни являются корнями из 1, лежащими в мнимом квадратичном поле (т.е. первообразными корнями из 1 степени 3, 4 или 6).

Все приводимые многочлены f с $b_0 = \pm 1$ и $D < 0$ перечислены в таблице 2.

Таблица 2

f	D
$x^3 - x^2 + x - 1 = (x^2 + 1)(x - 1)$	-16
$x^3 + x^2 + x + 1 = (x^2 + 1)(x + 1)$	-16
$x^3 - 1 = (x^2 + x + 1)(x - 1)$	-27
$x^3 + 2x^2 + 2x + 1 = (x^2 + x + 1)(x + 1)$	-3
$x^3 - 2x^2 + 2x + 1 = (x^2 - x + 1)(x - 1)$	-3
$x^3 + 1 = (x^2 - x + 1)(x + 1)$	-27

Так как дискриминант неприводимого кцбического многочлена не равен $-3, -16, -27$ (см., например, [8, с. 126]), то для исключения приводимого случая достаточно наряду с условием (22) наложить следующее ограничение:

$$D \neq -3, -16, -27. \tag{23}$$

Далее мы покажем, как задача описания исключительных последовательностей сводится к задаче о количестве представлений числа 1 бинарной кубической формой отрицательного дискриминанта. Точные оценки количества таких представлений были получены Б. Н. Делоне; см. [8, гл. VI].

Теорема 4 (Делоне). *Пусть* $c_0 = \pm 1$, $D = c_1^2 c_2^2 + 4c_1^3 - 4c_0 c_2^3 - 27c_0^2 - 18c_0 c_1 c_2 < 0$, $D \neq -3, -16, -27$. *Рассмотрим уравнение*

$$x^3 - c_2 x^2 y - c_1 x y^2 - c_0 y^3 = 1. \qquad (*)$$

1. *Если* $D = -23$, *то уравнение* $(*)$ *имеет* 5 *решение в целых числах.*

2. *Если* $D = -31$ *или* $D = -44$, *то уравнение* $(*)$ *имеет* 4 *решения в целых числах.*

3. *Если* $D < -44$, *то уравнение* $(*)$ *имеет не более трех решений в целых числах.*

Доказательство этой теоремы можно найти в [8, гл. VI].

Согласно теореме 1 и следствию к ней, для описания всех исключительных последовательностей в случае $k = 3$ надо найти все единицы λ в кубических порядках отрицательного дискриминанта, для которых найдейтся другая единица $\mu \in \mathbf{Z}[\lambda]$ такая, что $\lambda = \pm\mu^n$, $|n| \geqslant 2$. Заметим, что вместо μ можно брать $-\mu$. Так как нормы μ и $-\mu$ отличаются знаком, то, не умаляя общности, можно считать, что $N(\mu) = 1$, т.е. свободный коэффициент минимального многочлена для μ равен -1.

Рассмотрим сначала случай, когда дискриминант меньше -44.

Лемма 4. *Пусть* $k = 3$, $c_0 = 1$, $D = c_1^2 c_2^2 + 4c_1^3 - 4c_2^3 - 27 - 18c_1 c_2 < 0$. *Пусть* μ *– корень уравнения*

$$\mu^3 - c_2\mu^2 - c_1\mu - 1 = 0 \qquad (24)$$

и $\lambda = \mu^n$ *или* $\lambda = -\mu^n$ *для некоторого целого* n. *Для того, чтобы* $\mu \in \mathbf{Z}[\lambda]$ *необходимо и достаточно, чтобы выполнялось одно из следующих условий:*

(i) $|n| = 1$;

(ii) $c_1 = 0$, $c_2 \geqslant 2$ *и* $|n| = 2$;

(iii) $c_2 = 0$, $c_1 \leqslant -2$, *и* $|n| = 2$.

Доказательство. Необходимость.

Так как $\lambda = \pm\mu^n \in \mathbf{Z}[\mu]$ и по предположению леммы $\mu \in \mathbf{Z}[\lambda]$, то

$$\mathbf{Z}[\mu] = \mathbf{Z}[\lambda].$$

В частности, $\langle 1, \mu, \mu^2 \rangle$ и $\langle 1, \lambda, \lambda^2 \rangle$ будут базисами одного и того же модуля. Наряду с первым базисом рассмотрим еще один базис этого модуля: $\langle 1, \zeta, \eta \rangle$, где $\zeta = \mu - c_2$, $\eta = \mu^2 - c_2\mu - c_1$. Нетрудно проверить следующие соотношения (напомним, что $c_0 = 1$):

$$\begin{aligned} \mu\zeta &= \eta + c_1, \\ \zeta^2 &= c_1 - c_2\zeta + \eta, \\ \mu\eta &= 1, \\ \zeta\eta &= 1 - c_2\eta, \\ \eta^2 &= \zeta - c_1\eta. \end{aligned} \tag{25}$$

Пусть

$$\lambda = z + x\zeta + y\eta. \tag{26}$$

На основании приведенных выше соотношений проверяем, что

$$\lambda^2 = z^2 + c_1x^2 + 2xy + (-c_2x^2 + y^2 + 2xz)\zeta + (x^2 - c_1y^2 + 2yz - 2c_2xy)\eta.$$

Матрица перехода от базиса $\langle 1, \zeta, \eta \rangle$, к базису $\langle 1, \lambda, \lambda^2 \rangle$ имеет вид

$$C(\lambda) = \begin{pmatrix} 1 & z & z^2 + c_1x^2 + 2xy \\ 0 & x & -c_2x^2 + y^2 + 2xz \\ 0 & y & x^2 - c_1y^2 + 2yz - 2c_2xy \end{pmatrix}.$$

Так как матрица перехода от одного базиса к другому унимодулярна, т.е. является целочисленной матрицей с определителем ± 1 (см., например, [1, гл. 2, §2, п. 1]), то

$$\det C(\lambda) = x^3 - c_2x^2y - c_1xy^2 - y^3 = \pm 1.$$

Так как $\mathbf{Z}[\lambda] = \mathbf{Z}[-\lambda]$, то числа λ и $-\lambda$ или одновременно удовлетворяют или одновременно не удовлетворяют условиям леммы. Поэтому достаточно рассматривать лишь одно из чисел λ и $-\lambda$. Так как

$$C(-\lambda) = C(\lambda) \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

то $\det C(\lambda) = -\det C(-\lambda)$. Поэтому, не умаляя общности, можно считать, что $\det C(\lambda) = 1$, и

$$x^3 - c_2x^2y - c_1xy^2 - y^3 = 1 \tag{27}$$

(иначе заменим λ на $-\lambda$).

Аналогично можно рассмотреть λ^{-1}. Пусть $\lambda^{-1} = r + p\zeta + q\eta$. Как и выше, можно определелить $C(\lambda^{-1})$ – матрицу перехода от базиса $\langle 1, \zeta, \eta\rangle$ к базису $\langle 1, \lambda^{-1}, \lambda^{-2}\rangle$:

$$C(\lambda^{-1}) = \begin{pmatrix} 1 & r & r^2 + c_1p^2 + 2pq \\ 0 & p & -c_2p^2 + q^2 + 2pr \\ 0 & q & p^2 - c_1q^2 + 2qr - 2c_2pq \end{pmatrix}.$$

Покажем, что

$$\det C(\lambda) = -\det C(\lambda^{-1}).$$

Число λ удовлетворяет кубическому уравнению

$$\lambda^3 - b_2\lambda^2 - b_1\lambda - b_0 = 0,$$

где $b_i \in \mathbf{Z}$ и $b_0 = \pm 1$ (так как λ – единица кольца $\mathbf{Z}[\mu]$); в частности, $b_0^{-1} = b_0$. Тогда

$$\lambda^{-1} = b_0\lambda^2 - b_0b_2\lambda - b_0b_1,$$
$$\lambda^{-2} = -b_1\lambda^2 + (b_1b_2 + b_0)\lambda + b_1^2 - b_0b_2.$$

Следовательно, матрица перехода от базиса $\langle 1, \lambda, \lambda^2\rangle$ к базису $\langle 1, \lambda^{-1}, \lambda^{-2}\rangle$ имеет вид

$$C = \begin{pmatrix} 1 & -b_0b_1 & b_1^2 - b_0b_2 \\ 0 & -b_0b_2 & b_1b_2 + b_0 \\ 0 & b_0 & -b_1 \end{pmatrix}.$$

Так как $C(\lambda^{-1}) = C(\lambda)\cdot C$, то $\det C(\lambda^{-1}) = \det C(\lambda)\det C = -b_0^2\det C(\lambda) = -\det C(\lambda) = -1$. Следовательно,

$$p^3 - c_2p^2q - c_1pq^2 - q^3 = -1. \tag{28}$$

Итак, наша задача сведена к исследованию представлений 1 бинарными кубическими формами.

Укажем другие соотношения, которым удовлетворяют числа x, y, z, p, q, r, и которые потребуются в дальнейшем. Так как $(z + x\zeta + y\eta)(r + p\zeta + q\eta) = \lambda\lambda^{-1} = 1$, то, используя таблицу умножения (25) базиса $\langle 1, \zeta, \eta\rangle$, получаем следующие соотношения:

$$zr + c_1xp + xq + yp = 1, \tag{29}$$

$$zp + xr - c_2xp + yq = 0, \tag{30}$$

$$zq + xp - c_2xq - c_2yp + yr - c_1yq = 0. \qquad (31)$$

Так как по предположению леммы $D < -44$, то согласно результату Делоне (см. теорему 4) уравнение (27) имеет не более трех решений в целых числах. Легко указать два из них:

$$\begin{aligned} x &= 1, \quad y = 0; \\ x &= 0, \quad y = -1. \end{aligned} \qquad (32)$$

Будем обозначать третье решение (если оно существует) (X, Y). Заметим, что если пара (x, y) является решением уравнения (27) и $x = 0$ или $y = 0$, то (x, y) совпадает с одним из двух тривиальных решений (32). Следовательно,

$$X \neq 0, \quad Y \neq 0.$$

Решениями уравнения (28) будут $(-1, 0)$, $(0, 1)$ и (если есть третье решение) $(-X, -Y)$.

Рассмотрим возможные комбинации значений x, y, p, q. Отметим, что, вообще говоря, допустимые значения x, y, p, q, не являются независимыми. Действительно, $c = \lambda + \lambda^{-1} \notin \mathbf{Z}$ (иначе λ и λ^{-1} удовлетворяли бы квадратному уравнению с целыми коэффициентами, что невозможно). Поэтому, мы должны исключить 3 случая с $x = -p$, $y = -q$:

$$\begin{aligned} &x = 1, \quad y = 0, \qquad p = -1, \quad q = 0, \\ &x = 0, \quad y = -1, \qquad p = 0, \quad q = 1, \\ &x = X, \quad y = Y, \qquad p = -X, \quad q = -Y. \end{aligned}$$

Остается 6 возможных наборов решений.

Случай 1. $x = 1$, $y = 0$, $p = 0$, $q = 1$. Тогда согласно (31) $z = c_2$. Из (26) и определения η и ζ следует, что $\lambda = c_2 + \zeta = \mu$, т.е. в этом случае $n = 1$.

Случай 2. $x = 0$, $y = -1$, $p = -1$, $q = 0$. Тогда согласно (30) $z = 0$. Из (26) и определения η и ζ следует, что $\lambda = -\eta = -(\mu^2 - c_2\mu - c_1) = -\mu^{-1}$, т.е. в этом случае $n = -1$.

Отметим, что мы уже доказали, что если уравнение (27) имеет лишь два решения, то λ, удовлетворяющее условию теоремы, может принимать лишь тривиальные значения $\pm\mu, \pm\mu^{-1}$.

Рассмотрим те случаи, когда (27) имеет три решения.

Случай 3. $x = 1$, $y = 0$, $p = -X$, $q = -Y$. Согласно (31) $-zY - X + c_2Y = 0$. В частности, $Y \mid X$. Так как (X, Y) – решение уравнения (27), то отсюда заключаем, что $Y = \pm 1$.

(a) $Y = 1$. Подставляя в (27), получаем

$$X^3 - c_2X^2 - c_1X - 1 = 1. \tag{33}$$

Следовательно, $X \mid 2$, и X может принимать лишь значения $\pm 1, \pm 2$. Покажем, что на самом деле получающиеся при этом значения дискриминанта D не меньше -44, т.е. не удовлетворяют условиям леммы.

Если $X = 1$, то согласно (33) имеем $c_1 = -1 - c_2$. Тогда $D = c_2^4 - 6c_2^3 + 7c_2^2 + 6c_2 - 31 = (c_2^2 - 3c_2 - 1)^2 - 32 \geqslant 32$.

Если $X = -1$, то согласно (33) имеем $c_1 = 3 + c_2$. Тогда $D = c_2^4 + 6c_2^3 + 27c_2^2 + 54c_2 + 81 = (c_2^2 + 3c_2 + 9)^2 \geqslant 0$.

Если $X = 2$, то согласно (33) имеем $c_1 = 3 - 2c_2$. Тогда $D = 4c_2^4 - 48c_2^3 + 189c_2^2 - 270c_2 + 81 = (2c_2^2 - 12c_2 + 45/4)^2 - 729/16$. Оценим $|2c_2^2 - 12c_2 + 45/4| = |2(c_2 - 3)^2 - 27/4|$. Для целых c_2 минимум абсолютной величины достигается при $c_2 = 1$ или $c_2 = 5$ и равен $5/4$. Следовательно, $D \geqslant 25/16 - 729/16 = -44$.

Если $X = -2$, то согласно (33) имеем $c_1 = 5 + 2c_2$. Тогда $D = 4c_2^4 + 48c_2^3 + 229c_2^2 + 510c_2 + 473 = (2c_2^2 + 12c_2 + 85/4)^2 + 343/15 > 0$. Случай (a) разобран полностью.

(b) $Y = -1$. Как отмечено выше, $X \neq 0$. Тогда согласно (27) X удовлетворяет уравнению

$$X^2 + c_2X - c_1 = 0. \tag{34}$$

Обозначим второе решение этого уравнения через X'. Так как (1,0), (0,−1), $(X, -1)$ и $(X', -1)$ удовлетворяют (27), и по теореме Делоне при $D < -44$ уравнение (27) имеет не более трех решений, то либо $X = X'$, либо $X' = 0$.

Покажем, что возможность $X = X'$ не имеет места. Если бы $X = X'$, то $c_2^2 + 4c_1 = 0$ согласно (34). При этом $X = -c_2/2$. Так как $x = 1$, $y = 0$, $p = -X = c_2/2$, $q = -Y = 1$, то согласно (31) $z = c_2/2$. Следовательно, $\lambda = c_2/2 + \zeta = \mu - c_2/2$. Но тогда $\lambda^2 = \mu^2 - c_2\mu + c_2^2/4 = \mu^2 - c_2\mu - c_1 = \mu^{-1}$, что противоречит предположению о том, что $\lambda = \pm\mu^n$ при некотором целом n.

Рассмотрим случай $X' = 0$. Тогда $c_1 = 0$ согласно (34), и так как $X \neq 0$, то $X = -c_2$. Определим допустимые значения c_2. Так как $c_1 = 0$, то $D = -4c_2^3 - 27$. Так как мы рассматриваем

$D < -44$, то $c_2 \geqslant 2$. Теперь определим значение n. Согласно (31), поскольку $x = 1$, $y = 0$, $p = -X = c_2$, $q = -Y = 1$, заключаем, что $z = 0$. Следовательно, $\lambda = \zeta = \mu - c_2$. Так как $c_1 = 0$, то $\mu^2\lambda = \mu^2(\mu - c_2) = 1$ и $\lambda = \mu^{-2}$, т.е. $n = -2$.

Случай (b), а вместе с ним и случай 3 разобраны полностью.

Случай 4. $x = 0$, $y = -1$, $p = -X$, $q = -Y$. Согласно (30) $-zX - Y = 0$. В частности, $X \mid Y$. Так как (X, Y) – решение уравнения (27), то отсюда заключаем, что $X = \pm 1$.

(a) $X = -1$. Подставляя в (27), получаем

$$-1 - c_2Y + c_1Y^2 - Y^3 = 1. \tag{35}$$

Следовательно, $Y \mid 2$, и Y может принимать лишь значения $\pm 1, \pm 2$. Как и в случае 3(a) покажем, что дискриминанты $D \geqslant -44$, т.е. не удовлетворяют условиям леммы.

Если $Y = -1$, то согласно (35) имеем $c_2 = 1 - c_1$. Тогда $D = c_1^4 + 6c_1^3 + 7c_1^2 - 6c_1 - 31 = (c_1^2 + 3c_1 - 1)^2 - 32 \geqslant -32$.

Если $Y = 1$, то согласно (35), имеем $c_2 = -3 + c_1$. Тогда $D = c_1^4 - 6c_1^3 + 27c_1^2 - 54c_1 + 81 = (c_1^2 - 3c_1 + 9)^2 \geqslant 0$.

Если $Y = -2$, то согласно (35), имеем $c_2 = -3 - 2c_1$. Тогда $D = 4c_1^4 + 48c_1^3 + 189c_1^2 + 270c_1 + 81 = (2c_1^2 + 12c_1 + 45/4)^2 - 729/16$. Оценим $|2c_1^2 + 12c_1 + 45/4| = |2(c_1+3)^2 - 27/4|$. Для целых c_1 минимум абсолютной величины достигается при $c_1 = -1$ или $c_1 = -5$ и равен $5/4$. Следовательно, $D \geqslant 25/16 - 729/16 = -44$.

Если $Y = 2$, то согласно (35), имеем $c_2 = -5 + 2c_1$. Тогда $D = 4c_1^4 - 48c_1^3 + 229c_1^2 - 510c_1 + 473 = (2c_1^2 - 12c_1 + 85/4)^2 + 343/16 > 0$. Случай (a) разобран полностью.

(b) $X = 1$. Как отмечено выше, $Y \neq 0$. Тогда согласно (27) Y удовлетворяет уравнению

$$Y^2 + c_1Y + c_2 = 0. \tag{36}$$

Обозначим второе решение этого уравнения через Y' (Y' также целое). Так как $(1, 0)$, $(0, -1)$, $(1, Y)$ и $(1, Y')$ удовлетворяют (27), и по теореме Делоне при $D < -44$ уравнение (27) имеет не более трех решений, то либо $Y = Y'$, либо $Y' = 0$.

Покажем, что возможность $Y = Y'$ не имеет места. Если бы $Y = Y'$, то $c_1^2 - 4c_2 = 0$ согласно (36). При этом $Y = -c_1/2$. Так как $x = 0$, $y = -1$, $p = -X = -1$, $q = -Y = c_1/2$, то согласно (30) $z = -c_1/2$. Следовательно, $\lambda = -c_1/2 - \eta = -\mu^2 + c_2\mu + c_1/2 = -\mu^{-1} -$

$c_1/2$. Но тогда $\lambda^2 = \mu^{-2} + c_1\mu^{-1} + c_1^2/4 = \mu^{-2} + c_1\mu^{-1} + c_2 = \mu$, что противоречит предположению о том, что $\lambda = \pm\mu^n$ при некотором целом n. Следовательно, $Y \neq Y'$.

Рассмотрим случай $Y' = 0$. Тогда $c_2 = 0$ согласно (36), и так как $Y \neq 0$, то $Y = -c_1$. Определим допустимые значения c_1. Так как $c_2 = 0$, то $D = 4c_1^3 - 27$. Так как мы рассматриваем $D < -44$, то $c_1 \leqslant -2$. Теперь определим значение n. Согласно(30), поскольку $x = 0$, $y = -1$, $p = -X = -1$, $q = -Y = c_1$, заключаем, что $z = -c_1$. Следовательно, $\lambda = -c_1 - \eta = -\mu^2$ (напомним, что $c_2 = 0$), т.е. $n = 2$.

Случай (b), а вместе с ним и случай 4 разобраны полностью.

Случай 5. $x = X$, $y = Y$, $p = -1$, $q = 0$. Повторяя рассуждения пункта 3, с той лишь разницей, что вместо λ следует рассмотреть $-\lambda^{-1} = -r + \zeta$, получим, что $c_1 = 0$, $c_2 \geqslant 2$, $|n| = 2$.

Случай 6. $x = X$, $y = Y$, $p = 0$, $q = 1$. Повторяя рассуждения пункта 4, с той лишь разницей, что вместо λ следует рассмотреть $-\lambda^{-1} = -r - \eta$, получим, что $c_1 \leqslant -2$, $c_2 = 0$, $|n| = 2$.

Необходимость установлена.

Достаточность. Проверяется непосредственным вычислением. Лемма доказана.

Рассмотрим теперь случай, когда $|D|$ мало. Общая схема повторяет рассуждения леммы 4. Заметим, что достаточно в качестве μ взять ε – одну из фундаментальных единиц соответствующего кольца и найти такие λ, что $\lambda = \pm\varepsilon^n$, $|n| \geqslant 2$ и $\mathbf{Z}[\lambda] = \mathbf{Z}[\varepsilon]$.

В таблице 3 приведены минимальные многочлены фундаментальных единиц в кольцах кубических чисел с дискриминантами -23, -31, -44. Эти фундаментальные единицы взяты из [8, с. 230] (в [8] на самом деле перечислены фундаментальные единицы, обратные к приведенным ниже).

Таблица 3

-23	$\varepsilon^3 - \varepsilon - 1$
-31	$\varepsilon^3 - \varepsilon^2 - 1$
-44	$\varepsilon^3 - \varepsilon^2 - \varepsilon - 1$

Лемма 5. 1. *$D = -23$. Пусть ε удовлетворяет уравнению $\varepsilon^3 - \varepsilon - 1 = 0$ и $\lambda = \varepsilon^n$ или $\lambda = -\varepsilon^n$ для некоторого целого n. Для того, чтобы $\varepsilon \in \mathbf{Z}[\lambda]$ необходимо и достаточно, чтобы $n \in \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 9\}$.*

2. *$D = -31$. Пусть ε удовлетворяет уравнению $\varepsilon^3 - \varepsilon^2 - 1 = 0$ и $\lambda = \varepsilon^n$ или $\lambda = -\varepsilon^n$ для некоторого целого n. Для того, чтобы $\varepsilon \in \mathbf{Z}[\lambda]$ необходимо и достаточно, чтобы $n \in \{\pm 1, \pm 2, \pm 3, \pm 5\}$.*

3. *$D = -44$. Пусть ε удовлетворяет уравнению $\varepsilon^3 - \varepsilon^2 - \varepsilon - 1 = 0$ и $\lambda = \varepsilon^n$ или $\lambda = -\varepsilon^n$ для некоторого целого n. Для того, чтобы $\varepsilon \in \mathbf{Z}[\lambda]$ необходимо и достаточно, чтобы $n \in \{\pm 1, \pm 3\}$.*

Доказательство. Необходимость. $D = -23$. Повторяя рассуждения леммы 4, мы сводим задачу к нахождению единиц $\lambda = z + x\varepsilon + y(\varepsilon^2 - 1)$ таких, что

$$x^3 - xy^2 - y^3 = 1.$$

Все целочисленные решения этого уравнения исчерпываются парами (см. [8, гл. VI, с. 317])

$$\langle 1, 0\rangle, \quad \langle 0, -1\rangle, \quad \langle 1, -1\rangle, \quad \langle -1, -1\rangle, \quad \langle 4, 3\rangle.$$

Так как λ – обратимо в $\mathbf{Z}[\varepsilon]$, то норма λ есть ± 1, т.е.

$$N(z + x\varepsilon + y(\varepsilon^2 - 1)) = \det \begin{pmatrix} z - y & y & x \\ x & z & x + y \\ y & x & z \end{pmatrix} = \pm 1.$$

Подставляя допустимые значения x и y, получаем кубические уравнения относительно z, целочисленные решения которых следует найти. Все решения перечислены в таблице 4. Там же указаны соответствующие значения λ и $g_\lambda(t)$ – минимальный многочлен для λ. Эти значения потребуются далее.

$D = -31$. Аналогично, сводим задачу к нахождению единиц $\lambda = z + x(\varepsilon - 1) + y(\varepsilon^2 - \varepsilon)$ таких, что

$$x^3 - x^2 y - y^3 = 1.$$

Все решения этого уравнения в целых числах исчерпываются парами (см. [8, гл. VI, с. 317])

$$\langle 1, 0\rangle, \quad \langle 0, -1\rangle, \quad \langle -1, -1\rangle, \quad \langle 3, 2\rangle.$$

Так как λ – обратимо в $\mathbf{Z}[\varepsilon]$, то

$$N(z + x(\varepsilon - 1) + y(\varepsilon^2 - \varepsilon)) = \det \begin{pmatrix} -x+z & y & x \\ x-y & -x+z & y \\ y & x & z \end{pmatrix} = \pm 1.$$

Таблица 4

z	x	y	λ	$g_\lambda(t)$
0	1	0	ε	$t^3 - t - 1$
-1	1	0	ε^{-4}	$t^3 + 3t^2 + 2t - 1$
1	1	0	ε^3	$t^3 - 3t^2 + 2t - 1$
1	0	-1	ε^{-5}	$t^3 - 4t^2 + 5t - 1$
-1	0	-1	$-\varepsilon^2$	$t^3 + 2t^2 + t + 1$
0	0	-1	$-\varepsilon^{-1}$	$t^3 - t^2 + 1$
0	1	-1	ε^{-2}	$t^3 - t^2 + 2t - 1$
-1	1	-1	$-\varepsilon^3$	$t^3 + 2t^2 + 3t + 1$
-2	-1	-1	$-\varepsilon^5$	$t^3 + 5t^2 + 4t + 1$
-1	-1	-1	$-\varepsilon^4$	$t^3 + 2t^2 - 3t + 1$
2	-1	-1	$-\varepsilon^{-9}$	$t^3 - 7t^2 + 12t + 1$
5	4	3	ε^9	$t^3 - 12t^2 - 7t - 1$

Как и выше, подставляя допустимые значения x и y, находим целые значения z. Все решения перечислены в таблице 5.

Таблица 5

z	x	y	λ	$g_\lambda(t)$
0	1	0	ε^{-2}	$t^3 + 2t^2 + t - 1$
1	1	0	ε	$t^3 - t^2 - 1$
1	0	-1	ε^{-3}	$t^3 - 3t^2 + 4t - 1$
0	0	-1	$-\varepsilon^{-1}$	$t^3 + t + 1$
-2	-1	-1	$-\varepsilon^3$	$t^3 + 4t^2 + 3t + 1$
-1	-1	-1	$-\varepsilon^{-2}$	$t^3 - 2t^2 + t + 1$
1	-1	-1	$-\varepsilon^{-5}$	$t^3 - 5t^2 + 6t + 1$
4	3	2	ε^5	$t^3 - 6t^2 - 5t - 1$

$D = -44$. Аналогично, сводим задачу к нахождению единиц $\lambda = z + x(\varepsilon - 1) + y(\varepsilon^2 - \varepsilon - 1)$ таких, что

$$x^3 - x^2y - xy^2 - y^3 = 1.$$

Все решения этого уравнения в целых числах исчерпываются парами (см. [8, гл. VI, с. 317])

$$\langle 1,0\rangle,\quad \langle 0,-1\rangle,\quad \langle 2,1\rangle,\quad \langle -103,-56\rangle.$$

Так как λ – обратимо в $\mathbf{Z}[\varepsilon]$, то

$$\det\begin{pmatrix} -x-y+z & y & x \\ x-y & -x+z & x+y \\ y & x & z \end{pmatrix} = \pm 1.$$

Как и выше, подставляя допустимые значения x и y, находим целые значения z. Все решения перечислены в таблице 6.

Таблица 6

z	x	y	λ	$g_\lambda(t)$
1	1	0	ε	t^3-t^2-t-1
-1	1	0	$-\varepsilon^{-3}$	t^3+5t^2+7t+1
0	0	-1	$-\varepsilon^{-1}$	t^3-t^2+t+1
4	2	1	ε^3	t^3-7t^2+5t-1

Необходимость установлена.

Достаточность. Непосредственно проверяется, что в каждом случае для всех перечисленных в условии леммы значений n, дискриминант порядка $\mathbf{Z}[\pm\lambda]$ совпадает с дискриминантом содержащего его максимального порядка (т.е. с $-23, -31, -44$, соответственно). Следовательно, $\mathbf{Z}[\pm\lambda]$ совпадает с максимальным порядком соответствующего поля и $\varepsilon \in \mathbf{Z}[\pm\lambda]$. Достаточность установлена.

Теорема 5. *Пусть λ удовлетворяет уравнению $\lambda^3 - b_2\lambda^2 - b_1\lambda - b_0 = 0$, где $b_0 = \pm 1$, $D = b_1^2 b_2^2 + 4b_1^3 - 4b_0 b_2^3 - 27b_0^2 - 18b_0 b_1 b_2 < 0$, $D \neq -3, -16, -27$.*

1. *Если $\langle b_0, b_1, b_2\rangle$ совпадает с одной из троек*

$$\begin{array}{cccc} \langle 1,-2,1\rangle, & \langle 1,-1,2\rangle, & \langle -1,-2,-1\rangle, & \langle -1,-1,-2\rangle, \\ \langle 1,2,1\rangle, & \langle 1,-1,-2\rangle, & \langle -1,2,-1\rangle, & \langle -1,-1,2\rangle, \\ \langle 1,2t,t^2\rangle, & \langle 1,-t^2,-2t\rangle, & \langle -1,2t,-t^2\rangle, & \langle -1,-t^2,2t\rangle, \end{array}$$

где $t \geqslant 2$, то $[(\mathbf{Z}[\lambda])^* : \langle \pm\lambda^n \mid n \in \mathbf{Z}\rangle] = 2$.

2. *Если* $\langle b_0, b_1, b_2\rangle$ *совпадает с одной из троек*

$$\langle 1,-2,3\rangle,\quad \langle 1,-3,2\rangle,\quad \langle -1,-2,-3\rangle,\quad \langle -1,-3,-2\rangle,$$
$$\langle 1,-3,4\rangle,\quad \langle 1,-4,3\rangle,\quad \langle -1,-3,-4\rangle,\quad \langle -1,-4,-3\rangle,$$
$$\langle 1,-5,7\rangle,\quad \langle 1,-7,5\rangle,\quad \langle -1,-5,-7\rangle,\quad \langle -1,-7,-5\rangle,$$

то $[(\mathbf{Z}[\lambda])^* : \langle \pm\lambda^n \mid n \in \mathbf{Z}\rangle] = 3$.

3. *Если* $\langle b_0, b_1, b_2\rangle$ *совпадает с одной из троек*

$$\langle 1,3,2\rangle,\quad \langle 1,-2,-3\rangle,\quad \langle -1,3,-2\rangle,\quad \langle -1,-2,3\rangle,$$

то $[(\mathbf{Z}[\lambda])^* : \langle \pm\lambda^n \mid n \in \mathbf{Z}\rangle] = 4$.

4. *Если* $\langle b_0, b_1, b_2\rangle$ *совпадает с одной из троек*

$$\langle 1,5,6\rangle,\quad \langle 1,-6,-5\rangle,\qquad \langle -1,5,-6\rangle,\quad \langle -1,-6,5\rangle,$$
$$\langle 1,-4,5\rangle,\quad \langle 1,-5,4\rangle,\qquad \langle -1,-4,-5\rangle,\quad \langle -1,-5-4\rangle,$$

то $[(\mathbf{Z}[\lambda])^* : \langle \pm\lambda^n \mid n \in \mathbf{Z}\rangle] = 5$.

5. *Если* $\langle b_0, b_1, b_2\rangle$ *совпадает с одной из троек*

$$\langle 1,7,12\rangle,\quad \langle 1,-12,-7\rangle,\quad \langle -1,7,-12\rangle,\quad \langle -1,-12,7\rangle,$$

то $[(\mathbf{Z}[\lambda])^* : \langle \pm\lambda^n \mid n \in \mathbf{Z}\rangle] = 9$.

6. *Во всех остальных случаях* $(\mathbf{Z}[\lambda])^* = \langle \pm\lambda^n \mid n \in \mathbf{Z}\rangle$.

Доказательство. Перечисленные в пунктах 1–5 тройки $\langle b_0, b_1, b_2\rangle$ являются коэффициентами минимальных многочленов тех λ (либо $-\lambda$) из лемм 4 и 5, для которых $\lambda = \pm\mu^n$, $|n| \geqslant 2$ и $\mu \in \mathbf{Z}[\lambda]$.

Теорема 6. *Пусть* $k = 3$ *и последовательность* a_n *определена согласно* (2)–(3). *Пусть* $D = b_1^2 b_2^2 + 4b_1^3 - 4b_0 b_2^3 - 27b_0^2 - 18b_0 b_1 b_2 < 0$, $D \neq -3, -16, -27$. *Для того, чтобы соотношение* (13) *было характеристическим для данной последовательности необходимо и достаточно, чтобы тройка* $\langle b_0, b_1, b_2\rangle$ *не совпадала ни с одной из троек, в перечисленных пунктах* 1–5 *теоремы* 5.

Доказательство. Непосредственно следует из теорем 1 и 5.

Перейдем теперь к построению $\mathbf{Z}$-диофантовых представлений множеств значений последовательностей третьего порядка.

Для фиксированных коэффициентов b_0, b_1, b_2 рекуррентного соотношения (2) при $k = 3$ определим множества

$$\mathcal{M}(b_0, b_1, b_2) = \{\langle y_0, y_1, y_2\rangle : \exists n \in \mathbf{Z}\ [y_i = a_{n-i},\ i = 0,1,2]\} \tag{37}$$

$$\mathcal{M}^+(b_0, b_1, b_2) = \{\langle y_0, y_1, y_2\rangle : \exists n \in \mathbf{N}\ [y_i = a_{n-i},\ i = 0,1,2]\}. \tag{38}$$

Теорема 7. *Пусть b_0, b_1, b_2 таковы, как и в теореме 5. Пусть последовательность a_n определена согласно (2)–(3), а множества $\mathcal{M}$ и $\mathcal{M}^+$ определены согласно (37), (38).*

1. *Для того чтобы $\langle y_0, y_1, y_2\rangle \in \mathcal{M}(b_0, b_1, b_2)$ необходимо и достаточно, чтобы существовали целые x_0, x_1, x_2 такие, что выполнено (13) и*

$$\bigvee_{i=1}^{360}\{A(y_0, y_1, y_2) = B^i(A(x_0, x_1, x_2))^{360}\}, \tag{39}$$

где матрицы B и $A(x_0, x_1, x_2)$ определены согласно (8) и (9), соответственно.

2. *Для того чтобы $\langle y_0, y_1, y_2\rangle \in \mathcal{M}^+(b_0, b_1, b_2)$ необходимо и достаточно, чтобы существовали целые x_0, x_1, x_2 такие, что выполнены (13) и (39) и*

$$\det((A^2(y_0, y_1, y_2) - E)(B^2 - E)) > 0. \tag{40}$$

Доказательство. Возьмем λ такое, как в условии теоремы 5. Пусть $\xi \in (\mathbf{Z}[\lambda])^*$. Покажем, что для того чтобы $\xi = \lambda^n$ при некотором $n \in \mathbf{Z}$ необходимо и достаточно, чтобы нашлись $\mu \in (\mathbf{Z}[\lambda])^*$ и $i \in \{1, 2, \ldots, 360\}$ такие, что

$$\xi = \lambda^i \mu^{360}. \tag{41}$$

Пусть нашлись такие i и μ. Согласно теореме 5 индекс подгруппы $\langle \lambda^n \mid n \in \mathbf{Z}\rangle$ в группе $(\mathbf{Z}[\lambda])^*$ делит 360. Следовательно, $\mu^{360} \in \langle \lambda^n \mid n \in \mathbf{Z}\rangle$ и $\xi \in \langle \lambda^n \mid n \in \mathbf{Z}\rangle$. Обратно, если $\xi = \lambda^n$, то достаточно взять $i \equiv n \pmod{360}$, $1 \leqslant i \leqslant 360$ и $\mu = \lambda^{\frac{n-i}{360}}$.

Запишем $\xi = y_0 + y_1(\lambda - b_2) + y_2(\lambda^2 - b_2\lambda - b_1)$, $\mu = x_0 + x_1(\lambda - b_2) + x_2(\lambda^2 - b_2\lambda - b_1)$. Применяя к равенству (41) мономорфизм T, определенный в §3, мы завершаем доказательство первого утверждения.

Для доказательства второго утверждения заметим, что λ является собственным числом матрицы B, а $\xi = y_0 + y_1(\lambda - b_2) + y_2(\lambda^2 - b_2\lambda - b_1)$ – собственным числом матрицы $A(y_0, y_1, y_2)$, причем каждая из этих матриц имеет в точности одно вещественное собственное число. Согласно первому пункту теоремы условие (39) равносильно тому, что $\xi = \lambda^n$ для некоторого целого n. Условие (40) означает, что вещественные собственные числа матриц $A(y_0, y_1, y_2) = B^n$ и B либо одновременно лежат в интервале $(-1, 1)$, либо одновременно лежат вне него. Это равносильно тому, что $n > 0$. Теорема доказана.

Замечание. Если ограничиться только теми последовательностями, для которых (13) является характеристическим, то можно построить более простые $\mathbf{Z}$-диофантовы представления множеств $\mathcal{M}(b_0, b_1, b_2)$ и $\mathcal{M}^+(b_0, b_1, b_2)$. Действительно, так как в этом случае

$$[(\mathbf{Z}[\lambda])^* : \langle \lambda^n \mid n \in \mathbf{Z} \rangle] = [\langle \pm\lambda^n \mid n \in \mathbf{Z} \rangle : \langle \lambda^n \mid n \in \mathbf{Z} \rangle] = 2,$$

то в теореме 7 можно заменить 360 на 2. С другой стороны, приведенная выше формулировка позволяет охватить все возможные случаи.

Литература

1. З. И. Боревич, И. Р. Шафаревич, *Теория чисел.* М., Наука, 1972, 496 с.
2. М. А. Всемирнов, *О диофантовых представлениях линейных рекуррентных последовательностей.* II Международная конференция: Алгебраические, вероятностные, геометрические, комбинаторные и функциональные методы в теории чисел. Тезисы докладов. Воронеж, 1995, 36.
3. М. А. Всемирнов, *Диофантовы представления линейных рекуррентных последовательностей. I.* — Зап. научн. семинаров ПОМИ **227** (1995), 52–60.
4. М. А. Всемирнов, *Прямые методы построения диофантовых представлений линейных рекуррентных последовательностей.* Материалы международной конференции и Чебышевских чтений, посвященных 175-летию со дня рождения П. Л. Чебышева. М., изд-во МГУ, 1996, Т. 1, 101–103.
5. M. A. Vsemirnov, *Diophantine representations of linear recurrent sequences of small orders.* Number Theory conference: Abstracts. Eger (Hungary), 1996, 40–41.
6. M. Davis, *An explicit diophantine definition of the exponential function.* — Comm. Pure Appl. Math. **24**, No. **2** (1971), 137–145.
7. M. Davis, H. Putnam, J. Robinson, *The decision problem for exponential diophantine equations.* — Ann. Math. **74**, No. **3** (1961), 425–436.
8. Б. Н. Делоне, Д. К. Фаддеев, *Теория иррациональностей третьей степени.* — Тр. МИАН СССР **11** (1940).
9. P. Kiss, *On some properties of linear recurrences.* — Publ. Math. **30** (1983), 273–281.
10. Н. К. Косовский, *О диофантовых представлениях последовательности решений уравнения Пелля.* — Зап. научн. семин. ЛОМИ **20** (1971), 49–59.
11. Ю. В. Матиясевич, *Диофантовость перечислимых множеств.* — Доклады АН СССР **191, No. 2** (1970), 278–282.
12. Ю. В. Матиясевич, *Десятая проблема Гильберта.* М., Физматлит, 1993, 224 с.

13. Yu. V. Matijasevič, J. Robinson, *Reduction of an arbitrary diophantine equation to one in 13 unknowns.* — Acts Arithmetica **27** (1975), 521–553.
14. Г. В. Чудновский, *Диофантовы предикаты.* — Успехи мат. наук **25, No. 4** (1970), 185–186.

Vsemirnov M. A. Diophantine representations of linear recurrent sequences. II.

Direct constructions of diophantine representations of linear recurrent sequences are considered. Diophantine representations of the sets of values of third-order sequences with negative discriminant are found. As an auxiliary problem we study the structure of the multiplicative group of the ring $\mathbf{Z}[\lambda]$, where λ is an invertible algebraic number (unit) in a real quadratic field or in a cubic field of a negative discriminant. Tge index of the subgroup $\langle \pm\lambda^n \mid n \in \mathbf{Z}\rangle$ in the group $(\mathbf{Z}[\lambda])^*$ and the generator of $(\mathbf{Z}[\lambda])^*$ are evaluated explicitly.

Санкт-Петербургское отделение
Математичекого института
им. В. А. Стеклова РАН

Поступило 10 октября 1997 г.