Math-Net.Ru

Общероссийский математический портал

А. Ю. Нестеренко, Нахождение целочисленных решений системы связанных уравнений Пелля, *Матем. заметки*, 2009, том 86, выпуск 4, 588–600

DOI: <https://doi.org/10.4213/mzm4068>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением <http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.162.127.20

26 апреля 2023 г., 07:22:08

УДК 511.5

Нахождение целочисленных решений системы связанных уравнений Пелля

А. Ю. Нестеренко

В работе описывается алгоритм, позволяющий находить целочисленные решения системы связанных уравнений Пелля, эффективные оценки которых могут быть найдены с помощью теории линейных форм от логарифмов алгебраических чисел. Мы используем оценку Е. М. Матвеева для форм от трех логарифмов. Для уменьшения полученной оценки используется итерационный алгоритм. В заключение работы приведены результаты практической реализации предложенного алгоритма.

Библиография: 12 названий.

Введение

В данной работе описывается алгоритм, позволяющий находить целочисленные решения системы связанных уравнений Пелля или, по-другому, тройки целых чисел (x, y, z) , удовлетворяющих системе

$$\begin{cases} x^2 - (2k + 1)z^2 = k^2, \\ y^2 - (2l + 1)z^2 = l^2, \end{cases} \quad (1)$$

где параметры l, k – различные натуральные числа. Эта система диофантовых уравнений возникла в связи с некоторыми исследованиями в дифференциальной геометрии [1].

Поскольку все неизвестные входят в уравнения в четной степени, мы ограничимся поиском только положительных чисел x, y, z , удовлетворяющих системе (1). Мы не будем рассматривать те значения параметров, при которых значения $2k + 1$ или $2l + 1$ являются полным квадратом. В этом случае левая часть каждого уравнения является произведением двух различных линейных форм и неизвестные значения x, y, z находятся простым перебором делителей чисел k, l .

Мы также не будем рассматривать параметры, удовлетворяющие равенству

$$2k + 1 = r^2(2l + 1), \quad \text{где } r \in \mathbb{Q}.$$

В этом случае путем исключения переменной z можно перейти к одному квадратному уравнению от переменных x, y , значения которых также находятся простым перебором.

Для данной системы уравнений (1) можно сразу предъявить две тривиальные тройки решений: $(k, l, 0)$ и $(k + 1, l + 1, 1)$. Поиску всех остальных решений системы посвящена оставшаяся часть работы. Изложение состоит из нескольких частей. В разделе 1 работы приведен хорошо известный алгоритм нахождения решений одного уравнения системы. Используя аппарат непрерывных дробей и вычисления в квадратичных полях, мы получим несколько независимых бесконечных серий решений для каждого уравнения.

В разделе 2 работы мы получим первоначальную оценку сверху для величины возможных решений системы (1). Для этого будут использованы оценки линейных форм от трех логарифмов алгебраических чисел.

В разделе 3 работы приведен алгоритм, использующий вычисления с подходящими дробями иррациональных чисел и позволяющий уменьшить полученную ранее оценку.

В заключение работы приведены результаты практической реализации предложенного алгоритма.

Отметим ряд статей, посвященных решению связанных уравнений Пелля. Первой работой, в которой была описана общая для всех последующих алгоритмов схема, явилась публикация Бейкера и Дэвенпорта [2]. В дальнейшем, появились работы Гринстида [3], Пинча [4] и Англина [5], использующие схожие методы нахождения решений. Данная работа может рассматриваться как продолжение перечисленных публикаций.

1. Представление квадратичными формами

Пусть $k \geq 1$ – натуральное число такое, что $2k + 1$ не является полным квадратом. Опишем метод нахождения всех целых положительных чисел x, z , удовлетворяющих равенству

$$x^2 - (2k + 1)z^2 = k^2. \quad (2)$$

Другими словами, нам надо найти все целочисленные представления числа k^2 квадратичной формой $x^2 - (2k + 1)z^2$.

В общем виде для произвольной квадратичной формы решение было найдено еще Гауссом. Предложенный Гауссом метод, описание которого можно найти в книгах Венкова [6] или Дэвенпорта [7], использует преобразования эквивалентных квадратичных форм и находит решение в виде

$$x_{n+1} = f(x_n, z_n), \quad z_{n+1} = g(x_n, z_n),$$

где $f(x), g(z)$ – некоторые линейные функции, зависящие от коэффициентов квадратичной формы, а (x_n, z_n) удовлетворяют равенству (2).

В данной работе излагается хорошо известный метод, основанный на разложении в непрерывную дробь квадратичных иррациональностей. Данный метод аналогичен методу Гаусса, но на практике более эффективен.

Следующая теорема, являющаяся следствием изложенной в [8] теории, позволяет находить все целочисленные представления натурального числа произвольной квадратичной формой.

ТАБЛИЦА 1

	Знак $N(\alpha)$	Знак $N(\varepsilon)$	Серия решений
1	$N(\alpha) > 0$	$N(\varepsilon) = 1$	$\pm \alpha \varepsilon^n$
2	$N(\alpha) > 0$	$N(\varepsilon) = -1$	$\pm \alpha \varepsilon^{2n}$
3	$N(\alpha) < 0$	$N(\varepsilon) = 1$	решений нет
4	$N(\alpha) < 0$	$N(\varepsilon) = -1$	$\pm \alpha \varepsilon^{2n+1}$

ТЕОРЕМА 1. Рассмотрим произвольную квадратичную форму $ax^2 + bxz + cz^2$ с целыми коэффициентами, $(a, b, c) = 1$, $a > 0$, представляющую целое число $m > 0$. Пусть γ и $\bar{\gamma}$ – корни многочлена $at^2 + bt + c$ с условием $\gamma - \bar{\gamma} > 0$, $D = b^2 - 4ac$ – положительное, отличное от квадрата число. Тогда существует взаимнооднозначное соответствие между классами решений $\alpha = x - \gamma z \in \mathbb{Z} + \gamma\mathbb{Z}$ уравнения $a|N(\alpha)| = m$ и числами $\beta \in \mathbb{Q}(\sqrt{D})$, удовлетворяющими следующим условиям:

1) β эквивалентно γ , т.е.

$$\gamma = \frac{\lambda\beta + \mu}{\nu\beta + \rho},$$

где λ, μ, ν, ρ – целые числа, удовлетворяющие равенству $\lambda\rho - \mu\nu = \pm 1$;

2) пусть известно разложение $m = us^2$, $s \in \mathbb{Z}$, $s > 0$; тогда число β является корнем некоторого квадратного трехчлена $ut^2 + vt + w$ с целыми коэффициентами, $(u, v, w) = 1$, и представимо в виде

$$\beta = \frac{-v + \sqrt{D}}{2u},$$

где

$$v^2 - 4uw = D, \quad -u \leq v < u.$$

При этом $\alpha = (us/a)(\nu\beta + \rho)$ – представитель класса решений, соответствующего числу β .

В нашем случае квадратичная форма имеет вид $x^2 - (2k+1)z^2$, и мы будем представлять ею число $m = k^2$. Дискриминант D равен $4(2k+1)$ и $\gamma = \sqrt{2k+1}$. Применяя утверждения теоремы, мы будем находить числа $\alpha = x - z\sqrt{2k+1}$ такие, что $x, z \in \mathbb{Z}$ и $|N(\alpha)| = k^2$.

Далее, пусть ε – основная единица модуля $\{1, \sqrt{2k+1}\}$, которому принадлежит α . Тогда для любого $n \in \mathbb{Z}$ выполнено $|N(\alpha\varepsilon^n)| = k^2$. Таким образом, α образует бесконечную серию представлений числа k^2 , задаваемую таблицей 1.

Основываясь на приведенной таблице, будем считать, что бесконечная серия представлений числа k^2 имеет вид $\alpha\varepsilon_1^n$, $\alpha > 0$, в случае, когда она существует, где

$$\varepsilon_1 := \begin{cases} \varepsilon, & \text{для случая 1,} \\ \varepsilon^2, & \text{для случая 2,} \\ \varepsilon^2, \alpha := \alpha\varepsilon, & \text{для случая 4.} \end{cases}$$

В заключение заметим, что бесконечные серии представлений числа l^2 для второго уравнения системы (1) находятся аналогично.

2. Оценки числа решений

Вернемся к системе (1)

$$\begin{cases} x^2 - (2k+1)z^2 = k^2, \\ y^2 - (2l+1)z^2 = l^2. \end{cases}$$

Напомним, что мы ищем решения в целых неотрицательных числах. Решения первого уравнения системы представляются в виде

$$x + z\sqrt{2k+1} = \alpha\varepsilon_1^n,$$

где α – представитель одной из серий решений первого уравнения системы, а ε_1 – указанная в разделе 1 единица модуля $\{1, \sqrt{2k+1}\}$. Из этого равенства можно получить выражение для переменной z :

$$z = \frac{\alpha\varepsilon_1^n - \bar{\alpha}\bar{\varepsilon}_1^n}{2\sqrt{2k+1}}, \quad n \in \mathbb{Z}, \quad (3)$$

где $\bar{\alpha}$ – число, сопряженное к $\alpha \in \mathbb{Q}(\sqrt{2k+1})$.

Аналогично, из второго уравнения системы (1) можно получить равенство

$$z = \frac{\beta\varepsilon_2^m - \bar{\beta}\bar{\varepsilon}_2^m}{2\sqrt{2l+1}}, \quad m \in \mathbb{Z}, \quad (4)$$

где β – представитель одной из серий решений второго уравнения системы, $\bar{\beta}$ – число, сопряженное к $\beta \in \mathbb{Q}(\sqrt{2l+1})$, а ε_2 – единица модуля $\{1, \sqrt{2l+1}\}$.

Кроме того, выполнены следующие свойства:

$$\varepsilon_i > 1, \quad \bar{\varepsilon}_i = \varepsilon_i^{-1}, \quad i = 1, 2,$$

а также

$$\alpha\bar{\alpha} = k^2, \quad \alpha, \bar{\alpha} > 0, \quad \beta\bar{\beta} = l^2, \quad \beta, \bar{\beta} > 0.$$

Будем также считать, без ограничения общности, что выполнено неравенство

$$\varepsilon_1 < \varepsilon_2.$$

Приравнявая выражения (3) и (4) для переменной z , получим

$$\frac{\alpha\varepsilon_1^n}{\sqrt{2k+1}} - \frac{\beta\varepsilon_2^m}{\sqrt{2l+1}} = \frac{\bar{\alpha}\bar{\varepsilon}_1^n}{\sqrt{2k+1}} - \frac{\bar{\beta}\bar{\varepsilon}_2^m}{\sqrt{2l+1}}. \quad (5)$$

В случае, если найдутся целые n и m , удовлетворяющие этому равенству, мы сможем вычислить значение z и, далее, x, y .

Поскольку $z \geq 0$, то из (3) и (4) вытекают нижние оценки для индексов n и m :

$$n \geq H_1, \quad m \geq H_2,$$

где H_1, H_2 – наименьшие целые числа, удовлетворяющие неравенствам

$$H_1 \geq \frac{\log \bar{\alpha} - \log \alpha}{2 \log \varepsilon_1}, \quad H_2 \geq \frac{\log \bar{\beta} - \log \beta}{2 \log \varepsilon_1}. \quad (6)$$

2.1. Определение максимального индекса. Обозначим члены, стоящие в левой части равенства (5),

$$P = \frac{\alpha \varepsilon_1^n}{\sqrt{2k+1}}, \quad Q = \frac{\beta \varepsilon_2^m}{\sqrt{2l+1}}.$$

Сразу заметим, что величины P, Q принимают положительные значения при любых $n, m \in \mathbb{Z}$. Оценим эти величины снизу. Пусть R – наименьшее целое число, удовлетворяющее неравенству

$$R > \max\{0, 2H_1, 2H_2\}, \quad (7)$$

где H_1, H_2 определяются неравенствами (6). Тогда выполнено

$$\bar{\alpha} < \alpha \varepsilon_1^R, \quad \bar{\beta} < \beta \varepsilon_2^R.$$

В дальнейшем будем считать, что $n, m \geq R$. В противном случае мы получаем оценку сверху для индексов n и m .

Поскольку для любого $k \geq 1$ выполнено неравенство

$$2k+1 \leq 3k^2 = 3\alpha\bar{\alpha} < 3\alpha^2\varepsilon_1^R \quad \text{или} \quad \frac{\alpha}{\sqrt{2k+1}} > (3\varepsilon_1^R)^{-1/2}, \quad (8)$$

то при $n \geq R$ верна нижняя оценка $P \geq \sqrt{\varepsilon_1^R/3}$. Аналогично, при $m \geq R$, используя неравенство для l и β , можно получить нижнюю оценку $Q \geq \sqrt{\varepsilon_2^R/3}$.

Кроме того,

$$k = \sqrt{\alpha\bar{\alpha}} > \bar{\alpha}(\varepsilon_1^R)^{-1/2}. \quad (9)$$

Исходя из соотношений (5) и (9), получим оценку

$$|P - Q| = \left| \frac{\bar{\alpha}}{\varepsilon_1^n \sqrt{2k+1}} - \frac{\bar{\beta}}{\varepsilon_2^m \sqrt{2l+1}} \right| < k + l =: M. \quad (10)$$

Поскольку k, l – различные числа, удовлетворяющие неравенствам $k \geq 1, l \geq 1$, для M верна оценка снизу

$$M \geq 3. \quad (11)$$

ЛЕММА 1. Пусть выполнено неравенство $\varepsilon_1 < \varepsilon_2$ и $n \geq R, m \geq R$. Тогда существует константа D , зависящая от k и l , такая, что либо $D > m \geq n$, либо $n > m$. Можно выбрать D как наименьшее целое, удовлетворяющее неравенству

$$D > \frac{|\log \gamma| + \log(2M+1)}{\log \varepsilon_2 - \log \varepsilon_1}, \quad \text{где} \quad \gamma = \frac{\alpha \sqrt{2l+1}}{\beta \sqrt{2k+1}}. \quad (12)$$

ДОКАЗАТЕЛЬСТВО. Предположим, что $m \geq n$. Тогда выполнено неравенство

$$\log \frac{P}{Q} = \log \left(\frac{\alpha \varepsilon_1^n \sqrt{2l+1}}{\beta \varepsilon_2^m \sqrt{2k+1}} \right) \leq \log \left(\gamma \left(\frac{\varepsilon_1}{\varepsilon_2} \right)^m \right).$$

Поскольку выполнено неравенство (10) и $P \geq \sqrt{\varepsilon_1^R/3}$, получим неравенство

$$m(\log \varepsilon_2 - \log \varepsilon_1) \leq \log \gamma + \log \frac{Q}{P} \leq \log \gamma + \log \left(1 + \sqrt{\frac{3}{\varepsilon_1^R}} M \right) < \log \gamma + \log(2M+1),$$

и для индекса m верна следующая оценка сверху:

$$m < \frac{|\log \gamma| + \log(2M + 1)}{\log \varepsilon_2 - \log \varepsilon_1},$$

которая и завершает доказательство леммы.

Дальнейшие рассуждения будем производить, считая, что $n > m$.

Теперь, используя обозначения P и Q , получим линейную форму от трех логарифмов

$$\Lambda = \log \frac{P}{Q} = \log \frac{\alpha \varepsilon_1^n \sqrt{2l+1}}{\beta \varepsilon_2^m \sqrt{2k+1}} = n \log \varepsilon_1 - m \log \varepsilon_2 + \log \frac{\alpha \sqrt{2l+1}}{\beta \sqrt{2k+1}},$$

или

$$\Lambda = n \log \varepsilon_1 - m \log \varepsilon_2 + \log \gamma, \quad (13)$$

где γ определяется утверждением леммы 1.

2.2. Верхняя оценка линейной формы. Выберем константу C следующим образом:

$$C = \max \left(2, D, R + \frac{\log 4M}{\log \varepsilon_1} \right), \quad (14)$$

где величина R определяется из неравенства (7), величина D – из неравенства (12), а величина M определяется равенством (10).

Далее мы будем рассматривать случай, когда $n > C$. Если это не верно, то мы автоматически получаем оценку сверху для индекса n .

При $n > C$ имеем

$$\varepsilon_1^n > \varepsilon_1^C \geq 4M \varepsilon_1^R,$$

тогда, учитывая неравенство (8), получим

$$P = \frac{\alpha \varepsilon_1^n}{\sqrt{2k+1}} > 4M \sqrt{\frac{\varepsilon_1^R}{3}} > 2M. \quad (15)$$

Кроме того, из полученной оценки и неравенства (10) следует, что

$$\frac{|P - Q|}{P} < \frac{M}{P} < \frac{1}{2}, \quad (16)$$

откуда следует оценка $Q > P/2$.

Далее, учитывая соотношения (5) и (10), оценим еще раз модуль разности P и Q :

$$|P - Q| = \left| \frac{k^2}{2k+1} P^{-1} - \frac{l^2}{2l+1} Q^{-1} \right| < \frac{k+2l}{2} P^{-1} < \frac{M}{P}.$$

Учитывая полученную оценку, а также (13), (8), (11), (15), (16) и (14) находим

$$\begin{aligned} |\Lambda| &= \left| \log \left(1 - \frac{P - Q}{P} \right) \right| < \frac{|P - Q|}{P} + \frac{|P - Q|^2}{P^2} \\ &< P^{-2} (M + 1) = \frac{(2k+1)(M+1)}{\alpha^2} \varepsilon_1^{-2n} < 3\varepsilon_1^R (M+1) \varepsilon_1^{-2n} \leq \varepsilon_1^{-n}. \end{aligned}$$

Таким образом, выполнено окончательное неравенство

$$|\Lambda| < \varepsilon_1^{-n}. \quad (17)$$

2.3. Нижняя оценка линейной формы. Получение нижней оценки модуля линейной формы является далеко не тривиальной задачей. Классический результат принадлежит Бейкеру [8]. В работе Беннета [9], посвященной нахождению числа решений связанных уравнений Пелля, использовалась оценка Вальдшмидта [10].

В настоящей работе автором используется несколько лучшая оценка Матвеева [11], полученная для произвольного числа логарифмов. Мы сформулируем теорему Матвеева для случая трех логарифмов.

Пусть $\mathbb{K}$ – алгебраическое поле степени 4 над $\mathbb{Q}$, вложенное в $\mathbb{R}$. Даны отличные от нуля числа $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{K}$, имеющие абсолютные логарифмические высоты $h(\alpha_1), h(\alpha_2), h(\alpha_3)$. Абсолютная логарифмическая высота $h(\alpha)$ определяется следующим способом:

$$h(\alpha) = \frac{1}{r} \log \left(a_r \prod_j \max\{1, \alpha^{(j)}\} \right),$$

где r – степень основного многочлена числа α , a_r – коэффициент при старшем члене, $\alpha^{(j)}$ – сопряженные с α .

Рассмотрим линейную форму

$$\Lambda = b_1 \log \alpha_1 + b_2 \log \alpha_2 + b_3 \log \alpha_3, \quad (18)$$

где $b_1, b_2, b_3 \in \mathbb{Z}$, и обозначим

$$A_i \geq \max\{4h(\alpha_i), |\log \alpha_i|\}, \quad 1 \leq i \leq 3, \quad B = \max\left\{1, \max\left\{|b_i| \frac{A_i}{A_3}, 1 \leq i \leq 3\right\}\right\}.$$

ТЕОРЕМА 2 [11]. Если $\log \alpha_1, \log \alpha_2, \log \alpha_3$ линейно независимы над $\mathbb{Z}$ и $b_3 \neq 0$, то линейная форма (18) удовлетворяет неравенству

$$\log |\Lambda| > -3.1 \cdot 10^{11} A_1 A_2 A_3 \log(39B).$$

Согласно (13) мы будем использовать теорему в случае, когда числа $\alpha_1, \alpha_2, \alpha_3$ равны соответственно $\varepsilon_1, \varepsilon_2, \gamma$, а целые числа b_1, b_2, b_3 равны соответственно $n, -m, 1$.

Поскольку $\alpha, \beta, \gamma \in \mathbb{K} = \mathbb{Q}(\sqrt{2k+1}, \sqrt{2l+1})$, степень поля $\mathbb{K}$ может равняться либо 2, либо 4. Если степень равна 2, тогда выполнено равенство $2k+1 = r^2(2l+1)$, $r \in \mathbb{Q}$. В силу выбора параметров k, l это неравенство невозможно. Следовательно, степень поля $\mathbb{K}$ равна 4 и числа α, β, γ удовлетворяют условиям теоремы.

Поскольку для единиц выполнены неравенства $\varepsilon_i > 1 > \bar{\varepsilon}_i > 0$ и коэффициент при старшем члене основного многочлена ε_i равен 1,

$$h(\varepsilon_i) = \frac{1}{2} \log \varepsilon_i, \quad A_i := 2 \log \varepsilon_i \geq \max\{4h(\varepsilon_i), \log \varepsilon_i\} \quad \text{для } i = 1, 2. \quad (19)$$

С числом γ ситуация немного сложнее. Напомним, что

$$\gamma = \frac{\alpha \sqrt{2l+1}}{\beta \sqrt{2k+1}}.$$

Поскольку отношение $\sqrt{2l+1}/\sqrt{2k+1}$ не есть рациональное число, степень γ равна 4. Тогда существует четыре различных сопряженных с γ числа. Их абсолютные значения равны

$$\gamma_1 = \frac{\alpha\sqrt{2l+1}}{\beta\sqrt{2k+1}}, \quad \gamma_2 = \frac{\alpha\sqrt{2l+1}}{\beta\sqrt{2k+1}}, \quad \gamma_3 = \frac{\bar{\alpha}\sqrt{2l+1}}{\bar{\beta}\sqrt{2k+1}}, \quad \gamma_4 = \frac{\bar{\alpha}\sqrt{2l+1}}{\bar{\beta}\sqrt{2k+1}}.$$

Тогда для высоты $h(\gamma)$ верно следующее неравенство:

$$h(\gamma) \leq \frac{1}{4} \log \left(\prod_{j=1}^4 M_j \right),$$

где

$$\begin{aligned} M_1 &= \max(\alpha\sqrt{2l+1}, \bar{\beta}\sqrt{2k+1}), & M_2 &= \max(\alpha\sqrt{2l+1}, \beta\sqrt{2k+1}), \\ M_3 &= \max(\bar{\alpha}\sqrt{2l+1}, \bar{\beta}\sqrt{2k+1}), & M_4 &= \max(\bar{\alpha}\sqrt{2l+1}, \beta\sqrt{2k+1}). \end{aligned}$$

Исходя из этого будем выбирать значение параметра A_3 как наименьшее действительное число, удовлетворяющее неравенству

$$A_3 > \max \left\{ \log \left(\prod_{j=1}^4 M_j \right), |\log \gamma| \right\}.$$

Обозначим

$$S = \max \left\{ C, \frac{A_3}{2 \log \varepsilon_2} \right\}, \quad (20)$$

где C определено равенством (14), и будем считать, что $n > S$. В противном случае мы получаем оценку сверху для n .

Поскольку мы предполагаем, что $S < n$, $m < n$ и $\varepsilon_1 < \varepsilon_2$, для величины B с учетом (19) верна оценка сверху

$$B = \max \left\{ \frac{nA_1}{A_3}, \frac{mA_2}{A_3}, 1 \right\} < \frac{2n \log \varepsilon_2}{A_3}.$$

Теперь, используя утверждение теоремы 2, получим нижнюю оценку модуля линейной формы (13)

$$\log |\Lambda| > -3.1 \cdot 10^{11} (2 \log \varepsilon_1) (2 \log \varepsilon_2) A_3 \log \left(\frac{78n \log \varepsilon_2}{A_3} \right).$$

Учитывая для Λ верхнюю оценку (17), получаем неравенство

$$C_1 (\log C_2 n) > n, \quad \text{где} \quad C_1 = 1.24 \cdot 10^{12} \log \varepsilon_2 A_3, \quad C_2 = \frac{78 \log \varepsilon_2}{A_3}.$$

Обозначим через N максимальное из целых чисел, удовлетворяющих приведенному неравенству, а именно,

$$N = \max \{ n \in \mathbb{Z} : C_1 (\log C_2 n) > n \}. \quad (21)$$

Таким образом, доказана следующая

ТЕОРЕМА 3. Пусть $z \in \mathbb{Z}$ – неотрицательное решение системы уравнений (1), удовлетворяющее равенству (5). Кроме того, известно, что $\varepsilon_1 < \varepsilon_2$, тогда для индексов $n, m \in \mathbb{Z}$ выполнены неравенства

$$H_1 \leq n \leq \max(S, N), \quad H_2 \leq m \leq \max(S, N),$$

где H_1, H_2 определены согласно (6), S – согласно (20), а N – согласно (21).

3. Уменьшение верхней оценки

Ранее мы доказали конечность множества индексов, удовлетворяющих равенству (5), и получили для них согласно теореме 3 верхнюю оценку. Далее мы опишем итерационный алгоритм, позволяющий значительно уменьшить эту оценку в случае, если она совпадает со значением N .

Определим функцию $\|\cdot\|$ как расстояние до ближайшего целого числа, т.е.

$$\|\xi\| = \min_{n \in \mathbb{Z}} |n - \xi|, \quad \text{где } \xi \in \mathbb{R}.$$

Из определения функции $\|\cdot\|$ следует, что для любого ξ выполнено $0 \leq \|\xi\| \leq 1/2$, а кроме того, $\|\xi + n\| = \|\xi\|$ для любого $n \in \mathbb{Z}$.

В начале приведем лемму, утверждение которой будет использовано при дальнейших вычислениях. Первоначальный вариант этой леммы был доказан в работе [2].

ЛЕММА 2. Пусть λ, μ – положительные числа такие, что $\lambda + \mu \leq 1$. Далее, пусть ξ, θ – действительные числа, а q – натуральное. Тогда для любого $n \in \mathbb{Z}$ такого, что $1 \leq n < \lambda \|q\xi\| / \|q\theta\|$, выполнено неравенство

$$\|n\theta + \xi\| \geq \mu \frac{\|q\xi\|}{q}.$$

ДОКАЗАТЕЛЬСТВО. Пусть p – ближайшее целое к $q\theta$; тогда $\|q\theta\| = |q\theta - p|$. Далее, пусть m – ближайшее целое к $n\theta + \xi$, аналогично, $\|n\theta + \xi\| = |n\theta + \xi - m|$.

Предположим, что утверждение леммы не выполнено:

$$\|n\theta + \xi\| < \mu \frac{\|q\xi\|}{q},$$

тогда

$$q\|n\theta + \xi\| < \mu \|q\xi\|.$$

Оценим снизу величину $\|q\xi\|$:

$$\|q\xi\| \geq \lambda \|q\xi\| + \mu \|q\xi\| > n\|q\theta\| + q\|n\theta + \xi\| \geq |qm - np - q\xi|.$$

Поскольку $qm - np \in \mathbb{Z}$, последнее неравенство противоречиво. Полученное противоречие завершает доказательство леммы.

Теперь снова вернемся к линейной форме от трех логарифмов (13). По-прежнему будем предполагать, что $\varepsilon_1 < \varepsilon_2$. Выделяя в линейной форме отдельно индекс m , получим модуль

$$\left| \frac{\Lambda}{\log \varepsilon_2} \right| = \left| n \frac{\log \varepsilon_1}{\log \varepsilon_2} - m + \frac{\log \gamma}{\log \varepsilon_2} \right|.$$

Поскольку модуль исходной линейной формы ограничен сверху величиной, близкой к нулю (17), полученный модуль также принимает значения, близкие к нулю. Таким образом, m является ближайшим целым к величине

$$n\theta + \xi, \quad \text{где} \quad \theta = \frac{\log \varepsilon_1}{\log \varepsilon_2}, \quad \xi = \frac{\log \gamma}{\log \varepsilon_2}.$$

Величина θ не является рациональным числом. Пусть это не так, тогда выполнено равенство $\varepsilon_1^u = \varepsilon_2^v$ для некоторых целых u, v . Поскольку ε_i — единицы двух различных модулей, равенство возможно только в том случае, когда $2k+1 = r^2(2l+1)$, где $r \in \mathbb{Q}$. Это не верно, в силу выбора параметров k, l .

Поскольку θ иррационально, мы вычисляем бесконечную непрерывную дробь и, соответственно, подходящую дробь с заранее заданной точностью, а именно, для любого натурального $s > 1$ выполнено неравенство

$$\left| \theta - \frac{p_s}{q_s} \right| < \frac{1}{q_s q_{s+1}},$$

где p_s/q_s — s -я подходящая дробь. При этом, величина $\|q_s \theta\|$ ограничена сверху дробью $1/q_{s+1}$ и может принимать сколь угодно малые значения.

Теперь опишем итерационный алгоритм, позволяющий понизить оценку сверху для индекса n , полученную в утверждении теоремы 3. Пусть $n \leq N_i$, $i \in \mathbb{N}$, тогда, вычисляя подходящую дробь для θ , находим такое значение s , для которого выполнено неравенство

$$N_i < \frac{1}{2} \cdot \frac{\|q_s \xi\|}{\|q_s \theta\|}.$$

Выберем параметры λ и μ равными $1/2$. Поскольку $1 \leq n \leq N_i$, согласно лемме 2 для найденного индекса s выполнено неравенство

$$\|n\theta + \xi\| \geq \frac{1}{2} \cdot \frac{\|q_s \xi\|}{q_s}.$$

ТАБЛИЦА 2

k	l	Значения переменной z
7	45	0, 1, 4, 12, 33
52	10	0, 1, 5, 16, 39
10	70	0, 1, 8, 25, 77

Таблица 3

k	l	Значения переменной z	k	l	Значения переменной z
1	7	0, 1, 4, 56	1	45	0, 1, 4, 15
2	10	0, 1, 3, 8	2	70	0, 1, 8, 21
2	87	0, 1, 8, 377	3	16	0, 1, 4, 20
3	66	0, 1, 9, 144	3	91	0, 1, 9, 65
5	22	0, 1, 8, 15	5	32	0, 1, 8, 28
5	77	0, 1, 15, 28	6	10	0, 1, 5, 16
6	28	0, 1, 5, 16	6	42	0, 1, 9, 56
6	52	0, 1, 5, 16	6	91	0, 1, 9, 56
7	42	0, 1, 7, 56	7	55	0, 1, 7, 33
7	80	0, 1, 12, 260	8	16	0, 1, 6, 64
8	80	0, 1, 10, 64	9	38	0, 1, 15, 24
9	100	0, 1, 15, 260	10	15	0, 1, 25, 47
10	22	0, 1, 8, 77	10	28	0, 1, 5, 16
10	32	0, 1, 8, 120	10	63	0, 1, 16, 39
14	58	0, 1, 24, 35	15	32	0, 1, 8, 36
15	70	0, 1, 8, 25	16	85	0, 1, 20, 204
16	88	0, 1, 14, 64	16	99	0, 1, 20, 924
17	35	0, 1, 12, 2431	17	85	0, 1, 17, 204
18	45	0, 1, 15, 216	20	27	0, 1, 9, 48
20	58	0, 1, 35, 37961	20	66	0, 1, 9, 35
20	82	0, 1, 35, 48	21	28	0, 1, 16, 49
21	51	0, 1, 16, 1105	22	45	0, 1, 15, 528
22	70	0, 1, 8, 77	25	38	0, 1, 15, 1520
25	45	0, 1, 15, 175	25	64	0, 1, 20, 1520
25	85	0, 1, 20, 175	27	35	0, 1, 12, 63
28	36	0, 1, 21, 64	28	52	0, 1, 5, 16
28	70	0, 1, 21, 560	30	66	0, 1, 11, 35
30	72	0, 1, 27, 160	32	65	0, 1, 28, 120
33	64	0, 1, 20, 176	38	64	0, 1, 24, 1520
42	52	0, 1, 13, 32	42	72	0, 1, 32, 189
42	91	0, 1, 9, 56	45	55	0, 1, 33, 100
45	77	0, 1, 15, 33	52	63	0, 1, 16, 39
52	85	0, 1, 32, 1105	55	66	0, 1, 40, 121
55	77	0, 1, 33, 1540	65	77	0, 1, 28, 143
72	85	0, 1, 17, 32	76	90	0, 1, 19, 11375
77	90	0, 1, 33, 168	78	91	0, 1, 56, 169

С другой стороны, учитывая полученную ранее верхнюю оценку модуля линейной формы (17) и то, что $\varepsilon_2 \geq 1 + \sqrt{2l+1} > e$, получим неравенство

$$\|n\theta + \xi\| = |n\theta - m + \xi| < \frac{\varepsilon_1^{-n}}{\log \varepsilon_2} < \varepsilon_1^{-n}.$$

Объединяя приведенные выше оценки, получим неравенство, относительно n , позволяющее определить новую оценку N_{i+1} :

$$n < (\log \varepsilon_1)^{-1} \log \left(\frac{2q_s}{\|q_s \xi\|} \right) =: N_{i+1}. \quad (22)$$

Пусть константы N, S удовлетворяют утверждению теоремы 3. Тогда, определив в качестве начального значения $N_0 := N$, получим последовательность оценок $N_1, N_2, \dots$.

Вычисления будем производить до тех пор, пока для некоторого номера i не выполнено либо $N_{i+1} \geq N_i$, либо $N_{i+1} < S$. Тогда искомой оценкой будет

$$\max(n, m) < \max(S, N_i).$$

4. Результаты практических экспериментов

Алгоритм, изложенный выше, был реализован автором на ЭВМ. Анонс результатов был опубликован в 2001 г. [12]. Позднее исследования были продолжены, и автором были решены все системы вида (1), где k и l удовлетворяют неравенствам

$$1 \leq k < l \leq 100. \quad (23)$$

Для решения всех систем, параметры которых удовлетворяют приведенному выше неравенству, на ЭВМ с процессором Pentium IV, тактовая частота которого равнялась 1500 МГц, потребовалась 32 дня 2 часа и 38 минут суммарного времени (вычисления производились независимо на нескольких ЭВМ).

Приведем полученные решения. Поскольку значения переменных x, y могут быть восстановлены по заданной паре k, l и значению переменной z , мы ограничимся только этими значениями.

Были найдены 3 системы, имеющие три нетривиальных решения: см. табл. 2.

Были найдены 72 системы, имеющие два нетривиальных решения. Остальные решенные системы имели либо одно нетривиальное решение, либо не имели его вовсе. В заключение мы приводим решения всех систем с двумя нетривиальными решениями, параметры которых удовлетворяют условиям (23): см. табл. 3.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] И. Х. Сабитов, “Исследование жесткости и неизгибаемости аналитических поверхностей вращения с уплющением в полюсе”, *Вестн. Моск. ун-та. Сер. 1. Матем., мех.*, 1986, № 5, 29–36.
- [2] A. Baker, H. Davenport, “The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$ ”, *Quart. J. Math. Oxford Ser. (2)*, **20** (1969), 129–137.
- [3] C. M. Grinstead, “On a method of solving a class of Diophantine equations”, *Math. Comp.*, **32**:143 (1978), 936–940.

- [4] R. G. E. Pinch, “Simultaneous Pellian equations”, *Math. Proc. Cambridge Philos. Soc.*, **103**:1 (1988), 35–46.
- [5] W. S. Anglin, “Simultaneous Pell equations”, *Math. Comp.*, **65**:213 (1996), 355–359.
- [6] Б. А. Венков, *Элементарная теория чисел*, Математика в монографиях. Сер. обзоров, **4**, ОНТИ НКТП СССР, М., 1937.
- [7] Г. Дэвенпорт, *Высшая арифметика. Введение в теорию чисел*, Наука, М., 1965.
- [8] A. Baker, “Linear forms in the logarithms of algebraic numbers. IV”, *Mathematica*, **15** (1968), 204–216.
- [9] M. A. Bennet, *On the Number of Solutions of Simultaneous Pell Equations*, Preprint, Univ. of British Columbia, Vancouver, BC, 1991.
- [10] M. Waldschmidt, “A lower bound for linear forms in logarithms”, *Acta Arith.*, **37** (1980), 257–283.
- [11] Е. М. Матвеев, “Явная нижняя оценка однородной рациональной линейной формы от логарифмов алгебраических чисел. II”, *Изв. РАН. Сер. матем.*, **64**:6 (2000), 125–180.
- [12] А. Ю. Нестеренко, “О нахождении целочисленных решений системы связанных уравнений Пелля”, *Тезисы докладов IV Международной конференции “Современные проблемы теории чисел и ее приложения”*, ТГПУ, Тула, 2001, 88.

А. Ю. Нестеренко

Московский государственный университет

им. М. В. Ломоносова

E-mail: nesterenko_a_y@mail.ru

Поступило

14.04.2005

Исправленный вариант

29.06.2006