

СОДЕРЖАНИЕ И ТЕХНОЛОГИИ
МАТЕМАТИЧЕСКОГО ОБРАЗОВАНИЯ В ВУЗЕ

УДК 511 (07)

УРАВНЕНИЕ ПЕЛЛЯ

А. Ю. Эвнин

*Южно-Уральский государственный университет,
Россия, 454080, г. Челябинск, пр. Ленина, 76;
e-mail: evnin@prima.susu.ac.ru*

Предлагается компактный вариант изложения темы “Уравнение Пелля”, доступный для первокурсников. Приводится доказательство существования нетривиального решения, найденное в 2008 г. австралийским математиком Н. Вайлдбергером.

Ключевые слова: нелинейные диофантовы уравнения, уравнение Пелля.

Диофантово уравнение — это уравнение в целых числах вида

$$P(x_1, x_2, \dots, x_n) = 0,$$

где P — многочлен от n переменных с целыми коэффициентами.

Одним из немногих хорошо изученных нелинейных диофантовых уравнений является уравнение Пелля

$$x^2 - my^2 = 1, \tag{1}$$

где m — натуральное число, не являющееся полным квадратом (как известно, число $\sqrt{m}$ будет при этом иррациональным).

История этого уравнения уходит в глубины веков, однако исследования, посвященные уравнению Пелля, продолжаются (см., например, [1–3]).

При любом m пары чисел $(1; 0)$ и $(-1; 0)$ являются решениями уравнения (1). Назовем такие решения *тривиальными*. Остальные решения уравнения Пелля — *нетривиальные*. Как мы увидим позднее, нетривиальные решения всегда существуют.

Всякое решение (1) с натуральными значениями переменных x и y будем называть *натуральным* решением, а натуральное решение с наименьшим возможным значением x — *фундаментальным* решением. В дальнейшем нам пригодится следующий простой факт.

Если $(a; b)$ и $(c; d)$ — натуральные решения уравнения (1), то

$$a < c \iff b < d, \quad a = c \iff b = d, \quad a > c \iff b > d.$$

Ясно, что если $(a; b)$ — натуральное решение, то решениями (1) будут также пары $(a; -b)$, $(-a; b)$ и $(-a; -b)$. С другой стороны, если $(c; d)$ — произвольное нетривиальное решение диофантова уравнения (1), то $(|c|; |d|)$ — натуральное решение. Таким образом, решая уравнение Пелля, достаточно найти все его натуральные решения.

Рассмотрим числовое множество

$$\mathbb{Z}[\sqrt{m}] = \{x + y\sqrt{m} \mid x, y \in \mathbb{Z}\}.$$

Несложно видеть, что это множество содержит 0 и 1 и замкнуто относительно операций сложения и умножения. Поэтому $\mathbb{Z}[\sqrt{m}]$ — коммутативное кольцо с единицей.

Заметим, что соответствие

$$(x; y) \rightarrow x + y\sqrt{m}$$

между $\mathbb{Z}^2$ и $\mathbb{Z}[\sqrt{m}]$ является взаимно-однозначным. Действительно, если $x_1 + y_1\sqrt{m} = x_2 + y_2\sqrt{m}$ и $y_1 \neq y_2$, то $\sqrt{m} = \frac{x_1 - x_2}{y_2 - y_1}$, что противоречит иррациональности числа $\sqrt{m}$. Поэтому число $z \in \mathbb{Z}[\sqrt{m}]$ представляется в виде $x + y\sqrt{m}$ единственным способом.

Указанное соответствие позволяет отождествлять пару целых чисел $(x; y)$ с числом $z = x + y\sqrt{m}$. Ниже иногда мы будем говорить, что $z = x + y\sqrt{m}$ — решение уравнения (1), имея в виду, что таковым на самом деле является пара $(x; y)$.

Введем на кольце $\mathbb{Z}[\sqrt{m}]$ операцию сопряжения:

$$\overline{x + y\sqrt{m}} = x - y\sqrt{m}.$$

Очевидно, что сопряженное к сопряженному есть исходное число: $\overline{\bar{z}} = z$. Докажем, что сопряженное к произведению есть произведение сопряженных: $\overline{z_1 \cdot z_2} = \bar{z}_1 \cdot \bar{z}_2$. Действительно,

$$\begin{aligned} \overline{(x_1 + y_1\sqrt{m})(x_2 + y_2\sqrt{m})} &= \overline{x_1x_2 + y_1y_2m + (x_1y_2 + y_1x_2)\sqrt{m}} = \\ &= x_1x_2 + y_1y_2m - (x_1y_2 + y_1x_2)\sqrt{m} = (x_1 - y_1\sqrt{m})(x_2 - y_2\sqrt{m}). \end{aligned}$$

Введем норму числа $z = x + y\sqrt{m}$:

$$\|z\| = z \cdot \bar{z} = x^2 - my^2.$$

Решить уравнение Пелля означает найти все числа с единичной нормой.

Отметим свойства нормы: сопряженные числа имеют одинаковые нормы; норма произведения равна произведению норм. Действительно,

$$\|\bar{z}\| = \bar{z} \cdot \overline{\bar{z}} = \bar{z} \cdot z = \|z\|;$$

$$\|z_1 \cdot z_2\| = z_1 \cdot z_2 \cdot \overline{z_1 \cdot z_2} = z_1 \cdot z_2 \cdot \bar{z}_1 \cdot \bar{z}_2 = z_1 \cdot \bar{z}_1 \cdot z_2 \cdot \bar{z}_2 = \|z_1\| \cdot \|z_2\|.$$

Легко видеть, что числа из $\mathbb{Z}[\sqrt{m}]$ с единичной нормой образуют мультипликативную группу. Элементом, обратным к числу z , является сопряженное число $\bar{z}$. Если $(x_1; y_1)$ — решение уравнения (1) и

$$z_1 = x_1 + y_1\sqrt{m}, \quad z_k = z_1^k = x_k + y_k\sqrt{m},$$

то $(x_k; y_k)$ — также решение (1). Другими словами, степень каждого решения является решением. Оказывается, что степени фундаментального решения исчерпывают множество натуральных решений уравнения Пелля. Об этом говорит следующая теорема.

Теорема 1. Пусть $(x_1; y_1)$ — фундаментальное решение, а $(x; y)$ — произвольное натуральное решение уравнения (1). Тогда для некоторого натурального k имеет место равенство

$$z = x + y\sqrt{m} = (x_1 + y_1\sqrt{m})^k.$$

Доказательство. Пусть, как и выше,

$$z_k = (x_1 + y_1\sqrt{m})^k = x_k + y_k\sqrt{m}.$$

Возникают две бесконечные возрастающие последовательности натуральных чисел:

$$x_1 < x_2 < \dots < x_k < \dots; \quad y_1 < y_2 < \dots < y_k < \dots$$

Если решение уравнения (1) $z = x + y\sqrt{m}$ не является степенью числа z_1 , то найдется такое число n , что $x_n < x < x_{n+1}$. При этом выполняются также неравенства $y_n < y < y_{n+1}$ и

$$z_1^n < z < z_1^{n+1}. \quad (2)$$

Умножив неравенство (2) на $\bar{z}_1^n$, получим

$$1 < X + Y\sqrt{m} < z_1, \quad (3)$$

где $X + Y\sqrt{m} = (x + y\sqrt{m})(x_1 - y_1\sqrt{m})^n$. Число $X + Y\sqrt{m}$, будучи произведением чисел с единичной нормой, также имеет единичную норму:

$$(X + Y\sqrt{m})(X - Y\sqrt{m}) = 1. \quad (4)$$

Из соотношений (3) и (4) следует, что

$$0 < X - Y\sqrt{m} < 1. \quad (5)$$

Следствием (3) и (5) является неравенство $X - Y\sqrt{m} < X + Y\sqrt{m}$, из которого получаем, что $Y > 0$. Теперь из неравенства $X - Y\sqrt{m} > 0$ вытекает, что и $X > 0$. Таким образом, $(X; Y)$ — натуральное решение уравнения Пелля, причем

$$X + Y\sqrt{m} < x_1 + y_1\sqrt{m}.$$

Это противоречит фундаментальности решения $(x_1; y_1)$. $\square$

Теорема 2. Уравнение (1) имеет нетривиальные решения.

Доказательство. Опишем алгоритм нахождения некоторого нетривиального решения, придуманный в 2008 г. австралийским математиком Н. Вайлсбергером [7]. Этот способ доказательства теоремы 2 значительно проще ранее известных.

Рассмотрим квадратичную форму

$$Q(x, y) = (x \ y) \begin{pmatrix} a & b \\ b & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = ax^2 + 2bxy + cy^2.$$

Матрицу $A = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$ назовем *подходящей*, если $a > 0$, $c < 0$.

Уравнение Пелля $x^2 - my^2 = 1$ можно записать в виде $Q(x, y) = 1$ с матрицей квадратичной формы $A_0 = \begin{pmatrix} 1 & 0 \\ 0 & -m \end{pmatrix}$. Заметим, что эта матрица является подходящей, а число $-|A_0|$ не является полным квадратом.

Итог матрицы — сумма её элементов.

Введем в рассмотрение две матрицы: $L = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ и $R = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Будем строить последовательность матриц $A_i = \begin{pmatrix} a_i & b_i \\ b_i & c_i \end{pmatrix}$, где $i = 0, 1, 2, \dots$, в которой очередная матрица получается из предыдущей с помощью одного из следующих преобразований. *Левый шаг* — замена матрицы $A = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$ на матрицу $L'AL = \begin{pmatrix} a + 2b + c & b + c \\ b + c & c \end{pmatrix}$. *Правый шаг* — замена матрицы A на матрицу $R'AR = \begin{pmatrix} a & a + b \\ a + b & a + 2b + c \end{pmatrix}$. Здесь штрих означает транспонирование матрицы.

Если у матрицы положительный итог, будем делать левый шаг, а если отрицательный, то правый. Легко видеть, что из подходящей матрицы всегда получится подходящая.

Убедимся в том, что итог любой матрицы из нашей последовательности отличен от нуля. Поскольку $|L| = |R| = 1$, левый и правый шаги не меняют определителя матрицы. Значит, определитель каждой матрицы равен $|A_0| = -m$. С другой стороны, матрица с нулевым итогом имеет вид $\begin{pmatrix} a & b \\ b & -a - 2b \end{pmatrix}$, где a и b — целые числа, и её определитель равен $-(b - a)^2$. Получаем, что $m = (b - a)^2$, в то время как число m , по условию, не является полным квадратом.

Итак, мы имеем бесконечную последовательность матриц $A_i = \begin{pmatrix} a_i & b_i \\ b_i & c_i \end{pmatrix}$, таких, что $a_i > 0$, $c_i < 0$, $a_i c_i - b_i^2 = -m$. Числа a_i , $-c_i$ и b_i образуют решение в натуральных числах уравнения $xy + z^2 = m$. Очевидно, что это уравнение в натуральных числах имеет конечное множество решений. Значит, в последовательности (A_i) не все матрицы различны. Покажем, что первой повторится матрица A_0 .

Для этого сначала убедимся в том, что по матрице A_i можно однозначно определить ей предшествующую матрицу A_{i-1} .

Если $A_i = L'A_{i-1}L$, то $A_{i-1} = (L')^{-1}A_iL^{-1} =$

$$= \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a_i & b_i \\ b_i & c_i \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} a_i - 2b_i + c_i & b_i - c_i \\ b_i - c_i & c_i \end{pmatrix}.$$

Если $A_i = R'A_{i-1}R$, то $A_{i-1} = (R')^{-1}A_iR^{-1} =$

$$\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} a_i & b_i \\ b_i & c_i \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a_i & b_i - a_i \\ b_i - a_i & a_i - 2b_i + c_i \end{pmatrix}.$$

Значит, всё определяется величиной $t = a_i - 2b_i + c_i$. Если $t > 0$, то матрица A_i получена из A_{i-1} левым шагом; если же $t < 0$, то правым. Равенство $t = 0$ невозможно из-за того, что матрица A_{i-1} — подходящая (на её главной диагонали нет нулей).

Таким образом, если некоторая матрица A_i , отличная от A_0 , в нашей последовательности встретилась второй раз, то тем же свойством обладает и матрица A_{i-1} . Поэтому первой повторится матрица A_0 .

Поясним сказанное примерами. Выпишем последовательности матриц (A_i) между двумя вхождениями начальной матрицы A_0 для $m = 2$ и $m = 7$. Над стрелкой перехода указан итог матрицы, а под стрелкой вид шага: R или L .

$$\begin{pmatrix} 1 & 0 \\ 0 & -2 \end{pmatrix} \xrightarrow[R]{-1} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \xrightarrow[L]{2} \begin{pmatrix} 2 & 0 \\ 0 & -1 \end{pmatrix} \xrightarrow[L]{1} \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} \xrightarrow[R]{-2} \begin{pmatrix} 1 & 0 \\ 0 & -2 \end{pmatrix}.$$

Результирующее преобразование при $m = 2$ задается матрицей $N = RL^2R$.

$$\begin{aligned} & \begin{pmatrix} 1 & 0 \\ 0 & -7 \end{pmatrix} \xrightarrow[R]{-6} \begin{pmatrix} 1 & 1 \\ 1 & -6 \end{pmatrix} \xrightarrow[R]{-3} \begin{pmatrix} 1 & 2 \\ 2 & -3 \end{pmatrix} \xrightarrow[L]{2} \begin{pmatrix} 2 & -1 \\ -1 & -3 \end{pmatrix} \xrightarrow[R]{-3} \\ & \xrightarrow[R]{-3} \begin{pmatrix} 2 & 1 \\ 1 & -3 \end{pmatrix} \xrightarrow[L]{1} \begin{pmatrix} 1 & -2 \\ -2 & -3 \end{pmatrix} \xrightarrow[R]{-6} \begin{pmatrix} 1 & -1 \\ -1 & -6 \end{pmatrix} \xrightarrow[R]{-7} \begin{pmatrix} 1 & 0 \\ 0 & -7 \end{pmatrix}. \end{aligned}$$

Результирующее преобразование при $m = 7$ задается матрицей $N = R^2LRLR^2$.

Заметим, что первый шаг в последовательности преобразований всегда правый (поскольку итог начальной матрицы $1 - m < 0$). Но все шаги правыми быть не могут. Действительно, если матрица A_i получена правым шагом, то $b_i = a_{i-1} + b_{i-1} > b_{i-1}$, а числовая последовательность (b_i) не может быть возрастающей в силу своей периодичности.

Поэтому матрица $N = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, задающая результирующее преобразование, всегда состоит из натуральных чисел.

Итак, предъявлен алгоритм, позволяющий найти матрицу N , для которой выполнено матричное равенство

$$N'A_0N = A_0.$$

Пусть теперь $Q(x, y) = (x \ y)A_0 \begin{pmatrix} x \\ y \end{pmatrix} = 1$ и $\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = N \begin{pmatrix} x \\ y \end{pmatrix}$. Тогда

$$\begin{aligned} Q(x_1, y_1) &= (x_1 \ y_1)A_0 \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = (x \ y)N'A_0N \begin{pmatrix} x \\ y \end{pmatrix} = \\ &= (x \ y)A_0 \begin{pmatrix} x \\ y \end{pmatrix} = Q(x, y) = 1. \end{aligned}$$

Другими словами, если (x, y) — решение уравнения Пелля, то (x_1, y_1) тоже является решением. В частности, по тривиальному решению $(1, 0)$ находим решение (α, γ) , которое уже не является тривиальным, поскольку $\alpha, \gamma > 0$. $\square$

Примеры. Для $m = 2$ имеем $N = RL^2R = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}$ и решение $(3, 2)$.

Для $m = 7$ имеем $N = R^2LRLR^2 = \begin{pmatrix} 8 & 21 \\ 3 & 8 \end{pmatrix}$ и решение $(8, 3)$.

Итак, нетривиальное решение уравнения Пелля существует. Значит, существует и фундаментальное решение, знание которого позволяет указать все решения. Как показывают вычисления на компьютере, при $m \leq 150$ алгоритм Вайлдбергера находит фундаментальное решение. Но будет ли так при произвольном m , неизвестно.

С другими подходами к решению уравнения Пелля можно познакомиться по книгам и статьям [2–8].

ЛИТЕРАТУРА

1. Wildberger N.J. Pell's equation without irrational numbers // arXiv: 0806.2490v1 [math.NT] 16 June 2008.
2. Мешков В. А. Уравнения Пелля: мультипликативные свойства и ациклический метод решения // <http://www.n-t.ru/tp/ns/upa.doc>.
3. Щетников А. И. Задача Архимеда о быках, алгоритм Евклида и уравнение Пелля // Математика в высшем образовании. 2004. № 2. С. 27–40.
4. Арнольд В. И. Цепные дроби. — М.: Изд-во МЦНМО, 2001. 40 с.
5. Бугаенко В. О. Уравнения Пелля. — М.: Изд-во МЦНМО, 2001. 32 с.
6. Спивак А. В. Арифметика-2. — М.: Бюро Квантум, 2008. — 160 с. (Библиотечка «Квант». Вып. 109.)
7. Эвнин А. Ю. Элементы теории чисел. — Челябинск: Изд-во ЮУрГУ, 2007. 53 с.
8. Эдвардс Г. Последняя теорема Ферма. Генетическое введение в алгебраическую теорию чисел. — М.: Мир, 1980. 484 с.

THE PELL'S EQUATION

A. Yu. Evnin

A compact variant simple for beginners is proposed for the theme “Pell's equation”. The existence proof of a nontrivial solution to the Pell's equation found by the Australian mathematician N. Wildberger is demonstrated.

Keywords: nonlinear Diophantine equations, Pell's equation.