4. *Jungnickel D*. Finite fields: Structure and Arithmetics. Mannheim ; Leipzig ; Wien ; Zürich, 1993.

5. *Lidl R.*, *Niederreiter H*. Finite fields (Second edition). Cambridge University Press, 1997.

Об авторах

Сергей Иванович Алешников — канд. техн. наук, доц., Балтийский федеральный университет им. И. Канта, Калининград.

E-mail: elliptec@mail.ru

Марина Валерьевна Алешникова — ст. преп., Балтийский федеральный университет им. И. Канта, Калининград.

E-mail: aleshnikova_m_v@mail.ru

Андрей Александрович Горбачёв — канд. техн. наук, доц., Калининградский государственный технический университет.

E-mail: terjer@mail.ru

About the authors

Dr Sergey Aleshnikov, ass. prof., I. Kant Baltic Federal University, Kaliningrad.

E-mail: elliptec@mail.ru

Marina Aleshnikova, head teacher, I. Kant Baltic Federal University, Kaliningrad.

E-mail: aleshnikova_m_v@mail.ru

Dr Andrey Gorbachev, ass. prof., Kaliningrad State Technical University.

E-mail: terjer@mail.ru

УДК 511

С. И. Алешников, М. В. Алешникова, А. А. Горбачёв

ЭЛЕМЕНТАРНОЕ РЕШЕНИЕ ОДНОГО КУБИЧЕСКОГО ДИОФАНТОВА УРАВНЕНИЯ

Представлен элементарный подход к решению кубического диофантова уравнения $y^2 = x^3 - 2^{2s}$, *зависящего от одного натурального параметра s. Получено полное решение для всех значений s.*

An elementary approach to solving of the cubic Diophantine equations $y^2 = x^3 - 2^{2s}$, *depending on one natural parameter s is presented. The full solving for all values s is received.*

Ключевые слова: диофантово уравнение, квадратичное поле, число классов, уравнение Пелля, делимость, целые гауссовы числа, фундаментальная единица.

Key words: Diophantine equation, quadratic field, class number, Pell equation, divisibility, Gaussian integers, fundamental unit.

Введение

Криптосистемы на основе квадратичных полей используют конечную группу классов дробных идеалов, в частности необходимо вычислять (или хотя бы оценивать) порядок этой группы — число классов h квадратичного поля. Кроме того, важнейшая задача в криптографии на решетках — задача отыскания коротких образующих неглавных идеалов в квадратичных расширениях круговых числовых полей. Наконец, проблема отыскания целых точек эллиптических кривых не решена до конца и также представляет собой проблему решения кубического диофантова уравнения.

В статье [3] проблема оценки числа классов квадратичного поля связывается с решением диофантовых уравнений следующего вида:

$$1+4b^2k^{2n}=da^2,\quad a, b, k, n\in\mathbf{N}, k>1, n>1. \tag{1}$$

В [6] Лу доказал, что при $a=b=1$ в уравнении (1) число классов $h(d)$ квадратичного поля $\mathbf{Q}(\sqrt{d})$, где d — натуральное число, свободное от квадратов, удовлетворяет условию

$$h(d)\equiv 0 \pmod{n}. \tag{2}$$

В работе [5] Ли показал, что если $b=1$, $n>2$, число $2k^n+a\sqrt{d}$ является фундаментальным решением уравнения Пелля $x^2-dy^2=-1$ и наибольший общий делитель $(p, (q-1)q)=1$ для каждого нечетного простого делителя $p\mid n$ и $q\mid k$, то условие (2) выполняется, за исключением набора $(a, d, k, n) = (5, 41, 2, 4)$.

В [2] доказано, что если $b=1$, $n>2$, $2k^n+a\sqrt{d}$ является фундаментальным решением уравнения Пелля $x^2-dy^2=-1$, $a\leqslant k^{n/2}$ и 2 не делит k, то (2) выполняется.

В [3] главный результат следующий.

Если $b=1$, $n>2$ и имеет место одно из условий:

1) всякий простой делитель числа a делит d;

2) $(p, q^2-1)=1$ для каждого нечетного простого числа p числа n и простого делителя q числа a;

3) $a\leqslant 0{,}5k^{0{,}4226n}$ или $a\leqslant 0{,}5k^{0{,}5527n}$ и k нечетно,

то (2) выполняется.

Уравнение, аналогичное (1), изучается в [7; 8]. Его разрешимость также связывается с оценкой числа классов квадратичного поля.

Целью этой работы стало отыскание целочисленных решений уравнения

$$y^2=x^3-2^{2s}. \tag{3}$$

1. Случай четного y

Положим $y = 2y'$. Тогда из уравнения (3) следует, что x четно, т. е. $x = 2x'$. После подстановки и сокращения на 4 уравнение (3) сводится к виду

$$y'^2 = 2x'^3 - 2^{2(s-1)}, \tag{4}$$

откуда видно, что y' четно, т. е. $y' = 2y''$. Уравнение (4) после сокращения приобретает вид

$$2y''^2 = x'^3 - 2^{2s-3},$$

следовательно, x' четно, т. е. $x' = 2x''$. После постановки в предыдущее уравнение и сокращения получаем

$$y''^2 = 4x''^3 - 2^{2(s-2)}. \tag{5}$$

Продолжая анализ четности, получаем, что замена $x = 4x''$, $y = 8y'''$ сводит уравнение (3) к виду

$$y'''^2 = 2x''^3 - 2^{2(s-3)}, \tag{6}$$

что возвращает нас к первоначальному виду (3), если положить $s = s - 3$. При этом $x = 4x''$, $y = 8y'''$. Это означает, что если (x, y) — решение уравнения (3) для $s = 1$, то $(2^2x, 2^3y)$ — решение уравнения (3) для $s = 4$, далее $(2^4x, 2^6y)$ — решение (3) для $s = 7$. По индукции для произвольного $s = 1$ (mod 3) получаем решение $(2^{\frac{2s-2}{3}}x,\ 2^{s-1}y)$. Заметим, что этот результат справедлив, даже если первоначальное $y = y'''$ в решении уравнения (6) нечетно.

Рассмотрим частные случаи значений s.

1. Для $s = 1$ уравнение (4) сводится к

$$2x'^3 = y'^2 + 1 = (1 - iy')(1 + iy').$$

Легко проверить, что $(1 - iy', 1 + iy') = 1 + i$. Тогда

$$1 - iy' = i(1 + i)u,\ 1 + iy' = -i(1 + i)v$$

для некоторых взаимно простых u и v из кольца $\mathbf{Z}[i]$. Тогда

$$2x'^3 = (1 + i)^2uv = 2iuv,$$

значит, $x'^3(-i)^3 = uv$.

Так как u, v взаимно просты, то $u = (-b + ia)^3$ для некоторых целых a и b. Значит, $1 + iy' = i(1 + i)(-b + ia)^3 = (1 + i)(a + ib)^3$.

Сравнение действительной и мнимой частей последнего равенства дает

$$(a+b)(a^2-4ab+b^2)=1.$$

Это возможно лишь при $a=1$, $b=0$ или $a=0$, $b=1$, откуда $y'=\pm1$. Следовательно, $y=\pm2$, $x=2$.

2. Для $s=2$ уравнение (5) сводится к

$$y''^2+1=(y''+i)(y''-i)=4x''^3,$$

откуда следует, что y'' нечетно. Вновь нетрудно убедиться, что для нечетного y'' выполняется $(y''+i, y''-i)=1+i$.

Как и в предыдущем случае,

$$y''+i=(1+i)u,\ y''-i=(1+i)v$$

для некоторых взаимно простых u и v из кольца $\mathbf{Z}[i]$. Тогда

$$4x''^3=(1+i)^2uv=2iuv,$$

откуда $uv=2(-i)x''^3=2(ix'')^3=(1+i)(1-i)(ix'')^3$.

С учетом взаимной простоты u и v возможны следующие двенадцать случаев:

1) $u=2(a+ib)^3$, $v=(a'+ib')^3$;
2) $u=(a+ib)^3$, $v=2(a'+ib')^3$;
3) $u=(1+i)(a+ib)^3$, $v=(1-i)(a'+ib')^3$;
4) $u=(1-i)(a+ib)^3$, $v=(1+i)(a'+ib')^3$;
5) $u=2(ix'')^3$, $v=1$;
6) $u=1$, $v=2(ix'')^3$;
7) $u=1+i$, $v=(1-i)(ix'')^3$;
8) $u=2$, $v=(ix'')^3$;
9) $u=(ix'')^3$, $v=2$;
10) $u=(1-i)(ix'')^3$, $v=1+i$;
11) $u=1-i$, $v=(1+i)(ix'')^3$;
12) $u=(1+i)(ix'')^3$, $v=1-i$.

Сравнивая действительные и мнимые части предыдущих соотношений, получаем, что при нечетном y и $s=2$ уравнение не имеет целочисленных решений.

3. Аналогично рассматриваются случаи $s=3, 4, 5$.

Получаем, что при $s=3$ имеется решение $x=4$, $y=0$.

Для $s=4$ получаем решения $(8, \pm16)$, $(20, \pm88)$.

При $s=5$ уравнение не имеет целочисленных решений.

2. Случай нечетного y

Перепишем уравнение (3) в виде

$$y^2 + 2^{2s} = x^3$$

или эквивалентно в кольце целых гауссовых чисел $\mathbf{Z}[i]$

$$(2^s + iy)(2^s - iy) = x^3.$$

Лемма. *Для целого нечетного y числа $2^s + iy$ и $2^s - iy$ взаимно просты в* $\mathbf{Z}[i]$.

Доказательство леммы элементарно. Из нее сразу следует, что каждое из чисел $2^s + iy$ и $2^s - iy$ является кубом

$$2^s + iy = (a + ib)^3,$$

где a и b — целые, откуда получаем

$$2^s = a^3 - 3ab^2 = a(a^2 - 3b^2), \tag{7}$$
$$y = 3a^2b - b^3 = b(3a^2 - b^2). \tag{8}$$

Из этого следует, что a является степенью 2, а b нечетно. Из выражения (7) следует равенство

$$3b^2 = \frac{-2^s}{a} + a^2. \tag{9}$$

Так как b нечетно, то слагаемые в правой части (9) должны иметь разную четность. Ясно, что $-2^s / a$ четно, а a^2 нечетно при $a = \pm 1$, $-2^s / a$ нечетно, а a^2 четно при $a = \pm 2^s$. Таким образом, получаем четыре возможных значения для a: $a = \pm 1$ и $a = \pm 2^s$ и, значит, имеем следующие четыре случая.

1. Если $a = 1$, то $3b^2 = 1 - 2^s < 0$, чего не может быть.

2. Если $a = -1$, то $3b^2 = 2^s + 1$, откуда следует, что b нечетно, а согласно (8) тогда y четно, что противоречит исходному предположению, следовательно, и этот случай невозможен.

3. Если $a = 2^s$, то $3b^2 = a^2 - 1 = 2^{2s} - 1 = (2^s - 1)(2^s + 1)$ — произведение двух идущих подряд нечетных чисел. Так как 2^s не делится на 3, то остаток от деления 2^s на 3 равен либо 1, либо 2.

В обоих случаях тогда произведение $(2^s - 1)(2^s + 1)$ делится на 3, т. е. $b^2 = (2^{2s} - 1)/3$ — целое число.

Последнее равенство можно переписать в виде

$$2^{2s} - 3b^2 = (2^s - b\sqrt{3})(2^s + b\sqrt{3}) = 1.$$

Это означает, что числа $2^s - b\sqrt{3}$ и $2^s + b\sqrt{3}$ являются единицами вещественного квадратичного поля $\mathbf{Q}(\sqrt{3})$.

Найдем фундаментальную единицу этого поля. Для этого разложим $m = \sqrt{3}$ в цепную дробь:

$a_0 = [\sqrt{3}\,] = 1;$

$\alpha_1 = \dfrac{1}{\{\sqrt{3}\}} = \dfrac{1}{\sqrt{3}-1} = \dfrac{\sqrt{3}+1}{2}$, откуда $a_1 = [\alpha_1] = 1;$

$\alpha_2 = \dfrac{1}{\{\alpha_1\}} = \dfrac{1}{\alpha_1 - 1} = \sqrt{3} + 1$, откуда $a_2 = [\alpha_2] = 2;$

$\alpha_3 = \dfrac{1}{\{\alpha_2\}} = \dfrac{1}{\alpha_2 - 2} = \dfrac{\sqrt{3}+1}{2} = \alpha_1$, откуда $a_3 = a_1$.

Это означает, что $\sqrt{3} = [1, \overline{1, 2}]$ — периодическая цепная дробь с периодом $l = 2$. При этом фундаментальная единица имеет вид $\eta = p_{l-1} + q_{l-1}m$.

Найдем подходящую дробь с номером $l - 1 = 1$:

$$\frac{p_{l-1}}{q_{l-1}} = \frac{p_1}{q_1} = \frac{2}{1}.$$

Таким образом, фундаментальная единица $\eta = 2 + \sqrt{3}$, а любая единица поля $\mathbf{Q}(\sqrt{3}\,)$ равна

$$\varepsilon = \pm(2 + \sqrt{3}\,)^n = x_n + y_n\sqrt{3}.$$

Для различных n получаем:

$n = 1$: $(2 + \sqrt{3}\,)^1 = 2 + \sqrt{3}$, откуда $x_n = 2$, $y_n = 1$;

$n = 2$: $(2 + \sqrt{3}\,)^2 = 7 + 4\sqrt{3}$, откуда $x_n = 7$, $y_n = 4$;

$n = 3$: $(2 + \sqrt{3}\,)^3 = 26 + 15\sqrt{3}$, откуда $x_n = 26$, $y_n = 15$;

$n = 4$: $(2 + \sqrt{3}\,)^4 = 97 + 56\sqrt{3}$, откуда $x_n = 97$, $y_n = 56$;

$n = 5$: $(2 + \sqrt{3}\,)^5 = 362 + 209\sqrt{3}$, откуда $x_n = 362$, $y_n = 209$.

Индукция по n показывает, что

$$x_{n+1} = 4x_n - x_{n-1}, \quad y_{n+1} = 4y_n - y_{n-1}, \tag{10}$$

где вдобавок $x_0 = 1$, $y_0 = 0$, т. е.

$$(2 + \sqrt{3}\,)^{n+1} = (4x_n - x_{n-1}) + (4y_n - y_{n-1})\sqrt{3}.$$

Таким образом, чтобы число $2^s \pm b\sqrt{3}$ было единицей, необходимо, чтобы

$$2^s = x_{n+1} \tag{11}$$

для некоторых n и s. Из условия (11) сразу следует, что x_{n+1} четно.

Из равенств (10) получается, что числа x_{n-1} и x_{n+1} имеют одинаковую четность.

Из предыдущего x_{n+1} четно, если и только если $n + 1$ нечетно, т. е. n четно.

Подстановки (10) дают

$$x_{n+1} = 4x_n - x_{n-1} = 4x_n - (4x_{n-2} - x_{n-3}) = 4(x_n - x_{n-2}) + x_{n-3} =$$
$$= 4(x_n - x_{n-2}) + (4x_{n-4} - x_{n-5}) = 4(x_n - x_{n-2} + x_{n-4}) - x_{n-5} = \ldots =$$
$$= 4\left(x_n - x_{n-2} + x_{n-4} - \ldots + (-1)^{\frac{n-2}{2}} x_2\right) + (-1)^{\frac{n}{2}} x_1 =$$
$$= 4\left(x_n - x_{n-2} + x_{n-4} - \ldots + (-1)^{\frac{n-2}{2}} x_2\right) + (-1)^{\frac{n}{2}} \cdot 2 = 2C_n,$$

где

$$C_n = 2\left(x_n - x_{n-2} + x_{n-4} - \ldots + (-1)^{\frac{n-2}{2}} x_2\right) + (-1)^{\frac{n}{2}} -$$

нечетное число. С учетом этих вычислений равенство (11) сводится к $2^{s-1} = C_n$. Это возможно лишь при $s = 1$. При этом получаем $a = 2$, $b = \pm 1$. Тогда формула (8) дает $y = \pm 11$, а из уравнения (3) находим $x = 5$.

4. Если $a = -2^s$, то $3b^2 = a^2 + 1 = 2^{2s} + 1$. Мы уже доказали, что $2^{2s} - 1$ делится на 3, т. е. $2^{2s} - 1 = 3k$, откуда $2^{2s} + 1 = 3k + 2$ и не делится на 3, это противоречие. Таким образом, этот случай невозможен.

В итоге для нечетного y уравнение имеет целочисленные решения только при $s = 1$.

Заключение

Уравнение (3) имеет следующие целочисленных решения:
1) для $s = 1$: $(2, \pm 2)$, $(5, \pm 11)$;
2) для $s = 2$: решений нет;
3) для $s = 3$: $(4, 0)$.
Далее:
4) для $s \equiv 1 \pmod 3$: $\left(2^{\frac{2s+1}{3}}, \ \pm 2^s\right)$, $\left(5 \cdot 2^{\frac{2s-2}{3}}, \ \pm 11 \cdot 2^{s-1}\right)$;
5) для $s \equiv 2 \pmod 3$: решений нет;
6) для $s \equiv 0 \pmod 3$: $\left(2^{\frac{2s}{3}}, \ 0\right)$.

Непосредственное применение системы компьютерной алгебры Maple для $s = 10$ дает решения:

(128, 1024),
(128, –1024),
(320, 5632),
(320, –5632),

что соответствует полученным результатам.

Список литературы

1. *Айерлэнд К.*, *Роузен М.* Классическое введение в современную теорию чисел. М., 1987.

2. *Cao Z. F.* Diophantine equations and divisibility of class number of real quadratic fields // Acta Mathematica, Sinica. 1994. Vol. 37. P. 625—631.

3. *Dong X. L.*, *Cao Z. F.* Diophantine Equations and Class Numbers of Real Quadratic Fields // Acta Arithmetica, XCVII. 2001. Vol. 4. P. 313—328.

4. *Jacobson M. J.*, *Williams H. C.* Solving the Pell Equation. Springer Science + Business Media, LLC 2009.

5. *Le M.* Divisibility of class number of the real quadratic field $\mathbf{Q}\left(\sqrt{\frac{1+4k^{2n}}{a^2}}\right)$ // Acta Mathematica, Sinica. 1990. Vol. 33. P. 565—574.

6. *Lu H. W.* Divisibility of class number of some real quadratic fields // Ibid. 1985. Vol. 28. P. 756—762.

7. *Yuan P. Z.* Divisibility of class numbers of real quadratic fields // Ibid. 1998.Vol. 41. P. 525—530.

8. *Yuan P. Z.* Some basic problems in Diophantine equations. Ph.D. Thesis. Sichuan University, 1997.

Об авторах

Сергей Иванович Алешников — канд. техн. наук, доц., Балтийский федеральный университет им. И. Канта, Калининград.
E-mail: elliptec@mail.ru

Марина Валерьевна Алешникова — ст. преп., Балтийский федеральный университет им. И. Канта, Калининград.
E-mail: aleshnikova_m_v@mail.ru

Андрей Александрович Горбачёв — канд. техн. наук, доц., Калининградский государственный технический университет.
E-mail: terjer@mail.ru

About the authors

Dr Sergey Aleshnikov, ass. prof., I. Kant Baltic Federal University, Kaliningrad.
E-mail: elliptec@mail.ru

Marina Aleshnikova, head teacher, I. Kant Baltic Federal University, Kaliningrad.
E-mail: aleshnikova_m_v@mail.ru

Dr Andrey Gorbachev, ass. prof., Kaliningrad State Technical University.
E-mail: terjer@mail.ru