

О РЕШЕНИИ НЕКОТОРЫХ КЛАССОВ ДИОФАНТОВЫХ УРАВНЕНИЙ МЕТОДОМ ТОЖДЕСТВ

Ф.Х. УВИЖЕВА, М.Х. КАЛАЖОКОВА

Институт информатики и проблем регионального управления –
филиал ФГБНУ «Федеральный научный центр
«Кабардино-Балкарский научный центр Российской академии наук»
360000, КБР, г. Нальчик, ул. И. Арманд, 37-а
E-mail: iipru@rambler.ru

Решение в целых числах алгебраических уравнений с целыми коэффициентами более чем с одним неизвестным представляет собой одну из важнейших проблем теории чисел. Известно, что в общей постановке задача описания множества решений диофантовых уравнений в целых числах алгоритмически неразрешима. Несмотря на усилия многих поколений математиков, в этой области до сих пор отсутствуют общие эффективные методы их решения. В настоящей работе рассмотрены некоторые классы диофантовых уравнений, решение в целых числах которых представляет интерес как само по себе, так и, например, в процессе исследования сложных дискретных систем, при поиске оптимальных структур в органической химии и молекулярной физике, при расшифровке компьютерных алгоритмов, криптографии, в экономике и теории вероятностей. Используя известные в алгебре тождества и их модификации, а также метод математической индукции и метод Лагранжа, в работе показан эффективный метод решения как классических диофантовых уравнений, так и некоторых их обобщенных вариантов. В результате получены формулы, выражающие целые решения диофантовых уравнений. Этот метод можно применять также и для других классов диофантовых уравнений.

Ключевые слова: диофантовы уравнения, алгебраические тождества, метод математической индукции, тождества Лагранжа, уравнение Пелля.

Диофантово уравнение – это уравнение (как правило, с несколькими неизвестными), решение которого ищется в целых (иногда в натуральных) числах. Некоторые классы таких уравнений были впервые рассмотрены знаменитыми математиками древности Пифагором и Диофантом [1-6]. В память о последнем эти уравнения называются диофантовыми.

1. О решении уравнения $x^2 + y^2 = z^n$.

Пусть требуется решить диофантово уравнение в целых числах:

$$x^2 + y^2 = z^n. \quad (1)$$

Для построения решения уравнения (1) в целых числах воспользуемся тождеством:

$$\begin{aligned} (AA' + BB')(A_1A_1' + B_1B_1') = \\ = (AA' - BB')(A_1A_1' - B_1B_1') + (AB_1 - BA_1)(A_1B_1' - B_1A_1'). \end{aligned} \quad (2)$$

Полагая в тождестве (2) $A = A'$, $B = B'$, $A_1 = A_1'$, $B_1 = B_1'$, получим, что

$$(A^2 + B^2)(A_1^2 + B_1^2) = (AA_1 - BB_1)^2 + (AB_1 - A_1B)^2. \quad (3)$$

Из (3) видно, что произведение двух форм вида $A^2 + B^2$ есть форма такого же вида.

На основании правой части равенства (3) и при $A = a$, $B = b$ уравнение $z^3 = x^2 + y^2$ можно переписать следующим образом:

$$(a^2 + b^2)^3 = (a^3 - 3ab^2)^2 + (3a^2b - b^3)^2.$$

Отсюда получаем решение уравнения $z^3 = x^2 + y^2$ в виде:

$$z = a^2 + b^2, x = a^3 - 3ab^2, y = 3a^2b - b^3,$$

где a и b – произвольные целые числа.

Рассмотрим вывод рекуррентной формулы для решения уравнения $z^n = x^2 + y^2$ методом математической индукции.

Из приведенных вычислений видно, что форма, которой выражается z , не меняется. Поэтому решение уравнения $z^{n-1} = x^2 + y^2$ можно записать так:

$$z = a^2 + b^2, x = x_{n-1}(a, b), y = y_{n-1}(a, b).$$

$$\text{Отсюда имеем } (a^2 + b^2)^{n-1} = x_{n-1}^2(a, b) + y_{n-1}^2(a, b).$$

Умножая обе части последнего соотношения на $a^2 + b^2$, получим:

$$(a^2 + b^2)^n = [x_{n-1}^2(a, b) + y_{n-1}^2(a, b)](a^2 + b^2)$$

или

$$(a^2 + b^2)^n = [ax_{n-1}(a, b) + by_{n-1}(a, b)]^2 + [bx_{n-1}(a, b) - ay_{n-1}(a, b)]^2.$$

Отсюда для уравнения $z^n = x^2 + y^2$ получаем решение в виде рекуррентной формулы:

$$z = a^2 + b^2, x = ax_{n-1}(a, b) + by_{n-1}(a, b), y = bx_{n-1}(a, b) - ay_{n-1}(a, b).$$

Теорема. Решение уравнения $z^n = x^2 + y^2$ можно выразить следующим образом: $z = a^2 + b^2, x = \operatorname{Re}(a + ib)^n, y = \operatorname{Im}(a + ib)^n$, где a, b – целые числа.

Докажем это утверждение методом математической индукции. При $n = 2$ теорема верна. Допустим, что мы доказали ее для $n - 1$, т.е. решения уравнения $z^{n-1} = x^2 + y^2$ имеют вид:

$$z = a^2 + b^2, x_{n-1} = \operatorname{Re}(a + ib)^{n-1}, y_{n-1} = \operatorname{Im}(a + ib)^{n-1},$$

и докажем теорему для n .

Для уравнения $z^n = x^2 + y^2$ можно записать:

$$z = a^2 + b^2, x = a \operatorname{Re}(a + ib)^{n-1} - b \operatorname{Im}(a + ib)^{n-1},$$

$$y = b \operatorname{Re}(a + ib)^{n-1} + a \operatorname{Im}(a + ib)^{n-1},$$

но

$$\operatorname{Re}(a + ib)^{n-1} = \frac{1}{2}[(a + ib)^{n-1} + (a - ib)^{n-1}],$$

$$\operatorname{Im}(a + ib)^{n-1} = \frac{1}{2i}[(a + ib)^{n-1} - (a - ib)^{n-1}].$$

Поэтому

$$x = a \frac{1}{2}[(a + ib)^{n-1} + (a - ib)^{n-1}] - b \frac{1}{2i}[(a + ib)^{n-1} - (a - ib)^{n-1}],$$

$$y = b \frac{1}{2}[(a + ib)^{n-1} + (a - ib)^{n-1}] + a \frac{1}{2i}[(a + ib)^{n-1} - (a - ib)^{n-1}],$$

и получим, что $x = \operatorname{Re}(a + ib)^n$, $y = \operatorname{Im}(a + ib)^n$. Что и требовалось доказать.

2. Уравнение $x^2 + y^2 + z^2 = u^2$.

Полагая

$$A = a_1 + ia_2, A' = a_1 - ia_2, B = a_3 + ia_4, B' = a_3 - ia_4, \\ A_1 = b_1 + ib_2, A'_1 = b_1 - ib_2, B_1 = b_3 + ib_4, B'_1 = b_3 - ib_4$$

в тождестве (2) и произведя некоторые элементарные преобразования, получим:

$$(a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) = \\ = (a_1b_1 + a_2b_2 - a_3b_3 - a_4b_4)^2 + (a_1b_2 - a_2b_1 + a_4b_3 - a_3b_4)^2 + \\ + (a_1b_3 - a_2b_4 + a_3b_1 - a_4b_2)^2 + (a_2b_3 + a_3b_2 + a_1b_4 + a_4b_1)^2,$$

которое представляет собой тождество Эйлера в видоизмененной форме.

Пусть в полученном тождестве $a_1 = b_1$, $a_2 = b_2$, $a_3 = b_3$, $a_4 = b_4$. Тогда будем иметь:

$$(a_1^2 + a_2^2 + a_3^2 + a_4^2)^2 = (a_1^2 + a_2^2 - a_3^2 - a_4^2)^2 + (2a_1a_3 - 2a_2a_4)^2 + (2a_1a_4 + 2a_2a_3)^2. \quad (4)$$

Отсюда получаем формулы, выражающие целые решения уравнения $u^2 = x^2 + y^2 + z^2$ в виде:

$$u = a_1^2 + a_2^2 + a_3^2 + a_4^2, x = a_1^2 + a_2^2 - a_3^2 - a_4^2, y = 2(a_1a_3 - a_2a_4), z = 2(a_1a_4 + a_2a_3),$$

где a_1, a_2, a_3, a_4 – произвольные целые числа.

3. Уравнение $x^2 + y^2 + z^2 + t^2 = u^n$.

Умножая обе части тождества (4) на $(a_1^2 + a_2^2 + a_3^2 + a_4^2)$, получим решение уравнения $u^3 = x^2 + y^2 + z^2 + t^2$. Действительно,

$$(a_1^2 + a_2^2 + a_3^2 + a_4^2)^3 = \left[(a_1^2 + a_2^2 - a_3^2 - a_4^2)^2 + (2a_1a_3 - 2a_2a_4)^2 + \right. \\ \left. + (2a_1a_4 + 2a_2a_3)^2 \right] (a_1^2 + a_2^2 + a_3^2 + a_4^2). \quad (5)$$

Из тождества (5) после некоторых преобразований для решения уравнения $u^3 = x^2 + y^2 + z^2 + t^2$ получаем следующие формулы:

$$u = a_1^2 + a_2^2 + a_3^2 + a_4^2, \\ x = a_1(a_1^2 + a_2^2 - a_3^2 - a_4^2) + 2a_2(a_1a_3 - a_2a_4) - 2a_3(a_1a_4 + a_2a_3), \\ y = 2a_1(a_1a_3 - a_2a_4) - a_2(a_1^2 + a_2^2 - a_3^2 - a_4^2) + 2a_4(a_1a_4 + a_2a_3), \\ z = 2a_1(a_1a_4 + a_2a_3) + a_3(a_1^2 + a_2^2 - a_3^2 - a_4^2) - 2a_4(a_1a_3 - a_2a_4), \\ t = 2a_2(a_1a_4 + a_2a_3) + 2a_3(a_1a_3 - a_2a_4) + a_4(a_1^2 + a_2^2 - a_3^2 - a_4^2).$$

Рассмотрим теперь общий случай.

Пусть имеем уравнение: $u^{n-1} = x^2 + y^2 + z^2 + t^2$. Обозначим решение этого уравнения следующим образом:

$$u = a_1^2 + a_2^2 + a_3^2 + a_4^2, x = x_{n-1}(a_1, a_2, a_3, a_4), y = y_{n-1}(a_1, a_2, a_3, a_4), \\ z = z_{n-1}(a_1, a_2, a_3, a_4), t = t_{n-1}(a_1, a_2, a_3, a_4).$$

Таким образом, имеем соотношения:

$$(a_1^2 + a_2^2 + a_3^2 + a_4^2)^{n-1} = x_{n-1}^2 + y_{n-1}^2 + z_{n-1}^2 + t_{n-1}^2. \quad (6)$$

Умножая обе части рассматриваемого соотношения (6) на $(a_1^2 + a_2^2 + a_3^2 + a_4^2)$, будем иметь:

$$\begin{aligned} (a_1^2 + a_2^2 + a_3^2 + a_4^2)^n &= (a_1 x_{n-1} + a_2 y_{n-1} - a_3 z_{n-1} - a_4 t_{n-1})^2 + \\ &+ (a_1 y_{n-1} - a_2 x_{n-1} + a_4 z_{n-1} - a_3 t_{n-1})^2 + \\ &+ (a_1 z_{n-1} - a_2 t_{n-1} + a_3 x_{n-1} - a_4 y_{n-1})^2 + \\ &+ (a_2 z_{n-1} + a_3 y_{n-1} + a_1 t_{n-1} + a_4 x_{n-1})^2. \end{aligned}$$

Отсюда получаем рекуррентную формулу для решения рассматриваемого уравнения:

$$\begin{aligned} u &= a_1^2 + a_2^2 + a_3^2 + a_4^2, \\ x &= a_1 x_{n-1} + a_2 y_{n-1} - a_3 z_{n-1} - a_4 t_{n-1}, \\ y &= a_1 y_{n-1} - a_2 x_{n-1} + a_4 z_{n-1} - a_3 t_{n-1}, \\ z &= a_1 z_{n-1} - a_2 t_{n-1} + a_3 x_{n-1} - a_4 y_{n-1}, \\ t &= a_2 z_{n-1} + a_3 y_{n-1} + a_1 t_{n-1} + a_4 x_{n-1}. \end{aligned}$$

4. О решении уравнения $y^m = \sum_{i=1}^n x_i^2$.

Для получения формул, выражающих целые решения рассматриваемого уравнения, воспользуемся известным тождеством Лагранжа:

$$\begin{aligned} (a_1^2 + a_2^2 + a_3^2 + \dots a_n^2)(b_1^2 + b_2^2 + b_3^2 + \dots + b_n^2) &= \\ &= (a_1 b_1 + a_2 b_2 + a_3 b_3 + \dots a_n b_n)^2 + (a_1 b_2 - a_2 b_1)^2 + (a_1 b_3 - a_3 b_1)^2 + \\ &+ \dots + (a_1 b_n - a_n b_1)^2 + (a_2 b_3 - a_3 b_2)^2 + \dots + (a_{n-1} b_n - a_n b_{n-1})^2. \end{aligned} \quad (7)$$

Заменяя в тождестве (7) числа $b_2, b_3, b_4, \dots, b_n$ соответственно числами с противоположными знаками $-b_2, -b_3, -b_4, \dots, -b_n$, получим:

$$\begin{aligned} (a_1^2 + a_2^2 + a_3^2 + \dots a_n^2)(b_1^2 + b_2^2 + b_3^2 + \dots + b_n^2) &= \\ &= (a_1 b_1 - a_2 b_2 - a_3 b_3 - \dots - a_n b_n)^2 + (a_1 b_2 + a_2 b_1)^2 + (a_1 b_3 + a_3 b_1)^2 + \\ &+ \dots + (a_1 b_n + a_n b_1)^2 + (a_2 b_3 - a_3 b_2)^2 + \dots + (a_{n-1} b_n - a_n b_{n-1})^2. \end{aligned}$$

В полученном тождестве положим, что $a_1 = b_1, a_2 = b_2, \dots, a_n = b_n$. Тогда получим:

$$\begin{aligned} (a_1^2 + a_2^2 + a_3^2 + \dots a_n^2)^2 &= (a_1^2 - a_2^2 - a_3^2 - \dots - a_n^2)^2 + \\ &+ (2a_1 a_2)^2 + (2a_1 a_3)^2 + (2a_1 a_4)^2 + \dots + (2a_1 a_n)^2. \end{aligned} \quad (8)$$

Очевидно, что в первой части (8) имеем n слагаемых.

Следовательно, из (8) получаем формулы, дающие искомые решения рассматриваемого уравнения:

$$\begin{aligned} y^2 &= x_1^2 + x_2^2 + x_3^2 + \dots + x_n^2, \\ y &= a_1^2 + a_2^2 + a_3^2 + \dots + a_n^2, \quad x_1 = a_1^2 - a_2^2 - a_3^2 - \dots - a_n^2, \\ x_2 &= 2a_1 a_2, \dots, x_n = 2a_1 a_n, \end{aligned}$$

где $a_1, a_2, \dots, a_n$ — целые числа.

Пусть теперь мы имеем решения уравнения $y^{m-1} = \sum_{i=1}^n x_i^2$ в виде:

$$y^{m-1} = x_1^2 + x_2^2 + x_3^2 + \dots + x_n^2, y_{m-1} = a_1^2 + a_2^2 + a_3^2 + \dots + a_n^2,$$

$$x_{1,m-1} = x_1(a_1, a_2, \dots, a_n), x_2 = x_2(a_1, a_2, \dots, a_n), \dots,$$

$$x_{n,m-1} = x_n(a_1, a_2, \dots, a_n).$$

Тогда, подставляя решения в исходное уравнение, получим:

$$(a_1^2 + a_2^2 + a_3^2 + \dots + a_n^2)^{m-1} = [x_{1,m-1}]^2 + [x_{2,m-1}]^2 + \dots + [x_{n,m-1}]^2.$$

Умножив обе части полученного тождества на $(a_1^2 + a_2^2 + \dots + a_n^2)$, получим:

$$(a_1^2 + a_2^2 + \dots + a_n^2)^m = (a_1 x_{1,m-1} - a_2 x_{2,m-1} - \dots - a_n x_{n,m-1})^2 + \\ + (a_1 x_{2,m-1} + a_2 x_{1,m-1})^2 + (a_1 x_{3,m-1} + a_3 x_{1,m-1})^2 + \dots + (a_1 x_{n,m-1} + a_n x_{1,m-1})^2.$$

Из полученного тождества для решения уравнения $y^m = x_1^2 + x_2^2 + \dots + x_n^2$ имеем следующие рекуррентные соотношения:

$$y^m = a_1^2 + a_2^2 + \dots + a_n^2, x_{1,m} = a_1 x_{1,m-1} + a_2 x_{2,m-1} - \dots - a_n x_{n,m-1},$$

$$x_{2,m} = a_1 x_{2,m-1} + a_2 x_{1,m-1}, x_{3,m} = a_1 x_{3,m-1} + a_3 x_{1,m-1}, \dots, x_n = a_1 x_{n,m-1} + a_n x_{1,m-1}.$$

5. О решении уравнения $z^n = x^2 + cxy + my^2$.

Для решения рассматриваемого уравнения воспользуемся одним замечательным свойством бинарной квадратичной формы.

Известно, что произведение бинарных квадратичных форм вида $\Phi(a, b) = a^2 + cab + mb^2$ всегда может быть представлено такой же формой.

Это легко проверить непосредственно, если рассмотреть произведение двух бинарных форм вида $\Phi(a_1, b_1), \Phi(a_2, b_2)$:

$$(a_1^2 + ca_1b_1 + mb_1^2)(a_2^2 + ca_2b_2 + mb_2^2) = (a_1a_2 - mb_1b_2)^2 + c(a_1a_2 - mb_1b_2) \times \\ \times (a_1b_2 + b_1a_2 + cb_1b_2) + m(a_1b_2 + b_1a_2 + cb_1b_2)^2. \quad (9)$$

Преобразуем полученное тождество (9), полагая $a_1 = a_2 = a; b_1 = b_2 = b$:

$$(a^2 + cab + mb^2)^2 = (a^2 - mb^2)^2 + c(a^2 - mb^2) \cdot (2ab + cb^2) + m(2ab + cb^2)^2.$$

Отсюда получаем формулы для целочисленного уравнения $z^2 = x^2 + cxy + my^2$:

$$z = a^2 + cab + mb^2, x = a^2 - mb^2, y = 2ab + cb^2,$$

где c и m – данные целые числа, a и b – произвольные целые числа.

Рассмотрим теперь решение общего уравнения $z^n = x^2 + cxy + my^2$ методом математической индукции.

Пусть для уравнения $z^{n-1} = x^2 + cxy + my^2$ имеем решения в виде $z_{n-1} = a^2 + cab + mb^2, x_{n-1} = x_{n-1}(a, b), y_{n-1} = y_{n-1}(a, b)$ такие, что

$$z^{n-1} = x_{n-1}^2 + cx_{n-1}y_{n-1} + my_{n-1}^2. \quad (10)$$

Умножая обе части (10) на $(a^2 + cab + mb^2)$, получим:

$$\begin{aligned} (a^2 + cab + mb^2)^n &= (a^2 + cab + mb^2)(x_{n-1}^2 + cx_{n-1}y_{n-1} + my_{n-1}^2) = \\ &= (ax_{n-1} - mby_{n-1})^2 + c(ax_{n-1} - mby_{n-1})(ay_{n-1} + bx_{n-1} + cby_{n-1}) + m(ay_{n-1} + bx_{n-1} + cby_{n-1})^2. \end{aligned}$$

Отсюда получаем следующие рекуррентные соотношения для решения рассматриваемого уравнения $z^n = x^2 + cy + my^2$ в виде:

$$z = a^2 + cab + mb^2, x = ax_{n-1} - mby_{n-1}, y = ay_{n-1} + bx_{n-1} + cby_{n-1}.$$

Рассмотрим некоторые частные случаи:

1. Полагая в рассматриваемом уравнении $n = 2, m = 1, c = -1$, получим формулы для целочисленных треугольников с острым углом в 60° .

Действительно, $z^2 = x^2 + y^2 - xy$: $z = a^2 + b^2 - ab, x = a^2 - b^2, y = 2ab - b^2$.

Аналогично при $n = 2, m = 1, c = 1$ получаем следующие формулы для численных треугольников с тупым углом в 120° :

$$z^2 = x^2 + y^2 + xy: \quad z = a^2 + b^2 + ab, x = a^2 - b^2, y = 2ab + b^2.$$

2. При $c = 0$ получаем: $z^2 = x^2 + my^2$: $z = a^2 + mb^2, x = a^2 - mb^2, y = 2ab$. Для уравнения $z^3 = x^2 + my^2$ получаем:

$$z = a^2 + mb^2, x = a^3 - 3mab^2, y = 3ab - mb^3.$$

Для уравнения $z^n = x^2 + my^2$ будем иметь:

$$z = a^2 + mb^2, x = ax_{n-1} - maby_{n-1}, y = ay_{n-1} + bx_{n-1}.$$

Теорема 1. Формулы вида

$$z = a^2 + mb^2, x = \operatorname{Re}(a + i\sqrt{mb})^n, y = \frac{1}{\sqrt{m}} \operatorname{Im}(a + i\sqrt{mb})^n$$

дают целые решения уравнения $z^n = x^2 + my^2, m > 0$.

Доказательство (методом математической индукции):

Для $n = 2$ указанные формулы верны. Допустим, что мы доказали справедливость этих формул для $n = 1$. По допущению имеем, что

$$(a^2 + mb^2)^{n-1} = \left[\operatorname{Re}(a + i\sqrt{mb})^{n-1} \right]^2 + m \left[\frac{1}{\sqrt{m}} \operatorname{Im}(a + i\sqrt{mb})^{n-1} \right]^2.$$

Тогда для решения уравнения имеем, что:

$$z = a^2 + mb^2,$$

$$x = a \operatorname{Re}(a + i\sqrt{mb})^{n-1} - mb \frac{1}{\sqrt{m}} \operatorname{Im}(a + i\sqrt{mb})^{n-1},$$

$$y = a \frac{1}{\sqrt{m}} \operatorname{Im}(a + i\sqrt{mb})^{n-1} + b \operatorname{Re}(a + i\sqrt{mb})^{n-1},$$

но

$$\operatorname{Re}(a + i\sqrt{mb})^{n-1} = \frac{1}{2} \left[(a + i\sqrt{mb})^{n-1} + (a - i\sqrt{mb})^{n-1} \right],$$

$$\operatorname{Im}(a + i\sqrt{mb})^{n-1} = \frac{1}{2i} \left[(a + i\sqrt{mb})^{n-1} - (a - i\sqrt{mb})^{n-1} \right].$$

После некоторых преобразований выражений для x и y получим:

$$\begin{aligned} x &= a \frac{1}{2} \left[\left(a + i\sqrt{mb} \right)^{n-1} + \left(a - i\sqrt{mb} \right)^{n-1} \right] - mb \frac{1}{\sqrt{m}} \frac{1}{2i} \left[\left(a + i\sqrt{mb} \right)^{n-1} - \left(a - i\sqrt{mb} \right)^{n-1} \right] = \\ &= \frac{1}{2} \left[\left(a + i\sqrt{mb} \right)^n + \left(a - i\sqrt{mb} \right)^n \right] = \operatorname{Re} \left(a + i\sqrt{mb} \right)^n, \\ y &= \frac{1}{\sqrt{m}} \frac{a}{2i} \left[\left(a + i\sqrt{mb} \right)^{n-1} - \left(a - i\sqrt{mb} \right)^{n-1} \right] + \frac{b}{2} \left[\left(a + i\sqrt{mb} \right)^{n-1} + \left(a - i\sqrt{mb} \right)^{n-1} \right] = \\ &= \frac{1}{\sqrt{m}} \frac{1}{2i} \left[\left(a + i\sqrt{mb} \right)^n - \left(a - i\sqrt{mb} \right)^n \right] = \frac{1}{\sqrt{m}} \operatorname{Im} \left(a + i\sqrt{mb} \right)^n. \end{aligned}$$

Что и требовалось доказать.

3. Пусть теперь $m < 0$. В этом случае можно рассматривать уравнение $z^n = x^n - my^2$, где $m > 0$. Тогда будем иметь:

$$\begin{aligned} z^2 &= x^2 - my^2 & z^3 &= x^2 - my^2 & z^n &= x^2 - my^2 \\ z &= a^2 - mb^2 & z &= a^2 - mb^2 & z &= a^2 - mb^2 \\ x &= a^2 + mb^2 & x &= a^3 + 3mab^2 & x &= ax_{n-1} + mby_{n-1} \\ y &= 2ab & y &= 3a^2b + b^3 & y &= ay_{n-1} + bx_{n-1}, m > 0. \end{aligned}$$

Теорема 2. Формулы

$$\begin{aligned} z &= a^2 - mb^2, \\ x &= \frac{1}{2} \left[\left(a + \sqrt{mb} \right)^n + \left(a - \sqrt{mb} \right)^n \right], \\ y &= \frac{1}{2\sqrt{m}} \left[\left(a + \sqrt{mb} \right)^n - \left(a - \sqrt{mb} \right)^n \right] \end{aligned}$$

дают целые решения уравнения $z^n = x^2 - my^2$ при $m > 0$. Доказывается методом математической индукции с применением формул, приведенных выше.

6. Уравнение Пелля и уравнение $x^2 + my^2 = k^n$.

Доказанные выше теоремы 1 и 2 позволяют доказать следующие теоремы относительно уравнения Пелля $x^2 + my^2 = k$ и уравнения $x^2 + my^2 = k^n$.

Теорема 3. Всякое целочисленное решение уравнения $x^2 + my^2 = k^n$ при положительном m имеет вид:

$$x = \operatorname{Re} \left(x_0 + \sqrt{m}iy_0 \right)^n, y = \frac{1}{\sqrt{m}} \operatorname{Im} \left(x_0 + \sqrt{m}iy_0 \right)^n,$$

где (x_0, y_0) – произвольное решение Пелля $x_0^2 + my_0^2 = k$.

Доказательство: По условию теоремы $k = x_0^2 + my_0^2$, отсюда

$$k^n = \left(x_0^2 + my_0^2 \right)^n. \quad (11)$$

Правую часть равенства (11) на основании теоремы 1 можно переписать так:

$$\left(x_0^2 + my_0^2 \right)^n = \left[\operatorname{Re} \left(x_0 + i\sqrt{m}y_0 \right)^n \right]^2 + m \left[\frac{1}{\sqrt{m}} \operatorname{Im} \left(x_0 + i\sqrt{m}y_0 \right)^n \right]^2.$$

Отсюда

$$k^n = \left[\operatorname{Re} \left(x_0 + i\sqrt{m}y_0 \right)^n \right]^2 + m \left[\frac{1}{\sqrt{m}} \operatorname{Im} \left(x_0 + i\sqrt{m}y_0 \right)^n \right]^2.$$

Теорема 4. Всякое целочисленное решение уравнения $x^2 - my^2 = k^n$ при положительном m имеет вид:

$$x_n = \frac{1}{2} \left[\left(x_0 + \sqrt{m}y_0 \right)^n + \left(x_0 - i\sqrt{m}y_0 \right)^n \right],$$

$$y_n = \frac{1}{2\sqrt{m}} \left[\left(x_0 + \sqrt{m}y_0 \right)^n - \left(x_0 - \sqrt{m}y_0 \right)^n \right],$$

в которых x_0, y_0 являются решением уравнения Пелля.

Доказательство аналогично доказательству предыдущей теоремы. По условию теоремы имеем, что $x_0^2 - my_0^2 = k$.

Отсюда, найдя k^n , получим:

$$k^n = \left(x_0^2 + my_0^2 \right)^n = \left\{ \frac{1}{2} \left[\left(x_0 + \sqrt{m}y_0 \right)^n + \left(x_0 - \sqrt{m}y_0 \right)^n \right] \right\}^2 -$$

$$- m \left\{ \frac{1}{2\sqrt{m}} \left[\left(x_0 + \sqrt{m}y_0 \right)^n - \left(x_0 - \sqrt{m}y_0 \right)^n \right] \right\}^2.$$

Следствие. При $k=1$ получаем следующее утверждение: всякое решение уравнения $x^2 - my^2 = 1$ при положительном m имеет вид:

$$x_n = \frac{1}{2} \left[\left(x_0 + \sqrt{m}y_0 \right)^n + \left(x_0 - i\sqrt{m}y_0 \right)^n \right],$$

$$y_n = \frac{1}{2\sqrt{m}} \left[\left(x_0 + \sqrt{m}y_0 \right)^n - \left(x_0 - \sqrt{m}y_0 \right)^n \right],$$

где x_0, y_0 – какое-либо решение данного уравнения Пелля $x^2 - my^2 = 1$.

В заключение отметим, что изложенный в работе метод тождеств для решения диофантовых уравнений можно применить для решения и других классов диофантовых уравнений.

ЛИТЕРАТУРА

1. Виноградов И.М. Основы теории чисел. М.: Издательство «Наука». Главная редакция физико-математической литературы, 1965.
2. Арнольд И.В. Теория чисел. М.: Государственное учебно-педагогическое издательство Наркомпроса РСФСР, 1989.
3. Сушкевич А.К. Теория чисел. Харьков: Издательство Харьковского университета имени А.М. Горького. 1954.
4. Гельфонд А.О. Решение уравнений в целых числах. М.-Л.: Государственное издательство технико-теоретической литературы, 1952.
5. Серпинский В. О решении уравнений в целых числах. М.: Государственное издательство физико-математической литературы, 1961.
6. Минухин Б.Л. Об одном методе решения диофантовых уравнений. Математическое просвещение. Выпуск третий. М.: Государственное издательство физ.-мат. лит., 1958.
7. Новоселов С.И. Специальный курс элементарной алгебры. М.: Издательство «Высшая школа». 1965.
8. Давенпорт Г. Высшая арифметика. М.: Издательство «Наука». Главная редакция физико-математической литературы, 1965.

REFERENCES

1. Vinogradov I.M. *Osnovy teorii chisel* [Fundamentals of number theory]. M.: Nauka Publishing House. Main editorial office of physical and mathematical literature, 1965.
2. Arnold I.V. *Teoriya chisel* [Number theory]. M.: State Pedagogical Publishing House of the People's Commissariat of Education of the RSFSR, 1989.
3. Sushkevich A.K. *Teoriya chisel* [Number theory]. Kharkov: Publishing House of Kharkov University n.a. A.M. Gorky. 1954.
4. Gelfond A.O. *Reshenie uravnenij v celyh chislakh* [Solving equations in integers]. M.-L.: State Publishing House of technical and theoretical literature, 1952.
5. Serpinsky V. *O reshenii uravnenij v celyh chislakh* [On the solution of equations in integers]. M.: State Publishing House of physical and mathematical literature, 1961.
6. Minukhin B.L. *Ob odnom metode resheniya diofantovykh uravnenij* [On a method for solving diophantine equations]. Mathematical Enlightenment. Issue three. M.: State Publishing House for physical and mathematical lit., 1958.
7. Novoselov S.I. *Special'nyj kurs elementarnoj algebrы* [Special course of elementary algebra]. M.: "Higher School" Publishing House. 1965.
8. Davenport G. *Vyssshaya arifmetika* [Higher arithmetic]. M.: Nauka Publishing House. Main editorial office of physical and mathematical literature, 1965.

ON SOLVING OF SOME CLASSES OF DIOPHANTINE EQUATIONS BY THE METHOD OF IDENTITIES

F.KH. UVIZHEVA, M.KH. KALAZHOKOVA

Institute of Computer Science and Problems of Regional Management –
branch of Federal public budgetary scientific establishment "Federal scientific center
"Kabardin-Balkar Scientific Center of the Russian Academy of Sciences"
360000, KBR, Nalchik, 37-a, I. Armand St.
E-mail: iipru@rambler.ru

Solving algebraic equations with integer coefficients with more than one unknown integer coefficient is one of the most important problems in number theory. It is known that in the general formulation the problem of describing the set of solutions of Diophantine equations in integers is algorithmically insoluble. Despite the efforts of many generations of mathematicians, there are still no general effective methods for their solving in this area. In this paper, we consider some classes of Diophantine equations, the solution in integers of which is of interest both by itself and, for example, in the process of studying complex discrete systems, in searching for optimal structures in organic chemistry and molecular physics, in decoding of computer algorithms, in cryptography, economics and probability theory. Using the identities and their modifications known in algebra, as well as the method of mathematical induction and the Lagrange method, the work shows an effective method for solving both classical Diophantine equations and some of their generalized variants. As a result, we can get formulas expressing general solutions of Diophantine equations. This method can also be applied to other classes of Diophantine equations.

Keywords: Diophantine equations, algebraic identities, mathematical induction method, Lagrange identities, Pell equation.

Работа поступила 06.03.2019 г.