Вестник КРАУНЦ. Физ.-мат. науки. 2016. № 2(13). С. 18-23. ISSN 2079-6641

DOI: 10.18454/2079-6641-2016-13-2-18-23

УДК 517.91

О ЛИНЕЙНЫХ ДИОФАНТОВЫХ УРАВНЕНИЯХ И СПОСОБАХ ИХ РЕШЕНИЯ

А. Х. Кодзоков, З. О. Бесланеев, А. Л. Нагоров, М. Б. Тхамоков

Кабардино-Балкарский государственный университет им. Х.М. Бербекова
360004, КБР, г. Нальчик, ул. Чернышевского, 173
E-mail: kodzoko@mail.ru

В работе рассматриваются способы решения линейных диофантовых уравнений как в частном случае с двумя неизвестными, так и в общем случае с несколькими неизвестными. Основной результат содержится в теореме 1, в которой дается общий способ решения любого диофантова уравнения, основанный на сравнениях по подходящему модулю

Ключевые слова: линейные диофантовы уравнения, сравнения по модулю, метод алгоритма Евклида

MSC 34L99

ABOUT THE LINEAR DIOPHANTINE EQUATIONS AND WAYS OF THEIR SOLUTIONS

A. Kh. Kodzokov, Z. O. Beslaneev, A. L. Nagorov, M. B. Tkhamokov

Kabardino-Balkarian state university of H.M. Berbekov 360004, KBR, Nalchik, Chernyshevsky str., 173
E-mail: kodzoko@mail.ru

The paper discusses ways to solve linear Diophantine equations in the particular case of two unknowns, and, in general, with a few unknowns. The main result is contained in Theorem 1, which provides a general method for solving any Diophantine equation, based on a comparison of the relevant module.

Key words: linear Diophantine equations, congruence modulo, Euclidean algorithm method

Введение

Диофантовым или неопределенным уравнением называют уравнение, которое должно быть в целых числах [1]. Иначе говоря, уравнения вида:

$$P(x_1,\ x_2,\ldots,x_n)=0,\quad n\geq 2,$$

где $P(x_1,\ x_2,\ldots,x_n)$ – многочлен с целыми коэффициентами, которые требуется решить в целых числах, называются диофантовыми уравнениями, по имени греческого математика Диофанта (III век н.э.), изучавшего некоторые такие уравнения простейшего вида. Но и до Диофанта математики занимались такими уравнениями; так, например, Пифагор рассматривал уравнение $x^2+y^2=z^2$, называемое его именем. Геометрический смысл этого уравнения состоит в том, что решения дают прямоугольный треугольник, длины сторон которых являются целыми числами.

Определение. Линейным диофантовым уравнением с n неизвестными называется уравнение вида:

$$a_1x_1+a_2x_2+\ldots+a_nx_n=b, \tag{1}$$

где все коэффициенты $a_1,a_2,\ldots,a_n,b$ – целые числа, и неизвестные могут принимать только целые значения.

Линейные диофантовы уравнения с двумя неизвестными

Сначала будем рассматривать линейные диофантовы уравнения с двумя неизвестными

$$ax+by=c, \tag{2}$$

где a,b,c – целые числа, а неизвестные x,y принимают целые значения [2].

Рассмотрим свойства линейных диофантовых уравнений с двумя неизвестными [3], [4].

Предложение 1. Если правая часть уравнения (2) не делится на наибольший общий делитель $d=(a,b)$ коэффициентов при неизвестных, то это уравнение не имеет решений в целых числах.

Предложение 2. Пусть $d=(a,b)$, $d|c$ и (x_0,y_0) – некоторое решение уравнения (2) в целых числах совпадает с множеством пар $\left(x',y'\right)$, где $x'=x_0+\frac{b}{d}t$; $y'=y_0+\frac{a}{d}t$, где t – любое целое число.

Доказательство. Пусть $\left(x',y'\right)$ – произвольное решение уравнения (2), то есть

$$ax'+by'=c. \tag{3}$$

Так как по условию (x_0,y_0) есть решение уравнения (2), то

$$ax_0+by_0=c, \tag{4}$$

Вычитая теперь почленно из (3) равенство (4), получим

$$a\left(x'-x_0\right)+b\left(y'-y_0\right)=0.$$

Деля теперь обе части этого уравнения на d, будем иметь

$$\frac{a}{d}\left(x^{'}-x_0\right)+\frac{b}{d}\left(y^{'}-y_0\right)=0,$$

где коэффициенты $\frac{a}{d}$ и $\frac{b}{d}$ – целые взаимно простые числа. Из последнего равенства следует делимость

$$\frac{b}{d}\Big|\frac{a}{d}\left(x^{'}-x_0\right).$$

Но так как $\left(\frac{a}{d},\frac{b}{d}\right)=1$, то тогда $\frac{b}{d}\Big|\left(x^{'}-x_0\right)$. Отсюда следует, что $\left(x^{'}-x_0\right)=\frac{b}{d}t$ при некотором целом t, то есть $x^{'}=x_0+\frac{b}{d}t$, где t – любое число.

Далее, подставляя найденное значение x в (3), получаем

$$by^{'}=c-ax^{'}=c-a\left(x_0+\frac{b}{d}t\right)=c-ax_0-\frac{ab}{d}t=by_0-\frac{ab}{d}t,$$

откуда после сокращения на число b будем иметь

$$y^{'}=y_0-\frac{a}{d}t.$$

Таким образом, любое решение уравнения (2) в целых числах имеет вид

$$x^{'}=x_0+\frac{b}{d}t, y^{'}=y_0-\frac{a}{d}t,$$

где t – любое целое число. Предложение 2 доказано. □

Перейдем теперь к рассмотрению способов решения линейных диофантовых уравнений с двумя неизвестными. Нами уже получены формулы для нахождения значений неизвестных в линейном диофантовом уравнении (2), если известно какое-нибудь одно решение (x_0,y_0) этого уравнения.

Наша цель теперь состоит в том, чтобы рассмотреть способы нахождения частного решения уравнения (2).

Разработкой методов решения диофантовых уравнений первым начал заниматься Л. Эйлер. В «Универсальной арифметике» Эйлера изложены два способа решения в целых числах уравнения (2) с целыми коэффициентами.

Первый способ заключается в том, что неизвестное xв уравнении (2) выражается через y,то есть $x=\frac{c-by}{a}$, причем берутся только $y>0$, $x>0$. Подбираются такие целые положительные значения y, чтобы $c-by>0$, то есть чтобы выполнились неравенства $0<y<\frac{c}{b}$. Но этот способ действует только при $c>d$; при этом, если отношение $\frac{c}{b}$ является достаточно большим, то этот способ требует большого числа испытаний.

Второй способ (деление на наименьший коэффициент) Эйлер показывает на примере, причем он основан на алгоритме Евклида. Не нарушая общности рассуждений, будем искать частное решение уравнения (2) в следующем виде $x_0=\frac{c}{d}X_0$, $y_0=\frac{c}{d}Y_0$, где $d=(a,b)$. Тогда уравнение (2) преобразуется к виду:

$$aX_0+bY_0=d. \tag{5}$$

Полученное соотношение (5) есть линейное представление НОД чисел a и b. Поэтому неизвестные X_0 и Y_0 можно найти при помощи алгоритма Евклида, примененного к числам aи b, а значит, найдем значения и для x_0 и y_0.

Рассмотрим на примере метод алгоритма Евклида решения линейного диофантова уравнения с двумя неизвестными.

Пример. Решить с помощью алгоритма Евклида уравнение

$$50x - 42y = 34,$$

в целых числах. Здесь $(50,42) = 2$; причем $2|34$ и значит, что уравнение имеет решение в целых числах. Сначала найдем частное решение уравнения вида $50x - 42y = 2$.

Пусть (X_0, Y_0) – частное решение этого уравнения, то есть

$$50X_0 - 42Y_0 = 2.$$

Для этого к числам 50 и 42 применим алгоритм Евклида. Имеем следующую цепочку равенств, дающих деление с остатком:

$$50 = 42 \cdot 1 + 8,\ 42 = 8 \cdot 5 + 2,\ 8 = 4 \cdot 2,$$

Из предпоследнего равенства имеем $2 = 42 - 8 \cdot 5$. Из первого равенства находим $8 = 50 - 42$. Тогда для $(50,42)$ получим:

$$2 = 42 - (50 - 42) \cdot 5 = 42 \cdot 6 - 60 \cdot 5 = 50 \cdot (-5) - 42 \cdot (-6).$$

Это есть линейное представление $(50,42)$. Значит $X_0 = -5$; $Y_0 = -6$. Теперь получаем следующее частное решение:

$$x_0 = \frac{c}{d}X_0 = \frac{34}{2}(-5) = -85,\ y_0 = \frac{c}{d}Y_0 = \frac{34}{2}(-6) = -102.$$

Тогда общее решение исходного уравнения будет иметь вид:

$$x = x_0 + \frac{b}{d}t = -85 - \frac{42}{2}t = -85 - 21t,\ y = y_0 - \frac{a}{d}t = -102 - \frac{50}{2}t = -102 - 25t,$$

где t принимает любое целое значение.

Соответствующими преобразованиями это общее решение можно также привести к виду:

$$x = 20 + 21u,\ y = 23 + 25u,$$

где u принимает любое целое значение.

Более удобным, чем способ алгоритма Евклида, является способ решения линейного диофантова уравнения (2), основанный на замене данного уравнения сравнением по подходящему модулю.

Предложение 3. Если x_0 удовлетворяет сравнению $ax \equiv c \pmod{b}$, то упорядоченная пара чисел $\left(x_0, \frac{c - ax_0}{b}\right)$ есть решение линейного диофантова уравнения (2).

Доказательство. Из $ax_0 \equiv c \pmod{b}$ следует, что $b|c - ax_0$, то есть $\frac{c - ax_0}{b}$ есть целое число. Проверим, что $\left(x_0, \frac{c - ax_0}{b}\right)$ есть решение уравнения (2).

В самом деле, имеем $ax_0 + b \cdot \dfrac{c - ax_0}{b} = ax_0 + c - ax_0 = c$. Это и означает, что пара $\left(x_0, \dfrac{c - ax_0}{b}\right)$ есть решение уравнения (2). Предложение 3 доказано. □

Продемонстрируем этот метод на том же уравнении, решенным с помощью алгоритма Евклида.

Пример. Решить диофантово уравнение $50x - 42y = 34$ методом сравнения.

Решение. Заменим это уравнение сравнением $50x \equiv 34 \pmod{42}$. Сокращая обе части и модуль сравнения на 2, получим $25x \equiv 17 \pmod{21}$ или, что то же самое $4x \equiv 17 \pmod{21}$, то есть $4x \equiv -4 \pmod{21}$. Сокращая обе части этого сравнения на 4, получим $x \equiv -1 \pmod{21}$, то есть $x \equiv 20 \pmod{21}$. Значит, в силу предложения 3, $x_0 = 20$, $y_0 = \dfrac{c - ax_0}{b} = \dfrac{34 - 50 \cdot 20}{-42} = 23$ дают частное решение данного уравнения. Тогда, в силу предложения 2, любое решение данного диофантова уравнения имеет вид $x = 20 + 21t$, $y = 23 + 25t$, где t принимает любое целое значение.

Линейные диофантовы уравнения с n неизвестными

Перейдем теперь к обобщению способа решения любого линейного диофантова уравнения (1). Введем обозначения:

$$\Delta_1 = (a_1,\ a_2, \ldots, a_n), \Delta_2 = (a_2,\ a_3, \ldots, a_n),$$

$$\Delta_k = (a_k,\ a_{k+1}, \ldots, a_n), \Delta_n = (a_n) = a_n.$$

Уравнение (1) будет разрешено в целых числах, если $\Delta_1 | b$, если же $\Delta_1 \nmid b$, то уравнение (1) неразрешимо в целых числах. Пусть $\Delta_1 | b$, то есть уравнение (1) имеет решения в целых числах. Перепишем уравнение (1) в следующем виде:

$$a_2x_2 + \ldots + a_nx_n = b - a_1x_1.$$

Тогда найдется $x_1 = x_1^{(0)} \in Z$, что выполняется делимость $\Delta_2 | b - a_1x_1^{(0)}$, то есть

$$a_1x_1^{(0)} \equiv b \pmod{\Delta_2}.$$

Тогда в качестве значения неизвестного x_1 можно взять любое число из класса вычетов $x_1 \equiv x_1^{(0)} \pmod{\Delta_2}$. Обозначим

$$b_2 = b - a_1x_1^{(0)}$$

и рассмотрим уравнение

$$a_2x_2 + \ldots + a_nx_n = b_2.$$

Перепишем опять это уравнение в следующем виде

$$a_3x_3 + \ldots + a_nx_n = b - a_2x_2.$$

В силу предыдущего рассуждения имеем, что найдется целое значение $x_1 = x_1^{(0)} \in Z$, что выполняется делимость $\Delta_3 | b_2 - a_2x_2^{(0)}$, то есть

$$a_2x_2^{(0)} \equiv b_2 \pmod{\Delta_3}.$$

Тогда в качестве значения неизвестного x_2 можно взять любое число из класса вычетов $x_2 \equiv x_2^{(0)} \pmod{\Delta_3}$. Продолжая этот процесс, на предпоследнем шаге получим сравнение вида

$$a_{n-1}x_{n-1}^{(0)} \equiv b_{n-1} \pmod{\Delta_n}.$$

Тогда в качестве значения неизвестного x_{n-1} можно взять любое число из класса вычетов $x_{n-1} \equiv x_{n-1}^{(0)} \pmod{\Delta_n}$.

На последнем шаге получаем уравнение вида

$$a_n x_n = b_{n-1} - a_{n-1}x_{n-1}^{(0)},$$

откуда

$$x_n = \frac{b_{n-1} - a_{n-1}x_{n-1}^{(0)}}{\Delta_n},$$

или, если обозначить $b_n = b_{n-1} - a_{n-1}x_{n-1}^{(0)}$, то $x_n = \frac{b_n}{\Delta_n}$.

Аналогично случаю предложения 3 можно показать (но на этом не будем останавливаться), что получающийся набор чисел $\left(x_1^{(0)},\ x_2^{(0)}, \ldots, x_n^{(0)}\right)$ в указанном процессе действительно приводит к решению уравнения (1).

Таким образом, нами получена следующая

Теорема. *Любое решение линейного диофантова уравнения* $a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$, *при* $(a_1, a_2, \ldots, a_n) | b$ *имеет вид* $\left(x_1^{(0)},\ x_2^{(0)}, \ldots, x_n^{(0)}\right)$, *где* $a_k x_k^{(0)} \equiv b_k \pmod{\Delta_{k+1}}$ *при* $1 \le k \le n-1$; $x_n^{(0)} = \frac{b_n}{\Delta_n}$; b_k *определяются рекуррентными соотношениями* $b_k = b_{k-1} - a_{k-1}x_{k-1}^{(0)}$; $2 \le k \le n$.

Пример. Найти какое-нибудь решение уравнения

$$12x_1 + 10x_2 + 6x_3 + 15x_4 = 18,$$

в целых числах.

Решение. Рассматриваем сравнение $12x_1 \equiv 18 \pmod{1}$; здесь $\Delta_2 = (10, 6, 5) = 1$. Возьмем, например, $x_1^{(0)} = 1$.

Тогда рассмотрим новое уравнение $10x_2 + 6x_3 + 15x_4 = 6$; здесь $b_2 = 6$. Получаем сравнение $10x_2 \equiv 6 \pmod{3}$, здесь $\Delta_3 = (6, 15) = 3$.

Возьмем, например, $x_2^{(0)} = 3$. Тогда составляем еще новое уравнение $6x_3 + 15x_4 = -24$, здесь $b_3 = -24$. Опять рассматриваем сравнение $6x_3 \equiv -24 \pmod{15}$; здесь $\Delta_4 = 15$.

Возьмем $x_3^{(0)} = 1$. Тогда на последнем шаге получаем $15x_4 = -30$, откуда $x_4^{(0)} = -2$.

Таким образом $(1; 3; 1; -2)$ есть одно из решений данного уравнения.

Список литературы

[1] Башмакова И. Г., *Диофант и диофантовы уравнения*, Наука, М., 1972, 68 с.

[2] Соловьев Ю. Н., "Неопределенные уравнения первой степени", *Квант*, 1992, № 4, 42-46.

[3] Бухштаб А. А., *Теория чисел*, Просвещение, М., 1966, 385 с.

[4] Серпинский В., *О решении уравнений в целых числах*, Физматлит, М., 1961, 88 с.

Поступила в редакцию / Original article submitted: 29.03.2016