УДК 517.1

Ж.С.Сатаров – д. ф.-м. н., профессор, ОшТУ

ТЕОРИЯ ЛИНЕЙНЫХ ДИОФАНТОВЫХ УРАВНЕНИЙ: СТРУКТУРА РЕШЕНИЙ И ПРИКЛАДНЫЕ АСПЕКТЫ

В заметке выявляется структура решений линейного диофантова уравнения с n переменными. Находятся все неотрицательные решения этого уравнения. Продемонстрируетсятеориянаконкретномприкладномпримере.

Ключевые слова: Диофантово уровнение, общее решение, прикладные аспекты, структура решений

Satarov Zh.S.- D. of ph. and m. s., Professor of OshTU

OF THE THEORY LINEAR DIOFANT EQUATIONS: THE STRUCTURE OF SOLUTIONS AND APPLIED ASPECTS

This paper deals with the structure solutions of linear diofant equations with n variable. All nonnegative solutions of this equation are discoved. The theory of concrete applied models are being demonstrated

Keywords: Diofant's equation, general solution, applied aspects, structure of solutions.

1. Структура решений

Рассматривается диофантово уравнение

$$a_1x_1 + a_1x_2 + \cdots + a_nx_n = a_0, \quad n \geq 2, \ (a_0)$$

где $a_i \in Z, \quad a_1a_2 \ldots a_n \neq 0$ (и неизвестные x_i также считаются целыми). Пусть d_1 означает наибольший общий делитель (НОД) коэффициентов $a_1, \ldots, a_n$. Очевидно, что если d_1 не делит a_0, то уравнение (a_0) не имеет решений. Но при $d_1 | a_0$ оно (целые) решения уже имеет всегда (см, например, [1]). Нашей целью в этом пункте является выявление структуры (всех) решений (a_0) считая $a_0 : d_1$. Как показывают равенства $a_k x_k = (-a_k)(-x_k)$, при необходимости можно произвести замены коэффициентов из (a_0) на их противоположные. Наже мы коэффициенты $a_k, k = 1, \ldots, n,$ раз и навсегда (и без потери общности) будем считать натуральными.

Задав начальное значение как индуктивно вводим следующие НОД

Наш подход к вопросу основывается на какую-то (не важно какую!) систему линейных представлений этих НОД

$$\begin{cases} d_n = x_n a_n, \\ d_{n-1} = x_{n-1} a_{n-1} + y_{n-1} d_n, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ d_k = x_k a_k + y_k d_{k+1}, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ d_1 = x_1 a_1 + y_1 d_2, \\ d_0 = y_0 d_1 \end{cases} \quad (lp)$$

(здесь $x_k, y_k \in Z$ при всех $k = 1,\dots,n-1$ и положено для общности $x_n = y_0 = 1$). Пусть $k, q -$ произвольные номера, для которых $0 \le k \prec q \le n.$ Из коэффициентов (a_0) и разложений (lp) составим величины

$$\sigma_q^k = \frac{a_k}{d_k}\left(\prod_{k\prec i\prec q} y_i\right)x_q,$$

где для общности рассуждений считается $\prod_{r-1\prec i\prec r} y_i = 1.$ Умножая равенства из (lp) с номерами $t, t \ge k,$ на $\frac{d_k}{d_{k-1}}\prod_{t\prec i\prec n} y_i.$ соотвенственно и почленно складывая их, мы приходим к

$$\frac{a_{k-1}}{d_{k-1}}\cdot d_k = \sigma_k^{k-1}a_k + \sigma_{k+1}^{k-1}a_{k+1} + \dots + \sigma_n^{k-1}a_n \quad (lp_k)$$

(т.е. к линейному представлению $\frac{a_{k-1}}{d_{k-1}}\cdot d_k$ через коэффициенты $a_k, a_{k+1},\dots,a_n,$ здесь считается $d_0 = d_1$).

При $k = 1$ равенство (lp_k) дает нам

$$a_0 = \sigma_1^0 a_1 + \sigma_2^0 a_2 + \dots + \sigma_n^0 a_n.$$

Это означает, что вектор $A^0 = \langle \sigma_1^0, \sigma_2^0, \dots, \sigma_n^0 \rangle$ есть (какое-то) решение уравнения (a_0). При значениях $k \succ 1$ те же (lp_k) показывают, что векторы

$$A^{k-1} = \left\langle 0,\dots,0,-\frac{d_k}{d_{k-1}}, \sigma_k^{k-1},\dots,\sigma_n^{k-1} \right\rangle$$

(длины n, случай отсутствия нулей включается) являются решениями однородного уравнения $a_1x_1 + a_2x_2 + \dots + a_nx_n = 0. \ (0)$

Обозначим через $S(a_0)$ и множества решений уравнений (a_0) и соответственно. Между ними существует связь Она показывает, что строение решений польностью определяется слагаемым . Слагаемое образует абелеву группу (в частности, оно выдерживает сложение и умножения на целые числа).

Для векторов из и номеров к, вводим отношение положив

Взяв произвольно какой-нибудь вектор из , имеем импликации

$$a_1x_1 : d_2 \to \frac{a_1}{d_1}x_1 : \frac{d_2}{d_1} \underset{\left(\frac{a_1}{d_1},\frac{d_2}{d_1}\right)=1}{\to} x_1 : \frac{d_2}{d_1} \to \exists t_1 \in Z : x_1 - \frac{d_2}{d_1}t_1 \to$$

$$a_2x_2 + \cdots + a_nx_n = d_2 \cdot \frac{a_1}{d_1}t_1 \underset{(lp_k)}{\to} a_2\left(x_2 - t_1\sigma_2^1\right) + \cdots + a_n\left(x_n - t_1\sigma_n^1\right) = 0 \to \left(x - t_1A^1\right)'' \geq ''2.$$

Принимая за x вектор $x - t_1A^1$ и повторяя для него только что проведенные рассуждения при помощи (lp_3), мы приходим к заключению $\left(x - t_1A^1 - x_2A^2\right)'' \geq ''3$ при некотором $t_2 \in Z$ и т.д. Продолжая описанный процесе отщепления и далее, на $(n-1)-м$ шаге будем иметь
$\left(x - t_1A^1 - x_2A^2 - \cdots - t_{n-1}A^{n-1}\right)'' \geq ''n.$

Поскольку для любого $y \in S(0)$ $y'' \geq ''n \to y = 0$ (ибо $Z -$ область целостности), мы имеем $x = t_1A^1 + \cdots + t_{n-1}A^{n-1}$,

где $t_1,\ldots,t_{n-1} \in Z.$ Из той же целостности Z легко следует и линейная независимость векторов $A^1 \cdots A^{n-1}$, т.е. $rangS(0) = n-1.$ Поэтому сюръекция
$Z^{n-1} \to S(a_0),\ \ \langle t_1,\ldots,t_{n-1}\rangle \to A^0 + t_1A^1 + \cdots + t_{n-1}A^{n-1}$ является также инъекцией, т.е. биективным соответствием (здесь $Z^{n-1} = Zx\cdots xZ - (n-1) - я$ прямая степень).Последнее показывает, что мощность множества решений уравнения (a_0) (при $d_1|a_0$) будет равна $|S(a_0)| = |Z^{n-1}| = |Z|^{n-1} = |N|^{n-1} = |N|$ (см. по этому поводу $[2]$, стр. 85).

Иногда, особенно в практических приложениях, решения из $S(a_0)$ удобно представлять в параметрическом виде

$$\begin{cases} x_1 = \sigma_1^0 - t_1\dfrac{d_2}{d_1}, \\ x_2 = \sigma_2^0 + t_1\sigma_2^1 - t_2\dfrac{d_3}{d_2}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_{n-1} = \sigma_{n-1}^0 + t_1\sigma_{n-1}^1 + t_2\sigma_{n-1}^2 + \cdots + t_{n-2}\sigma_{n-1}^{n-2} - t_{n-1}\dfrac{d_n}{d_{n-1}}, \\ x_n = \sigma_n^0 + t_1\sigma_n^1 + t_2\sigma_n^2 + \cdots + t_{n-2}\sigma_n^{n-2} + t_{n-1}\sigma_n^{n-1}, \end{cases} \qquad (p)$$

где $t_1,\ldots,t_{n-1}$ независимо друг от друга пробегают множество (напомним, что здесь).

2. Линейные представления длины два

Как мы видем в п решение уравнения сводилось к вычислению раз линейных представлений НОД двух чисел через сами эти числа. Нам известен невнятный и примитивный способ последовательных подстановок представлений остатков в в алгоритиме Евклида. Ниже мы укажем на одну практическую рекомендацию, которая гораздо быстрее приводит нас к цели, избегая неоправданно излишних вычислений. Ее суть состоит в следующем.

Пусть нам заданы два целых чисел и . Выпольним для них алгоритм Евклида

$$\begin{cases} a = вq_1 + r_1,\ 0 \prec r_1 \prec в, \\ в = r_1 q_2 + r_2,\ 0 \prec r_2 \prec r_1, \\ r_1 = r_2 q_3 + r_3,\ 0 \prec r_3 \prec r_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ r_{m-2} = r_{m-1} q_m + r_m,\ 0 \prec r_m \prec r_{m-1}, \\ r_{m-1} = r_m q_{m+1.}. \end{cases}$$

Последовательность $r_1, \ldots, r_m$ (равносильным образом!) можно задать и по формулам $r_k = x_k a + y_k в$, где коэффициенты определены рекуррентно как $x_k = x_{k-2} - q_k x_{k-1}$, $y_k = y_{k-2} - q_k y_{k-1}$, с начальными значениями $x_{-1} = y_0 = 1$ и $x_0 = y_{-1} = 0.$ Эти вычисления удобно выполнять по известной (и легко запоминающееся) схеме

Таблица 1

Схема Горнера

k	-1	0	1	2	$\cdots$	k	$\cdots$	m
$-q_k$			$-q_1$	$-q_2$	$\cdots$	$-q_k$	$\cdots$	$-q_m$
x_k	1	0	x_1	x_2	$\cdots$	x_k	$\cdots$	x_m
y_k	0	1	y_1	y_2	$\cdots$	y_k	$\cdots$	y_m

В этой таблице позиции $x_k (k \geq 1)$ заполняются индуктивно умножением позиций x_{k-1} и $-q_k$ и прибавлением к полученному позицию x_{k-2}. Взяв строчки $-q_k$ и y_k, вычисления y_k – ых производятся совершенно аналогично. В приведеной схеме последний столбец дает нам и требуемое представление $d = (a, в) = ax_m + вy_m$.

Пример. Применением описанного способа НОД чисел $a = -210147,\ в = 96089$ линейно представляется через них так. Выполнение алгоритма Евклида для этих чисел показывает, что здесь $m = 9, r_9 = 7$ и $q_1 = -3,\ q_2 = 1,\ q_3 = 4,\ q_1 = -3,\ q_4 = 2,\ q_5 = 1,\ q_6 = 7,\ q_7 = 5,\ q_8 = 2,\ q_9 = 4.$ тогда схема Горнера для a и $в$ даст нам следущие результаты.

Таблица 2

Табличный пример

k			1	2	3	4	5	6	7	8	9

Отсюда мы находим сразу

3. Неотрицательные решения уравнения

Многие вопросы теории и практики сводятся к выявлению неотрицательных решений (т.е. решений, которых все компоненты неотрицательны) уравнений вида . Неотрицательность

решения, представленного в виде (p), означает

$$\begin{cases} x_1 = \sigma_1^0 - t_1 \dfrac{d_2}{d_1} \geq 0, \\ x_2 = \sigma_2^0 + t_1\sigma_2^1 - t_2 \dfrac{d_3}{d_2} \geq 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_{n-1} = \sigma_{n-1}^0 + t_1\sigma_{n-1}^1 + t_2\sigma_{n-1}^2 + \cdots + t_{n-2}\sigma_{n-1}^{n-2} - t_{n-1}\dfrac{d_n}{d_{n-1}} \geq 0, \\ x_n = \sigma_n^0 + t_1\sigma_n^1 + t_2\sigma_n^2 + \cdots + t_{n-2}\sigma_n^{n-2} + t_{n-1}\sigma_n^{n-1} \geq 0, \\ t_1, \ldots, t_{n-1} \in Z. \end{cases} \qquad (\geq 0)$$

Находим ограничения сверху и снизу для параметров t_k в (≥ 0). Оценка сверху для t_k (из к-го неравенства) находится сразу $t_k \leq \dfrac{d_k}{d_{k+1}}\left(\sigma_k^0 + t_1\sigma_k^1 + \cdots + t_{k-1}\sigma_k^{k-1}\right)$. Чтобы получить оценку снизу, вводим для номеров $0 \leq r \prec k \prec n$ суммы $\sum{}_k^r = a_k\sigma_k^r + a_{k+1}\sigma_{k+1}^r + \cdots + a_n\sigma_n^r$. Перемножая неравенства из (≥ 0) с номерами $q, q \succ k,$ на a_q соответственно и складывая их почленно, получаем

$$t_k \geq -\frac{d_k}{a_k d_{k+1}}\left(\sum{}_{k+1}^0 + t_1\sum{}_{k+1}^1 + \cdots + t_{k-1}\sum{}_{k+1}^{k-1}\right).$$

Итак, мы пришли к следующей системе-следствию из (≥ 0):

$$\begin{cases} -\dfrac{d_1}{d_2 a_1}\sum{}_2^0 \leq t_1 \leq \dfrac{d_1}{d_2}\sigma_1^0, \\ -\dfrac{d_2}{d_3 a_2}\left(\sum{}_3^0 + t_1\sum{}_3^1\right) \leq t_2 \leq \dfrac{d_2}{d_3}\left(\sigma_2^0 + t_1\sigma_2^1\right), \\ -\dfrac{d_3}{d_4 a_3}\left(\sum{}_4^0 + t_1\sum{}_4^1 + t_2\sum{}_4^2\right) \leq t_3 \leq \dfrac{d_3}{d_4}\left(\sigma_3^0 + t_1\sigma_3^1 + t_2\sigma_3^2\right), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ -\dfrac{d_{n-1}}{d_n a_{n-1}}\left(\sum{}_n^0 + t_1\sum{}_n^1 + \cdots + t_{n-2}\sum{}_n^{n-2}\right) \leq t_{n-1} \leq \dfrac{d_{n-1}}{d_n}\left(\sigma_{n-1}^0 + t_1\sigma_{n-1}^1 + \cdots + t_{n-2}\sigma_{n-1}^{n-2}\right), \\ t_1, \ldots, t_{n-1} \in Z. \end{cases} \qquad (\leq t_k \leq)$$

Оказывается, и $(\leq t_k \leq)$ влечет за собой (≥ 0). То, что правая часть к-го $(1 \leq k \leq n)$ неравенства из повлечет за собой к-ое неравенство , очевидно. Далее поскольку имеем

Поэтому левая часть последнего неравенства из с учетом и дает нам

т.е. и последнее неравенство из является следствием из .

Пусть $S(\le t_k \le)$ и $S_{\ge}(0)$ обозначает множества решений системы $(\le t_k \le)$ и неотрицательных решений уравнения (a_0) соответственно. Установленная эквивалентность $(\le t_k \le) \leftrightarrow (\ge 0)$ показывает, что отображение $S(\le t_k \le) \to S_{\ge}(0),$ ставящее каждому кортежу $\langle t_1,\ldots,t_{n-1}\rangle$ в соответствие вектор $\langle x_1,\ldots,x_n\rangle,$ определенный по правилу (p), является биекцией. Поскольку здесь множество $S(\le t_k \le)$ конечно, число неотрицательных решений из (a_0) также будет конечным (и оно будет равно $|S_{\ge}(0)| = |S(\le t_k \le)|$). Очевидно, система двойных неравенств $(\le t_k \le)$ представляет собой индуктивно-разветвляющуюся форму решения системы неравенств (≥ 0).

4. Приложение теории

Продемонстрируем применение теории к одной конкретной практической задаче. Пусть требуется проложить прямую канализационную трассу длиной 81м.керамическими трубами длин 5, 6 и 8м. В каких целочисленных вариантах (т.е. не разрезая труб) можно выполнить эту работу?

Если обозначить через x_1, x_2 и x_3 количества нужных труб длин 5,6 и 8м. соответственно, то это задача примет следующую модельную форму

$$\begin{cases} 5x_1 + 6x_2 + 8x_3 = 81, \\ 0 \le x_i \in Z, \quad i = 1,2,3. \ (m) \end{cases}$$

Чтобы ответить на вопрос задачи, нам нужно решить систему (m). В уравнении системы $a_0 = 81, \quad a_1 = 5, \quad a_2 = 6, \quad a_3 = 8, \quad (n = 3)$ и $d_3 = 8\,(= a_3),\ d_2 = (6,8) = 2,$ $d_1 = (5,2) = 1$ (из последнего видно существование решений уравнения). Здесь в качестве отправной точки мы возьмем следующие (простые) двумерные линейные представления:

$d_3 = 1 \cdot a_3 \quad (x_3 = 1);$

$d_2 = 2 = 6(-1) + 8 \cdot 1 \quad (x_2 = -1,\ y_2 = 1);$

$d_1 = 1 = 5 \cdot 1 + 2(-2) \quad (x_1 = 1,\ y_1 = -2);$

$d_0 = 1 \cdot d_1.$

Прямые вычисления показывают, что для них

$$\sigma_1^{\,0} = \frac{a_0}{d_0}\left(\prod_{0<i<1} y_i\right)x_1 = \frac{81}{1} \cdot 1 \cdot 1 = 81;$$

$$\sigma_2^{\,0} = \frac{a_0}{d_0}\left(\prod_{0<i<2} y_i\right)x_2 = 81 y_1 x_2 = 2 \cdot 81;$$

Составим теперь систему неравенств (≥ 0):

$$\begin{cases} x_1 = \sigma_1^0 - t_1 \dfrac{d_2}{d_1} = \quad 81 - 2t_1 \geq 0, \\ x_2 = \sigma_2^0 + t_1\sigma_2^1 - t_2 \dfrac{d_3}{d_2} = 2 \cdot 81 - 5t_1 - 4t_2 \geq 0, \\ x_3 = \sigma_3^0 + t_1\sigma_3^1 + t_2\sigma_3^2 = -2 \cdot 81 + 5t_1 + 3t_2 \geq 0, \\ t_1, t_2 \in Z. \end{cases}$$

Поскольку здесь $\sum_2^0 = a_2\sigma_2^0 + a_3\sigma_3^0 = -4 \cdot 81$ и $\sum_3^0 + t_1 \sum_3^1 = a_3\sigma_3^0 + t_1 a_3\sigma_3^1 = 8\,(-2 \cdot 81 + 5t_1)$, формулы из $(\leq t_k \leq)$ дают нам следующие (индуктивно-разветвляющиеся) решения последней системы

$$\begin{cases} \dfrac{2}{5} \cdot 81 \leq t_1 \leq \dfrac{1}{2} \cdot 81, \\ \dfrac{1}{3}(2 \cdot 81 - 5t_1) \leq t_2 \leq \dfrac{1}{4} = (2 \cdot 81 - 5t_1), \\ t_1, t_2 \in Z. \end{cases}$$

$(\leq t_1, t_2 \leq)$

Первое неравенство из $(\leq t_1, t_2 \leq)$ дает нам, что $t_1 = 33, 34, 35, 36, 37, 38, 39, 40.$

Второе же неравенство решается относительно каждого из этих значений t_1. Например, положив $t_1 = 33,$ мы имеем $-1 \leq t_2 \leq -\dfrac{3}{4} \to t_2 = -1.$ Аналогичные вычисления производив и для остальных значений t_1, мы приходим к следующей таблице всех возможных решений системы (m)

Таблица 3

Решения модельной системы

t_1	33	34	35	36		37		38			39			40		
t_2	-1	-2	-4	-6	-5	-7	-6	-9	-8	-7	-11	-10	-9	-12	-11	-10
x_1	15	13	11	9	9	7	7	5	5	5	3	3	3	1	1	1
x_2	1	0	3	6	2	5	1	8	4	0	11	7	3	10	6	2
x_3	0	2	1	0	3	2	5	1	4	7	0	3	6	2	5	8

Как показывает эта таблица, без труб длины 5м. выполнить работу никак невозможно. Но не взяв труб длины 6м. это возможно сделать, что видно из 3-ей и 9-ой колонок. Варианты без труб длины 8м. также возможны (см. 2-ую, 5-ую и 12-ую колонки).

Литература:

1. **Ляпин, Е.С.** Алгебра и теория чисел: 1.числа. [Текст] / А.Е. Евсеев /М., «Просвещение», 1974, 383с.
2. **Мальцев, А.И.** Алгебраические системы. М., «Наука», 1970, 392с.