УДК 512
DOI: https://doi.org/10.52754/16948645_2024_1(4)_36

О СТРУКТУРЕ РЕШЕНИЙ ЛИНЕЙНОГО ДИОФАНТОВА УРАВНЕНИЯ

Сатаров Жоомарт, д. ф.-м.н., профессор
Зулпукаров Жакшылык Алибаевич, к.ф.-м. н.
zulpukarov66@mail.ru
Ошский технологический университет им. М. М. Адышева
Кошокова Бактыгул Карыевна, магистрант
Ошский государственный педагогический университет
Ош, Кыргызстан

Аннотация. *Теория решения подобных уравнений является классическим разделом математике. В ней не приходится писать сложные и громоздкие формулы, а необходимо проводить аккуратные рассуждения, базирующиеся на определенных понятиях теории чисел связанные в стройную логическую конструкцию. В рамках этой теории можно дать исчерпывающее решение рассматриваемого класса задач с четко описанным алгоритмом получения ответа. Именно этими чертами характеризуется хорошая математическая теория.*

В заметке находятся решения линейного диофантова уравнения с n неизвестными. Строятся они конструктивно. Выявляется также структурное строение этих решений.

Ключевые слова: *диофантово уравнение, наибольший общий делитель, линейные представления, множества решений, абелевой группа.*

СЫЗЫКТУУ ДИОФАНТТЫК ТЕҢДЕМЕНИН ЧЕЧИМДЕРИНИН СТРУКТУРАСЫ ЖӨНҮНДӨ

Сатаров Жоомарт, ф.-м.и.д., профессор
Зулпукаров Жакшылык Алибаевич, ф.-м. и.к.
zulpukarov66@mail.ru
М. М. Адышев атындагы Ошский технологиялык университети
Кошокова Бактыгул Карыевна, магистрант
Ош мамлекеттик педагогикалык университети
Ош, Кыргызстан

Аннотация. *Мындай теңдемелерди чечүү теориясы математиканын классикалык тармагы болуп саналат. Ал татаал жана түйшүктүү формулаларды жазууга милдеттүү эмес, бирок ыраатту логикалык конструкцияга байланышкан сандар теориясынын айрым түшүнүктөрүнүн негизинде так ой жүгүртүүнү жүргүзүү зарыл. Бул теориянын чегинде жооп алуу үчүн так сүрөттөлгөн алгоритм менен каралып жаткан маселелердин классына толук чечимди берүүгө болот. Булар жакшы математикалык теориянын өзгөчөлүктөрү.*

Эскертмеде n белгисиз сызыктуу диофанттык теңдеменин чечимдери камтылган. Алар конструктивдүү түрдө курулган. Бул чечимдердин структуралык структурасы да ачылган.

Ачкыч сөздөр: *Диофанттык теңдеме, эң чоң жалпы бөлүүчү, сызыктуу көрүнүштөр, чечимдердин көптүгү, абелиялык топ.*

ON THE STRUCTURE OF SOLUTIONS NO A LINEAR DIOPHANTINE EQUATION

Satarov Zhoomart Doctor of Ph. & Math. Sc., professor
Zulpukarov Zhakshylyk Alibaevich Candidat of Ph. & Math. Sc.
zulpukarov66@mail.ru
Osh Technological University named after M. M. Adysheva

Koshokova Baktygul Karyevna, graduate student
Osh State Pedagogical University
Osh, Kyrgyzstan

Abstract: *The theory of solving such equations is a classical branch of mathematics. It does not have to write complex and cumbersome formulas, but it is necessary to carry out accurate reasoning based on certain concepts of number theory, connected into a coherent logical construction. Within the framework of this theory, it is possible to give an exhaustive solution to the considered class of problems with a clearly described algorithm for obtaining an answer. These are the characteristics of a good mathematical theory.*

The note contains solutions to a linear Diophantine equation in n unknowns. They are built constructively. The structural structure of these solutions is also revealed.

Key words: *Diophantine equation, greatest common divisor, linear combinations, sets, abelian group.*

Рассматривается диофантово уравнение

$$a_1x_1 + a_2x_2 + a_3x_3 + ... + a_nx_n = a_0, \quad n \geq 2 , \qquad (ld)$$

где $a_i \in Z,\ a_1a_2...a_n \neq 0$ (и неизвестные x_i также ищутся в области Z). Нашей целью в этой заметке является нахождение всех решений уравнения (*ld*). Здесь выявляется также структура найденных решений.

Обозначим через $d = (a_1, a_2, ..., a_n)$ наибольший общий делитель (НОД) коэффициентов $a_1, a_2, ..., a_n$ из (*ld*). Очевидно при $a_0 \vdots d$ заданное уравнение никакого решения не имеет. Поэтому всюду далее мы будем считать, что в (*ld*) $a_0 \vdots d$. Положив $d_n = a_n$, индуктивно вводим к рассмотрению следующие НОД

$$d_k = (a_k, d_{k+1}), \qquad k = n-1, ..., 1 .$$

С целью сохранения общности в рассуждениях, вводим еще одно число $d_0 = d_1$.

Здесь очевидны делимости $d \vdots d_1$ и $d_k \vdots d_{k-1}$ при всех рассмотренных выше значениях k .

Наш подход в заметке основывается на какую-нибудь (не важно какую!) систему линейных представлений НОД $d_k,\ k = n, ..., 1$:

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

(здесь $x_k, y_k \in Z$ при всех $k = n-1, ..., 1$ и $x_n = 1$).

Пусть $k, q -$ произвольные номера, для которых $0 \leq k < q \leq n$. Из коэффициентов уравнения (*ld*) и разложений (*lp*) составим величины

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

где для общности рассуждений при соседних $k = q-1$ и q считается $\prod_{k<i<q} y_i = 1$.

Умножив равенства (lp) с номерами $t,\ t \ge k,$ на $\frac{a_{k-1}}{d_{k-1}} \prod_{k \le i < t} y_i$ соответственно и почленно складывая их, мы приходим к

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

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

При $k = 1$ равенство (lp_k) дает нам

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

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

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

(длины n, где случай отсутствия нулей также включается) являются решениями однородного (для (ld)) уравнения

$$a_1 x_1 + a_n x_2 + ... + a_n x_n = 0 . \qquad (ld_0)$$

Если обозначить через $S(ld)$ и $S(ld_0)$ множества решений уравнений (ld) и (ld_0) соответственно, то они будут связаны соотношением

$$S(ld) = A^0 + S(ld_0) .$$

Это означает, что решения из $S(ld)$ полностью определяются вторым слагаемым. Слагаемое $S(ld_0)$, очевидно, образует абелеву группу (в частности, оно выдерживает умножения на целые числа).

Далее, для векторов $x = \langle x_1, x_2, ..., x_n \rangle$ из $S(ld_0)$ и номеров $k,\ 2 \le k \le n$, вводим (бинарное) отношение "$\ge$", положив

$$x \ \text{"}\ge\text{"}\ k \leftrightarrow x_1 = ... = x_{k-1} = 0 .$$

Теперь взяв произвольно вектор $x = \langle x_1, x_2, ..., x_n \rangle$ из $S(ld_0)$, имеем импликации

$$a_1 x_1 \vdots d_2 \to \frac{a_1}{d_1} x_1 \vdots \frac{d_2}{d_1} \xrightarrow[\left(\frac{a_1}{d_1}, \frac{d_2}{d_1}\right)=1]{} x_1 \vdots \frac{d_2}{d_1} \to \exists t_1 \in Z : x_1 = -\frac{d_2}{d_1} t_1 \to$$

$$a_2 x_2 + ... + a_n x_n = d_2 \cdot \frac{a_1}{d_2} t_1 \xrightarrow[(lp_2)]{} a_2 (x_2 - t_1 \sigma_2^1) + ... + a_n (x_n - t_1 \sigma_n^1) = 0$$

$$\to (x - t_1 A^1) \text{"}\ge\text{"} 2.$$

Принимая за x вектор $x - t_1 A^1$ и повторяя для него только что проведенные рассуждения при помощи (lp_3), мы приходим к заключению $(x - t_1 A^1 - t_2 A^2) \text{"}\ge\text{"} 3$ при

некотором $t_2 \in Z$ и т.д. Продолжая описанный процесс отщепления и далее, на $(n-1)$-м шаге будем иметь

$$(x - t_1 A^1 - t_2 A^2 - \ldots - t_{n-1} A^{n-1})''\geq''n.$$

Поскольку для любого $y \in S(ld_0)$ $y''\geq''n \to y = 0$ (ибо Z – область целостности), мы для рассматриваемого вектора имеем представление

$$x = t_1 A^1 + \ldots + t_{n-1} A^{n-1}, \qquad (lk)$$

где $t_1,\ldots,t_{n-1} \in Z$. Целостность кольца Z влечет за собой также инъективность сюръекции

$$Z^{n-1} \to S(ld),\ \langle t_1,\ldots,t_{n-1}\rangle \to A^0 + t_1 A^1 + \ldots + t_{n-1} A^{n-1} \qquad (bi)$$

(здесь $Z^{n-1} = Z \times \ldots \times Z$ – $(n-1)$-я прямая степень кольца Z), т.е. биективность указанного соответствия. Итак, установлено, что решения $S(ld_0)$ представляются, причем единственном образом, в виде линейной комбинации (*lk*). Это означает, что $S(ld_0)$ не только является абелевой группой, но и как Z -модуль имеет ранг $n-1$.

Иногда, особенно при практических приложениях, решения из $S(ld_0)$ удобно представлять в параметрическом виде

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

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

Далее, как показывает биективность отображения (*bi*), для мощности всех решений уравнения (*ld*) имеет место (цепочка)

$$|S(ld)| = |S(ld_0)| = |Z^{n-1}| = |Z|^{n-1} = |N|^{n-1} = |N|$$

(см. по этому поводу [1], стр.85), т.е. она будет равна алеф-нулю. Как показывают проделанные выкладки, наша заметка в некотором перекрытии содержит в себе результат из [2] (см. стр.121), где была показана лишь бесконечность множества решений $S(ld)$.

Литература

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