Bulletin KRASEC. Phys. & Math. Sci. 2016. V. 13. no. 2. pp. 16-21. ISSN 2313-0156

DOI: 10.18454/2313-0156-2016-13-2-16-21

MSC 34L99

LINEAR DIOPHANTINE EQUATIONS AND WAYS TO SOLVE THEM

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 the ways to solve linear Diophantine equations both in a special case with two unknown quantities, and in a general case with few unknowns. The main result is contained in Theorem 1, which assumes the general method to solve any Diophantine equation based on the congruence modulo.

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

Introduction

A Diophantine or an indefinite equation is the equation which should be in integral numbers [1]. In other words, the equations of the form

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

where $P(x_1, x_2, \dots, x_n)$ is a polynomial with integral coefficients, which are to be solved in integral numbers, are called a Diophantine equations by the name of a Greek mathematician, Diophantus (III A.D.), who studied such equations of the simplest forms. Before Diophantus, other mathematicians studied such equations, for example, Pythagoras considered the equation $x^2 + y^2 = z^2$, which was called by his name. The geometric sense of this equation is that a right triangle, the lateral lengths of which are integral numbers, gives the solution.

Defination. A linear Diophantine equation with n unknown quantities is the equation of the form

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

where the coefficients $a_1, a_2, \dots, a_n, b$ are integers and the unknown quantities may take only integral values.

Kodzokov Azamat Khasanovich – Senior Lecturer, Dep. of Mathematical Analysis and Function Theory, Kabardino-Balkarian state university of H.M. Berbekov, Nalchik, Republic of KabardinoBalkaria,Russia.

Beslaneev Zalimbek Olegovich – High teacher of IMOAS chair, Kabardino-Balkarian state university of H.M. Berbekov, Nalchik, Republic of Kabardino-Balkaria, Russia.

Nagorov Aslan L'vovich – High teacher of IMOAS chair, Kabardino-Balkarian state university of H.M. Berbekov, Nalchik, Republic of Kabardino-Balkaria, Russia.

Tkhamokov Muslim Bashirovich – Senior Lecturer, Department of Computational Mathematics, Kabardino-Balkarian state university of H.M. Berbekov, Nalchik, Republic of KabardinoBalkaria, Russia.

Linear Diophantine equations with two unknown quantities

First, we consider linear Diophantine equations with two unknown quantities

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

where a,b,c are integers and the unknown x,y take integral values [2].

We consider the properties of linear Diophantine equations with two unknown quantities [3], [4].

Proposition 1. If the right part of equation (2) cannot be divided by the greatest common factor $d=(a,b)$ of the coefficients for the unknown quantities, then this equation does not have any solution in integral numbers.

Proposition 2. Assume that $d=(a,b)$, $d|c$ and (x_0,y_0) some solution of equation (2) in integral numbers coincides with a pair set $\left(x^{'},y^{'}\right)$, where $x^{'}=x_0+\frac{b}{d}t$; $y^{'}=y_0+\frac{a}{d}t$, where t is any integral number.

Proof. Assume that $\left(x^{'},y^{'}\right)$ is an arbitrary solution of equation (2), that is

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

As long as (x_0,y_0) is the solution of equation (2) by condition, then

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

Subtracting term by term of equality (4) from (3), we obtain

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

Dividing the both parts of this equation by d, we have

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

where the coefficients $\frac{a}{d}$ and $\frac{b}{d}$ are integral mutually prime numbers. From the latest equality follows the divisibility

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

However, as long as $GCD\left(\frac{a}{d},\frac{b}{d}\right)=1$, then $\frac{b}{d}\bigg|\left(x^{'}-x_0\right)$. Thus, $\left(x^{'}-x_0\right)=\frac{b}{d}t$ for some integer t, that is $x^{'}=x_0+\frac{b}{d}t$, where t is any number.

Then, substituting the determined value x into (3), we obtain

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

whence, after the reducing by a number b, we have

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

Thus, any solution of equation (2) in integral numbers has the form

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

where t is any integral number. The proposition 2 has been proved. □

Now we turn to the methods of solution of Diophantine equations with two unknown numbers. We have already obtained the formulas to find the unknown values in a linear Diophantine equation (2), when one solution (x_0, y_0) of this equation is known.

We intend to consider the methods of finding of a particular solution of equation (2).

L. Euler was the first one who began to develop the methods to solve Diophantine equations. Two methods of solution in integral numbers of equation (2) with integral coefficients are described in «Universal Arithmetic» by Euler.

The first way is when an unknown x in equation (2) is expressed through y, that is $x = \frac{c-by}{a}$, and only $y > 0$, $x > 0$ are taken. We also try only positive values of y so that $c - by > 0$, that means that the inequality $0 < y < \frac{c}{b}$ is fulfilled. This method holds only when $c > d$. If the relation $\frac{c}{b}$ is large enough, the method requires a large number of tests.

Euler shows the second way (division by the least coefficient) on an example and it is based on the Euclidean algorithm. Then we seek for a particular solution of equation (2) in the following form: $x_0 = \frac{c}{d}X_0$, $y_0 = \frac{c}{d}Y_0$, where $d = GCD(a,b)$. Thus, equation (2) is changed as

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

The obtained relation (5) is the linear representation of the greatest common divisor of the numbers a and b. Thus, the known X_0 and Y_0 can be found by the Euclidean algorithm applied to the numbers a and b. That means that we find the values for x_0 and y_0.

We consider the method of Euclidean algorithm to solve the Diophantine equation with two unknown quantities on an example.

FOREXAMPLE. Solve the equation

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

in integral numbers by the Euclidean algorithm. Here $GCD(50,42) = 2$, and $2|34$ and that means that the equation has a solution in integral numbers. First, we find a particular solution of the equation of the form $50x - 42y = 2$.

Assume that (X_0, Y_0) is a particular solution of this equation, that is

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

In order to do that, we apply the Euclidean algorithm to the numbers 50 and 42. We have the following continued equality yielding the division with remainder:

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

From the next-to-last equality we have $2 = 42 - 8 \cdot 5$. From the first equality we find $8 = 50 - 42$. Then for $GCD(50,42)$ we obtain:

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

It is the linear presentation of $GCD(50,42)$. Thus, $X_0 = -5$; $Y_0 = -6$. Now we obtain the following particular solution:

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

Then the initial equation general solution has the form

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

where t possesses any integral value.

By the corresponding transformations, this general solution may be reduced to the form

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

where u possesses any integral value.

In comparison to the Euclidean algorithm, a more convenient method to solve a linear Diophantine equation (2) is the one based on the change of this equation by congruence modulo.

PROPOSITION 3. If x_0 satisfies the congruence $ax \equiv c \pmod{b}$, the number ordered pair $\left(x_0, \dfrac{c - ax_0}{b}\right)$ is the solution of the linear Diophantine equation (2).

Proof. It follows from $ax_0 \equiv c \pmod{b}$ that $b | c - ax_0$, that is $\dfrac{c - ax_0}{b}$ is an integral number. We check that $\left(x_0, \dfrac{c - ax_0}{b}\right)$ is the solution of equation (2).

In fact, we have $ax_0 + b \cdot \dfrac{c - ax_0}{b} = ax_0 + c - ax_0 = c$. This means that the pair $\left(x_0, \dfrac{c - ax_0}{b}\right)$ is the solution of equation (2). The proposition 3 has been proved. □

We shall show this method on the same equation solved by Euclidean algorithm.

FOREXAMPLE. Solve the Diophantine equation $50x - 42y = 34$ by the congruence method.

Solution. We change this equation by a congruence $50x \equiv 34 \pmod{42}$. Reducing the both parts and the congruence modulo by 2, we obtain $25x \equiv 17 \pmod{21}$ or that is the same $4x \equiv 17 \pmod{21}$, that is $4x \equiv -4 \pmod{21}$. Reducing the both parts of this congruence by 4, we obtain $x \equiv -1 \pmod{21}$, that is $x \equiv 20 \pmod{21}$. Thus, owing to the proposition 3, $x_0 = 20$, $y_0 = \dfrac{c - ax_0}{b} = \dfrac{34 - 50 \cdot 20}{-42} = 23$ yield a particular solution of this equation. Then owing to 2, any solution of this Diophantine equation takes the form $x = 20 + 21t$, $y = 23 + 25t$, where t possesses any integral value.

Linear Diophantine equations with n unknown quantities

Now we turn to the generalization of the method to solve any linear Diophantine equation (1). We introduce the notations:

$$\Delta_1 = GCD\left(a_1, \; a_2, \ldots, a_n\right), \Delta_2 = GCD\left(a_2, \; a_3, \ldots, a_n\right),$$

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

Equation (1) is solvable in integral numbers if $\Delta_1 | b$. If $\Delta_1 \nmid b$, equation (1) is unsolvable in integral numbers. Assume that $\Delta_1 | b$, that means that equation (1) has solutions in integral numbers. We rewrite equation (1) as follows:

$$a_2 x_2 + \cdots + a_n x_n = b - a_1 x_1.$$

Then there is $x_1 = x_1^{(0)} \in Z$, when the divisibility $\Delta_2 | b - a_1 x_1^{(0)}$ is realized, that is

$$a_1 x_1^{(0)} \equiv b \left(\mathrm{mod}\ \Delta_2\right).$$

Then as the unknown x_1 value we may take any number from the residue class $x_1 \equiv x_1^{(0)} \left(\mathrm{mod}\ \Delta_2\right)$. Denote

$$b_2 = b - a_1 x_1^{(0)}$$

and consider the equation

$$a_2 x_2 + \cdots + a_n x_n = b_2.$$

We rewrite this equation again in the following form:

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

Owing to the previous arguments, we have that there is such an integral value $x_1 = x_1^{(0)} \in Z$, that the divisibility $\Delta_3 | b_2 - a_2x_2^{(0)}$ is realized, that is

$$a_2x_2^{(0)} \equiv b_2 \, (\mathrm{mod} \; \Delta_3) \, .$$

Then as an unknown x_2 value, we may take any number from the residue class $x_2 \equiv x_2^{(0)} \, (\mathrm{mod} \; \Delta_3)$. If we continue this process, we obtain the following congruence at the next-to-last step:

$$a_{n-1}x_{n-1}^{(0)} \equiv b_{n-1} \, (\mathrm{mod} \; \Delta_n) \, .$$

Then as an unknown x_{n-1} value we may take any number from the residue class $x_{n-1} \equiv x_{n-1}^{(0)} \, (\mathrm{mod} \; \Delta_n)$.

At the last step, we obtain the equation

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

whence,

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

or, if we denote $b_n = b_{n-1} - a_{n-1}x_{n-1}^{(0)}$, then $x_n = \frac{b_n}{\Delta_n}$.

Similar to the case of the proposal 3, we can show (but we don not stop at that) that the obtained set of numbers $\left(x_1^{(0)},\, x_2^{(0)}, \ldots, x_n^{(0)}\right)$ really yields the solution of equation (1) in the described process.

Thus, we obtained the following

Theorem. *Any solution of a linear Diophantine equation $a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$, for GCD $(a_1, a_2, \ldots, a_n) | b$ has the form $\left(x_1^{(0)},\, x_2^{(0)}, \ldots, x_n^{(0)}\right)$, where $a_kx_k^{(0)} \equiv b_k \, (\mathrm{mod} \; \Delta_{k+1})$ for $1 \le k \le n-1$; $x_n^{(0)} = \frac{b_n}{\Delta_n}$; b_k are determined by recurrent relations $b_k = b_{k-1} - a_{k-1}x_{k-1}^{(0)}$; $2 \le k \le n$.*

FOREXAMPLE. Find any solution of the equation

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

in integral numbers.

Solution. We consider the congruence $12x_1 \equiv 18 \, (\mathrm{mod} \; 1)$. Here $\Delta_2 = (10, 6, 5) = 1$. For example, we take $x_1^{(0)} = 1$.

Then we consider a new equation $10x_2 + 6x_3 + 15x_4 = 6$. Here $b_2 = 6$. We obtain the congruence $10x_2 \equiv 6 \, (\mathrm{mod} \; 3)$, here $\Delta_3 = (6, 15) = 3$.

For example, we take $x_2^{(0)} = 3$. Then we set up one more new equation $6x_3 + 15x_4 = -24$, here $b_3 = -24$. We consider the congruence $6x_3 \equiv -24 \, (\mathrm{mod} \; 15)$ again; here $\Delta_4 = 15$.

We take $x_3^{(0)} = 1$. Then at the last step we obtain $15x_4 = -30$, whence $x_4^{(0)} = -2$.

Thus, $(1; 3; 1; \; -2)$ is one of the solutions of this equation.

References

1. Bashmakova I. G. Diofant i diofantovy uravneniya [Diophant and Diophantine equations]. Moscow. Nauka. 1972. 68 p.

2. Solov'ev Yu. N. Neopredelennye uravneniya pervoy stepeni [Undetermined equations of the first degree]. Kvant – Quantum. 1992. no. 4. 42–46.

3. Bukhshtab A. A. Teoriya chisel [Theory of numbers]. Moscow. Prosveshchenie. 1966. 385 p.

4. Serpinskiy V. O reshenii uravneniy v tselykh chislakh [On the solution of equations in integral numbers]. Moscow. Fizmatlit. 1961. 88 p.

For citation: Kodzokov A. Kh., Beslaneev Z. O., Nagorov A. L., Tkhamokov M. B. Linear Diophantine equations and ways to solve them. *Bulletin KRASEC. Physical and Mathematical Sciences* 2016, vol. **13**, no **2**, 16-21. DOI: 10.18454/2313-0156-2016-13-2-16-21

Original article submitted: 29.03.2016