DOI: 10.31319/2519-8106.2(51)2024.317496
UDC 004.023:519.6

Oliinyk Leonid, Candidate of Physical and Mathematical Sciences (Ph. D.), Associate Professor
Олійник Л.О., кандидат фізико-математичних наук, доцент
ORCID: 0000-0002-4392-0048
e-mail: l.olejnik57@gmail.com

Dniprovsky State Technical University, Kamianske
Дніпровський державний технічний університет, м. Кам'янське

APPLICATION OF THE OPERATOR GENETIC ALGORITHM FOR SOLUTION OF DIOPHANTINE EQUATIONS

ЗАСТОСУВАННЯ ОПЕРАТОРНОГО ГЕНЕТИЧНОГО АЛГОРИТМУ ДО РОЗВ'ЯЗАННЯ ДІОФАНТОВИХ РІВНЯНЬ

*The paper presents the results of the study of the effectiveness of the **operator genetic algorithm** when applied to the solution of Diophantine equations.*

As is known, the solution of Diophantine equations is performed in the ring of integers. In this paper, the operator genetic algorithm, which operates in the field of real numbers, is adapted in a certain way for finding integer solutions. The research topic of this paper is of interest considering that Diophantine equations play a major role in mathematical methods of cryptology. On the other hand, the history of these equations is so rich and majestic that getting even a small result in this field is important for every mathematician. Great mathematicians of different eras were engaged in the study of Diophantine equations, and even today these studies have not lost their significance.

***Keywords**: involutive operator, stochastic operator, fitness function, n-dimensional hypercube, binary code, Gray code, Diophantine equation.*

*У роботі приведено результати дослідження дієвості **операторного генетичного алгоритму** при застосуванні до розв'язання діофантових рівнянь.*

Як відомо розв'язання діофантових рівнянь виконується у кільці цілих чисел. У роботі операторний генетичний алгоритм, який діє в полі дійсних чисел, певним чином пристосовано для пошуку цілих розв'язків. Тема досліджень даної роботи представляє інтерес з огляду на те, що діофантові рівняння відіграють велику роль у математичних методах криптології. З іншого боку, історія цих рівнянь настільки багата і велична, що отримання, хоч незначного, результату в цій галузі є важливим для кожного математика. Дослідженнями діофантових рівнянь, займались великі математики різних епох і сьогодні ці дослідження не втратили своєї значущості.

***Ключові слова**: інволютивний оператор, стохастичний оператор, фітнес-функція, n-вимірний гіперкуб, бінарний код, код Грея, діофантове рівняння.*

Problem's Formulation

Diophantine equations, despite the thousand-year history of their study, remain the subject of scientific research of theoretical mathematics, particular number theory. Today, with the development of computing technology, the results of these studies have found application in applied fields, in particular in the mathematical foundations of cryptography and in computer science itself. Modern computing has given impuls to the search and development of new algorithmic approaches to solving Diophantine equations. The relevance of the search of such algorithms, including iterative ones, is confirmed by a significant number of scientific works of the modern mathematical community. This work is devoted to the problem of developing an algorithm for solving Diophantine equations.

Analysis of recent research and publications

There are many topics devoted to the study of Diophantine equations. Among which the following are closest to the algorithm given in this work: in the paper ([5]), among the given examples of the application of the genetic algorithm to optimization problems, there are examples of solving Diophantine equations with a large number of unknowns; the papers ([6],[7]) give the results of applying Diophantine equations to encryption methods; the paper ([8]) investigates the algorithm of using a neural network to determine integer solutions; the paper ([9]) examines a type of Diophantine equation important for cryptography $3^x + 7^y = z^2$. These publications testify to the scientific relevance of research of Diophantine equations and their applications in cryptography. Providing a complete list of scientific works in this direction over the past 5—8 years is not possible within the scope of this article.

Formulation of the study purpose

Statement of the problem: to develop a version of the operator genetic algorithm for solving Diophantine equations, to investigate the effectiveness of the operator genetic algorithm when applying it to the solution of known Diophantine equations.

Presenting main material

The paper presents a version of the operator genetic algorithm (OGA), the description of which is given in the author's works ([1—4]), adapted to the solution of Diophantine equations, and examples of linear and nonlinear equations of different types with different number of unknowns are considered.

To solve Diophantine equations, which are considered on the set of integers, this work uses modified in a certain way operator genetic algorithm that operates in the field of real numbers. The research topic of this work is of interest considering that Diophantine equations play a major role in the mathematical methods of the theory of cryptography. On the other hand, the thousand-year history of the study of Diophantine equations testifies to their significance in mathematics. Great mathematicians of different eras were engaged in the study of Diophantine equations, and today these studies have not lost their importance. In 1900, at the World Mathematical Congress in Paris, David Hilbert formulated the important mathematical problems of the next century in his report. Among them, there is 10th problem formulated as follow: "Let a Diophantine equation with arbitrary unknowns and integer rational numerical coefficients be given. Specify the method by which it is possible, after a finite number of operations, to determine whether this equation is solvable in integer rational numbers." In 1970, Yuriy Matiyasevich solved this Hilbert problem, proving the algorithmic intractability of the problem of building a universal algorithm for finding solutions to Diophantine equations. This fact is the basis for the use of the so-called "Diophantine difficulties" in modern cryptography.

In this work, a version of OGA is presented, which allows finding solutions of Diophantine equations. The OGA determines an integer solution of the equation, if at some iterative step the best point falls into the unitary neighborhood of the solution. In this case, some of the vertices of the neighborhood (n-dimensional hypercube) with integer coordinates will deliver the solution of the equation. Therefore, at each step of the algorithm, the vertices of the unitary integer neighborhood obtained by approximation are determined.

This work presents a version of OGA for finding solutions of Diophantine equations of two or more variables, both linear and nonlinear. The effectiveness of the algorithm is analyzed on specific examples.

The operator genetic algorithm for finding integer extremal points.

Let's consider the Diophantine equation $P(x_1, x_2, \dots x_n) = 0$, where P — a polynomial of n variables with integer coefficients. The solution of this equation can be reduced to the problem of finding an integer solution, which delivers the minimum value(s) of the function $F(x) = |P(x_1, x_2, \dots x_n)|$ defined in a closed region $\Omega \in R^n$, which is defined as follows:

$$\Omega = \{(\xi_1, \dots, \xi_n) : a_m \le \xi_m \le b_m,\ m = \overline{1,n}\}.$$

Region Ω is some n-dimensional hypercube in space R^n with a "cubic" norm $\|x\| = \max_j\{|\xi|\}$. Binary Gray codes are unambiguously assigned to the vertices of this hypercube $\Omega \in R^n$, in such a way, that the vertex with the minimum coordinate values $A = (a_1, \dots, a_n)$ has a zero code, and the vertex with the maximum coordinate values $B = (b_1, \dots, b_n)$ has a unitary code. Hypercube

$\Omega \in R^n$ has 2^n vertices consisting of 2^{n-1} pairs of "opposite" vertices that are at the maximum Hamming distance.

To determine the coordinates of all vertices of a hypercube, it is enough to have the coordinates of two vertices $A = (a_1, \dots, a_n)$ and $B = (b_1, \dots, b_n)$.

For the operator matrix $\hat{P}_j^k = \begin{pmatrix} P_j^k & I - P_j^k \\ I - P_j^k & P_j^k \end{pmatrix}$, where $P_j^k x = P_j^k(\sum_{i=1}^n \xi_i e_i) = \sum_{i=j}^k \xi_i e_i$, where $\forall x = (\xi_1, \dots, \xi_n) \in R^n$ and $\{e_1, \dots, e_n\} \subset R^n$ orthonormal basis, let's accept the notation $\hat{P}(\sigma)$, where $\sigma = (\sigma_1, \dots, \sigma_n)$ the binary code, defining the vertex coordinate permutation operator [1]. Applying operators $\hat{P}(\sigma)$ to a vector composed of vertices $A = (a_1, \dots, a_n)$ and $B = (b_1, \dots, b_n)$, we obtain all pairs of vertices that are maximally distant.

The number of operators $\hat{P}(\sigma)$ depends on the dimensionality of the space R^n, that is equal to $2^{n-1} - 1$.

To find the minimum value of the function $F(x)$, we choose pairs of hypercube vertices with the maximum Hamming distance between them. So, these are pairs of hypercube vertices:

$$A_{\sigma_j} = W(\sigma_j) = \left(w(\sigma_{j1}), \dots, w(\sigma_{jn})\right), A_{\bar{\sigma}_j} = W(\bar{\sigma}_j) = \left(w(\bar{\sigma}_{j1}), \dots, w(\bar{\sigma}_{jn})\right), j = 0, \dots, 2^{n-1}.$$

Let's consider vectors $\hat{X}_j = \begin{pmatrix} W(\sigma_j) \\ W(\bar{\sigma}_j) \end{pmatrix} = P(\sigma)\begin{pmatrix} A \\ B \end{pmatrix} \in R^n \times R^n,\ j = 0, \dots, 2^{n-1}$.

Let's apply stochastic operators to these vectors $\hat{P}(\alpha), \hat{Q}(\beta) \in L(R^n \times R^n \times R^n)$

$$\hat{P}(\alpha) = \begin{pmatrix} P(\alpha) & I - P(\alpha) \\ I - P(\alpha) & P(\alpha) \end{pmatrix}, \hat{Q}(\beta) = \begin{pmatrix} I - Q(\beta) & Q(\beta) \\ Q(\beta) & I - Q(\beta) \end{pmatrix},$$

where $P(\alpha), Q(\beta) \in L(R^n; R^n)$, which act as follows: $\forall x = (\xi_1, \dots, \xi_n) \in R^n$

$$P(\alpha)x = P(\alpha)(\sum_{i=1}^n \xi_i e_i) = \sum_{i=1}^n \alpha_i \xi_i e_i,$$

$$Q(\beta)x = Q(\beta)(\sum_{i=1}^n \xi_i e_i) = \sum_{i=1}^n \beta_i \xi_{n-i+1} e_i,$$

where $\alpha = (\alpha_1, \dots, \alpha_n),\ \beta = (\beta_1, \dots, \beta_n) \in R^n,\ \{e_1, \dots, e_n\} \subset R^n$ basis, we will get:

$$\hat{P}(\alpha)\hat{X}_j = \hat{P}(\alpha)P(\sigma)\begin{pmatrix} A \\ B \end{pmatrix} = \hat{Z}_j = \begin{pmatrix} z_{j1} \\ z_{j2} \end{pmatrix}, \hat{Q}(\beta)\hat{X}_j = \hat{Q}(\beta)P(\sigma)\begin{pmatrix} A \\ B \end{pmatrix} = \hat{V}_j = \begin{pmatrix} v_{j1} \\ v_{j2} \end{pmatrix},$$

where $\alpha = (\alpha_1, \dots, \alpha_n),\ \beta = (\beta_1, \dots, \beta_n),\ 0 \le \alpha_i < 1, 0 \le \beta_i < 1$, stochastic vectors.

The result of these actions are vectors, the components of which are the points of the search area with real coordinates, for which the values of the $F(x)$ function are calculated.

$$F(z_{jk}),\ F(v_{jk}),\ k = 1,2,\ j = 1, \dots, 2^n.$$

After determining for each iterative step, the best point of the space R^n, it is necessary to find the value of the fitness function at the vertices of its unitary cubic neighborhood with integer vertices. To obtain such a neighborhood of point $Z_i(z_1^i, z_2^i, \dots, z_n^i)$ need to determine points $Z_0^i(z_1^0, z_2^0, \dots, z_n^0)$ and $Z_{2^n-1}^i(z_1^{2^n-1}, z_2^{2^n-1}, \dots, z_n^{2^n-1})$ with integer coordinates such, that $\forall k: Z_k^0 \le z_k^i,\ z_k^{2^n-1} \ge z_k^i$ and the Euclidean distance between them $\left\|Z_0^i - Z_{2^n-1}^i\right\| = \sqrt{n}$. If the vertex Z_0^i with the minimum coordinate values is assigned a zero binary code, and the vertex $Z_{2^n-1}^i$ with the maximum coordinate values, respectively, a unitary code, then the Hamming distance between them will be maximal and equal to n.

Applying operators $\hat{P}(\sigma)$ to the vector composed of vertices $Z_0^i\ Z_{2^n-1}^i$, we will obtain at the i-th iteration step all maximally distant pairs Z_1, Z_{2^n-2}; Z_2, Z_{2^n-3} … of vertices of the hypercube (which is a unitary neighborhood of point $Z_i(z_1^i, z_2^i, \dots, z_n^i)$) with integer coordinates. Suppose that point $D \in R^n\ D = (d_1, \dots, d)$, is a solution of the Diophantine equation. At the same time, it is one of the vertices of unitary hypercubes. Therefore, point $Z_i(z_1^i, z_2^i, \dots, z_n^i)$ falling into one unitary neighborhood of point $D = (d_1, \dots, d)$, means that when calculating the value of the function $F(x)$ at the vertices of this neighborhood, we must determine the integer solution of the equation, that is, point D. At the same time, the Euclidean distance from point $Z_D(z_1^i, z_2^i, \dots, z_n^i)$ to each of the vertices of the resulting integer cubic neighborhood does not exceed $\sqrt{n}$.

Thus, for a certain finite number of attempts to select operators $\hat{P}(\alpha), \hat{Q}(\beta) \in L(R^n \times R^n; R^n \times R^n)$ [1], we will obtain a solution. Note, that the algorithm can determine several different solutions in a finite number of steps.

At each iterative step, the OGA forms almost always (except for the cases of applying the mutation procedure [1]) a new search area, with a measure smaller than the area of the previous step.

It should be noted, that the search area for the minimum points of the function $|P(x_1, x_2, \dots x_n)|$ can expand, move, and go beyond the initial area Ω, at some iteration steps, which is explained by the nature of the action of stochastic operators $\hat{P}(\alpha), \hat{Q}(\beta) \in$.

Application to Diophantine equations.

Consider the Diophantine equation $P(x_1, x_2, \dots x_n) = 0$, where P — is a polynomial of n variables with integer coefficients. As known, the solution of this equation is defined in natural or integer numbers. Consider the function $F(x) = |P(x_1, x_2, \dots x_n)|$. If the equation has solutions, then at these points the function takes the minimal zero value.

Let us consider examples of application to some Diophantine equations.

The effectiveness of the operator genetic algorithm will be demonstrated by a series of numerical experiments for Diophantine equations with different number of unknowns, both linear and nonlinear. For each type of equation, the experiment consists of 20 trials. Each trial, in turn, consists of a series of attempts that are performed until a positive result is obtained. For equations with the number of unknowns no more than 5, each attempt consists in applying a pair of operators $\hat{P}(\alpha), \hat{Q}(\beta) \in L(R^n \times R^n; R^n \times R^n)$, obtained randomly and in a complete review of all the vertices of the unitary neighborhood to which the best point of a given iterative step has fallen. If the number of unknowns increases, then a complete review of all vertices of a unitary hypercube requires many calculations. For example, for 10 unknowns, a unitary hypercube has 1024 vertices. To reduce the number of calculations, an incomplete review of vertices (for example, 5 % — 10 %) is performed, which are also chosen randomly. Then each attempt is divided into two stages: 1 — random selection of a pair of stochastic operators, 2 — random reviewing of a given set of vertices of a unitary hypercube. For each attempt, the algorithm works with a limited number of iterations (no more than 20). For each trial, the number of attempts, the number of obtained solutions and the corresponding iteration step number are recorded. After receiving a positive result, a new test is performed.

I. ***Linear equations:*** $a_1x_1 + a_2x_2 + \dots + a_nx_n = a$. It is known that the solution of this equation exists under the condition that the $GCD(a_1, a_2, \dots, a_n)$ is a divisor of a.

a) The simplest of such equations is Bezou's equation $ax + by = d$, which has to be solved, for example, when applying bigram encryption using Hill's method. The numerical experiment was carried out for many equations. A positive result was obtained in all tests. For example, consider the equation:

$$28x + 13y = 841.$$

Initial solution search area $\Omega = [1; 28] \times [1; 28]$. The set of solutions $R = \{(24; 13), (37; -15), (11; 41), (115; -183), (271; -519)\}$ obtained as a result of the experiment. Tabl. 1 presents the main parameters of the experiment (notation: B — number of trials; C — total number of attempts; C_c — average number of attempts per trial; C_{max} — maximum number of attempts in one trial; C_{min} — number of trials with a successful first attempt; I_c — average number of iteration steps in all attempts; K_R — is the number of different solutions).

Table 1

B	C	C_c	C_{max}	C_{min}	I_c	K_R
20	42	2	8	9	9	5

All trials ended with a positive result. Note, that the solution $(24; 13)$ was obtained in 12 trials. Accordingly, the solutions $(37; -15)$ — in 4 trials, $(11; 41)$ — in 2 trials. Solutions $(115; -183), (271; -519)$ were obtained once each.

b) The equation of the following form is more complicated:

$$11x_1 + 13x_2 + 15x_3 + 17x_4 + 18x_5 + 9x_6 + 21x_7 + 23x_8 + 31x_9 + 12x_{10} = 1503450.$$

For this equation, 10 trials were carried out, which consisted in the random selection of a pair of stochastic operators and for each pair a random selection of five sets of 25 pairs of vertices of a

10-dimensional hypercube. A positive result was obtained in all trials (50 different solutions were obtained). Tabl. 2 presents the result of the experiment:

Table 2

B	C	C_c	C_{max}	C_{min}	I_c	K_R
10	320	6	58	6	15	50

Below is one of the solutions:

x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}
20419	-12095	32761	35007	39571	-50040	17719	50000	-32191	25900

II. ***Nonlinear equations.*** Let's consider several well-known equations and the results of OGA work.

a) quadratic equation

Consider a quadratic equation with ten unknowns

$11x_1^2 + 13x_2^2 + 15x_3^2 + 17x_4^2 + 18x_5^2 + 9x_6^2 + 21x_7^2 + 23x_8^2 + 31x_9^2 + 12x_{10}^2 = 2013360.$

For this equation, as in the previous case, 10 trials were carried out, which consisted in the random selection of a pair of stochastic operators and for each pair a random selection of five sets of 25 pairs of vertices of a 10-dimensional hypercube. A positive result was obtained in all trials (50 different solutions were obtained). Tabl. 3 presents the result of the experiment:

Table 3

B	C	C_c	C_{max}	C_{min}	I_c	K_R
10	1195	24	226	47	11	50

Below is one of the solutions:

x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}
-81	-28	1	22	97	73	-178	70	193	29

b) an equation of order higher than the second.

$$x^3 + 2y^3 + 3z^3 = 254$$

The numerical experiment for this equation consisted of 21 trials. A positive result was obtained in all trials.

Area of search for solutions $\Omega = [-10; 10] \times [-10; 10] \times [-10; 10]$. It is easy to see, that in this domain, the equation has five solutions $R = \{(1; 5; 1), (2; 3; 4), (6; 7; -6), (4; -1; 4), (-7; -6; 7)\}$. As a result of the experiment, all five solutions were obtained. Tabl. 4 presents the main parameters of the experiment:

Table 4

B	C	C_c	C_{max}	C_{min}	I_c	K_R
21	70	3	16	1	4	5

Note, that the solution $(4; -1; 4)$ was obtained in 11 trials. Solution $(2; 3; 4)$ — in 7 trials. Other solutions were obtained once.

c) Let's consider an equation with four unknowns:

$$\frac{x}{y} + \frac{y}{z} + \frac{z}{t} + \frac{t}{x} = 1.$$

The numerical experiment for this equation consisted of 20 trials. A positive result was obtained in all trials.

Initial solution search area $\Omega = [-10;10] \times [-10;10] \times [-10;10] \times [-10;10]$. As a result of the experiment, fifteen different solutions were obtained, among them $(3;-9;-6;4), (9;-6;-4;12), (-3;9;-6;-4)$ — obtained twice, and solution $(4;3;-2;6)$ — trice. Tabl. 5 presents the main results of the experiment:

Table 5

B	C	C_c	C_{max}	C_{min}	I_c	K_R
20	210	11	50	1	5	15

d) exponential equations.

$$7^x + 5^y + 3^z = 19619.$$

The numerical experiment for this equation consisted of 20 trials. A positive result was obtained in all trials. Initial solution search area $\Omega = [0;20] \times [0;20] \times [0;20]$. As a result of the experiment in the search area, a solution $(5;4;7)$ was obtained in all trials. Tabl. 6 presents the main results of the experiment:

Table 6

B	C	C_c	C_{max}	C_{min}	I_c	K_R
20	311	16	41	3	4	1

e) $7^x 5^y 2^z = 336140000$

The numerical experiment for this equation consisted of 21 trials. A positive result was obtained in all trials. Initial solution search area $\Omega = [0;10] \times [0;10] \times [0;10]$. As a result of the experiment in the search area, a solution $(5;4;5)$ was obtained in all trials. Tabl. 7 presents the main results of the experiment:

Table 7

B	C	C_c	C_{max}	C_{min}	I_c	K_R
21	246	12	43	1	3	1

f) Let's consider an equation $8^x + 17^y = z^2$. In [9] it is stated that this equation has only four non-negative integer solutions.

The numerical experiment for this equation consisted of 20 trials. A positive result was obtained in all trials, that is, all solutions were obtained $(1;0;3)$ — 18 trials, $(1;1;5)$ — 17 trials, $(2;1;9)$ — 5 trials, $(3;1;23)$ — 2 trials.

g) Let's consider Catalan equation

$$x^z - y^t = 1, \text{ where } z,t > 1.$$

As known, it has a single solution under given restrictions $(3;2;2;3)$. (A partial case of the Catalan equation is the Euler equation $x^3 - y^2 = 1$, which has a single solution (3,2)). If $z,t > 1$ limit is not considered, then the equation has infinite solutions.

The numerical experiment for this equation consisted of 21 trials without limit $z,t > 1$. A positive result was obtained in all trials. Initial solution search area $\Omega = [0;10] \times [0;10] \times [0;10] \times [0;10]$. As a result of the experiment, 7 times different solutions containing single values of the unknowns z,t were obtained in the search area. In the other 14 trials, a solution $(3;2;2;3)$ was obtained. Tabl. 8 presents the main results of the experiment:

Table 8

B	C	C_c	C_{max}	C_{min}	I_c	K_R
20	52	6	7	1	3	1

III. Finally, let's consider the rather difficult problem of finding the roots of the Diophantine equation with symmetric encryption, i.e. consider an example with the so-called "**Diophantine difficulties**".

Let's consider the mathematical model of the alphabetic cryptosystem of information protection ([6]) $\sum = \langle M^*, Q, C^*, E(m), D(c) | V(E(m), D(c)) \rangle$, where M^* — is the set of all messages $m = m_1 m_2 ,. . ., m_k$ (open text) over alphabet M; m_i, $i = 1 .. . k$ — elementary messages; Q — is a set of numerical equivalents of elementary messages m_i with M^*; C^* — is the set of all ciphergrams $c = c_1 c_2 \ldots c_k$ over alphabet C, (perhaps $M = Q = C$); $E(m)$ — direct conversion algorithm of message m into c; $D(c)$ — inverse transformation algorithm of ciphergram c into $m \in M^*$. We emphasize, that the direct and inverse transformation in this algorithm is unambiguous. For example, let's consider a model of a data protection system based on finding the roots of a Diophantine equation of the form:

$$x^2 + py^2 = z^2, \quad p \in N, \tag{1}$$

for which the $E(m)$ and $D(c)$ algorithms are built on the basis of the solutions of the equation (1). It is known ([6]), that the class of solutions of this equation over N, is as follow:

$$x = -a^2 + pb^2, \qquad y = 2ab, \qquad z = a^2 + pb^2, \qquad \forall a, b \in N, \qquad b > a .$$

Let's consider the encryption of some message (elementary — bigrams of letters of the Latin alphabet, which, including spaces, has 27 characters). Numerical equivalent of bigrams $m_i m_{i+1}$ can be obtained using the formula $27q_i + q_{i+1}$.

Direct conversion function $E(a, b, \mu) = (-a^2 + pb^2)^2 + (2ab)^2 + \mu$, where μ — is a secret key.

Inverse transformation function $D(a, b, \mu) = (a^2 + pb^2)^2 - \mu$.

Let's consider an example of the application of OGA to the given procedure for encrypting and decrypting a message.

Let $p = 13$, alphabet $M = \{a, b, c, d, \ldots, y, z\}$, message $m = \boldsymbol{diophant}$.

The numerical equivalents of the letters of this message are presented in the tabl. 9.

Table 9

d	i	o	p	h	a	n	t
3	8	14	15	7	0	13	19

Let's assume for the bigram "di" the secret key is $\mu = 27a + b = 27 \cdot 3 + 8 = 89$, for the bigram "op" the secret key is $\mu = 27a + b = 27 \cdot 14 + 15 = 393$, for the bigram "ha" – $\mu = 27a + b = 27 \cdot 7 + 0 = 189$, and for the bigram "nt" – $\mu = 27a + b = 27 \cdot 13 + 19 = 370$.

Then the cipher of the first bigram "di" gets the value $E(a, b, \mu) = E(3,8,89) = 707370$. Similarly: the bigram "op" corresponds to the number $E(a, b, \mu) = E(14,15,89) = 9741034$, bigram "ha" corresponds to the number $E(a, b, \mu) = E(7,0,89) = 2590$, bigram "nt" corresponds to the number $E(a, b, \mu) = E(13,19,89) = 23639414$.

If the secret key is known (for example, for bigrams «nt» μ=370), then decoding is quite easy by solving the Diophantine equation $D(a, b, \mu) = (a^2 + 13b^2)^2 = 23639414 - 370 = 23639044 = 4862^2$, therefore $a^2 + 13b^2 = 4862$. The solution a=13, b=19 is quite easy to determine (also, using OGA).

In order to find the values of a, b, without having a secret key, it is necessary to solve the following Diophantine equations:

for bigram «di» $E(a, b, \mu) = (-a^2 + pb^2)^2 + (2ab)^2 + 27a + b = 707370$,

bigram «op» $E(a, b, \mu) = (-a^2 + pb^2)^2 + (2ab)^2 + 27a + b = 9741034$,

bigram «ha» $E(a, b, \mu) = (-a^2 + pb^2)^2 + (2ab)^2 + 27a + b = 2590$,

bigram «nt» $E(a, b, \mu) = (-a^2 + pb^2)^2 + (2ab)^2 + 27a + b = 23639414$.

Solving such nonlinear Diophantine equations (given that the solution is unique) is a rather difficult task. The OGA proposed in this work allows quickly and efficiently find solutions of these equations.

When applying OGA, it is necessary to find the minimum of the function $F(a,b) = |(-a^2 + pb^2)^2 + (2ab)^2 + 27a + b - E(a,b,\mu)|$ within area $\Omega = [0{,}28] \times [0{,}28] \in R \times R$.

For example, let's consider decoding of bigram "nt", means, we need to find the solution of the Diophantine equation $(-a^2 + pb^2)^2 + (2ab)^2 + 27a + b = 23639414$. 20 trials were conducted for this equation. A positive result was obtained in all trials. The solution obtained is (13; 19). Tabl. 10 presents the main results of the experiment:

Table 10

B	C	C_c	C_{max}	C_{min}	I_c	K_R
20	135	7	25	1	4	1

Fig. 1 shows the sequence of iterative steps for finding a solution when using operators

$$\hat{P}(\alpha) = \begin{pmatrix} 0{,}16 & 0 & 0{,}84 & 0 \\ 0 & 0{,}20 & 0 & 0{,}80 \\ 0{,}84 & 0 & 0{,}16 & 0 \\ 0 & 0{,}80 & 0 & 0{,}20 \end{pmatrix}, \hat{Q}(\beta) = \begin{pmatrix} 0 & 0{,}94 & 0 & 0{,}06 \\ 0{,}83 & 0 & 0{,}17 & 0 \\ 0 & 0{,}06 & 0 & 0{,}94 \\ 0{,}17 & 0 & 0{,}83 & 0 \end{pmatrix},$$

where, at the seventh step of approximation, the point number 5 with coordinates $z_5 = [12{,}65097; 19{,}05951]$ is obtained. The square, surrounding this point, has the following coordinates of the vertices [12,19], [12,20], [13,20], [13,19] and in the point [13,19], the function $F(13{,}19) = 0$, as a result, an integer solution is obtained that decodes the bigram "nt".

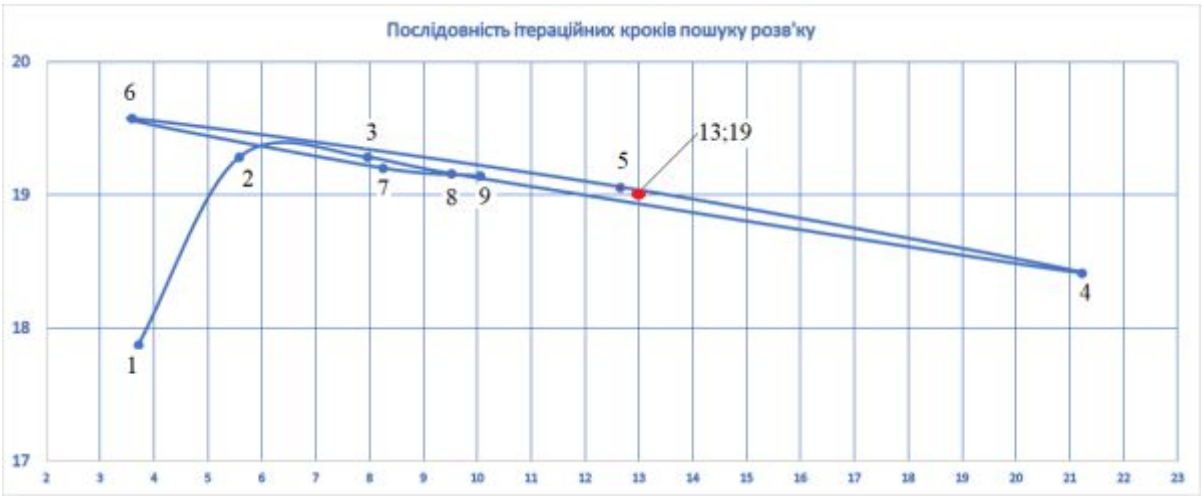

Fig. 1. Similarly, the solutions of the other three equations can be obtained

Conclusions

The application of the operator genetic algorithm to the solution of Diophantine equations of different types and with different number of unknowns demonstrated the effectiveness of the proposed version. As a result of computational experiments (with a small number of iterative steps), which were performed for six known types of equations, positive results were obtained in 100% of the trials. It is important to highlight the positive result of applying the operator genetic algorithm to the problem of symmetric encryption and decryption, that is, the possibility of its use by cryptanalysts.

References

[1] Oliinyk L. (2019) Operatorna model recombinacii v genetichnih algoritmah [Operator model of recombination in genetic algorithms]. *Mathematical modeling*. – issue 1(40). Kamianske. DDTU. P. 14–21. (in Ukrainian).

[2] Oliinyk L., Oliinyk D. (2021) Pro efectivnist operatornoi modificacii genetichnogo algoritmu v zadachah dvovimirnoi optimizacii (On the effectiveness of operator modification of the genetic algorithm in two-dimensional optimization problems). - *"Grail of Science" magazine* No. 11. P. 221–229. (in Ukrainian).
[3] Oliinyk L., Dovzhenko O. (2023) Demonstraciynyi programnyi zasib tryvymirnoi operatornoi modeli genetichnogo algoritmu (Demonstration software of the three-dimensional operator model of the genetic algorithm). *Mathematical problems of technical mechanics - 2023,* , theses of the report International scientific conference, volume 2, Kyiv, Dnipro, Kamianske. (in Ukrainian). P. 5–7.
[4] Oliinyk L. (2023) Operatornyj genetichnyj algoritm i navchannia nejronnoj meregi. *Computer Science and Applied Mathematics* № 2. Zaporiggia, ZNU. P. 53–58.
[5] Hlybovets M.. Gulaeva N. (2013) Evolyuciyni algorytmi (Evolutionary algorithms): textbook. K.: NaUKMA, (in Ukrainian). 828 p.
[6] Osipyan V. O. (2018) Mathematical modeling of a data protection system based on Diophantine equations. *Caspian Journal: Control and High Technologies.* № 1 (41). P. 151–160.
[7] Chandrasegar T., Senthilkumar M., R.Silambarasan, Carlos B.W. (2016) Analyzing the strength of Pell's RSA.- *IJPT*. Dec-2016. Vol. 8. Issue № 4. P. 21869–21874.
[8] Siby A., Sugata S., Mukund S. A Connectionist Network Approach to Find Numerical Solutions of Diophantine Equations. *arXiv:1206.*1971 [cs.NE]
[9] Chikkavarapu G. R. (2018) On the Diophantine equation $3^x + 7^y = z^2$. *Research & Development EPRA International Journal of (IJRD) Monthly Peer Reviewed & Indexed International Online Journal.* Volume 3, Issue:6, June 2018. P. 93–95.

Список використаних джерел

1. Олійник Л.О. Операторна модель рекомбінації в генетичних алгоритмах. Математичне моделювання. 2019. вип.1(40). Кам'янске. ДДТУ. С. 14–21.
2. Олійник Л.О., Олійник Д.Л. Про ефективність операторної модифікації генетичного алгоритму в задачах двовимірної оптимізації. МНЖ «Грааль науки» № 11. 2021. С. 221–229.
3. Олійник Л.О., Довженко О.О. Демонстраційний програмний засіб тривимірної операторної моделі генетичного алгоритму. Математичні проблеми технічної механіки – 2023: зб. тез доп. міжнар. наук.- конф, том 2, м. Київ, Дніпро, Кам'янське.18-20 квітня 2023 р., Кам'янське. 2023. С. 5–7.
4. Олійник Л.О. Операторний генетичний алгоритм і навчання нейронної мережі. Computer Science and Applied Mathematics № 2. 2023. Запоріжжя. ЗНУ. С. 53–58.
5. Глибовець М.М., Гулаєва Н.М. Еволюційні алгоритми: підручник. Київ.: НаУКМА, 2013. 828 с.
6. Osipyan V.O. Mathematical modeling of a data protection system based on Diophantine equations. Caspian Journal: Control and High Technologies, 2018. № 1 (41). P. 151–160.
7. Chandrasegar T., Senthilkumar M., Silambarasan R., Carlos B.W. Analyzing the strength of Pell's RSA. IJPT. 2016. Vol. 8. Issue No.4. p. 21869–21874.
8. Siby A., Sugata S., Mukund S. A Connectionist Network Approach to Find Numerical Solutionsof Diophantine Equations. *arXiv:1206.*1971 [cs.NE]
9. Chikkavarapu G. R. On the Diophantine equation $3^x + 7^y = z^2$. Research & Development EPRA International Journal of (IJRD) Monthly Peer Reviewed & Indexed International Online Journal Volume. 3. Issue.6, 2018. P. 93–95.

Надійшла до редколегії 15.10.2024