UDC 621.316.13

MODELING OF THE PRIMITIVE ROOTS STRUCTURE THAT ARE ASSOCIATED WITH GIVEN PRIME NUMBERS

G. Vostrov, I. Yakshyn
Odessa national polytechnic university

Abstract. *The problem of calculating the set of all primitive roots of an arbitrary prime number is considered. The algorithm for checking the natural number on the property of being the primitive root of a given prime number is constructed. The properties of the structures of recursive cycles of primitive roots are investigated. It is proved that all primitive roots of any prime number form pairs in which the recursive cycle of one is the inverse of the recursive cycle of the other element of the pair. The possibilities of representing recursive cycles in two-dimensional space are investigated. It is shown that recursive cycles form dynamic processes.*

Keywords: *Fermat's little theorem, cyclic group, permutation group, algebraic dynamical system, computational complexity, recursion structure, primitive root.*

Introduction

In modern as pure, and applied mathematics the theory of prime numbers has an exceptional appeal. The solution of many problems of modern theory of prime numbers will make it possible, on the one hand, to deepen the idea of how to develop the fundamental foundations of mathematics, and on the other hand, it will allow creating more and more effective arithmetic methods for constructing fast algorithms for discrete orthogonal transformations in the analysis and processing of complex data [2]. To the complex data is the modern area of Big Data Science [3], signal processing, cryptography [4] and others.

The experience of working on the problems of pure and applied mathematics shows that there are unsolved mathematical problems whose solution is important both for deepening and developing new methods for solving complex problems of pure mathematics and for creating effective algorithms for solving problems from applied fields, some of which are listed above.

Until now, the unproved validity of the Artin's conjecture [5] according to which, if the natural number is not 0, ± 1, and the perfect square, then the equality

$$\pi(x,a) = c(a) \cdot \pi(x), \qquad (1)$$

where - number of primes , the number of prime numbers for which is the primitive root, – constant depends only on the value . In [6] we formulated the generalized Artin conjecture, where simultaneously the ways of solving it were determined by means of experimental mathematics [7, 8].

Certainly, any results obtained on the basis of computer modeling should be further proved by analytical methods [9].

Simply attracting analytical methods to solve this Artins hypothesis and its generalization at the moment is not possible. The existence of a constant $c(a)$ in (1) confirms a simple consideration, namely, that there must be a procedure for regular sifting of primes for any number for which a is an primitive root. In [10] it is proved that there are infinitely many such prime numbers. Until now, it has not been proved by what properties all prime numbers have, for which a is the primitive root, that is, a is the generating element of the cyclic group $(Z/Z_p)^*$ for any $p \in P$, where P is the set of all primes [12].

To solve this problem, it makes sense to solve initially a different, as it seems to us, simpler problem. For some simple number p, find all its primordial roots and explore their properties. Clearly, what if a is primitive number root it is sufficient to consider $a < p$. In the general case, the number a can be a composite, but not ± 1 and a perfect square. It is known that for any p number of its primitive roots is equal to $\varphi(p-1)$, where φ – Euler function. With increasing p, the number of primitive roots increases. Let m_i be some primitive root of a prime number p. Let's pretend that $m_p = \{m_{1p}, m_{2p}, \text{K}, m_{\varphi(p-1)p}\}$ - set of all primitive roots, prime number p. Potentially primitive roots of a prime number p can be any number from 2 to $p-1$, except those that are perfect squares.

Checking the number m for the possibility of being the primitive root of a prime number p is computationally complex from an algorithmic point

of view if one takes into account that the number of checks increases with increasing p. In addition, for any prime number, it is not a simple task to calculate the Euler function $\varphi(p-1)$, which is defined by expression:

$$\varphi(p-1)=\prod_{i=1}^{k}(p_i^{\alpha_i}-p_i^{\alpha_{i-1}}), \qquad (2)$$

where $p-1=\prod_{i=1}^{k}p_i^{\alpha_i}$ - its prime factorization. The computation of the Euler function itself is computationally a simple task. A much more complicated problem is the factorization of the number $p-1$. If $p-1$ not a large number, for example order 10^6, then the factorization problem is solved quite simply. At significantly higher values, computational difficulties of subexponential character arise. To solve the factorization problem, the methods described in [12] were used.

Calculation a primitive root of prime number and the analysis of their properties

According to the little Fermat theorem, if the number m is an antiderivative root of the number p, then condition

$$m^{p-1}\equiv 1(\mathrm{mod}\, p) \qquad (3)$$

This condition is necessary, but not sufficient. For this reason, it is necessary to perform a check on the more complicated procedure given in the monograph [12]. Let a prime number p be given and a candidate for primitive roots be m. We perform factorization $p-1$ presenting $p-1=\prod_{i=1}^{k}p_i^{\alpha_i}$ and for each prime factor from $\{p_1, p_2, \mathrm{K}, p_k\}$ we check that condition

$$m^{\frac{p-1}{p_i}}\neq 1(\mathrm{mod}\, p). \qquad (4)$$

For this, a recursive procedure is implemented

$$x_{n+1}=mx_n(\mathrm{mod}\, p), \qquad (5)$$

at $x_0=1$ to $n+1=\frac{p-1}{p_i}$ and the above condition (4) must be satisfied at the last step of the recursion.

Suppose that for a certain number condition (4) is satisfied, then we compute a sequence of values

$$x_p=1,\ x_{n+1}=mx_n(\mathrm{mod}\, p) \text{ to } x_{p-1}\equiv 1(\mathrm{mod}\, p) \qquad (6)$$

and we obtain the vector $(x_{1\cdot m_1}, x_{2\cdot m_1}, \mathrm{K}, x_{(p-r)\cdot m_1})$ of lenght $p-2$. Such vectors are constructed for all

$$m_i\in m_p=\{m_{1\cdot p}, m_{2\cdot p}, \mathrm{K}, m_{(p-1)\cdot p}\} \qquad (7)$$

It is obvious that for all primitive roots of the set m all vectors have the same length equal to $p-2$. The set of such vectors is the basis for analyzing the properties of the set of primitive roots of a prime number p. Note that the recursion cycle for the primitive root m_i actually has the form:

$$(1, x_{1\cdot m_i}, x_{2\cdot m_i}, \mathrm{K}, x_{(p-1)\cdot m_i}) \qquad (8)$$

The last unit refers to the next cycle, and therefore the cycle length is $p-1$, which agrees with Fermat's little theorem [1]. The analysis of cycles (orbits) of recursions for the set of all primitive roots allowed us to establish, that for any $m_{i\cdot p}\in\{m_{1\cdot p}, m_{2\cdot p}, \mathrm{K}, m_{\varphi(p-1)\cdot p}\}$ there is always $m_{j\cdot p}$ at $j\neq p$, that a recursive cycle $m_{i\cdot p}$ without the first unit is the inversion of the cycle $m_{j\cdot p}$. In essence, the set $\{m_{1\cdot p}, m_{2\cdot p}, \mathrm{K}, m_{\varphi(p-1)\cdot p}\}$ decomposes into pairs of primitive roots. This is a new property of the set of primitive roots that was not previously known. The number of primitive roots is greatest for primes $p^*=Z_p+1$ for $p*\&p\in P$, which are usually called prime numbers of Sophie Germain and the smallest number of smooth prime numbers [12]. For various $p\in P$ the number of compound primitive roots is always significantly larger than the number of simple primitive roots. This is explained simply enough, since $\varphi(p-1)$ shows the number of natural numbers that are relatively prime to $p-1$.

Each primitive root is the parent of the group $(Z/Z_p)^*$. In addition, each of them generates a set of pseudo-random numbers. If we average over the set of all cycles, we get a pseudo-random sequence in which all randomness tests allow us to state that in this sequence there are no inner cycles in any form.

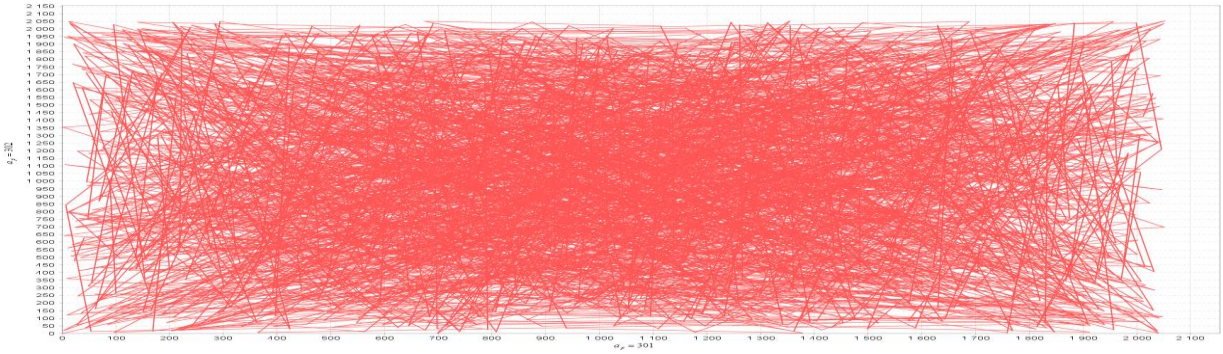

Figure 1. The interaction of recursive cycles in a two-dimensional system.

Consider primitive roots and cycles for a prime number $p = 37$.

Table 1.
The inverse recursive cycle of primitive roots 2 and 19 of prime number 37

Primitive root	Cycle
2	2, 4, 8, 16, 32, 27, 17, 34, 31, 25, 13, 26, 15, 30, 23, 9, 18, 36, 35, 33, 29, 21, 5, 10, 20, 3, 6, 12, 24, 11, 22, 7, 14, 28, 19, 1
19	19, 28, 14, 7, 22, 11, 24, 12, 6, 3, 20, 10, 5, 21, 29, 33, 35, 36, 18, 9, 23, 30, 15, 26, 13, 25, 31, 34, 17, 27, 32, 16, 8, 4, 2, 1

Table 2.
The inverse recursive cycle of primitive roots 5 and 15 of prime number 37

Primitive root	Cycle
5	5, 25, 14, 33, 17, 11, 18, 16, 6, 30, 2, 10, 13, 28, 29, 34, 22, 36, 32, 12, 23, 4, 20, 26, 19, 21, 31, 7, 35, 27, 24, 9, 8, 3, 15, 1
15	15, 3, 8, 9, 24, 27, 35, 7, 31, 21, 19, 26, 20, 4, 23, 12, 32, 36, 22, 34, 29, 28, 13, 10, 2, 30, 6, 16, 18, 11, 17, 33, 14, 25, 5,1

Table 3.
The inverse recursive cycle of primitive roots 13 and 20 of prime number 37

Primitive root	Cycle
13	13, 21, 14, 34, 35, 11, 32, 9, 6, 4, 15, 10, 19, 25, 29, 7, 17, 36, 24, 16, 23, 3, 2, 26, 5, 28, 31, 33, 22, 27, 18, 12, 8, 30, 20, 1
20	20, 30, 8, 12, 18, 27, 22, 33, 31, 28, 5, 26, 2, 3, 23, 16, 24, 36, 17, 7, 29, 25, 19, 10, 15, 4, 6, 9, 32, 11, 35, 34, 14, 21, 13, 1

Table 4.
The inverse recursive cycle of primitive roots 17 and 24 of prime number 37

Primitive root	Cycle
17	17, 30, 29, 12, 19, 27, 15, 33, 6, 28, 32, 26, 35, 3, 14, 16, 13, 36, 20, 7, 8, 25, 18, 10, 22, 4, 31, 9, 5, 11, 2, 34, 23, 21, 24, 1
24	24, 21, 23, 34, 2, 11, 5, 9, 31, 4, 22, 10, 18, 25, 8, 7, 20, 36, 13, 16, 14, 3, 35, 26, 32, 28, 6, 33, 15, 27, 19, 12, 29, 30, 17, 1

Table 5.
The inverse recursive cycle of primitive roots 18 and 35 of prime number 37

Primitive root	Cycle
18	18, 28, 23, 7, 15, 11, 13, 12, 31, 3, 17, 10, 32, 21, 8, 33, 2, 36, 19, 9, 14, 30, 22, 26, 24, 25, 6, 34, 20, 27, 5, 16, 29, 4, 35, 1
35	35, 4, 29, 16, 5, 27, 20, 34, 6, 25, 24, 26, 22, 30, 14, 9, 19, 36, 2, 33, 8, 21, 32, 10, 17, 3, 31, 12, 13, 11, 15, 7, 23, 28, 18, 1

Table 6.
The inverse recursive cycle of primitive roots 22 and 32 of prime number 37

Primitive root	Cycle
22	22, 3, 29, 9, 13, 27, 2, 7, 6, 21, 18, 26, 17, 4, 14, 12, 5, 36, 15, 34, 8, 28, 24, 10, 35, 30, 31, 16, 19, 11, 20, 33, 23, 25, 32, 1
32	32, 25, 23, 33, 20, 11, 19, 16, 31, 30, 35, 10, 24, 28, 8, 34, 15, 36, 5, 12, 14, 4, 17, 26, 18, 21, 6, 7, 2, 27, 13, 9, 29, 3, 22, 1

The value of the Euler function for this number will be $\varphi(p-1)=12$, which is equal to the number of primitive roots for a given prime number. As follows from the data above, all primitive roots have a recursively inversion pair.

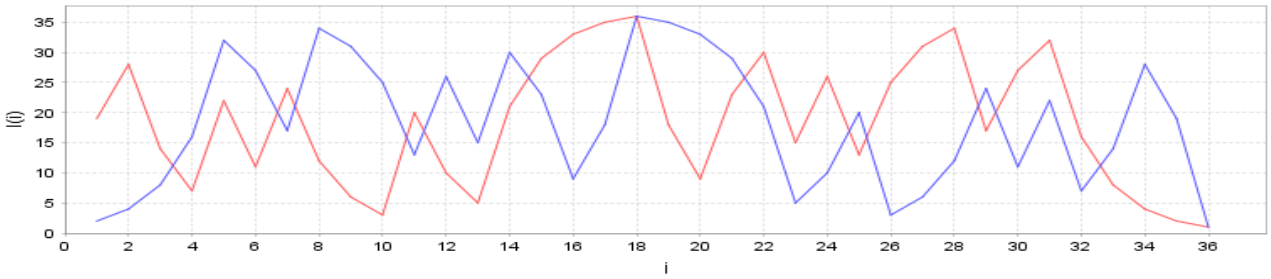

Figure 2 – The primitive roots 2 and 19 of prime number 37 in a two-dimensional system

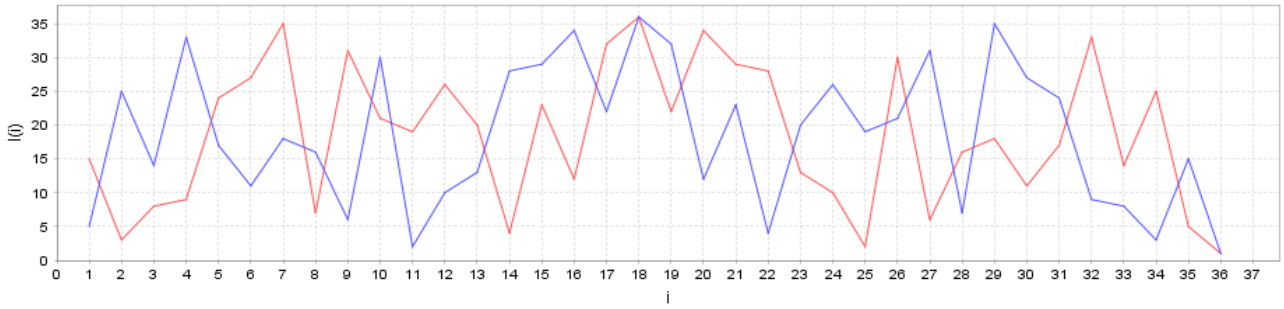

Figure 3 – The primitive roots 5 and 15 of prime number 37 in a two-dimensional system.

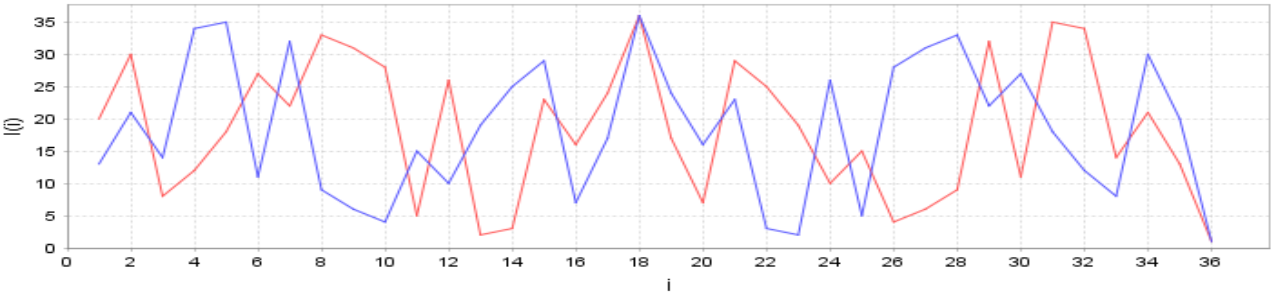

Figure 4 – The primitive roots 13 and 20 of prime number 37 in a two-dimensional system.

Actually, based on the data on the primitive roots of a prime number, the following model for the study of the set of primes is added up, for which a given number a is a primitive root. Suppose a is chosen and it is established that for some p, a is a primitive root. We find a set of primitive roots of the number $m_p=\{m_{1\cdot p}, m_{2\cdot p}, \text{K}, m_{\varphi(p-1)\cdot p}\}$ and let a belong to this set. In addition, let some $p^*>a$ also belongs to m_p. From the analysis of the mathematical experiment follows, that a is also an antiderivative root for p^*. Thus, the scheme.

$$a \to p^* \to p \Rightarrow a \to p \qquad (9)$$

If this transitive "law" turns out to be correct, then additional information will appear on the laws of formation of the set of primes for which a is a primitive root. So in the Artin's hypothesis, based on the data of experimental mathematics, two facts are established:

1) for any $p \in P$ a set

$$m_p=\{m_{1\cdot p}, m_{2\cdot p}, \text{K}, m_{\varphi(p-1)\cdot p}\} \qquad (10)$$

divide into pairs in which the recursion on the basis of one element is the inverse of the recursion of the other element of the pair. The pairs can be formed by two prime numbers, two compound ones and one simple and one compound. It is necessary to prove this fact analytically. For the existence of an inversion it is necessary and sufficient that in any pair $(m_{1\cdot p}, m_{2\cdot p})$ first element of recursion m_1 was equal to the last in m_2 and vice versa. This implies the equality of two recursions. The conditions under which this happens are probably easy to establish. It is more difficult to prove that the recursions coincide under inversion.

2) Suppose, that is a - is a primitive root for all $p \in P_a=\{p_1, \text{K}, p_a\}$.

Prove it: Let $a \to p_i$ and $p_i \to p_j = a \to p_i$ at $a < p_i < p_j$.

That is, there is transitivity. It is entirely possible that this is transferred to the theory of finite fields, elliptic curves, and modular forms.

An important question: how to find a module m such that the residues of this module by P_a differ from the residues of this module on the set $P - P_a$. The question of the existence of such a module is open. It is possible that there is a system of modules $\{m_1, \text{K}, m_x\}$ the residues over which have properties that are defined by some function like $f(Z_{m_l}, \text{K}, Z_{m_k})$. This may be due to the Dirichlet theorem on arithmetic progression. The question of whether it can be generalized to a system of arithmetic progressions remains open.

Conclusions

Analyzing primordial roots, it was found that there are pairs of primitive roots in which recursion on the basis of one element is an inversion of the recursion of another element of the pair. If we explain this point in an analytical way, we will get additional information on the laws of the formation of a set of primes for which a is a primitive root. The processes of interaction of recursive cycles between different pairs of primitive roots of a prime number p. It is proved that dynamic processes have a chaotic nature, the investigations of which are an important task of theories of dynamical systems.

References

1. Manin, U. I., Panchishkin, A. A., (2009), Introduction to modern number theory [Vvedenie v sovremennyu teoriu chisel], Moscow center for continuous mathematical education, pp. 76–89.

2. Chernov, V. M., (2007), Arithmetic methods for the synthesis of fast algorithms for discrete orthogonal transformations [Arifmeticheskie metody sinteza bystryh algoritmov diskretnyh ortogonalnyh preobrazovaniy], Firmalit, pp. 112–118.

3. Mallat, S., (2016), Course "High Dimensional Data Analysis", École Normale Supérieure, pp. 221–223.

4. Chakraborty, R. S., Scgwabe, P., Solwaeth, J., (2016), Security, Privacy and Cryptography Engineering, Springer International Publishing, pp. 37–42.

5. Ambrose, C. D., (2018), Artin's Primitive root conjecture, Gottingen university, pp. 312–315.

6. Vostrov, G. N., Opjata, R. J., (2018), Computer modeling of dynamic processes in analytic number theory [Komputernoe modelirovanie dynamicheskih processov v analiticheskoy teoriy chisel], Odessa National Polytechnic University ELTECS, pp. 18–24.

7. Caragin, M., (2017), Sequential Experiments with Primes, Springer International Publishing, pp. 276–277.

8. Bailey, O. N., Borwein, J. M., Calkin, N. J., Girgensohn, R., Luke, D. R., Moll, V. H., (2006), Experimental Mathematic in Action, A K Perers/CRC press, pp. 77–79.

9. Murty, M. R., (2008), Problems in Analytic Number Theory, Springer Science + Business Media LLC, pp. 98–101.

10. Moree, P., (1993), A note on Artin's conjecture, Simon Stevin vo1.67.N:3–4, pp. 12–13.

11. Brudern, J., Godinho, H., (2002), On Artin's conjecture, Paris of additive Forms / Proe. London Math Soe, pp. 141–144.

МОДЕЛЮВАННЯ СТРУКТУРИ ПЕРВІСНИХ КОРЕНІВ ПОВ'ЯЗАНИХ З ЗАДАНИМИ ПРОСТИМИ ЧИСЛАМИ

Г. М. Востров, І. М. Якшин
Одеський національний політехнічний університет

Анотація. *Рішення багатьох завдань сучасної теорії простих чисел дозволяє, з одного боку, поглибити уявлення про те, як розвивати фундаментальні основи математики, а з іншого - створювати більш ефективні арифметичні методи побудови швидких алгоритмів або дискретних ортогональних перетворень при аналізі та обробці складних даних. Однією із проблем сучасної математики у сукупності із криптографією є задача пошуку первісних коренів. У даній статті розглянуто задачу обчислення множини всіх первісних коренів довільного простого числа p. Окрім того, була описана важливість даної задачі в сучасному світі, а зокрема, використання теорії первісних коренів у криптографії. Побудований алгоритм перевірки натурального числа n на властивість бути первісним коренем заданого простого числа. У ході роботи було з'ясовано, що існують неспецифічні рекурсивні цикли, було досліджено властивості структур рекурсивних циклів первісних коренів. Доведено, що всі первісні коріння будь-якого простого числа утворюють пари, в яких рекурсивний цикл одного є інвер-*

сією рекурсивного циклу іншого елемента пари. Приведено приклади первісних коренів та їх внутрішніх циклів, а також інверсійні пари. Дана властивість первісних коренів не зазначалася раніше у літературі. У ході роботи також було досліджено можливості представлення рекурсивних циклів в двовимірному просторі. Результати представлені в виді графіків інверсійних пар первісних коренів простих чисел. Показано, що рекурсивні цикли утворюють динамічні процеси. Доведено, що динамічні процеси мають хаотичний характер, дослідження якого є важливим завданням теорії динамічних систем. У подальшому планується детально дослідити структуру внутрішніх циклів для пар чисел. Аналіз таких структур є кроком до вирішення складних теоретико – математичних задач та задач криптографії, де використовуються первісні корені.

Ключові слова: *Мала теорема Ферма, циклічна група, група перестановок, алгебраїчна динамічна система, обчислювальна складність, структура рекурсії, первісний корінь*

МОДЕЛИРОВАНИЕ СТРУКТУРЫ ПЕРВООБРАЗНЫХ КОРНЕЙ СВЯЗАННЫХ С ЗАДАННЫМИ ПРОСТЫМИ ЧИСЛАМИ

Г. Н. Востров, И. Н. Якшин
Одесский национальный политехнический университет

Аннотация. *Рассмотрена задача вычисления множества всех первообразных корней произвольного простого числа p. Исследованы свойства структур рекурсивных циклов первообразных корней. Доказано, что все первообразные корни любого простого числа образуют пары, в которых рекурсивный цикл одного является инверсией рекурсивного цикла другого элемента пары. Показано, что рекурсивные циклы образуют динамические процессы.*

Ключевые слова: *Малая теорема Ферма, циклическая группа, группа перестановок, алгебраическая динамическая система, вычислительная сложность, структура рекурсии, первообразный корень.*

Received: 15.11.2018.

George Vostrov, Ph. D. of Technical Sciences, Associate Professor of the Department of Applied Mathematics and Information Technologies, Odessa National Polytechnic University. Shevchenko ave., 1, Odessa, Ukraine.
E-mail: vostrov@gmail.com, mob. +380503168776
Востров Георгій Миколайович, кандидат технічних наук, доцент кафедри прикладної математики та інформаційних технологій Одеського національного політехнічного університету. Проспект Шевченко, 1, Одеса, Україна. E-mail: vostrov@gmail.com, тел. +380503168776
ORCID ID: 0000-0003-3856-5392

Illia Yakshyn, Student of the Department of Applied Mathematics and Information Technologies, Odessa National Polytechnic University. Shevchenko ave., 1, Odessa, Ukraine.
E-mail: ilya.yakshun@gmail.com
Якшин Ілля Миколайович, студент кафедри прикладної математики та інформаційних технологій, Одеського національного політехнічного університету. Проспект Шевченко, 1, Одеса, Україна.
E-mail: ilya.yakshun@gmail.com
ORCID ID: 0000-0003-4780-4148