UDC 621.316.13

EFFECTIVE COMPUTABILITY OF THE STRUCTURE OF THE DYNAMIC PROCESSES OF THE FORMATION OF PRIMES

G. Vostrov, R. Opiata
Odessa national polytechnic university

Abstract. *An interval method for studying the dynamics of the formation of primes is developed. On the basis of Fermat's theorem and the residue theorem, a method is developed for analyzing the properties of prime numbers in terms of the length of the iterative cycle of fixed points determined by prime numbers. Classification of prime numbers is constructed. The results of computer simulation of the processes of the formation of prime numbers with account of classification properties are presented.*

Key words: *Dynamical system, Prime numbers, The theory of residues, Fermat's theorem, Classes of prime numbers, Class structure, Theorems on properties of prime numbers, Interval method of computer modeling.*

Introduction

Mathematics is the queen of sciences
and number theory is the queen of mathematics
- K.F. Gauss

The fundamental importance of number theory in modern mathematics not only does not decrease, but on the contrary increases continuously. This fact has been constructively proved in numerous publications and monographs [1, 2]. The bases of the theory of numbers are prime numbers [3].

Despite the high level of research in the theory of prime numbers to date, the laws of the formation of primes remain largely unexplored. The infinity of the set of primes is easy to prove [2, 3]. The law of distribution of primes in the set of natural numbers is established quite accurately [2], but the dynamics of the formation of prime numbers, and consequently of the constitutive numbers, is still unknown.

The properties of rational, algebraic, transcendental numbers are largely determined by the properties of primes [4]. One of the subspecies of the study of the dynamics of the formation of prime numbers is based on the construction of the classification of prime numbers with accounting for the dynamic processes of class formation. The selection of classes is based on a functional approach. On the basis of the theory of functional analysis, each class defined by the property AA is given by a computable function $f(A)$ which defines the property of the formation of prime numbers allocated in a certain ordered sequence. The set of such prime numbers forms the class P_A, and the $P_{\overline{A}}$ is an additional class that includes all prime numbers that do not have this distinguished property. Such a classification can be called Boolean. Currently, more than a hundred different Boolean classifications have been singled out [5, 6]. Classifications exist, but so far with each of these classifications there are many unresolved problems, practically for none of them there is a proof that the number of prime numbers in a given class is infinite or if it is finite then there is no estimate of their number. There are classes in which only a finite set of elements is known. These are the numbers of Fermat, Mersenne, Wagstaff, Sophie-Germain and other types of primes [2, 3].

For almost all known classes, the question is whether the set of primes in these classes is infinite. The answer to this question is of fundamental importance for the modern theory of numbers as a whole. If in some class there is a finite set of elements, this means that there exists a dynamic property of prime numbers, which after some simple number p can not arise for a certain reason. Fermat numbers of the form $p = 2^{2^n} + 1$, where n is a natural number, according to the Gauss theory, confirms his hypothesis that the correct p - square can only be constructed using a compass and a ruler only when p is a prime number. The answer to this question is important within the mathematical meaning.

Simple Mersenne numbers of the form $2^p - 1$, where p is a prime number, on the basis of the Lucas-Lemer test allows us to simply verify its simplicity. This is the way to find the largest known prime numbers. So the fiftieth prime Mersenne number equal to the value of $2^{74207281} - 1$ was received in early 2016. Mersenne's grand prime numbers have not yet been received, although the premium for this result exceeds $ 100,000. This result is worth it, since it carries information about the formation of prime numbers according to a certain law.

For a functional approach to the construction of classes P_A prime numbers is characteristic that the dynamics of distribution, as a rule, nothing is known. It is possible that the classification of P_A will be a source of new information on the dynamics of the formation of primes of this type. At present, no internal classification has been studied for any of the additional classes $P_{\bar{A}}$.

The considered approach to the construction of classes of primes is of great importance for the study of the properties of prime numbers at the general mathematical level. The applied significance of such classes of primes is much less pronounced. To study the dynamics of the formation of classes P_A, probabilistic methods are applied [7]. To do this, on the set of all prime numbers, define a discrete probability space (Ω, F, P), where Ω is assumed to be equal to the set of all primes P. The probability measure P^* is defined as $P^*(P_A) > 0$ for any $p \in P_A$. If for P_A the measure $P^*(P_A) > 0$ for any of its subsets as p tends to infinity, then this proves that the class P_A contains infinitely many prime numbers.

A probabilistic approach of this kind is based on the distribution of prime numbers $\pi(x) \sim \frac{x}{\log x}$, where x is a natural number, $\pi(x)$ the number of prime numbers is less than x or equal to x. The specification of the measure P^* on the set P_A is pseudo-random, since the measure P^* is chosen, as a rule, by different deterministic pseudo-random methods [7]. The use of a pseudo-random measure should be constructively justified. This is possible only when the dynamics of this class P_A is taken into account fairly correctly. To achieve the necessary level of constructiveness, provided that there is enough complete information about the laws of formation of each class P_A. In all cases it is necessary to prove in parallel the correctness of the introduction of the measure P^* [7].

Another approach to investigating the dynamics of prime numbers is based on the theory of residues with respect to an arbitrary natural number $n \geq 2$. Obviously, the fractions of positive integers with $\{0, ... m-1\}$ residues for any $m \in N$ and $m \geq 2$ are equal to $\frac{1}{m}$. This statement can not be simply transferred to the set of primes P. The reason is not the ideal equal-number law for the formation of prime numbers. In [8] it is proved that the assertion

$$\pi(x,4,1) - \pi(x,4,3) = \Omega_{\pm}\left(\frac{x^{\frac{1}{2}}}{\log x} \log\log\log x\right),$$

where $\Omega_{\pm}$ is a constant which, at + shows that $\pi(x,4,1)$ tends to $\frac{1}{2}$ from above, and Ω_{-}, that $\pi(x,4,3)$ tends from below. In this expression, $\pi(x,4,1)$ and $\pi(x,4,3)$ are respectively the number of prime numbers for which the residues modulo 4 are 1 and 3, respectively [8].

Similarly, [9] is devoted to the proof of the assertion $\pi(x,24,1) \cong \pi(x,24,l) \cong \frac{1}{8}$ for l such that $GCD(24,l) = 1$ and $1 < l < 24$.

There are other works of this type. They confirm that, at the level of the theory of residues, there is also a special form of the uniform law of the formation of prime numbers.

At present, a high level of research has been achieved by the theory of deterministic dynamical systems defined by functions $g(x)$ having iterative fixed points of the form when $g^{(n)}(x_0) = x_0$, where n is the number of iterations $x_{m+1} = g(x_m)$.

In this paper, we aim to investigate the possibility of constructing a classification of prime numbers on the basis of information on the structure of cycles and their lengths on the set of primes for a class of mappings based on the theory of residues [2, 3]. From a large variety of possible mappings of the set of natural numbers into itself, a symmetric mapping is called a tent map.

Simulation of the dynamics of prime numbers based on the theory of the primitive root.

Initially, to study the dynamics of the formation of prime numbers, we used the symmetric mapping "tent1", defined by the expression:

$$x_{n+1} = \begin{cases} 2x_n, & \text{если} \quad x_n < \frac{1}{4} \\ 1 - 2x_n, & \text{если} \quad x_n \geq \frac{1}{4} \end{cases} \quad (1)$$

The graphical representation of the given map on the interval $(0,1)$ is shown in Fig. 1.

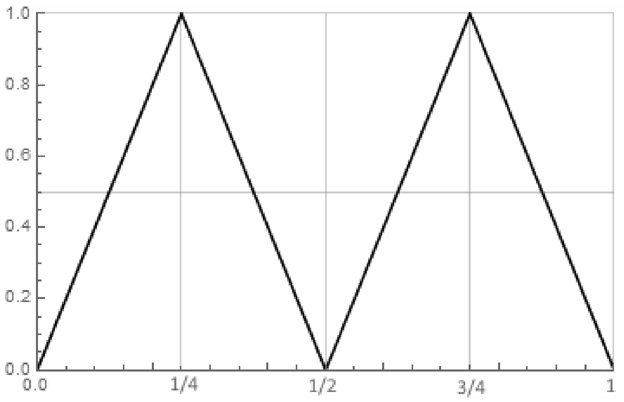

Fig. 1 Graph of the display "tent1"

The reason for this choice were the results obtained in [10] in the theory of dynamical systems. Since for $x_0 = \frac{1}{7}$ the length of the cycle of wound 3, then, according to the Sharkovsky theorem [10], there exist iterative cycles of any length. Since for large $n = 2m+1$, $\frac{1}{(2m+1)}$ values are rounded up in the iteration process, which leads to inaccurate completion of iterative cycles. To eliminate errors of this kind, the mapping (1) was transformed into an integer form

$$x_{n+1} = \begin{cases} 2x_n, & если \quad 4x_n < 2n+1, \\ (2n+1) - 2x_n, & если \quad 4x_n \geq 2n+1 \end{cases} \quad (2)$$

For any value of $n \in N$, the initial value x_0 of the iteration cycle is set equal to 1. For each number $m = 2n+1$, the length of the cycle $l(m)$ was determined. In the first stage of, $(m = 2n+1, l(m))$ pairs were computed for the first 100,000 odd natural numbers, and hence for all primes in this interval. Even numbers have not been considered, since the mapping on them given mapping does not have iterative fixed points.

Analysis of the iterative cycles of fixed points made it possible to immediately extract those $m = 2n+1$ numbers for which the cycle length is n. The assertion was proved.

Statement. If the cycle length is equal to $2n+1$ in the "tent1" mapping for the number, then the given number is simple.

It follows from the proof that this permutation cycle without repetitions on the set $(1,...,n)$ is given in Figure 2. By the Sharkovsky theorem [10] with $n \to \infty$, the iteration cycle length tends to ∞. An analysis of the evidence made it possible to formulate the assumption that this is a pseudo-random sequence. This became the basis for deepening further studies of such iteration cycles.

This intermediate variant necessitated the deepening of the analysis of the entire set of pairs $(m = 2n+1, l(m))$ on the selected interval $(0,100000)$. A graphic representation of this set of pairs is shown in Figure 2.

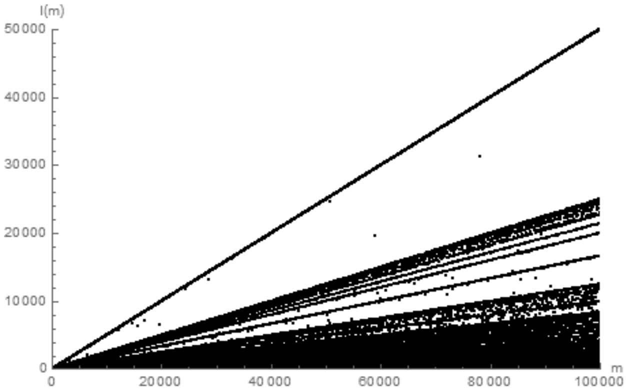

Fig. 2 Graph of pairs $(m = 2n+1, l(m))$

An analysis of the results of this computer simulation process led to the conclusion that it is necessary to separate simple and composite odd numbers. Such a solution is connected with the fact that compound odd numbers in this paper are not the object of investigation. For prime numbers $p \in P$ and corresponding pairs $(p = 2n+1, l(p))$, computer simulation data were obtained, which are presented in Figure 3.

Particular attention was paid to the availability of clear linear structures for the distribution of prime numbers, depending on the corresponding cycle lengths of the given map.

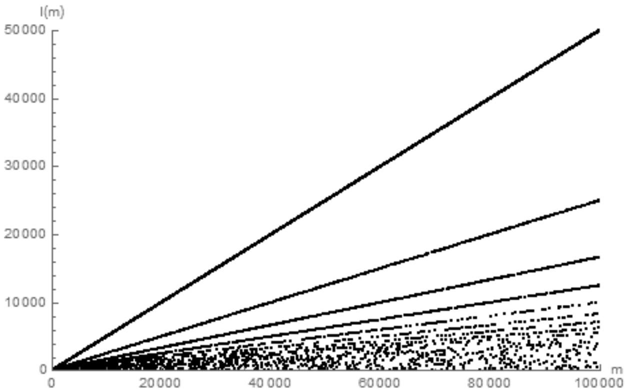

Fig. 3 Graph of the distribution of cycles for $(p = 2n+1, l(p))$

The analysis of the intermediate results obtained made us pay attention to the studies carried out by the project of the famous mathematician Sloan in the On-line Encyclopedia Integer Sequences [5]. The object of attention was the work of OEIS A082654. The authors of the work considered the length of the cycle as an integer description of prime numbers. Problems in the classification of primes were not considered. We have established that in this case, according to Fermat's theorem [2], for any prime number p, $p-1$ is always divisible by $l(p)$. The value of the particular $p-1$ and the length of the cycle became the basis for the dynamics of the formation of prime numbers.

In this paper, the authors set out to characterize the entire set of prime numbers by iterative cycles of fixed points given by a mapping: given $p \in P$ and $x_0 = 0$

$$x_{n+1} = \begin{cases} 4 \cdot x_n, & если \quad x_n < p, \\ 4 \cdot x_n \equiv l(\mathrm{mod}\, p) \end{cases} \quad (3)$$

The integer display "tent1" is executed for large values of $p = 2n+1$ slowly, while in the Wolfram Mathematica system the display (3) is executed very quickly. Moreover, the analysis of Fig. 3 will allow to draw a conclusion that essentially the method of construction of classification of prime numbers by values of lengths of cycles is received.

On the basis of Fermat's theory and properties of the primitive root [2], it is proved that all prime numbers are divided into classes. If for p the cycle length is $l(p)$ then $(p-1)/l(p)$ is the slope of the straight line advising all prime numbers with a given angle of inclination. It was proved that all prime numbers form $P_2, P_4, ..., P_{2k}, ...$ classes by tangents of slope angles equal $1/2k$ at $k = 1, ..., m, ...$.

The implementation of the mapping (3) in the Wolfram Mathematica system allowed to significantly increase the speed of construction of iterative cycles of fixed points, and hence the volume of processed prime numbers in the process of computer simulation of the dynamics of the formation of prime numbers. As a result, an interval model of dynamics development was implemented. $(a_{n+1}, a_n) \in N$ intervals were sequentially allocated, which for each n value contained 500,000 prime numbers.

Interval computer simulation of the dynamics of the formation of prime numbers in the system Wolfram Mathematica and MS Excel.

To study the dynamics of the formation of prime numbers, we can consider two models for the formation of primes on the intervals defined on the set N. The first approach to constructing intervals is based on the principle of arithmetic progression. The interval (a_n, a_{n+1}) is constructed by the trivial feature $a_{n+1} = a_n + d$, where $a_0 = 1$, and d is the difference in the progression. Similar to $d = 10^7$. On the interval (a_n, a_{n+1}) we find all prime numbers and investigate their pattern of formation, i.e. Their dynamics taking into account the dynamics of prime numbers in the previous interval. At the same time, the basis was the assumption that in this way it will be possible to find the fundamental regularities in the formation of prime numbers. The known law of distribution of prime numbers [2] $\pi(x) \cong \frac{x}{\log x}$, where x is an arbitrary natural number, $\pi(x)$ the number of prime numbers less than or equal to x, will be refined in the process of its computer simulation.

However, since the maximum distance between prime numbers in the (a_n, a_{n+1}) interval will grow with increasing n, and the structure of the clusters will vary, then starting from a certain value of n, the set of primes of the interval (a_n, a_{n+1}) will not reflect the dynamics of the formation of prime numbers. It is necessary to change d according to a certain law. Of course, this fact does not mean that such an approach without prospects. A certain model of the change in d is needed. For example, taking $\pi(x) \cong \frac{x}{\log x}$ into account, it would make sense to change d_n in conjunction with a_n so that there are a number of simple numbers on the interval, for example $\pi(a_n + 1) - \pi(a_n) = 500000$ for all n. Such interval strategy allows to assert that more number of important regularities of the formation of prime numbers will be available. Although it is possible that 500,000 for some problems of analysis of the dynamics of the formation of prime numbers may not be sufficient to assess the stability of the estimated parameters of the dynamics of the formation of prime numbers. This can refer to the prime numbers of Fermat, Mersenne, Wagstaff, and their various generalizations.

In particular, for generalized Sophie-Germain prime numbers in the form $p^* = 2^l \cdot p + 1$, where p^* and p are prime numbers and l is an arbitrary natural number, there are obvious problems for large l. They can be overcome by the same principle by increasing according to a certain law. It should be noted that when analyzing the process of forming prime numbers, it is necessary to take into account and investigate the decomposition into simple factors $p-1$ and $p+1$. This is important because, for any prime number p, the decomposition of $p-1$ into simple factors is very important for several reasons. The properties of $p-1$ define p. The question is to what extent the factorization of $p-1$ can be judged on the properties of p. For example, what properties should $p-1$ have for p to be a prime number belonging to one of the classes $P_2, P_4, ..., P_{2k}, ...$.

Discussion of the two models of the interval formation (a_n, a_{n+1}) testifies to an important fact. Intervals form a hierarchical structure with increasing complexity. It is obvious that on each new interval there appear prime numbers with new properties, a set of primes with new dynamic laws of their formation of an additional infinite expansion, ie, The system of intervals develops.

In any interval (a_{n+1}, a_n), each prime number was represented by a set of parameters. The estimated parameters of a prime number were: the number of a prime number in the interval, the value of a prime number p, the length of a cycle, the prime number class p, the decomposition of $p-1$ into simple factors, the decomposition of $p+1$ into simple factors, the values of the functions defining the properties of the prime to be analyzed. Each function implemented in Excel computes certain properties of the considered prime number.

In particular, the number of simple numbers in each of the $P_2, P_4, ..., P_{2k}, ...$ classes on each interval was calculated. Table 1 lists the values of the number of elements in the first ten classes, which are more than 0.91 of all prime numbers. The most stable dynamics of the formation of classes P_2, P_4, P_6, less stable for classes P_{16}, P_{18}, P_{20}. This fact is easily explained by the fact that primes from the latter classes are much rarer in the entire set of primes. When the length of the modeling interval is increased, the same level of stability is achieved.

Table 1

Class distribution by interval systems

Interval, Million	P2	P4	P6	P8	P10	P12	P14	P16	P18	P20
0.0 - 0,5	280631	46805	49832	35060	14176	8325	6662	8717	5507	2387
0.5 - 1,0	280598	46781	49941	35098	14188	8322	6610	8743	5556	2351
1.0 - 1,5	280371	46784	49732	35043	14200	8255	6724	8838	5675	2343
1.5 - 2,0	280216	46680	49802	35374	14186	8243	6853	8726	5391	2324
2.0 - 2,5	280681	46775	49938	34864	14251	8309	6656	8924	5573	2411
2.5 - 3,0	280328	46625	49748	35292	14349	8408	6733	8687	5519	2333
3.0 - 3,5	280900	46692	49867	34960	14090	8326	6792	8741	5424	2319
3.5 - 4,0	280397	47025	49904	34785	14157	8315	6773	8896	5560	2358
4.0 - 4,5	280329	46855	49977	35291	14150	8167	6555	8898	5505	2361
4.5 - 5,0	280196	46782	49653	35130	14359	8347	6697	8755	5652	2333
5.0 - 5,5	280376	46664	49971	34963	14139	8254	6585	8823	5544	2412
5.5 - 6,0	280331	46779	49905	35057	14096	8244	6819	8789	5569	2391
6.0 - 6,5	280491	46752	49912	35152	14209	8235	6545	8768	5626	2314
6.5 - 7,0	280653	46938	49850	34618	13991	8427	6670	8860	5594	2383
7.0 - 7,5	280456	46525	49619	35188	14006	8345	6777	8837	5535	2405
7.5 - 8,0	280523	46812	49833	34969	14110	8315	6687	8741	5642	2335
8.0 - 8,5	280794	46568	49907	35098	14059	8250	6627	8867	5654	2348
8.5 - 9,0	280373	46759	49705	35193	14082	8344	6822	8664	5508	2381
9.0 - 9,5	280228	46975	49810	34961	14234	8282	6824	8772	5574	2401
9.5 – 10.0	280547	46740	49839	35042	14137	8366	6576	8744	5483	2413

It follows from the table that the dynamics of classes on the system of intervals that has been carried out has a stable law. On the basis of number-theoretic considerations, it is proved that such a law of the formation of primes takes place for the whole set of primes.

Classes of residues

$$|\pi(x,m,l_1)| \cong |\pi(x,m,l_2)| \cong ... \cong |\pi(x,m,l_k)| \cong \frac{1}{k}$$

which consist of the set of all prime numbers $\leq x$ whose residue modulo m is equal to l by many authors is considered as random events of probability which converge to $\frac{1}{k}$ [8, 9]. Interval modeling of the dynamics of prime numbers allows us to assert that it is more correct to consider the residue classes as equidistant subsets of the set of primes, that is, The following theorem holds:

Теорема 1. Для любого m

$$|\pi(x,m,l_1)| \cong |\pi(x,m,l_2)| \cong ... \cong |\pi(x,m,l_k)| \cong \frac{1}{k}$$

where $1 \leq l_1,...,l_k < m$ and are relatively prime to m.

This theorem in this case is confirmed by the results of computer simulation. The proof of this theorem by means of group theory and number theory is beyond the scope of this paper. From the same considerations follows the validity of the following assertion:

Statement. The fraction of prime numbers of the class P_2 in the set of all primes is $m \cong 0.5608...$

The validity of this statement follows from Table 1. On the basis of the same computer simulation on the entire sequence of intervals containing 500,000 prime numbers, this estimate is stable. However, this fact has not been proved theoretically.

Similar statements are formulated for all classes P_{2k} for $k \geq 2 \in N$. With increasing k, the fraction tends to zero.

This statement does not apply to the prime numbers of Fermat, Mersenne, Wagstaff, and some of their generalizations. However, the theorem is true.

Theorem 2. The set of primes of the form

$$\left\{p^* = 2^{2^n} \cdot p + 1 \mid p \in P\right\}$$

in which for any $n > 0$ there are infinitely many prime numbers p^*, such that they form an infinite sequence.

From this theorem it does not follow that the set of Mersenne prime numbers, Fermat is infinite, but reflects one of the models for the formation of prime numbers.

Theorem 3. The set of primes of the form

$$p^* = 2p + 1$$

where p^* and $p \in P$, are infinite; The set of primes Sophie-Germain is infinite.

Moreover, the generalized theorem is true.

Theorem 4. The set of primes for any $l \geq 1$ of the form $p^* = 2^l p + 1$, where p^* and $p \in P$ is infinite.

In this paper, the validity of these theories is justified by the results of computer simulation of the dynamics of the formation of prime numbers. The rigorous mathematical proof of Theorems 2, 3, and 4 goes beyond the scope of this paper.

Note that all classes of primes are distributed on linear functions of the form:

$$m = r \cdot \frac{1}{2k} - c, \ k \geq 1$$

where $\frac{1}{2k}$ is the slope of the straight line corresponding to class P_{2k} with the cycle length m. Constant $c \to 0$ with $k \to \infty$. In particular, a straight line of class P_2 corresponds only to prime numbers, this can not be asserted with respect to other classes.

Conclusions

The constructed computer model of the dynamics of the formation of primes implies the validity of the above statements and theorems. A constructive mathematical proof of these theorems and statements is carried out by methods of number theory, group theory, combinatorics, and abstract algebra [1, 2, 3].

A complete classification of prime numbers is constructed and a computer model for studying the dynamics of the formation of all classes is implemented.

On the basis of the constructed method of interval modeling of the dynamics of the formation of prime numbers, it is shown that the number of both Sophie-Germain prime numbers and generalized infinitely many.

References

1. Rogers, H. (1967). Theory of Recursive functions and Effective Computability. New York: McGraw-Hill Book Company, p. 623.
2. Manin, Y. and Panchishkin, A. (2009). Introduction to the modern theory of numbers. Moscow: MTSNMO, p 551.

3. Crandall, R. and Pomerance, C. (2005). Prime Numbers A Computational Perspective. Portland: Springer, p. 664.

4. Shidlovsky, A. (1987). Transcendental numbers. Moscow: Nauka, p. 447.

5. Sloane, N. J. A. and Plouffe S. (1995). The Encyclopedia of Integer Sequences. San Diego: Academic Press, p. 680.

6. Wikipedia.org, (2013). List of prime numbers. [online] Available at: https://wikipedia.org/wiki/List_of_prime_numbers/ [Accessed 14 May 2017].

7. Grenander, U.(1963). Probabilities in Algebraic Structures, London: ALMAVIST and WIKSELL, p. 275.

8. De L'eglise, M. and Dusart, P. and Roblot, X-F. (2004). Counting primes in residue classes, Mathematics of Computation, Volume 73, Number 247, pp. 1565-1575.

9. Meshkoff, V. (2015). Prime Numbers Classification with Linear and Quadratic Forms, Universal Journal of Applied Mathematics 3(3), pp. 35-39.

10. Sharkovsky, A. (2013). Attractors of trajectories and their basins. Kiev: Naukova Dumka, p. 319.

ЭФФЕКТИВНАЯ ВЫЧИСЛИМОСТЬ СТРУКТУРЫ ДИНАМИЧЕСКИХ ПРОЦЕССОВ ФОРМИРОВАНИЯ ПРОСТЫХ ЧИСЕЛ

Г.Н. Востров, Р.Ю. Опята
Одесский национальный политехнический университет

Аннотация. *Разработан интервальный метод исследования динамики формирования простых чисел. На основе теоремы Ферма и теоремы вычетов создан метод анализа свойств простых чисел по величине длины итерационного цикла неподвижных точек определяемыми простыми числами. Построена классификация простых чисел. Приведены результаты компьютерного моделирования процессов формирования простых чисел с учетом свойств классификации.*

Ключевые слова: *Динамическая система, Простые числа, Теория вычетов, Теорема Ферма, Классы простых чисел, Структура классов, Теоремы о свойствах простых чисел, Интервальный метод компьютерного моделирования.*

Received 14.05.2017

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 Георгий Николаевич, кандидат технических наук, доцент кафедры прикладной математики и информационных технологий Одесского национального политехнического университета. Просп. Шевченко, 1, Одесса, Украина.

ORCID ID: 0000-0003-3856-5392

Roman Opiata, PhD student of the Department of Applied Mathematics and Information Technologies, Odessa National Polytechnic University. Shevchenko ave., 1, Odessa, Ukraine.
E-mail: roma.opyata@gmail.com, mob. +38095249753

Опята Роман Юрьевич, аспирант кафедры прикладной математики и информационных технологий Одесского национального политехнического университета. Просп. Шевченко, 1, Одесса, Украина.

ORCID ID: 0000-0001-5806-9615