# COMPUTER MODELING OF THE PROCESSES OF DEVELOPMENT OF INFORMATION TECHNOLOGY IN DYNAMIC PROCESSES OF THE FORMATION OF CLASSES OF THE GENERALIZED ARTIN'S HYPOTHESIS

**Vostrov G., Opiata R.**

*Abstract. The relationship between the processes of formation of classes of primes in the generalized Artin's hypothesis and the theory of information, and as a consequence, information technology, is investigated.*

*It is proved that probabilistic methods of the theory of information and information technologies are the basis for constructing computer models of classes of primes in accordance with the generalized Artin's hypothesis. Methods for calculating the Artin's constants are developed and the convergence of the estimates of the constants in probability to limit values is established. The foundations of a number-theoretic analysis of Artin's constants and related classes are created.*

*Keywords. Generalized Artin's classes, Artin's constants, class probabilities, stability of estimates of the Artin's constants? convergence in probability.*

## INTRODUCTION

The solution of many problems in such applied areas as electronics, electrical engineering, modeling of complex, both deterministic and stochastic, nonlinear dynamic systems, information technology and many other applied areas of human activity, depends on solving a significant number of mathematical problems that have not yet been solved. Artin's hypothesis of primitive roots is one of these fundamental mathematical problems. For almost a century, it remains unresolved. The solution to Artin's problem is important for research in such applied areas as the creation of effective methods of protecting information using cryptographic methods, the development of pseudo-random number generators, the modeling of dynamic processes in stock markets, and the construction of advanced algorithms for testing software products of high complexity. One of the options for cryptographic information protection is the discrete logarithm method. The development of the Monte Carlo method and its application in the theory of modeling complex systems depends on the creation of effective generators of pseudo random numbers given by the laws of probability distribution. The construction of such generators is especially important in the methods of testing software applications. Modeling processes in modern stock markets is not possible without high-quality random number generators with a given distribution law [1-3]. Another urgent applied problem is the modeling of self-organizing nonlinear dynamic systems, which are commonly called synergetics, taking into account the deep modeling of the phenomenon of self-organization in

complex systems consisting of transition sequences from one phase state to another using random number generators with a given probability distribution law [3] . The numerical sequences of iterative models of cyclic fixed points of dynamical systems are determined by the properties of the primes with which they are represented. In this case, the question always arises: what distribution laws obey prime numbers. Riemann in 1869 proposed the function:

$$\xi(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}=\prod_{p\in P}\left(1+\frac{1}{p^s}+\frac{1}{p^{2s}}+...\right)$$

where $s$ is a complex variable, $P$ is the set of all primes [3,4]. The function is called the Riemann's zeta function. Concerning this Riemann's function, a hypothesis was formed according to which all non-trivial zeros of this function are on line $1/2+iy$, where $i=\sqrt{-1}$ and $y\in R$. It follows that all primes lie on this line since $y$ – takes values from a set that includes all primes $P$. Moreover, for any prime number $p$ $\xi(1/2+ip)=0$. In essence, this was the first attempt to find the law of the distribution of primes. So far, the hypothesis has not been proved. Note that any function $f(s)$ that is defined in the complex space $C$, and therefore $s\in C$, is usually called analytic.

The study of the Riemann's analytic zeta function has been done by many mathematicians. In particular, it was proved that $\xi(-2)=1+2^2+3^2+...+k^2+...=0$ is the value of $s$ is a trivial zero. This paradoxical fact for applicants does not contradict the theory of analytic functions, but from the point of view of the distribution of primes it does not give an adequate description of the distribution of primes on the number line $R$ or $Q$ or $Z$. Starting with the works of Fermat, Euler, Dirichlet, Gauss, Chebyshev [3,4], systematic attempts were made to establish their distribution law in two-dimensional real space [4]. In 1896, independently, Adamard and Valle Poussin proved that equality is true:

$$\pi(x)=\int_2^x\frac{dt}{\ln t}+O\left(x\cdot e^{-c\sqrt{\ln x}}\right) \qquad (1)$$

where $\pi(x)$ is the number of primes $p\le x$, and the first term in the form of a logarithmic smooth function determines the logarithmic law of the distribution of primes in approximate form, and the second term is the remainder term that describe the inconsistency of the step function $\pi(x)$ when it is approximated by a logarithmic function. In many studies, an analysis of the residual term is given, it is proved that if it is considered as a function of $x$, it has a fractal nature [3,8].

It is known that the distance between primes increases, and the relation:

$$p_{n+1} - p_n > \varepsilon \frac{\ln(n) \cdot \ln\ln(n) \cdot \ln\ln\ln\ln(n)}{(\ln\ln\ln(n))^2} \quad (2)$$

where $n$ is the prime number in the ordered whole set of primes [5,6], a constant that is generally difficult to calculate. The proof of this relation does not mean at all that absolutely complete information on the distribution of primes in the system of the logarithmic distribution law has been obtained.

It should be noted that the Riemann's hypothesis, numerous studies of its trivial and non-trivial zeros, the proof of the logarithmic law of the distribution of primes were a source of new information that is fundamental to the modern world, on the one hand, and on the other, these results led to the creation of new information technologies. One of the areas of deepening information technology was the formulation in 1927 by the French mathematician Artin's of a hypothesis about the primitive roots of primes $p \in P$, and accordingly the primitive roots of residue groups $(Z/pZ)^*$ modulo prime $p$. Consider the definition of the primitive root of a prime number $p$. The numbers $a \neq 1$, $a \neq k^2$ is the primitive (antiderivative) root of the number $p$, if the following relations are true:

$$\begin{cases} a^{p-1} \equiv 1 (\mathrm{mod}\ p) \\ a^{\frac{p-1}{n}} \not\equiv 1 (\mathrm{mod}\ p), \quad n > 1 \end{cases} \quad (3)$$

The $n$ is the divisor of $p - 1 = \prod_{i=1}^{k} p_i^{\alpha_i}$.

Given the definition of a primitive root, Artin's hypothesis is:

$$\pi(x, a) = c(a) \cdot \pi(x) \quad (4)$$

where $\pi(x, a)$ is the number of primes $p$ less than or equal to $x$, for which $a \neq \pm 1$ and $a \neq k$ are according to (1) their primitive roots, $c(a)$ is the Artin's constant. More precisely, this hypothesis should be presented as follows:

$$\begin{cases} \pi(x, a) = c(a, x) \cdot \pi(x), \\ \lim\limits_{x \to \infty} c(a, x) = c(a) \end{cases} \quad (5)$$

But then $c(a,x)=\frac{\pi(x)}{\pi(x,a,x)}$ and in probability converges to $c(a)$, and therefore has a probability theory interpretation: $c(a)$ is the probability of choosing from the set $P$ a prime number $p$ such that $a$ is its primitive root. Note that the first relation in (1) is always satisfied if $a$ and $p$ are coprime numbers according to Fermat's theory [3].

It should be noted that Artin's proposed his ratings for $c(a)$ at $a=2$. But as proved by Hooley [5], these estimates are not true. He also proved the validity of the relation:

$$\pi(x,2)=\frac{c(2)\cdot x}{\ln x}+O\left(x\frac{\ln\ln(x)}{(\ln(x))^2}\right) \qquad (6)$$

at the same time $c(2)=\prod_{p\in P}\left(1-\frac{1}{p(p-1)}\right)$ and an assessment of the value of $c(2)=0{,}373955813\ldots$ As will be shown later, this estimate is true only with the accuracy of the first two decimal places. This can be easily explained by a very simple consideration. The expression for $c(2)$ proposed in (4) depends on all primes, but this is not true because $a=2$ is not a primitive root for all primes $p\in P$. The values of the constants $c(a)$ for $a>2$ and $a\neq k^2$ were not presented in more than one scientific article.

It should be noted that any number $a>1$ and coprime to $p$ is the basis for considering the recursive function $f(x)\equiv a\cdot x(\mathrm{mod}\ p)$, which leads to a recursive iterative sequence.

$$f(x_0=1)=1,\ f(x_{n+1})=x_{n+1}\equiv ax_n(\mathrm{mod}\ p) \qquad (7)$$

According to Fermat's theorem [4], if a is not a primitive root for $p$, then the process of recursive computations will continue for such $m$ that equality $f(x_n=m)\equiv x_{m-1}\cdot a(\mathrm{mod}\ p)=1$ is achieved i.e.

$$a^m\equiv t(\mathrm{mod}\ p)\ \text{и}\ m<p-1 \qquad (8)$$

From Fermat's theorem and the properties of the group $(Z/pZ)^*$ residues modulo $p$, it follows that in this case $a$ is the primitive (antiderivative) root of some subgroup of the group $(Z/pZ)^*$. Moreover, $m$ is the order of this subgroup, which is usually denoted by $card_a(p)$, the

number of adjacency classes for this subgroup is denoted by $ind_a(p)$. According to the cyclic group theorem $(Z/pZ)^*$, the equality:

$$p-1 = card_a(p) \cdot ind_a(p) \quad (9)$$

The validity of equality (6) follows also from Fermat's theorem. In conclusion, it should be noted that from the relations (5) and (6) the validity of the equation follows:

$$c \equiv a^x (\mathrm{mod}\ p) \quad (10)$$

No more complicated analysis of this equation leads to the consideration of four options for its solution: Given $a, x, p$ - calculate $c$; Given $c, a, p$ - calculate $x$; Given $c, x, p$ - calculate $a$; Given $c, a, x$ - calculate $p$;

The first equation is solved using recursion (7), (8). The second equation is the formulation of the discrete logarithm problem. The variable $p$ can also be a pseudo prime number equal to $p^k$ or equal to $2^p$, as noted in [3], this problem in the general case may be algorithmically unsolvable.

In the third and fourth cases, the solution of such equations is a problem of extreme complexity. There are no publications on this subject.

From the above analysis it follows that equation (5) allows us to study the Artin's hypothesis from a more general point of view, when any natural number $a > 1$ and it can be used as a classifier of the set of all primes in the magnitude of $ind_a(p)$, which is the object of further research. As will be established, Artin's hypothesis of primitive roots will be a frequent case of its more general formulation.

**MODELING THE PROCESSES OF GENERATING DYNAMIC INFORMATION ABOUT THE STRUCTURE OF CLASSES OF PRIMES ON A GIVEN BASIS**

Now we return to the logarithmic law of the distribution of primes [1-4] in order to pay attention to the fact that the above equality does not provide comprehensive information about the structure of spaces between primes. Obviously, with increasing prime numbers, the gaps between them increase quite significantly. From relation (2) it is completely impossible to conclude by what laws the distance between the gaps changes, how often the dips appear statistically and most importantly how the structure of the decomposition of p-1 numbers into simple factors changes. It is especially important to have information about the distribution of smooth primes [3]. This information is especially important when solving the discrete logarithm problem and applying algorithms for solving it in the modern coding theory

and in modern cryptographic methods of information protection. As shown in [7], it is practically impossible to find smooth large prime numbers. It follows that it is of considerable interest to establish the laws of distribution of primes not only with respect to their primitive roots, but to the roots of subgroups of the residue group modulo a prime number. Artin's hypothesis does not imply such detailed studies. Moreover, it is necessary to find the laws of the relationship between the laws of the distribution of primes in sets corresponding to various primitive roots and roots of subgroups. Such tasks were not considered at all.

The second circumstance is that simultaneously with this fact, the dynamics of change in $O\left(x \cdot e^{-\frac{c}{2}\sqrt{\ln x}}\right)$ [8] is investigated. In [3, 4], the entropy estimate of this estimate was obtained and it was proved that it has a fractal character. These facts are the basis for the formation of proposals on the need to study other models of the distribution of prime numbers. Another problem related to the distribution of primes appeared in 1927, when the famous mathematician Artin's formed a hypothesis about the distribution of primes for which the natural number $a > 1$ is given is its primitive root [1,5].

In addition, it is generally accepted, even at the present time, that it makes sense to study it more fundamentally. The first attempt was made by D. Zagier [8], but not completed. The results obtained by the author confirm the very complex fractal behavior of this component. It follows that it is necessary to significantly improve the study of the depth of classification of primes, taking into account all models for the formation of classes of primes for any given basis $a > 1$. Further more detailed studies of this component confirm that although the logarithmic distribution law is fulfilled, nevertheless, complete information on the dynamic properties of primes and their relationships with their primitive roots remains poorly studied. In the future we will consider any values of the base and large units.

According to Artin's hypothesis [5], the set of such primes has the distribution law $\pi(x,a)$ as an expression:

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

where $\pi(x)$ is the distribution of prime numbers, and $c(a)$ is a constant dependent on $a$. Until now, despite numerous studies, this hypothesis has not been resolved. However, it is not known if this is true for any $a$ values. If the hypothesis is correct, then the question remains how to estimate the constant $c(a)$ for each concrete $a$ and which properties of the number $a$ influence its value. Answers to these questions are still missing. In works [3, 5] a detailed analysis of all the results of research in the field of solving the Artin's

hypothesis is given. It should be noted that the proof of Artin's hypothesis is important both from a theoretical point of view in number theory, and from an applied rhenium point, because it's positive solution is important in cryptography, coding theory, and the theory of dynamical systems. In [6], a generalized Artin's hypothesis was formed for any $a > 1$, i.e. and at the same time $a$ may not be a primitive root. According to Artin's generalized theory, the following equality is true:

$$\pi(x,a,i) = c(a,i)\cdot\pi(x) \tag{11}$$

where $a > 1$, $i$ – is the index of the subgroup of the group $(Z/pZ)^*$ of primes in the classification of prime numbers generated by the numbers $a$, $c(a,i)$ is a constant. According to the classification built in [6]:

$$P(a,i) = \{p \in P \mid (p-1)/card_a(p) = i\} \tag{12}$$

where $card_a(p)$ is the length of the dynamic recursion $x_{n+1} \equiv ax_n (\mathrm{mod}\ p)$ at $x_0 = 1$, $P$ is the set of all primes.

It is not difficult to show that for any $a > 1$ the equality:

$$\sum_{i=1}^{\infty} c(a,i) = 1 \tag{13}$$

This means that primes are evenly distributed in classes $P(a,i)$ for any $a$. By uniformity is meant that within each class of primes $P(a,i)$ a logarithmic law of the distribution of primes is preserved. The constant $c(a,i)$ determines the measure of puncturing prime numbers, based on the value $a$. If $i = 1$ then $a$ is the primitive root of all primes $P(a,1)$. For an arbitrary natural number $x$, the equality

$$\pi(x,a,i) = c(a,i,x)\cdot\pi(x)$$

Moreover, if $x \to \infty$, then $c(a,i,x)$ tends to the limit value $c(a,i)$. If we put $i = 1$ then $c(a,1)$ will be Artin's constant for primitive roots. In this case $a \neq \pm 1$, and $a \neq k^2$ for none $k \in N$. This is true according to Fermat's theorem [3, 4]. Wherein, $a$ is the primitive root of the group of residues $(Z/pZ)^*$ for any $p \in P$ such that $P(a,1) = \{p \in P \mid (p-1)/card_a(p) = 1\}$. It is important to investigate the classes of primes $P(a,i)$ for $i > 1$ since in this case the positive integer a will be the primitive root for the subgroups of the group $(Z/pZ)^*$ with the index defined by the relations:

$$P(a,i)=\{p\mid(p-1)/card_a(p)=ind_a(p)\}$$

where $ind_a(p)=i$ is the index of the subgroup of $(Z/pZ)^*$. The classes of primes $P(a,i)$ have not yet been studied and the distribution of primes in these classes is not known. In [1], an assumption was made that $P(a,i)$ at $i>1$ is proportional to $P(a,1)$ with a factor of $1/i^2$. Since $i>1$ is considered, in this case it is important to know the distribution of prime numbers for the value $a=k^2$. This is an important generalization of Artin's hypothesis. At the same time, the probability of:

$$\mathrm{P}(p\in P(a,i)\,\&\,p\in P)=|P(a,i)|/|P|=c(a,i)$$

Membership agrees exactly with the provisions of the theory of probability, and therefore, estimating $c(a,i)$ on the basis of successive statistical tests and the law of large numbers is parity.

The determination of $c(a,i)$ for any $a,i$ using analytical methods is unlikely in the near term. However, the formation and development of experimental mathematics [1, 2] opens up another way to solve this problem by using computer simulation of nonlinear dynamic processes for the formation of classes of prime numbers.

The process of modeling the distribution of primes in classes $P(a,1),P(1,2),...,P(a,k),...$ was reduced to choosing a set of consecutive primes from a set of a sufficiently large sample of these classes. The number of primes analyzed at each interval of natural numbers was chosen to be 500,000. This choice was largely due to the fact that it was previously established that reducing this value leads to more significant fluctuations in estimates, although convergence to the limit over the entire set of any intervals, even if they are not placed consistently, has the same character.

The process of statistical testing of $p\in P$ primes for checking their belonging to class $P(a,i)$ was reduced to calculating for the selected number $p$ the recursive procedure $x_0=1$, $x_{n+1}=ax_n(\mathrm{mod}\ p)$ until the pairs $ax_l\equiv 1(\mathrm{mod}\ p)$ were reached at some step $i$. Then $card_a(p)=i$ and according to Fermat's theory and the cyclic group theorem the number $p-1$ is divisible by i and then $ind_a(p)=(p-1)/card_a(p)=i$, and therefore $p\in P(a,i)$ and if $i=1$, then $a$ is the primitive root of the cyclic group $(Z/pZ)^*$, and otherwise it is the primitive root of some subgroup. At $i>1$,

we obtain the primitive roots of the subgroups of the $(Z/pZ)^*$ residue group with the index $i>1$. The study of the distribution law of prime numbers $p$ on their belonging to $P(a,i)$ had the character of consistent statistical tests on the set of natural numbers containing the first 500,000 primes. At the first stage, primes $p$ were chosen from the set $\{p_1, p_2,..., p_{500000}\}$. With this $x = p_{500000}$. For each $n \in \{2,...,x\}$, we had to solve two problems: check $n$ for simplicity, and if $n = p \in P$, then $p-1$ was decomposed into simple factors, i.e. systematically solved two non-simple problems of checking numbers for simplicity and decomposition into simple factors. An effective algorithm for solving them was created based on probabilistic methods in the theory of elliptic curves. As a result of analyzing $a \in \{2,...,k\}$, $P(a,1),...,P(a,l)$ sets were obtained for some $l < x$ and absolutely exact values of their powers were calculated, i.e. $|P(a,1)|,...,|P(a,l)|$, and then estimates of:

$$c(a,1,x) = |P(a,1,x)|/\pi(x),...,c(a,l,x) = |P(a,l,x)|/\pi(x)$$

while $c(a,1,x) \to c(a,l),...,c(a,l,x) \to c(a,l)$ with $x \to \infty$ were obtained.

At the next stage, work was also carried out for prime numbers from the $\{p_{500001},..., p_{1000000}\}$ interval and the values of the $c(a,1),...,c(a,l)$ constants were calculated using the same scheme. At the same time $l$ increases. The $\{p_1,..., p_{5000000}\}$ and $\{p_{500001},..., p_{1000000}\}$ sequences were combined, and the estimates of the generalized Artin's constants were again calculated and the process of their refinement was studied on the basis of the theory of large numbers in probability theory. This procedure continued until $x = p = 179424673$ and this is a ten million prime numbers. It was found that $c(a,1),...,c(a,k)$ in probability converges to some values, the exact values of which are irrational and possibly transcendental numbers. In the process of estimating the $c(a,i)$ constants, two important theorems were proved:

Theorem 1. For any $a \in \{2,3,...,k,...\}$ that is not a square, i.e. $a \neq k^2$. The number of non-empty classes of primes tends to infinity at $x \to \infty$.

Theorem 2. For any $a \in \{2,3,...k,...\}$ that is not a square, i.e. $a \neq k^2$ The number of prime numbers in $P(a,i)$ tends to infinity at $x \to \infty$.

These theorems are the basis of the convergence of a sequence of statistical tests to marginal values. Since for any $x \in N$ it is obvious that:

$$\sum_{i=1}^{k} |P(a,i,x)| = \pi(x)$$

$$P(a,i,x) \cap P(a,j,x) = \phi$$

at $i \neq j$, it follows from this that:

$$\sum_{i=1}^{k} c(a,i) = 1$$

This is true for all values of $x \to \infty$. The review [5] provides an estimate of $c(2,1)$, which is identified by $c(2,1)$ in our sense, but $c(2,1)$ differs from the estimate of $c(2,1)$ starting from the fifth decimal place and this is a theoretical error of the survey works. For different $a \in \{2,3,5,6,7,8,10,11,...\}$, the behavior of the $c(a,i)$ constants is complex group-theoretic and number-theoretic. The study of their dynamic properties is beyond the scope of this work. It should be noted that the results of computer simulation of the processes of distribution of primes are calculated with an accuracy of the eleventh decimal place for estimates of $c(2,1), c(3,1), c(5,1), c(6,1),...$ values. This cannot be asserted for classes by the $i \geq 2$ index. To achieve the same accuracy with $i \geq 2$, it is necessary to significantly increase the number of prime numbers. With an increase in the $i$ class index $P(a,i)$ more than three requirements and the volume of the analyzed primes increases in accordance with the unexplored laws.

Probability-theoretic interpretation of the constant:

$$c(a) = \frac{\pi(x,a)}{\pi(x)} \text{ at } x \to \infty$$

Consider the probability space $(\Omega, F, P)$ based on:

$$\Omega = \{\omega_1,..., \omega_n,...\} = \{p_1,..., p_n,...\} = P$$

Obviously at $x \to \infty$ the numbers are $\pi(x) \to \infty$, $\pi(x,a) \to \infty$, but:

$$\pi(x,a) = |P(a,1,x)|,\ \pi(x) = |P(x)|,\ c(a,1,x) = \frac{|P(a,1,x)|}{|P(x)|}$$

and at $x \to \infty$ it is obvious that:

$$|P(a,1,x)|/|P(x)| \to c(a,1)$$

is where $x \in P$, $P \to \infty$,

$$P(a,i,x) = \{p \mid p \le x \,\&\, (p-1)/card_a(p) = i\}$$

is at $x \to \infty$ $P(a,i,x) \to P(a,i)$. Thus:

$$c(a) = \lim_{x \to \infty} \pi(x,a)/\pi(x)$$

It follows from Artin's hypothesis that with $c(a,1)$ there is precisely the probability of a random event $P(a,1)$ consisting of a choice of $\Omega = \{p_1,..., p_n,..\}$ of a prime number $p$ for which $a$ is an original root of the cyclic group $(Z/pZ)^*$. To estimate this probability, the law of large numbers and the method of successive statistical tests were used. The essence of the method is that the first test group was reduced and calculated for $\{p_1, p_2,..., p_{500000}\}$ for each $a \in \{2,3,...,16\}$ evaluation of the values of $c(a,i,x)$ at $x = p_{500000}$ for all possible values of $i = \{1,2,...,k,..\}$, that is, $\tilde{c}_1(a,1,x),...,\tilde{c}_1(a,k,x),...$ was calculated on the next iteration, the same tests were performed for the second iteration on the set $\{p_{500001},..., p_{1000000}\}$. $\tilde{c}_1(a,1,x),...,\tilde{c}_k(a,1,x),...$ Estimates were obtained at the same time $\tilde{c}_1(a,1,x),...,\tilde{c}_k(a,k,x),...$, provided that the first and second samples were combined and computed values and were determined by $|\tilde{c}(a,i,x) - c(a,i,x)| \le \varepsilon$ for all $x$. The main focus was on $c(a,1,x)$. As a result of some iterations, it was found that for all $a$ the estimates obtained:

$$P(x) = \{p \mid p \le x\}$$

$$P(a,i,x) = \{p \mid p \le x \,\&\, (p-1)/card_a(p) = i\}$$

The order of the cyclic group of the subgroup $(Z/pZ)^*$. If $l = p-1$, then $a$ is an original root, and if $l < p-1$ is the original form of the $c(a)$ Artin's measure, $c(a,i)$ is a measure of classes by $P(a,i)$ in $P$. At that $c(a,i) = |P(a,i)/|P||$ and at the same time:

$$\sum_{i=1}^{\infty} c(a,i) = 1 \text{ for all } a > 1$$

This applies only to classes with indexes $i=1$. For $i \geq 2$ it is necessary to increase the number of statistical tests. This is naturally due to the fact that the classes $P(a,i,x)$ for $i \geq 2$ from numerical theorems contain less than prime numbers. In [1] it is stated that this decrease should be of the order of $1/i^2$, but this is an erroneous assertion. The degree of decline essentially depends on the properties of $a$ and requires a separate study. Case $a \in \{4,9,16\}$ requires separate investigations, because these numbers cannot be primitive roots of that number $p$, in accordance with the Fermat theorem [3] cannot be generating elements of groups $(Z/pZ)^*$. However, they are generating elements of the subgroups of the group $(Z/pZ)^*$ with even indices. All classes with odd indices are empty sets. Table 1 shows the constants for $c(a,1)$ for all $a$ except $\{4,9,16\}$. Analysis of the table. The table contains over a thousand columns. The analysis of these data is numerically theoretical and group-specific and goes beyond the scope.

The simulation process of the dynamics of the formation of prime numbers was constructed on the following assumptions. Suppose that an ordered set of prime numbers $P=\{p_1,p_2,...,p_k,...\}$ is given, whose elements are ordered in ascending order. All this set was split into a subset of 500,000 primes. The number of 500,000 is due to the limitations of MS Excel, as a statistical analysis tool, on a number of characteristics of the process of generating prime numbers. Only one restriction is important. We always select 500,000 consecutive primes of the set $P$. In the current version of Excel, this number can be increased to one million. If you use a powerful computer, you can choose a larger number instead of a million.

The implemented version of the study of dynamic processes for the formation of primes includes the following indicators: the number of a simple number in the $p$ in the ordered set of $P$, the value of a simple number of $p$, the value of the recursion length of the numbers $card_a(p)$ at the same value of $a$ for all prime numbers $P$, the index $ind_a(p)$ of the index of the class:

$$ind_a(p)=(p-1)/card_a(p)$$

The value of the residues modulo any natural module $n>1$, for all classes and any other analytic properties of primes or factors of the decomposition of the number of $p-1$ into simple factors. For each simple multiplier $p_i$ in the:

$$p-1=\prod_{i=1}^{n} p_i^{\alpha_i}$$

Decomposition, one parameter of the dynamic process of generating primes is presented, with separate indicators that can be analyzed for any other indicators, the values for them are deducted by the modulus of the natural number $n>1$. The only exception is $ind_a(p)$. The number of controlled indicators analyzed in the Excel environment can be expanded.

## DYNAMICAL PROPERTIES OF THE PROCESSES OF THE FORMATION OF CLASSES PRIMES IN THE GENERALIZED ARTIN'S HYPOTHESIS

According to the idea of experimental mathematics on the first iteration, we proceed from hypothetically known data. But it is also the basis for obtaining experimental information on the basis of which the analytical methods of the theory of numbers yield an expanded representation of the hypothesis in the form $H_i$. It is possible that at the same time the hypothesis can be corrected or even rejected as not true. From the point of view of information technology in mathematics, the hypothesis $H_i$ is used to develop from the point of view of deepening the experimental mathematics of the model of in-depth studies at the level $I_1$.

The iterations process is continued until an analytically based solution of the generated hypothesis is obtained. Since the Artin's generalized hypothesis is considered in the paper, we present the results of the estimation of the constant $c(a,i)$ for the case $a=4$ and $i=2$. The number $a=4$ is a perfect square, and therefore it cannot be a primitive root. In terms of Artin's generalized hypothesis, this is as interesting and important as in the case when $a$ is an original root.

Based on the data presented in [6], we obtained estimates for $c(a,i)$ for $a=2,3,....9,10$ and $i=1,2,...,9,...$. It is shown that their values are stable for class $P(4,2)$ i.e. class with $ind_4(p)=2$ to within a fourth decimal place. They are presented in the table 1.

An analysis of the data in the tables shows that for these numbers Artin's hypothesis is true on the set of primes $|P|=10^9$.

The estimates for the $c(a,i)$ constants given in table 2 have the unique $i=1$ property, which is that for $a\in\{2,3,5,6,7,10,11,12,13,14,15\}$ they coincide with the accuracy of the third decimal place. An analysis of

these classes will make it possible to establish that these classes have the same number of common primes. For any pair of $P(a_i,1) \cap P(a_j,1)$ at $i \neq j$, the values of:

$$\left|P(a_i,1,x) \cap P(a_j,1,x)\right| / \left|P(x)\right| = 0.1473$$

at $x = 179424673$ take the same value, with the exception of the pair:

$$\left|P(3,1,x) \cap P(12,1,x)\right| / \left|P(x)\right| = 2 \cdot 0.1473$$

This means that all these sets have the same number of common identical primes. An analysis of this fact shows that the formation of classes for:

$$a \in \{2,3,5,6,7,10,11,12,13,14,15,16,17,29,53\}$$

In the generalized Artin's hypothesis is subject to the same mathematical laws. Cases $a \in \{4,9\}$ do not relate to this fact because, according to Fermat's theorem, these values are not primitive roots. Special attention should be paid to the case of a pair $(3,12)$ for which classes:

$$P(3,1,x) \cap P(12,1,x)$$

with probability $0.8$ regarding these classes, consist of the same prime numbers. The study of these facts will require the creation of new methods of mathematical analysis of the formation of classes in the classical and, therefore, generalized Artin's hypotheses. The solution to this problem is beyond the scope of this work.

The data in table 2 and table 3 allow us to make an important conclusion that there are many primitive roots for which the generalized Artin's constant $c(a,1)$ is equal to the same value $0.3739\ldots$. In addition, from the same table it follows that all pairs of $(P(a,i),P(a,j))$ sets have sets of common primes of the same power. Deepening research in this direction will parallelly create the theoretical basis for solving the classical Artin's hypothesis. The generalized Artin's hypothesis for all classes $P(a,1),\ldots,P(a,i),\ldots$ will require additional studies based on probabilistic computer simulation on the set of prime numbers of data beyond the limits of the first hundred million.

The results of experimental mathematics in table 1 of the first iteration confirm that Artin's hypothesis is correct. The estimates of the constants are obtained with the accuracy of the third decimal place. For $a \in \{2,3,5,6,7,8,10\}$ the:

$$\sum_{i=1}^{\infty} c(a,i) = 1$$

and for $a \in \{4,9\}$ all $c(a,2i+1) = 0$ and:

$$\sum_{i=1}^{\infty} c(a,2i) = 1$$

This is due to the fact that for all $a = k^2$ this is true because they are primitive roots of $(Z/pZ)^*$ groups, but primitive roots of their subgroups with even indices [3]. The results obtained are the basis for constructing an analytical proof of Artin's hypothesis and its generalization. The $c(a,1)$ ratings given in the table for the set of primitive roots $\{2,3,...,16\}$ are obtained for the first time based on the results of computer simulation. The literature is known estimation $c(2,1)$, which, starting from the fourth decimal place, is estimated analytically incorrect, due to the fact that the formula:

$$c(2,1) = \prod_{p \in P} \left(1 - \frac{1}{p \cdot (p-1)}\right)$$

It is not true, because it includes all primes and among them those primes for which $a = 2$ is not a primitive root [5]. An important result is the creation of a computer model of the process of forming classes $P(a,1),...,P(a,i),....$ For any values of $a > 1$, the interactions between the classes Table 2 and Table 3 are investigated (as a continuation). The first estimates were $c(a,i)$ for $i \geq 2$, and it was established that the statement that $c(a,i)$ is proportional to $1/i^2$ is absolutely false [1]. Obtaining the results is the basis for further deepening research on the Artin's hypothesis using analytical methods. In accordance with the developed mathematical model for the formation of primes on the base $a > 1$ and the calculated values of the generalized constants $c(a,i)$ for $i \geq 1$, as a result of computer simulation it was established that the generalized hypothesis is true. Tables 1, 2, 3 show the values of the Artin's constants, the relationships between classes, the dynamics of the formation of classes and its properties on the set of all primes $P$. The first column of Table 2 contains the values of the Artin's constants for the antiderivatives of the set $\{2,3,5,6,7,8,9,10,11,12\}$. Actually, the modeling of $P(a,i)$ classes was carried out for many:

$$a \in \{2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,29,53\}$$

Numbers $a \in \{4,9,16\}$ as squares of other numbers according to Fermat's theorem [2] cannot be primitive (primitive) roots of $p \in P$, and, accordingly, of residue groups $(Z/pZ)^*$ modulo $p$. Particular attention was paid to the numbers $\{5,13,17,29,53\}$ due to the fact that they belong to the class of numbers of the Chebyshev's type [3] that is, they have representations $p = 4k+1$, while $p \in P$, and the number $n$ is a natural number. According to Chebyshev's assumption, the behavior of these numbers in residue classes modulo a prime number should differ from other primes.

To solve the problem of modeling classes of primes for a given base and evaluating the generalized constants of Artin's $c(a,i)$, an Excel-based software package was created that allows you to extend the modeling process to any natural numbers $a > 1$ and any set of consecutive primes whose power is a multiple of 500,000. This is the number of primes was chosen for the reason that it is statistically represented and provides an accurate representation of the dynamic processes of the formation of classes $P(a,i)$. Table 1 shows a fragment of the modeling process for $a \in \{2,3,5,8,12\}$ values. $a = 2$ is included in this set for the reason that it can be verified that the estimate [5,6] is different from the exact value. The difference begins with the third decimal place. This fact is important due to the fact that expression (4), although from an asymptotic point of view is close to the exact value of $c(2)$, nevertheless, it does not take into account all the features of the formation of classes $P(a,1)$ for $a = 2$. The number $a = 5$ is included in the analysis of the dynamics, because $a = 5 = 4 \cdot 1 + 1$ is the smallest Chebyshev's number, which is as sensitive as possible to the established fact that all $P(5,10k+5)$ classes for $k \geq 0$ are empty. This is true for all Chebyshev's numbers. The proof of this fact is of a number-theoretic nature, and therefore, is excluded from consideration. The number $a = 8$ is included in the representation of dynamics for the reason that the dynamic properties of the classes $P(8,i)$ are radically different from the other classes studied. In particular, it was established that if $a = 8$ is the primitive root of $p \in P$, then $a = 2$ is also the primitive root of the same prime number. Conversely, if $a = 2$ is the primitive root of $p \in P$, then $a = 8$ will be either the same primitive root of $p$ or $p \in P(8,3)$. This is completely new information about the generalized Artin's constants; the developed information technologies have become the basis of fundamentally new results from

modern number theory, and as a consequence of modern cryptography. The numbers $a = 3$ and $a = 12$ are included in table 1 for the reason that $P(3,1)$ and $P(12,1)$ contain 0.8 common primes, while for any other pairs of sets $P(a_l,1)$ and $P(a_s,1)$, the total fraction of common primes is $0.4$ for $l \neq s$ from the considered set of values. These two facts are obtained on the basis of the analysis of the information presented in table 3. This result was also based on the methods of modern number theory and probability theory.

Table 1. The quantity of prime numbers into intervals for a=2,3,5,8,12

| Interval / a | 2 | 3 | 5 | 8 | 12 |
|---|---|---|---|---|---|
| 0 – 0.5 | 187111 | 187011 | 196980 | 112331 | 187013 |
| 0.5 – 1.0 | 186912 | 186948 | 196836 | 112075 | 187057 |
| 1.0 – 1.5 | 186953 | 186960 | 197030 | 112175 | 187040 |
| 1.5 – 2.0 | 186846 | 186856 | 196894 | 112201 | 186958 |
| 2.0 – 2.5 | 187410 | 186896 | 196720 | 112345 | 186792 |
| 2.5 – 3.0 | 186711 | 186777 | 196957 | 112042 | 186767 |
| 3.0 – 3.5 | 187096 | 186926 | 197025 | 112335 | 187157 |
| 3.5 – 4.0 | 186975 | 187176 | 196942 | 112283 | 186984 |
| 4.0 – 4.5 | 187197 | 187148 | 196543 | 112296 | 187317 |
| 4.5 – 5.0 | 186713 | 186796 | 196689 | 121919 | 186721 |
| 5.0 – 5.5 | 186828 | 187013 | 197050 | 112093 | 187005 |
| 5.5 – 6.0 | 187197 | 186771 | 196790 | 112362 | 186936 |
| 6.0 – 6.5 | 186881 | 187116 | 196851 | 112226 | 187056 |
| 6.5 – 7.0 | 187065 | 187214 | 196478 | 112093 | 187122 |
| 7.0 – 7.5 | 187039 | 186718 | 196957 | 112236 | 187050 |
| 7.5 – 8.0 | 187045 | 186756 | 196764 | 112128 | 187161 |
| 8.0 – 8.5 | 187299 | 186805 | 196840 | 112187 | 186594 |
| 8.5 – 9.0 | 186663 | 187050 | 196583 | 111967 | 187144 |
| 9.0 – 9.5 | 186874 | 187156 | 196795 | 112133 | 186976 |
| 9.5 – 10.0 | 187034 | 187072 | 197083 | 111993 | 186947 |

In conclusion, by returning attention to table 1c of another theory of vision. The essence of a fundamentally new fact is that wherever 500,000 primes $p \in P$ are selected for any $a >$, the number of primes in classes ranges from no more than 500, which is no more than a thousandth of them. This means that on any set of consecutive primes we obtain an estimate of the Artin's constants up to the fifth decimal place. Statistical summation of values over the entire set of the first ten million primes made it possible to obtain estimates of the constants $c(a,1)$ to the eighth decimal place.

It follows that the methods of computer simulation of the processes of forming classes of primes $P(a,1), P(a,2),..., P(a,i),...$ and estimation of constants $c(a,1), c(a,2),..., c(a,i),...$ are the basis for the development of information technologies in modern both pure and applied mathematicians.

Table 2 shows the values of the estimates of the generalized Artin's constants for the marked set of values of a, which were studied as classifiers of the set of all primes. Table 2 shows a fragment of the entire huge number of obtained estimates of the Artin's constants. The first column contains estimates of Artin's constants in its original form. They belong to primitive roots. The numbers 4, 9, 16 are not primitive roots, since according to Fermat's theorem they, like the squares of other numbers, cannot be primitive roots. However, they can be classifiers of primes as roots of subgroups of residues modulo primes. An interesting fact is that they can be used to build pseudo-random number generators. In addition, the diskette logarithm problem can be considered on their basis.

Table 2. The distribution of prime numbers in 1 to 10 classes in the generalized Artin's conjecture

| a | *P(a,1)* | *P(a,2)* | *P(a,3)* | *P(a,4)* | *P(a,5)* | *P(a,6)* | *P(a,7)* | *P(a,8)* | *P(a,9)* | *P(a,10)* |
|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 0,374 | 0,280 | 0,066 | 0,046 | 0,018 | 0,049 | 0,008 | 0,035 | 0,007 | 0,014 |
| 3 | 0,373 | 0,299 | 0,066 | 0,056 | 0,019 | 0,033 | 0,008 | 0,014 | 0,007 | 0,015 |
| 4 | 0 | 0,560 | 0 | 0,093 | 0 | 0,099 | 0 | 0,070 | 0 | 0,028 |
| 5 | 0,393 | 0,265 | 0,070 | 0,066 | 0 | 0,047 | 0,009 | 0,016 | 0,007 | 0,028 |
| 6 | 0,374 | 0,280 | 0,066 | 0,074 | 0,018 | 0,049 | 0,008 | 0,014 | 0,007 | 0,014 |
| 7 | 0,374 | 0,282 | 0,066 | 0,068 | 0,018 | 0,050 | 0,008 | 0,017 | 0,007 | 0,014 |
| 8 | 0,224 | 0,168 | 0,199 | 0,028 | 0,011 | 0,149 | 0,005 | 0,021 | 0,022 | 0,008 |
| 9 | 0 | 0,598 | 0 | 0,112 | 0 | 0,066 | 0 | 0,028 | 0 | 0,030 |
| 10 | 0,374 | 0,280 | 0,066 | 0,071 | 0,018 | 0,049 | 0,008 | 0,016 | 0,007 | 0,014 |
| 11 | 0,374 | 0,281 | 0,066 | 0,069 | 0,018 | 0,050 | 0,008 | 0,017 | 0,007 | 0,014 |
| 12 | 0,374 | 0,299 | 0,066 | 0,056 | 0,018 | 0,033 | 0,009 | 0,014 | 0,007 | 0,015 |
| 13 | 0,376 | 0,278 | 0,067 | 0,069 | 0,019 | 0,049 | 0,009 | 0,017 | 0,007 | 0,014 |
| 14 | 0,373 | 0,280 | 0,066 | 0,070 | 0,018 | 0,049 | 0,008 | 0,017 | 0,007 | 0,014 |
| 15 | 0,373 | 0,279 | 0,066 | 0,070 | 0,018 | 0,050 | 0,008 | 0,017 | 0,007 | 0,015 |
| 16 | 0 | 0,374 | 0 | 0,186 | 0 | 0,066 | 0 | 0,140 | 0 | 0,018 |
| 17 | 0,375 | 0,279 | 0,066 | 0,069 | 0,019 | 0,049 | 0,009 | 0,017 | 0,007 | 0,014 |
| 29 | 0,374 | 0,280 | 0,066 | 0,070 | 0,018 | 0,049 | 0,008 | 0,017 | 0,007 | 0,014 |
| 53 | 0,374 | 0,280 | 0,066 | 0,070 | 0,019 | 0,049 | 0,009 | 0,017 | 0,007 | 0,014 |

An interesting result is the equality of the constants $c(2,1)=c(3,1)=c(6,1)=c(7,1)=c(10,1)=\ldots=c(15,1)=c(17,1)\ldots$ up to one thousandth, although $c(8,1)$ and $c(5,1)$ are radically different. On the basis of modern number theory and the theory of random processes, the validity of such results is proved. Evidence of these allegations of remoteness is built only on the basis of data obtained by computer simulation. When analyzing the data, an assumption arose that the constructed classes for primitive roots have common primes. Table 3 shows the results of the analysis of sets of classes $P(a,1)$ for all pairs of primitive roots that were obtained using the constructed filter system. It turned out that all pairs of primitive roots have the same number of common primes with great accuracy. However, the classes $P(3,1)$ and $P(12,1)$ have exactly twice as many primes. This fact

is strictly mathematically justified. Note that other sets of primes of the form $P(a,k)$ with values greater than unity were not the object of even a brief analysis, since in order to obtain their exact values it is necessary to increase the number of primes analyzed, at least by an order of magnitude. This is due to the fact that they are found much less frequently in the set of primes.

Table 3. The intersection of prime numbers with a=2..16 and a=2…10

| a\base | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|
| 2 | 0,3740 | 0,1473 | 0 | 0,1619 | 0,1474 | 0,1473 | 0,2243 | 0 | 0,1328 |
| 3 | 0,1473 | 0,3739 | 0 | 0,1619 | 0,1474 | 0,1500 | 0,1020 | 0 | 0,1474 |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0,1619 | 0,1619 | 0 | 0,3937 | 0,1620 | 0,1620 | 0,1120 | 0 | 0,1620 |
| 6 | 0,1474 | 0,1474 | 0 | 0,1620 | 0,3741 | 0,1474 | 0,1020 | 0 | 0,1474 |
| 7 | 0,1473 | 0,1500 | 0 | 0,1620 | 0,1474 | 0,3741 | 0,1019 | 0 | 0,1474 |
| 8 | 0,2243 | 0,1020 | 0 | 0,1120 | 0,1020 | 0,1019 | 0,2243 | 0 | 0,0919 |
| 9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 10 | 0,1328 | 0,1474 | 0 | 0,1620 | 0,1474 | 0,1474 | 0,0919 | 0 | 0,3741 |
| 11 | 0,1474 | 0,1483 | 0 | 0,1620 | 0,1474 | 0,1476 | 0,1020 | 0 | 0,1473 |
| 12 | 0,1473 | 0,2947 | 0 | 0,1619 | 0,1474 | 0,1500 | 0,1020 | 0 | 0,1474 |
| 13 | 0,1492 | 0,1493 | 0 | 0,1639 | 0,1492 | 0,1493 | 0,1033 | 0 | 0,1493 |
| 14 | 0,1474 | 0,1474 | 0 | 0,1619 | 0,1499 | 0,1474 | 0,1020 | 0 | 0,1473 |
| 15 | 0,1473 | 0,1327 | 0 | 0,1619 | 0,1474 | 0,1471 | 0,1020 | 0 | 0,1474 |
| 16 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

When analyzing the data, an assumption arose that the constructed classes for primitive roots have common primes. Table 3 shows the results of the analysis of sets of classes $P(a,1)$ for all pairs of primitive roots that were obtained using the constructed filter system. It turned out that all pairs of primitive roots have the same number of common primes with great accuracy. However, the classes $P(3,1)$ and $P(12,1)$ have exactly twice as many primes. This fact is strictly mathematically justified. Note that other sets of primes of the form $P(a,k)$ with values greater than unity were not the object of even a brief analysis, since in order to obtain their exact values it is necessary to increase the number of primes analyzed, at least by an order of magnitude. This is due to the fact that they are found much less frequently in the set of primes.

## CONCLUSION

Based on the analysis of the processes of formation of classes of primes for any bases, fundamentally new information technologies for solving complex mathematical problems by the methods of modern experimental mathematics were created. The correctness of the developed approach and computational efficiency are proved. A generalized theory of Artin's hypothesis has been developed which its classical version is a very special case. Estimates of the Artin's constants for bases greater than two are

obtained, and the statistical validity of the estimates obtained is proved. A detailed analysis of the classes of primes is carried out and the foundations of effective methods for the structural analysis of classes are created. It is proved that a new method for modeling the dynamics of the formation of classes of primes and a description of their properties creates the basis for constructing more advanced models of pseudo-prime generators, the development of new methods of information protection in modern cryptography, opens up new possibilities for constructing models of nonlinear dynamic systems.

**REFERENCES**

[1]. Ambrose D. (2014). On Artin's Primitive Root Conjecture. Dissertation zur Erlangung des mathematisch -naturwissenschaftlichen Doctorgrades "Doctor rerum naturalium" der Georg-August-Universitat Gottingen. – 169 p.
[2]. Artin E. (1982). Collected papers. Edited by Serge, Lang and T. John, Springer-Verlag, New York. – 467 p.
[3]. Crandall R., Pomerance C. (2005). Prime Numbers A Computational Perspective. Springer, Portland. – 659 p.
[4]. Manin Yu. I., Panchishkin A. A. (2009). Introduction to the modern theory of numbers. MTSNMO, Moscow. – 547 p.
[5]. Hooley C.(1973) Application of sieve methods to the theory of numbers. Cambridge, London,q. – 234 p.
[6]. Moree P. (2012). Artin's Primitive root conjecture a survey, arXiv: math/0412262v2. – 86 p.
[7]. Vostrov G., Opiata R. (2019). A generalized probabilistic model of computer proof of the Artin's hypothesis, International Simposium Computer Data Analysis and Modeling Stochastic Processes, Minsk. – P. 240– 247.
[8]. Zagier D., (1977). First 50 million prime numbers, Math Intell.– P. 42–71.

**КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ ПРОЦЕССОВ РАЗВИТИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ДИНАМИЧЕСКИХ ПРОЦЕССАХ ФОРМИРОВАНИЯ КЛАССОВ ОБОБЩЕННОГО ГИПОТЕЗА АРТИНА**

**Востров Г., Опиата Р.**

*Исследована взаимосвязь процессов формирования классов простых чисел в обобщенной гипотезе Артина и теории информации, и, как следствие, информационных технологий. Доказано, что вероятностные методы теории информации и информационных технологий являются основой для построения компьютерных моделей классов простых чисел в соответствии с обобщенной гипотезой Артина. Разработаны методы расчета артинских констант и установлена сходимость оценок констант по вероятности для ограничения значений. Созданы основы теоретико-числового анализа констант Артина и родственных классов.*

*Ключевые слова. Обобщенные классы Артина, постоянные Артина, классовые вероятности, устойчивость оценок постоянных Артина, сходимость по вероятности*