UDC 621.316.13

MODELING THE PROCESSES OF FORMING CLASSES OF PRIME NUMBERS AND EVALUATING THE CONSTANTS OF ARTIN'S GENERALIZED HYPOTHESIS ON THE BASIS OF ANALYTICAL AND COMPUTER METHODS OF THEIR FORMATION

G. Vostrov, R. Opiata
Odessa Polytechnic State University

Abstract. *It is proved that modern methods of analytical number theory do not allow obtaining estimates for generalized Artin constants. A method for calculating Artin's constants is developed and the convergence of the estimates of the constants in probability to the limiting values is established. The basic principles of the number-theoretic analysis of Artin's constants and related classes are formulated.*

Key word: *generalized Artin classes, Artin's constants, class probabilities, stability of estimates for Artin's constants, convergence in probability.*

Introduction

The solution of many problems associated with the theory of dynamical systems, with methods of modeling information security processes in the analysis and processing of complexly organized multidimensional data in various areas of applied mathematics depends on the solution of a significant number of problems of pure mathematics that have not yet been solved. Artin's hypothesis of primitive roots is one of such fundamental mathematical problems. For almost a century, it has not been resolved. Some of the results obtained by various researchers are interesting, but they are far from being brought to such a level that would allow improving methods for solving the discrete logarithm problem, developing effective algorithms for modern cryptography, constructing methods for creating pseudo-random number generators, developing the theory of modeling algebraic dynamical systems, creating methods of analysis and processing. complex data. The most important is that the solution of this problem would allow a deeper study and study of the variety of relations between natural and prime numbers.

The study of Artin's hypothesis is important for the study of the relationship between the properties of natural numbers other than zero and plus or minus one, and the properties of the classes of primes generated by recursive mappings based on Fermat's little theorem [1,2,3]. Another topical applied problem is the modeling of self-organizing nonlinear dynamical systems, which are usually called synergetic, taking into account the deep modeling of the phenomena of self-organization in complex systems consisting of sequences of transitions from one phase state to another using random number generators with a given law of probability distribution [3].

Numerical sequences of recursive models of cyclic fixed points of dynamical systems are determined by the properties of primes, which are used to study their behavior under the initial conditions $x(0)=1/p$, where p is a prime number. In this case, it is necessary to know the distribution law of prime numbers. Riemann in 1869 proposed the zeta 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 [1,2]. A hypothesis was formed regarding this Riemann function, according to which all non-trivial zeros of this function are on the line $1/2+iy$, where $i=\sqrt{-1}$ and $y\in R$. This does not mean that all primes lie on this line since y – takes values from the set of real numbers, and it is not known whether it includes at least one prime number from the set P. At the same time, no prime number p is known for which the equality $\xi(1/2+ip)=0$ would be satisfied. Billions of non-trivial zeros have been calculated, but there are no prime numbers among them. Yet the distribution law of prime numbers was found on the basis of the Riemann zeta function.

In 1896, independently of each other, Hadamard and de la Vallée-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 distribution of primes in asymptotic form. However,

this information is not enough to determine whether the prime number x, due to the simple fact that the logarithmic law does not follow the answer to the question: this number x is prime or composite. Moreover, even if x is a prime number, $n(x)$ does not necessarily have to be its number in the ordered sequence of all primes. Enumeration of primes with given properties is an even more difficult task [1,2]. When solving many both applied and mathematical problems, it becomes necessary to use large arrays of primes with specified properties. An expressive example of such a set is the set of all primes for which a given number a is the primitive root. The construction of such sets is a very difficult problem in modern number theory.

One of the directions of deepening the logarithmic law of distribution of primes was the formulation in 1927 by the French mathematician Artin of the hypothesis about primitive roots of primes $p \in P$, and, accordingly, primitive roots of residue groups $(Z/pZ)^*$ modulo a prime number p [4,5,6,7].

Consider the definition of a primitive root of a prime number p. The number $a \neq 1$ and $a \neq k^2$ is the primitive (antiderivative) root of the number p, if the following relations are true:

$$\begin{cases} a^{p-1} \equiv 1 (\text{mod } p) \\ a^{\frac{p-1}{n}} \not\equiv 1 (\text{mod } p), \quad n > 1 \end{cases} \tag{2}$$

and n is a divisor of $p-1 = \prod_{i=1}^{k} p_i^{\alpha_i}$. Checking this condition for large primes, and especially if k is also large, is computationally intensive. It is much easier to use the following theorem:

Theorem 1. The number a is the primitive root of the prime number p if and only if the condition is satisfied:

$$\frac{a^*(p-1)}{2} \equiv (p-1) (\text{mod } p)$$

assuming that in $x(n+1) = ax(n) (\text{mod } p)$ recursion the value $p-1$ appears for the first time at $(p-1)/2$ calculation step.

The validity of the theorem obviously follows from the fact that condition $x(n) \cdot x(p-1-n) \equiv 1 (\text{mod } p)$ is always satisfied in the above recursion. The application of this theorem greatly simplifies the verification of the fact that the number a is the primitive root of the given prime number p.

Taking into account the definition of a primitive root, Artin's hypothesis has the form:

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

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

$$\begin{cases} \pi(x,a) = c(a,x) \cdot \pi(x), \\ \ln c(a,x) = c(a), \quad x \to \infty \end{cases} \tag{3}$$

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

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

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

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

with $c(2) = \prod_{p \in P} \left(1 - \frac{1}{p(p-1)} \right)$, and the estimate is $c(2) = 0{,}373955813 \ldots$. As will be shown later, this estimate is correct only with the precision of the first two decimal places. In addition, this expression assumes that the entire set of primes is always used to calculate $c(2)$, which, as will be shown, is completely wrong, due to the fact that the process of forming Artin's constants has a completely different law of their formation.

It should be noted that any number $a > 1$ and is relatively prime with p is the basis for considering a recursive function $f(x) \equiv a \cdot x (\text{mod } p)$, which results in a recursive iterative sequence.

$$f(x_0 = 1) = 1, \; f(x_{n+1}) = x_{n+1} \equiv a x_n (\text{mod } p) \tag{4}$$

According to Fermat's theorem [1,2], if a is not a primitive root for p, then the process of

recursive computations will continue for such m, for which the equality $f(x_n = m) \equiv x_{m-1} \cdot a (\mathrm{mod}\ p) = 1$ will be achieved, i.e.

$$a^m \equiv x_m (\mathrm{mod}\ p) \text{ and } m < p-1 \qquad (5)$$

From Fermat's theorem and the properties of the $(Z/pZ)^*$ coset group over the ring of integers modulo a prime number p or the properties of the cyclic Galois group F_p^* isomorphic to it modulo p of residues over a finite field [1,2], it follows that in this case a is a generating element of some subgroups of group $(Z/pZ)*$ or group F_p^* respectively. Moreover (5), m is the order of this subgroup, which is usually denoted $card_a(p)$, and the number of cosets for this subgroup is denoted by $ind_a(p)$. According to the theorem on the cyclic group F_p^*, in this case, the equality always holds:

$$p-1 = card_a(p) \cdot ind_a(p) \qquad (6)$$

It follows from the above analysis that equation (6) allows us to investigate Artin's hypothesis from a more general point of view, when any natural number $a > 1$ can be used as a classifier of the set of all primes by value $ind_a(p)$, which is the object of further research. As will be established, Artin's primitive root conjecture is a frequent case of its more general formulation.

1. Analysis of the analytical asymptotic method for solving the classical Artin hypothesis

The first attempts to solve Artin's problem are of a number-theoretic nature based on analytical number theory. First of all, it should be noted that they are based on the assumption that the generalized Riemann hypothesis based on the Dedekind zeta function is correct. This does not take into account all the variety of relationships between integers, which can be primitive roots, and the set of all primes for which the selected integer is the primitive root. The importance of this assumption lies in the fact that it is assumed that the Dedekind zeta function takes into account all the many options for the dependence of the formation of classes of all primes for a given number a on its properties, which are described by decomposing it into prime factors. It should be noted that although the definition of the Dedekind zeta function based on the theory of ideals is based on the Galois theory, this dependence cannot be revealed by analytical methods for a simple reason. The norm of an ideal is uniquely determined, but it is a function of the coefficients of polynomials over the Galois field, and the roots do not have an unambiguous representation according to the theory of Kummer's circular fields [1,2]. In addition, only primitive roots of prime numbers are taken into account and the generating elements of the subgroups of the cyclic residue group F_p^*, as well as their properties, are not taken into account. At the same time, information about their properties is important, if only because we get new information about the structure of the residue group modulo a prime number p. From the point of view of the mathematical theory of information technologies and the theory of entropy, there is an incompleteness of information, which leads to inaccurate and incorrect estimates of the Artin coefficients even for primitive roots and does not allow taking into account the processes of influence of the generating elements of the cyclic group F_p^*. This simple fact led to the fact that the Artin coefficient $c(2)$ in the Hooley method depends on all primes, the incorrectness of such an estimate is obvious due to the fact that this constant must depend on the primes p for which it is an antiderivative root and nothing more. As will be shown later, in fact, Artin's constants $c(a,i,x)$ with a i index greater than or equal to one on any sufficiently large interval of consecutive primes depend on a significant number of factors, the nature of which has not been investigated in number theory.

Probabilistic methods for estimating generalized Artin constants based on computer modeling will be considered as another model for solving this problem and as a generalization of Artin's original hypothesis. The creation of this approach was preceded for a long time by the analysis of the method for its solution by the English mathematician H. Holly, who published in the article [4] and then re-presented for the particular case $a = 2$ in the monograph [5]. First of all, let's pay attention to the attitude of well-known specialists in the field of number theory to this solution. The Soviet and American mathematician Yu. I. Manin in his monograph [2] unambiguously asserts that Artin's conjecture has not been proven and is rather complicated. The same position is taken by such well-known mathematicians as Cohen [6], Rosen [7], Moree [8] and others, but at the same time C. Pomerance in the monograph [1] notes that this problem was solved by Ch. Hooley and the solution is given in work [4]. Due to this ambiguity in the attitude to the work of Ch. Hooley and the importance of solving it both from a theoretical and applied point of view, let us dwell on the works of Ch. Hooley [4] in more detail.

Note that the Riemann zeta function (1) was used to prove the logarithmic distribution law of prime numbers (2), but the Riemann hypothesis on the distribution of nontrivial zeros of the zeta function was not used in any way. Ch. Hooley in [4] and monograph [5] uses the Dedekind zeta function over Galois fields. At the same time, the author assumes that the hypothesis is valid:

Hypothesis. The real part β of each complex zero $p=\beta+i\gamma$ of the Dedekind zeta function is $1/2$ for any Galois field of type Q.

This assumption is in complexity equivalent to the millennium Riemann hypothesis, i.e. the millennium hypothesis that as presented this assumption is highly restrictive. The theorem proved by the author has the form:

Theorem 2. If we assume the validity of the Riemann hypothesis for zeta functions of Galois fields of type $Q\left(\sqrt[k_1]{l},\sqrt[k]{1}\right)$, where k is a squarefree number and they are coprime numbers $k_1 \mid k$ then we have:

a) for any $a \neq 0 \& \pm 1$ and other than an exact square, let $N_a(x)$ denote the number of primes $p \le x$, for each of which a is the primitive root of $\bmod p$, let also a_1 be the square-free part of a, let h be the largest integer such that a is h-th power of an integer and let:

$$c(h)=\prod_{q\mid h}\left(1-\frac{1}{q-1}\right)\cdot\prod_{q+h}\left(1-\frac{1}{q(q-1)}\right)$$

Then, if $a_1 \not\equiv 1(\bmod 4)$, we have:

$$N_a(x)=c(h)\frac{x}{\ln x}+O\left(\frac{x\ln\ln x}{\ln^2 x}\right)$$

at $x\to\infty$, if $a_1 \equiv 1(\bmod 4)$, we have:

$$N_a(x)=c(h)\cdot\left(1-\mu\left(|a_x|\right)\right)\cdot\prod_{\substack{q\mid h\\ q\mid a_1}}\frac{1}{q-2}\cdot$$

$$\cdot\prod_{\substack{q\mid h\\ q\mid h_1}}\frac{1}{q^2-q-1}\cdot\frac{x}{\ln x}+O\left(\frac{x\ln\ln x}{\ln^2 x}\right)$$

at $x\to\infty$.

b) If $a \neq 0,\pm 1$ is not an exact square, then there are an infinite number of primes p for which a is the primitive root of $\bmod p$.

The proof of this theorem given in the first article is difficult to recognize as irreproachable and even correct for a number of reasons. The author refers to the theory of indices without highlighting those properties of indices that allow the existence of a residue a of degree q modulo a prime number p, while a is considered as an antiderivative root for other primes, but this condition is not satisfied for a given prime number p, then is and is the generating element of the group F_p^*. This means that there can be several equations:

$$Y_q^* = a(\bmod p)$$

with different q which are divisors of $p-1$ and such a variety of equations is not taken into account in the work. The author did not use the theory of indices correctly, since in such cases it is necessary to take into account the variety of equations of this kind in the analysis given by the author. But in this case, there may be several variants of estimates constructed by the author, and at the same time it is difficult to take into account their influence on the developed theory. Moreover, there are potentially infinitely many such cases for each a, and there is no effective algorithm, a method that would take into account their influence on the calculation of constants based on the Dedekind zeta function and the influence of these estimates on subsequent conclusions.

In monograph [5], the author corrected the analysis and repeats the proof only under the assumption $a=2$ and the theorem has the following formulation:

Theorem 3 (Hooley Ch.). If we assume that the extended Riemann hypothesis is valid for the Dedekind zeta functions over Galois fields and Kummer circular fields of type $Q\left(\sqrt[k]{2},\sqrt[k]{1}\right)$, where k is a squarefree number, then:

a) Let $N_2(x)$ be the number of primes p not exceeding x, for which 2 is the primitive root modulo p. Then:

$$N_2(x)=\frac{c\cdot x}{\ln x}+O\left(\frac{x\ln\ln x}{\ln^2 x}\right)$$

$$c=\prod_q\left(1-\frac{1}{q(q-1)}\right)$$

b) There are infinitely many primes p for which 2 is the primitive root modulo p.

In proving this theorem, the author states:

"Index theory shows that for $p\neq 2$ and any prime divisor q of $p-1$, the comparison is resolvable:

$$\upsilon^q \equiv 2(\bmod p)$$

is equivalent to the divisibility of the index of the number 2 (in any base) by q. Thus, we have a criterion, for each 2 is an antiderivative root modulo p if and only if $p \neq 2$, and there is no such prime divisor q of $p-1$ for which 2 is a residue of q modulo p". Based on the above analysis, verification of this condition cannot be performed without analyzing the behavior of the Dedekind zeta function, which is excluded by the given rating system.

A comparative analysis of these two theorems suggests that the author has come to the conclusion that the first theorem is not perfect. It is obvious that for the $a = 2$ case of the expression:

$$c(h) = \prod_{q|h}\left(1-\frac{1}{q-1}\right)\prod_{q|h}\left(1-\frac{1}{q(q-1)}\right)$$

$$c = \prod_{q}\left(1-\frac{1}{q(q-1)}\right)$$

do not match. According to Hooley's work, h is the maximum positive integer for which a is the h-th power of an integer modulo p. Analysis of the expression $c(2)$ and the results obtained below allow us to assert that this Artin constant, like all other $c(a)$ for any other values of a, is actually formed in accordance with completely different laws.

Now let's pay attention to several facts that follow from Hooley's theorems and the results of estimating the generalized Artin constants given in the table. Hooley's score starting at the third decimal place is different from the exact score obtained from computer simulations. It should be noted that the basis of any method for checking whether the number a is the primitive root of a prime number p or the generating element of the subgroup of the residue group $(Z/pZ)^*$ modulo p is a recursive function, which is always determined by the iterative sequence (4). If a natural number a is given, which is different from ± 1 and a perfect square, and a prime number p, then the length of recursion (4) in the general case can be determined only as a result of calculations in accordance with this expression. Based on this remark, we can conclude that for different values of the number a for the same prime number p, the values of the length of the recursive sequence (4) may differ significantly. The existing information technologies for the analysis of the command of all (a, p) pairs are not reflected in the generalized Dedekind zeta function. Therefore, the estimate of the Artin constant for a in the case when $a = 2$, obtained by analytical methods, can be considered as a value asymptotically close to a value that is not an absolute constant. As will be shown below, Artin's constants fluctuate on the entire infinite set of primes around a certain value for each a, but these fluctuations have values of the order of the fifth decimal place and they are natural due to the fact that the distribution of primes has a complex irregular structure with elements of randomness. An estimate of the behavior of constants on the entire set of (a, p) pairs, which is infinite both in a and p, does not reflect the entire possible variety of values.

From the table below, we can conclude that there is a wide variety of Artin constants. Hooley's theorems not only do not allow obtaining their estimates, but also do not provide information about their values and the dependence of these values on the properties of primitive roots determined by decomposition into prime factors or their representation in the form $a = 4k+1$ or $a = 4k+3$ as proposed by Chebyshev [1,2]. Natural numbers n other than ± 1 are most interesting to consider as classifiers of the set of prime numbers, according to the value of the index determined from expression (6). In this case, perfect squares of natural numbers are the carrier of important information about primes.

In addition to the above problems related to the solution of Artin's conjecture by analytical methods, much more complex problems arise when it is necessary to investigate the dynamic properties of the behavior of generating elements of subgroups of F_p^*. In this case, one should take into account the existence of subgroups of different orders in such groups. Moreover, the orders of all subgroups of these cyclic groups depend on the structure of the decomposition of $p-1$ into prime factors. The transition from one prime number to the next prime number p^* usually leads to unforeseen changes in the structure of decomposition into prime factors p^*-1. The Dedekind zeta function does not contain information about the structure of the F_p^* subgroups for all primes. There is only one way to study and estimate Artin's constants for the whole variety of subgroups including the group itself is to use the recursion $x(n+1) = a \cdot x(n) (\mathrm{mod}\ p)$ with the initial condition $x(0) = 1$, under which, in accordance with Fermat's little theorem, for each prime number p, the recursion length and its index will be calculated in accordance with the formula (6). Considering large arrays of sequential primes, we obtain a set of statistical data that will be

the basis for the application of modern randomization methods in the analysis of the statistical properties of the analyzed data arrays [12,13,14,15].

Arrays of statistical data will make it possible to obtain estimates of the Artin constants $c(a,i,x)$ based on modern randomization methods, for any values of a and index i, for sufficiently large values of x, which determine the representativeness of statistics. Methods for evaluating constants and their analysis are given in the second part of this article.

2. Modeling the processes of forming dynamic information about the structure of classes of prime numbers on a given basis.

Now let's return to the logarithmic law of distribution of primes [1,2] in order to draw attention to the fact that the given equality does not provide exhaustive information about the structure of the spaces between primes. It is especially important to have information about the distribution of smooth primes [1]. This information is especially important when solving the discrete logarithm problem and applying algorithms for its solution in modern coding theory, modern cryptography. It is known that it is very difficult to find large smooth prime numbers. Hence it follows that it is of considerable interest to search for the distribution laws of prime numbers not only with respect to their primitive roots, but also the generating elements of subgroups of the residue group modulo a prime number $(Z/pZ)^*$. Artin's hypothesis does not imply such detailed research. Such tasks were not considered at all.

The second circumstance is that simultaneously with this fact, the dynamics of change in $O\left(x\cdot e^{-\frac{c}{2}\sqrt{\ln x}}\right)$ is investigated. In [7,8], the entropy of function $f(x)=P(x)-Li(x)$ where $Li(x)=\int_2^x \frac{dt}{\ln t}$ was estimated and 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. Such proposals can be a study of the fractal structure of the set of all primes, for which the given number is a primitive root.

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 from this 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 prime numbers for any given base $a>1$. Further more detailed studies of this proposal confirm that although the logarithmic distribution law is fulfilled, nevertheless, complete information about the dynamic properties of primes and their relationship with their primitive roots remains poorly studied. Therefore, we will further consider any values of the base a large units.

According to Artin's hypothesis [4,5,6], 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 [6,7] 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 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:

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

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]:

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

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:

$$\sum_{i=1}^{\infty} c(a,i) = 1 \qquad (7)$$

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 $c(a,i)$. It should be noted already now that the convergence is not absolute, that is, the estimates will fluctuate around a certain constant and the magnitude of the fluctuations potentially converges to zero, however, for each value of a, it has its own value, which is not precisely computable. 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 $a \neq k^2$. This is true according to Fermat's theorem [1,2]. Wherein, a is the primitive root of the group of residues $(Z/pZ)^*$ for any, 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:

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

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 [9,10,11,12].

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 [13,14,15] 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 $x_0 = 1$, $x_{n+1} = ax_n \pmod p$ until the pairs $ax_l \equiv 1 \pmod p$ 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 the analyzing $a \in \{2,..., x\}$, $P(a,1),..., P(a,l)$ 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:

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

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 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:

$$\bigcup_{i=1} P(a,i)=\pi(x)$$

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

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

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

and 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 (Ω,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 $x\in P,\ P\to\infty$,

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

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 $|\tilde{c}(a,i,x)-\tilde{c}(a,1,x)|\le\varepsilon$ 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 $i\ge 2$ 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 $i\ge 2$ from numerical theorems contain less than prime numbers. In [1] it is stated that this decrease should be of the order of $1/i^2$ [15], but this is an erroneous assertion. This is clearly seen from table 1. The degree of decline essentially depends on the properties of a and requires a separate study. Case $a\in\{4,9,16,25\}$ 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 $\{4,9,16,25\}$ Since for these numbers the constant is 0. Full analysis of the table 1 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.

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 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 $a\in\{2,3,...,32,53\}$ and $i=1,2,...,10,...$. 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.

The estimates for the $c(a,i)$ constants given in table 1 have the unique $i=1$ property, which is that for $a\in\{2,3,5,6,7,10,...,15,17,...,24,26,28,...,32,53\}$ they coincide with the accuracy of the third decimal place.

The data in table 1 allow us to make an important conclusion that there are many primitive roots for which the generalized Artin constant $c(a,1)$ is equal to the same value $0.3739...$. The generalized Artin hypothesis for all classes $P(a,1),...,P(a,i),...$ 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 $a\in\{2,3,5,...,8,10,...,15,17,...,24,26,32,53\}$ the:

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

And for $a\in\{4,9,16,25\}$ 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 general form without using the Dedekind zeta function, which will be presented in the next works of the authors.

The $c(a,1)$ ratings given in the table for the set of primitive roots $a\in\{2,3,5,6,7,10,...,15,17,...,24,26,28,...,32,53\}$ 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:

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

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.

3. Dynamic properties of processes of formation of classes of prime numbers in the generalized Artin hypothesis

In accordance with the developed mathematical model for the formation of classes of primes based 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 modeling, it was established that the generalized hypothesis is correct. Table 1 shows the values of Artin's constants, relationships between classes, the dynamics of the formation of classes and its properties on the set of all primes P.

In reality, modeling of the processes of formation of $P(a,i)$ classes was carried out for the $a\in\{2,3,...,32,53\}$ set. The numbers $a\in\{4,9,16,25\}$ as squares of numbers, according to Fermat's theorem [2], cannot be the primitive roots of $p\in P$, and, accordingly, the residue group $(Z/pZ)^*$ modulo p. However, they are generating elements of the subgroups of this group, and therefore they are considered on a par with primitive roots. A detailed analysis of their behavior can be done on the basis of the same table 1. In this work, we will not dwell on this problem due to the need to build an extended model for the formation of generalized Artin constants. In [4], the assumption was

formulated that if the index is equal to $i \geq 2$, the probability of belonging to the corresponding class is proportional to $1/i^2$. A simple analysis of the above table shows that this is completely wrong.

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 type [1,2], 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 be different from other primes. The non-standard behavior of such values is not only in a different dynamics of the formation of generalized Artin constants, but also in the fact that the $P(a,i,x)$ classes are empty for some i values. This fact can be seen in the table below. A complete analysis and exact mathematical proof of this behavior of the generating elements of the F_p^* group will be considered in subsequent works. The point is that this property is also observed for $a = 4k+1$ values. An example of such behavior of classes is observed for $a = 27$, which does not belong to the marked class, as can be seen from the table. This brief analysis shows that the developed theory of classes is much deeper than all the assumptions that have been expressed about Artin's hypothesis so far and is of fundamental importance both for number theory and for the theory of discrete logarithm, modern theory of coding and cryptography, the theory of constructing pseudo-random number generators and modeling dynamic systems [1,2,13,14,15].

To solve the problem of modeling classes of primes on a given base and estimating the generalized constants of Artin $c(a,i)$, 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 cardinality is a multiple of 500,000. This is the number of primes was chosen because it is statistically presented and provides an accurate representation of the dynamic processes of generating $P(a,i)$ classes. Table 1 shows the results of the simulation process for $a \in \{2,3,...,32,53\}$ values. $a = 2$ is included in this set for the reason that one can make sure that the estimate [5,6] differs from the exact value. The difference starts at the third decimal place. This fact is important because expression (7), 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 $P(a,1)$ classes for $a = 2$. The number $a = 5$ is interesting because $a = 5 = 4 \cdot 1 + 1$ is the smallest Chebyshev number that is most sensitive to the established fact that all $P(5,10k+5)$ classes for $k \geq 0$ are empty. This is true for all numbers a which are Chebyshev numbers. The proof of this fact is of a number-theoretic nature, and therefore, is not given.

Table 1

Table of generalized Artin constants with index i values less than or equal to 10

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	0,3740	0,2805	0,0664	0,0467	0,0189	0,0498	0,0089	0,0351	0,0074	0,0141
3	0,3739	0,2992	0,0666	0,0561	0,0190	0,0332	0,0089	0,0140	0,0074	0,0151
4	0	0,5609	0	0,0935	0	0,0997	0	0,0701	0	0,0283
5	0,3937	0,2657	0,0700	0,0664	0	0,0473	0,0094	0,0166	0,0078	0,0284
6	0,3741	0,2805	0,0665	0,0748	0,0189	0,0498	0,0089	0,0140	0,0074	0,0142
7	0,3741	0,2827	0,0664	0,0684	0,0188	0,0503	0,0089	0,0170	0,0074	0,0143
8	0,2243	0,1683	0,1995	0,0281	0,0114	0,1496	0,0054	0,0211	0,0222	0,0085
9	0	0,5983	0	0,1122	0	0,0666	0	0,0281	0	0,0303
10	0,3741	0,2804	0,0665	0,0713	0,0189	0,0499	0,0089	0,0166	0,0074	0,0142
11	0,3741	0,2813	0,0664	0,0695	0,0189	0,0500	0,0089	0,0173	0,0074	0,0142
12	0,3740	0,2991	0,0665	0,0561	0,0189	0,0333	0,0090	0,0140	0,0074	0,0152
13	0,3764	0,2787	0,0670	0,0697	0,0191	0,0495	0,0090	0,0174	0,0074	0,0141
14	0,3739	0,2806	0,0665	0,0707	0,0189	0,0498	0,0089	0,0171	0,0074	0,0141
15	0,3739	0,2796	0,0665	0,0708	0,0189	0,0508	0,0089	0,0177	0,0074	0,0151
16	0	0,3740	0	0,1869	0	0,0664	0	0,1403	0	0,0189
17	0,3754	0,2794	0,0667	0,0698	0,0190	0,0497	0,0090	0,0175	0,0075	0,0141
18	0,3740	0,2805	0,0664	0,0467	0,0189	0,0498	0,0089	0,0350	0,0074	0,0142
19	0,3739	0,2808	0,0665	0,0700	0,0189	0,0499	0,0089	0,0175	0,0074	0,0142
20	0,3936	0,2657	0,0700	0,0664	0	0,0472	0,0094	0,0166	0,0078	0,0284
21	0,3722	0,2819	0,0681	0,0705	0,0188	0,0486	0,0107	0,0176	0,0076	0,0142
22	0,3740	0,2805	0,0665	0,0704	0,0189	0,0499	0,0089	0,0174	0,0074	0,0141

Continuation of Table 1

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)
23	0,3741	0,2808	0,0664	0,0699	0,0189	0,0499	0,0089	0,0175	0,0074	0,0141
24	0,3740	0,2805	0,0665	0,0748	0,0189	0,0498	0,0089	0,0140	0,0074	0,0142
25	0	0,5708	0	0,1328	0	0,1015	0	0,0333	0	0,0190
26	0,3741	0,2805	0,0664	0,0702	0,0189	0,0499	0,0090	0,0174	0,0074	0,0142
27	0,2244	0,2244	0,1994	0	0,0113	0,0997	0,0054	0	0,0222	0,0114
28	0,3740	0,2828	0,0665	0,0684	0,0188	0,0503	0,0090	0,0171	0,0074	0,0143
29	0,3745	0,2801	0,0666	0,0700	0,0189	0,0498	0,0089	0,0176	0,0074	0,0141
30	0,3740	0,2805	0,0665	0,0699	0,0189	0,0499	0,0089	0,0178	0,0074	0,0142
31	0,3741	0,2806	0,0665	0,0701	0,0188	0,0499	0,0089	0,0175	0,0074	0,0142
32	0,2953	0,2214	0,0524	0,0369	0,0945	0,0394	0,0070	0,0277	0,0058	0,0709
53	0,3740	0,2804	0,0665	0,0701	0,0190	0,0498	0,0090	0,0175	0,0074	0,0142

The numbers $a=8,27,32$ are interesting because the dynamical properties of the $P(8,i)$ classes are radically different from the other studied classes. In particular, it has been established that if $a=8$ is a primitive root $p\in P$ then $a=2$ is also a primitive root of the same prime number. Conversely, if $a=2$ is a primitive root $p\in P$, then $a=8$ will either be the same primitive root p or $p\in P(8,3)$. This is completely new information about generalized Artin constants. The developed approach made it possible to obtain fundamentally new results in modern number theory, and, as a consequence, in modern cryptography. You should pay attention to $a=32$ for the reason that, according to the assumption, the expected $c(32,1,x)$ for this number should be of the same order as $c(8,1,x)$, however, the estimate of this constant, as you can see, has a completely different meaning. For the same reason, note that the $c(20,1,x)$ score coincides with the $c(20,1,x)$ score, but there are no empty sets of $P(29,i,x)$ type for $i\geq 2$ The number $21=4\cdot 5+1$ belongs to the class of composite numbers, perhaps for this reason the constant $c(21,1,x)$ takes a different value. For these reasons, we can conclude that it is necessary to further develop information technologies for solving the generalized hypothesis of Artin both on the basis of the method of computer modeling and analytical methods of deepening and substantiating the results obtained. A deeper and more detailed analysis of the estimates of Artin's constants for values of indices greater than unity will be the subject of a separate analysis.

Let's look at the above table from a different theory of vision. The essence of a fundamentally new fact is that wherever 500,000 $p\in P$ primes are allocated sequentially for any $a>1$, the number of primes in classes fluctuates within no more than 500, which is no more than a thousandth of them. This means that, on any set of sequential primes, we obtain an estimate for the Artin constants up to the fifth decimal place. The summation of the values over the entire set of the first ten million primes by statistical methods made it possible to obtain estimates of the $c(a,1)$ constants with an accuracy of the eighth decimal place.

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

An interesting result is the equality of the constants:

$$c(2,1)=c(3,1)=c(6,1)=c(7,1)=c(10,1)=...$$
$$=c(15,1)=c(17,1)...$$

to within one thousandth, although $c(8,1)$ and $c(5,1)$ are radically different from them. On the basis of modern number theory and the theory of random processes, the foundations of the classification of both prime numbers and natural numbers as their classifiers have been created, the validity of the developed method has been empirically proven to create mathematical foundations for solving the entire spectrum of problems in this area. Proofs of the above statements can only be constructed on the basis of empirical data obtained as a result of computer modeling.

Conclusions

On the basis of the analysis, the processes of forming classes of prime numbers, for any reason, fundamentally new information technologies for solving complex mathematical problems were created using the methods of modern experimental mathematics. The correctness of the developed approach and computational efficiency are proved. A

generalized theory of Artin's hypothesis has been developed, for which its classical version is a very special case. Estimates for the Artin constants for bases greater than two are obtained, and the statistical consistency of the estimates obtained is proved. A detailed analysis of the classes of prime numbers is carried out and the foundations of effective methods of structural analysis of classes are created. It is proved that a new method for modeling the dynamics of the formation of classes of prime numbers and describing their properties creates the basis for constructing more advanced models of generators of pseudo-random numbers, the development of new methods of information protection in modern cryptography, and opens up new opportunities for constructing models of nonlinear dynamic systems. To estimate the values of the generalized Artin constants, we used randomization methods [10,11,12] and strategies for applying the methods of experimental mathematics [13,14,15], however, in both cases, the authors made significant adjustments that took into account the fact that the numbers $p-1$ for all primes P have a completely different law of probability distribution for $w(p-1)$, which differs significantly from the normal law of probability distribution for $w(n)$ in the case when n is an arbitrary composite natural number. The $w(n)$ function denotes the number of different prime factors in the factorization n.

References

1. Crandall R., Pomerance C. (2005), "Prime Numbers A Computational Perspective" Springer Science, Portland, pp. 663.
2. Manin Yu. I., Panchishkin A. A. (2009), "Introduction to the modern theory of numbers" MTSNM. Springer, pp. 528.
3. Vostrov G., Opiata R. (2019), "Computer modeling of dynamic processes in analytic number theory" Imternational Simposium Computer Data Analysis and Modeling Stochastic Processes, Minsk, pp. 240–247.
4. Ambrose D. (2014), "On Artin's Primitive Root Conjecture" Dissertation zur Erlangung des mathematisch -Naturwissenschaftlichen Doctorgrades "Doctor rerum naturalium" der Georg-August-Universitat Gottingen, pp. 169.
5. Artin E. (1982), "Collected papers" Edited by Serge, Lang and T. John, Springer-Verlag, New York.
6. Hooley C. (1973), "Application of sieve methods to the theory of numbers", Cambridge, London, pp. 1–234.
7. Moree P. (2012), "Artin's Primitive root conjecture a survey", arXiv: math/0412262v2, pp. 1–86.
8. Zagier D. (1977), "Firs't 50 million prime numbers", Math Intell, pp. 42–71.
9. Cohen H. (2007), "Number Theory. vol. 2, Analytic and modern tools", Springer-Verlag, New-York.
10. Mitzenmacher M., Upfal E. (2005), "Probability and Computing. Randomized Algorithms and Probabilistic Analysis", Cambridge University Press, pp. 356.
11. Habib M., McDiarmid C., Ramirez-Alfonsin J., Reed B. (1998), "Probabilistic Methods for Algorithmic Discrete Mathematics", Springer, pp. 344.
12. SkorochodA V., Hoppensteadt F., Habib S. (2002), "Random Perturbation Methods with Application in Science and Engineering", Springer, pp. 496.
13. Bailey D. H., Bauscke H. H.(2013), M. Thera, J. D. Vanderwerff, "Computational and Analytical Mathematics", Springer, New York, pp. 692.
14. Borwein J, Bailey D. H., Girgensohn R. (2005), "Experimentation in Mathematics. Computational Path to Discovery", Printed in Canada, pp. 371.
15. Borwein P., Choi S., Rooney B., Weirathmueller A. (2008), "The Riemann Hypothesis", Canadian Mathematical Society, Springer, pp. 541.

МОДЕЛЮВАННЯ ПРОЦЕСІВ ФОРМУВАННЯ КЛАСІВ ПРОСТИХ ЧИСЕЛ І ОЦІНЮВАННЯ КОНСТАНТ УЗАГАЛЬНЕНОЇ ГІПОТЕЗИ АРТІНА НА ОСНОВІ АНАЛІТИЧНОГО ТА КОМП'ЮТЕРНОГО МЕТОДІВ ЇХ ФОРМУВАННЯ

Г. М. Востров, Р. Ю. Опята
Державній університет «Одеська політехніка»

Анотація. *Виконано аналіз залежності між процесами формування класів простих чисел в узагальненій гіпотезі Артіна на основі теорії рандомізації алгоритмів імовірнісного методу і аналітичної теорії чисел. Досліджено ймовірні методи побудови комп'ютерних моделей формування класів простих чисел, відповідно до узагальненої гіпотезою Артіна. Доведено, що сучасні методи*

аналітичної теорії чисел не дозволяють отримати оцінки узагальнених констант Артіна. Створено метод обчислення констант Артіна і встановлена збіжність оцінок констант за ймовірністю до граничних значень. Сформульовано основні принципи теоретико-числового аналізу констант Артіна і пов'язаними з ними класами.

Рішення багатьох проблем пов'язаних з теорією динамічних систем, з методами моделювання процесів захисту інформації при аналізі і обробці складно організованих багатовимірних даних в різних областях прикладної математики залежить від рішення значної кількості проблем чистої математики, які до сих пір не вирішені. Гіпотеза Артіна про первісних коренях відноситься до числа таких фундаментальних математичних проблем. Протягом майже століття вона не вирішена. Деякі отримані результати різними дослідниками цікаві, але далеко не доведено до такого рівня, який дозволяв би вдосконалювати методи вирішення проблеми дискретного логарифма, розробляти ефективні алгоритми сучасної криптографії, будувати методи створення генераторів псевдовипадкових чисел, розвивати теорію моделювання алгебраїчних динамічних систем, створювати методи аналізу і обробки складно організованих даних.

Ключові слова: *Узагальнені класи Артіна. Константи Артіна. Ймовірності класів. Стійкість оцінок констант Артіна. Збіжність за ймовірністю.*

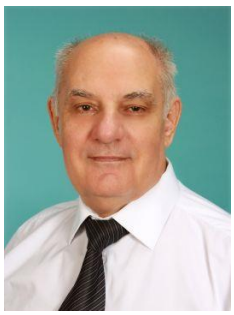
МОДЕЛИРОВАНИЕ ПРОЦЕССОВ ФОРМИРОВАНИЯ КЛАССОВ ПРОСТЫХ ЧИСЕЛ И ОЦЕНИВАНИЕ КОНСТАНТ ОБОБЩЕННОЙ ГИПОТЕЗЫ АРТИНА НА ОСНОВЕ АНАЛИТИЧЕСКОГО И КОМПЬЮТЕРНОГО МЕТОДОВ ИХ ФОРМИРОВАНИЯ

Г. Н. Востров, Р. Ю. Опята
Государственный университет «Одесская политехника»

Аннотация. *Исследованы вероятностные методы построения компьютерных моделей формирования классов простых чисел, в соответствии с обобщенной гипотезой Артина. Доказано, что современные методы аналитической теории чисел не позволяют получить оценки обобщенных констант Артина. Создан метод вычисления констант Артина и установлена сходимость оценок констант по вероятности к предельным значениям. Сформулированы основные принципы теоретико-числового анализа констант Артина и связанными с ними классами.*

Ключевые слова: *Обобщенные классы Артина. Константы Артина. Вероятности классов. Устойчивость оценок констант Артина. Сходимость по вероятности.*

Received 15.04.2021



George Vostrov, Odessa Polytechnic State University, Ph. D. of Technical Sciences, Associate Professor of the Department of Applied Mathematics and Information Technologies. Shevchenko ave., 1, Odessa, Ukraine. E-mail: vostrov@gmail.com, mob. +380503168776

Востров Георгій Миколайович, державний університет "Одеська політехніка", кандидат технічних наук, доцент кафедри прикладної математики та інформаційних технологій. Просп. Шевченко, 1, Одеса, Україна.
Эл. адрес: vostrov@gmail.com, тел. +380503168776

ORCID ID: 0000-0003-3856-5392

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

Опята Роман Юрійович, державний університет "Одеська політехніка", аспірант кафедри прикладної математики та інформаційних технологій. Просп. Шевченко, 1, Одеса, Україна. Эл. адрес: roma.opyata@gmail.com, тел. +38095249753

ORCID ID: 0000-0001-5806-9615