Probabilistic Methods in Computer Simulation of the Formation of Classes of Primes and Estimation of the Constants of the Generalized Artin Hypothesis

George Vostrov[1][0000-0003-3856-5392], Roman Opiata[2][0000-0001-5806-9615]

[1]Odessa National Polytechnic University, Shevchenko avenue 1, 65000, Ukraine
vostrov@gmail.com
[2]Odessa National Polytechnic University, Shevchenko avenue 1, 65000, Ukraine
roma.opyata@gmil.com

Abstract. The relationship between the processes of forming classes of primes in the generalized Artin hypothesis based on the theory of randomized algorithms of the probabilistic method is investigated. It is proved that probabilistic methods are the basis for constructing computer models of classes of primes in accordance with the generalized Artin hypothesis. Methods for calculating the Artin constants are developed and the convergence of the estimates of the constants in probability to the limiting values is established. The foundations of a number-theoretic analysis of Artin's constants and related classes are created.

Keywords. generalized Artin classes, Artin constants, class probabilities, stability of estimates of the Artin constants, convergence in probability

1 Introduction

The solution of many problems in various fields of applied mathematics depends on the solution of a significant number of problems of pure mathematics, which are still not solved. Artin's hypothesis of primitive roots is one of these fundamental mathematical problems.

The solution to the Artin problem is important for investigating the relationship between the properties of natural numbers other than zero and plus or minus 1 and the properties of the classes of primes generated by recursive mappings based on Fermat's small theorem [1 – 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.

It is necessary to know the law of distribution of primes. Riemann proposed a zeta function in 1869:

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

where s is a complex variable, P is the set of all primes [1,2]. Concerning this Riemann 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.

In 1896, independently, Hadamard and Vallee-Poussin proved that equality is true:

$$\pi(x)=\int_2^x \frac{dt}{\ln t}+O\left(x\cdot e^{-c\sqrt{\ln x}}\right) \tag{2}$$

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 asymptotic form.

One of the ways to deepen the logarithmic law of the distribution of primes was the formulation in 1927 by the French mathematician Artin of the hypothesis of primitive roots of primes $p \in \mathsf{P}$ and, accordingly, of primitive roots of residue groups $(Z/pZ)^*$ modulo prime p [4 – 7].

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

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

Moreover, 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:

$$\pi(x,a)=c(a,x)\cdot\pi(x) \tag{4}$$

where $\pi(x,a)$ is the number of primes p less than or equal to x, for which $a \ne \pm 1$ and $a \ne k^2$ are according to (2) their primitive roots, $c(a)$ is the Artin constant. More precisely, this hypothesis should be presented as follows:

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

But then $c(a,x) = \dfrac{\pi(x)}{\pi(x,a)}$ 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 (primitive) root. Note that the first relation in (5) is always satisfied if a and p are coprime numbers according to Fermat's theory [1].

It should be noted that Artin 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:

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

at the same time $c(2) = \prod_{p\in\mathsf{P}} \left(1 - \dfrac{1}{p(p-1)} \right)$, and an estimate of the value $c(2) = 0{,}373955813\ldots$. As will be shown later, this estimate is true only with the accuracy of the first two decimal places.

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.

$$f(x_0 = 1) = 1,\ f(x_{n+1}) = x_{n+1} \equiv a x_n (\mathrm{mod}\ p) \tag{7}$$

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 that equality $f(x_n = m) \equiv x_{m-1}\cdot a (\mathrm{mod}\ p) = 1$ is reached, i.e.

$$a^m \equiv 1 (\mathrm{mod}\ p) \text{ and } m < p-1 \tag{8}$$

From Fermat's theorem and the properties of the group of residues $(Z/pZ)^*$ modulo p [1,2], it follows that in this case a is a generating element 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:

$$p-1=card_a(p)\cdot ind_a(p) \tag{9}$$

From the above analysis it follows that equation (9) allows us to study the Artin 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 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.

2 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 [1,2] Information about the distribution of smooth primes [1] is important when solving the discrete logarithm problem and applying algorithms for solving it in the modern coding theory, modern cryptography. It is known that finding smooth large prime numbers is very difficult. This implies that it is of considerable interest to search for the laws of distribution of primes not only with respect to their primitive roots, but also to the generating elements of the subgroups of the residue group modulo prime $(Z/pZ)^*$. Artin's hypothesis does not imply such detailed studies. 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 $f(x)=\pi(x)-Li(x)$ was estimated and was proved that it has a fractal character.

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 [4 – 6], the set of such primes has the distribution law $\pi(x,a)$ as an expression:

$$\pi(x,a)=c(a)\cdot\pi(x) \tag{10}$$

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 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:

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

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]:

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

where $card_a(p)$ is the length of the dynamic recursion $x_{n+1} \equiv ax_n \pmod p$ 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 $\mathsf{P}(a,i)$ for any a. By uniformity is meant that within each class of primes $\mathsf{P}(a,i)$ 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 $\mathsf{P}(a,1)$. For an arbitrary natural number x, the equality

$$\pi(x,a,i) = c(a,i,x) \cdot \pi(x) \tag{14}$$

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 [1,2]. Wherein, a is the primitive root of the group of residues $(Z/pZ)^*$ for any $p \in \mathsf{P}$ such that $\mathsf{P}(a,1) = \{p \in \mathsf{P} \mid (p-1)/card_a(p) = 1\}$. It is important to investigate

the classes of primes $\mathrm{P}(a,i)$ 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:

$$\mathrm{P}(a,i)=\{p\,|\,(p-1)/card_a(p)=ind_a(p)\} \tag{15}$$

where $ind_a(p)=i$ is the index of the subgroup of $(Z/pZ)^*$. The classes of primes $\mathrm{P}(a,i)$ have not yet been studied and the distribution of primes in these classes is not known. In [1], an assumption was made that $\mathrm{P}(a,i)$ at $i>1$ is proportional to $\mathrm{P}(a,1)$ 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:

$$\mathrm{P}\big(p\in\mathrm{P}(a,i)\big)=\big|\mathrm{P}(a,i)\big|/\big|\mathrm{P}\big|=c(a,i) \tag{16}$$

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 – 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 – 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 $\mathrm{P}(a,1),\mathrm{P}(a,2),...,\mathrm{P}(a,k),...$ 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 $p\in\mathrm{P}$ primes for checking their belonging to class $\mathrm{P}(a,i)$ 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 $p\in\mathrm{P}(a,i)$ 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 $\mathrm{P}(a,i)$ 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 $n = p \in \mathrm{P}$, 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 $a \in \{2,...,x\}$, $\mathrm{P}(a,1),...,\mathrm{P}(a,l)$ sets were obtained for some $l < x$ and absolutely exact values of their powers were calculated, i.e. $|\mathrm{P}(a,1)|,...,|\mathrm{P}(a,l)|$, and then estimates of:

$$c(a,1,x) = |\mathrm{P}(a,1,x)|/\pi(x),...,c(a,l,x) = |\mathrm{P}(a,l,x)|/\pi(x) \qquad (17)$$

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. 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 $\mathrm{P}(a,i)$ 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:

$$\bigcup_{i=1} \mathrm{P}(a,i) = \pi(x) \qquad (18)$$

$$\mathrm{P}(a,i) \cap \mathrm{P}(a,j) = \phi \qquad (19)$$

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

$$\sum_{i=1}^{k} c(a,i) = 1 \tag{20}$$

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 $\mathrm{P}(a,i)$ more than three requirements and the volume of the analyzed primes increases in accordance with the unexplored laws.

Probability-theoretic interpretation of the constant:

$$c(a) = \frac{\pi(x,a)}{\pi(x)} \text{ at } x \to \infty \tag{21}$$

Consider the probability space (Ω, F, P) based on:

$$\Omega = \{\omega_1,...,\omega_n,...\} = \{p_1,...,p_n,...\} = \mathrm{P} \tag{22}$$

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

$$\pi(x,a) = |\mathrm{P}(a,1,x)|,\ \pi(x) = |\mathrm{P}(x)|,\ c(a,1,x) = \frac{|\mathrm{P}(a,1,x)|}{|\mathrm{P}(x)|} \tag{23}$$

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

$$|\mathrm{P}(a,1,x)| / |\mathrm{P}(x)| \to c(a,1) \tag{24}$$

is where $x \in \mathrm{P}$, $\mathrm{P} \to \infty$,

$$\mathrm{P}(a,i,x) = \{p \mid p \leq x \,\&\, (p-1)/card_a(p) = i\} \tag{25}$$

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

$$c(a) = \lim_{x\to\infty} \pi(x,a)/\pi(x) \tag{26}$$

It follows from Artin's hypothesis that with $c(a,1)$ there is precisely the probability of a random event $\mathrm{P}(a,1)$ 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:

$$\mathrm{P}(x) = \{p \mid p \le x\} \tag{27}$$

$$\mathrm{P}(a,i,x) = \{p \mid p \le x \,\&\, (p-1)/card_a(p) = i\} \tag{28}$$

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 measure, $c(a,i)$ is a measure of classes by $\mathrm{P}(a,i)$ in P. At that $c(a,i) = |\mathrm{P}(a,i)/|\mathrm{P}\|$ and at the same time:

$$\sum_{i=1}^{\infty} c(a,i) = 1 \text{ for all } a > 1 \tag{29}$$

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 $\mathrm{P}(a,i,x)$ 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 essential-

ly 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 $\mathrm{P} = \{p_1, p_2, ..., p_k, ...\}$ 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 [16].

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:

$$ind_a(p) = (p-1)/card_a(p) \tag{30}$$

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:

$$p-1 = \prod_{i=1}^{n} p_i^{\alpha_i} \tag{31}$$

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.

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 $a \in \{2,...,32,53\}$ 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 $a \in \{2,3,...,32,53\}$ the:

$$\sum_{i=1}^{\infty} c(a,i)=1 \tag{32}$$

and for $a \in \{4,9,16,25\}$ all $c(a,2i+1)=0$ and:

$$\sum_{i=1}^{\infty} c(a,2i)=1 \tag{33}$$

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

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:

$$c(2,1)=\prod_{p \in P}\left(1-\frac{1}{p\cdot(p-1)}\right) \tag{34}$$

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 $\mathsf{P}(a,1),...,\mathsf{P}(a,i),....$ 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 Formation of Classes of Prime Numbers in the Generalized Artin Hypothesis

In accordance with the developed mathematical model for the formation of base classes of primes on the basis of $a > 1$ 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. Table 1 shows the values of the Artin constants, the relationship between classes, the dynamics of the formation of classes and its properties on the set of all primes P.

Actually, the modeling of $\mathsf{P}(a,i)$ classes was carried out for many $a \in \{2,...,32,53\}$. Numbers $a \in \{4,9,16,25\}$ as squares of numbers according to Fermat's theorem [2] cannot be primitive roots of $p \in \mathsf{P}$, 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 type [1,2] that is, they have representations $p = 4k+1$, while $p \in \mathsf{P}$, 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 on a given basis and evaluating 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 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 $\mathsf{P}(a,i)$. Table 1 shows the results of the simulation 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 (5),

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 $\mathsf{P}(a,1)$ for $a=2$. The number $a=5$ is interesting because $a=5=4\cdot 1+1$ is the smallest Chebyshev number, which is as sensitive as possible to the established fact that all classes $\mathsf{P}(5,10k+5)$ for $k\geq 0$ are empty. This is true for all Chebyshev numbers. The proof of this fact is of a theoretical number, and therefore, is not given.

Table 1. The distribution of prime numbers in the generalized Artin hypothesis

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)***
2	0,3740	0,2805	0,0664	0,0467	0,0189	0,0498	0,0089	0,0351	0,0074
3	0,3739	0,2992	0,0666	0,0561	0,0190	0,0332	0,0089	0,0140	0,0074
4	0	0,5609	0	0,0935	0	0,0997	0	0,0701	0
5	0,3937	0,2657	0,0700	0,0664	0	0,0473	0,0094	0,0166	0,0078
6	0,3741	0,2805	0,0665	0,0748	0,0189	0,0498	0,0089	0,0140	0,0074
7	0,3741	0,2827	0,0664	0,0684	0,0188	0,0503	0,0089	0,0170	0,0074
8	0,2243	0,1683	0,1995	0,0281	0,0114	0,1496	0,0054	0,0211	0,0222
9	0	0,5983	0	0,1122	0	0,0666	0	0,0281	0
10	0,3741	0,2804	0,0665	0,0713	0,0189	0,0499	0,0089	0,0166	0,0074
11	0,3741	0,2813	0,0664	0,0695	0,0189	0,0500	0,0089	0,0173	0,0074
12	0,3740	0,2991	0,0665	0,0561	0,0189	0,0333	0,0090	0,0140	0,0074
13	0,3764	0,2787	0,0670	0,0697	0,0191	0,0495	0,0090	0,0174	0,0074
14	0,3739	0,2806	0,0665	0,0707	0,0189	0,0498	0,0089	0,0171	0,0074
15	0,3739	0,2796	0,0665	0,0708	0,0189	0,0508	0,0089	0,0177	0,0074
16	0	0,3740	0	0,1869	0	0,0664	0	0,1403	0
17	0,3754	0,2794	0,0667	0,0698	0,0190	0,0497	0,0090	0,0175	0,0075
18	0,3740	0,2805	0,0664	0,0467	0,0189	0,0498	0,0089	0,0350	0,0074
19	0,3739	0,2808	0,0665	0,0700	0,0189	0,0499	0,0089	0,0175	0,0074
20	0,3936	0,2657	0,0700	0,0664	0	0,0472	0,0094	0,0166	0,0078
21	0,3722	0,2819	0,0681	0,0705	0,0188	0,0486	0,0107	0,0176	0,0076
22	0,3740	0,2805	0,0665	0,0704	0,0189	0,0499	0,0089	0,0174	0,0074
23	0,3741	0,2808	0,0664	0,0699	0,0189	0,0499	0,0089	0,0175	0,0074
24	0,3740	0,2805	0,0665	0,0748	0,0189	0,0498	0,0089	0,0140	0,0074
25	0	0,5708	0	0,1328	0	0,1015	0	0,0333	0
26	0,3741	0,2805	0,0664	0,0702	0,0189	0,0499	0,0090	0,0174	0,0074
27	0,2244	0,2244	0,1994	0	0,0113	0,0997	0,0054	0	0,0222
28	0,3740	0,2828	0,0665	0,0684	0,0188	0,0503	0,0090	0,0171	0,0074
29	0,3745	0,2801	0,0666	0,0700	0,0189	0,0498	0,0089	0,0176	0,0074
30	0,3740	0,2805	0,0665	0,0699	0,0189	0,0499	0,0089	0,0178	0,0074
31	0,3741	0,2806	0,0665	0,0701	0,0188	0,0499	0,0089	0,0175	0,0074
32	0,2953	0,2214	0,0524	0,0369	0,0945	0,0394	0,0070	0,0277	0,0058
53	0,3740	0,2804	0,0665	0,0701	0,0190	0,0498	0,0090	0,0175	0,0074

The numbers $a=8,27,32$ are interesting for the reason that the dynamic properties of the classes $\mathsf{P}(8,i)$ are radically different from the other classes studied. In particular, it was established that if $a=8$ is the primitive root of $p\in\mathsf{P}$, then

$a = 2$ is also the primitive root of the same prime number. Conversely, if $a = 2$ is the primitive root of $p \in \mathsf{P}$, then $a = 8$ will be either the same primitive root of p or $p \in \mathsf{P}(8,3)$. This is completely new information about the generalized Artin constants. The developed approach allowed us to obtain fundamentally new results in modern number theory, and as a consequence of modern cryptography.

In conclusion, look back at Table 1 from a different theory of vision. The essence of a fundamentally new fact is that wherever 500,000 primes $p \in \mathsf{P}$ are selected for any $a > 1$, 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 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 $c(a,1)$ accurate to the eighth decimal place.

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

An interesting result is the equality of constants:

$$\begin{aligned} &c(2,1) \cong c(3,1) \cong c(6,1) \cong c(7,1) \cong c(10,1) \cong c(11,1) \cong c(12,1) \cong \\ &c(14,1) \cong c(15,1) \cong c(18,1) \cong c(19,1) \cong c(22,1) \cong c(23,1) \cong \\ &c(24,1) \cong c(26,1) \cong c(28,1) \cong c(30,1) \cong c(31,1) \cong c(53,1)... \end{aligned} \tag{35}$$

accurate 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 as a result of computer modeling. The dynamic properties of the values of other classical Artin's constants confirm the assumption that there is no universal law of their formation. The generalized Artin's constants $c(a,i)$ for $i > 1$ obey even more complex laws and will be the subject of further research.

4 Conclusion

Based on the analysis of the processes of formation of classes of primes for any bases, fundamentally new information technologies were created for solving complex mathematical problems using 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 which its classical version is a very special case. Estimates of the Artin 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 number generators, the development of new methods of information protection in modern cryptography, opens up new possibilities for constructing models of nonlinear dynamic systems.

5 REFERENCE

1. Pomerance C, Rassias M (2015) Analytic Numbers Theory. Springer, pp 378
2. Manin Yu, Panchishkin A (2016) Introduction to the modern theory of numbers. Springer, Berlin, pp 528
3. Vostrov G, Opiata R (2019) A generalized probabilistic model of computer proof of the Artin hypothesis, International Simpoium Computer Data Analysis and Modeling Stochastic Processes, Minsk
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, 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 87
8. Koukoulopoulos D (2017) The Distribution of Prime Numbers. Springer, pp 370
9. Cohen H (2017) Number Theory. Volume II: Analytic and modern tools. Springer, New-York, pp 637
10. Mitzenmacher M, Upfal E (2017) Probability and Computing: Randomized Algorithms and Probabilistic Analysis. Cambridge University Press, pp 490
11. Noga A, Joel H Spencer (2016) Probabilistic Method. Willey, Third Edition, pp 373
12. Hytonen T, van Neerven J, Veraar M, Weis L (2017) Analysis in Banach Spaces: Volume II: Probabilistic Methods and Operator Theory. Springer, pp 616
13. Bailey D, Bauscke H, Thera M, Vanderwerff J (2013) Computational and Analytical Mathematics. Springer, New York, pp 701
14. Borwein J, Bailey D, Girgensohn R (2015) Experimentation in Mathematics. Computational Path to Discovery. Canada, pp 368
15. Borwein P, Choi S, Rooney B, Weirathmueller A (2018) The Riemann Hypothesis. Canadian Mathematical Society, Springer-Verlag New York, pp 533
16. Zeigler B, Muzy A, Kofman E (2019) Theory of Modeling and Simulation. Academic Press, pp 692