UDC:

СТАТИСТИЧНІ ТА АЛГЕБРАЇЧНІ ВЛАСТИВОСТІ РОЗПОДІЛУ ПЕРВІСНИХ КОРЕНІВ ПРОСТИХ ЧИСЕЛ В МНОЖИНАХ ПОСЛІДОВНИХ ПРОСТИХ ЧИСЕЛ

Г. Востров, Р. Опята, М. Ставратій, О. Щербанюк
Національний університет «Одеська політехніка»

Abstarct. *Приведено обґрунтування необхідності в повній якісній інформації стосовно алгебраїчних властивостей первісних коренів в множинах послідовних простих чисел з урахуванням області їх розташування в множині усіх простих чисел та величини її потужності. Доведено, що при значному поглиблені розташування множини послідовних простих чисел значення* $\omega(p-1)$ *плавно, але систематично збільшується в такій мірі, що на певному етапі процесу поглиблення середня величина відстані між первісними коренями простих чисел таких множин послідовних простих чисел плавно збільшується в певній мірі. Розроблені основи математичного оцінювання величини ентропії ймовірностей зміни статистичних властивостей математичного сподівання середньої величини відстані між первісними коренями. Створені методи комп'ютерного моделювання процесів формування статистичних законів розподілу первісних коренів в таких системах послідовних простих чисел значної потужності.*

Keywords*: розподіл первісних коренів; константи Артіна; класи простих чисел; розподіл індексів за простим модулем; відстані між первісними коренями.*

Вступ

Гіпотеза Артіна в її первісній формі була повністю орієнтована на методи оцінювання константи $A(2)$, які враховують розподіл простих чисел для яких число 2 є первісним коренем. На той час повна інформація стосовно закону розподілу простих чисел з такими властивостями була відсутня. З цієї причини, Артін в співпраці з Хассе запропонували математичний вираз $A(2)=\prod(1-1/q(q-1))$, який був обґрунтований як оцінка щільності розподілу простих чисел для яких число 2 є первісним коренем[1,2,3].

Приведене обґрунтування стало основою доведення, що така оцінка коректна. В подальшому, Ch. Hooley[4], на основі аналітичної теорії чисел, довів теорему, яка має наступне формулювання.

Теорема 1. Якщо допустити, що розширена гіпотеза Рімана справедлива для дзета-функцій Дедекінда над куммеровськими полями типу $Q(2^{1/k}, 1^{1/k})$, де k-безквадратне число , тоді:

а) Нехай N(2,x) – число простих *p*, що не перевищують *x*, для яких число 2 є первісним коренем по модулю *p*. Тоді:

$$N(2,x)=cx/\ln x+O\left(x\ln(\ln x)/(\ln x)^2\right)$$
$$\text{де}\quad c=\prod\left(1-1/q(q-1)\right);$$

б) Існує безмежна кількість простих чисел *p*, для яких число 2 є первісним коренем по модулю *p*.

Приведена теорема є обґрунтуванням формули методами аналітичної теорії чисел, але при умові що справедлива гіпотеза Рімана в формі Дедекінда над куммеровськими полями. Справедливість гіпотези Рімана не доведена до цього часу. Більше того приведена теорема стосується тільки випадку коли $a=2$ при розгляді $A(2)$. Перенести методи аналітичної теорії чисел на загальний випадок $A(k)$, при умові що k – будь-яке натуральне число, яке відмінне від плюс або мінус одиниці та повного квадрату на основі такого математичного методу практично не можливо. Крім того значення цієї оцінки $A(2)=0.3739552..$ носить апроксимаційний характер, а тому вона ні в якій мірі не характеризує динамічні властивості формування цієї характеристики процесу формування множини простих чисел $P(2,1,x)$, для яких число 2 є первісним коренем коли *x* збігається до нескінченості.

Якщо розглядати її з статистичної точки зору то як було доведено в роботах [5,6,7] не враховується ряд факторів які впливають на

процеси формування класів простих чисел в множинах послідовних простих чисел $[p_n, p_{n+500000}]$ на основі рекурсивної функції формування первісних коренів всієї множини простих чисел, яка має вигляд

$$x(1), \quad x(n+1) = 2x(n) \pmod{p} \qquad (1)$$

При цьому, із цієї множини вибираються ті, і тільки ті прості числа *p*, для яких довжина циклу рекурсивних обчислень дорівнює $p-1$. Це означає, що для цього простого числа p , число 2 є первісним коренем. При такому аналізі точно обчислюється кількість простих чисел в приведеній множині послідовних простих чисел, для яких число 2 є первісним коренем. Знаючи кількість таких простих чисел, легко обчислити значення $c(2,1,x) = A(2)$. Очевидно, якщо отримана таким чином оцінка константи Артіна для будь-якої множини послідовних простих чисел буде давати її оцінку з необхідною точністю, то виникає можливість даний метод використовувати для оцінювання констант Артіна для будь-яких значень числа *a*.

Властивості цієї рекурсивної процедури ніяк не пов'язані з властивостями методу Артіна та аналітичного методу запропонованого для оцінки $A(2)$ в роботах Ch. Hooley перш за все, тому що методи комп'ютерного моделювання процесів формування класів простих чисел $P(a,i,x)$ для будь-яких значень числа *a* та індексу *i* то ми отримуємо точні значення оцінки константи Артіна $c(a,i,x)$ для множини послідовних простих чисел виділеного інтервалу. При такому підході обчислюються значення узагальненої константи Артіна, в якій враховуються не тільки первісні корені, для яких $ind(a,p)=1$, але і значення індексу будь-якої величини. Приведена рекурсивна процедура для кожного простого числа дає відповідь - у якому відношенні знаходиться число *a* та відповідне просте число *p*.

Оцінювання констант $A(a) = c(a,1,x)$ для будь-якого числа *a* в загальному випадку вимагає розглядання гіпотези Артіна значно більш фундаментальними методами. Перш за все, для будь-якого простого числа *p* множини усіх простих чисел P, необхідно знати ймовірнісний закон розподілу $\omega(p-1)$ у будь-якій множині послідовних простих чисел $[p_n, p_{n+M}]$ та динаміку зміни його параметрів при переході до іншої множини послідовних простих чисел тієї ж потужності. Доведено, що має місце систематичне зростання його математичного сподівання та величини дисперсії при переході від однієї множини послідовних простих чисел до іншої.

В роботі[5] на основі евристичного обґрунтування було доведено, що величина $\omega(p-1)$ розподілена згідно з логнормальним законом із теорії ймовірностей. Зростання математичного сподівання та дисперсії, при збільшені p_n для приведеної системи інтервалів послідовних простих чисел, а це приводить до зміни щільності розподілу первісних коренів простих чисел. Нескладно довести, що якщо таке гіпотетичне допущення правильне, то це призведе до того, що поведінка констант Артіна на множині усіх простих чисел буде мати інші динамічні властивості. Тому важливо знати закони розподілу не тільки первісних коренів, а і закони розподілу індексів для усіх чисел множини $\{1,2,3,...,p-3,p-2,p-1\}$ простого числа *p*. Поки що обмежимося аналізом певних властивостей закону розподілу первісних коренів.

Аналіз алгебраїчного зв'язку констант Артіна із теорією первісних коренів та індексів.

Необхідно звернути увагу на те що гіпотеза Артіна в його формулюванні стосується виключно первісних коренів, але як було показано[6,7] якщо не володіти інформацією стосовно законів розподілу індексів $ind(a,p)$ то для $c(5,1,x)$ неможливо привести чітке пояснення чому $c(5,1,x) > c(2,1,x)$. Обґрунтування приведене в роботі[7]. Подібним чином не можливо було б пояснити чому справедлива ціла множина нерівностей.

$$\{c(2,1,x) > c(8,1,x),\ c(2,1,x) > c(27,1,x),\ c(2,1,x) > c(125,1,x),\ ...\} \qquad (2)$$

Можна привести важливі інші приклади, які стосуються в першу чергу первісних коренів, а в загальному випадку і індексів простих чисел при оцінюванні констант Артіна не тільки для окремих натуральних чисел *a*, але і для систем таких чисел. Якщо розглядати проблему Артіна як фундаментальну проблему теорії чисел, то при аналізі множин послідовних простих чисел $[p_n, p_{n+M}]$ необхідно враховувати первісні корні простих чисел в даній множині послідовних простих чисел.

Досі закони розподілу первісних коренів простих чисел в загальному випадку не досліджені. Необхідно відмітити, що з класами

простих чисел $P(a,i,x)$ пов'язані системи арифметичних прогресій, з якими пов'язана гіпотеза Elliott-Halberstams, згідно з якою структури арифметичних прогресій повинні бути узгоджені з точки зору значень їх різниць. Це пов'язане з тим, що коли обрана множина послідовних простих чисел $[p_n, p_{n+M}]$ та при цьому значення $a = p$ досить велике відносно p_{n+M} , то необхідно значно збільшити M , тому що інакше оцінки $c(a,i,x)$ та властивості $P(a,i,x)$, можуть бути некоректними з точки зору властивостей арифметичних прогресій.

Доведено[7], що «стійкість» з точністю до ε_{p_n} оцінок для $c(a,i,x)$ та властивості класів $P(a,i,1)$ для всіх можливих значень індексу на множинах $[p_n, p_{n+M}]$ обумовлена законами розподілу $ind(a,p)$ для будь-якого p_n на множині $\{1,2,3,4,5,...l-1,l,l+1,...,p_k-2,p_k-1\}$. Індекси можуть бути парними та непарними, при цьому їх кількість однакова - $(p_k-1)/2$. До цього часу детально не досліджені в загальному випадку закони розподілу як парних так і непарних індексів. Володіння знаннями про властивості таких законів має важливе значення для створення детальної моделі розв'язання проблем гіпотези Артіна. Досі є невідомим закон розподілу непарних індексів, а ще більш інтригуючим є відсутність будь-яких даних стосовно закону розподілу первісних коренів. Якщо створювати методи комп'ютерного моделювання процесів формування класів $P(a,i,x)$ та оцінювання $c(a,i,x)$ на основі аналітичних методів, то інформація про закони розподілу $ind(a,p)$ на приведених упорядкованих множинах простих чисел є просто необхідною.

Перший серйозний крок у розв'язувані гіпотези Артіна був зроблений в роботі Ch.Hooley [6]. В даній роботі, особлива увага приділялася випадку, коли a не є первісним коренем для простого числа p. Тоді як стверджує Ch.Hooley, знайдеться таке q - просте число, яке ділить $p-1$, та при цьому буде справедлива рівність:

$$a^{(p-1)/q} \equiv 1 \pmod{p} \qquad (3)$$

Як уже було відмічено, в загальному випадку, це не зовсім коректне допущення. В тому випадку, коли a для даного простого числа p не є первісним коренем, ми можемо припустити що $ind(a,p) = m$. Наступним кроком повинен бути виконаний аналіз усіх варіантів значення m, Якщо $m = q$, і при цьому q - просте число, то подальший аналіз може співпадати з аналізом Ch. Hooley, а у випадку коли m не є простим числом, виникає множина варіантів пов'язаних з розкладанням його на прості множники. При цьому виникає значна кількість варіантів, які пов'язані з тим, що в цьому випадку неможливо просто вибрати один із співмножників, на які розкладається $m = \prod q_i^{\alpha_i}$. Такий вибір не може бути просто виконаний без детального обґрунтування. Таким чином аналіз такого випадку приведе до аналізу системи послідовності варіантів

$$\begin{aligned} &a^{(p-1)/m} \equiv 1 \pmod{p} \\ &при \quad m = \prod q_i^{\alpha_i} > q_i \end{aligned} \qquad (4)$$

які відповідають розкладанню m на прості множники, що не може бути чітко обґрунтованою, а довільний вибір приводить до помилок. Приведене зауваження є ще одним фактором обґрунтування необхідності застосування методу комп'ютерного моделювання процесів формування класів $P(a,i,x)$ для всіх $ind(a,p) = I$ та оцінювання констант $c(a,i,x)$. Таким чином, рівняння дзета функції Рімана у формі Дедекінда при таких обставинах не може бути обґрунтуванням цього методу аналізу проблеми при різних значеннях числа a, як класифікатора множини простих чисел. Тому необхідно створити основи методів аналізу розподілу первісних коренів для простих чисел.

Розглянемо алгоритм обчислення $ind(a,p)$ для всіх a з упорядкованої множини цілих чисел, пов'язаних з простим числом p:

$$\{1,2,3,4,5,\ \ldots, n-1, n, n+1,\ \ldots, p-2, p-1\} = A_p \qquad (5)$$

Визначимо $ind(a,p) = (p-1)/card(a,p)$, при цьому величина $card(a,p)$ дорівнює найменшому k , при якому $a^k \equiv 1 \pmod{p}$. Очевидно, якщо $k = p-1$ то $a^{p-1} \equiv 1 \pmod{p}$ та $a^{(p-1)/p_1} \neq 1 \pmod{p}$, для жодного простого дільника p_1 числа $p-1$. В тому випадку, коли $k < p-1$, то k завжди ділить $p-1$, та при цьому $ind(a,p) > 1$, а якщо a - первісний корінь, то $ind(a,p) = 1$. Припустимо, що a - первісний корінь простого числа p. Розглянемо основи теорії індексів в рекурсії:

$$\begin{aligned} &x(0) = 1, \quad x(1) = a, \\ &x(n+1) \equiv a x(n) \pmod{p} \end{aligned} \qquad (6)$$

при цьому n змінюється до $n = p-1 = \prod_{i=1}^{k} p_i^{\alpha_i}$. Обчислимо функцію Ейлера $\varphi(p-1) = \prod_{i=1}^{k_p} p_i^{\alpha_i - 1}(p_i - 1)$. Приведена функція визначає кількість чисел, які є взаємно простими з $p-1$. В рекурсії (1) в $x(n)$, величину n будемо називати індексом, а $x(n)$ лишком по модулю p. Очевидно, що якщо a - первісний корінь числа p, то індекс пробігає всі значення від 1 до $p-1$. Зрозуміло, що між індексами та лишками для кожного a, яке є первісним коренем даного простого числа p, існує взаємно однозначна відповідність відносно $p-1$та навпаки. Припустимо, що відома множина всіх первісних коренів:

$$\{a_1, a_2, a_3, ..., a_{\varphi(p-1)}\} \qquad (7)$$

Будемо вважати, якщо $a = a_1$, то $x(n)$ в (1) буде пробігати усі елементи тієї ж самої множини значень, але в іншій послідовності. В загальному випадку, простого алгоритму пошуку цієї послідовності не існує. На основі теореми Ейлера про первісні корені справедлива наступна теорема:

Теорема 2. Якщо в $x(n)$ індекс n не ділиться на жодний простий дільник $p-1 = \prod_{i=1}^{k} p_i^{\alpha_i}$, то лишок $x(n) \equiv a_1$ є первісним коренем p [12]. Доведення випливає з теореми Ейлера про первісні корені. Очевидно, що в таких випадках n - взаємно просте число з $p-1$, а тому в рекурсії $x(n+1) \equiv ax(n) \pmod p$ таких чисел, тобто первісних коренів завжди буде $\varphi(p-1)$. Звідси випливає, що якщо в послідовності $x(n)$, n ділиться на число k, яке ділить $p-1$, то $x(n)$ не є первісним коренем p, а це означає, що коли $x(n) = a$, то $ind(a, p) > 1$. Таким чином знаходимо найбільше значення k, при якому дане число ділить n в $x(n)$. Тоді присвоюємо $ind(a, p) = k$, а $card(a, p) = (p-1)/ind(a, p)$, а тому справедливо, що $a^{(p-1)/k} \equiv 1 \pmod p$. Таким чином справедлива теорема.

Теорема 3. Якщо в послідовності $x(n)$ обчислення на основі первісного кореня, а індекс n ділиться на максимальне число k то $ind(a, p) = k$, а $card(a, p) = (p-1)/k$. Дана теорема справедлива для будь-якого первісного кореня a_j з множини усіх первісних коренів $\{a_1, ..., a_j, ..., a_{\varphi(p-1)}\}$. На основі приведених міркувань можливо сформулювати теорему

Теорема 4. В множині $\{1, 2, 3, ..., p-1\}$ для кожного первісного кореня a_i в рекурсії Ферма *формула (3),* для будь-якого можливого дільника l числа $p-1$, знайдеться множина чисел $\{a_{1,1}, ..., a_{1,\varphi((p-1)/l)}\}$ які є лишками рекурсії по модулю р, індекси яких $ind(a_{1,i}, p) = l$ та $(p-1)/l = card(a_{1,i}, p)$, при цьому у відповідній системі індексів кожний з них ділиться на l та l є їх найбільшим дільником. Справедливість теореми випливає з того, що всі числа множини $\{a_{1,1}/l, a_{1,2}/l, ..., a_{1,\varphi((p-1)/2)}/l\}$ взаємно прості з $\varphi((p-1)/l)$ та є породжуючими елементами відповідних підгруп групи лишків Fp^*.

Таким чином отримаємо множину чисел a, для яких $ind(a, p) = l$. Необхідно звернути увагу на те, що в приведеному аналізі вважалося, що найменший первісний корінь був відомий. В загальному випадку вибору множини послідовних простих чисел $[p_n, p_{n+M}]$, значення p_n та M можуть бути вибрані великими, а тому приведені обчислення методами комп'ютерного моделювання формування класів $P(a, i, x)$ та обчислення констант $c(a, i, x)$ можуть значно ускладнюватися у зв'язку з тим що для кожного наступного простого числа необхідно знаходити найменший первісний корінь. При відсутності такої інформації пошук найменшого первісного кореня може значно ускладнити обчислення[15].

Таким чином, звідси можна зробити висновок, що $p-1 = \prod_{i=1}^{k} p_i^{\alpha_i}$ фактично визначає цілу множину різних дільників $\{l_1, l_2, ..., l_\varphi\}$. Значення $l_1 = 1, ..., l_\varphi = p-1$ такі, що кожне l_j, на основі теореми (3), визначає $\varphi((p-1)/l_i)$ та $\{a_{1,j}, a_{2,j}, ..., a_{\varphi((p-1)/l_i),j}\}$ – множину взаємно простих між собою чисел таких, що $ind(a_j, p) = l_j$ та $card(a_{l,j}, p) = (p-1)/l_j$. Закон розподілу $a_{2,j}$ для кожного дільника l_j на множині $\{1, 2, ..., p-1\}$ невідомий у множині всіх $ind(a, p)$ для кожного p є досі не розв'язаною математичною проблемою. Все ж таки можливо припустити, що такий закон існує для всіх простих чисел p, але для чисел $p = 4k+1$ закон розподілу індексів буде значно відрізнятися від закону розподілу для простих чисел типу $p = 4k+3$.

Необхідно відмітити, що $ind(a, p)$ діляться на два класи значень a. В один клас будемо відносити ті a, для яких $ind(a, p) = 2l+1$, $l \in \{0, 1, 2, ..\}$, а ті a, *для яких* $ind(a, p) = 2l$,

$l \in \{0,1,2,..\}$ - в другий клас. Випадок, коли $ind(a,p)=1$ відноситься до класу $ind(a,p)=2l+1$ при $l=0$, він радикально відрізняється від випадку $ind(a,p)=2l$. Прийнято вважати, якщо $ind(a,p)=2l$, то a є квадратичним лишком, в той час коли $ind(a,p)=2l+1$, то a не є квадратичним лишком. Кількість квадратичних лишків та неквадратичних лишків однакова - $(p-1)/2$, проте їх розподіл на множині $\{1,2,...,p-1\}$ досить різний. Розглянемо випадок $ind(a,p)=1$. Знайдемо розподіл первісних коренів за величиною відстані між ними. Легко довести, що середня відстань між первісними коренями визначається виразом $(p-1)/\varphi_1(p-1)$. Необхідність пошуку такого закону обумовлена в першу чергу гіпотезою Артіна та необхідністю пошуку чисел a, при яких структура класу $P(a,1,x)$ та значення константи відрізняються від приведених раніше випадків.

Термін: розподіл первісних коренів простого числа, необхідно розглядати з різ- них точок зору, а тому не слід виключати можливість застосу- вання ймовірнісних мето методів. Припустимо, що задане просте число p з множини $[p_n, p_{n+M}]$: $A_p=\{1,2,3,...,n-1,n,n+1,...,p-2,p-1\}$. Простий аналіз цієї множини свідчить що при $a=1$ або $a=p-1$, то вони не можуть бути первісними коренями на основі тривіальної причини - $card(1,p)=1$, а $card(p-1,p)\equiv 2 \pmod p$ для будь-якого p, а тому $ind(a,p)=p-1$ та $ind(p-1,p)=(p-1)/2$, і крім того, це виключні елементи подібної множини для будь-якого іншого простого числа. Якщо розглядати будь-яке інше число a з цієї множини, то оцінити ймовірність того, що a - первісний корінь p досить складно, і її міра, при зростанні величини p, зростає за експонентою.

Все ж таки, існують прості ідеї аналізу законів формування таких оцінок. Згідно з теорією Ейлера, кількість первісних коренів простого числа p визначається функцією Ейлера $\varphi(p-1)=\prod_{i=1}^{k_p} p_i^{\alpha_{i-1}}(p_i-1)$, тому можливо використати оцінку $p(a=a_i(p))=\varphi(p-1)/((p-3)-k_p)$, де k_p - кількість квадратів в A_p, $\{1,p-1\}\notin A_p$. Розподіл первісних повинен давати оцінку величини найменшого первісного кореня, в літературі відомі спроби отримання таких оцінок[11], але це є досить складною проблемою.

Оскільки для кожного p кількість первісних коренів дорівнює $\varphi(p-1)$, то середня відстань між первісними коренями буде $(p-1)/\varphi_1(p-1)$ при умові, що розглядаються випадки, коли найменший первісний корінь не є великим. Однією з таких властивостей можна вважати закони розподілу відстані між суміжними первісними коренями та закони розподілу множин первісних коренів на інтервалах певної величини. Розглянемо універсальну програму обчислення всіх первісних коренів простих чисел типів $4k+1$ та $4k+3$ з різними значеннями $\omega(p-1)$ на основі універсального алгоритму обчислення їх первісних коренів. При цьому для кожного простого числа, множина всіх первісних коренів розподіляється в систему упорядкованих підмножин, кожна з яких включала первісні корені, відстань між якими дорівнювала послідовно $1,2,3,...n,...$. При цьому системно досліджувались закони розподілу для всіх типів та класів простих чисел. Було виявлено, що у всіх випадках математична форма закону розподілу мала один і той самий вигляд. Графічний аналіз привів до висновку, що розподіл має експоненційну форму, параметри якої залежать від властивостей відповідних простих чисел. Було доведено, що відстань l між первісними коренями має експоненційну форму імовірнісного закону розподілу :

$$f_p(l)=\lambda_{qp}e^{-q\lambda pl} \quad \text{для} \quad p=4k+1 \ \& \ p=4k+3 \tag{8}$$

Розглянемо довільно обрану систему послідовних восьми простих чисел:

Таблиця 1.

Структура розкладання $p-1$ на прості множники

p	Розкладання p	$p-1$	Розкладання $p-1$	$\varphi(p-1)$
2423	$4\cdot 605+3$	2422	$2\cdot 7\cdot 173$	1032
2437	$4\cdot 609+1$	2436	$2^2\cdot 3\cdot 7\cdot 29$	672
2441	$4\cdot 610+1$	2440	$2^3\cdot 5\cdot 61$	960
2447	$4\cdot 611+3$	2446	$2\cdot 1223$	1222

2459	$4\cdot614+3$	2458	$2\cdot1229$	1228
2467	$4\cdot616+3$	2466	$2\cdot3^2\cdot137$	816
2473	$4\cdot618+1$	2472	$2^3\cdot3\cdot103$	816
2477	$4\cdot619+1$	2476	$2^2\cdot619$	1236

Експоненційний закон розподілу відстані між первісними коренями

Аналіз приведених для прикладу простих чисел свідчить про те, що формування первісних коренів та їх розподіл значно відрізняються навіть для послідовно розташованих простих чисел. Кількість первісних коренів коливається досить в широких межах при тому, що різниця між приведеними простими числами незначна. Даний елементарний факт став фундаментальною основою для пошуку законів, згідно з якими над такими множинами послідовних простих чисел узагальнені константи Артіна приймають одні і ті самі значення. Якщо значення M зафіксувати, при умові що його величина забезпечує точність оцінювання, то тоді важливо знайти математичне обґрунтування такої стійкості отриманих оцінок[6,8]. Фактично формування класів $P(a,i,x)$ та констант $c(a,i,x)$ для усіх значень $i=ind(a,p)$ можливо трактувати як процес проектування системи характеристик простих чисел над множиною $[p_n, p_{n+M}]$. При цьому якість оцінок констант Артіна не залежить від p_n, але значною мірою залежить від величини M[8]. Відстань між послідовними первісними коренями будь-якого простого числа розподілена відповідно до експоненційного закону. Математичне обґрунтування експоненційної форми імовірнісного закону розподілу відстані між первісними коренями будь-яких простих чисел $p>10^3$, носить непростий характер. Коректність такої гіпотези випливає з того, що процеси формування первісних коренів є пуасоновськими[16]. Таке твердження справедливе, тому що формування $ind(a,p)$ відбувається під впливом значної кіль- кості факторів, які є незалежними між собою та при цьому вплив кожного з них незначний, що приводить до формування простих чисел, а тому справедлива теорема.

Теорема 4. Для будь-якого простого числа *p,* множина первісних коренів за величиною відстані між послідовними первісними коренями між ними має показникову форму закону,

$$f_p(l)=\lambda_p e^{-\lambda_p l}$$

Відмітимо, що статистична оцінка параметру λ_p буде коректною тільки при умові, що відомі оцінки значень усіх первісних коренів простого числа *p,* тобто множина $\{a_1,a_2,...,a_{\varphi(p-1)}\}$. При цьому можна стверджувати, що чим більше просте число «гладке», тим менше $\varphi(p-1)$, а відповідно і λ_p. Таким чином, якщо міра гладкості простого числа p_k більше за міру гладкості простого числа p_{k+1}, то справедлива нерівність $\lambda_{p_k}<\lambda_{p_{k+1}}$. Необхідно звернути увагу на ще одну важливу властивість первісних коренів, яка пов'язана з існуванням внутрішніх циклів первісних коренів, які виникають в процесах реалізації рекурсивної функції при переході до іншого первісного кореня обраного простого числа *p.*

Таблиця 2

. Розподіл відстані між первісними коренями

Відстань	p=2423	p=2437	p=2441	p=2447	p=2459	p=2467	p=2473	p=2477
1	444	189	377	610	614	281	274	617
2	244	126	228	306	306	162	178	304
3	147	86	135	150	152	121	114	158
4	87	58	94	80	79	89	68	86
5	48	34	46	38	36	61	68	38
6	24	32	32	19	19	27	46	8
7	12	24	16	9	14	19	22	10
8	14	10	14	4	2	20	16	6
9	4	8	6	3	3	10	8	6
10	4	6	2	1	1	14	6	2
11	2	6	2	1	1	2	10	

12		2	6			5	2	
13		2				1	1	
14		2				1	2	
15		2				1		
16	1	2				1		

Можна стверджувати, що чим більш гладке $p-1$, тим λ_p менше. Оскільки термін «$p-1$ гладке число» не має чіткого визначення, то в теорії чисел[12,13] приведені результати будемо розглядати як експериментальний факт, який можливо змістовно обгрунтувати, проте детальний математичний аналіз для коректного доведення всіх теорем, пов'язаних з розподілом первісних коренів та індексів будь-якої величини, подібний до аналізу, приведеного в роботах Ердеша-Каца[14] та E.Kowalski[15], буде предме- том окремої роботи. Імовірнісне доведення експоненційного закону розподілу $f_p(l)$ буде предметом окремого дослідження, паралельного з дослідженням законів розподілу не тільки первісних коренів, але і індексів $ind(a, p) > 1$. Ця проблема в теорії чисел досить складна і при цьому відсутні достатньо глибокі результати[13].

Поглиблення експоненційного закону розподілу відстані між суміжними первісними кореняими пов'язане ще з однією властивістю розподілу первісних коренів та індексів, яка полягає в тому, що для будь-якої множини послідовних простих чисел $[p_n, p_{n+M}]$, при умові, що M не менше ніж певна величина (прийнято $M = 500000$) тоді знайдеться таке число *Q*, що для кожного простого числа *p* з цього інтервалу, множина $\{1, 2, 3, \ldots .. p-2, p-1\}$ покривається послідовно системою таких інтервалів, кожен інтервал містить однакову кількість первісних коренів. Це твердження можна перенести і на індекси до певної величини, яка залежить від величини *M*. Більш глибокий аналіз теорії такого покриття буде розглянутий як рівномірний закон розподілу первісних коренів.

Висновки

Обчислення первісних коренів для будь-якого простого числа *p* можна впевнено віднести до класу складних математичних проблем, у зв'язку з тим, що на даний момент не існує ефективного алгоритму пошуку найменшого первісного кореня[17]. Як було відмічено раніше, в основі будь-якого алгоритму знаходиться рекурсивна функція Ферма. Рекурсивна функція (1) визначає необхідну, але не достатню умову. Для щоб рекурсія була і достатньою умовою, необхідно знайти мінімальний первісний корінь, в загальному випадку така інформація як правило відсутня.

Список використаної літератури

1. Artin E., The Collected papers. Addison-Wesley publishing company.INC 1965.
2. Hasse H., Uber die Artinische Vernutung und Verwandte Dichtefragen. Annales Academiae Scientiarum Fennicae, A. I. Math.-Phys, 116 (1952).
3. Bilharz H. Primitivisoren mit vorgegenbener Primitivwurzel, Math. Ann. 114 (1937) 476-492.
4. Hooley Ch., On Artin's conjecture. Journal fur die reine und angewandte Mathematics. Sonderabruck aus Band 225, 1967, Seite 209 bis 220.
5. Vostrov G., Ponomarenko o., Statistical of the smooth number properties and their search. International Conference –Computer analysis and data modeling, Minsk, 2019.
6. Vostrov G., Opiata R., Probabilistic methods in computer simulations of the formation of classes of primes and estimations of the constant of the generalized Artin's hypothesis. JMLR Workshop and Conference Proceedings 1:1-13, 2020, 9th Symposium on COPA.
7. Vostrov G., Opiata R., Modeling the processes forming classes of prime numbers and evaluating the constants of Artin's generalized hypothesis on the basis of analytical for computer methods of their formation, ISSN 2221-3805, Електротехнічні та комп'ютерні системи. 2021, N 34 (110), National University Odessa Polytechnic.
8. Crandall R., Pomerance C., Prime Numbers. A Computational Perspective. Springer, 2005.
9. Manin Y., Panchishkin A., An Introduction to Modern Number Theory. Springer, 2005.
10. Pomerance C., Rassias Th. M., Editors. Analytic Number Theory, Springer, 2015.
11. Murty Ram M., Problems in analytic Number Theory. Springer. 2008.
12. Lacasa L., Luque B., Gomes I., Miramontes O., On a Dynamical Approach to Some Prime Number Sequences. Entropy. MDPI.2021.
13. Tenenbaum G., Introduction to analytic and Probabilistic Number Theory. American Mathematical Society, 2015.

14. Granville A., Smooth numbers: computational number theory and beyond Algorithmic Number Theory MSRI Publications Volume 44, 2008 .

15. Kac M., Statistical the independence in probability, analysis and number theory, the carus Mathematical Monographs Number 12, JOHN WILEY and SONS, inc.1959.

16. Kowalski E., Arithmetic Randonnee. An Introduction to probabilistic number theory. Versus of May,2021

17. Kevin J. McGown, Jonathan p. Sorenson. Computational of the least primitive roots. arXiv:2206.14193v1 [Math NT] 28 Jun 2022.

STATISTICAL AND ALGEBRAIC PROPERTIES OF THE DISTRIBUTION OF PRIMITIVE ROOTS IN SETS OF CONSECUTIVE PRIMES

G. Vostrov, R. Opiata, M. Stavratii, O. Shcherbaniuk
National University «Odessa Polytechnic»

Abstract. *The justification of the necessity of full qualitative information about the algebraic properties of primitive roots in the sets of consecutive primes is given, taking into account the area of their location in the set of all primes and its cardinality. It is proven that with a significant deepening of the location of the set of consecutive primes, the value of* $\omega(p-1)$ *smoothly but systematically increases to such an extent that at a certain stage of the deepening process the average distance between the primitive roots of such sets of consecutive primes smoothly increases to a certain extent. The foundations of mathematical estimation of the entropy of probabilities of changes in the statistical properties of the mathematical expectation of the average distance between the primitive roots are developed. The methods of computer modeling of processes of formation of statistical laws of distribution of primitive roots in such systems of consecutive prime numbers of significant power are created.*

Keywords: *distribution of primitive roots; Artin's constants; classes of prime numbers; distribution of indices modulo prime; distances between primitive roots.*

Отримано 15.09.2022

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

Востров Георгій Миколайович, кандидат технічних наук, доцент кафедри прикладної математики та інформаційних технологій Національного університету «Одеська політехніка». Проспект Шевченко, 1, Одеса, Україна.

ORCID ID: 0000-0003-3856-5392

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

Опята Роман Юрійович, аспірант кафедри прикладної математики та інформаційних технологій Національного університету «Одеська політехніка». Проспект Шевченко, 1, Одеса, Україна.

ORCID ID: 0000-0001-5806-9615

Maksym Stavratii, undergraduate student of the Department of Applied Mathematics and Information Technologies, National University «Odesa Polytechnic». Shevchenko ave., 1, Odessa, Ukraine.
E-mail: maxim.stavratii@gmail.com, mob. +380964879273

Ставратій Максим Олександрович, студент бакалаврату кафедри прикладної математики та інформаційних технологій Національного університету «Одеська політехніка». Проспект Шевченко, 1, Одеса, Україна.

Olexandr Shcherbaniuk, graduate student of the Department of Applied Mathematics and Information Technologies, National University «Odesa Polytechnic». Shevchenko ave., 1, Odessa, Ukraine.

Щербанюк Олександр, студент магістратури кафедри прикладної математики та інформаційних технологій Національного університету «Одеська політехніка». Проспект Шевченко, 1, Одеса, Україна.