UDC:

СИСТЕМНИЙ АНАЛІЗ РОЗПОДІЛУ ПЕРВІСНИХ КОРЕНІВ ПРОСТИХ ЧИСЕЛ В ГІПОТЕЗІ АРТІНА

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

Анотація. *Приведені результати дослідження законів розподілу первісних коренів простих чисел p на множинах натуральних чисел та їх зв'язок з гіпотезою Артіна . Доведено системний характер формування класів простих чисел та узагальнених констант. Приведене повне обґрунтування законів формування класів простих чисел з певним значенням індексів та відповідних констант Артіна. Знайдені закономірності формування класів Артіна та доведено, що вони залежать від значної кількості факторів, пов'язаних з властивостями відповідних простих чисел. Приведено аналіз факторів та досліджені закономірності, які значною мірою впливають на процеси формування розподілу первісних коренів.*

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

Вступ

Гіпотезу Артіна стосовно розподілу простих чисел, для яких число a є первісним коренем, можна впевнено віднести до класу складних математичних проблем, розв'язання яких має фундаментальне теоретичне та прикладне значення. Незважаючи на велику кількість надрукованих наукових праць, присвячених її розв'язанню, досі відсутній повний аналіз отриманих результатів[1,2]. Для удосконалення математичної ефективності таких досліджень важливо довести якою мірою властивості числа a впливають на закони розподілу простих чисел, для яких дане число є первісним коренем. Перший крок в цьому напрямку зробили Артін, Хассе[3,4,] коли Артін в дискусії з Хассе запропонував обрати $a=2$ та знайти закон розподілу простих чисел, для яких a є первісним коренем. В основі теорії, яка розвивається знаходиться теорія первісних коренів множини усіх простих чисел P. Число 2 є первісним коренем певної множини простих чисел, та при цьому вона має певну щільність $A(2)$ в множині P, яка може трактуватися як ймовірність того, що для простого числа p, число 2 є первісним коренем. Проблема аналізу $A(a)$ для будь-якого числа, яке не дорівнює плюс-мінус одиниці та не є квадратом має ідентичне трактування. Артін в 1927 році висловив гіпотезу, що для будь-якого числа a, $A(a)=A(2)$, що може бути обчислене згідно з виразом $A(2)=\prod(1-1/q(q-1))$, де q пробігає множину усіх простих чисел. Така думка була висловлена та проаналізована в співпраці з Хассе та приведена в роботах[3,4]. В роботі[5] відзначено, що трактування приведеної

формули Артіна та Хассе при $a=5$ носить помилковий характер, тому що $A(5)>A(2)$ приблизно на п'ять відсотків.

Основи поглиблень досліджень гіпотези носять багатогранний характер. В гіпотезі Артіна в загальному випадку використовується рекурсивна функція, яка є основою малої теореми Ферма [1,6,8], згідно з якою число a, буде первісним коренем простого числа p, коли в рекурсивній функції: $x(0)=1,\ x(n+1)\equiv ax(n)\ (\mathrm{mod}\ p)$ виконується умова $a^{p-1}\equiv 1\ (\mathrm{mod}\ p)$, і тоді кількість ітерацій рекурсії дорівнює $p-1$. При цьому необхідно взяти до уваги те, що в загальному випадку в процесі обчислень може бути отримане число один, коли кількість ітерацій в приведеній рекурсивній функції буде менше числа $p-1$. Якщо показник степені при цьому дорівнює k і $k<p-1$, то $card(a,p)=k$ це довжина рекурсії. Легко довести, що $p-1$ завжди ділиться на $k=card(a,p)$, а $ind(a,p)=(p-1)/card(a,p)$ прийнято називати індексом числа a по модулю p. Необхідно прийняти до уваги, що при усій простоті приведеної функції для довільних чисел a та p практично неможливо без обчислення згідно з її формулою визначити значення $ind(a,p)$. Це пов'язано з тим, що в загальному випадку просте число p може бути як завгодно великим. В той же час в сучасній теорії чисел, алгебрі, теорії динамічних систем надзвичайно важливо володіти повною інформацією стосовно поведінки цієї

рекурсивної функції при будь-яких значеннях числа *a* та простого числа *p*. Відсутність такої повної інформації може бути причиною широкого застосування методів апроксимації при розв'язувані значної кількості математичних проблем, які мають велике як теоретичне, так і прикладне значення.

Аналіз методів оцінювання констант Артіна.

Проблеми, до яких відноситься гіпотеза Артіна та множина фундаментальних задач сучасної математики, пов'язаних з теорією простих чисел і методами дослідження їх законів розподілу та узагальненням їх на прості ідеали в теорії алгебраїчних чисел[1], характеризуються значною мірою складності, що обумовило значну увагу до її розв'язання. Предметом аналізу було число 2 та множина усіх простих чисел P. Згідно з їх попереднім аналізом була запропонована формула для обчислення константи $A(2)$, яка визначала щільність, а можна сказати ймовірність розподілу простих чисел, для яких 2 є первісним коренем. При цьому була запропонована формула для обчислення числової характеристики оцінки $A(2)$, яка має наступний вигляд:

$$A(2) = \prod (1 - 1/q(q-1)), \qquad (1)$$

де добуток виконується по всій множині простих чисел $q \in \mathrm{P}$. Обґрунтуванням такої форми апроксимації щільності простих чисел $q \in \mathrm{P}$, для яких $a = 2$ є первісним коренем, стали наступні роздуми Артіна та його партнера в проведеному аналізі. Кожен співмножник є оцінкою ймовірності наступної події. Число $1/q(q-1)$ є ймовірністю того, що для простого числа *p* виконуються наступні умови. Число $p-1$ ділиться на просте число *q* та при цьому одночасно справедливе рівняння

$$2^{(p-1)/q} \equiv 1 \pmod{p} \qquad (2)$$

А це означає що 2 не є первісним коренем для простого числа *p*. Необхідно відмітити, що згідно з теоремою Діріхле[4] для простих чисел *p* ймовірність, що $p-1$ ділиться на *q* дорівнює $1/q(q-1)$. Справедливість теореми Діріхле не визиває сумніву, та крім того вона була перевірена нами як теоретично так і методами комп'ютерного моделювання. В той же момент, взяти до уваги, що ймовірність того, що 2 не є первісним коренем для простого числа p на думку Артіна дорівнює $1/q$, якщо справедлива рівність $2^{(p-1)/q} \equiv 1 \pmod{p}$. При цьому можна довести, що це помилкова оцінка в загальному випадку.

Необхідно взяти до уваги, що можлива рівність $2^{(p-1)/m} \equiv 1 \pmod{p}$, і при цьому m є добутком простих чисел $q_1^{i_1},...,q_k^{i_k}$, які ділять $p-1$. Звідси випливає, що у такому випадку одночасно справедливо $2^{(p-1)/q_1} \equiv 1 \pmod{p}$,..., $2^{(p-1)/q_k} \equiv 1 \pmod{p}$. Усі такі випадки протирічать реальним методам обчислення $ind(a,p)$, а тому необхідно враховувати ймовірність таких випадків. Множина таких випадків не прийнята автором до уваги, а тому ймовірність $1/q$ оцінена автором некоректно. Про те на думку автора ці дві випадкові події незалежні, а тому добуток $1/q(q-1)$ є ймовірність того, що *a* не є первісним коренем для простого числа *p*. Звідси ймовірність протилежної події дорівнює $1/q(q-1)$. Взявши добуток по всім простим числам, ми отримаємо формулу, запропоновану автором. Обчислення добутку ще меншою мірою обґрунтовано. Необхідно звернути увагу на те, що кожний наступний множник наближається до одиниці для простих чисел порядку 10^3, що зовсім протирічить процесам формування класу $P(2,1,x)$ на множині простих чисел, при цьому $a = 2$, $ind(a,p) = 1$ та $x = p \in [p_n, p_{n+M}]$ - множина послідовних простих чисел.

Необхідно відмітити, якщо справедливість теореми Діріхле не визиває жодного сумніву, то оцінку ймовірності події пов'язаної з фактом, що $a = 2$ не є первісним коренем простого числа *p*, при умові Артіна неможливо вважати коректним. Даний факт теж був перевірений на основі математичного моделювання [6]. Найбільша помилка пов'язана з усім добутком в тому випадку коли $a = 4k+1$. Білгарц[5] в 1937 році на основі обчислень відмітив що $A(5) > A(2)$, не привівши обґрунтування для даного факту. В роботі [6] було доведено, що такий результат правильний, а потім в роботі[9] приведене обґрунтування математичної теорії формування констант Артіна при різноманітних властивостях числа *a*, відмінного від $a = 2$. В наступному розділі, в теоремі 3, приведене обґрунтування даного факту та деяких інших фактів стосовно того що можлива нерівність $A(8) < A(2)$ та багато інших фактів.

В 1967 році з'явилася робота К.Хоолі [7], в якій вперше була розглянута можливість доведен- ня коректності гіпотези Артіна чітко

математич- ними методами на основі теорії решета. Робота була відмічена нагородою університетом Кембриджу (Великобританія). В першій роботі були певні недоліки, які були виправлені в монографії[8], але проблема залишилася далекою від розв'язання. Автор не вийшов за межі випадку оцінки $A(2)$. Крім того, як було відзначено вище, були отримані оцінки константи Артіна для чисел $a=5,\ a=13,\ a=17$ та при інших значеннях числа *a*. В роботах[6,9] були отримані оцінки $A(5)=0.3837$, $A(13)=0.3764$, $A(17)=0.3764$. В дійсності, результати вірні, не зважаючи на те, що існувала помилкова точка зору, що для усіх значень *a* константа Артіна повинна приймати одне і теж значення, що є значною помилкою і в даний час. В роботі [9] було показано, що при $a=8$ та при $a=27$ та інших кубах простих чисел константа Артіна має значення 0.224.... Необхідно відмітити, що спектр значень констант Артіна значно ширший та їх коливання мають значно більше фундаментальне значення.

Гіпотеза Артіна стала фактором, який привів до формування цілого спектру досліджень [9-17] в теорії чисел, теорії рекурсивних функцій, математичній теорії динамічних систем та методах кодування та захисту інформації. Ядром системи широкомасштабних досліджень стала теорія чисел, розпочинаючи з натуральних та простих чисел. Наступним поглибленням досліджень до рівня алгебраїчних чисел із застосуванням різноманітних форм їх представлення стало створення принципово нових методів дослідження складних проблем сучасної математики на основі аналітичних, алгебраїчних, та комп'ютерних технологій їх розв'язання. Такі процеси обумовили необхідність створення системних комбінованих технологій розв'язування проблем теорії чисел, які пов'язані з однієї сторони з теорією із поглибленням аналітичних та алгебраїчних методів, а з іншого боку - із розвитком комп'ютерних технологій розв'язування проблем сучасної математики.

Основи комбінованого системного методу аналізу та поглиблення методів розв'язування проблем, пов'язаних з гіпотезою Артіна, став цикл робіт [6,7,9]. В означених наукових роботах доведено, що для детального дослідження гіпотези Артіна необхідно паралельно використовувати методи алгебраїчної, аналітичної теорії чисел та методи комп'ютерного моделювання процесів формування класів простих чисел. При цьому будуть використовуватися довільні значення індексу, який будемо в дальше позначати $ind(a,p)$, при цьому *a* є будь-яке ціле число, яке є більшим за одиницю та *p* - просте число, а для індексу завжди справедлива нерівність $ind(a,p)>1$, якщо *a* не є первісним коренем простого числа *p*, та $ind(a,p)=1$ в тому випадку, коли *a* є первісним коренем простого числа *p*. Як було відзначено в приведених працях, завжди справедлива рівність:

$$p-1=card(a,p)ind(a,p) \qquad (3)$$

при цьому $card(a,p)$ - довжина циклу рекурсії $x(0)=1,\ x(n+1)\equiv ax(n)\ (\mathrm{mod}\ p)$, який закінчується, коли буде отримане значення, що дорівнює одиниці. В роботах [6,9] було доведено, що кожне число *a*, відмінне від плюс-мінус одиниці, є класифікатором множини усіх простих чисел при цьому множина всіх простих чисел P ділиться на систему множин, які не мають спільних чисел згідно наступному виразу, який описує множину простих чисел для яких $ind(a,p)=I$ та $P(a,i,x)=\{p\,|\,ind(a,p)=i\ \&\ p=x\in[p_n,p_{n+M}]\}$ і при цьому справедливо $P=\bigcup P(a,I,x)$. Квадратні числа не можуть бути первісними коренями, проте вони можуть створювати класифікацію простих чисел, в якій такі класи мають тільки парні індекси, які в даній роботі розглядатися не будуть. Необхідно звернути увагу на змінну *x* у всіх множинах простих чисел $P(a,i,x)$ та оцінках констант Артіна $c(a,i,x)$, яка відзначає, що ці оцінки отримані на множин простих чисел $x=p$, які належать до множини послідовних простих чисел $[p_n,p_{n+M}]$. В тих випадках, коли будуть розглядатися оцінки, отримані на множині всіх простих чисел, символ *x* буде відсутній.

У відмічених роботах доведено, що якісні методи розв'язання гіпотези Артіна та їх застосування для обчислення узагальнених констант Артіна необхідно володіти перш за все законами розподілу первісних коренів будь-яких простих чисел *p* з врахуванням властивостей $p-1$. Необхідність виконання цієї вимоги обумовлена рядом важливих факторів. Перш за все, у зв'язку з тим, що було доведено, що при різних значеннях *a* та індексу $i=1$ константи $c(a,1,x)$ приймають різні значення, виникла необхідність детально дослідити як величина *a* та її властивості впливають на величину константи $c(a,1,x)$. Ще більш складна проблема пов'язана з дослідженням, від яких властивостей

a залежить величина константи. Одночасно було доведено, що для отримання оцінок констант $c(a,1,x)$, необхідно враховувати властивості різних простих чисел, які входять до множини послідовних простих чисел $[p_n, p_{n+M}]$ де p_n - найменше просте число з номером n в послідовності всіх простих чисел, при цьому в послідовності є M таких простих чисел. Для отримання такої інформації на даному етапі було вирішено обмежитися тільки первісними коренями, а тому виникла необхідність для простих чисел обчислювати їх первісні корні та дослідити закони їх розподілу і врахувати їх особливості в приведених множинах послідовних простих чисел.

Розширення гіпотези Артіна перш за все полягає в тому що класи простих чисел $P(a,i,x)$ мають глибокий зв'язок теоремою Діріхле стосовно арифметичної прогресії. Число *a* можна пов'язати з модулем m наступним чином. Розглянемо детально термін «узагальнена та розширена гіпотеза Артіна» означає, що для всіх $a \neq 1$ та $i = ind(a,p)$, об'єктом дослідження є властивості множин $\underset{x\to\infty}{P}(a,i,x)$. Кожна така множина пов'язана з системою арифметичних прогресій. Перш за все кожна множина $P(a,i,x)$ може бути описана наступним чином $P(a,i,x) = \{p \mid ind(a,p) = i\}$ при $x = p$. Число *a* можна пов'язати з модулем m наступним чином. Призначимо $m = 4a$, якщо *a* по модулю 4 не дорівнює одиниці та $m = 2a$, якщо $a = 4k+1$. Обґрунтування такого правила пов'язане з теорією модулей в теорії чисел[10-14]. Для m знаходимо систему лишків, які взаємно прості з модулем. В даній роботі приведений факт, згідно з яким усі класи $P(a,i,x)$ діляться на систему арифметичних прогресій

$$P(a,i,x \mid km + m_{1,j}) \quad для\ \ i = 2k+1\ \ i\ \ m_{1,j} \in \{m_{1,1},...,m_{1,\varphi(N/2)}\} \tag{4}$$

$$P(a,i,x \mid km + m_{2,j}) \quad для\ \ i = 2k\ \ i\ \ m_{2,j} \in \{m_{2,1},...,m_{2,\varphi(N/2)}\} \tag{5}$$

Для коректно вибраного модуля m для різних a завжди формується система арифметичних прогресій. При цьому при збільшені a кількість різних прогресій в приведеній схемі зростає. Приведена модель апроксимації класів $P(a,i,x)$ арифметичними прогресіями являється першим кроком в поглиблені гіпотези Артіна. А це означає, що складність представлення цих множин та підкласів простих чисел $P(a,i,x \mid 4k + m_{1,j})$ та $P(a,i,x \mid k + m_{2,j})$ можуть значно відрізнятися [14].

Необхідно відмітити, якщо *a* - складне натуральне число, то структури класів приведених типів стають зовсім непередбачуваними. Наприклад при $a = 8$ та $a = 27$ константа Артіна має порядок $0.224...$, а це означає що константи Артіна для різних значень *a* можуть значно відрізнятися. При такому розширені гіпотези Артіна, шляхом опису системою арифметичних прогресій по модулю m класів з парними індексами $\{m_{2,1},...,m_{2,\varphi(N/2)}\}$ поведінка класів $P(a,2i,x)$ значно відрізняється від класів з непарними індексами $\{m_{1,1},...,m_{1,\varphi(N/2)}\}$, з точки зору значень лишків і при цьому структури арифметичних прогресій значно відрізняються, а тому будуть предметом окремої роботи.

Розподіл простих чисел в множинах послідовних простих чисел обмеженої величини

Розширення та узагальнення гіпотези Артіна про формування класів простих чисел $P(a,i,x)$ та оцінювання констант $c(a,i,x)$ в загальному випадку пов'язане з необхідністю обчислювати їх значення так само для значень $i = ind(a,p) > 1$, тому що при різних значеннях *a* величина індексу $ind(a,p)$ має важливе значення для обґрунтування властивостей поведінки $c(a,1,x)$. Наприклад, коли *a* просте число та $a = 4k+1$ та $a = 5$ давно було відомо, що $c(5,1,x) > c(2,1,x)$ [8,9]. Для усіх оцінок констант Артіна для $c(5,1,x)$ простих чисел $x = p$, які належать до будь-якої множини послідовних простих чисел . $[p_k, p_{k+M}]$. при умові, що $M = 10^5$ теж виконується приведена нерівність. При цьому була обґрунтована нерівність з точки зору теорії чисел при умові, що значення константи були обчислені на таких множинах для приведених значень *M*. Доведено, що коли навіть $M = 1000$, то оцінки констант Артіна вже для перших двох десяткових знаків можуть бути коректні і при цьому нерівність справедлива. Нижче буде приведений детальний аналіз процесів які обумовлюють такі властивості певного класу констант Артіна при умові що $a = 4k+1$.

Стосовно приведеної множини послідовних простих чисел необхідно привести результати

аналізу їх властивостей з точки зору зв'язку між простими числами цієї множини простих чисел та розподілом їх первісних коренів з врахуванням зв'язків між ними. Розглянемо представлення простих чисел p по модулю чотири. Якщо $p=4k+1$ або $p=4k+3$, то при цьому необхідно прийняти до уваги що розподіл первісних коренів таких чисел значно відрізняється. **В теоремах (1) та (2)** сформульовані елементарні властивості первісних коренів таких простих чисел. Вибір елементарних властивостей може стати стимулом для поглиблення дослідження.

Нескладно довести, що коли $p=4k+1$то всі його первісні корені володіють наступними тривіальними властивостями.

Теорема 1. Для будь-якого простого числа $p=4k+1$ та множини $\{1,2,3,...,p-2,p-1\}$ справедливо:

1. якщо число a - первісний корінь простого числа p, то $p-a$ також його первісний корінь;

2. якщо a_1 та a_2 - первісні корені простого числа p, то $a_1 \cdot a_2$ не може бути первісним коренем p.

Одночасно динаміка розташування первісних коренів простого числа $p=4k+3$ в значній мірі інша.

Теорема 2. Для будь-якого простого числа $p=4k+3$ та множини $(1,2,3,...,p-2,p-1)$ справедливо:

1. усі первісні корені a розташовані асиметрично відносно середини множини:

2. якщо a_1 та a_2 - первісні корені простого числа p, то $a_1 \cdot a_2$ не може бути первісним коренем p

Властивості тривіальні, проте міра асиметрії розподілення первісних коренів для $p=4k+3$ до цього часу невідома і не зрозуміло, якою мірою вона впливає на процеси формування констант Артіна. Одночасно невідомо, як симетричне розміщення первісних коренів $p=4k+1$ призводить до стійкості оцінок. Елементарні теореми свідчать про те що, в приведеній множині послідовних простих чисел дані прості числа по різному впливають на сумарний розподіл первісних коренів та при цьому для будь-якої множини $[p_n, p_{n+M}]$ послідовних простих чисел, значення констант Артіна зберігаються з точністю, яка визначається величиною числа M. Те що пункти (2) співпадають, зовсім не означає, що динаміка формування класів простих чисел $P(a,i,x)$ на простих числах типу $p=4k+1$ та $p=4k+3$ не може радикально не відрізнятися. Перший пункт свідчить про те, що існує різниця між процесами формування таких класів на простих числах таких типів. Відмітимо, що ймовірності таких простих чисел однакові. Поки що відсутні дані, яким чином компенсується ефект асиметрії в розподілі первісних коренів.

Жодна з приведених тривіальних теорем не має фундаментального впливу на процеси формування важливої інформації відносно законів розподілу первісних коренів на усій множині послідовних простих чисел не залежно від вибору p_n, але при умові що M не менше певної величини. Необхідно відмітити, що між простими числами типів $p=4k+1$ та . $p=4k+3$. існує досить глибока різниця, яка була об'єктом дослідження протягом довгого часу з точки зору їх розподілу в множині усіх простих чисел. В даний час уже доведено, що ці класи простих чисел однаково ймовірні [15,16,17].

Розподіл простих чисел $P_1=\{p \mid p=4k+1 \mid k \in N\}$ та $P_3=\{p \mid p=4k+3 \mid k \in N\}$ такий, що при цьому $|P_1|/|P|=|P_3|/|P|=1/2$ та закономірності розподілу коливань $p=4k+1$ і $p=4k+3$ на множині усіх простих P не досліджені в повній мірі, проте можна вважати, що рівність має граничний характер у вигляді:

$$\lim_{x\to\infty}|P_1(x)|/|P(x)|=\lim_{x\to\infty}|P_3(x)|/|P(x)|=1/2 \quad (6)$$

Відмітимо, що на множинах послідовних простих чисел $[p_n, p_{n+M}]$такого типу відношення можуть відхилятися «суттєво» від $1/2$. Характер такого типу відхилень в ймовірнісній моделі розв'язування «узагальненої гіпотези Артіна» такого типу коливання необхідно приймати до уваги при зміні значень n та M в $[p_n, p_{n+M}]$.

Тепер необхідно розглянути аналіз причин, які приводять до необхідності аналізу розподілу не тільки первісних коренів, але і індексів $ind(a,p)$. Вище була звернута увага на нерівність $c(5,1)>c(2,1)$. Взагалі справедлива більш загальна нерівність $c(4k+1,1)>c(2,1)$. Причиною її появи є наступна теорема.

Теорема 3. Для всіх $a=4k+1$ $c(4k+1,(4k+1)2l+(4k+1),x)=0$ для усіх $l \geq 0$, а це означає, що усі індекси , які обчислюються за приведеною формулою, дорівнюють нулю та при цьому завжди виконується рівність:

$$\sum c(a,2m+1,x)=1/2$$

Доведення теореми основане на простій властивості узагальнених констант Артіна з парними та непарними індексами. Легко довести, що для будь-якого a справедлива рівність:

$$\sum c(a,2m+1,x)=\sum c(a,2m,x)=1/2 \quad (7)$$

Якщо деяка множина непарних індексів більших за одиницю дорівнює нулю при умові, що завжди $c(a,i)>c(a,j)$, якщо $i>j$, тоді сума буде дорівнювати $1/2$ тільки при умові, що $c(a,1)>c(b,1)$, якщо $p=4k+1$ та b число типу $4k+3$. Доведення існування таких індексів, при яких відповідні константи дорівнюють нулю приведені в роботі[7].

Таким чином приходимо до висновку, що розширення та узагальнення гіпотези Артіна має суттєве значення для поглиблення наших знань в теорії чисел та теорії рекурсії. Детальний аналіз математичних проблем, пов'язаних з гіпотезою Артіна, свідчить про те, що структури класів $P(a,i,x)$ в значній мірі залежать від властивостей числа *a* та простих чисел *p* при їх взаємодії в процесі обчислень за допомогою рекурсивної функції динамічні властивості якої не досліджені при взаємодії *a* та *p* в процесах обчислення. Відсутність такої інформації стосовно глибинних процесів взаємодії між *a* та *p* при умовах складності *a* та великих значеннях *p* при значній складності $p-1$, приводить до практично непрогнозованих значень результатів обчислення як алгебраїчними методами, так і в процесах комп'ютерного моделювання. Необхідно більш детально обґрунтувати паралельне використання аналітичних методів та технологій комп'ютерного моделювання при детальному аналізі та розв'язуванні розширеної та узагальненої гіпотези Артіна. На основі аналітичних методів практично неможливо створити універсальний метод обчислення констант Артіна для будь-якого *a* у зв'язку з тим, що надзвичайно складно врахувати детально алгебраїчні властивості натуральних чисел *a* та властивості приведеної рекурсивної функції на множині усіх простих чисел. При цьому необхідно враховувати властивості простих чисел з точки зору розкладання $p-1$ на прості множники та враховувати динаміку зміни ймовірнісного закону розподілу простих чисел за величиною $\omega(p-1)$. Використання методів комп'ютерного моделювання процесів формуван- ня класів $P(a,i,x)$ та обчислення констант Артіна $c(a,i,x)$ в значній мірі обмежене не тільки обчислювальною складністю. В той же час практично неможливо врахувати усі проблеми, які можуть виникати при повномасштабному аналізі даної математичної проблеми. Перспек- тивність методу комп'ютерного моделювання процесів формування класів простих чисел з даним *a* та індексом *i* полягає в тому, що в універсальних програмних комплексах можливо тільки змінювати параметри при необхідності та отримувати результати моделювання. Така стратегія реалізована і в подальшому буде використана в даній роботі для створення системи аналізу розподілу первісних коренів.

Важливим фактом є просте обґрунтування причини того, що $c(5,1,x)>c(2,1,x)$ на будь-якому інтервалі $[p_n,p_{n+M}]$ простих чисел, як було Відмічено вище, обумовлено тим, що класи $P(a,i,x)$ можуть бути пустими при умові, що $i>1$ та *a* не є квадратом. Було доведено, що завжди $P(5,5,x)=\varnothing$ & $P(5,25,x)=\varnothing$ & ... і це вірно для всіх $a=4k+1$ та *a* не обов'язково просте число. ***Теорема 3*** обґрунтовує цей факт в загальному випадку. Проте необхідно звернути увагу на одну особливість даної теореми. Якщо $a=4k+1$- просте число 53, то $c(a,1,x)$ практично співпадає з $c(2,1,x)$ на основі тієї ж теореми у зв'язку з тим, що тільки для індексу $i=53$ справедливо $c(53,53,x)=0$. Наступний індекс, при якому буде справедливо $c(a,i,x)=0$ є $i=2\cdot 53+53=159$, а за ним значення індексу $i=4\cdot 53+53=265$ і так далі. В роботі Ch. D. Ambrose[18] проведене дослідження властивостей $ind(a,p)$, на основі яких приблизно справедливо $P(a,i,x)|=|1/i^2\cdot|P(a,1,x)|$. Тоді нескладно довести, що при такому допущені будуть приблизно справедливі наступні рівності: $|P(53,53,x)|=1/53^2\cdot|P(53,1,x)|$ та $|P(53,159,x)|=1/159^2\cdot|P(53,1,x)|$ і так далі. Тоді їх сума складає приблизно три десятитисячних від $P(53,1,x)$, а тому приведений ефект $c(5,1,x)>c(2,1,x)$ не реалізується, якщо *a* більше 53 при умові, що прості числа $x=p$ належать до множини $[p_n,p_{n+M}]$ або будь-якої іншої множини послідовних простих чисел з даною кількістю простих чисел. Це свідчить про те, що доля таких простих чисел незначна, а тому вона не може впливати на величину $c(4k+1,1,x)$, при умові $4k+1>53$. При цьому необхідно приймати до уваги **теорему (3)** та те, що буде доведено в

наступних роботах, існує практично безмежна кількість значень числа a при яких $c(a,1,x)=0.396...$

Необхідно відмітити, що не можливо виключити існування інших чисел а поведінка яких в даній рекурсивній процедурі формування класів простих чисел не приведе до подібних ефектів і в цьому полягає велика складність дослідження розширеної та узагальненої гіпотези Артіна. Така складність даної математичної проблеми при спробах узагальнити її на множину алгебраїчних чисел на основі простих ідеалів потребує повної інформації стосовно законів розподілу первісних коренів.

Величина числа a та його властивості обумовлені його розкладанням на прості множники в значній мірі впливають на класи простих чисел та відповідні узагальнені константи , які виникають в тих випадках коли необхідно дослідити структуру класів $P(a,i,x)$ для всіх значень $ind(a,p)$ та оцінити значення констант $c(a,i,x)$. Наприклад, якщо $a=128$, то виникає запитання стосовно величини $c(128,1,x)$. В часи Артіна було б приведене значення тієї ж величини, що і при $a=2$. Оцінити значення $c(a,i,x)$ при будь-яких значеннях a та i навіть при умові грубої його оцінки поки що не можливо, якщо не володіти більш глибокими знаннями. Аналіз оцінок констант Артіна в узагальненій формі для будь-яких значень a та індексу i методами комп'ютерного моделювання процесів формування класів простих чисел $P(a,i,x)$ на множинах послідовних простих чисел типу $[p_n, p_{n+M}]$ приводить до висновку, що оцінки залежать від величини M. При умові, що число $M=500000$ та будь-яких значеннях p_n, оцінки констант $c(a,1,x)$ співпадають для чотирьох десятичних знаків. При збільшені M до 10^6 ситуація не змінюється. Для цього факту існує непросте пояснення. При послідовному збільшені M та при умові, що приведені множини простих чисел не перетинаються, структура множин простих чисел поступово змінюється відносно наступної системи властивостей. Множина $[p_n, p_{n+M}]$ простих чисел характеризується законом розподілу $\omega(p-1)$. В роботі[8] доведено, що максимальне значення $\omega(p-1)$ на приведених інтервалах послідовних простих чисел зростає при збільшені p_n на величину порядку 10^7.

Поки відсутні ефективні алгоритми та методи оцінювання $c(a,i,x)$, та побудова класів $P(a,i,x)$ для будь-яких значень a та i у вигляді математичного методу, для якого створене теоретичне обґрунтування. Розглянемо випадок коли $a=p^3$ та при цьому p - просте число. В цьому випадку справедлива теорема:

Теорема 4. Якщо $a=p^3$ та p – просте число, то константа Артіна $c(a,1,x)=0.224..$ для всіх значень a такого типу. Справедливість теореми випливає з аналізу поведінки $c(2,1,x)$ для усіх простих чисел p. Нехай p - довільне просте число, для якого 2 є його первісний корінь. При цьому $2^{(p-1)}\equiv 1 \pmod p$. Розглянемо випадок коли $p-1$ ділиться на 3. Тоді справедлива рівність $2^{(p-1)}=(2^{(p-1)/3})^3=(2^3)^{(p-1)/3}=8^{(p-1)/3}\equiv$ $\equiv 1 \pmod p$. Така рівність виникає в тих випадках коли просте число p таке що число 8 не є його первісним коренем та має індекс 3. Таких простих чисел безмежна кількість на основі теореми Діріхле та аналізу випадків коли 8 не є первісний корінь. Методом комп'ютерного моделювання процесів формування класів $P(8,i,x)$ було доведено, що $c(8,1,x)=0.224...$ Такі ж перетво- рення можливі при $a=3$ або $a=5$, або $a=7$ і так далі. Для $a=27$ та $a=125$ були отримані такі ж оцінки $c(27,1,x)$ та $c(125,1,x)$. Одночасно отрму- вались оцінки для значень $i>1$.

Приведену теорему можна досить просто узагальнити на прості показники $5,7,11,...$ та при цьому, при збільшені показника, $c(a,i,x)$ також зростає і поступово наближається до $c(2,i,x)$ для всіх значень i та для будь-якої множини послідовних простих чисел, коли $x=p\in[p_n, p_{n+M}]$. Нескладно обґрунтувати висновок, що існують a з іншими властивостями, при яких оцінки констант Артіна можуть приймати значення відмінні від приведених, можливо в незначній мірі, але за іншими законами формування класів простих чисел $P(a,i,x)$ та відповідних їм констант Артіна $c(a,i,x)$. Необхідно відмітити, що числа 2 та 8 можуть бути одночасно первісними коренями простого числа тоді, і тільки тоді, коли умови теореми не виконуються. Звідси випливає, що дослідження законів розподілу первісних коренів для простих чисел є важливою математичною проблемою, яка досі не розв'язана.

Висновки

Приведені основи методів формування класів простих чисел на основі рекурсивної функції Ферма та властивостей натуральних чисел, відмінних від плюс-мінус одиниці та квадрата, які являються основою формування класів. Доведено що властивості класів простих чисел в кількісній формі описуються константами Артіна властивості яких завжди визначаються властивостями натуральних чисел а як класифікаторів множини простих чисел. Знайдені обґрунтовані значення меж в яких можуть приймати значення константи Артіна. Приведений аналіз зв'язку констант Артіна з їх аналітичними апроксимаційними оцінками. Визначені основи створення систем арифметичних прогресій які повністю покривають класи простих чисел незалежно з парними та не парними індексами.

Список використаної літератури

1. Crandall R., Pomerance C., Prime Numbers. A Computational Perspective. Springer, 2005.
2. Moree P. Artin's primitive root conjecture -a survey- 2011.
3. Artin E., The Collected papers. Addison-Wesley publishing company.INC 1965.,
4. Hasse H., Uber die Artinische Vernutung und Verwandte Dichtefragen. Annales Academiae Scientiarum Fennicae, A. I. Math.-Phys, 116 (1952).
5. Bilharz H. Primitivisoren mit vorgegenbener Primitivwurzel, Math. Ann. 114 (1937) 476-492.
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. Hooley Ch., On Artin's conjecture. Journal fur die reine und angewandte Mathematics. Sonderabruck aus Band 225, 1967, Seite 209 bis 220.
8. Hooley Ch., Applications of sieve methods in the theory of numbers. Cambridge University Press. 1976.
9. 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.
10. Manin Y., Panchishkin A., An Introduction to Modern Number Theory. Springer, 2005.
11. Pomerance C., Rassias Th. M., Editors. Analytic Number Theory, Springer, 2015.
12. Murty Ram M., Problems in analytic Number Theory. Springer. 2008.
13. Lacasa L., Luque B., Gomes I., Miramontes O., On a Dynamical Approach to Some Prime Number Sequences. Entropy. MDPI.2021.
14. Tenenbaum G., Introduction to analytic and Probabilistic Number Theory. American Mathematical Society, 2015.
15. Granville A., Smooth numbers: computational number theory and beyond Algorithmic Number Theory MSRI Publications Volume 44, 2008.
16. Kac M., Statistical the independence in probability analysis and number theory. The Carus Mathematical Monographs. Mathematical Monographs Number 12, JOHN WILEY and SONS, inc.1959.
17. Kowalski E., Arithmetic Randonnee. An Introduction to probabilistic number theory. Versus of May,2021.
18. Ambrose Ch. D. On Artin's Primitive Root Conjecture. Georg-August-Universitat Gottingen. Geiidelberg. Dissertation 2014.

SYSTEMATIC ANALYSIS OF THE DISTRIBUTION OF PRIMITIVE ROOTS OF PRIME NUMBERS IN ARTIN'S CONJECTURE

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

Abstract. *The results of the study of the laws of distribution of primitive roots of prime numbers p on sets of natural numbers and their connection with Artin's conjecture are presented. The systematic nature of the formation of classes of prime numbers and generalized constants is proven. A complete justification of the laws of formation of classes of prime numbers with a certain value of indices and the corresponding Artin constants is given. The regularities of the formation of Artin classes are found and it is proven that they depend on a significant number of factors related to the properties of the corresponding primes. The analysis*

of the factors is given and the regularities that significantly affect the processes of formation of the distribution of prime roots are investigated.

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.

Георгій

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.