

DOI: <https://doi.org/10.15276/ict.03.2026.78>

УДК 004:519.688

Математичне та алгоритмічне забезпечення добору параметрів мультиплікативних послідовностей

Щербанюк Олександр Вікторович¹⁾

ORCID: <https://orcid.org/0009-0005-1388-2481>; alex12200@stud.op.edu.ua

Востров Георгій Миколайович¹⁾

ORCID: <https://orcid.org/0000-0003-3856-5392>; vostrov@gmail.com

¹⁾ Національний університет «Одеська політехніка», пр. Шевченка, 1. Одеса, 65044, Україна

АНОТАЦІЯ

Розглянуто задачу добору параметрів мультиплікативних послідовностей із заданими характеристиками періоду та циклічної структури ненульових станів. Систематизовано арифметичні умови такого добору та визначено межі перенесення властивостей між структурно пов'язаними основами. Використано результати обчислювального експерименту, виконаного мовою C#, для двох тисяч шістдесяти семи основ на вибірці з п'ятисот тисяч послідовних простих модулів. Зіставлення груп за безквадратною частиною та степеневим представленням дало змогу розмежувати близькість емпіричних частот, спільні необхідні обмеження та точну еквівалентність за первісністю. Показано, що спільна безквадратна частина визначає однакові окремі арифметичні обмеження, але не гарантує збігу мультиплікативних порядків або множин модулів первісності. Водночас для окремих степеневих сімейств встановлено умови, за яких ознака первісності може коректно переноситися між пов'язаними основами. На дослідженій вибірці також показано, що близькі емпіричні частоти самі по собі не є достатньою підставою для перенесення властивостей між кандидатами. На основі відомих співвідношень для мультиплікативного порядку та індексу сформульовано алгоритмічну процедуру добору параметрів, що передбачає перевірку допустимості, відхилення несумісних кандидатів, точне обчислення порядку та збереження придатних пар «основа – модуль». Наведено приклад вибору множника для формування двох циклів ненульових станів за модулем сімнадцять. Запропонована послідовність перевірки поєднує попереднє застосування точних структурних обмежень із завершальним обчисленням мультиплікативного порядку. Практичним результатом є математично обґрунтоване алгоритмічне забезпечення добору параметрів мультиплікативних послідовностей за заданою циклічною структурою. Прискорення пошуку та статистичну якість генераторів у роботі не оцінювали.

Ключові слова: інформаційні системи; мультиплікативна конгруентна послідовність; добір параметрів; алгоритмічне забезпечення; обчислювальний експеримент; циклічна структура; мультиплікативний порядок; первісні корені; константи Артіна; класи простих чисел.

Для цитування: Щербанюк О. В., Востров Г. М. “Математичне та алгоритмічне забезпечення добору параметрів мультиплікативних послідовностей”. *Інформатика. Культура. Техніка.* 2026; Том 3 № 2 (4): 1015–1024. DOI: <https://doi.org/10.15276/ict.03.2026.78>

Постановка проблеми. У комп'ютерних та інформаційних системах, що використовують мультиплікативні конгруентні послідовності, їхній період і структура циклів ненульових станів залежать від вибору множника та модуля. Такі послідовності застосовуються, зокрема, у програмних засобах моделювання та під час проведення обчислювальних експериментів. Тому під час програмної реалізації виникає задача добору таких параметрів, які забезпечують заданий період або задану кількість циклів.

Для конкретної пари «основа – простий модуль» ці характеристики визначаються мультиплікативним порядком. Безпосередня перевірка всіх кандидатів не використовує відомі арифметичні обмеження, пов'язані зі степеневою структурою основи, її безквадратною частиною та можливими значеннями індексу. Доцільно спочатку відхиляти несумісні пари за точними структурними умовами, а для решти виконувати обчислення порядку. Практичне значення мають правила, які дають змогу виявити несумісні вимоги до параметрів або коректно перенести вже перевірену властивість між пов'язаними основами.

Дослідження розподілу простих чисел, за якими фіксоване ціле число є первісним коренем, пов'язане з гіпотезою Артіна. Для додатної цілої основи, більшої за одиницю і відмінної від повного квадрата, класична гіпотеза передбачає існування нескінченної множини відповідних простих модулів. Кількісна постановка описує їхню граничну частку з урахуванням арифметичних властивостей основи [1], [2]. Водночас частоти, одержані для груп модулів, не визначають придатність кожної конкретної пари параметрів.

Прикладний інтерес становить не лише клас первісних коренів, а й класи з іншими значеннями індексу. Вони визначають, наскільки фактичний період рекурентної процедури менший за кількість ненульових станів. Водночас знання частоти класу на вибірці не дає відповіді щодо кожного конкретного модуля. Тому необхідно розмежовувати статистичний опис класів, точні арифметичні обмеження та перевірку конкретних параметрів.

Аналіз останніх досліджень і публікацій. Алгоритми генерації та добір параметрів. Knuth [3] розглядає алгоритми генерації псевдовипадкових чисел, періодичність і методи оцінювання генераторів. Park і Miller [4] пов'язують математичні умови з програмною реалізацією мультиплікативного генератора; реалізації доступні також у GSL [5]. Steele і Vigna [6] досліджують добір множників за спектральними характеристиками й обчислювальною вартістю для модулів, що є степенями двійки. Ці роботи показують, що вибір параметрів є алгоритмічною задачею з різними критеріями. У нашій постановці модулі прості, а критеріями прийняття є точний період і кількість циклів; результати для степенів двійки безпосередньо не переносяться.

Математична основа. Класи простих модулів із заданим залишковим індексом вивчаються в теорії near-primitive roots. Moree [7] досліджує їхні щільності за припущення узагальненої гіпотези Рімана та арифметичні причини їх зникнення. Lenstra, Moree і Stevenhagen [8] описують поправки до щільностей через суми характеристик. Ці результати забезпечують теоретичну основу аналізу класів; у процедурі добору використовуються точні обмеження для окремих пар, а не припущення про їхню придатність на основі щільності.

Програмна перевірка та оцінювання. L'Esuyer і Simard [9] пропонують бібліотеку TestU01 для емпіричного статистичного тестування генераторів. На відміну від перевірки порядку, ці випробування оцінюють статистичні властивості вихідних послідовностей. Таким чином, перевірка періоду, спектральний аналіз і статистичні тести розв'язують різні задачі; ця робота стосується першої з них і структурних умов добору параметрів.

У попередній спільній роботі [10] досліджено внутрішні структури сформованих послідовностей із використанням порівняння фрагментів і спектрального подання. Нинішня робота зосереджена на іншому етапі – арифметичних умовах добору параметрів за періодом та кількістю циклів. Її задача полягає в розмежуванні близькості емпіричних частот, спільних необхідних обмежень і тотожності множин модулів первісності. Таке розмежування визначає, які властивості можна коректно переносити між кандидатами. Теорія щільностей [7], [8] і дослідження вибору кандидатів [11] становлять теоретичну основу для зіставлення результатів і визначення меж застосування структурних умов добору.

Мета та завдання роботи. Мета роботи – розробити математичне та алгоритмічне забезпечення добору параметрів мультиплікативних послідовностей за заданим періодом та кількістю циклів.

Вхідні дані – додатні цілі основи та спільна вибірка простих модулів, що не ділять їх. Потрібно зіставити частоти первісності структурних груп і визначити, які властивості параметрів можна коректно переносити між основами. Прикладним результатом є обґрунтовані умови допустимості періодів і кількості циклів та алгоритмічна послідовність перевірки кандидатів.

Для досягнення мети розв'язуються задачі:

- систематизувати арифметичні умови добору параметрів мультиплікативних послідовностей;
- встановити структурні обмеження на допустимі значення порядку та індексу;
- зіставити структурні групи основ за результатами обчислювального експерименту;
- визначити умови коректного перенесення властивостей між структурно пов'язаними основами;
- сформулювати алгоритмічну послідовність перевірки та відбору допустимих пар «основа-модуль».

Теоретичні твердження обґрунтовуються арифметичними співвідношеннями, а емпіричні висновки стосуються дослідженої вибірки. Обчислювальний експеримент

охоплює частоти індексу 1; повне емпіричне розподілення всіх індексів у цій роботі не заявляється. Перевірка конкретних параметрів має спиратися на точний порядок, а не лише на частоту класу.

Теоретичні співвідношення та структурні обмеження

1. Порядок, індекс і класи простих модулів

Нехай $a > 1$ – ціла основа, p – просте число, яке не ділить a . Мультиплікативний порядок визначається як найменший додатний показник, за якого степінь основи дорівнює одиниці за модулем:

$$\text{ord}_p(a) = \min\{t \in \mathbb{N}: a^t \equiv 1 \pmod{p}\}. \quad (1)$$

За теоремою Лагранжа порядок ділить $p - 1$. Визначимо індекс:

$$I_a(p) = \frac{p-1}{\text{ord}_p(a)}. \quad (2)$$

Основа є первісним коренем тоді й лише тоді, коли її порядок дорівнює $p - 1$, тобто індекс дорівнює одиниці. Сама рівність $a^{p-1} \equiv 1 \pmod{p}$ не є достатнім критерієм первісності: за малою теоремою Ферма вона виконується для кожної допустимої основи. Визначальним є найменший показник повернення до одиниці.

Для фіксованої основи допустимі прості модулі поділяються на класи:

$$\mathcal{P}_{a,i} = \{p: p \text{ – просте, } p \nmid a, I_a(p) = i\}, \quad i \in \mathbb{N}. \quad (3)$$

Тут $p \nmid a$ означає, що p не ділить a . Класи попарно не перетинаються, а їх об'єднання містить усі допустимі прості модулі. Деякі класи можуть бути порожніми внаслідок арифметичних обмежень. Відсутність представників у скінченній вибірці, однак, не доводить порожності класу серед усіх простих чисел.

Для обчислювального аналізу розглянемо множину послідовних простих чисел $B = \{p_n, \dots, p_{n+M-1}\}$, де p_n – n -те просте число, а $M \geq 1$ – кількість елементів блоку, та її допустиму частину $B_a = \{p \in B: p \nmid a\}$. За умови $|B_a| > 0$ частота класу дорівнює

$$f_{a,i}(B) = \frac{|B_a \cap \mathcal{P}_{a,i}|}{|B_a|}. \quad (4)$$

Це точна характеристика обраної скінченної вибірки. Якщо всі модулі перевищують основу, жоден із них не ділить її і знаменник дорівнює M . Частоти класів у такій класифікації в сумі дорівнюють одиниці, але це не є доведенням існування відповідних граничних щільностей.

2. Гіпотеза Артіна та інтерпретація частот

Константа Артіна задається добутком за всіма простими числами q :

$$A = \prod_{q \text{ — просте}} \left(1 - \frac{1}{q(q-1)}\right). \quad (5)$$

У кількісній гіпотезі Артіна щільність для конкретної основи не слід безумовно ототожнювати з одним і тим самим значенням A . Враховуються степенева структура основи та залежності між арифметичними умовами. Відомі поправки, зокрема для основи 5, розглянуто в огляді [2]. Отже, виявлення різних частот для різних основ слід зіставляти з наявною теорією, а не трактувати саме по собі як її спростування.

Гулі отримав умовний результат щодо гіпотези Артіна за відповідних припущень узагальненої гіпотези Рімана [12]. Він не обмежується лише основою 2. Теоретичні твердження про асимптотичний розподіл і результати обчислень на скінченних інтервалах мають різний статус та не можуть взаємно підмінятися.

3. Арифметичні обмеження та структура класів

3.1. Степеневі основи

Для цілої основи $b > 1$, простого $p \nmid b$ та цілого $h \geq 1$ справедливе стандартне співвідношення:

$$\text{ord}_p(b^h) = \frac{\text{ord}_p(b)}{\gcd(\text{ord}_p(b), h)}. \quad (6)$$

Дійсно, якщо порядок b дорівнює t , то $(b^h)^k \equiv 1 \pmod{p}$ еквівалентно умові $t \mid hk$. Найменше додатне k , для якого вона виконується, дорівнює $t/\gcd(t, h)$. Звідси випливає: b^h є первісним коренем за модулем

$$p \Leftrightarrow \text{ord}_p(b) = p - 1 \text{ і } \gcd(p - 1, h) = 1. \quad (7)$$

Таким чином, степенева структура основи накладає точні обмеження на допустимі параметри. Для квадратної основи та непарного простого модуля максимальний порядок неможливий. Для кубічної основи необхідно, зокрема, щоб $p - 1$ не ділилося на 3; ця умова не замінює вимоги первісності початкової основи b .

3.2. Класи лишків і симетрія первісних коренів

Для непарного простого модуля первісний корінь є квадратичним нелишком. Тому умови квадратичної лишковості дають необхідні обмеження на можливі модулі. Застосування квадратичного закону взаємності дозволяє виражати частину цих обмежень через класи лишків. Проте належність дозволеному класу лишків загалом не є достатнім критерієм первісності: залишаються умови, пов'язані з іншими простими дільниками $p - 1$ [1], [2].

Якщо $1 \leq g \leq p - 1$ є первісним коренем за модулем непарного простого p , то $-1 \equiv g^{(p-1)/2} \pmod{p}$. Тому властивості $p - g$ визначаються показником $1 + (p - 1)/2$. Для $p \equiv 1 \pmod{4}$ цей показник взаємно простий із $p - 1$, звідки $p - g$ також є первісним коренем. Множина первісних коренів у цьому випадку симетрична відносно середини інтервалу ненульових лишків.

Для $p \equiv 3 \pmod{4}$ найбільший спільний дільник зазначеного показника та $p - 1$ дорівнює 2. Отже, порядок $p - g$ становить $(p - 1)/2$, і цей елемент не є первісним коренем. Таким чином, одна й та сама операція зміни знака має різний вплив на період залежно від класу модуля.

Добуток двох первісних коренів за непарним простим модулем також не є первісним коренем. Якщо виразити обидва через степені одного генератора, їхні показники будуть непарними, а показник добутку – парним і тому не взаємно простим із $p - 1$. Ці властивості є стандартними наслідками циклічності групи; у прикладній постановці вони використовуються як обмеження на перетворення параметрів.

3.3. Заборонені непарні індекси та безквадратна частина основи. Одна з центральних задач структурного аналізу полягає у виявленні індексів, які неможливі не лише в обчисленій вибірці, а й для будь-якого допустимого простого модуля. Для уточнення цієї властивості подамо основу єдиним чином у вигляді $a = ds^2$, де d і s — додатні цілі числа, а d не ділиться на квадрат жодного простого числа. Число d називатимемо безквадратною частиною основи: множник s^2 є найбільшим квадратним дільником a . Наприклад, $20 = 5 \cdot 2^2$ та $45 = 5 \cdot 3^2$, тому в обох випадках $d = 5$. Для повного квадрата $d = 1$. Безквадратну частину не слід плутати з добутком усіх різних простих дільників числа.

Для непарного простого $p \nmid a$ позначення $\left(\frac{a}{p}\right)$ означає символ Лежандра: він дорівнює 1 для квадратичного лишку і -1 для квадратичного нелишку. Оскільки s^2 є ненульовим квадратом за модулем p , символи Лежандра для a та d збігаються.

Нехай g – первісний корінь за модулем p , а $a \equiv g^e \pmod{p}$, де $0 \leq e \leq p-2$ — цілий показник. Тоді $I_a(p) = \gcd(e, p-1)$. Оскільки $p-1$ парне, індекс непарний тоді й лише тоді, коли e непарний. Отже,

$$I_a(p) \text{ непарний} \Leftrightarrow \left(\frac{a}{p}\right) = -1. \quad (8)$$

Для безквадратної основи заборону непарного індексу, кратного цій основі за умови її порівнянності з 1 за модулем 4, та аргумент через квадратичну взаємність наведено вже у вступі до [7]. Нижче подано цей відомий аргумент із явним виділенням безквадратної частини довільної додатної основи. Саме обмеження не заявляється як нове відкриття.

Твердження. Якщо $a = ds^2$, $d > 1$ є безквадратним, $d \equiv 1 \pmod{4}$, а p – непарний простий модуль, який не ділить a , то індекс $I_a(p)$ не може бути непарним кратним d .

Доведення. Припустімо, що індекс непарний і $d \mid I_a(p)$. Оскільки індекс ділить $p-1$, одержуємо $p \equiv 1 \pmod{d}$. Квадратичний закон взаємності для символів Якобі за умови $d \equiv 1 \pmod{4}$ дає

$$\left(\frac{a}{p}\right) = \left(\frac{d}{p}\right) = \left(\frac{p}{d}\right) = 1. \quad (9)$$

Тут символ із знаменником d є символом Якобі — добутком символів Лежандра за простими дільниками безквадратного d ; остання рівність випливає з $p \equiv 1 \pmod{d}$. Це суперечить (8).

Отже, для всіх цілих $\ell \geq 0$ відповідні класи порожні:

$$\mathcal{P}_{a,d(2\ell+1)} = \emptyset. \quad (10)$$

Модуль 2 також не утворює винятку до (10): для непарної основи його індекс дорівнює 1, а для парної основи він недопустимий. Якщо $a \equiv 1 \pmod{4}$ і не є квадратом, його безквадратна частина також задовольняє $d \equiv 1 \pmod{4}$. Тому, зокрема, неможливі непарні індекси, кратні самому a . Формулювання через d дає точніше обмеження і поширює його на інші основи з тією самою безквадратною частиною.

Для основ 5, 20 та 45 неможливі індекси 5, 15, 25 та інші непарні кратні 5. Для основ 13, 208 та 325 аналогічно виключаються непарні кратні 13. Цей висновок отримано з квадратичної взаємності; він не потребує існування граничних щільностей класів. Водночас із порожності певних класів не впливає універсальна нерівність між частотами первісності різних основ.

Важливо розрізнити спільні обмеження та тотожність класів. Основи 5 і 20 мають однакову безквадратну частину, але за модулем 7 їхні порядки дорівнюють відповідно 6 і 2. Отже, спільна безквадратна частина визначає однакову квадратичну лишковість та парність індексів на спільних допустимих непарних простих модулях, але не гарантує однакових порядків або однакових множин модулів первісності.

4. Обчислювальний експеримент та аналіз результатів

4.1. Дані та спосіб зіставлення

Для перевірки виявлених структурних закономірностей та аналізу різних груп основ виконано обчислювальний експеримент. Його результати використовуються не як заміна точних арифметичних умов, а як обчислювальна основа для зіставлення структурно пов'язаних основ. Експеримент проведено для 2067 основ від 2 до 2112, за винятком повних квадратів, на спільній вибірці з 500 000 послідовних простих чисел, починаючи з 2113. Для кожної основи підраховано кількість модулів, за якими вона є первісним коренем. Усі модулі перевищують досліджені основи, тому знаменник частоти однаковий. Експеримент виконано Щербанюком О. із використанням програмної реалізації мовою C#; попередній структурний аналіз результатів виконано авторами спільно.

Методика експерименту. Для кожної пари «основа – модуль» у виконаній програмі C# послідовно обчислювалися лишки степенів основи множенням за модулем до першого повернення до одиниці. Кількість кроків визначала порядок; модуль зараховувався до класу первісності, якщо порядок дорівнював модулю мінус один. Кількість таких модулів ділилася на 500 000. Це пряме обчислення порядку, а не застосування критерію через факторизацію, наведеного нижче для добору параметрів.

Структурний аналіз виконано авторами зіставленням основ за трьома ознаками: спільною безквадратною частиною, типом степеневого представлення та належністю до степенів однієї основи. Для кожної групи порівнювалися частоти первісності; спостережувана близькість або рівність перевірялася на відповідність точним арифметичним умовам. Результатом аналізу є розмежування спільних необхідних обмежень і достатніх умов перенесення ознаки первісності. Близькість частот використано описово, без введення статистичного порога кластеризації.

У Таблиці 1 наведено вибрані приклади для зіставлення безквадратних частин та степеневих представлень. Частоти відтворюють значення вихідного набору; арифметичні представлення наведено в узгодженій формі. Таблиця містить вибрані результати цього експерименту й не охоплює всі структурні групи набору.

Таблиця 1. Приклади частот первісності на спільній вибірці простих модулів

Основа	Структурне представлення	Частота
2	2	0,374218
5	5	0,393940
20	$5 \cdot 2^2$	0,394040
45	$5 \cdot 3^2$	0,393848
13	13	0,376516
208	$13 \cdot 4^2$	0,376472
325	$13 \cdot 5^2$	0,376508
21	$3 \cdot 7$	0,371850
84	$21 \cdot 2^2$	0,372168
8	2^3	0,224650
27	3^3	0,224370
125	5^3	0,236456
128	2^7	0,319626
512	2^9	0,224650
2048	2^{11}	0,339754

Джерело: розроблено авторами

4.2. Інтерпретація спостережень

У вибраних групах зі спільною безквадратною частиною 5 та 13 спостерігаються близькі частоти. Це узгоджується з доцільністю врахування безквадратної частини під час аналізу, але не доводить, що лише вона визначає частоту або склад класу первісності. Приклад для основ 5 і 20 у підрозділі про заборонені індекси показує, чому близькість агрегованих характеристик не можна ототожнювати з однаковою придатністю кожного модуля.

Основа 21 має вигляд $4k + 1$, але її частота в цій вибірці менша за частоту основи 2. Отже, сам клас лишків основи за модулем 4 не забезпечує універсального перевищення емпіричної частоти. Це конкретне обмеження інтерпретації наведеного набору, а не висновок про всі граничні щільності.

Для кубів 8 і 27 частоти близькі, тоді як для 125 значення відрізняється. Належність до кубів простих чисел тому недостатня для приписування однакового емпіричного значення всім таким основам. Формула (6) пояснює обмеження на модулі, але не дає універсальної

константи для всіх кубічних основ. Скінченна таблиця також не є самостійним доведенням або спростуванням рівності граничних щільностей.

Особливий випадок становлять основи 8 і 512: їхні частоти збігаються точно. Для непарного простого модуля основи 2^3 та 2^9 є первісними коренями за однакових умов: основа 2 повинна бути первісним коренем і $p - 1$ не повинно ділитися на 3. Тут рівність частот має точне пояснення через тотожність множин допустимих модулів первісності, а не лише через числову близькість оцінок.

Загальніше, для степенів однієї основи b^{h_1} та b^{h_2} множини модулів первісності збігаються, якщо додатні цілі показники h_1 і h_2 мають однакові прості дільники; розглядаються модулі $p \nmid b$. Це безпосередній наслідок (7). Порядки на модулях, де ці основи не є первісними коренями, при цьому можуть відрізнятися. Отже, еквівалентність за ознакою максимального періоду слабша за еквівалентність повної циклічної структури.

5. Застосування до добору параметрів послідовностей

Розглянемо мультиплікативну конгруентну послідовність за простим модулем p , де станами є канонічні лишки від 0 до $p - 1$, а n – невід’ємний цілий номер кроку:

$$x_{n+1} = ax_n \bmod p, \quad n \geq 0, \quad p \nmid a, \quad 1 \leq x_0 \leq p - 1. \quad (11)$$

За індукцією $x_n \equiv a^n x_0 \pmod{p}$. Оскільки ненульове x_0 має обернений елемент, умова повернення до початкового стану еквівалентна $a^n \equiv 1 \pmod{p}$. Отже, період становить

$$T(a, p) = \text{ord}_p(a) = \frac{p-1}{I_a(p)}. \quad (12)$$

Множення на a є перестановкою ненульових лишків. Орбіта кожного стану є суміжним класом підгрупи, породженої a . Усі такі цикли мають довжину $T(a, p)$, а їхня кількість дорівнює

$$N_{\text{cycles}}(a, p) = I_a(p). \quad (13)$$

Нульовий стан є окремою нерухомою точкою. Ці висновки стосуються саме рекурсії (11) за простим модулем; перенесення їх на змішані генератори з додаванням сталої або на довільний складений модуль потребує окремого аналізу.

Для фіксованого модуля умова $I_a(p) = 1$ означає один цикл на всіх ненульових станах. Якщо індекс більший за одиницю, простір ненульових станів розпадається на кілька циклів. За фіксованого індексу та різних модулів абсолютні періоди можуть відрізнятися: однаковий індекс характеризує однакове відношення періоду до $p - 1$, а не однакову довжину циклу.

5.1. Пояснювальний приклад. За модулем 17 основа 3 має порядок 16 та індекс 1, основа 2 – порядок 8 та індекс 2, основа 4 – порядок 4 та індекс 4. Відповідно, ненульові стани утворюють один цикл довжини 16, два цикли довжини 8 або чотири цикли довжини 4. Для основи 2 послідовність із початковим станом 1 проходить стани 1, 2, 4, 8, 16, 15, 13, 9 і повертається до 1. Приклад ілюструє інтерпретацію класифікації, а не є результатом масштабного статистичного експерименту.

Приклад добору. Нехай модуль дорівнює 17, кандидати на множник – 2, 3 та 4, а вимога – два цикли ненульових станів однакової довжини. Тоді потрібний період дорівнює 8, а індекс – 2. Обчислені порядки кандидатів становлять відповідно 8, 16 та 4, тому серед заданих кандидатів придатний лише множник 2. Його цикли: (1, 2, 4, 8, 16, 15, 13, 9) та (3, 6, 12, 7, 14, 11, 5, 10). Вони охоплюють усі ненульові стани без перетину. Це перевірка конкретного вибору, а не вимірювання швидкодії чи якості випадковості.

Алгоритм добору параметрів мультиплікативних послідовностей. Вхід: скінченні множини основ і простих модулів та вимога до періоду або кількості циклів. Вихід: перелік допустимих пар із перевіреними порядками та індексами. Якщо одночасно задано період і кількість циклів, їхній добуток повинен дорівнювати модулю мінус один.

Крок 1. Виключити пари, в яких модуль ділить основу, і перевірити сумісність заданої довжини циклу з кількістю ненульових станів.

Крок 2. Визначити степеневе представлення та безквадратну частину основи; застосувати лише ті точні обмеження, які стосуються заданого індексу. Зокрема, заборона індексу 5 сама по собі не виключає кандидата з індексом 1.

Крок 3. Для кандидатів, що залишилися, обчислити порядок і перевірити вимогу; для максимального періоду можна використати критерій (14). Переносити ознаку первісності між степенями однієї основи дозволено лише за доведених умов (7), не підміняючи цим обчислення довільного порядку.

Крок 4. Зберегти придатні пари разом із періодом, індексом та підставою перевірки. Емпірична частота не є умовою відхилення окремої пари.

Коректність процедури ґрунтується на необхідності застосованих обмежень і завершальній точній перевірці. Якщо кожне правило відхилення застосоване в межах його умов, придатні пари не виключаються; остаточна перевірка не допускає прийняття непридатних пар.

Для прикладного добору параметрів потрібно: визначити допустимі модулі й вимогу до періоду; застосувати обґрунтовані арифметичні обмеження; перевірити порядок кандидатів; зберегти придатні пари разом із порядком та індексом. Для максимального періоду може використовуватися відомий критерій [1], [2]:

$$a \text{ є первісним коренем за модулем } p \Leftrightarrow a^{\frac{p-1}{q}} \not\equiv 1 \pmod{p} \text{ для кожного простого } q \mid p-1. \quad (14)$$

Критерій застосовується за умови $p \nmid a$. Він є стандартним засобом перевірки, а не новим результатом цієї роботи.

Для основ $a = ds^2$ із безквадратною частиною $d > 1$, що задовольняє $d \equiv 1 \pmod{4}$, індекси $d, 3d, 5d$ та інші непарні кратні d неможливі. У термінах рекурентності це виключає відповідну кількість циклів і періоди $(p-1)/i$, навіть коли i ділить $p-1$. Наприклад, для основ 5, 20 та 45 неможлива структура з п'ятьма циклами ненульових станів за будь-яким допустимим простим модулем. Така інформація дає змогу відкинути несумісну вимогу до параметрів ще до побудови послідовності. Водночас для степеневих сімейств з однаковими простими дільниками показників переноситься лише ознака максимального періоду, а не всі значення періодів.

5.2. Межі практичного використання

Межі результатів. Виконаний C#-експеримент характеризує частоти первісності на зазначеній вибірці; структурне зіставлення виконано авторами, а наведена процедура формалізує застосування отриманого аналізу та відомих арифметичних умов. Порівняння часу роботи автоматизованого добору з фільтрами та без них не проводилося. Період і кількість циклів не визначають статистичної якості або криптографічної стійкості; випробування TestU01 та спектральна оцінка генераторів не входили до цього експерименту [3], [6], [9].

Висновки і перспективи подальших досліджень. На спільній вибірці з 500 000 простих модулів для 2067 основ зіставлено вибрані групи за безквадратною частиною та степеневим представленням. Для основ 5, 20 і 45 спостерігаються близькі частоти, але це не означає тотожності множин модулів первісності. Приклади 21 та 125 показують, що лише лишок основи за модулем 4 або належність до кубів не визначають єдиного емпіричного значення частоти. Ці спостереження стосуються скінченної вибірки, а не доведених граничних щільностей.

Розмежовано спільні необхідні обмеження та точну еквівалентність за первісністю. Для степенів однієї основи з однаковими наборами простих дільників показників множини модулів первісності збігаються. Це пояснює рівність частот для 8 та 512 у наявному наборі, але не означає збігу всіх порядків для цих основ.

Сформульовано відоме [7] структурне обмеження на індекси: для основи $a = ds^2$, де $d > 1$ – безквадратна частина числа a , неможливі непарні індекси, кратні d , якщо d має остачу 1 від ділення на 4. Обґрунтування через квадратичну взаємність відокремлює точну порожність класу від відсутності його представників у скінченній вибірці.

Сформульовано послідовність добору параметрів: перевірка допустимості, застосування точних структурних обмежень, обчислення порядку та збереження придатних пар. Для основ 5, 20 і 45 відома заборона індексу 5 виключає вимогу п'яти циклів ненульових станів; для пов'язаних степеневих основ переноситься ознака максимального періоду. На прикладі модуля 17 продемонстровано вибір множника 2 для двох циклів довжини 8. Практичним результатом роботи є математично обґрунтована обчислювальна процедура добору параметрів мультиплікативних послідовностей за заданою циклічною структурою. Вона поєднує попереднє відхилення несумісних кандидатів на основі структурних арифметичних обмежень із точною перевіркою мультиплікативного порядку. Такий підхід може бути використаний як математичне та алгоритмічне забезпечення комп'ютерного формування мультиплікативних послідовностей із заданим періодом і кількістю циклів.

Конфлікт інтересів: Автори декларують, що не мають конфлікту інтересів, зокрема фінансового, особистого, авторського чи будь-якого іншого характеру, який міг би вплинути на дослідження, а також на результати, опубліковані в цій статті.

Фінансування: Дослідження проводилося без фінансової підтримки.

Доступність даних: Дані та програмні матеріали, використані для одержання наведених результатів, можуть бути надані авторами за обґрунтованим запитом.

Використання засобів штучного інтелекту: Під час підготовки рукопису використовувався інструмент ChatGPT, модель GPT-5.6 Sol, OpenAI, для граматичної, стилістичної перевірки та редагування окремих фрагментів тексту. Усі запропоновані формулювання були перевірені та відредаговані авторами. ШІ не використовувався для отримання експериментальних результатів, виконання розрахунків, формування наукової новизни або самостійного формулювання наукових висновків. Наукові положення, результати та висновки є власним інтелектуальним внеском авторів

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Crandal, R. & Pomerance C. “Prime numbers: A computational perspective”. *2nd ed. Springer*. 2005. DOI: <https://doi.org/10.1007/0-387-28979-8>.
2. Moree, P. “Artin’s primitive root conjecture - A survey”. *Integers*. 2012. 12 (6). DOI: <https://doi.org/10.1515/integers-2012-0043>.
3. Knuth, D. E. “The art of computer programming”. *Seminumerical Algorithms*. 3rd ed. Addison-Wesley; 1997; 2;
4. Park, S. K. & Miller, K. W. “Random number generators: good ones are hard to find”. *Communications of the ACM*. 1988; 31 (10). 1192–1201. DOI: <https://doi.org/10.1145/63039.63042>.
5. “GNU scientific library”. *Random Number Generation*. Available from: <https://www.gnu.org/software/gsl/doc/html/rng.html>. [Accessed: 08 September 2025].
6. Steele, G. L. & Jr., Vigna S. “Computationally easy, spectrally good multipliers for congruential pseudorandom number generators”. *Software: Practice and Experience*. 2022; 52 (2): 443–458. DOI: <https://doi.org/10.1002/spe.3030>.
7. Moree, P. “Near-primitive roots”. *Functiones et Approximatio Commentarii Mathematici*. 2013; 48 (1): 133–145. DOI: <https://doi.org/10.7169/facm/2013.48.1.11>.
8. Lenstra, H. W., Jr., Moree P. & Stevenhagen P. “Character sums for primitive root densities”. *Mathematical Proceedings of the Cambridge Philosophical Society*. 2014; 157: 489–511. DOI: <https://doi.org/10.1017/S0305004114000450>.
9. L’Ecuyer, P. & Simard, R. “TestU01: A C library for empirical testing of random number generators”. *ACM Transactions on Mathematical Software*. 2007; 33 (4): 22. DOI: <https://doi.org/10.1145/1268776.1268777>.
10. Shcherbaniuk, O., Khrynenko, A. & Vostrov, G. “Analysis properties of trajectories of nonlinear dynamical systems”. 2025 *IEEE 13th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*. 2025.

p. 1–6. DOI: <https://doi.org/10.1109/IDAACS68557.2025.11322306>.

11. Perucca, A. & Tholl, M. “Computing primitive roots according to Artin’s conjecture”. *JP Journal of Algebra, Number Theory and Applications*. 2024; 63 (5): 435–445. DOI: <https://doi.org/10.17654/0972555524026>.

12. Hooley, C. “On Artin’s conjecture”. *Journal für die reine und angewandte Mathematik*. 1967; 225: 209–220. DOI: <https://doi.org/10.1515/crll.1967.225.209>.

Received 03.09.2026

Received after revision 07.10.2026

Accepted 12.10.2026

DOI: <https://doi.org/10.15276/ict.03.2026.78>

UDC 004:519.688

Mathematical and algorithmic support for selecting parameters of multiplicative sequences

Oleksander V. Shcherbaniuk¹⁾

ORCID: <https://orcid.org/0009-0005-1388-2481>; alex12200@stud.op.edu.ua

George M. Vostrov¹⁾

ORCID: <https://orcid.org/0000-0003-3856-5392>; vostrov@gmail.com

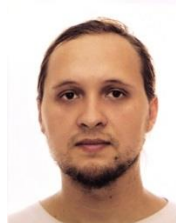
¹⁾ Odessa National Polytechnic University Shevchenko Ave., 1, Odessa, Ukraine, 65044

ABSTRACT

The problem of selecting parameters for multiplicative sequences with specified period characteristics and a prescribed cyclic structure of nonzero states is considered. The arithmetic conditions for such selection are systematized, and the limits of transferring properties between structurally related bases are determined. The results of a computational experiment implemented in C# for two thousand sixty-seven bases using a sample of five hundred thousand consecutive prime moduli are analyzed. Comparison of groups by square-free part and power representation made it possible to distinguish between the proximity of empirical frequencies, shared necessary constraints, and exact equivalence with respect to primitivity. It is shown that a common square-free part implies certain shared arithmetic constraints but does not guarantee equality of multiplicative orders or of the sets of prime moduli for which the bases are primitive roots. At the same time, conditions are established for certain power families under which the property of primitivity can be correctly transferred between related bases. The investigated sample also shows that close empirical frequencies alone are not sufficient grounds for transferring properties between candidates. Based on known relationships for multiplicative order and index, an algorithmic procedure for parameter selection is formulated, including admissibility checking, rejection of incompatible candidates, exact order computation, and storage of suitable «base–modulus» pairs. An example of multiplier selection for forming two cycles of nonzero states modulo seventeen is presented. The proposed verification sequence combines the preliminary application of exact structural constraints with the final computation of the multiplicative order. The practical result is mathematically justified algorithmic support for selecting parameters of multiplicative sequences with a prescribed cyclic structure. Search acceleration and the statistical quality of the generators were not evaluated in this study.

Keywords: INFORMATION systems; multiplicative congruential sequence; parameter selection; algorithmic support; computational experiment; cyclic structure; multiplicative order; primitive roots; Artin constants; classes of prime numbers.

ІНФОРМАЦІЯ ПРО АВТОРІВ



Щербанюк Олександр Вікторович - аспірант кафедри Прикладної математики та Інформаційних Технологій. Національний університет «Одеська політехніка», пр. Шевченка, 1. Одеса, 65044, Україна

Галузь досліджень: комп'ютерні науки та інформаційні технології, математичні та обчислювальні методи, алгоритмічне забезпечення, псевдовипадкові послідовності.

Oleksander V. Shcherbaniuk - PhD Student of the Department of Applied Mathematics and Information Technologies. Odessa Polytechnic National University, 1, Shevchenko Ave. Odessa, 65044, Ukraine

ORCID: <https://orcid.org/0009-0005-1388-2481>; alex12200@stud.op.edu.ua

Research field: computer science and information technologies, mathematical and computational methods, algorithmic support, pseudorandom sequences



Востров Георгій Миколайович – кандидат технічних наук, доцент кафедри Прикладної математики та інформаційних технологій. Національний університет «Одеська політехніка», пр. Шевченка, 1. Одеса, 65044, Україна

Галузь досліджень: комп'ютерні науки та інформаційні технології, математичне моделювання, математичні та обчислювальні методи, теорія чисел, аналіз алгоритмів, псевдовипадкові та динамічні системи

George M. Vostrov – PhD, Associate Professor, Department of Applied Mathematics and Information Technologies. Odessa Polytechnic National University, 1, Shevchenko Ave. Odessa, 65044, Ukraine.

ORCID: <https://orcid.org/0000-0003-3856-5392>; vostrov@gmail.com

Research field: computer science and information technologies, mathematical modeling, mathematical and computational methods, number theory, algorithm analysis, pseudorandom and dynamical systems