УДК 004:519.688

СПІЛЬНИЙ АНАЛІЗ ІНДЕКСІВ ПІДГРУП ДЛЯ ПОРІВНЯННЯ МУЛЬТИПЛІКАТИВНИХ ПОСЛІДОВНОСТЕЙ

Щербанюк О.В.; Востров Г.М., к.т.н., доц.
Національний університет «Одеська політехніка»
Україна, Одеса
0009-0005-1388-2481; 0000-0003-3856-5392

Анотація. *Запропоновано процедуру спільного аналізу індексів підгруп для порівняння множників мультиплікативних послідовностей. На наборі простих модулів показано відмінність між близькістю частот первісності та збігом періодів. Результати дають змогу визначати модулі, на яких заміна множника зберігає циклічні характеристики.*

Ключові слова: *мультиплікативна послідовність; індекс підгрупи; первісний корінь; спільний розподіл; обчислювальний експеримент.*

Вступ. У програмних засобах моделювання та обчислювальної теорії чисел використовуються мультиплікативні послідовності $x_{n+1} = ax_n \bmod p$, де p — просте число, $p \nmid a$, а початковий стан ненульовий за модулем p. Період такої послідовності та кількість циклів ненульових станів визначаються мультиплікативним порядком основи й індексом породженої нею підгрупи [1]. Тому заміна множника потребує зіставлення не лише узагальнених частот, а й характеристик на кожному спільному модулі.

Спільні індекси підгруп розглядаються в сучасних узагальненнях задач типу Артіна [2, 3]. Ці дослідження описують, зокрема, щільності класів простих за відповідних теоретичних припущень. Для прикладного порівняння множників на заданому скінченному наборі потрібен інший вихід: перелік модулів зі збереженими або зміненими характеристиками та кількісна оцінка таких змін. Окремі розподіли індексів не зберігають відповідності між результатами для двох основ на одному модулі.

Мета дослідження — розробити процедуру спільного обліку індексів двох основ на однакових простих модулях для розмежування близькості частот первісності та збігу періодів і кількості циклів мультиплікативних послідовностей.

Основна частина. Нехай $a, b > 1$ — цілі основи, B — скінченний непорожній набір різних непарних простих чисел, для яких $p \nmid ab$, а $N = |B|$. Для кожного модуля визначимо

$$I_a(p) = \frac{p-1}{\mathrm{ord}_p(a)}, \qquad I_b(p) = \frac{p-1}{\mathrm{ord}_p(b)}. \qquad (1)$$

Тут $\mathrm{ord}_p(a)$ — найменше додатне число t, для якого $a^t \equiv 1 \pmod p$. Індекс $I_a(p)$ дорівнює кількості циклів відображення $x \mapsto ax \bmod p$ на ненульових станах; довжина кожного циклу становить $\mathrm{ord}_p(a)$. Значення $I_a(p) = 1$ означає, що a є первісним коренем за модулем p. На одному модулі рівність індексів двох основ еквівалентна рівності їхніх періодів. Вона не вимагає однакового порядку проходження станів у циклах.

Спільний облік виконується за таблицею

$$H(i,j) = \mathrm{card}\{p \in B : I_a(p) = i,\ I_b(p) = j\}. \qquad (2)$$

Тут card позначає кількість елементів множини. Кожен модуль додає одиницю лише до однієї комірки. Суми рядків і стовпців відновлюють чисельності класів для кожної основи окремо. Діагональ $i = j$ відповідає модулям, на яких зберігаються період і кількість циклів, а

позадіагональні комірки — їх зміні. Поряд із таблицею зберігаються записи $\big(p, I_a(p), I_b(p)\big)$, щоб відновлювати конкретні модулі, а не лише їх кількості.

Для розділення двох аспектів порівняння обчислюються частоти первісності f_a, f_b та частка незбіжних індексів D_I:

$$f_a = \frac{\sum_j H\,(1,j)}{N}, \qquad f_b = \frac{\sum_i H\,(i,1)}{N}, \qquad D_I = 1 - \frac{\sum_i H\,(i,i)}{N}. \qquad (3)$$

Додатково визначається D_{PR} — частка модулів, на яких лише одна з основ є первісним коренем. Для її обчислення підсумовуються комірки першого рядка й першого стовпця без $H(1,1)$, а результат ділиться на N. Різниця $|f_a - f_b|$ характеризує відмінність чисельностей двох класів первісності, тоді як D_{PR} характеризує відмінність їхнього складу.

Процедура складається з чотирьох кроків. Спочатку формується спільний набір допустимих модулів. Далі для кожного p обчислюються порядки обох основ та індекси (1). За відомою факторизацією $p-1$ порядок знаходиться послідовним зменшенням початкового значення $t = p-1$: для простого дільника q поточного значення t останнє замінюється на t/q, якщо $a^{t/q} \equiv 1 \pmod p$, і перевірка повторюється [1]. Потім заповнюються таблиця (2) та список записів. Нарешті обчислюються показники (3), D_{PR} і виділяються модулі зі збігом індексів. Після підготовки індексів агрегація потребує одного проходу по N записах; зберігати достатньо ненульові комірки таблиці.

Обчислювальний експеримент. Для перевірки процедури використано основи $a = 5$, $b = 20$ та перші 8192 прості числа після 10^8: від 100000007 до 100150747 включно. Усі модулі допустимі для обох основ. Для кожного обчисленого порядку t перевірено $a^t \equiv 1 \pmod p$ та $a^{t/q} \not\equiv 1 \pmod p$ для кожного простого дільника q числа t; аналогічні перевірки виконано для другої основи. Результати спільного обліку первісності наведено в таблиці 1.

Таблиця 1 — Спільний облік первісності основ 5 та 20 на 8192 модулях

Умова для основи 5	20 - первісний корінь	20 - не первісний корінь	Разом
5 - первісний корінь	2628	579	3207
5 - не первісний корінь	583	4402	4985
Разом	3211	4981	8192

Частоти первісності дорівнюють 39,14795 % та 39,19678 %: чисельності класів відрізняються лише на чотири модулі. Водночас лише одна основа є первісним коренем на 1162 модулях, тобто $D_{\mathrm{PR}} = 14{,}18457\,\%$. Повний спільний облік індексів виявив 3787 модулів із різними індексами, тому $D_I = 46{,}22803\,\%$. Отже, заміна 5 на 20 змінює період і кількість циклів майже на половині досліджених модулів, хоча частоти первісності дуже близькі. На решті 4405 модулів ці характеристики зберігаються. Наведені частоти описують саме досліджений скінченний набір.

Висновки. Запропоновано процедуру порівняння множників мультиплікативних послідовностей, що поєднує спільну таблицю індексів зі збереженням відповідності конкретним модулям. На прикладі основ 5 та 20 встановлено, що близькі чисельності класів первісності можуть супроводжуватися істотною відмінністю їхнього складу та періодів послідовностей. Практичний результат — визначення множини модулів, на яких заміна множника зберігає задані циклічні характеристики. Такий спосіб аналізу придатний як окрема процедура дослідницького програмного забезпечення для добору й порівняння параметрів.

Використання інструментів ШІ. Модель GPT-6-astra, використовувалася виключно для перевірки правопису та граматичної корекції тексту. Після використання цього інстру-

менту автори переглянули та відредагували текст і беруть на себе повну відповідальність за зміст публікації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Shoup, V. (2008). *A computational introduction to number theory and algebra* (2nd ed.). Cambridge University Press.
[2] Järviniemi, O., & Perucca, A. (2023). Unified treatment of Artin-type problems. *Research in Number Theory*, 9, Article 10. http://doi.org/10.1007/s40993-022-00418-6.
[3] Järviniemi, O., Perucca, A., & Sgobba, P. (2025). Unified treatment of Artin-type problems II. *Research in Number Theory*, 11, Article 42. https://doi.org/10.1007/s40993-025-00620-2.

Shcherbaniuk O. V., Vostrov G. M.

Joint analysis of subgroup indices for comparing multiplicative sequences

Abstract. *A joint subgroup-index analysis procedure is proposed for comparing multipliers of multiplicative sequences. A finite prime-modulus experiment distinguishes similar primitive-root frequencies from matching periods. The procedure identifies the moduli on which replacing a multiplier preserves the period and number of cycles.*

Keywords: *multiplicative sequence; subgroup index; primitive root; joint distribution; computational experiment.*