

УДК: 004.056.55:519.6

**ЕКСПЕРИМЕНТАЛЬНИЙ АНАЛІЗ ПЕРІОДИЧНОСТІ
ГЕНЕРАТОРА LCG****Тарас КІС, Наталія МАСЛОВА, Андрій ЛАГУН***Львівський державний університет безпеки життєдіяльності*

У роботі проведено експериментальне дослідження залежності довжини періоду псевдовипадкових послідовностей, що формуються лінійним конгруентним генератором (LCG), від взаємного розташування його параметрів: множника a , зсуву c , модуля m та початкового значення X_0 .

Ключові слова: лінійний конгруентний генератор, період, параметри, теорема Халла–Добелла

An experimental study was conducted to investigate how the period length of pseudorandom sequences generated by a linear congruential generator (LCG) depends on the configuration of its parameters: multiplier a , increment c , modulus m , and initial value X_0 .

Keywords: linear congruential generator, period, parameters, Hull–Dobell theorem.

Псевдовипадкова генерація чисел є основою сучасних криптографічних систем, статистичного моделювання та симуляційних процесів. Забезпечення достатньої довжини періоду та рівномірності розподілу послідовностей безпосередньо впливає на якість отриманих результатів і стійкість алгоритмів, що їх використовують.

Метою дослідження є встановлення закономірностей формування повного або часткового періоду лінійного конгруентного генератора залежно від співвідношення параметрів, перевірка виконання умов теореми Халла–Добелла.

Актуальність. Надійність псевдовипадкових чисел залишається ключовою складовою криптографічного захисту, моделювання стохастичних процесів, машинного навчання та комп'ютерної симуляції. Лінійний конгруентний генератор (LCG) залишається одним із найпоширеніших інструментів у цих сферах завдяки простоті реалізації, високій швидкодії та низьким обчислювальним витратам. Водночас помилки під час вибору параметрів LCG можуть призвести до суттєвого скорочення довжини періоду та формування статистично передбачуваних підциклів, що критично впливає на безпеку та достовірність моделювання.

Методика дослідження. Для наборів параметрів обчислювався період шляхом покрокової генерації до повторення X_0 . Реалізовано частотний і серійний тести для оцінки рівномірності та структури отриманих послідовностей.

Математична модель лінійного конгруентного генератора:

$$X_{n+1} = (a X_n + c) \bmod m$$

Залежність довжини періоду LCG від параметра a при Заданому X_0 та фіксованих $c=13$ та $m=12$ відображена рисунку 1.

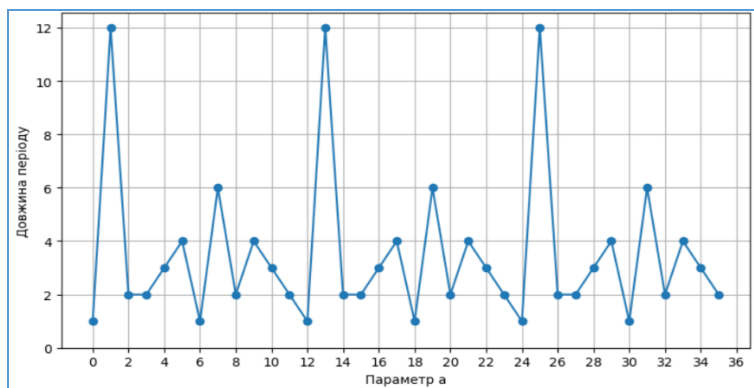


Рисунок 1 – Залежність довжини періоду LCG від параметра a при $c=13$, $m=12$, $X_0=199$

Рисунок демонструє повторюваність періоду LCG й те, його поведінка залежить від значення $a \bmod m$. Тож повні періоди виникають, коли $a - 1$ кратне m . Так, для $m=12 \rightarrow a=1,13,25,37$. Інші значення дають короткі цикли (2, 3, 4, 6), що призводить до нерівномірного розподілу, зниження випадковості й непридатності LCG для криптографії.

Таким чином, параметр a — головний чинник періодичності LCG при фіксованих c і m .

Проведемо ще серію експериментів, в яких значення параметрів X_0 , a , c , та m обирались випадковим чином й дослідим зміни періоду при різних значеннях вказаних параметрів (Таблиця 1).

Таблиця 1 – Експериментальні результати генератора LCG

№	X_0	a	c	Тип й значення m	Умова Халла–Добелла	Виконання	Період :: Характеристика послідовності
1	217	31	17	Простий, $m=13$	$(a-1)=30$ не кратне 13	Ні	$p=4$:: короткий цикл, нерівномірність
2	311	13	19	Простий, $m=11$	$\gcd(c,m)=1$	Так	$p=11$:: повний період, рівномірний розподіл
3	131	29	21	Простий, $m=17$	$(a-1)=28$ не кратне 17	Ні	$p=8$:: частковий період
4	253	21	7	Парний, $m=10$	$\gcd(7,10)=1$	Так	$p=10$:: повний, лінійна гістограма
5	167	43	29	Ступінь 2, $m=16$	$(a-1)=42$ не кратне 4	Ні	$p=8$:: рівномірний підцикл, період половинний
6	199	20	7	Парний, $m=12$	$\gcd(7,12)=1$, але $(a-1)$ не кратне 3	Ні	$p=2$:: короткий, чергування 2 значень

7	199	25	7	Парний, $m=12$	$(a-1)=24$ кратне 3 і 4	Так	$p=12$:: повний період, рівномірність підтверджено
8	274	22	53	Складений, (3^2) , $m=9$	$\gcd(8,9)=1$	Так	$p=9$:: повний цикл, рівно- мірний розподіл
9	307	29	49	Парний, $m=14$	$\gcd(7,14)=7$	Ні	$p=2$:: короткий період, парні цикли
10	307	29	29	Парний, $m=14$	$\gcd(1,14)=1$	Так	$p=14$:: повний період
11	157	18	3	Складений, $m=15$	$\gcd(3,15)=3$	Ні	$p=4$:: неповний цикл, зсув серій
12	157	6	3	Складений, $m=15$	a змінене: $(a-1=5)$	Не повніс- тю	$p=5$:: цикл довжиною 5

Результати. Експериментально підтверджено, що:

- повний період досягається лише за виконання всіх умов теореми Халла–Добелла, а саме: $\gcd(c, m)=1$, кратності $(a-1)$ усім простим дільникам m , та кратності 4, якщо m ділиться на 4;
- порушення хоча б однієї умови призводить до скорочення періоду в 2–5 разів;
- для модулів, кратних степеню двійки, порушення кратності $a-1$ до 4 одразу зменшує період удвічі;
- парні модулі зберігають лінійний характер гістограм, але можуть утворювати короткі повтори, якщо $\gcd(c, m) \neq 1$;
- заміна одного параметра (наприклад, a) може радикально змінити довжину циклу, що показано в експерименті №12.

Висновки. Експериментальні результати показали, що довжина періоду лінійного конгруентного генератора повністю залежить від добору параметрів a , c та m . Повний період виникає лише за виконання всіх умов теореми Халла–Добелла. Найсуттєвіший вплив має множник a , зміна якого навіть за сталих c і m здатна перетворити рівномірну послідовність на короткий повторюваний підцикл. Отже, коректний вибір параметрів є критичним для забезпечення повного періоду й рівномірності генерації псевдовипадкових чисел.

Література

1. Q. Sun, Z. Liu, H. Wang. An Online Evaluation Method for Random Number Entropy and Pseudo-Random Number Generators. *Entropy*. 2025. Vol. 27, № 2, 136. URL: <https://www.mdpi.com/1099-4300/27/2/136>. MDPI
2. E. Faure, E. Fedorov, I. Myronets, S. Sysoienko. Method for Generating Pseudorandom Sequence of Permutations Based on Linear Congruential Generator. *CEUR Workshop Proceedings*. 2022, Vol. 3137, pp. 15-24. URL: <https://ceur-ws.org/Vol-3137/paper15.pdf>.