

ЧЕБЫШЕВСКИЙ СБОРНИК

Том 27. Выпуск 2.

УДК: 511.36, 511, 519.6, 004.421.5

DOI: 10.22405/2226-8383-2026-27-2-118-127

О подходе к построению последовательности псевдослучайных чисел, основанном на разложениях E -функций с периодическими коэффициентами

В. Г. Чирский, А. Ю. Нестеренко, В. Ю. Матвеев

Чирский Владимир Григорьевич — доктор физико-математических наук, профессор, Московский государственный университет им. М. В. Ломоносова; Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации (г. Москва).
e-mail: vgchirskii@yandex.ru

Нестеренко Алексей Юрьевич — доктор физико-математических наук, профессор, Московский институт электроники и математики (г. Москва).
e-mail: nesterenko_a_y@mail.ru

Матвеев Владимир Юрьевич — кандидат физико-математических наук, Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации (г. Москва).
e-mail: salomaa@mail.ru

Аннотация

Пусть $T_1, \dots, T_m$ — попарно взаимно простые натуральные числа. Рассмотрим последовательности целых чисел $a_n^{(k,j)}$, $j = 1, \dots, m$, $k = 1, \dots, T_j$ удовлетворяющие условиям

$$a_n^{(k,j)} = a_{n+T_j}^{(k,j)}, j = 1, \dots, m, k = 1, \dots, T_j, n = 0, 1, \dots$$

Будем считать, что выполнены следующие условия.

- 1) Для каждого $j = 1, \dots, m$ пусть $a_n^{(1,j)} = 1$ для всех n .
- 2) Для каждого $j = 1, \dots, m$ пусть векторы $(a_0^{(k,j)}, \dots, a_{T_j-1}^{(k,j)})$, $k = 2, \dots, T_j$ линейно независимы с вектором $(a_0^{(1,j)}, \dots, a_{T_j-1}^{(1,j)}) = (1, \dots, 1)$.

Обозначим

$$F_{j,k}(z) = \sum_{n=0}^{\infty} \frac{a_n^{(k,j)}}{n!} z^n, j = 1, \dots, m, k = 1, \dots, T_j. \quad (1)$$

Проведённые эксперименты показали хорошие статистические свойства последовательностей двоичных цифр значений этих функций. Результаты экспериментов приведены в статье.

Ключевые слова: почти полиадические числа, псевдослучайные числа

Библиография: 15 названий.

Для цитирования:

Чирский В. Г., Нестеренко А. Ю., Матвеев В. Ю. О подходе к построению последовательности псевдослучайных чисел, основанном на разложениях E -функций с периодическими коэффициентами // Чебышевский сборник, 2026, т. 27, вып. 2, с. 118–127.

CHEBYSHEVSKII SBORNIK

Vol. 27. No. 2.

UDC: 511.36, 511, 519.6, 004.421.5

DOI: 10.22405/2226-8383-2026-27-2-118-127

An approach to constructing a sequence of pseudo-random numbers based on the expansions of E -functions with periodic coefficients

V. G. Chirskii, A. Y. Nesterenko, V. Y. Matveev

Chirskii Vladimir Grigor'evich — doctor of physical and mathematical sciences, professor, Lomonosov Moscow State University, Ranepa (Moscow).

e-mail: vgchirskii@yandex.ru

Nesterenko Alexey Yur'evich — doctor of physical and mathematical sciences, professor, Moscow Institute of Electronics and Mathematics (Moscow).

e-mail: nesterenko_a_y@mail.ru

Matveev Vladimir Yur'evich — candidate of physical and mathematical sciences, Russian Presidential Academy of National Economy and Public Administration (Moscow).

e-mail: salomaa@mail.ru

Abstract

Let $T_1, \dots, T_m$ be pairwise coprime natural numbers. Consider the sequences of integers $a_n^{(k,j)}$, $j = 1, \dots, m$, $k = 1, \dots, T_j$ that satisfy the conditions

$$a_n^{(k,j)} = a_{n+T_j}^{(k,j)}, j = 1, \dots, m, k = 1, \dots, T_j, n = 0, 1, \dots$$

We assume that the following conditions are met:

- 1) For each $j = 1, \dots, m$ let $a_n^{(1,j)} = 1$ for all n .
- 2) For each $j = 1, \dots, m$ let the vectors $(a_0^{(k,j)}, \dots, a_{T_j-1}^{(k,j)})$, $k = 2, \dots, T_j$ are linearly independent with the vector $(a_0^{(1,j)}, \dots, a_{T_j-1}^{(1,j)}) = (1, \dots, 1)$.

Denote

$$F_{j,k}(z) = \sum_{n=0}^{\infty} \frac{a_n^{(k,j)}}{n!} z^n, j = 1, \dots, m, k = 1, \dots, T_j. \quad (2)$$

The experiments conducted demonstrated good statistical properties of the binary digit sequences of these function values. The experimental results are presented in the article.

Keywords: almost polyadic numbers, pseudorandom numbers

Bibliography: 15 titles.

For citation:

Chirskii, V. G., Nesterenko, A.Yu., Matveev, V.Yu. 2026, "An approach to constructing a sequence of pseudo-random numbers based on the expansions of E -functions with periodic coefficients", *Chebyshevskii sbornik*, vol. 27, no. 2, pp. 118–127.

1. Основной результат

Пусть $T_1, \dots, T_m$ попарно взаимно простые натуральные числа. Рассмотрим последовательности целых чисел $a_n^{(k,j)}$, $j = 1, \dots, m$, $k = 1, \dots, T_j$ удовлетворяющие условиям

$$a_n^{(k,j)} = a_{n+T_j}^{(k,j)}, j = 1, \dots, m, k = 1, \dots, T_j, n = 0, 1, \dots$$

Будем считать, что выполнены следующие условия:

- 1) Для каждого $j = 1, \dots, m$ пусть $a_n^{(1,j)} = 1$ для всех n .
- 2) Для каждого $j = 1, \dots, m$ пусть векторы $(a_0^{(k,j)}, \dots, a_{T_j-1}^{(k,j)})$, $k = 2, \dots, T_j$ линейно независимы с вектором $(a_0^{(1,j)}, \dots, a_{T_j-1}^{(1,j)}) = (1, \dots, 1)$.

Обозначим

$$F_{j,k}(z) = \sum_{n=0}^{\infty} \frac{a_n^{(k,j)}}{n!} z^n, j = 1, \dots, m, k = 1, \dots, T_j. \quad (3)$$

В работе [1] доказана теорема:

Пусть целые числа $a_n^{(k,j)}$, $j = 1, \dots, m$, $k = 1, \dots, T_j$, $n = 0, 1, \dots$ удовлетворяют сформулированным выше условиям. Тогда функции

$$1, e^\gamma, F_{j,k}(z), j = 1, \dots, m, k = 2, \dots, T_j$$

линейно независимы над $\mathbb{C}(z)$ и для любого рационального $\gamma \neq 0$ числа

$$1, e^\gamma, F_{j,k}(\gamma), j = 1, \dots, m, k = 2, \dots, T_j \quad (4)$$

линейно независимы. Для любой ненулевой линейной формы

$$L(1, e^\gamma, F_{1,2}(\gamma), \dots, F_{1,T_1}(\gamma), \dots, F_{m,2}(\gamma), \dots, F_{m,T_m}(\gamma))$$

с целыми коэффициентами, не превосходящими по абсолютной величине числа H и любого ε , $0 < \varepsilon < \frac{1}{2}$ существует эффективная постоянная $b > 0$, зависящая от числа ε и чисел (4) такая, что

$$|L(1, e^\gamma, F_{1,2}(\gamma), \dots, F_{1,T_1}(\gamma), \dots, F_{m,2}(\gamma), \dots, F_{m,T_m}(\gamma))| > bH^{m-1-T_1-\dots-T_m}.$$

Были построены наборы линейно независимых векторов $a_n^{(k,j)}$, $j = 1, \dots, m$, $k = 1, \dots, T_j$ удовлетворяющих условиям

$$a_n^{(k,j)} = a_{n+T_j}^{(k,j)}, j = 1, \dots, m, k = 1, \dots, T_j, n = 0, 1, \dots$$

размером 3×3 , 5×5 и вычислены суммы вида $\sum_{n=1}^{100} \frac{a_n^{(k,j)}}{n!}$. Вычисленные суммы были переведены в двоичный вид и подвергнуты испытаниям с помощью статистического пакета NIST.

Для преобразования целой части числа полученных частичных сумм в двоичный вид, целая часть числа последовательно делилась на 2 с остатком, пока результат деления не становился равным нулю. Полученные при делении остатки – цифры нужного числа записывались начиная с последнего остатка.

Для преобразования дробной части числа полученных частичных сумм в двоичный вид, дробная часть числа последовательно умножалась на основание системы – 2 до тех пор, пока целая часть числа не становилась равной 1.0. Если в результате умножения снова появлялись целые части, они повторно обращались в нуль, предварительно запомнив значение получившейся целой части. Операция заканчивалась, когда дробная часть полностью обращалась в нуль.

Для теста использовалась последовательность из совмещенных двоичных последовательностей целой и дробной частей.

В приведенных ниже таблицах в правом столбце стоят дроби вида p/q , где q – количество выборок двоичных последовательностей, p – минимальное значение проходимости для каждого статистического теста, за исключением теста на случайное отклонение (вариант). Минимальное значение проходимости для теста на случайное отклонение (вариант) не определено. При проведении тестов размер выборки не превосходил 1500000 двоичных знаков, количество выборок равно 8.

Выбраны наихудшие результаты прохождения тестов.

$$a_n^{(k,j)} = (6, 5, 9)$$

Наименование в пакете NIST	$\sum_{n=1}^{100} \frac{a_n^{(k,j)}}{n!}$
Frequency	10/10
BlockFrequency	10/10
CumulativeSums	10/10
CumulativeSums	10/10
Runs	10/10
LongestRun	9/10
Rank	10/10
FFT	10/10
NonOverlappingTemplate	8/10
OverlappingTemplate	10/10
Universal	10/10
ApproximateEntropy	9/10
RandomExcursions	— — — — —
RandomExcursionsVariant	— — — — —
Serial	10/10
LinearComplexity	10/10

$$a_n^{(k,j)} = (9, 4, 6)$$

Наименование в пакете NIST	$\sum_{n=1}^{100} \frac{a_n^{(k,j)}}{n!}$
Frequency	10/10
BlockFrequency	10/10
CumulativeSums	10/10
CumulativeSums	10/10
Runs	10/10
LongestRun	10/10
Rank	10/10
FFT	10/10
NonOverlappingTemplate	8/10
OverlappingTemplate	9/10
Universal	10/10
ApproximateEntropy	10/10
RandomExcursions	— — — — —
RandomExcursionsVariant	— — — — —
Serial	10/10
LinearComplexity	10/10

$$a_n^{(k,j)} = (1, 1, 1, 1, 1)$$

Наименование в пакете NIST	$\sum_{n=1}^{100} \frac{a_n^{(k,j)}}{n!}$
Frequency	10/10
BlockFrequency	10/10
CumulativeSums	10/10
CumulativeSums	10/10
Runs	10/10
LongestRun	10/10
Rank	10/10
FFT	10/10
NonOverlappingTemplate	8/10
OverlappingTemplate	10/10
Universal	10/10
ApproximateEntropy	9/10
RandomExcursions	— — — — —
RandomExcursionsVariant	— — — — —
Serial	10/10
LinearComplexity	10/10

$$a_n^{(k,j)} = (4, 5, 1, 4, 2)$$

Наименование в пакете NIST	$\sum_{n=1}^{100} \frac{a_n^{(k,j)}}{n!}$
Frequency	9/10
BlockFrequency	10/10
CumulativeSums	9/10
CumulativeSums	9/10
Runs	10/10
LongestRun	10/10
Rank	10/10
FFT	9/10
NonOverlappingTemplate	9/10
OverlappingTemplate	10/10
Universal	10/10
ApproximateEntropy	9/10
RandomExcursions	— — — — —
RandomExcursionsVariant	— — — — —
Serial	10/10
LinearComplexity	9/10

$$a_n^{(k,j)} = (8, 7, 5, 7, 5)$$

Наименование в пакете NIST	$\sum_{n=1}^{100} \frac{a_n^{(k,j)}}{n!}$
Frequency	10/10
BlockFrequency	10/10
CumulativeSums	10/10
CumulativeSums	10/10
Runs	10/10
LongestRun	10/10
Rank	9/10
FFT	10/10
NonOverlappingTemplate	9/10
OverlappingTemplate	10/10
Universal	10/10
ApproximateEntropy	10/10
RandomExcursions	— — — — —
RandomExcursionsVariant	— — — — —
Serial	10/10
LinearComplexity	8/10

$$a_n^{(k,j)} = (2, 6, 2, 2, 1)$$

Наименование в пакете NIST	$\sum_{n=1}^{100} \frac{a_n^{(k,j)}}{n!}$
Frequency	9/10
BlockFrequency	10/10
CumulativeSums	9/10
CumulativeSums	9/10
Runs	10/10
LongestRun	10/10
Rank	10/10
FFT	9/10
NonOverlappingTemplate	9/10
OverlappingTemplate	10/10
Universal	10/10
ApproximateEntropy	9/10
RandomExcursions	— — — — —
RandomExcursionsVariant	— — — — —
Serial	10/10
LinearComplexity	9/10

$$a_n^{(k,j)} = (9, 6, 3, 1, 8)$$

Наименование в пакете NIST	$\sum_{n=1}^{100} \frac{a_n^{(k,j)}}{n!}$
Frequency	10/10
BlockFrequency	10/10
CumulativeSums	9/10
CumulativeSums	9/10
Runs	10/10
LongestRun	10/10
Rank	10/10
FFT	9/10
NonOverlappingTemplate	8/10
OverlappingTemplate	10/10
Universal	10/10
ApproximateEntropy	10/10
RandomExcursions	— — — — —
RandomExcursionsVariant	— — — — —
Serial	9/10
LinearComplexity	10/10

Для проверки совокупного качества полученных последовательностей цифр все эти три последовательности были совмещены в одну (просто поставлены одна за другой) и снова подвергнуты проверке с помощью тестов NIST.

$$a_n^{(k,j)} = \begin{pmatrix} 1 & 1 & 1 \\ 6 & 5 & 9 \\ 9 & 4 & 6 \end{pmatrix}$$

Наименование в пакете NIST	$\sum_{n=1}^{100} \frac{a_n^{(k,j)}}{n!}$
Frequency	10/10
BlockFrequency	10/10
CumulativeSums	10/10
CumulativeSums	10/10
Runs	10/10
LongestRun	10/10
Rank	10/10
FFT	10/10
NonOverlappingTemplate	9/10
OverlappingTemplate	10/10
Universal	10/10
ApproximateEntropy	10/10
RandomExcursions	1/1
RandomExcursionsVariant	1/1
Serial	10/10
LinearComplexity	9/10

$$a_n^{(k,j)} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 5 & 4 & 1 & 4 & 2 \\ 8 & 7 & 5 & 7 & 5 \\ 2 & 6 & 2 & 2 & 1 \\ 9 & 6 & 3 & 1 & 8 \end{pmatrix}$$

Наименование в пакете NIST	$\sum_{n=1}^{100} \frac{a_n^{(k,j)}}{n!}$
Frequency	10/10
BlockFrequency	10/10
CumulativeSums	10/10
CumulativeSums	10/10
Runs	10/10
LongestRun	10/10
Rank	10/10
FFT	9/10
NonOverlappingTemplate	9/10
OverlappingTemplate	10/10
Universal	10/10
ApproximateEntropy	10/10
RandomExcursions	— — — — —
RandomExcursionsVariant	— — — — —
Serial	9/10
LinearComplexity	9/10

2. Заключение

Отметим что специально выбраны наихудшие из результатов испытаний и даже они оказались весьма хорошими. Кроме приведённых выше примеров, были проведены числовые экс-

перименты с различными $a_n^{(k,j)}$, N и они также дали хорошие результаты.

В работе [7] были рассмотрены ряды вида $\sum_{n=0}^{\infty} a_n \cdot n!$ с хорошими статистическими свойствами и простотой получения частичных сумм.

Планируется расширить класс рассматриваемых объектов и получить новые источники хороших псевдослучайных чисел.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Нестеренко А. Ю., Чирский В. Г. Линейная независимость значений E -функций с периодическими коэффициентами // Чебышевский сборник, 2025, т. 26, вып. 4, с. 461—466.
2. Чирский В. Г.; Нестеренко А. Ю. Об одном подходе к преобразованию периодических последовательностей. // Дискрет. матем.-2015.-т.27.-№4.-с. 150—157
3. Шидловский А. Б. Трансцендентные числа.-М: "Наука".-1987.-448 с. (Английский перевод: [3] Andrei B. Shidlovskii. Transcendental Numbers. W. de Gruyter.-Berlin.-New York.-1989.-
4. Салихов В. Х. Об алгебраической независимости значений E -функций, удовлетворяющих линейным дифференциальным уравнениям первого порядка. // Мат. заметки.-1973.- Т.13.- №1.- С.29—40.
5. Bertrand D; Chirskii V, Yebbou J. Effective estimates for global relations on Euler-type series. // Ann. Fac. Sci. Toulouse.-2004.-V.XIII.-no.2.-PP.241—260.
6. Алферов А. П.; Зубов А. Ю.; Кузьмин А. С.; Черемушкин А. В. Основы криптографии.- М.: Гелиос.-2001.-480с.
7. Матвеев В. Ю. Бесконечная алгебраическая независимость некоторых почти полиадических чисел. // Чебышевский сборник. 2024;25(3):365—372.
8. Chirskii V. G. Product formula, global relations and polyadic integers. // Russian Journal of Mathematical Physics, 2019, том 26, №3, с. 286—305.
9. Chirskii V. G. Arithmetic properties of generalized hypergeometric F series // Russ. J. Math. Phys., 2020, v.27, no.2, pp.175—184.
10. Чирский В. Г. Арифметические свойства значений обобщенных гипергеометрических рядов с полиадическими трансцендентными параметрами // Доклады Академии наук, сер. матем. информ, проц, управл., 2022, т.506, с.95—107.
11. Чирский В. Г. Трансцендентность p -адических значений обобщенных гипергеометрических рядов с трансцендентными полиадическими параметрами // Доклады Академии наук, сер. матем. информ, проц, управл., 2023, т.510, с.29—32.
12. Чирский В. Г. Трансцендентность некоторых 2-адических чисел // Чебышевский сборник.- 2023.- т. 24.- вып.5, с.194 — 200.
13. Матвеев В. Ю. Свойства элементов прямых произведений полей // Чебышевский сборник.- 2019.- т. 20.- вып. 2, с. 383 — 390.
14. Чирский В. Г. Бесконечная алгебраическая независимость полиадических рядов с периодическими коэффициентами // Доклады Российской академии наук. Математика, информатика, процессы управления, издательство Российская академия наук (Москва), 2024, том 519, с. 16—19

15. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications // <https://doi.org/10.6028/NIST.SP.800-22r1a>

REFERENCES

1. Nesterenko, A.Yu. & Chirskii, V.G. 2025, “Linear independence of values of E -functions with periodic coefficients”, *Chebyshevskii Sbornik*, vol. 26, no. 4, pp. 461–466.
2. Chirskii, V.G. & Nesterenko, A.Yu. 2017, “An approach to the transformation of periodic sequences”, *Discrete Mathematics and Applications*, vol. 27, no. 1, pp. 1–6, Walter de Gruyter, Berlin – New York.
3. Shidlovskii, A.B. 1989, *Transcendental numbers*, Walter de Gruyter, Berlin – New York, 467 p.
4. Salikhov, V.Kh. 1973, “On algebraic independence of the values of E -functions satisfying first order linear differential equations” [Ob algebraicheskoi nezavisimosti znachenii E -funktsii, udovletvoryayushchikh lineinym differentsialnym uravneniyam pervogo poriyadka], *Matematicheskie Zametki*, vol. 13, no. 1, pp. 29–40.
5. Bertrand, D., Chirskii, V. & Yebbou, J. 2004, “Effective estimates for global relations on Euler-type series”, *Annales de la Faculté des Sciences de Toulouse*, vol. 13, no. 2, pp. 241–260.
6. Alferov, A.P., Zubov, A.Yu., Kuzmin, A.S. & Cheremushkin, A.B. 2001, *Fundamentals of cryptography* [Osnovy kriptografii], Helios, Moscow, 480 p.
7. Matveev, V.Yu. 2024, “Infinite algebraic independence of some almost polyadic numbers”, *Chebyshevskii Sbornik*, vol. 25, no. 3, pp. 365–372.
8. Chirskii, V.G. 2019, “Product formula global relations and polyadic integers”, *Russian Journal of Mathematical Physics*, vol. 26, no. 3, pp. 286–305.
9. Chirskii, V.G. 2020, “Arithmetic properties of generalized hypergeometric F -series”, *Russian Journal of Mathematical Physics*, vol. 27, no. 2, pp. 175–184.
10. Chirskii, V.G. 2022, “Arithmetic properties of the values of generalized hypergeometric series with polyadic transcendental parameters”, *Doklady Akademii Nauk*, vol. 506, pp. 95–107.
11. Chirskii, V.G. 2023, “Transcendence of p -adic values of generalized hypergeometric series with transcendental polyadic parameters”, *Doklady Akademii Nauk*, vol. 510, pp. 29–32.
12. Chirskii, V.G. 2023, “Transcendence of some 2-adic numbers”, *Chebyshevskii Sbornik*, vol. 24, no. 5, pp. 194–200.
13. Matveev, V.Yu. 2019, “Properties of elements of direct products of fields”, *Chebyshevskii Sbornik*, vol. 20, no. 2, pp. 383–390.
14. Chirskii, V.G. 2024, “Infinite algebraic independence of polyadic series with periodic coefficients”, *Doklady Rossiiskoi Akademii Nauk. Matematika, Informatika, Protsessy Upravleniya*, vol. 519, pp. 16–19.
15. National Institute of Standards and Technology (NIST) 2010, *A statistical test suite for random and pseudorandom number generators for cryptographic applications*, NIST Special Publication 800-22 Revision 1a, [Online] Available at: <https://doi.org/10.6028/NIST.SP.800-22r1a> [Accessed 13 May 2026].

Получено: 23.01.2026

Принято в печать: 19.05.2026