ЧЕБЫШЕВСКИЙ СБОРНИК

Том 17 Выпуск 3

УДК 511.36

О ПРЕОБРАЗОВАНИЯХ ПЕРИОДИЧЕСКИХ
ПОСЛЕДОВАТЕЛЬНОСТЕЙ

В. Г. Чирский (г. Москва)

Аннотация

При исследовании генераторов псевдослучайных чисел одна из проблем — является ли периодической вырабатываемая генератором последовательность? Некоторые генераторы в принципе дают периодическую последовательность.

Для того, чтобы избавиться от периодичности или увеличить длину периода, применяются различные методы. Упомянем фильтрующие или комбинирующие генераторы. Однако их использование может привести к тому, что общая длина вырабатываемой последовательности сократится.

Выразим общую идею предлагаемого другого подхода следующими словами: требуется указать простой способ, который вносит беспорядок в изначально упорядоченное множество. Представим себе, что заданная периодическая последовательность состоит из цифр в некоторой позиционной системе счисления. Сопоставим этим цифрам новое число, полученное в результате некоторого, достаточно простого, преобразования этой последовательности цифр. Если это новое число является иррациональным, то последовательность его цифр является непериодической.

Например, если рассматривать натуральные числа $a_1, \dots, a_T$ как элементы периодической цепной (непрерывной) дроби, то по теореме Лагранжа, полученное число является квадратичной иррациональностью. Отметим, что это число является плохо приближаемым рациональными числами.

Другой способ, основанный на той же основной идее состоит в рассмотрении рядов вида

$$\sum_{n=0}^{\infty} \frac{a_n}{n!}$$

с периодической последовательностью целых чисел $\{a_n\}$, $a_{n+T} = a_n$ возможность получения оценки порядка приближения этих чисел.

Однако для вычисления цифр числа такого вида требуется много операций деления. Можно рассмотреть ряды вида

$$\sum_{n=0}^{\infty} a_n n!$$

с периодической последовательностью натуральных чисел $\{a_n\}$, $a_{n+T} = a_n$. Описываются некоторые свойства таких рядов.

Ключевые слова: периодические последовательности, полиадические числа.

Библиография: 15 названий.

ON TRANSFORMATIONS OF PERIODIC SEQUENCES

V. G. Chirskii (Moscow)

Abstract

One of essential problems in generating pseudo-random numbers is the problem of periodicity of the resulting numbers. Some generators output periodic sequences. To avoid it several ways are used.

Here we present the following approach: supposed we have some order in the considered set. Let's invent some algorithm which produces disorder in the set. E.g. if we have a periodic sequence of integers, let's construct an irrational number implying the given set. Then the figures of the resulting number form a non-periodic sequence.

Here we can use continued fractions and Lagrange's theorem asserts that the resulting number is irrational.

Another approach is to use series of the form $\sum_{n=0}^{\infty} \frac{a_n}{n!}$ with a periodic sequence of integers $\{a_n\}$, $a_{n+T} = a_n$ which is irrational.

Here we consider polyadic series $\sum_{n=0}^{\infty} a_n n!$ with a periodic sequence of positive integers $\{a_n\}$, $a_{n+T} = a_n$ and describe some of their properties.

Keywords: periodic sequences, polyadic integers.

Bibliography: 15 titles.

1. Введение и постановка задачи

При исследовании генераторов псевдослучайных чисел одна из проблем — является ли периодической вырабатываемая генератором последовательность? Некоторые генераторы в принципе дают периодическую последовательность, например, линейный конгруэнтный метод [1].

Для того, чтобы избавиться от периодичности или увеличить длину периода, применяются различные методы. Упомянем фильтрующие или комбинирующие генераторы. Однако их использование может привести к тому, что общая длина вырабатываемой последовательности сократится.

2. Об одном подходе к преобразованию периодических последовательностей

Выразим общую идею предлагаемого другого подхода следующими словами: требуется указать простой способ, который вносит беспорядок в изначально упорядоченное множество. Представим себе, что заданная периодическая последовательность состоит из цифр в некоторой позиционной системе счисления. Сопоставим этим цифрам новое число, полученное в результате некоторого, достаточно простого, преобразования этой последовательности цифр. Если это новое число является иррациональным, то последовательность его цифр является непериодической.

Например, если рассматривать натуральные числа $a_1, \dots, a_T$ как элементы периодической цепной (непрерывной) дроби, то по теореме Лагранжа [2], полученное число является квадратичной иррациональностью. Отметим, что это число является плохо приближаемым рациональными числами [3].

Другой способ, основанный на той же основной идее, приведен в статье [4]. Там рассматривались ряды вида

$$\sum_{n=0}^{\infty} \frac{a_n}{n!} \quad (1)$$

с периодической последовательностью целых чисел $\{a_n\}$, $a_{n+T} = a_n$ и была доказана иррациональность таких чисел, если хотя бы одно из чисел $a_1, \dots, a_T$ отлично от 0. Кроме того, использование метода Зигеля–Шидловского дает имеется возможность получения оценки порядка приближения этих чисел рациональными числами (1). рациональными числами. Более точные оценки можно получить, например, используя аппроксимации Эрмита–Паде [5].

Однако для вычисления цифр числа вида (1) требуется много операций деления. В работе [5] рассматривались ряды вида

$$\sum_{n=0}^{\infty} a_n n! \quad (2)$$

с периодической последовательностью натуральных чисел $\{a_n\}$, $a_{n+T} = a_n$. Вычисление частичных сумм таких рядов значительно легче. Их можно строить, используя только операцию сложения. Разумеется, ряды вида (2) расходятся в поле действительных чисел, однако сходятся в любом поле p -адических чисел. Действительно, для сходимости таких чисел требуется, чтобы $|a_n n!|_p \rightarrow 0$ при $n \rightarrow \infty$. Справедливо равенство $|n!|_p = p^{-\frac{n-S_n}{p-1}}$, где S_n обозначает сумму цифр в p -ичном разложении числа n , так что $S_n \leq (p-1) \log_p n$. Ввиду неравенства $|a_n|_p \leq 1$ (число a_n — целое), получаем требуемое: $|a_n n!|_p \rightarrow 0$ при $n \rightarrow \infty$.

Доказательство иррациональности чисел вида (2) в каждом конкретном поле p -адических чисел представляет собой очень трудную задачу. Однако если рассматривать всю совокупность полей p -адических чисел, можно установить определенные арифметические свойства рядов (2).

В работе [5] предложена классификация, учитывающая всю совокупность полей p -адических чисел. Пусть $\mathbb{Z}_p$ обозначает кольцо целых чисел поля p -адических чисел. Рассмотрим прямое произведение этих колец по всем простым числам p . Это прямое произведение называется кольцом целых полиадических чисел [6], [7]. Оно изоморфно канторову множеству. Кстати, рассматриваемые ряды вида (2) образуют счетное множество. Действительно, выписав подряд все цифры десятичных разложений чисел $a_1, \dots, a_T$ мы получим некоторое натуральное число, цифры которого можно считать периодом разложения некоторого рационального числа. Каждому такому числу соответствует конечное число возможных различных наборов натуральных чисел, цифры которых дают это число. (Например, числу 123 соответствуют наборы $\{1, 2, 3\}, \{12, 3\}, \{1, 23\}, \{123\}$).

Элементы $\mathbf{a}$ этого кольца — целые полиадические числа — имеют каноническое представление в виде $\mathbf{a} = \sum_{n=0}^{\infty} a_n n!$, $a_n \in \{0, 1, \dots, n\}$. Рассмотренные выше ряды (2) не являются каноническими разложениями, так как для начальных членов ряда неравенство $a_n \leq n$ может не выполняться, однако суммы этих рядов — целые полиадические числа и преобразовав начальную часть ряда к каноническому виду мы получим полиадическое число, каноническое разложение которого является периодическим, начиная с некоторого места.

Так как ряд (2) сходится в любом кольце $\mathbb{Z}_p$, обозначим $\mathbf{a}^{(p)}$ сумму ряда в этом кольце. Таким образом, полиадическое число $\mathbf{a}$ можно рассматривать как вектор с координатами $\mathbf{a}^{(p)}$. На прямом произведении колец вводится покоординатное сложение и умножение элементов. Поэтому многочлену $P(x)$ с целыми коэффициентами сопоставляется его полиадическое значение в точке $\mathbf{a}$, обозначаемое $P(\mathbf{a})$ и представляющее собой полиадическое число с координатами $P(\mathbf{a}^{(p)})$ в каждом кольце $\mathbb{Z}_p$. Если для полиадического числа $\mathbf{a}$ существует отличный от тождественного нуля многочлен $P(x)$ с целыми коэффициентами такой, что $P(\mathbf{a}^{(p)}) = 0$ в каждом кольце $\mathbb{Z}_p$, то это полиадическое число $\mathbf{a}$ называется алгебраическим. В противном случае оно называется трансцендентным. Это означает, что для любого отличного от тождественного нуля многочлена $P(x)$ с целыми коэффициентами существует кольцо $\mathbb{Z}_p$ такое, что в нем $P(\mathbf{a}^{(p)}) \neq 0$. Число называем бесконечно трансцендентным, если для любого отличного от тождественного нуля многочлена $P(x)$ с целыми коэффициентами существует бесконечное множество колец $\mathbb{Z}_p$ таких, что в них $P(\mathbf{a}^{(p)}) \neq 0$. Глобальная трансцендентность означает, что

для любого отличного от тождественного нуля многочлена $P(x)$ с целыми коэффициентами и любого кольца $\mathbb{Z}_p$ выполнено неравенство $P(a^{(p)}) \neq 0$.

Как уже отмечено выше, доказательство глобальной трансцендентности — трудная задача. Однако в работе [5] установлена бесконечная трансцендентность чисел вида (2), в частности, бесконечная трансцендентность числа Эйлера $\sum_{n=0}^{\infty} n!$.

В работе [8] приведена общая теорема о бесконечной трансцендентности полиадических значений a некоторого подкласса F -рядов. В ней также даны зависящие от параметров многочлена $P(x)$ границы бесконечного множества интервалов, в каждом из которых есть хотя бы одно простое число p такое, что $P(a^{(p)}) \neq 0$ в кольце $\mathbb{Z}_p$. Отметим работы [9] – [14], в которых устанавливаются.

Хотя из приведенных выше результатов не следует иррациональность ряда (2) в каком-то кольце $\mathbb{Z}_p$ (означающая непериодичность соответствующего p -ичного разложения), практические вычисления [15] показали, что даже для простейшего ряда Эйлера $\sum_{n=0}^{\infty} n!$ цифры десятичных разложений его частичных сумм $\sum_{n=0}^N n!$ распределены достаточно случайно.

Это наблюдение, как и приведенные выше сведения о периодических цепных дробях и рядах вида (1) с периодическими коэффициентами, поддерживает гипотезу о том, что наличие периодичности коэффициентов в некоторых непозиционных способах представлений приводит к отсутствию периодичности в позиционных разложениях этих чисел.

В заключение приведем еще одно соображение. Позиционную q -ичную систему счисления часто изображают в виде дерева, из каждой вершины которого выходит q ветвей, соответствующих цифрам этой системы счисления. Это дает самоподобную фрактальную структуру. Если же рассматривать полиадические разложения, то это приведет к дереву, у которого количество ветвей на каждом следующем уровне на единицу больше, чем было на предыдущем уровне. Это, конечно, не доказывает, что если число имело периодическое полиадическое разложение (2), то в позиционной системе счисления его представление не является периодическим, но служит некоторым пояснением к этой гипотезе.

3. Заключение

Статья дает краткий обзор задачи о преобразовании периодической последовательности в непериодическую.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Д. Кнут. Искусство программирования для ЭВМ. (том 2). -М. : Мир. -1977. -724 с.
2. А. Я. Хинчин. Цепные дроби. -М. :Физматгиз. -1961
3. С. Ленг. Введение в теорию диофантовых приближений. -М. : Мир. -1979. -104с.
4. Чирский В. Г., Нестеренко А. Ю. Об одном подходе к преобразованию периодических последовательностей // Дискретная математика. 2015, том 27, выпуск 4, 150–157.
5. Нестеренко Ю. В. Приближения Эрмита-Паде обобщенных гипергеометрических функций. // Матем. сб. 1994, т. 185, № 3, с. 39–72.
6. Чирский В. Г. Арифметические свойства полиадических рядов с периодическими коэффициентами // Доклады Академии наук. Математика. 2014. т. 439, № 6, с. 677–679
7. Новоселов Е. В. Введение в полиадический анализ. -Петрозаводск, -1982. -112 с.
8. Постников А. Г. Введение в аналитическую теорию чисел. -М. : Наука. -1971. -416с.

9. Чирский В. Г. Арифметические свойства целых полиадических чисел // Чебышевский сборник. т. 16, вып. 1(2015), с. 254–264.
10. Чирский В. Г., Матвеев В. Ю. О ряде из произведений членов арифметической прогрессии. // Преподаватель 21 века, № 4, 2013, стр. 245–254
11. В. Ю. Матвеев «О значениях некоторого ряда в полиадических точках, хорошо приближаемых натуральными числами», Преподаватель 21 век, № 4, 2013, стр. 339–354
12. Матвеев В. Ю. О бесконечной алгебраической независимости некоторых полиадических чисел. // Материалы международной конференции «Математика и информатика», Москва, 13-17 марта 2016. с. 125–126.
13. Чирский В. Г. О преобразованиях периодических последовательностей. // Материалы международной конференции «Математика и информатика», Москва, 13-17 марта 2016. с. 143–144.
14. Лужина Л. М., Макаров Ю. Н. Достаточное условие алгебраической зависимости полиадических рядов // Материалы международной конференции «Математика и информатика», Москва, 13-17 марта 2016. с. 123–124.
15. Чирский В. Г., Матвеев В. Ю. О некоторых свойствах полиадических разложений // Чебышевский сборник. т. 14, вып. 2(2013), с. 163–172.

REFERENCES

1. Knuth. D., 1969, "The art of computer programming", *Addison-Wesley*.
2. Khintchin A. Ya., 1964, "Continued fractions", *Univ. Chicago Press*.
3. Lang S., 1966, "Introduction to Diophantine approximation", *Addison-Wesley*.
4. Chirskii V. G., Nesterenko A. Yu., 2015, "On an approach to transforming periodic sequences", *Discretnaya matematika*, v. 27, no. 4, pp. 150–157 (Russian)
5. Nesterenko Yu. V., 1995, "Hermite-Pade approximations of generalized hypergeometric functions", *Engl. transl. Russ. Acad. Sci. Sb. Math*, 85, pp. 189–219.
6. Chirskii V. G., 2014, "Arithmetic properties of polyadic series with periodic coefficients", *Doklady Mathematics*, v. 90, no. 3, pp. 766–768.
7. Novoselov E. V., 1982, "Introduction to polyadic calculus", *Petrozavodsk*, 112 p. (Russian)
8. Postnikov A. G., 1971, "Introduction to analytic number theory", Moscow, *Nauka*, 416 p. (Russian)
9. Chirskii V. G., 2015, "Arithmetic properties of polyadic integers", *Tchebyshevskiy sbornik*, v. 16, no. 1, pp. 254–264. (Russian)
10. Chirskii V. G., Matveev V. Yu., 2013, "On a series of products of terms of an arithmetic progression", *Prepodavatel 21 veka*, no. 4, pp. 245–254. (Russian)
11. Matveev V. Yu., 2013, "On the values of a certain series at points, well approximable by positive integers", *Prepodavatel 21 veka*, no. 4, pp. 339–354. (Russian)

12. Matveev V. Yu., 2016, "On the infinite algebraic independence of certain polyadic numbers", *Proceedings of an international conference "Matematica I informatica"*, Moscow, March 13-17, pp. 125–126. (Russian)
13. Chirskii V. G., 2016, "On transformations of periodic sequences", *Proceedings of an international conference "Matematica I informatica"*, Moscow, March 13-17, pp. 143–144. (Russian)
14. Luzhina L. M., Makarov Yu. N., 2016, "A sufficient condition of the algebraic dependence of polyadic series", *Proceedings of an international conference "Matematica I informatica"*, Moscow, March 13-17, pp. 123–124. (Russian)
15. Chirskii V. G., Matveev V. Yu., 2013, "On certain properties of polyadic expansions", *Chebyshevskiy sbornik*, v. 14, no. 2, pp. 163–172. (Russian)

Московский педагогический государственный университет.

Получено 30.06.2016 г.

Принято в печать 12.09.2016 г.