МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

УЧЕНЫЕ ЗАПИСКИ ОРЛОВСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА

НАУЧНЫЙ ЖУРНАЛ

№ 6

Часть 2

ОРЕЛ – 2012

УЧЕНЫЕ ЗАПИСКИ
ОРЛОВСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА
НАУЧНЫЙ ЖУРНАЛ
№ 6
Часть 2

Серия «Естественные, технические и медицинские науки»

Решением Президиума ВАК Министерства образования и науки Российской Федерации журнал «Ученые записки Орловского государственного университета» включен в перечень ведущих рецензируемых научных журналов и изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученых степеней доктора и кандидата наук по следующим отраслям научных специальностей: 01.00.00 – физико-математические науки; 02.00.00 – химические науки; 03.00.00 – биологические науки; 06.00.00 – сельскохозяйственные науки; 07.00.00 – исторические науки; 08.00.00 – экономические науки; 09.00.00 – философские науки; 10.00.00 – филологические науки; 12.00.00 – юридические науки; 13.00.00 – педагогические науки; 14.00.00 – медицинские науки; 17.00.00 – искусствоведение; 19.00.00 – психологические науки; 25.00.00 – науки о Земле.

Труды опубликованы по решению редакционно-издательской коллегии журнала «Ученые записки Орловского государственного университета» и организационного комитета X Международной конференции «Алгебра и теория чисел: современные проблемы и приложения» (Волгоград, 10–16 сентября 2012 г.); подготовлены в Издательстве ВГСПУ «Перемена» при поддержке Российского фонда фундаментальных исследований, проект №12-01-06064-г.

Учредитель –

ФГБОУ ВПО «Орловский государственный университет»
Адрес редакции: 302026, г. Орел, ул. Комсомольская, 95,
Орловский государственный университет
Редакция журнала «Ученые записки ОГУ»
E-mail: utchen-zap@univ-orel.ru

ISSN 1998-2739

СОДЕРЖАНИЕ

***А.Ю. НЕСТЕРЕНКО* (*Москва*)**

О СТАТИСТИЧЕСКИХ СВОЙСТВАХ НЕКОТОРЫХ ТРАНСЦЕНДЕНТНЫХ ЧИСЕЛ

Предложен подход к генерации псевдослучайных последовательностей, основанный на представлениях одного класса действительных чисел. Описаны алгоритм генерации, результаты практических вычислений, а также дана методика тестирования полученных последовательностей.

Ключевые слова: ***генерация псевдослучайных последовательностей, нормальные и трансцендентные числа, статистические тесты.***

Пусть $\alpha > 0$ — действительное число и $b \geq 2$ — некоторое натуральное число. Мы будем говорить, что число α представлено в системе счисления по основанию b, если выполнено равенство

$$\alpha = \sum_{n=0}^{\infty} a_n b^{-n}, \quad a_n \in \mathbb{Z}, \quad \text{и} \quad 0 \leq a_n < b \quad \text{при} \quad n > 0. \tag{1}$$

Величину a_0 мы будем называть *целой частью* числа α, а натуральные числа $a_1,\ a_2, \ldots$ — *коэффициентами* разложения числа α по основанию b.

Мы будем называть ряд (1) *периодическим*, если найдется такое натуральное τ и некоторый индекс n_0, что для всех $n > n_0$ выполнено равенство $a_n = a_{n+\tau}$. Хорошо известно следующее утверждение.

Лемма 1 (см., напр., [8, п. 4.6]). *Разложение (1) конечно или периодично тогда и только тогда, когда число α рационально.*

Из утверждения леммы следует, что последовательность $a_1,\ a_2, \ldots$ коэффициентов разложения любого иррационального числа является бесконечной и не имеет периода. Рассмотрим вопрос о распределении элементов этой последовательности более внимательно.

Для некоторого натурального k зафиксируем произвольные целые числа $\delta_1, \ldots, \delta_k$ такие, что $0 \leq \delta_i < b$ для всех $i = 1,\ \ldots,\ k$, и определим величину $N_m(\alpha, b, \delta_1, \ldots, \delta_k)$, задающую число выполнений равенства

$$(a_{n+1},\ \ldots,\ a_{n+k}) = (\delta_1,\ \ldots,\ \delta_k), \quad n = 1,\ 2,\ \ldots,\ m.$$

Мы будем называть число α *нормальным* по основанию b [9], если при любом натуральном k и любом наборе $(\delta_1,\ \ldots,\ \delta_k)$ выполнено равенство

$$\lim_{m\to\infty} \frac{N_m(\alpha, b, \delta_1, \ldots, \delta_k)}{m} = \frac{1}{b^k}.$$

Мы будем называть число *абсолютно нормальным*, если оно является нормальным по любому основанию b.

Для некоторых иррациональных чисел специального вида известно, что они являются нормальными [7; 9; 15; 16]. Однако для произвольного иррационального числа α не известен критерий, позволяющий определить, является ли число α нормальным или нет. Известен лишь следующий результат.

Теорема 1 (Н.М. Коробов, [7]). *Пусть $\alpha > 0$ — иррациональное число. Тогда α является нормальным числом по основанию b, если последовательность величин*[1] $\{\alpha b^n\}$, $n = 0,\ 1,\ \ldots$ *является реализацией равновероятно распределенной на интервале $(0,1)$ случайной величины.*

[1] Напомним, что символом $\{\alpha\}$ мы обозначаем дробную часть числа α, т.е. $\{\alpha\} = \alpha - \lfloor\alpha\rfloor$.

Вместе с тем известна гипотеза [14] о том, что число π является нормальным при $b = 10$ и $b = 16$. В настоящей статье мы рассматриваем некоторый класс чисел и на основании проведенных экспериментов выдвигаем гипотезу о том, что числа из данного класса также являются нормальными при $b = 256$.

1. Трансцендентность некоторых чисел

Рассмотрим множество действительных чисел α, которые могут быть представлены в виде

$$\alpha = \sum_{n=0}^{\infty} R(n) b^{-n}, \quad R(n) > 0, \quad R(n) \in \mathbb{Q}, \tag{2}$$

где $R(x)$ есть рациональная функция с коэффициентами из поля $\mathbb{Q}$ такая, что

$$R(x) = \frac{P(x)}{Q(x)}, \quad P(x), Q(x) \in \mathbb{Q}[x], \quad \deg P(x) < \deg Q(x).$$

В большом множестве рассмотрим частное подмножество и определим величины $R(n)$ равенством

$$R(n) = \frac{u_1}{(dn+1)^s} + \dots + \frac{u_m}{(dn+m)^s} \tag{3}$$

для некоторых натуральных d, s, m и величин $u_1, \ \dots, \ u_m \in \mathbb{Q}$. В работе [13] для таких чисел было введено обозначение

$$\alpha = P(b, s, d, (u_1, \ \dots, \ u_m)) = \sum_{n=0}^{\infty} \sum_{k=1}^{m} \frac{u_k b^{-n}}{(dn+k)^s}. \tag{4}$$

Многие константы [12] могут быть представлены в виде (4), например:

$$\begin{aligned}
\pi &= P(16, 1, 8, (4, 0, 0, -2, -1, -1, 0, 0)),\\
\ln 2 &= P(2, 1, 1, (1)),\\
\arctan 2 &= P(16, 1, 8, (8, 0, 4, 0, -2, 0, -1, 0)),\\
8\sqrt{2} \ln\left(1 + \sqrt{2}\right) &= \alpha(16, 1, 8, (8, 0, 4, 0, 2, 0, 1, 0)).
\end{aligned}$$

Легко показать, что при $s = d = 1$ числа α с рациональной функцией вида (3) являются трансцендентными.

Лемма 2. *Пусть $m \geq 1$ — целое число, $u_1, \ \dots, \ u_m \in \mathbb{Q}$ и*

$$R(n) = \frac{u_1}{n+1} + \dots + \frac{u_m}{n+m}. \tag{5}$$

Тогда функция $f(x) = \sum_{n=0}^{\infty} R(n) x^n$ принимает трансцендентные значения во всех отличных от нуля и корней многочлена $P(x) = \sum_{k=0}^{m-1} u_{m-k} x^k$ алгебраических точках интервала $-1 \leq x < 1$.

Доказательство. Вначале напомним [1, п. 601.1], что для всех действительных значений x таких, что $-1 \leq x < 1$, выполнено равенство

$$\ln(1-x) = -\sum_{k=1}^{\infty} \frac{x^k}{k}.$$

Из определения функции $f(x)$ с учетом приведенного равенства получаем

$$f(x) = \sum_{n=0}^{\infty} \sum_{i=1}^{m} \frac{u_i x^n}{n+i} = \sum_{i=1}^{m} u_i \sum_{n=0}^{\infty} \frac{x^n}{n+i} = \sum_{i=1}^{m} u_i x^{-i} \sum_{n=0}^{\infty} \frac{x^{n+i}}{n+i} =$$

$$= \sum_{i=1}^{m} u_i x^{-i} \sum_{k=i}^{\infty} \frac{x^k}{k} = \sum_{i=1}^{m} u_i x^{-i} \left(-\ln(1-x) - \sum_{k=1}^{i-1} \frac{x^k}{k} \right)$$

при $-1 \leq x < 1$. Следовательно, выполнено

$$f(x) = x^{-m} P(x) (S(x^{-1}) - \ln(1-x))$$

для некоторого многочлена $S(t) \in \mathbb{Q}[t]$. Утверждение леммы следует из того, что значения функции $\ln(1-x)$ трансцендентны во всех алгебраических точках, отличных от нуля [11, § 10.1].

Из утверждения леммы следует, что при $x = b^{-1}$, отличном от корней многочлена $P(x)$, действительное число $\alpha = f(b^{-1})$ трансцендентно. Однако в общем случае трансцендентность чисел вида (4) доказать не удается. Мы можем лишь свести равенство (4) к виду

$$\alpha = P(b, s, d, (u_1, \ \dots, u_m)) = \frac{1}{d^s}\sum_{k=1}^{m}\sum_{n=0}^{\infty}\frac{u_k b^{-n}}{(n+\frac{k}{d})^s} = \frac{1}{d^s}\sum_{k=1}^{m} u_k \Phi\left(\frac{1}{b}, s, \frac{k}{d}\right),$$

в котором нами используется функция $\Phi(z, s, \delta) = \sum_{n=0}^{\infty}\frac{z^n}{(n+\delta)^s}$, определенная при $|z| < 1$, $0 < \delta \le 1$. В настоящее время не доказана даже иррациональность суммы $\sum_{n=0}^{\infty}\frac{(-1)^n}{(2n+1)^2}$, называемой постоянной Каталана.

2. Разложения чисел

Пусть иррациональное число α задано равенством (2). Самый простой способ разложения α по основанию b заключается в следующем. Определим начальное значение $\delta_{-1} = 0$ и последовательность величин

$$\alpha_n = \delta_{n-1}b + R(n), \quad a_n = \lfloor \alpha_n \rfloor, \quad \delta_n = \alpha_n - a_n, \quad n = 0,\ 1,\ \dots, \tag{6}$$

а также частичную сумму

$$s_k = \sum_{n=0}^{k} a_n b^{-n}, \quad k = 0,\ 1,\ \dots.$$

Верна следующая лемма.

Лемма 3. *Для введенных в (6) коэффициентов a_n, $n = 0,\ 1,\ \dots$ выполнено равенство $\alpha = \sum_{n=0}^{\infty} a_n b^{-n}$. Более того,*

$$\alpha - s_k = b^{-k}\left(\delta_k + \sum_{n=1}^{\infty} R(n+k) b^{-n}\right). \tag{7}$$

Доказательство. Зафиксируем произвольный индекс $n > 0$, тогда из (6) следует равенство

$$\frac{\alpha_n}{b^n} = \frac{\alpha_{n-1} - a_{n-1}}{b^{n-1}} + \frac{R(n)}{b^n} \quad \text{или} \quad \frac{\alpha_{n-1}}{b^{n-1}} - \frac{\alpha_n}{b^n} = \frac{a_{n-1}}{b^{n-1}} - \frac{R(n)}{b^n}.$$

Просуммируем полученные равенства для всех $n = 1,\ 2,\ \dots$ и получим

$$\alpha_0 = \sum_{n=0}^{\infty} a_n b^{-n} - \sum_{n=1}^{\infty} R(n) b^{-n}.$$

Поскольку $\alpha_0 = R(0)$ и ряд $\sum_{n=0}^{\infty} R(n) b^{-n}$ сходится, получим искомое равенство.

Для доказательства второго утверждения леммы заметим, что $R(n) - a_n = \delta_n - \delta_{n-1}b$. Пользуясь этими равенствами, находим

$$\alpha - s_k = \sum_{n=0}^{k}(R(n) - a_n)b^{-n} + \sum_{n=k+1}^{\infty} R(n)b^{-n} = \sum_{n=0}^{k}(\delta_n b^{-n} - \delta_{n-1}b^{-n+1}) + \sum_{n=1}^{\infty} R(n+k)b^{-n} =$$

$$= \delta_k b^{-k} + b^{-k}\sum_{n=1}^{\infty} R(n+k) b^{-n}.$$

Лемма доказана.

Отметим, что равенства (6) не дают нам окончательное представление числа α в виде (1). Действительно, пусть n_0 индекс такой, что $R(n_0) < 1$, тогда для всех $n \ge n_0$ выполнено неравенство

$$a_n = \lfloor \alpha_n \rfloor \le \alpha_n = \delta_{n-1} b + R(n) < b + 1,$$

т.е. коэффициенты a_n, вычисленные в соответствии с равенствами (6), удовлетворяют неравенствам $a_n \le b$. Для получения точного равенства (1) необходимо скорректировать полученные значения: если для некоторого индекса n величина $a_n = b$, то необходимо определить $a_n = 0$ и $a_{n-1} = a_{n-1}+1$, продолжая коррекцию далее, если оказалось, что $a_{n-1} = b$ и т.д.

Введем обозначение для бесконечных сумм, возникающих в равенстве (7), а именно:

$$\gamma_k = \sum_{n=1}^{\infty} R(n+k) b^{-n}. \tag{8}$$

В формулировке следующей леммы фигурные скобки будут обозначать дробную часть числа.

Лемма 4. *Последовательность величин γ_k, $k = 0,\ 1,\ \ldots$, определенная равенством (8), удовлетворяет следующим условиям.*

(1) *Выполнено равенство* $\{\alpha b^k\} = \{\delta_k + \gamma_k\}$.
(2) *Выполнено равенство* $\lim_{k\to\infty} \gamma_k = 0$.

Доказательство. Первое утверждение леммы следует из равенства (7). Действительно,

$$\alpha b^k = s_k b^k + \delta_k + \gamma_k, \quad \text{и} \quad s_k b^k = \sum_{n=0}^{k} a_n b^{k-n} \in \mathbb{Z}.$$

Согласно условию, последовательность $R(n)$ стремится к нулю. Поэтому для любого положительного числа ε найдется номер k_0 такой, что для всех $k \ge k_0$ выполняется $R(k) < \varepsilon$. Для таких k имеем

$$\gamma_k = \sum_{n=1}^{\infty} R(n+k) b^{-n} \le \varepsilon \sum_{n=1}^{\infty} b^{-n} = \frac{\varepsilon}{b-1} \le \varepsilon.$$

Это доказывает второе утверждение леммы.

Верно следующее утверждение.

Лемма 5 [4]. *Если последовательность $\delta_0, \delta_1,\ \ldots$ равномерно распределена на интервале* $(0,1)$, *а последовательность $\gamma_0, \gamma_1,\ \ldots$ имеет конечный предел, то последовательность $\{\delta_n + \gamma_n\}_{n=0}^{\infty}$ также является последовательностью равномерно распределенных на интервале* $(0,1)$ *величин.*

Суммируя утверждения лемм 4 и 5, а также теоремы 1, мы получаем, что вопрос о нормальности действительного числа α, определенного равенством (2), сводится к рассмотрению вопроса о равномерном распределении последовательности величин $\delta_0,\ \delta_1, \ldots$. Нормальность числа α, в свою очередь, ведет к равномерному распределению коэффициентов a_n, определяемых равенством (1), на интервале $[0, b-1]$.

3. Результаты практических экспериментов

Основываясь на изложенных выше теоретических результатах, мы предлагаем следующий способ генерации псевдослучайных последовательностей.

Фиксируем значение $b = 256$ и рассмотрим в качестве начальных значений генератора множество различных натуральных чисел $x_1,\ \ldots, x_m$. Определим рациональную функцию $R(n)$ равенством

$$R(n, x_1, \ldots,\ x_m) = \frac{1}{n+x_1} + \cdots + \frac{1}{n+x_m}.$$

Обозначим $w = \max\{x_1, \ldots, x_m\}$. Так как многочлен $P(x) = \sum_{k=1}^{m} x^{M-k_i-1}$ не обращается в нуль в точке 256^{-1}, то, согласно лемме 2, число $\alpha = \sum_{n=0}^{\infty} R(n, x_1,\ \ldots,\ x_m) 256^{-n}$ является трансцендентным. В качестве псевдослучайной последовательности рассмотрим последовательность целых чисел $a_1,\ a_2, \ldots$.

Для проверки гипотезы о нормальности числа α мы выполнили два независимых исследования (для каждого набора величин $x_1,\ \ldots,\ x_m$). Первое заключается в проверке равновероятного распределения величин $\delta_0, \delta_1, \ldots \delta_{N-1}$, принимающих значения на интервале $(0, 1)$. Второе исследование — проверка равномерного распределения элементов последовательности $a_1, a_2, \ldots,\ a_N$. При проведении экспериментов величина N принимала значения 2^{16}, $2 \cdot 10^5$ и 10^6.

***Исследование значений в интервале* $(0, 1)$.** Принятие или отвержение гипотезы о равномерном распределении элементов последовательности $\delta_0, \delta_1, \ldots \delta_{N-1}$ зависит от некоторого параметра — уровня значимости θ. Данная величина задает вероятность отвергнуть гипотезу о равномерном распределении, если она является истинной. Величина θ должна принимать действительные значения, близкие к нулю.

При заданном значении θ мы последовательно применяем следующие критерии согласия:

(1) критерий χ-квадрат с k степенями свободы[6], где величина k определяется равенством $k = 1 + 3.22 \lg N$ [20];
(2) критерий Морана [17];
(3) критерий Шермана [19];
(4) критерий Янга [21],

каждый из которых позволяет принять или опровергнуть гипотезу о равномерном распределении.

Мы принимаем гипотезу о равномерном распределении элементов последовательности $\delta_0, \delta_1, \ldots, \delta_{N-1}$, если все перечисленные выше критерии не отвергли данную гипотезу.

Исследование целых значений. Опишем методику исследования распределения элементов последовательности $a_1,\ a_2,\ \ldots$. Решение о равномерном распределении принимается путем последовательного применения некоторого числа критериев согласия, каждый из которых независимо проверяет гипотезу о равномерном распределении элементов исходной последовательности $a_1,\ a_2,\ \ldots$ на интервале $[0, b-1]$.

Мы рассматриваем каждый критерий как некоторую функцию, на вход которой подается исходная последовательность элементов кольца $\mathbb{Z}_b$. В результате выполнения критерия вычисляется величина p_{value} — действительное число, расположенное между нулем и единицей. Данное число интерпретируется как мера соответствия исследуемых данных гипотезе о равномерном распределении — чем ближе величина p_{value} к единице, тем большее соответствие.

Как и для случая действительных значений, принятие гипотезы о равномерном распределении зависит от уровня значимости θ.

Последовательность действий при проведении анализа исследуемой последовательности $a_1, a_2, \ldots$ заключается в следующем.

(1) Выбирается значение величины уровня значимости θ.

(2) Выполняется частотный тест, вычисляющий частоты появления нулей и единиц в исследуемой последовательности. Если количество единиц не сравнимо с количеством нулей, то исследуемая последовательность признается неравновероятной и дальнейшие исследования не проводятся. Подробное описание частотного теста может быть найдено, например, в [5] или [18].

(3) Последовательно применяются выбранные критерии согласия. Для каждого критерия мы используем два различных подхода.

• *Глобальный подход*, когда заданный критерий согласия применяется ко всей исходной последовательности целиком. В результате применения критерия вычисляется значение p_{value}. Если выполняется неравенство $p_{value} \geq \theta$, то гипотеза о равномерном распределении исходной последовательности принимается. В противном случае гипотеза отвергается.

• *Локальный подход* как более сложная процедура. Исходная последовательность разбивается на подпоследовательности некоторой длины r. Величина r для каждого статистического критерия, как правило, принимает свое собственное значение. Для каждой подпоследовательности независимо применяется выбранный статистический критерий и вычисляется собственное значение величины p_{value}. Далее полученная последовательность действительных значений тестируется описанным выше способом на равновероятное распределение на интервале $(0, 1)$. В случае, если гипотеза о равновероятном распределении последовательности действительных значений не отвергается, то для исходной последовательности также не отвергается гипотеза о равномерном распределении.

Заметим, что в случае, когда применение глобального подхода позволяет отвергнуть гипотезу о равномерном распределении исходной последовательности, локальный подход не применяется.

При проведении исследований применялись следующие статистические критерии согласия:

(1) частотный тест для k-грамм [18];
(2) критерий числа невозрастающих последовательностей;
(3) критерий числа пустых ящиков [3; 10];
(4) критерий линейной сложности [18];
(5) критерий, основанный на свойствах случайных подстановок [2].

Приведенный перечень может быть дополнен другими критериями (см., напр., [5; 6; 18]).

Результаты исследований. При проведении исследований мы фиксировали уровень значимости $\theta = 0.01$. При таком значении θ для всех выбранных нами случайным образом наборов чисел x_1, $\ldots$, x_m при $m = 4$ и $m = 8$ гипотеза о равновероятном распределении последовательности значений $\delta_0,\ \delta_1,\ \ldots,\ \delta_{N-1}$ не отвергалась.

При исследовании последовательности $a_1,\ \ldots,\ a_N$ частотный тест появления единиц и нулей всегда не отвергал гипотезу о равновероятном распределении.

При использовании глобального подхода все перечисленные выше критерии не отвергали гипотезу о равновероятном распределении последовательности $a_1,\ \ldots,\ a_N$.

Однако при использовании локального подхода для значений $N = 2 \cdot 10^5$ и $N = 10^6$ некоторыми критериями была отвергнута гипотеза о равновероятном распределении последовательности значений p_{value}. Указанные значения группировались около фиксированных точек, зависящих от используемого критерия, образовывая непересекающиеся интервалы внутри интервала $(0, 1)$.

С точки зрения статистических исследований, указанное наблюдение позволяет высказать предположение о том, что исследуемая последовательность не является истинно случайной, а выработана при помощи некоторого алгоритма.

Заключение

В настоящей работе мы рассмотрели способ генерации псевдослучайных последовательностей, основанный на представлении некоторого класса трансцендентных чисел в системе счисления по основанию b. Проведенные нами эксперименты показали, что получающиеся последовательности могут рассматриваться как реализация случайной величины, равномерно распределенной на интервале $[0, b-1]$. Это позволяет нам выдвинуть гипотезу о том, что все числа из рассматриваемого нами класса являются нормальными.

Для дальнейших исследований представляется важной задача об определении значений параметров $x_1, \ldots, x_m$ трансцендентного числа α по его рациональному приближению, т.е. по заданному отрезку последовательности $a_0, \ldots, a_r,\ r \geq 1$. Построение алгоритма решения данной задачи и получение оценки его трудоемкости позволило бы обосновать целесообразность использования разработанного нами способа генерации псевдослучайных последовательностей в средствах защиты информации.

Библиографический список

1. *Двайт Г.Б.* Таблицы интегралов и другие математические формулы. М.: Наука, 1983.
2. *Ивченко Г.И., Медведев Ю.И.* Математическая статистика. М.: Высш. шк., 1992.
3. *Идье В., Драйад Д., Джеймс Ф., Рус М., Садуле Б.* Статистические методы в экспериментальной физике. М.: Атомиздат, 1976.
4. *Кейперс Л., Нидеррайтер Г.* Равномерное распределение последовательностей. М.: Наука, 1985.
5. *Кнут Д.* Искусство программирования для ЭВМ. Получисленные алгоритмы. Т. 2. М.: Мир, 1977.

6. *Кобзарь А.И.* Прикладная математическая статистика для инженеров и научных работников. М.: Физматлит, 2006.

7. *Коробов Н.М.* О некоторых вопросах равномерного распределения // Изв. АН СССР. Сер. мат. 1950. Т. 14. С. 215–231.

8. *Нестеренко Ю.В.* Теория чисел. М.: Академия, 2008.

9. *Постников А.Г.* Арифметическое моделирование случайных процессов // Труды МИАН СССР. Т. 57. М.: Изд-во АН СССР, 1960. 84 с.

10. *Сачков В.Н.* Вероятностные методы в комбинаторном анализе. М.: Наука, 1978.

11. *Фельдман Н.И.* Седьмая проблема Гильберта. М.: Изд-во Моск. ун-та, 1982.

12. *Bayley D.H.* A Compendium of BBP-type Formulas for Mathematical Constants. Preprint. 2010. URL: http://crd.lbl.gov/ dhbailey/dhbpapers/bbp-formulas.pdf.

13. *Bailey D.H, Borwein P.B. and Plouffe S.* On The Rapid Computation of Various Polylogarithmic Constants // Mathematics of Computation. 1997. V. 66. № 218. P. 903–913.

14. *Bayley D.H., Crandall R.E.* On the Random Character of Fundamental Constant Expansions // Experimental Mathematics. Jun. 2001. V. 10. № 2. P. 175–190.

15. *Champernowne D.G.* The Construction of the Decimals Normal in the Scale of Ten // J. London Math. Soc. 1933. V. 8. P. 254–260.

16. *Copeland A.H., Erdös P.* Note on Normal Numbers // Bull. Americ. Math. Soc. 1946. V. 52. P. 857–860.

17. *Moran P.A.P.* The Random Division of an Interval // JRSS. 1951. V. 13. P. 147–150.

18. *Rukhin A., Soto J., Nechvatal J., Smid M., Barker E., Leigh S., Levenson M., Vangel M., Banks D., Heckert A., Dray J. and Vo S.* A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800-22, Rev. 1a. 2010.

19. *Sherman B.* A Random Variable Related to the Spacing of Sample Values // AMS. 1950. V. 21. № 3. P. 339–361.

20. *Sturges H.A.* The Choice of a Class Interval // JASA. 1926. V.21. P. 65–66.

21. *Young D.L.* The Linear Nearest Neighbour Statistic // Biometrica. 1982. V. 69. № 2. P. 447–480.

A. YU. NESTERENKO

STATISTICAL PROPERTIES OF SOME TRANSCENDENTAL NUMBERS

We present a new method for generating pseudo random sequences which is based on represenation of real numbers in some numeral systems. We describe an algorithm for generation sequences, present experimental results and methodology of randomness checking.

Key words: ***sequences of random numbers, normal and transcendental numbers, statistical tests.***

10. *Varbanets P.D. and Varbanets S.P.* Inversive congruential generator with a variable shift // Proceedings, 5th Chaotic Modeling and Simulation International Conference, 12 – 15 June 2012, Athens Greece. P. 623–630.

П.Д. ВАРБАНЕЦ, С.П. ВАРБАНЕЦ

ИНВЕРСНЫЙ КОНГРУЭНТНЫЙ ГЕНЕРАТОР С ПЕРЕМЕННЫМ СДВИГОМ

Рассматривается инверсный конгруэнтный генератор с переменным сдвигом, продуцирующий последовательность псевдослучайных чисел (ПСЧ), которая проходит s-мерный сериальный тест на равнораспределенность и непредсказуемость. Найдены представления элементов порождаемой последовательности в виде многочленов от инициального значения исходной рекурсии и номера элемента последовательности. Получены оценки тригонометрических сумм на последовательностях ПСЧ и указаны условия, при которых порождаемая последовательность ПСЧ имеет максимальный период.

Ключевые слова: ***последовательности псевдослучайных чисел, конгруэнтный генератор, дискрепансия, непредсказуемость, тригонометрическая сумма.***

СВЕДЕНИЯ ОБ АВТОРАХ
УКАЗАТЕЛЬ ИМЕН

М.М. Глухов,	доктор физико-математических наук, академик Академии криптографии РФ, профессор Ин-та криптографии, связи и информатики Академии ФСБ России. E-mail: glukhovmm@rambler.ru	11
И.Ш. Джаббаров,	кандидат физико-математических наук, доцент, зав. каф. геометрии и алгебры Гянджинского гос. ун-та (Азербайджан). E-mail: jabbarovish@rambler.ru	80
С. Гонсалес,	доктор, профессор департамента математики Университета Овьедо (Испания). E-mail: santos@uniovi.es	73
Л.П. Добровольская,	кандидат физико-математических наук, доцент каф. бухгалтерского учета, анализа и аудита Тульского ин-та экономики и управления. E-mail: lbocharova6565@mail.ru	90
Н.М. Добровольский,	доктор физико-математических наук, профессор, зав. каф. алгебры, математического анализа и геометрии Тульского гос. пед. ун-та им. Л.Н. Толстого. E-mail: dobrovol@tspu.tula.ru	90
Н.Н. Добровольский,	аспирант каф. прикладной математики и информатики Тульского гос. ун-та. E-mail: nikolai.dobrovolsky@gmail.com	90
В.К. Карташов,	кандидат физико-математических наук, профессор, зав. каф. алгебры и геометрии Волгоградского гос. соц.-пед. ун-та. E-mail: kartashovvk@yandex.ru	99
А.В. Карташова,	кандидат физико-математических наук, доцент каф. алгебры и геометрии Волгоградского гос. соц.-пед. ун-та. E-mail: kartashovaan@yandex.ru	99,106
И.Б. Кожухов,	доктор физико-математических наук, профессор каф. высшей математики 1 Национального исследовательского ун-та «МИЭТ». E-mail: kozhuhov_i_b@mail.ru	45
А.В. Кокорев,	аспирант каф. геометрии и методики преподавания математики Орловского гос. ун-та. E-mail: pears911@mail.ru	114
А.Е. Коротков,	ассистент каф. компьютерной алгебры и теории чисел Саратовского гос. ун-та им. Н.Г. Чернышевского. E-mail: korotkov@info.sgu.ru	118
А.В. Кравченко,	кандидат физико-математических наук, старший научный сотрудник лаборатории логических систем ИМ СО РАН. E-mail: a.v.kravchenko@mail.ru	124
В.М. Кусов,	старший преподаватель каф. алгебры и геометрии Волгоградского гос. соц.-пед. ун-та. E-mail: kvm64@yandex.ru	130
О.А. Малюшева,	студентка 5-го курса ФМиИТ Ульяновского гос. ун-та. E-mail: malyusheva_o_a@mail.ru	136
В.Т. Марков,	кандидат физико-математических наук, доцент каф. высшей алгебры МГУ им. М.В. Ломоносова. E-mail: vtmarkov@mech.math.msu.su	73
О.В. Маркова,	кандидат физико-математических наук, научный сотрудник лаборатории компьютерных учебников Центра новых информационных технологий МГУ им. М.В. Ломоносова. E-mail: ov_markova@mail.ru	145
К. Мартинес,	доктор, профессор департамента математики Университета Овьедо (Испания). E-mail: cmartinez@uniovi.es	73
О.А. Матвеева,	студентка Саратовского гос. ун-та им. Н.Г. Чернышевского. E-mail: olga.matveeva.0@gmail.com	153
Е.В. Мещерина,	аспирант каф. алгебры и математической кибернетики Оренбургского гос. ун-та. E-mail: elena_lipilina@mail.ru	156
С.П. Мищенко,	доктор физико-математических наук, профессор, зав. каф. алгебро-геометрических вычислений Ульяновского гос. ун-та. E-mail: mishchenkosp@mail.ru	136
В.А. Молчанов,	доктор физико-математических наук, профессор каф. теоретических основ компьютерной безопасности и криптографии Саратовского гос. ун-та им. Н.Г. Чернышевского. E-mail: v.molchanov@inbox.ru	163
А.Ю. Нестеренко,	кандидат физико-математических наук, доцент каф. компьютерной безопасности МИЭМ НИУ ВШЭ. E-mail: anesterenko@hse.ru	170

А.А. Нечаев,	доктор физико-математических наук, профессор, ведущий научный сотрудник Центра новых информационных технологий МГУ им. М.В. Ломоносова. E-mail: alexnechaev@inbox.ru	73
Н.К. Огородничук,	аспирант каф. алгебры, математического анализа и геометрии Тульского гос. пед. ун-та им. Л.Н. Толстого. E-mail: nadj_nadj@mail.ru	90
У.М. Пачев,	доктор физико-математических наук, профессор каф. геометрии и высшей алгебры Кабардино-Балкарского гос. ун-та. E-mail: urusbi@rambler.ru	177
А.А. Петров,	аспирант каф. алгебры и дискретной математики Вятского гос. гуманит. ун-та. E-mail: andreipetrow.ru	60
А.Г. Пинус,	доктор физико-математических наук, профессор каф. алгебры и математической логики Новосибирского гос. техн. ун-та. E-mail: ag.pinus@gmail.com	182
С.А. Пихтильков,	доктор физико-математических наук, профессор каф. алгебры и математической кибернетики Оренбургского гос. ун-та. E-mail: pikhtilkov@mail.ru	156
О.А. Пихтилькова,	кандидат физико-математических наук, доцент каф. математического анализа Оренбургского гос. ун-та. E-mail: opikhtilkova@mail.ru	156
А.Л. Расстригин,	аспирант каф. алгебры и геометрии Волгоградского гос. соц.-пед. ун-та. E-mail: rasal@fizmat.vspu.ru	190
З.Х. Рахмонов,	доктор физико-математических наук, профессор, чл.-кор. АН Республики Таджикистан, директор Ин-та математики АН Республики Таджикистан. E-mail: zarullo-r@rambler.ru	194
Е.Д. Ребров,	аспирант каф. теории чисел Московского пед. гос. ун-та. E-mail: pilot87@mail.ru	90
И.Ю. Реброва,	кандидат физико-математических наук, доцент, декан факультета математики, физики и информатики Тульского гос. пед. ун-та им. Л.Н. Толстого. E-mail: i_rebrova@mail.ru	90
Т.В. Скорая,	кандидат физико-математических наук, старший преподаватель каф. алгебро-геометрических вычислений Ульяновского гос. ун-та. E-mail: skorayatv@yandex.ru	203
П.В. Снурницын,	кандидат физико-математических наук, инженер МГУ им. М.В. Ломоносова. E-mail: snurnitsyn@gmail.com	212
С.В. Сыроватская,	аспирант каф. алгебры и геометрии Волгоградского гос. соц.-пед. ун-та. E-mail: svs_kagi@mail.ru	216
Х.Х. Усманов,	кандидат физико-математических наук, доцент, зав. каф. высшей математики Волжского филиала Национального исследовательского ун-та «МЭИ». E-mail: vfmei@vfmei.ru	219
В.Л. Усольцев,	кандидат физико-математичеких наук, доцент каф. информатики и информатизации образования Волгоградского гос. соц.-пед. ун-та. E-mail: usl2004@mail.ru	229
Ю.Ю. Фролова,	кандидат физико-математичеких наук, старший преподаватель каф. алгебро-геометрических вычислений Ульяновского гос. ун-та. E-mail: yuyufrolova@mail.ru	136
А.А. Хусаинов,	доктор физико-математических наук, профессор каф. математического обеспечения и применения ЭВМ Комсомольского-на-Амуре гос. техн. ун-та. E-mail: husainov51@yandex.ru	237
Д.С. Чистяков,	кандидат физико-математических наук, докторант каф. алгебры Московского пед. гос. ун-та. E-mail: chistyakovds@yandex.ru	244
В.Н. Чубариков,	доктор физико-математических наук, профессор, зав. каф. математических и компьютерных методов анализа МГУ им. М.В. Ломоносова. E-mail: chubarik1@mech.math.msu.su	5
А.В. Шутов,	кандидат физико-математических наук, доцент каф. информатики и информационных технологий в образовании Владимирского гос. ун-та им. А.Г. и Н.Г. Столетовых. E-mail: a1981@mail.ru	249
Н.А. Щучкин,	кандидат физико-математических наук, доцент каф. алгебры и геометрии Волгоградского гос. соц.-пед. ун-та. E-mail: nikolaj_shchuchkin@mail.ru	68,130,254

V. Garbaliauskienė,	доктор (dr.) математики, доцент каф. математики Шяуляйского ун-та (Литва). E-mail: vgarbaliauskiene@gmail.com	260
A. Laurinčikas,	габилитированный доктор (habil.dr.), профессор каф. теории вероятностей и теории чисел Вильнюсского ун-та (Литва). E-mail: antanas.laurincikas@mif.vu.lt	260
R. Macaitienė,	доктор математики, доцент каф. математики Шяуляйского ун-та (Литва). E-mail: renata.macaitiene@mi.su.lt	260
D. Šiaučiūnas,	доктор математики, доцент, профессор каф. математики Шяуляйского ун-та (Литва). E-mail: siauciunas@fm.su.lt	260
P.D. Varbanets,	доктор физико-математических наук, профессор, зав. каф. компьютерной алгебры и дискретной математики Одесского национального ун-та им. И.И. Мечникова (Украина). E-mail: varb@sana.od.ua	266
S.P. Varbanets,	кандидат физико-математических наук, доцент каф. компьютерной алгебры и дискретной математики Одесского национального ун-та им. И.И. Мечникова (Украина). E-mail: varb@sana.od.ua	266

РЕДАКЦИОННО-ИЗДАТЕЛЬСКАЯ КОЛЛЕГИЯ

РЕДАКЦИОННО-ИЗДАТЕЛЬСКАЯ КОЛЛЕГИЯ СЕРИИ

УЧЕНЫЕ ЗАПИСКИ
ОРЛОВСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА

НАУЧНЫЙ ЖУРНАЛ

СЕРИЯ «ЕСТЕСТВЕННЫЕ, ТЕХНИЧЕСКИЕ И МЕДИЦИНСКИЕ НАУКИ»

№ 6

Часть 2

Свидетельство о регистрации СМИ ПИ № ФФС 77-29955 от 17.10.2007.
Включен в каталог «Издания органов НТИ» ОАО «Агентство “Роспечать”»
(почтовый индекс: 66005)

Оригинал-макет подготовили:
А.П. Бощенко, О. И. Молоканова, Ю.А. Антюфеева

Подписано в печать 19.10.2012 г. Формат 60x84 $^{1}/_{8}$. Бумага офс.
Усл. печ. л. 25,0. Тираж 1000 экз. Заказ № 530.

Издательство ВГСПУ «Перемена»
Типография Издательства ВГСПУ «Перемена»
400131, Волгоград, пр. им. В. И. Ленина, 27